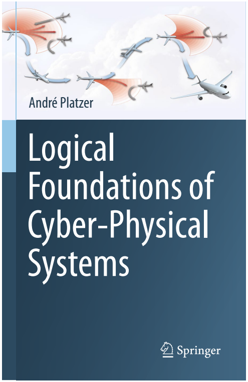
20: Virtual Substitution & Real Equations

Logical Foundations of Cyber-Physical Systems



André Platzer

Carnegie Mellon University
Computer Science Department

Outline

1. Learning Objectives
2. Framing the Miracle
3. Quantifier Elimination
   - Homomorphic Normalization for QE
   - Term Substitutions for Linear Equations
4. Square Root $\sqrt{\cdot}$ Virtual Substitution for Quadratics
   - Square Root Algebra
   - Virtual Substitutions of Square Roots
   - Example
5. Summary

Outline

1 Learning Objectives

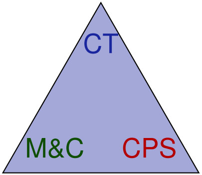
2 Framing the Miracle

3 Quantifier Elimination
- Homomorphic Normalization for QE
- Term Substitutions for Linear Equations

4 Square Root $\sqrt{\cdot}$ Virtual Substitution for Quadratics
- Square Root Algebra
- Virtual Substitutions of Square Roots
- Example

5 Summary

rigorous arithmetical reasoning
miracle of quantifier elimination
logical trinity for reals
switch between syntax & semantics at will
virtual substitution lemma
bridge gap between semantics and inexpressibles



analytic complexity
modeling tradeoffs

verifying CPS at scale

Outline

1. Learning Objectives
2. Framing the Miracle
3. Quantifier Elimination
   - Homomorphic Normalization for QE
   - Term Substitutions for Linear Equations
4. Square Root $\sqrt{\cdot}$ Virtual Substitution for Quadratics
   - Square Root Algebra
   - Virtual Substitutions of Square Roots
   - Example
5. Summary

Evaluating Real Arithmetic Formulas

$x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!]$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \leq 2^2 = \mathit{false}$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \leq 2^2 = \mathit{false}$$

When $\nu(x) = -1$

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!]$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \leq 2^2 = \mathit{false}$$

When $\nu(x) = -1$

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = (-1)^2 > 2 \land 2 \cdot (-1) < 3 \lor (-1)^3 \leq (-1)^2 = \mathit{true}$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \leq 2^2 = \mathit{false}$$

When $\nu(x) = -1$

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = (-1)^2 > 2 \land 2 \cdot (-1) < 3 \lor (-1)^3 \leq (-1)^2 = \mathit{true}$$

Are the following formulas valid, i.e., true in all states?

$$x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2$$
$$\forall x\, (x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2)$$
$$\exists x\, (x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2)$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \le x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \le 2^2 = \mathit{false}$$

When $\nu(x) = -1$

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 \le x^2]\!] = (-1)^2 > 2 \land 2 \cdot (-1) < 3 \lor (-1)^3 \le (-1)^2 = \mathit{true}$$

Are the following formulas valid, i.e., true in all states?

$$\not\models x^2 > 2 \land 2x < 3 \lor x^3 \le x^2$$
$$\forall x\, (x^2 > 2 \land 2x < 3 \lor x^3 \le x^2)$$
$$\exists x\, (x^2 > 2 \land 2x < 3 \lor x^3 \le x^2)$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \leq 2^2 = \mathit{false}$$

When $\nu(x) = -1$

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2]\!] = (-1)^2 > 2 \land 2 \cdot (-1) < 3 \lor (-1)^3 \leq (-1)^2 = \mathit{true}$$

Are the following formulas valid, i.e., true in all states?

$$\not\models x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2$$

$$\not\models \forall x\, (x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2)$$

$$\exists x\, (x^2 > 2 \land 2x < 3 \lor x^3 \leq x^2)$$

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 \le x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 \le 2^2 = \mathit{false}$$

When $\nu(x) = -1$

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 \le x^2]\!] = (-1)^2 > 2 \land 2 \cdot (-1) < 3 \lor (-1)^3 \le (-1)^2 = \mathit{true}$$

Are the following formulas valid, i.e., true in all states?

$$\not\models x^2 > 2 \land 2x < 3 \lor x^3 \le x^2$$
$$\not\models \forall x\, (x^2 > 2 \land 2x < 3 \lor x^3 \le x^2)$$
$$\models \exists x\, (x^2 > 2 \land 2x < 3 \lor x^3 \le x^2)$$

