15-819M: Data, Code, Decisions

13: Real Arithmetic

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA

Outline

Outline

Real Computation and Floating-Point Arithmetic

- Floating-point arithmetic in "first" computer Z1 [Zuse, 1937]

Real Computation and Floating-Point Arithmetic

- Floating-point arithmetic in “first” computer — Z1 [Zuse, 1937]
- Square root operation by micro-op algorithm — Z3 [Zuse, 1941]

Real Computation and Floating-Point Arithmetic

- Floating-point arithmetic in "first" computer Z1 [Zuse, 1937]
- Square root operation by micro-op algorithm Z3 [Zuse, 1941]

Real Computation and Floating-Point Arithmetic

- Floating-point arithmetic in "first" computer — Z1 [Zuse, 1937]
- Square root operation by micro-op algorithm — Z3 [Zuse, 1941]

```
r=a-1; q=1; p=1/2;
while (2*p*r >= err) {
  if (2*r - 2*q - p >= 0) {
    r = 2*r - 2*q - p;
    q = q+p;
    p = p/2;
  } else {
    r = 2*r;
    p = p/2;
  }
}
```

Real Computation and Floating-Point Arithmetic

- Floating-point arithmetic in "first" computer — Z1 [Zuse, 1937]
- Square root operation by micro-op algorithm — Z3 [Zuse, 1941]

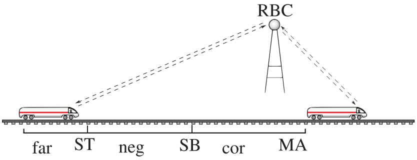
```
r=a-1; q=1; p=1/2;
while (2*p*r >= err) {
  if (2*r - 2*q - p >= 0) {
    r = 2*r - 2*q - p;
    q = q+p;
    p = p/2;
  } else {
    r = 2*r;
    p = p/2;
  }
}
```

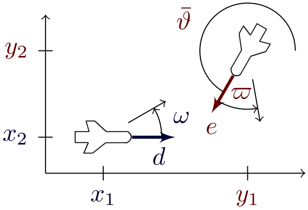
@loop_invariant(a = q^2+2*p*r)

Motivation + Applications of Real Arithmetic

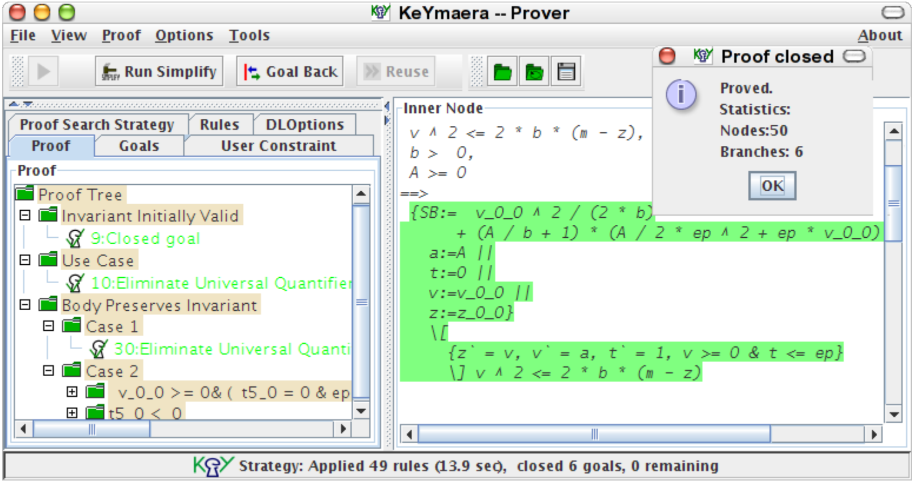
Real arithmetic is used in:

- Mathematical algorithms in real or floating-point arithmetic
- Hybrid systems, i.e., joint discrete and continuous dynamics
- Geometric problems

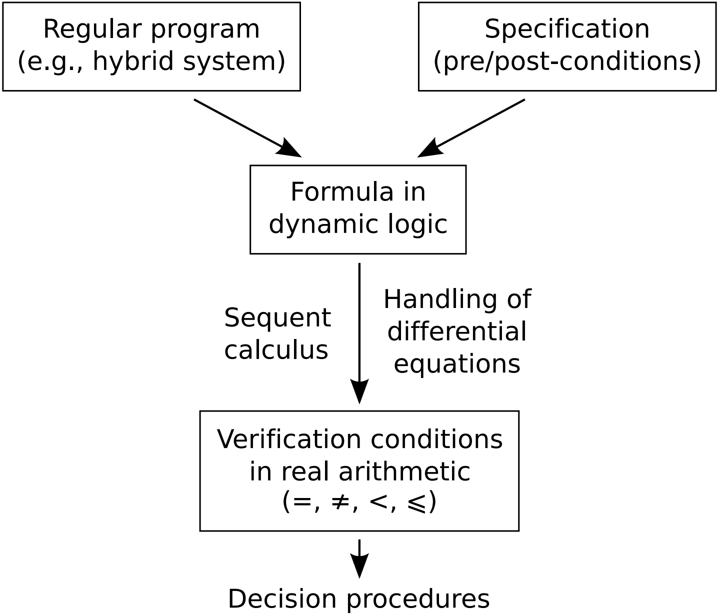




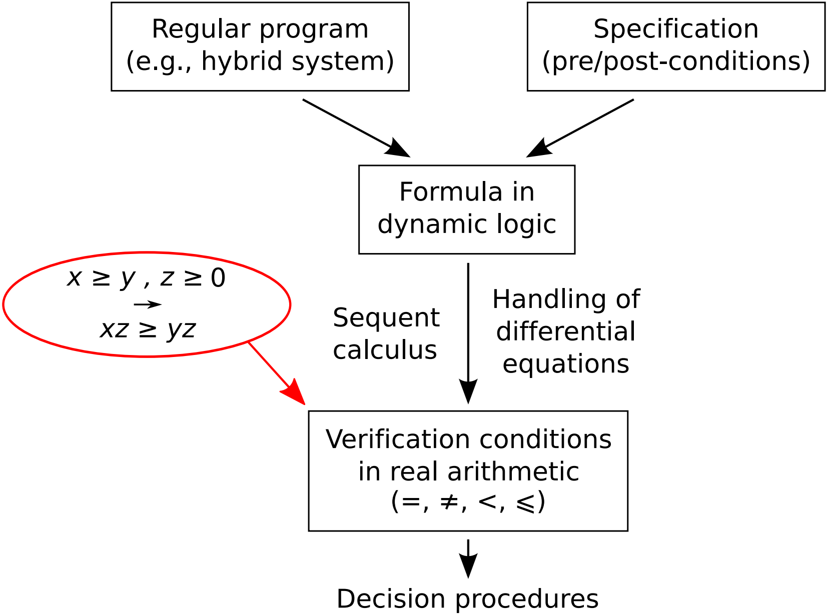
KeYmaera = KeY + Math for Hybrid Systems



Overall Verification Approach



Overall Verification Approach



Outline

Interpreted First-order Logic of Real Arithmetic

- In a formula like

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 > p^2$$

  how do we get "$+$" and "$-$" and "ˆ2" and "$>$" to mean what we want?

Interpreted First-order Logic of Real Arithmetic

- In a formula like

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 > p^2$$

  how do we get "$+$" and "$-$" and "ˆ2" and "$>$" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.

Interpreted First-order Logic of Real Arithmetic

- In a formula like

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 > p^2$$

  how do we get "$+$" and "$-$" and "ˆ2" and "$>$" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.
- Interpreted first-order logic is like first-order logic, except that some symbols have a fixed semantics (all interpretations agree on the semantics of those symbols).

