A Verified Decision Procedure for Univariate Real Arithmetic with the BKR Algorithm

Katherine Cordwell, Yong Kiam Tan, and André Platzer

Carnegie Mellon University

This material is based upon work supported by the NSF under Grant No. CNS-1739629, the NSF Graduate Research Fellowship Program under Grants Nos. DGE1252522 and DGE1745016, by A*STAR Singapore, and by the AFOSR under grant number FA9550-16-1-0288. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF, AFOSR, or A*STAR Singapore.

Problem

- Real arithmetic questions involving the **∃ (exists) and ∀ (for all) quantifiers** (ranging over the reals) are difficult for computers
- **Quantifier elimination (QE)**: The process of transforming a quantified statement into a ***logically equivalent*** quantifier-free statement

Examples

Example

$$\forall x.\ x^2 + 1 > 0$$

QE

True

Example*

$$\forall x \forall y.\ ((x^2 + ay^2 \leq 1) \Rightarrow (ax^2 - a^2xy + 2 \geq 0))$$

QE

$$(a \geq 0) \text{ and } (a^3 - 8a - 16 \leq 0)$$

QE is identifying exactly what conditions on a will make the original formula true!

*This example is taken from some of Pablo Parrilo's lecture notes (Lecture 18 of his 2006 course, "Algebraic Techniques and Semidefinite Optimization"). Accessible through his webpage: https://www.mit.edu/~parrilo/index.html

A Miraculous Result

- Algorithms for QE exist (Tarski, 1930)
- Algorithms for QE are complicated

Alfred Tarski

Terminology

- **Formulas:** Conjunctions and disjunctions of polynomial inequalities and equations (with rational coefficients)
- If a formula in a QE problem involves only one variable, we call it a **univariate** QE problem. Else it is a **multivariate** QE problem
- **Decision problems** are problems where all variables are quantified

Examples, Revisited

Example

$\forall x.\ x^2 + 1 > 0$

$\Downarrow$ **QE**

True

A univariate decision problem

Example*

$$\forall x \forall y.\ ((x^2 + ay^2 \leq 1) \Rightarrow (ax^2 - a^2xy + 2 \geq 0))$$

$\Downarrow$ **QE**

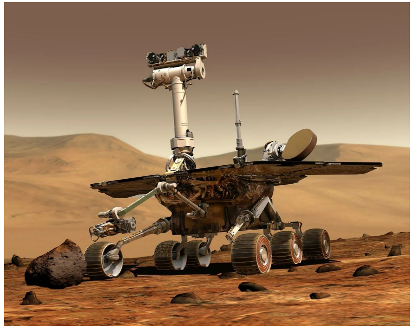
$$(a \geq 0) \text{ and } (a^3 - 8a - 16 \leq 0)$$

A multivariate QE question
***Not* a decision problem**

*This example is taken from some of Pablo Parrilo's lecture notes (Lecture 18 of his 2006 course, "Algebraic Techniques and Semidefinite Optimization"). Accessible through his webpage: https://www.mit.edu/~parrilo/index.html

Motivation

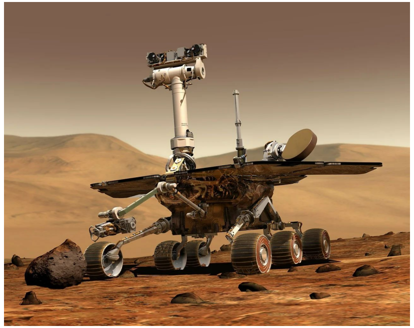
- Quantified statements arise in a number of applications
  - Geometry proofs
  - Stability analysis
  - Verification of cyber-physical systems (like robots!)



For more information, see:
Sturm, T. A Survey of Some Methods for Real Quantifier Elimination, Decision, and Satisfiability and Their Applications. *Math.Comput.Sci.* 11, 483–502 (2017).