Is validity of formulas decidable/semidecidable/undecidable/not semidecidable for:

1. Propositional logic [no variables]
- ✓ $\mathrm{FOL}[p, f, \ldots]$ uninterpreted
2. $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$
3. $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$
4. $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$
5. $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] decidable
- ✓ FOL$[p, f, \dots]$ uninterpreted
- 2 FOL$_{\mathbb{N}}[+, \cdot, =]$
- 3 FOL$_{\mathbb{R}}[+, \cdot, =, <]$
- 4 FOL$_{\mathbb{Q}}[+, \cdot, =]$
- 5 FOL$_{\mathbb{C}}[+, \cdot, =]$

Framing the Miracle: Quiz

Is validity of formulas decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ $\mathrm{FOL}[p, f, \dots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- 2 $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$
- 3 $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$
- 4 $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$
- 5 $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

✓ Propositional logic [no variables] decidable

✓ FOL$[p, f, \dots]$ uninterpreted semidecidable [Gödel'30,Herbrand'30]

× FOL$_{\mathbb{N}}[+,\cdot,=]$ Peano arithmetic not semidecidable [Gödel'31]

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

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ FOL$[p, f, \dots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$ — decidable [Tarski'31..51]
- 4. $\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$
- 5. $\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ FOL$[p, f, \dots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$ — decidable [Tarski'31..51]
- × $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$ — not semidecidable [Robinson'49]
5. $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ $\mathrm{FOL}[p, f, \ldots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$ — decidable [Tarski'31..51]
- × $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$ — not semidecidable [Robinson'49]
- ✓ $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$ — decidable [Tarski'51,Chevalley'51]

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ $\mathrm{FOL}[p, f, \dots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$ — decidable [Tarski'31..51]
- × $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$ — not semidecidable [Robinson'49]
- ✓ $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$ — decidable [Tarski'51,Chevalley'51]

6. $\mathrm{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$
7. $\mathrm{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$
8. $\mathrm{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$
9. $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$
10. $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ FOL$[p, f, \dots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$ — decidable [Tarski'31..51]
- × $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$ — not semidecidable [Robinson'49]
- ✓ $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$ — decidable [Tarski'51,Chevalley'51]
- ✓ $\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$ — decidable Gaussian elim. [179 CE]

7. $\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$
8. $\text{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$
9. $\text{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$
10. $\text{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ $\mathrm{FOL}[p, f, \ldots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$ — decidable [Tarski'31..51]
- × $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$ — not semidecidable [Robinson'49]
- ✓ $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$ — decidable [Tarski'51,Chevalley'51]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$ — decidable Gaussian elim. [179 CE]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$ — decidable [Fourier 1826]

8. $\mathrm{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \ldots]$
9. $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$
10. $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$

Framing the Miracle: Quiz

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ FOL$[p, f, \dots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$ — decidable [Tarski'31..51]
- × $\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$ — not semidecidable [Robinson'49]
- ✓ $\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$ — decidable [Tarski'51,Chevalley'51]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+,=,\wedge,\exists]$ — decidable Gaussian elim. [179 CE]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+,\leq,\wedge,\exists]$ — decidable [Fourier 1826]
- ✓ $\mathrm{FOL}_{\mathbb{N}}[+,=,2|,3|,\dots]$ — decidable [Presburger'29,Skolem'31]
- 9 $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\exp,=,<]$
- 10 $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\sin,=,<]$

Framing the Miracle: Quiz

Is validity of formulas
decidable/semidecidable/undecidable/not semidecidable for:

- ✓ Propositional logic [no variables] — decidable
- ✓ $\mathrm{FOL}[p, f, \ldots]$ uninterpreted — semidecidable [Gödel'30,Herbrand'30]
- × $\mathrm{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic — not semidecidable [Gödel'31]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, =, <]$ — decidable [Tarski'31..51]
- × $\mathrm{FOL}_{\mathbb{Q}}[+, \cdot, =]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$ — not semidecidable [Robinson'49]
- ✓ $\mathrm{FOL}_{\mathbb{C}}[+, \cdot, =]$ — decidable [Tarski'51,Chevalley'51]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$ — decidable Gaussian elim. [179 CE]
- ✓ $\mathrm{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$ — decidable [Fourier 1826]
- ✓ $\mathrm{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \ldots]$ — decidable [Presburger'29,Skolem'31]
- ? $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$ — unknown
- 10 $\mathrm{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$