Interpreted First-order Logic of Real Arithmetic

- In a formula like

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 > p^2$$

  how do we get "$+$" and "$-$" and "ˆ2" and "$>$" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.
- Interpreted first-order logic is like first-order logic, except that some symbols have a fixed semantics (all interpretations agree on the semantics of those symbols).
- Our primary focus: first-order real arithmetic $\text{FOL}_{\mathbb{R}}$

First-order Logic of Real Arithmetic: Syntax

Definition (Interpreted $\text{FOL}_{\mathbb{R}}$ Term t)

$t ::=$

x	for variable $x \in V$
r	for rational number r
$t_1 + t_2$	(infix notation)
$t_1 - t_2$	(infix notation)
$t_1 \cdot t_2$	(infix notation)
$f(t_1, \dots, t_n)$	for function $f/n \in \Sigma$ of arity $n \geq 0$

First-order Logic of Real Arithmetic: Syntax

Definition (Interpreted $\text{FOL}_{\mathbb{R}}$ Term t)

$t ::=$

x	for variable $x \in V$
r	for rational number r
$t_1 + t_2$	(infix notation)
$t_1 - t_2$	(infix notation)
$t_1 \cdot t_2$	(infix notation)
$f(t_1, \ldots, t_n)$	for function $f/n \in \Sigma$ of arity $n \geq 0$

First-order Logic of Real Arithmetic: Syntax

Definition (Interpreted $\text{FOL}_{\mathbb{R}}$ Formula F, G)

$F ::=$

$t_1 \geq t_2$	(infix notation)
$t_1 > t_2$	(infix notation)
$t_1 = t_2$	(infix notation)
$p(t_1, \ldots, t_n)$	for predicate $p/n \in \Sigma$ of arity $n \geq 0$
$\neg F$	“not”
$(F \land G)$	“and”
$(F \lor G)$	“or”
$(F \to G)$	“implies”
$(F \leftrightarrow G)$	“equivalent/bi-implies”
$\forall x\, F$	“universal quantifier/forall” for $x \in V$
$\exists x\, F$	“existential quantifier/exists” for $x \in V$

First-order Logic of Real Arithmetic: Syntax

Definition (Interpreted $\text{FOL}_{\mathbb{R}}$ Formula F, G)

$F ::=$

$t_1 \geq t_2$	(infix notation)
$t_1 > t_2$	(infix notation)
$t_1 = t_2$	(infix notation)
$p(t_1, \ldots, t_n)$	for predicate $p/n \in \Sigma$ of arity $n \geq 0$
$\neg F$	"not"
$(F \wedge G)$	"and"
$(F \vee G)$	"or"
$(F \rightarrow G)$	"implies"
$(F \leftrightarrow G)$	"equivalent/bi-implies"
$\forall x\, F$	"universal quantifier/forall" for $x \in V$
$\exists x\, F$	"existential quantifier/exists" for $x \in V$

Quiz

Is this a formula of first-order real arithmetic?

1. $F \lor (G \land (H \leftrightarrow \neg F) \to J)$
2. $\forall x\, (p(x) \to \exists y\, (p(y) \land \exists x\, \neg r(x, y)))$
3. $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$
4. $x < y \land \exists z\, x > z^2$
5. $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
6. $\forall x\, \exists y\, x > x^y$
7. $\exists x\, \forall y\, x > y + \pi$
8. $(\exists x\, \neg \exists y\, x > y + 3.1415926) \to \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

? $F \lor (G \land (H \leftrightarrow \neg F) \rightarrow J)$

2. $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \land \exists x\, \neg r(x, y)))$
3. $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$
4. $x < y \land \exists z\, x > z^2$
5. $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
6. $\forall x\, \exists y\, x > x^y$
7. $\exists x\, \forall y\, x > y + \pi$
8. $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

? $F \lor (G \land (H \leftrightarrow \neg F) \rightarrow J)$

? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \land \exists x\, \neg r(x, y)))$

3. $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$
4. $x < y \land \exists z\, x > z^2$
5. $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
6. $\forall x\, \exists y\, x > x^y$
7. $\exists x\, \forall y\, x > y + \pi$
8. $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

? $F \lor (G \land (H \leftrightarrow \neg F) \rightarrow J)$

? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \land \exists x\, \neg r(x, y)))$

✓ $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$

4. $x < y \land \exists z\, x > z^2$
5. $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
6. $\forall x\, \exists y\, x > x^y$
7. $\exists x\, \forall y\, x > y + \pi$
8. $(\exists x\, \neg\exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

? $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$

? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \wedge \exists x\, \neg r(x, y)))$

✓ $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$

✓ $x < y \wedge \exists z\, x > z^2$

5. $x > 0 \wedge \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
6. $\forall x\, \exists y\, x > x^y$
7. $\exists x\, \forall y\, x > y + \pi$
8. $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

? $F \lor (G \land (H \leftrightarrow \neg F) \rightarrow J)$

? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \land \exists x\, \neg r(x, y)))$

✓ $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$

✓ $x < y \land \exists z\, x > z^2$

✓ $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$

6. $\forall x\, \exists y\, x > x^y$
7. $\exists x\, \forall y\, x > y + \pi$
8. $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

? $F \lor (G \land (H \leftrightarrow \neg F) \rightarrow J)$

? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \land \exists x\, \neg r(x, y)))$

✓ $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$

✓ $x < y \land \exists z\, x > z^2$

✓ $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$

× $\forall x\, \exists y\, x > x^y$

7. $\exists x\, \forall y\, x > y + \pi$

8. $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

- ? $F \lor (G \land (H \leftrightarrow \neg F) \rightarrow J)$
- ? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \land \exists x\, \neg r(x,y)))$
- ✓ $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$
- ✓ $x < y \land \exists z\, x > z^2$
- ✓ $x > 0 \land \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
- × $\forall x\, \exists y\, x > x^y$
- ? $\exists x\, \forall y\, x > y + \pi$
- 8 $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

Quiz

Is this a formula of first-order real arithmetic?

- ? $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- ? $\forall x\, (p(x) \rightarrow \exists y\, (p(y) \wedge \exists x\, \neg r(x, y)))$
- ✓ $\forall x\, \forall y\, (x > y \leftrightarrow x - y > 0)$
- ✓ $x < y \wedge \exists z\, x > z^2$
- ✓ $x > 0 \wedge \forall y\, \exists z\, (x > z^2 + y \cdot z - 5)$
- × $\forall x\, \exists y\, x > x^y$
- ? $\exists x\, \forall y\, x > y + \pi$
- ✓ $(\exists x\, \neg \exists y\, x > y + 3.1415926) \rightarrow \forall x\, (x^2 > x^3)$

First-order Logic of Real Arithmetic: Semantics

Definition ($\text{FOL}_{\mathbb{R}}$ Interpretation I)

1. $D = \mathbb{R}$
2. I assigns relations and functions on $\mathbb{R}$ to all symbols in Σ
   - function $I(f) : \mathbb{R}^n \to \mathbb{R}$ for each function symbol f of arity n
   - relation $I(p) \subseteq \mathbb{R}^n$ for each predicate symbol p of arity n
   - element $I(c) \in \mathbb{R}$ for each constant symbol (function of arity 0)
   - truth-value $I(p) \in \{true, false\}$ for each predicate symbol of arity 0

   such that

   - $I(+)$ is addition on $\mathbb{R}$
   - $I(-)$ is subtraction on $\mathbb{R}$
   - $I(\cdot)$ is multiplication on $\mathbb{R}$
   - $I(=)$ is equality on $\mathbb{R}$
   - $I(>)$ is the greater relation on $\mathbb{R}$
   - $I(\geq)$ is the greater-equals relation on $\mathbb{R}$
   - $I(r) = r$ for all numbers $r \in \mathbb{Q}$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

