Real World Verification

André Platzer[1] Jan-David Quesel[2] Philipp Rümmer[3]

[1]Carnegie Mellon University, Computer Science Department

[2]University of Oldenburg, Department of Computing Science

[3]Oxford University Computing Laboratory

22nd International Conference on Automated Deduction
7 August 2009

Outline

Motivation, real world applications

Survey of real world methods

New procedure:

- Gröbner bases for the Real Nullstellensatz
- decides quantifier-free real arithmetic

Empirical evaluation:

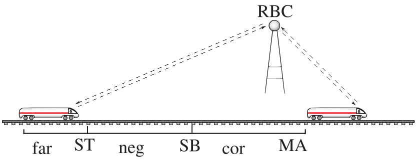
- Comparison of various decision procedures for real arithmetic

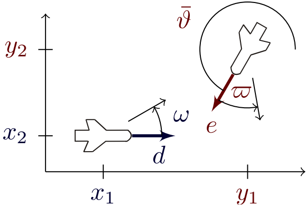
Conclusion

Motivation + applications

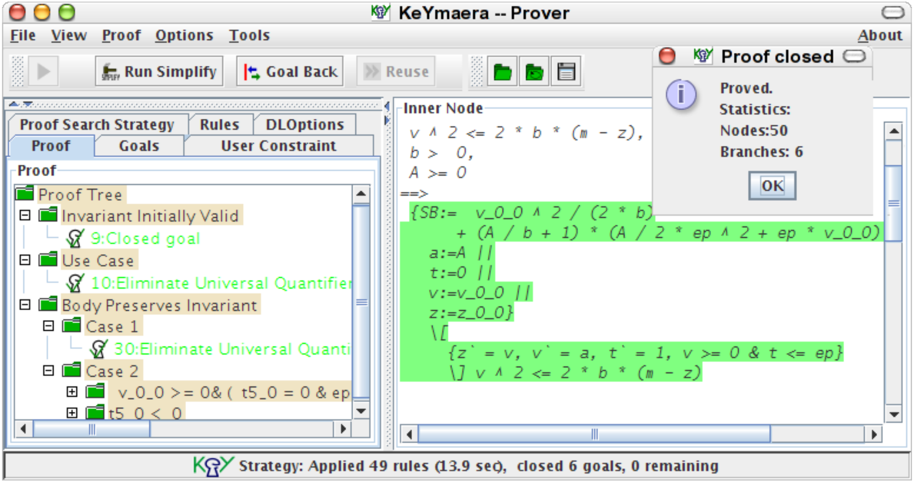
Verification in the KeYmaera system:

- Hybrid systems
- Mathematical algorithms in real or floating-point arithmetic
- Geometric problems