Motivation

- Quantified statements arise in a number of applications
  - Geometry proofs
  - Stability analysis
  - Verification of cyber-physical systems (like robots!)
- Two conclusions
  - We want to know how to do QE
  - We want to be sure that we know how to do QE **correctly**

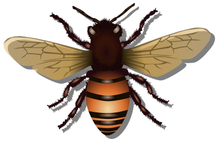


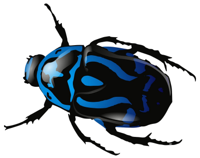
Motivation

- **What we want:** Formally verified QE algorithms

Motivation

- **What we want:** Formally verified QE algorithms
- **Problem:** Dearth of efficient verified QE support
  - CPS theorem prover KeYmaera X outsources QE to unverified software
  - This can introduce bugs





Related Work

✓ = YES

✗ = NO

■ = IN BETWEEN

	Efficient?	Verified?	Multivariate case builds directly on univariate?
Cohen-Hörmander	✗	✓	✓
Tarski	✗	✓	✓
CAD	✓	■	✗

Related Work

✓ = YES

✗ = NO

= IN BETWEEN

	Efficient?	Verified?	Multivariate case builds directly on univariate?
Cohen-Hörmander	✗	✓	✓
Tarski	✗	✓	✓
CAD	✓		✗
BKR & Renegar Potential sweet spot!		✗	✓

BKR and Renegar

- Originally BKR* was a decision procedure
- Renegar** extended BKR to a general-purpose QE algorithm
  - Explains BKR in more detail
  - Fixes an error in BKR's multivariate complexity analysis

*Michael Ben-Or, Dexter Kozen, and John H. Reif. The complexity of elementary algebra and geometry. *J. Comput. Syst. Sci.,* 32(2):251-264, 1986.

**James Renegar. On the computational complexity and geometry of the first-order theory of the reals, part III: quantifier elimination. *J. Symb. Comput.,* 13(3):329-352,1992.

We formally verify* the univariate cases of BKR and Renegar in Isabelle/HOL.

*Available on the Archive of Formal Proofs at:
https://www.isa-afp.org/entries/BenOr_Kozen_Reif.html

High-level Context

- ~7000 LOC
  - Algorithm: ~110 LOC
  - Matrix library extensions: ~1800 LOC

High-level Context

- ~7000 LOC
    - Algorithm: ~110 LOC
    - Matrix library extensions: ~1800 LOC
- Why Isabelle/HOL?
    - Well-suited to formalizing mathematics
    - Strong math libraries
    - Sledgehammer

Univariate BKR: Bird's Eye View

- Transform the problem:
    1. Decision problems to sign determination
    2. Sign determination to restricted sign determination
    3. To solve restricted sign determination, set up a matrix equation.

The main formalization challenge

Step 1: Decision to Sign Determination

- Solve decision problems by finding the ***consistent sign assignments (CSAs)*** for a set of polynomials (sign determination)

Definition (sign assignment for $\{g_1, \ldots, g_n\}$). A mapping $\sigma: \{g_1, \ldots, g_n\} \to \{+, -, 0\}$
σ is **consistent** if there is a real x where, for all i, the sign of $g_i(x)$ matches $\sigma(g_i)$.

Step 1: Decision to Sign Determination

- Solve decision problems by finding the ***consistent sign assignments (CSAs)*** for a set of polynomials (sign determination)

Decision Problem:
$\exists x. (x^2+1 \geq 0 \land 3x < 0)$

Find all consistent sign assignments for $x^2 + 1$ and $3x$

CSAs: (+, -), (+, 0), (+, +)

CSA (+, -) indicates the existence of a point k with $(k^2+1 \geq 0 \land 3k < 0)$

Correctness Results for Step 1

```
theorem decision_procedure:
  "(∀x::real. fml_sem fml x) ⟷ decide_universal fml"
  "(∃x::real. fml_sem fml x) ⟷ decide_existential fml"
```

Canonical semantics for formulas (defines what it means for a formula to hold at x in the standard way)

Our algorithms

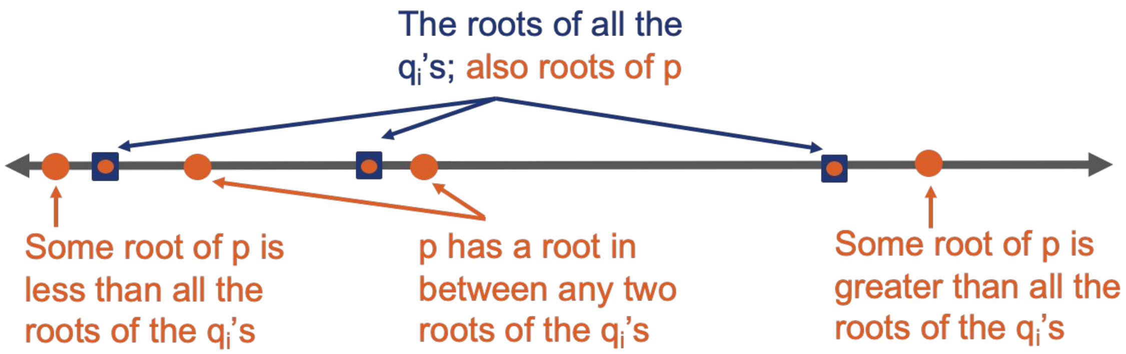
Step 2: Restricted Sign Determination

- Restrict sign determination to finding all **CSAs** for a set of polynomials $\{q_1, \ldots, q_n\}$ ***at the roots of*** an auxiliary nonzero polynomial p