1. PL_0
2. FOL
3. $\text{FOL}_{\mathbb{N}}[+,\cdot,=]$
4. $\text{FOL}_{\mathbb{R}}[+,\cdot,=,<]$
5. $\text{FOL}_{\mathbb{Q}}[+,\cdot,=]$
6. $\text{FOL}_{\mathbb{C}}[+,\cdot,=]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

✓ PL_0 decidable

2. FOL
3. $FOL_{\mathbb{N}}[+, \cdot, =]$
4. $FOL_{\mathbb{R}}[+, \cdot, =, <]$
5. $FOL_{\mathbb{Q}}[+, \cdot, =]$
6. $FOL_{\mathbb{C}}[+, \cdot, =]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

✓ PL_0 decidable

? FOL undecidable but semidecidable

3. $\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$
4. $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$
5. $\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$
6. $\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

✓ PL_0 decidable

? FOL undecidable but semidecidable

× $FOL_{\mathbb{N}}[+,\cdot,=]$ not semidecidable “Peano arithmetic” [Gödel’31]

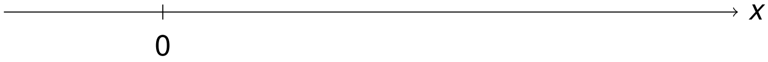
4. $FOL_{\mathbb{R}}[+,\cdot,=,<]$
5. $FOL_{\mathbb{Q}}[+,\cdot,=]$
6. $FOL_{\mathbb{C}}[+,\cdot,=]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $FOL_{\mathbb{N}}[+, \cdot, =]$ not semidecidable "Peano arithmetic" [Gödel'31]
- ✓ $FOL_{\mathbb{R}}[+, \cdot, =, <]$ decidable [Tarski'51]
5. $FOL_{\mathbb{Q}}[+, \cdot, =]$
6. $FOL_{\mathbb{C}}[+, \cdot, =]$

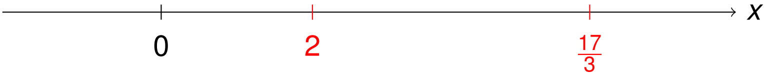
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$\exists x (x > 2 \land x < \frac{17}{3})$$

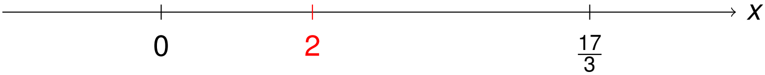
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$\exists x (x > 2 \land x < \frac{17}{3})$$

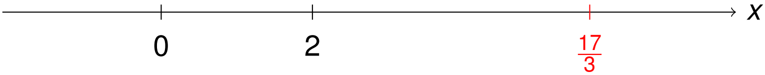
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$\begin{array}{ll} & \exists x (x > 2 \land x < \frac{17}{3}) \\ \equiv & (2 > 2 \land 2 < \frac{17}{3}) \qquad \text{border case “} x = 2 \text{”} \end{array}$$

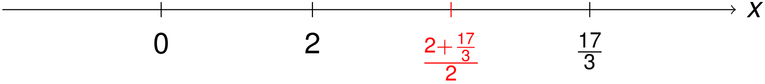
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$\begin{array}{lll} & \exists x (x > 2 \land x < \frac{17}{3}) & \\ \equiv & (2 > 2 \land 2 < \frac{17}{3}) & \text{border case "} x = 2 \text{"} \\ \lor & (\frac{17}{3} > 2 \land \frac{17}{3} < \frac{17}{3}) & \text{border case "} x = \frac{17}{3} \text{"} \end{array}$$

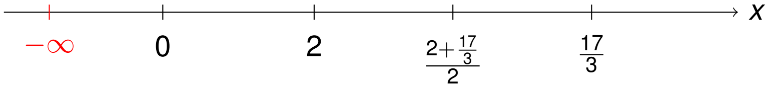
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$
\begin{array}{lll}
 & \exists x (x > 2 \land x < \frac{17}{3}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{3}) & \text{border case “} x = 2 \text{”} \\
\lor & (\frac{17}{3} > 2 \land \frac{17}{3} < \frac{17}{3}) & \text{border case “} x = \frac{17}{3} \text{”} \\
\lor & (\frac{2+\frac{17}{3}}{2} > 2 \land \frac{2+\frac{17}{3}}{2} < \frac{17}{3}) & \text{intermediate case “} x = \frac{2+\frac{17}{3}}{2} \text{”}
\end{array}
$$

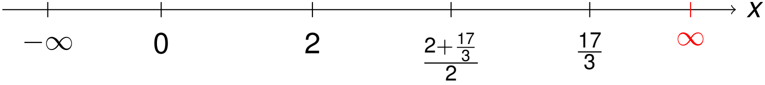
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$
\begin{array}{lll}
 & \exists x (x > 2 \land x < \frac{17}{3}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{3}) & \text{border case “} x = 2 \text{”} \\
\lor & (\frac{17}{3} > 2 \land \frac{17}{3} < \frac{17}{3}) & \text{border case “} x = \frac{17}{3} \text{”} \\
\lor & (\frac{2+\frac{17}{3}}{2} > 2 \land \frac{2+\frac{17}{3}}{2} < \frac{17}{3}) & \text{intermediate case “} x = \frac{2+\frac{17}{3}}{2} \text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{3}) & \text{extremal case “} x = -\infty \text{”}
\end{array}
$$

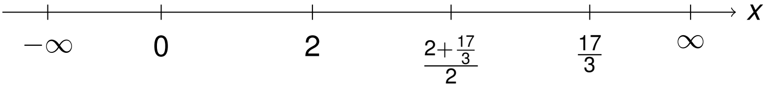
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

$$
\begin{array}{lll}
 & \exists x (x > 2 \land x < \frac{17}{3}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{3}) & \text{border case “}x = 2\text{”} \\
\lor & (\frac{17}{3} > 2 \land \frac{17}{3} < \frac{17}{3}) & \text{border case “}x = \frac{17}{3}\text{”} \\
\lor & (\frac{2+\frac{17}{3}}{2} > 2 \land \frac{2+\frac{17}{3}}{2} < \frac{17}{3}) & \text{intermediate case “}x = \frac{2+\frac{17}{3}}{2}\text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{3}) & \text{extremal case “}x = -\infty\text{”} \\
\lor & (\infty > 2 \land \infty < \frac{17}{3}) & \text{extremal case “}x = \infty\text{”}
\end{array}
$$

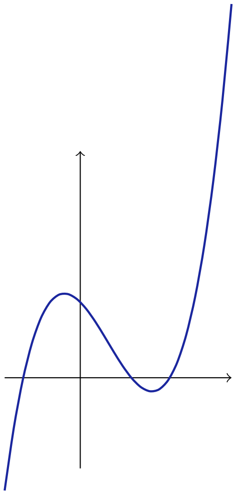
Quantifier Elimination by Example



Can we get rid of the quantifier without changing the semantics of the formula?