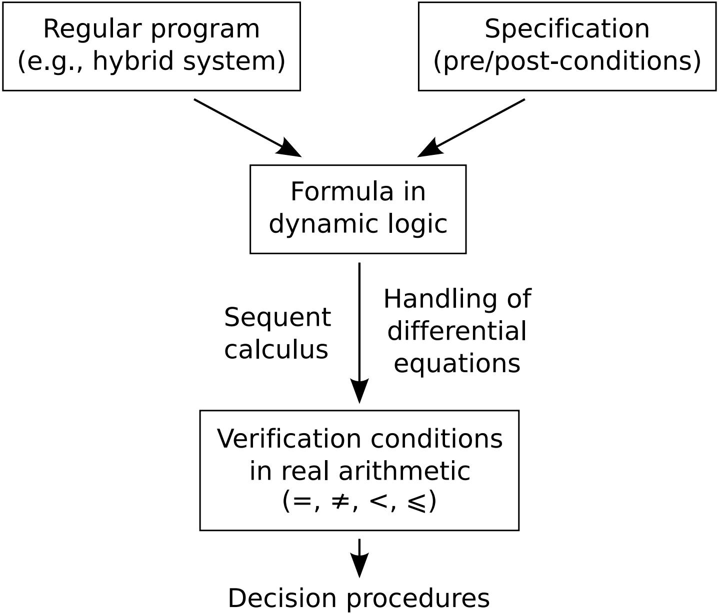




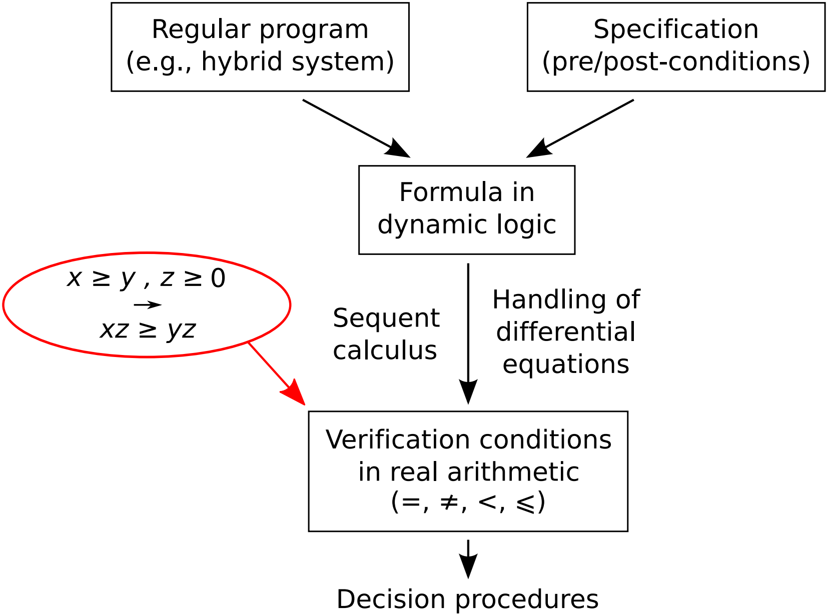
KeYmaera


KeYmaera -- Prover
File View Proof Options Tools About
Run Simplify
Goal Back
Reuse
Proof Search Strategy
Rules
DLOptions
Proof
Goals
User Constraint
Proof
Proof Tree
Invariant Initially Valid
9:Closed goal
Use Case
10:Eliminate Universal Quantifier
Body Preserves Invariant
Case 1
30:Eliminate Universal Quanti
Case 2
v_0_0 >= 0& (t5_0 = 0 & ep
t5_0 < 0
Inner Node
v ^ 2 <= 2 * b * (m - z),
b > 0,
A >= 0
==>
{SB:= v_0_0 ^ 2 / (2 * b)
+ (A / b + 1) * (A / 2 * ep ^ 2 + ep * v_0_0)
a:=A ||
t:=0 ||
v:=v_0_0 ||
z:=z_0_0}
\[
{z` = v, v` = a, t` = 1, v >= 0 & t <= ep}
\] v ^ 2 <= 2 * b * (m - z)
Proof closed
Proved.
Statistics:
Nodes:50
Branches: 6
OK
Strategy: Applied 49 rules (13.9 sec), closed 6 goals, 0 remaining

Overall verification approach



Overall verification approach



Short history of symbolic methods in real arithmetic

1930	First quantifier elimination procedure by Tarski (Non-elementary)
1965	Buchberger introduces Gröbner bases
1973	Real Nullstellensatz and Positivstellensatz by Stengle
1975	Cylindrical algebraic decomposition (CAD) by Collins (Doubly exponential)
1983	Cohen-Hörmander elimination procedure
2003	Parrilo introduces semidefinite programming for the Positivstellensatz (Later refined by Harrison)
2005	Tiwari's polynomial simplex method

Short history of symbolic methods in real arithmetic

1930 First quantifier elimination procedure by Tarski
(Non-elementary)

1965 Buchberger introduces Gröbner bases

1973 Real Nullstellensatz and Positivstellensatz by Stengle

1975 Cylindrical algebraic decomposition (CAD) by Collins
(Doubly exponential)

1983 Cohen-Hörmander elimination procedure

2003 Parrilo introduces semidefinite programming for the Positivstellensatz
(Later refined by Harrison)

2005 Tiwari's polynomial simplex method

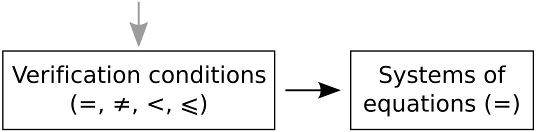
Gröbner bases for quantifier-free real arithmetic

Verification conditions
(=, ≠, <, ⩽)

Gröbner bases for quantifier-free real arithmetic

Inequalities and disequations can be eliminated:

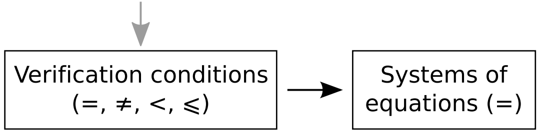
$$
\begin{aligned}
f \neq g &\equiv \exists z.\ (f-g)z = 1 \\
f \geq g &\equiv \exists z.\ f-g = z^2 \\
f > g &\equiv \exists z.\ (f-g)z^2 = 1
\end{aligned}
$$



Gröbner bases for quantifier-free real arithmetic

Goal: prove unsatisfiability of:

$$\bigwedge_i t_i = 0$$

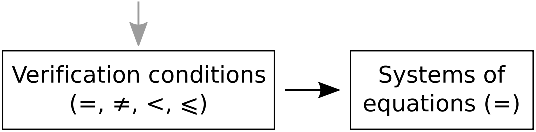


Gröbner bases for quantifier-free real arithmetic

Witnesses for unsatisfiability:

$$\Big(\sum_i s_i t_i\Big) = 1 \quad \Longrightarrow \quad \bigwedge_i t_i = 0 \ \text{ unsatisfiable}$$

How to determine coefficients s_i?



Gröbner bases for quantifier-free real arithmetic

Witnesses for unsatisfiability:

$$\Big(\sum_i s_i t_i\Big) = 1 \quad \Longrightarrow \quad \bigwedge_i t_i = 0 \text{ unsatisfiable}$$

How to determine coefficients s_i?

Need some more notation:

- Ideal generated by $\{t_1, \ldots, t_n\} \subseteq \mathbb{Q}[X_1, \ldots, X_n]$:

$$(t_1, \ldots, t_n) \;=\; \Big\{ \sum_i s_i t_i \mid s_1, \ldots, s_n \in \mathbb{Q}[X_1, \ldots, X_n] \Big\}$$

Verification conditions ($=, \neq, <, \leqslant$) → Systems of equations ($=$) → $1 \in (t_1, \ldots, t_n)$?

Gröbner bases for quantifier-free real arithmetic

Gröbner bases to solve the ideal membership problem:

- Monomial ordering $\prec$: admissible total well-founded ordering on monomials
- Reduction of a polynomial s w.r.t. $B = \{t_1, \ldots, t_n\}$:

$$
\begin{aligned}
s &\succ s + u_1 t_{i_1} \\
&\succ s + u_1 t_{i_1} + u_2 t_{i_2} \\
&\succ \cdots \\
&\succ \mathrm{red}_B\, s
\end{aligned}
$$

- B is called Gröbner basis if $\mathrm{red}_B\, s = 0$ for all $s \in (B)$

Verification conditions ($=, \neq, <, \leqslant$) → Systems of equations ($=$) → $1 \in (t_1, \ldots, t_n)$?

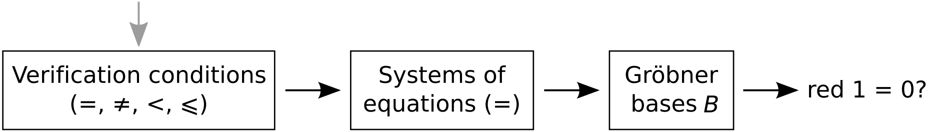
Gröbner bases for quantifier-free real arithmetic

Gröbner bases to solve the ideal membership problem:

- Monomial ordering $\prec$: admissible total well-founded ordering on monomials
- Reduction of a polynomial s w.r.t. $B = \{t_1, \ldots, t_n\}$:

$$\begin{aligned} s &\succ s + u_1 t_{i_1} \\ &\succ s + u_1 t_{i_1} + u_2 t_{i_2} \\ &\succ \cdots \\ &\succ \mathrm{red}_B\, s \end{aligned}$$

- B is called Gröbner basis if $\mathrm{red}_B\, s = 0$ for all $s \in (B)$



The Nullstellensatz

Method is sound and complete over complex numbers:

Theorem (Hilbert's Nullstellensatz)

$$\neg\exists x \in \mathbb{C}^n : \bigwedge_i t_i(x) = 0 \quad \textit{iff} \quad 1 \in (t_1, \dots, t_n)$$