Framing the Miracle: Quiz

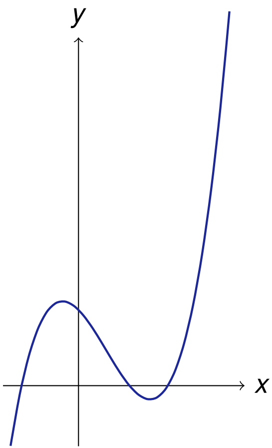
Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:

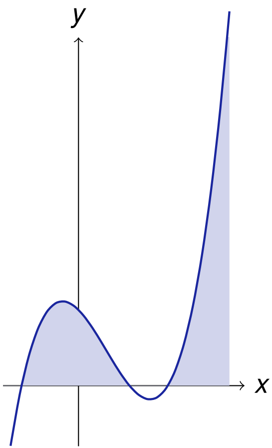
✓	Propositional logic [no variables]	decidable
✓	$\text{FOL}[p, f, \ldots]$ uninterpreted	semidecidable [Gödel'30,Herbrand'30]
×	$\text{FOL}_{\mathbb{N}}[+, \cdot, =]$ Peano arithmetic	not semidecidable [Gödel'31]
✓	$\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$	decidable [Tarski'31..51]
×	$\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$ $\sqrt{2} \notin \mathbb{Q}$, $\exists x\, x^2 = 2$	not semidecidable [Robinson'49]
✓	$\text{FOL}_{\mathbb{C}}[+, \cdot, =]$	decidable [Tarski'51,Chevalley'51]
✓	$\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$	decidable Gaussian elim. [179 CE]
✓	$\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$	decidable [Fourier 1826]
✓	$\text{FOL}_{\mathbb{N}}[+, =, 2\vert, 3\vert, \ldots]$	decidable [Presburger'29,Skolem'31]
?	$\text{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$	unknown
×	$\text{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$ $\sin x = 0$	not semidecidable [Richardson'68]

Outline

1. Learning Objectives
2. Framing the Miracle
3. Quantifier Elimination
   - Homomorphic Normalization for QE
   - Term Substitutions for Linear Equations
4. Square Root $\sqrt{\cdot}$ Virtual Substitution for Quadratics
   - Square Root Algebra
   - Virtual Substitutions of Square Roots
   - Example
5. Summary