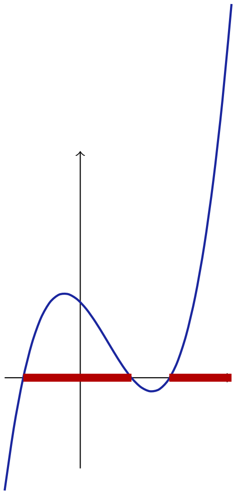
$$
\begin{array}{lll}
 & \exists x (x > 2 \land x < \frac{17}{3}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{3}) & \text{border case “}x = 2\text{”} \\
\lor & (\frac{17}{3} > 2 \land \frac{17}{3} < \frac{17}{3}) & \text{border case “}x = \frac{17}{3}\text{”} \\
\lor & (\frac{2+\frac{17}{3}}{2} > 2 \land \frac{2+\frac{17}{3}}{2} < \frac{17}{3}) & \text{intermediate case “}x = \frac{2+\frac{17}{3}}{2}\text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{3}) & \text{extremal case “}x = -\infty\text{”} \\
\lor & (\infty > 2 \land \infty < \frac{17}{3}) & \text{extremal case “}x = \infty\text{”} \\
\equiv & \mathit{true} & \text{evaluate}
\end{array}
$$

Quantifier Elimination and Projection



$$\exists y\,(y \geq 0 \land 1 - x - 1.83x^2 + 1.66x^3 > y)$$

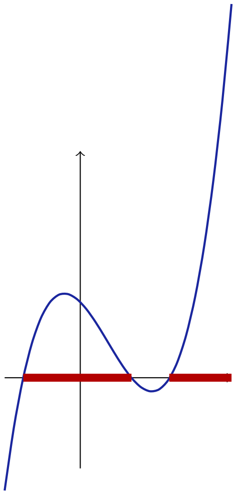
Quantifier Elimination and Projection



$\exists y\,(y \geq 0 \land 1 - x - 1.83x^2 + 1.66x^3 > y)$

Quantifier Elimination and Projection

$\exists y\, (y \geq 0 \land 1 - x - 1.83x^2 + 1.66x^3 > y)$



$0.75 < x \land x < 0.68 \lor x > 1.17$

Quantifier Elimination in Real-Closed Fields

Definition (Quantifier elimination)

A first-order theory admits *quantifier elimination* if to each formula ϕ, a quantifier-free formula QE(ϕ) can be effectively associated that is equivalent (i.e., $\phi \leftrightarrow$ QE(ϕ) is valid) and has no other free variables. The operation QE is further assumed to evaluate ground formulas (i.e., without variables), yielding a decision procedure for this theory.

Quantifier Elimination in Real-Closed Fields

Definition (Quantifier elimination)

A first-order theory admits *quantifier elimination* if to each formula ϕ, a quantifier-free formula QE(ϕ) can be effectively associated that is equivalent (i.e., $\phi \leftrightarrow$ QE(ϕ) is valid) and has no other free variables. The operation QE is further assumed to evaluate ground formulas (i.e., without variables), yielding a decision procedure for this theory.

Theorem (Tarski'30,'51, Seidenberg'54)

$\mathrm{FOL}_{\mathbb{R}}$ *admits quantifier elimination and is decidable.*

Quantifier Elimination in Real-Closed Fields

Definition (Quantifier elimination)

A first-order theory admits *quantifier elimination* if to each formula ϕ, a quantifier-free formula $\mathrm{QE}(\phi)$ can be effectively associated that is equivalent (i.e., $\phi \leftrightarrow \mathrm{QE}(\phi)$ is valid) and has no other free variables. The operation QE is further assumed to evaluate ground formulas (i.e., without variables), yielding a decision procedure for this theory.

Theorem (Tarski'30,'51, Seidenberg'54)

$\mathrm{FOL}_{\mathbb{R}}$ *admits quantifier elimination and is decidable.*

Theorem (Complexity, Davenport&Heintz'88,Weispfenning'88)

(Time and space) complexity of QE *for* $\mathbb{R}$ *is doubly exponential in the number of quantifier (alternations).*

Quiz

(Validity of) which of the following logics is
decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$ not semidecidable “Peano arithmetic” [Gödel’31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$ decidable [Tarski’51]
- 5 $\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$
- 6 $\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $FOL_{\mathbb{N}}[+, \cdot, =]$ not semidecidable “Peano arithmetic” [Gödel’31]
- ✓ $FOL_{\mathbb{R}}[+, \cdot, =, <]$ decidable [Tarski’51]
- × $FOL_{\mathbb{Q}}[+, \cdot, =]$ not even semidecidable [Robinson’49]
- 6 $FOL_{\mathbb{C}}[+, \cdot, =]$

Quiz

(Validity of) which of the following logics is
decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $FOL_{\mathbb{N}}[+, \cdot, =]$ not semidecidable "Peano arithmetic" [Gödel'31]
- ✓ $FOL_{\mathbb{R}}[+, \cdot, =, <]$ decidable [Tarski'51]
- × $FOL_{\mathbb{Q}}[+, \cdot, =]$ not even semidecidable [Robinson'49]
- ✓ $FOL_{\mathbb{C}}[+, \cdot, =]$ decidable [Tarski'51,Chevalley'51]

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

✓ PL_0 decidable

? FOL undecidable but semidecidable

× $FOL_{\mathbb{N}}[+,\cdot,=]$ not semidecidable “Peano arithmetic” [Gödel’31]

✓ $FOL_{\mathbb{R}}[+,\cdot,=,<]$ decidable [Tarski’51]

× $FOL_{\mathbb{Q}}[+,\cdot,=]$ not even semidecidable [Robinson’49]

✓ $FOL_{\mathbb{C}}[+,\cdot,=]$ decidable [Tarski’51,Chevalley’51]

7. $FOL_{\mathbb{N}}[+,=,2|,3|,\ldots]$
8. $FOL_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$
9. $FOL_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $FOL_{\mathbb{N}}[+, \cdot, =]$ not semidecidable "Peano arithmetic" [Gödel'31]
- ✓ $FOL_{\mathbb{R}}[+, \cdot, =, <]$ decidable [Tarski'51]
- × $FOL_{\mathbb{Q}}[+, \cdot, =]$ not even semidecidable [Robinson'49]
- ✓ $FOL_{\mathbb{C}}[+, \cdot, =]$ decidable [Tarski'51,Chevalley'51]
- ✓ $FOL_{\mathbb{N}}[+, =, 2|, 3|, \ldots]$ decidable "Presburger arithmetic"
- 8 $FOL_{\mathbb{R}}[+, \cdot, exp, =, <]$
- 9 $FOL_{\mathbb{R}}[+, \cdot, sin, =, <]$

Quiz

(Validity of) which of the following logics is
decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $FOL_{\mathbb{N}}[+,\cdot,=]$ not semidecidable "Peano arithmetic" [Gödel'31]
- ✓ $FOL_{\mathbb{R}}[+,\cdot,=,<]$ decidable [Tarski'51]
- × $FOL_{\mathbb{Q}}[+,\cdot,=]$ not even semidecidable [Robinson'49]
- ✓ $FOL_{\mathbb{C}}[+,\cdot,=]$ decidable [Tarski'51,Chevalley'51]
- ✓ $FOL_{\mathbb{N}}[+,=,2|,3|,\ldots]$ decidable "Presburger arithmetic"
- ? $FOL_{\mathbb{R}}[+,\cdot,exp,=,<]$ unknown
- 9 $FOL_{\mathbb{R}}[+,\cdot,sin,=,<]$

Quiz

(Validity of) which of the following logics is decidable/semidecidable/undecidable/not semidecidable?

- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $FOL_{\mathbb{N}}[+,\cdot,=]$ not semidecidable “Peano arithmetic” [Gödel’31]
- ✓ $FOL_{\mathbb{R}}[+,\cdot,=,<]$ decidable [Tarski’51]
- × $FOL_{\mathbb{Q}}[+,\cdot,=]$ not even semidecidable [Robinson’49]
- ✓ $FOL_{\mathbb{C}}[+,\cdot,=]$ decidable [Tarski’51,Chevalley’51]
- ✓ $FOL_{\mathbb{N}}[+,=,2|,3|,...]$ decidable “Presburger arithmetic”
- ? $FOL_{\mathbb{R}}[+,\cdot,exp,=,<]$ unknown
- × $FOL_{\mathbb{R}}[+,\cdot,sin,=,<]$ not even semidecidable

Axioms of Reals

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$
3. Inverse $\forall x \, \exists y \; x + y = 0$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$
3. Inverse $\forall x \, \exists y \; x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \; x \cdot (y \cdot z) = (x \cdot y) \cdot z$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$
3. Inverse $\forall x \, \exists y \; x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \; x \cdot 1 = x$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\,\forall y\,\forall z\; x + (y + z) = (x + y) + z$
2. Neutral $\forall x\; x + 0 = x$
3. Inverse $\forall x\,\exists y\; x + y = 0$
4. Abelian $\forall x\,\forall y\,(x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\,\forall y\,\forall z\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\; x \cdot 1 = x$
7. Inverse $\forall x\,(x \neq 0 \rightarrow \exists y\; x \cdot y = 1)$
8. Abelian $\forall x\,\forall y\,(x \cdot y = y \cdot x)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$
3. Inverse $\forall x \, \exists y \; x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \; x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \rightarrow \exists y \; x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \to \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \land y \geq z \to x \geq z)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$
3. Inverse $\forall x \, \exists y \; x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \; x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \rightarrow \exists y \; x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x \, \forall y \, \forall z \, (x \geq y \land y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x \, \forall y \, (x \geq y \land y \geq x \rightarrow x = y)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \land y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x\, \forall y\, (x \geq y \land y \geq x \rightarrow x = y)$
12. Total $\forall x\, \forall y\, (x \geq y \lor y \geq x)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \, x + (y + z) = (x + y) + z$
2. Neutral $\forall x \, x + 0 = x$
3. Inverse $\forall x \, \exists y \, x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \, x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \rightarrow \exists y \, x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x \, \forall y \, \forall z \, (x \geq y \land y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x \, \forall y \, (x \geq y \land y \geq x \rightarrow x = y)$
12. Total $\forall x \, \forall y \, (x \geq y \lor y \geq x)$
13. Additive $\forall x \, \forall y \, \forall z \, (x \geq y \rightarrow x + z \geq y + z)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \land y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x\, \forall y\, (x \geq y \land y \geq x \rightarrow x = y)$
12. Total $\forall x\, \forall y\, (x \geq y \lor y \geq x)$
13. Additive $\forall x\, \forall y\, \forall z\, (x \geq y \rightarrow x + z \geq y + z)$
14. Positive $\forall x\, \forall y\, (x \geq 0 \land y \geq 0 \rightarrow xy \geq 0)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \wedge y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x\, \forall y\, (x \geq y \wedge y \geq x \rightarrow x = y)$
12. Total $\forall x\, \forall y\, (x \geq y \vee y \geq x)$
13. Additive $\forall x\, \forall y\, \forall z\, (x \geq y \rightarrow x + z \geq y + z)$
14. Positive $\forall x\, \forall y\, (x \geq 0 \wedge y \geq 0 \rightarrow xy \geq 0)$
15. Sup “Non-empty subsets with upper bounds have supremum”

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

Theorem (downward Skolem-Löwenheim'1915-20)

Let Γ be a countable set of first-order formulas.
Γ *has a model* $\Rightarrow$ Γ *has an infinite countable model*
"first-order logic cannot distinguish different infinities"

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

Theorem (downward Skolem-Löwenheim'1915-20)

Let Γ be a countable set of first-order formulas.
Γ *has a model* $\Rightarrow$ Γ *has an infinite countable model*
"first-order logic cannot distinguish different infinities"

Corollary

The reals cannot be characterized (up to isomorphism) in first-order logic (nor any other infinite structure really, not even in the generated case)

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

Theorem (downward Skolem-Löwenheim'1915-20)

Let Γ be a countable set of first-order formulas.

Γ *has a model* $\Rightarrow$ Γ *has an infinite countable model*

"first-order logic cannot distinguish different infinities"

Corollary

The reals cannot be characterized (up to isomorphism) in first-order logic (nor any other infinite structure really, not even in the generated case)

But the first-order "view" of the reals is still fairly amazing

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.
2. For every $x_1, \ldots, x_n \in R$, $\sum_{i=1}^{n} x_i^2 = 0$ implies $x_1 = \cdots = x_n = 0$.

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.
2. For every $x_1, \ldots, x_n \in R$, $\sum_{i=1}^{n} x_i^2 = 0$ implies $x_1 = \cdots = x_n = 0$.
3. R admits an ordering that makes R an ordered field.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.
3. R is not algebraically closed but its algebraic closure is a finite extension, i.e., finitely generated over R.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2+1)$ is algebraically closed.
3. R is not algebraically closed but its algebraic closure is a finite extension, i.e., finitely generated over R.
4. R has the *intermediate value property*, i.e., R is an ordered field such that for any polynomial $p \in R[X]$ with $a, b \in R$, $a < b$ and $p(a)p(b) < 0$, there is a ζ with $a < \zeta < b$ such that $p(\zeta) = 0$.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.
3. R is not algebraically closed but its algebraic closure is a finite extension, i.e., finitely generated over R.
4. R has the *intermediate value property*, i.e., R is an ordered field such that for any polynomial $p \in R[X]$ with $a, b \in R$, $a < b$ and $p(a)p(b) < 0$, there is a ζ with $a < \zeta < b$ such that $p(\zeta) = 0$.
5. R is a real field such that no proper algebraic extension is a formally real field.

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

- Computable numbers, i.e., those that can be approximated by a computable function up to any desired precision.

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

- Computable numbers, i.e., those that can be approximated by a computable function up to any desired precision. π lives here!

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

- Computable numbers, i.e., those that can be approximated by a computable function up to any desired precision. π lives here!
- ZFC-Definable numbers, i.e., those real numbers $a \in \mathbb{R}$ for which there is a first-order formula φ in set theory with one free variable such that a is the unique real number for which φ holds true.

$$I \models \varphi \text{ iff } I(x) = a$$

The advantages of implicit definition over construction are roughly those of theft over honest toil [Russell]

First-Order Axiom Schemes of Real-Closed Fields

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. $\neg \exists x_1 \, \dots \exists x_n\, (-1 = x_1^2 + \cdots + x_n^2)$ for any n
11. $\forall x\, \forall y\, (x < y \land p(x)p(y) < 0 \rightarrow \exists z\, (x < z < y \land p(z) = 0))$ for polynomial p (intermediate value property)

First-Order Axiom Schemes of Real-Closed Fields

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. $\neg \exists x_1 \ldots \exists x_n\, (-1 = x_1^2 + \cdots + x_n^2)$ for any n
11. $\forall x\, \forall y\, (x < y \land p(x)p(y) < 0 \rightarrow \exists z\, (x < z < y \land p(z) = 0))$ for polynomial p (intermediate value property)

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
1993	Virtual substitution by Weispfenning
2003	Parrilo introduces semidefinite programming for the Positivstellensatz (Later refined by Harrison)
2005	Tiwari's polynomial simplex method

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

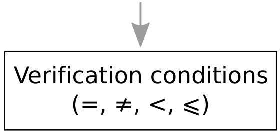
1993 Virtual substitution by Weispfenning

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

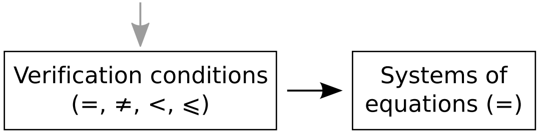
2005 Tiwari's polynomial simplex method

Outline

Gröbner Bases for Quantifier-Free Real Arithmetic



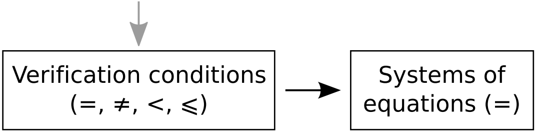
Inequalities and disequations?