$\Rightarrow$ Method cannot be complete over reals:

e.g.	$x^2 + 1 = 0$	is unsatisfiable
but	$(x^2 + 1)$	does not contain a unit

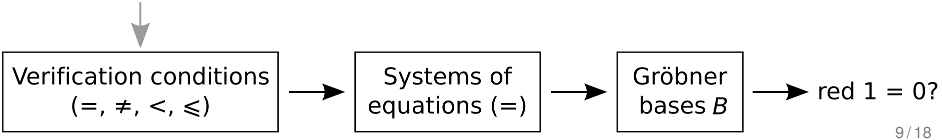
We present an extension that is complete over the reals

The Real Nullstellensatz

Theorem (Stengle's Real Nullstellensatz, 1973)

$$\neg\exists x \in \mathbb{R}^n : \bigwedge_i t_i(x) = 0 \quad \textit{iff}$$

$$\exists s_1, \ldots, s_k \in \mathbb{R}[X_1, \ldots, X_m] : \; 1 + s_1^2 + \cdots + s_k^2 \in (t_1, \ldots, t_n)$$

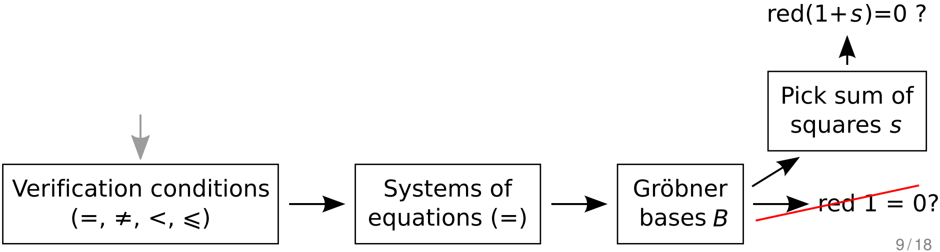


The Real Nullstellensatz

Theorem (Stengle's Real Nullstellensatz, 1973)

$$\neg\exists x \in \mathbb{R}^n : \bigwedge_i t_i(x) = 0 \quad \textit{iff}$$

$$\exists s_1, \ldots, s_k \in \mathbb{R}[X_1, \ldots, X_m] : \; 1 + s_1^2 + \cdots + s_k^2 \in (t_1, \ldots, t_n)$$



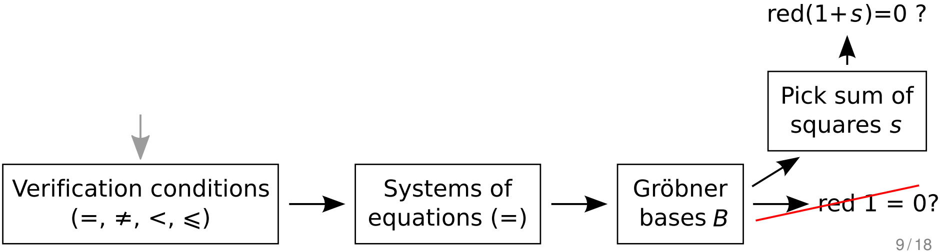
The Real Nullstellensatz

Theorem (Stengle's Real Nullstellensatz, 1973)

$$\neg \exists x \in \mathbb{R}^n : \bigwedge_i t_i(x) = 0 \quad \textit{iff}$$

$$\exists s_1, \ldots, s_k \in \mathbb{R}[X_1, \ldots, X_m] : \; 1 + s_1^2 + \cdots + s_k^2 \in (t_1, \ldots, t_n)$$

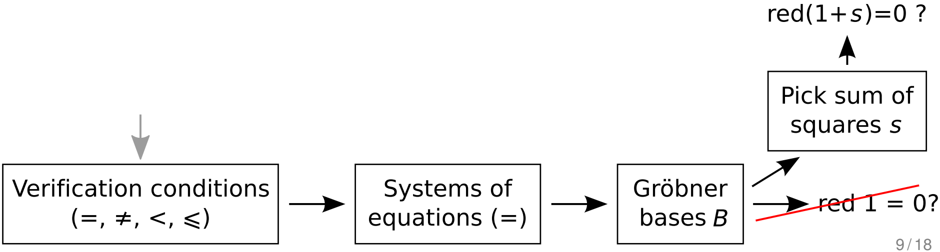
How to pick sum of squares $s_1^2 + \cdots + s_n^2$?