Technical detail: BKR imposes some conditions on $\{q_1, \ldots, q_n\}$, p

Step 2: Restricted Sign Determination

- Restrict sign determination to finding all **CSAs** for a set of polynomials $\{q_1, \ldots, q_n\}$ ***at the roots of*** an auxiliary nonzero polynomial p



Correctness Results for Step 2

```
definition roots :: "real poly ⇒ real set" where "roots p = {x. poly p x = 0}"

definition consistent_signs_at_roots :: "real poly ⇒ real poly list ⇒ rat list set"
where "consistent_signs_at_roots p qs = (sgn_vec qs) ‘ (roots p)"
```

Plug in the roots to the q_i's, take the resulting signs

Solve for the roots of a polynomial

Correctness Results for Step 2

```
definition roots :: "real poly ⇒ real set" where "roots p = {x. poly p x = 0}"

definition consistent_signs_at_roots :: "real poly ⇒ real poly list ⇒ rat list set"
where "consistent_signs_at_roots p qs = (sgn_vec qs) ` (roots p)"

theorem find_consistent_signs_at_roots:
assumes "p ≠ 0"
assumes "⋀q. q ∈ set qs ⟹ coprime p q"
shows "set (find_consistent_signs_at_roots p qs) = consistent_signs_at_roots p qs"
```

our (constructive) algorithm

the nonconstructive definition

Step 3: The Matrix Equation

- Stores all relevant information for sign determination
- Idea dates back to Tarski; similarities to Cohen and Mahboubi's formalization*
- But BKR does it efficiently

Alfred Tarski

*Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination. Log. Methods Comput. Sci., 8(1), 2012. doi:10.2168/ LMCS-8(1:2)2012.

Step 3: The Matrix Equation

Find sign assignments to $q_1, \ldots, q_n$ at the roots of p

Tarski

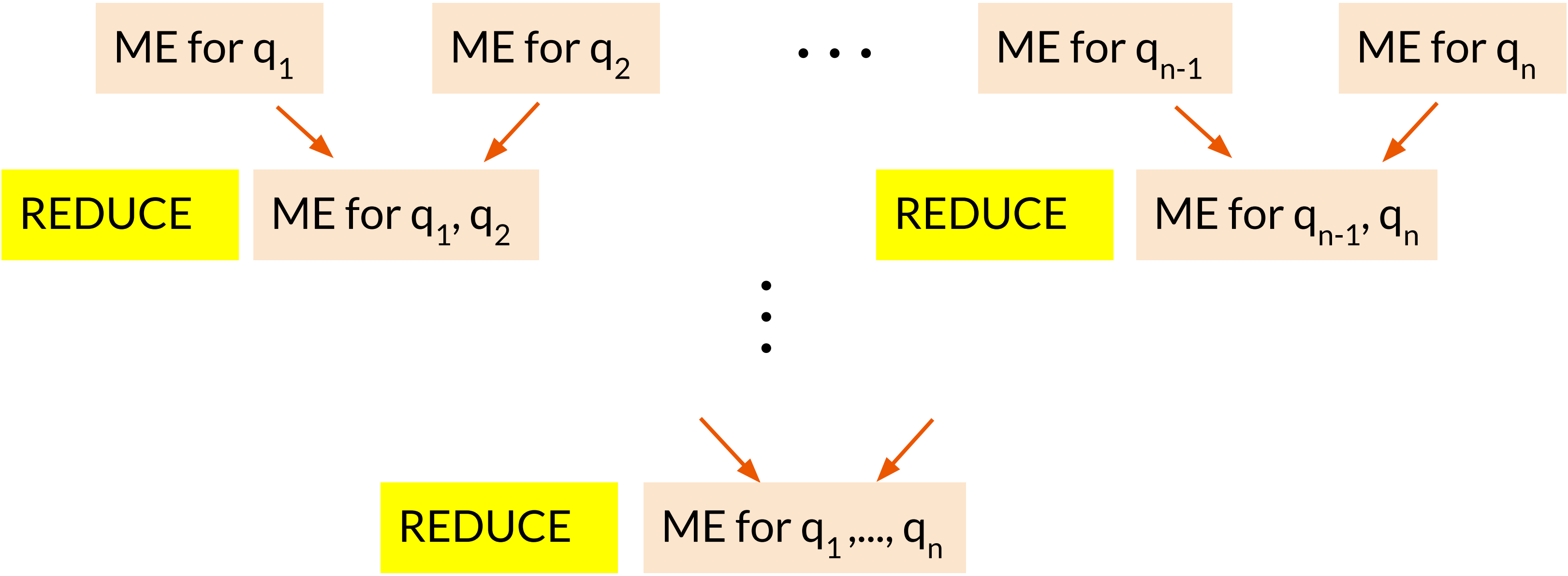
TQ stands for "Tarski query", refers to invoking the (computational) Sturm-Tarski theorem