Gröbner Bases for Quantifier-Free Real Arithmetic

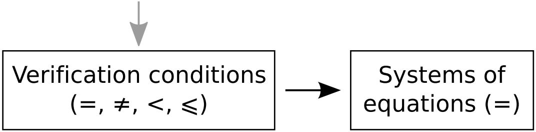
Inequalities and disequations can be eliminated:

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



Goal: prove unsatisfiability of:

$$\bigwedge_i t_i = 0$$

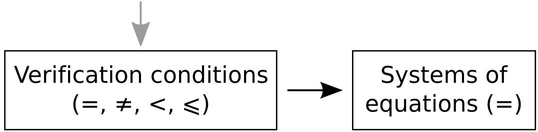


Gröbner Bases for Quantifier-Free Real Arithmetic

Witnesses for unsatisfiability:

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

How to determine coefficients s_i?



Witnesses for unsatisfiability:

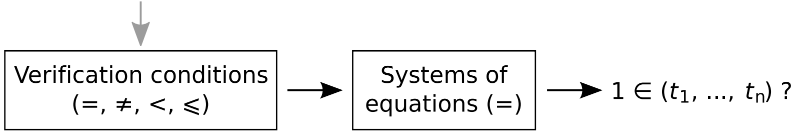
$$\left(\sum_i s_i t_i\right) = 1 \quad\Longrightarrow\quad \bigwedge_i t_i = 0 \ \text{ unsatisfiable}$$

How to determine coefficients s_i?

Need some more notation:

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

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



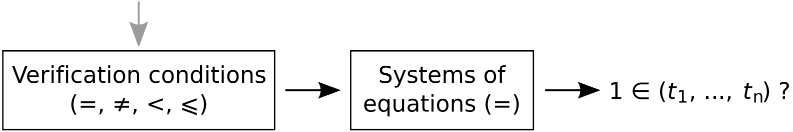
Gröbner Bases for Quantifier-Free Real Arithmetic

Gröbner bases to solve the ideal membership problem:

- Monomial ordering $\prec$: admissible total well-founded ordering on monomials (Gives the order in which to try eliminating 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 $s \in (B)$



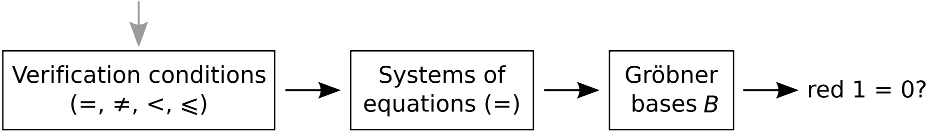
Gröbner Bases for Quantifier-Free Real Arithmetic

Gröbner bases to solve the ideal membership problem:

- Monomial ordering $\prec$: admissible total well-founded ordering on monomials (Gives the order in which to try eliminating monomials)
- Reduction of a polynomial s w.r.t. $B = \{t_1, \dots, t_n\}$:

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

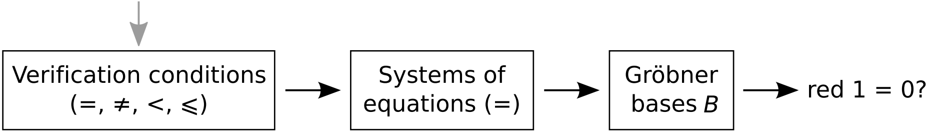
- B is called Gröbner basis if $\mathrm{red}_B\, s = 0$ for all $s \in (B)$



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
- $\prec$ admissible iff its reflexive closure $\preceq$ satisfies
  1. $X^\nu \preceq X^\mu$ then $X^\nu X^\lambda \preceq X^\mu X^\lambda$ for all $\nu, \mu, \lambda \in \mathbb{N}^n$
  2. $X^\nu | X^\mu$ then $X^\nu \preceq X^\mu$ for all $\nu, \mu \in \mathbb{N}^n$



The Nullstellensatz

Method is sound and complete over complex numbers:

Theorem (Hilbert's Nullstellensatz)

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

What about the real numbers?

The Nullstellensatz

Method is sound and complete over complex numbers:

Theorem (Hilbert's Nullstellensatz)

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

$\Rightarrow$ Method sound but cannot be complete over reals:

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

Next: an extension that is complete over the reals

Gröbner Bases

Definition (Gröbner basis)

Finite set $G \subseteq k[X_1, \dots, X_n]$ with $(G) = I$ is *Gröbner basis* of ideal I iff, equivalently:

1. Reduction with respect to G gives 0 for any $p \in I$.

Gröbner Bases

Definition (Gröbner basis)

Finite set $G \subseteq k[X_1, \ldots, X_n]$ with $(G) = I$ is *Gröbner basis* of ideal I iff, equivalently:

1. Reduction with respect to G gives 0 for any $p \in I$.
2. $\text{red}_G\, p = 0$ iff $p \in I$.

Gröbner Bases

Definition (Gröbner basis)

Finite set $G \subseteq k[X_1, \ldots, X_n]$ with $(G) = I$ is *Gröbner basis* of ideal I iff, equivalently:

1. Reduction with respect to G gives 0 for any $p \in I$.
2. $\text{red}_G\, p = 0$ iff $p \in I$.
3. Reduction with respect to G gives a unique remainder.

Gröbner Bases

Definition (Gröbner basis)

Finite set $G \subseteq k[X_1, \ldots, X_n]$ with $(G) = I$ is *Gröbner basis* of ideal I iff, equivalently:

1. Reduction with respect to G gives 0 for any $p \in I$.
2. $\text{red}_G\, p = 0$ iff $p \in I$.
3. Reduction with respect to G gives a unique remainder.

Theorem (Hilbert's basis theorem)

Every ideal in the ring $k[X_1, \ldots, X_n]$ of multivariate polynomials over a field k is finitely generated.

Gröbner Bases

Definition (Gröbner basis)

Finite set $G \subseteq k[X_1, \ldots, X_n]$ with $(G) = I$ is *Gröbner basis* of ideal I iff, equivalently:

1. Reduction with respect to G gives 0 for any $p \in I$.
2. $\text{red}_G\, p = 0$ iff $p \in I$.
3. Reduction with respect to G gives a unique remainder.

Theorem (Hilbert's basis theorem)

Every ideal in the ring $k[X_1, \ldots, X_n]$ of multivariate polynomials over a field k is finitely generated.