Observation: [Parrilo, 2003]
Sums of squares can be represented as scalar products

E.g.

$$2x^2 - 2xy + y^2 \;=\; x^2 + (x-y)^2 \;=\; \begin{pmatrix} x \\ y \end{pmatrix}^t \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

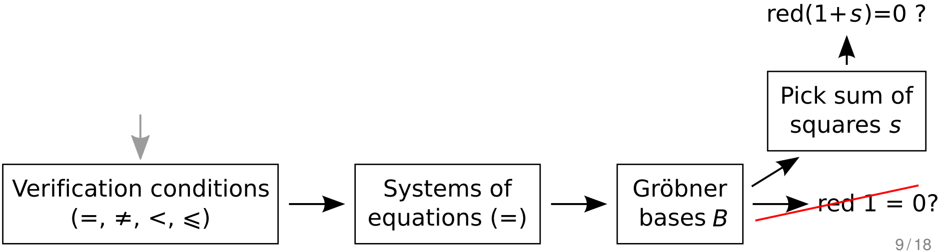


Lemma

Every sum of squares can be represented as $p^t Xp$, where $p \in \mathbb{R}[X_1, \ldots, X_m]^k$ and X is positive semi-definite (and vice versa).

Matrix X is called positive semi-definite if

- X is symmetric
- $x^t Xx \geq 0$ for all $x \in \mathbb{R}^n$.

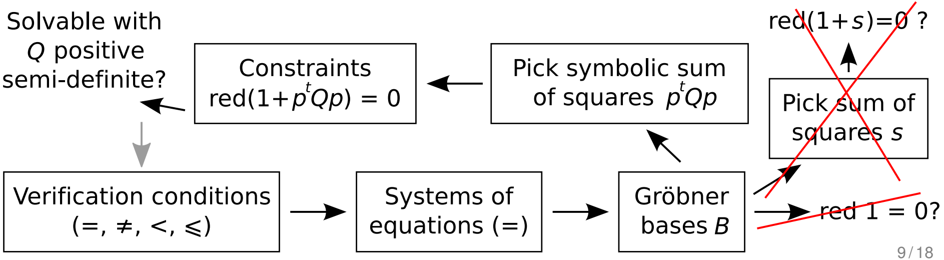


Lemma

Every sum of squares can be represented as $p^t X p$, where $p \in \mathbb{R}[X_1, \ldots, X_m]^k$ and X is positive semi-definite (and vice versa).

Matrix X is called positive semi-definite if

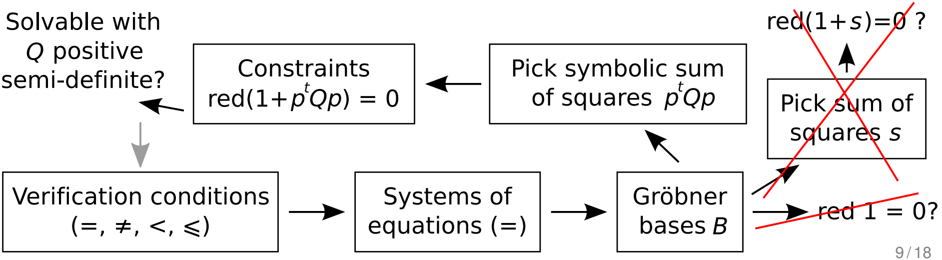
- X is symmetric
- $x^t X x \geq 0$ for all $x \in \mathbb{R}^n$.



The Real Nullstellensatz

Constraint solving by semidefinite programming (convex optimisation):

- Has been used successfully in combination with Positivstellensatz [Parrilo, 2003; Harrison, 2007]



Example

Prove unsatisfiability of:

$$x \geq y,\ z \geq 0,\ yz > xz$$

Example

Prove unsatisfiability of:

$$x \geq y,\ z \geq 0,\ yz > xz$$

Translated to system of equations:

$$x - y = a^2,\ z = b^2,\ (yz - xz)c^2 = 1$$

Example

Prove unsatisfiability of:

$$x \geq y,\ z \geq 0,\ yz > xz$$

Translated to system of equations:

$$x - y = a^2,\ z = b^2,\ (yz - xz)c^2 = 1$$

Corresponding Gröbner basis:

$$B\ =\ \{a^2 - x + y,\ b^2 - z,\ xzc^2 - yzc^2 + 1\}$$

Example

Prove unsatisfiability of:

$$x \geq y,\ z \geq 0,\ yz > xz$$

Translated to system of equations:

$$x - y = a^2,\ z = b^2,\ (yz - xz)c^2 = 1$$

Corresponding Gröbner basis:

$$B \ = \ \{a^2 - x + y,\ b^2 - z,\ xzc^2 - yzc^2 + 1\}$$

Pick basis monomials and symmetric matrix Q:

$$p \ = \ \begin{pmatrix} 1 \\ a^2 \\ abc \end{pmatrix} \qquad Q \ = \ \begin{pmatrix} q_{1,1} & q_{1,2} & q_{1,3} \\ q_{1,2} & q_{2,2} & q_{2,3} \\ q_{1,3} & q_{2,3} & q_{3,3} \end{pmatrix}$$

$$p^t Q p \ = \ q_{1,1} 1^2 + 2q_{1,2}a^2 + 2q_{1,3}abc + 2q_{2,3}a^3bc + q_{3,3}a^2b^2c^2$$

Example (2)

$$p^t Qp \;=\; q_{1,1}1^2 + 2q_{1,2}a^2 + 2q_{1,3}abc + 2q_{2,3}a^3bc + q_{3,3}a^2b^2c^2$$

Example (2)

$$p^t Q p \;=\; q_{1,1}1^2 + 2q_{1,2}a^2 + 2q_{1,3}abc + 2q_{2,3}a^3bc + q_{3,3}a^2b^2c^2$$

Reduce $1 + p^t Qp$ w.r.t. B:

$$\begin{aligned}\mathrm{red}_B(1 + p^t Qp) \;=\;& 1 + q_{1,1} - q_{3,3} + 2q_{1,2}x - 2q_{1,2}y + \\ & 2q_{1,3}abc + 2q_{2,3}abcx - 2q_{2,3}abcy\end{aligned}$$

Example (2)

$$p^t Qp = q_{1,1}1^2 + 2q_{1,2}a^2 + 2q_{1,3}abc + 2q_{2,3}a^3bc + q_{3,3}a^2b^2c^2$$

Reduce $1 + p^t Qp$ w.r.t. B:

$$\begin{aligned}\mathrm{red}_B(1 + p^t Qp) = \; & 1 + q_{1,1} - q_{3,3} + 2q_{1,2}x - 2q_{1,2}y + \\ & 2q_{1,3}abc + 2q_{2,3}abcx - 2q_{2,3}abcy\end{aligned}$$

Set up semidefinite program $\mathrm{red}_B(1 + p^t Qp) = 0$:

$$\begin{array}{rrr} 1 + q_{1,1} - q_{3,3} = 0 & -2q_{1,2} = 0 & 2q_{2,3} = 0 \\ 2q_{1,2} = 0 & 2q_{1,3} = 0 & -2q_{2,3} = 0 \end{array}$$

Example (2)

$$p^t Q p \;=\; q_{1,1} 1^2 + 2q_{1,2} a^2 + 2q_{1,3} abc + 2q_{2,3} a^3 bc + q_{3,3} a^2 b^2 c^2$$

Reduce $1 + p^t Q p$ w.r.t. B:

$$\begin{aligned} \mathrm{red}_B(1 + p^t Q p) \;=\; & 1 + q_{1,1} - q_{3,3} + 2q_{1,2} x - 2q_{1,2} y + \\ & 2q_{1,3} abc + 2q_{2,3} abcx - 2q_{2,3} abcy \end{aligned}$$

Set up semidefinite program $\mathrm{red}_B(1 + p^t Q p) = 0$:

$$\begin{aligned} 1 + q_{1,1} - q_{3,3} &= 0 & -2q_{1,2} &= 0 & 2q_{2,3} &= 0 \\ 2q_{1,2} &= 0 & 2q_{1,3} &= 0 & -2q_{2,3} &= 0 \end{aligned}$$

Solve the program: $q_{3,3} = 1$ and $q_{i,j} = 0$ for all $(i, j) \neq (3, 3)$

$$1 + p^t Q p \;=\; \underbrace{1 + (abc)^2}_{\text{Witness for unsatisfiability}} \;\in (B)$$

Gröbner bases for the Real Nullstellensatz (GRN)

Properties of the procedure

- Sound + complete method for quantifier-free real arithmetic
- Sums of squares as certificates (“proof producing”)
- Termination criteria can be given $\rightarrow$ decision procedure
- In practice:
  We enumerate basis monomials with ascending degree