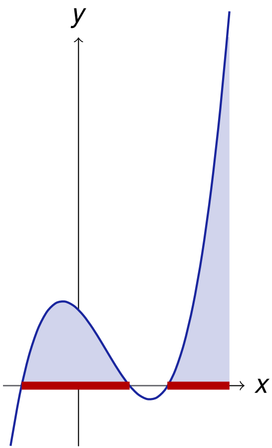


$$F \equiv \exists y\, (y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$

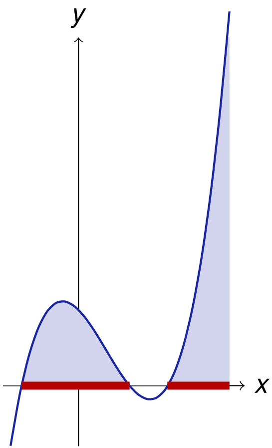


$$F \equiv \exists y\,(y \geq 0 \land 1 - x - 1.83x^2 + 1.66x^3 > y)$$

Quantifier Elimination ⇝ Projection



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



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

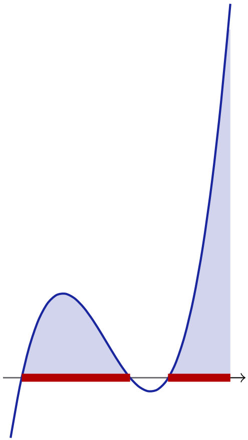
QE

$$\mathrm{QE}(F) \equiv -0.75 < x \land x < 0.68 \lor x > 1.18$$

Quantifier Elimination $\leftrightsquigarrow$ Projection

$\text{QE}(F) \equiv -0.75 < x \land x < 0.68 \lor x > 1.18$

Quantifier Elimination $\leftrightsquigarrow$ Projection

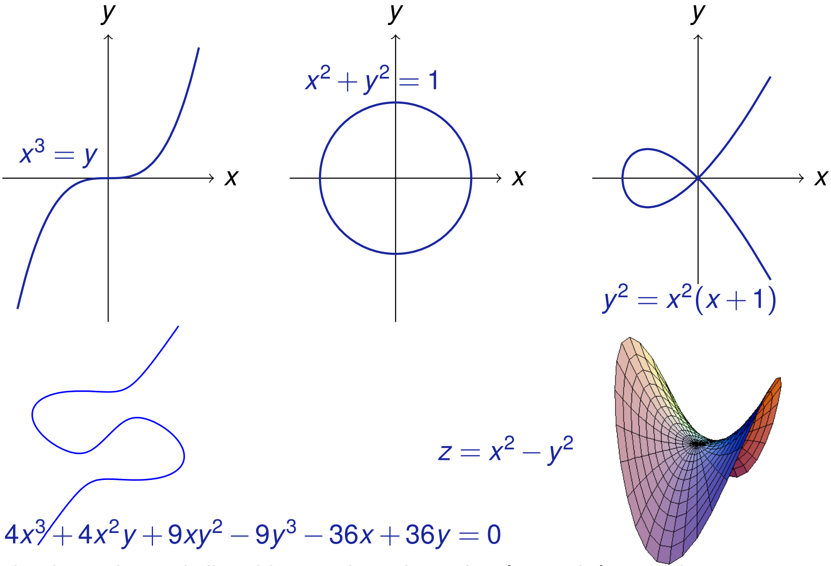


$$F \equiv \exists y\,(y \geq 0 \land 1 - x - 1.83x^2 + 1.66x^3 > y)$$

QE

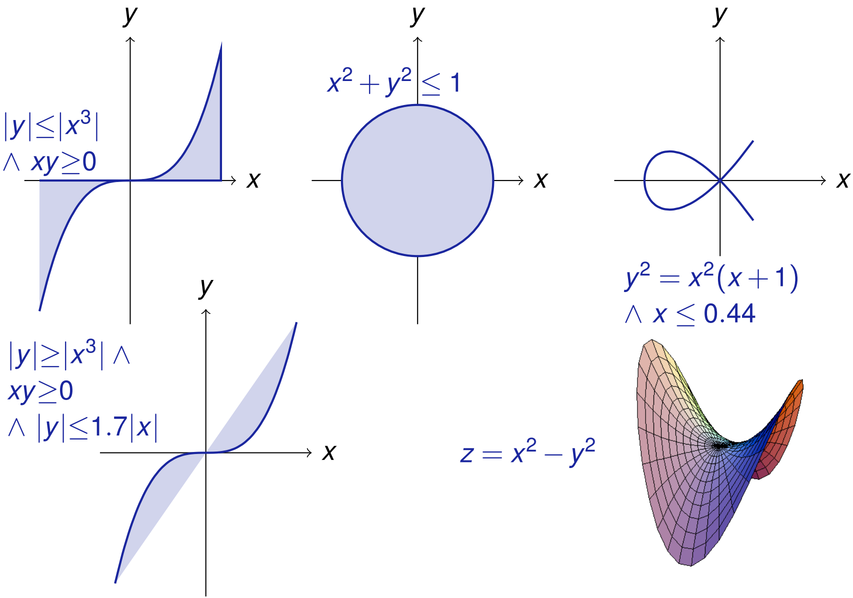
$$\mathrm{QE}(F) \equiv -0.75 < x \land x < 0.68 \lor x > 1.18$$

If all but one variable has fixed value: Finite union of intervals.
Univariate polynomials have finitely many roots. Signs change finitely often.



Algebraic variety: defined by conjunction of polynomial equations

Polynomial Inequalities $\leftrightsquigarrow$ Semialgebraic Sets



Theorem (Tarski'31)

First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e., for each formula P, compute quantifier-free formula $\mathrm{QE}(P)$ *that is equivalent, i.e.,* $P \leftrightarrow \mathrm{QE}(P)$ *is valid.*

Quantifier Elimination in Real Arithmetic

Theorem (Tarski'31)

First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e., for each formula P, compute quantifier-free formula $\mathrm{QE}(P)$ that is equivalent, i.e., $P \leftrightarrow \mathrm{QE}(P)$ is valid.

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

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

$$2^{2^{O(n)}}$$

Quantifier Elimination in Real Arithmetic

Theorem (Tarski'31)

First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e., for each formula P, compute quantifier-free formula $\mathrm{QE}(P)$ that is equivalent, i.e., $P \leftrightarrow \mathrm{QE}(P)$ is valid.