Can be computed effectively by Buchberger's algorithm

Buchberger's Algorithm for Computing Gröbner Bases

GB(finite $F \subset k[X_1, \ldots, X_n]$):

1. choose $f, g \in F$
2. $s := \frac{lcm(\ell(f),\ell(g))}{\ell(f)} f - \frac{lcm(\ell(f),\ell(g))}{\ell(g)} g$
   let the leading terms $\ell(...)$ cancel by construction
3. $F := F \cup \{\mathrm{red}_F\, s\}$

Buchberger's Algorithm for Computing Gröbner Bases

GB(finite $F \subset k[X_1, \ldots, X_n]$):

1. choose $f, g \in F$
2. $s := \frac{lcm(\ell(f),\ell(g))}{\ell(f)} f - \frac{lcm(\ell(f),\ell(g))}{\ell(g)} g$
   let the leading terms $\ell(...)$ cancel by construction
3. $F := F \cup \{\text{red}_F\, s\}$

Buchberger's Algorithm for Computing Gröbner Bases

GB(finite $F \subset k[X_1, \ldots, X_n]$):

1. choose $f, g \in F$
2. $s := \frac{lcm(\ell(f),\ell(g))}{\ell(f)} f - \frac{lcm(\ell(f),\ell(g))}{\ell(g)} g$
   let the leading terms $\ell(...)$ cancel by construction
3. $F := F \cup \{\text{red}_F\, s\}$

Buchberger's Algorithm for Computing Gröbner Bases

GB(finite $F \subset k[X_1, \ldots, X_n]$):

1. choose $f, g \in F$
2. $s := \frac{lcm(\ell(f),\ell(g))}{\ell(f)} f - \frac{lcm(\ell(f),\ell(g))}{\ell(g)} g$
   let the leading terms $\ell(\ldots)$ cancel by construction
3. $F := F \cup \{\mathrm{red}_F\, s\}$

Buchberger's Algorithm for Computing Gröbner Bases

GB(finite $F \subset k[X_1, \ldots, X_n]$):

1. choose $f, g \in F$
2. $s := \frac{lcm(\ell(f),\ell(g))}{\ell(f)} f - \frac{lcm(\ell(f),\ell(g))}{\ell(g)} g = \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$
   let the leading terms $\ell(...)$ cancel by construction
3. $F := F \cup \{\text{red}_F\, s\}$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$S(f, g) =$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$S(f,g) = \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)$$

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$\begin{aligned} S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1) \\ &= x^2y + 2xy^3 - (x^2y + 2xy^3 - x) \end{aligned}$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$\begin{aligned} S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1) \\ &= x^2y + 2xy^3 - (x^2y + 2xy^3 - x) \\ &= x =: h \quad \rightsquigarrow G = \{f, g, h\} \end{aligned}$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$S(f,g) = \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)$$
$$= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)$$
$$= x =: h \quad \rightsquigarrow G = \{f, g, h\}$$
$$S(g,h) = \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$\begin{aligned}
S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)\\
&= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)\\
&= x =: h \quad \rightsquigarrow G = \{f, g, h\}\\
S(g,h) &= \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)\\
&= xy + 2y^3 - 1 - xy
\end{aligned}$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$
\begin{aligned}
S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1) \\
&= x^2y + 2xy^3 - (x^2y + 2xy^3 - x) \\
&= x =: h \quad \rightsquigarrow G = \{f, g, h\} \\
S(g,h) &= \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x) \\
&= xy + 2y^3 - 1 - xy \\
&= 2y^3 - 1 =: e \quad \rightsquigarrow G = \{f, g, h, e\}
\end{aligned}
$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$\begin{aligned}
S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)\\
&= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)\\
&= x =: h \quad \rightsquigarrow G = \{f, g, h\}\\
S(g,h) &= \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)\\
&= xy + 2y^3 - 1 - xy\\
&= 2y^3 - 1 =: e \quad \rightsquigarrow G = \{f, g, h, e\}\\
S(f,h) &= \frac{x}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(x)
\end{aligned}$$

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$\begin{aligned}
S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)\\
&= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)\\
&= x =: h \quad \rightsquigarrow G = \{f, g, h\}\\
S(g,h) &= \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)\\
&= xy + 2y^3 - 1 - xy\\
&= 2y^3 - 1 =: e \quad \rightsquigarrow G = \{f, g, h, e\}\\
S(f,h) &= \frac{x}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(x)\\
&= x^2 + 2xy^2 - x^2
\end{aligned}$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$
\begin{aligned}
S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)\\
&= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)\\
&= x =: h \quad \rightsquigarrow G = \{f, g, h\}\\
S(g,h) &= \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)\\
&= xy + 2y^3 - 1 - xy\\
&= 2y^3 - 1 =: e \quad \rightsquigarrow G = \{f, g, h, e\}\\
S(f,h) &= \frac{x}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(x)\\
&= x^2 + 2xy^2 - x^2\\
&= 2xy^2
\end{aligned}
$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$
\begin{aligned}
S(f,g) &= \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)\\
&= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)\\
&= x =: h \quad \rightsquigarrow G = \{f, g, h\}\\
S(g,h) &= \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)\\
&= xy + 2y^3 - 1 - xy\\
&= 2y^3 - 1 =: e \quad \rightsquigarrow G = \{f, g, h, e\}\\
S(f,h) &= \frac{x}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(x)\\
&= x^2 + 2xy^2 - x^2\\
&= 2xy^2 = 2y^2h \quad \rightsquigarrow 0 \text{ by } red_G
\end{aligned}
$$

Buchberger's Algorithm for Computing Gröbner Bases

2. $s := \frac{\ell(g)}{gcd(\ell(f),\ell(g))} f - \frac{\ell(g)}{gcd(\ell(f),\ell(g))} g$

Example (GB($\{f = x^2 + 2xy^2,\ g = xy + 2y^3 - 1\}$ with $x \succ y$ lex)

$$S(f,g) = \frac{xy}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(xy + 2y^3 - 1)$$
$$= x^2y + 2xy^3 - (x^2y + 2xy^3 - x)$$
$$= x =: h \quad \rightsquigarrow G = \{f, g, h\}$$
$$S(g,h) = \frac{x}{x}(xy + 2y^3 - 1) - \frac{xy}{x}(x)$$
$$= xy + 2y^3 - 1 - xy \qquad G = \{x, 2y^3 - 1\}!$$
$$= 2y^3 - 1 =: e \quad \rightsquigarrow G = \{f, g, h, e\}$$
$$S(f,h) = \frac{x}{x}(x^2 + 2xy^2) - \frac{x^2}{x}(x)$$
$$= x^2 + 2xy^2 - x^2$$
$$= 2xy^2 = 2y^2h \quad \rightsquigarrow 0 \text{ by } red_G$$

Outline

The Nullstellensatz

Method is sound and complete over complex numbers:

Theorem (Hilbert's Nullstellensatz)

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

$\Rightarrow$ Method sound but cannot be complete over reals:

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

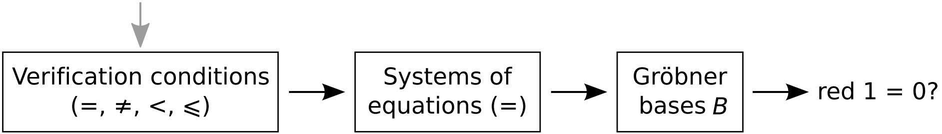
Next: an extension that is complete over the reals

The Real Nullstellensatz

Theorem (Stengle's Real Nullstellensatz, 1973)

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

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

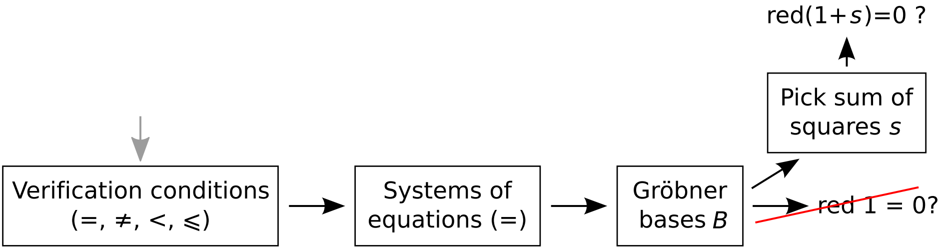


The Real Nullstellensatz

Theorem (Stengle's Real Nullstellensatz, 1973)

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

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



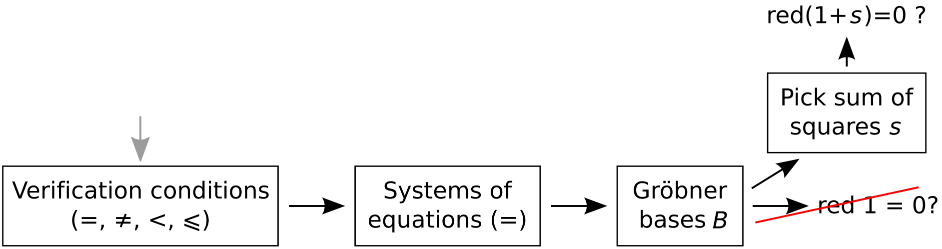
The Real Nullstellensatz

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 $s_1^2 + \cdots + s_n^2$?