$$\begin{pmatrix} \#\text{ of } (+,\ldots,+,+) \\ \#\text{ of } (+,\ldots,+,-) \\ \vdots \\ \#\text{ of } (-,\ldots,-,-) \end{pmatrix} = M^{-1} * \begin{pmatrix} \text{TQ subset } 1 \\ \text{TQ subset } 2 \\ \vdots \\ \text{TQ subset } 2^n \end{pmatrix}$$

Invertible matrix
Size 2^n x 2^n
Can be computed

Step 3: The Matrix Equation

Find sign assignments to $q_1, \dots, q_n$ at the roots of p
BKR builds its matrix equation (ME) inductively



Step 3: The Matrix Equation

After each combination, remove all inconsistent sign assignments **(reduction step)**

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 1 \\ -1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix}$$

Signs: ++, + - , - +, --

Signs: ++, + - , - +

Reflections on Formalizing the Matrix Equation

- Inductive construction, inductive proof!
  - It took some work to identify the right inductive invariant
  - The reduction step poses the biggest challenge
- The reduction step requires extra proofs

*Wenda Li. The Sturm-Tarski theorem. Archive of Formal Proofs, September 2014. https://isa-afp.org/entries/Sturm_Tarski.html, Formal proof development.

Reflections on Formalizing the Matrix Equation

- Isabelle/HOL has well-developed libraries
  - The Sturm-Tarski theorem is already formalized* (the key computational tool for the matrix equation)
  - A number of linear algebra libraries are available

*Wenda Li. The Sturm-Tarski theorem. Archive of Formal Proofs, September 2014. https://isa-afp.org/entries/Sturm_Tarski.html, Formal proof development.

Extending the Matrix Libraries

- We build on a matrix library by Thiemann and Yamada*
- Our additions (~1800 LOC):
  - A computational notion of the Kronecker product
  - An algorithm to extract a basis from the rows of a matrix
    - Involved proving that row rank equals column rank

*Rene Theimann and Akihisa Yamada. Matrices, Jordan normal forms, and spectral radius theory. *Archive of Formal Proofs,* August 2015.

Code Export and Experiments

Experiments with SML code

- We export our formally verified algorithm to SML for experimentation
- Compare to:
  - A naive (unverified) version of Tarski's algorithm
  - Li, Passmore, and Paulson*

*Wenda Li, Grant Olney Passmore, and Lawrence C. Paulson. Deciding univariate polynomial problems using untrusted certificates in Isabelle/HOL. J. Autom. Reason., 62(1):69–91, 2019.

Experiments with SML code

- We export our formally verified algorithm to SML for experimentation
- Compare to:
  - A naive (unverified) version of Tarski's algorithm
  - Li, Passmore, and Paulson*
- Li et. al is faster:
  - CAD is generally faster than BKR
  - Their procedure is highly optimized
  - They use Mathematica as an untrusted oracle

*Wenda Li, Grant Olney Passmore, and Lawrence C. Paulson. Deciding univariate polynomial problems using untrusted certificates in Isabelle/HOL. J. Autom. Reason., 62(1):69–91, 2019.