Numerical issues

- Existing solvers for semidefinite programming are numeric (we use CSDP)
- Solution:
  Solve program numerically, then round to exact solution [Harrison, 2007]

Optimisations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$
- Rewriting with polynomials $x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$ (with $\alpha_i > 0$)
- Elimination of polynomials $xy - 1$, $x^n + t$
- Splitting polynomials $\alpha_1 m_1^2 + \cdots + \alpha_n m_n^2 \in B$ with $\alpha_i > 0$

Comparison with related work

Positivstellensatz methods [Parrilo, 2003; Harrison, 2007]:

- Positivstellensatz [Stengle, 1973]:
  Extension of Real Nullstellensatz for inequalities
- Differences: Gröbner bases, simpler certificates

Tiwari's method [Tiwari, 2005]:

- Differences: less heuristic $\Rightarrow$ completeness,
  semidefinite programming

Proof-producing quantifier elimination
[McLaughlin, Harrison, 2005]:

- Differences: universal fragment vs. full real arithmetic,
  performance

Numeric methods:

- Differences: soundness + completeness

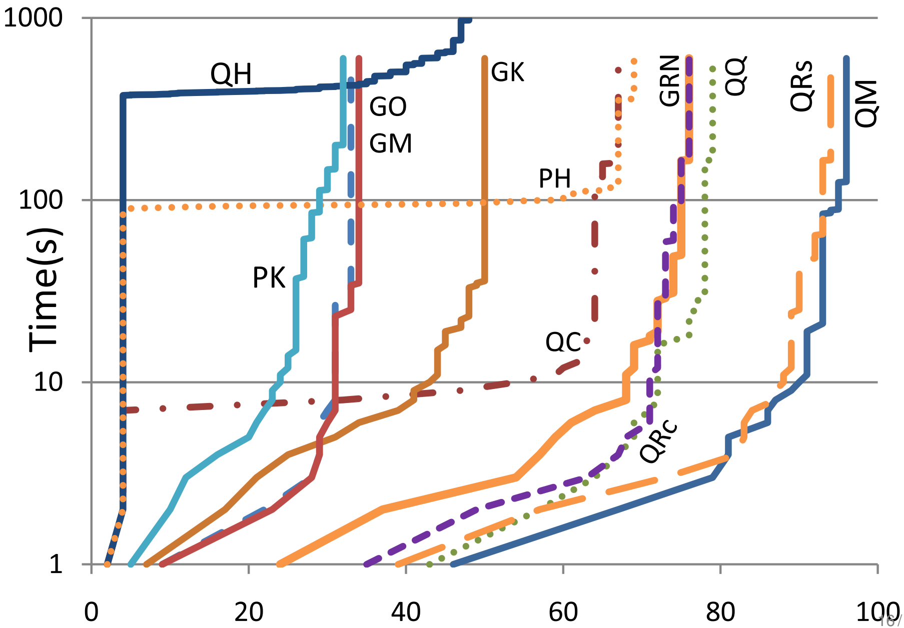
Empirical comparison of decision procedures

- Gröbner basis approaches
  - **GM**, **GO**: pure Gröbner bases (inequalities $\rightarrow$ equations)
  - **GK**: Gröbner bases combined with Fourier-Motzkin
  - **GRN**: Gröbner bases for the Real Nullstellensatz
- Quantifier elimination procedures
  - **QQ**, **QM**, **QR**$_c$: cylindrical algebraic decomposition (CAD)
  - **QR**$_s$: CAD + virtual substitution
  - **QC**, **QH**: Cohen-Hörmander
- Semidefinite programming for the Positivstellensatz
  - **PH**: Harrison's implementation
  - **PK**: own implementation in KeYmaera

Benchmarks: 100 problems taken from . . .

- Case studies in hybrid systems verification
- Verification of mathematical algorithms, geometry
- (A few) synthetic problems

Experiments



Conclusion

New decision procedure for quantifier-free real arithmetic:

- Gröbner bases for the Real Nullstellensatz
- Procedure is competitive with CAD + produces certificates
- Current implementation is straightforward
  $\Rightarrow$ Much room for improvements

Comparison of symbolic methods for real arithmetic:

- Gröbner bases
- Quantifier elimination
- Positivstellensatz + Real Nullstellensatz methods

Future work

- Optimise our procedure
- Empirical comparison with Tiwari's method
- Integration with methods to check satisfiability

Thanks for your attention!