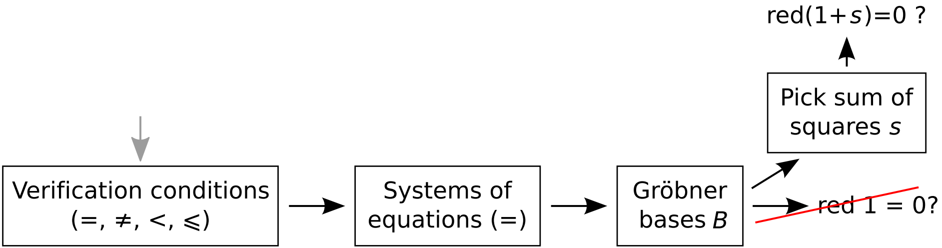


The Real Nullstellensatz

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

E.g.

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



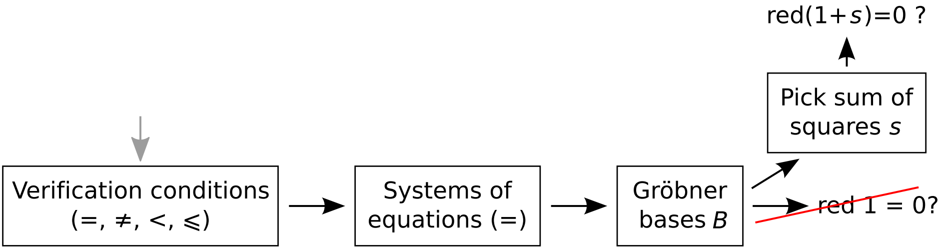
The Real Nullstellensatz

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

1. X is symmetric (i.e., $X^t = X$)
2. $x^t X x \geq 0$ for all $x \in \mathbb{R}^n$.

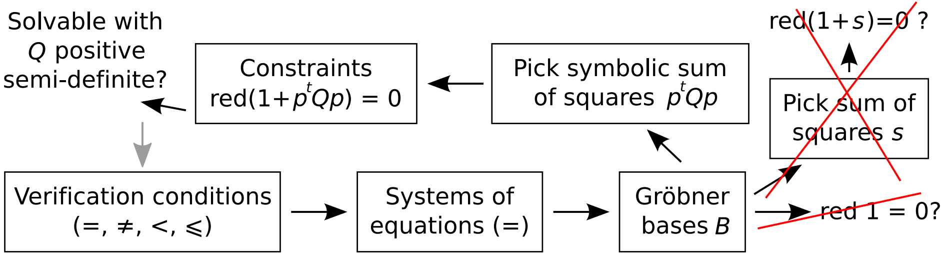


Lemma

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

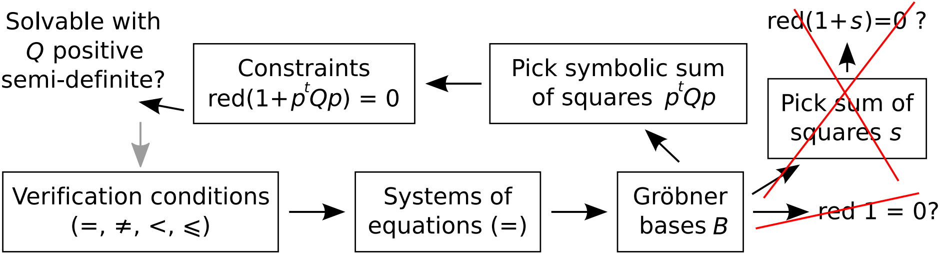
1. X is symmetric (i.e., $X^t = X$)
2. $x^t Xx \geq 0$ for all $x \in \mathbb{R}^n$.



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 p 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)

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

Example (2)

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

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

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

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

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

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

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

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 → decision procedure
- In practice:
  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]

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \notin t$)

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \notin t$)
  $\rightsquigarrow$ x and polynomial can be eliminated

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \not\in t$)
  $\leadsto$ x and polynomial can be eliminated
- Rewriting with polynomials $\alpha_0^2 x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$
  (where $\alpha_i > 0$ and x only with even degree elsewhere)

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \notin t$)
  $\rightsquigarrow$ x and polynomial can be eliminated
- Rewriting with polynomials $\alpha_0^2 x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$
  (where $\alpha_i > 0$ and x only with even degree elsewhere)
  $\rightsquigarrow$ x and polynomial can be eliminated

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \not\in t$)
  $\leadsto$ x and polynomial can be eliminated
- Rewriting with polynomials $\alpha_0^2 x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$
  (where $\alpha_i > 0$ and x only with even degree elsewhere)
  $\leadsto$ x and polynomial can be eliminated
- Elimination of polynomials $xy - 1$, $x^n + t$ (where $x^n \not| t$)

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \notin t$)
  $\leadsto$ x and polynomial can be eliminated
- Rewriting with polynomials $\alpha_0^2 x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$
  (where $\alpha_i > 0$ and x only with even degree elsewhere)
  $\leadsto$ x and polynomial can be eliminated
- Elimination of polynomials $xy - 1$, $x^n + t$ (where $x^n \not| t$)
  $\leadsto$ x and polynomial $xy - 1$ can be eliminated by multiplying all polynomials with some y^m and reducing with $xy - 1$

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \notin t$)
  $\leadsto$ x and polynomial can be eliminated
- Rewriting with polynomials $\alpha_0^2 x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$
  (where $\alpha_i > 0$ and x only with even degree elsewhere)
  $\leadsto$ x and polynomial can be eliminated
- Elimination of polynomials $xy - 1$, $x^n + t$ (where $x^n \not| t$)
  $\leadsto$ x and polynomial $xy - 1$ can be eliminated by multiplying all polynomials with some y^m and reducing with $xy - 1$
- Splitting polynomials $\alpha_1 m_1^2 + \cdots + \alpha_n m_n^2 \in B$ with $\alpha_i > 0$

Optimizations

Pre-processing of Gröbner basis is a good idea:

- Rewriting with polynomials $x + t$ (where $x \notin t$)
  $\rightsquigarrow$ x and polynomial can be eliminated
- Rewriting with polynomials $\alpha_0^2 x^2 - \alpha_1 m_1^2 - \cdots - \alpha_n m_n^2$
  (where $\alpha_i > 0$ and x only with even degree elsewhere)
  $\rightsquigarrow$ x and polynomial can be eliminated
- Elimination of polynomials $xy - 1$, $x^n + t$ (where $x^n \not| t$)
  $\rightsquigarrow$ x and polynomial $xy - 1$ can be eliminated by multiplying all polynomials with some y^m and reducing with $xy - 1$
- Splitting polynomials $\alpha_1 m_1^2 + \cdots + \alpha_n m_n^2 \in B$ with $\alpha_i > 0$
  $\rightsquigarrow$ replace by $m_1, \ldots, m_n$

Outline

Other Approaches

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 → 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**: our implementation in KeYmaera

Benchmarks: 100 problems taken from . . .

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

Experiments