Experiments with SML code

*Compiled with mlton
*Run on a laptop
*Dashes indicate timeout
*Times in seconds

Benchmarks from [18]

Formula	#Poly	$\#N(p,q)$ (Naive)	$\#N(p,q)$ (BKR)	Time (Naive)	Time (BKR)	Time ([18])
ex1	4 (12)	20	31	0.003	0.006	3.020
ex2	5 (6)	576	180	5.780	0.442	3.407
ex3	4 (22)	112	120	1794.843	1865.313	3.580
ex4	5 (3)	112	95	0.461	0.261	3.828
ex5	8 (3)	576	219	28.608	8.333	3.806
ex6	22 (9)	50331648	-	-	-	6.187
ex7	10 (12)	6144	-	-	-	-
ex1 $\wedge$ 2	9 (12)	2816	298	317.432	3.027	3.033
ex1 $\wedge$ 2 $\wedge$ 4	13 (12)	28672	555	-	51.347	3.848
ex1 $\wedge$ 2 $\wedge$ 5	16 (12)	131072	826	-	436.575	3.711

3s startup time for Mathematica

[18] Wenda Li, Grant Olney Passmore, and Lawrence C. Paulson. Deciding univariate polynomial problems using untrusted certificates in Isabelle/HOL. J. Autom. Reason., 62(1):69–91, 2019.

Experiments with SML code

*Compiled with mlton
*Run on a laptop
*Dashes indicate timeout
*Times in seconds

Formula	#Poly	$\#N(p,q)$ (Naive)	$\#N(p,q)$ (BKR)	Time (Naive)	Time (BKR)	Time ([18])
ex1	4 (12)	20	31	0.003	0.006	3.020
ex2	5 (6)	576	180	5.780	0.442	3.407
ex3	4 (22)	112	120	1794.843	1865.313	3.580
ex4	5 (3)	112	95	0.461	0.261	3.828
ex5	8 (3)	576	219	28.608	8.333	3.806
ex6	22 (9)	50331648	-	-	-	6.187
ex7	10 (12)	6144	-	-	-	-
ex1 $\wedge$ 2	9 (12)	2816	298	317.432	3.027	3.033
ex1 $\wedge$ 2 $\wedge$ 4	13 (12)	28672	555	-	51.347	3.848
ex1 $\wedge$ 2 $\wedge$ 5	16 (12)	131072	826	-	436.575	3.711

[18] Wenda Li, Grant Olney Passmore, and Lawrence C. Paulson. Deciding univariate polynomial problems using untrusted certificates in Isabelle/HOL. J. Autom. Reason., 62(1):69–91, 2019.

Experiments with SML code

*Compiled with mlton
*Run on a laptop
*Dashes indicate timeout
*Times in seconds

Formula	#Poly	$\#N(p,q)$ (Naive)	$\#N(p,q)$ (BKR)	Time (Naive)	Time (BKR)	Time ([18])
ex1	4 (12)	20	31	0.003	0.006	3.020
ex2	5 (6)	576	180	5.780	0.442	3.407
ex3	4 (22)	112	120	1794.843	1865.313	3.580
ex4	5 (3)	112	95	0.461	0.261	3.828
ex5	8 (3)	576	219	28.608	8.333	3.806
ex6	22 (9)	50331648	-	-	-	6.187
ex7	10 (12)	6144	-	-	-	-
ex1 $\wedge$ 2	9 (12)	2816	298	317.432	3.027	3.033
ex1 $\wedge$ 2 $\wedge$ 4	13 (12)	28672	555	-	51.347	3.848
ex1 $\wedge$ 2 $\wedge$ 5	16 (12)	131072	826	-	436.575	3.711

[18] Wenda Li, Grant Olney Passmore, and Lawrence C. Paulson. Deciding univariate polynomial problems using untrusted certificates in Isabelle/HOL. J. Autom. Reason., 62(1):69–91, 2019.

Future Work and Conclusion

Future Work

- Optimizing univariate BKR
  - Add parallelism
  - Optimize Tarski queries
- Formally verified complexity analysis (ambitious!)
- Formalizing multivariate BKR

Conclusion

- We have formally verified the univariate case of BKR’s QE algorithm
    - BKR hits a potential **sweet spot** in between practicality and ease of verification
    - Contributes to Isabelle/HOL’s matrix libraries
    - Export code to SML for faster runtime
- Multivariate BKR is ongoing work

Conclusion

- We have formally verified the univariate case of BKR's QE algorithm
  - BKR hits a potential **sweet spot** in between practicality and ease of verification
  - Contributes to Isabelle/HOL's matrix libraries
  - Export code to SML for faster runtime
- Multivariate BKR is ongoing work

$\exists$ Questions?