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

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

$$2^{2^{O(n)}}$$

Answer even for one *free* variable and only linear polynomials

Quantifier Elimination Examples

$$\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2 + c \le 5)) &\equiv \\
\mathrm{QE}(\forall c\,\exists x\,(2x^2 + c \le 5)) &\equiv
\end{aligned}$$

$$\begin{aligned}
\mathrm{QE}(\exists x\,(a = b + x^2)) &\equiv \\
\mathrm{QE}(\exists x\,(x^2 = 2)) &\equiv \\
\mathrm{QE}(\exists x\,(x^2 = 2 \land y = x)) &\equiv
\end{aligned}$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c\le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv
\end{aligned}
$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\leq 5)) &\equiv c\leq 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\leq 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\leq 5))
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv
\end{aligned}
$$

Quantifier Elimination Examples

$$\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\leq 5)) &\equiv c\leq 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\leq 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\leq 5)) \equiv \mathrm{QE}(\forall c\,(c\leq 5))
\end{aligned}$$

$$\begin{aligned}
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2\wedge y=x)) &\equiv
\end{aligned}$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c\le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\le 5)) \equiv \mathrm{QE}(\forall c\,(c\le 5))\\
&\equiv -100\le 5\land 5\le 5\land 100\le 5\\
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv
\end{aligned}
$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c\le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\le 5)) \equiv \mathrm{QE}(\forall c\,(c\le 5))\\
&\equiv -100\le 5\land 5\le 5\land 100\le 5\equiv \mathit{false}\\
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv
\end{aligned}
$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c\le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\le 5)) \equiv \mathrm{QE}(\forall c\,(c\le 5))\\
&\equiv -100\le 5\land 5\le 5\land 100\le 5 \equiv \mathit{false}\\
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv a\ge b\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv
\end{aligned}
$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c\le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\le 5)) \equiv \mathrm{QE}(\forall c\,(c\le 5))\\
&\equiv -100\le 5\land 5\le 5\land 100\le 5\equiv \mathit{false}\\
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv a\ge b\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv \mathit{true}\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv
\end{aligned}
$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c\le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\le 5)) \equiv \mathrm{QE}(\forall c\,(c\le 5))\\
&\equiv -100\le 5\land 5\le 5\land 100\le 5\equiv \mathit{false}\\
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv a\ge b\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv \mathit{true}\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv y=\pm\sqrt{2}
\end{aligned}
$$

Quantifier Elimination Examples

$$
\begin{aligned}
\mathrm{QE}(\exists x\,(2x^2+c\le 5)) &\equiv c \le 5\\
\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\le 5)) &\equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\le 5)) \equiv \mathrm{QE}(\forall c\,(c\le 5))\\
&\equiv -100\le 5\land 5\le 5\land 100\le 5 \equiv \mathit{false}\\
\mathrm{QE}(\exists x\,(a=b+x^2)) &\equiv a\ge b\\
\mathrm{QE}(\exists x\,(x^2=2)) &\equiv \mathit{true}\\
\mathrm{QE}(\exists x\,(x^2=2\land y=x)) &\equiv y=\pm\sqrt{2}\equiv y^2=2
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \\
\mathrm{QE}(A \vee B) &\equiv \\
\mathrm{QE}(\neg A) &\equiv \\
\mathrm{QE}(\forall x\, A) &\equiv \\
\mathrm{QE}(\exists x\, A) &\equiv && A \text{ has quantifiers}
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{QE}(A \land B) &\equiv \mathrm{QE}(A) \land \mathrm{QE}(B) \\
\mathrm{QE}(A \lor B) &\equiv \mathrm{QE}(A) \lor \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\, \mathrm{QE}(A)) && A \text{ has quantifiers}
\end{aligned}
$$

Framework: Logical Normalization for QE

$$
\begin{aligned}
\mathrm{QE}(A \land B) &\equiv \mathrm{QE}(A) \land \mathrm{QE}(B)\\
\mathrm{QE}(A \lor B) &\equiv \mathrm{QE}(A) \lor \mathrm{QE}(B)\\
\mathrm{QE}(\neg A) &\equiv \neg\,\mathrm{QE}(A)\\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A)\\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\, \mathrm{QE}(A)) && A \text{ has quantifiers}\\
\mathrm{QE}(\exists x\, (A \lor B)) &\equiv\\
\mathrm{QE}(\exists x\, \neg(A \land B)) &\equiv\\
\mathrm{QE}(\exists x\, \neg(A \lor B)) &\equiv\\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv
\end{aligned}
$$

Framework: Logical Normalization for QE

$$
\begin{aligned}
\mathrm{QE}(A \land B) &\equiv \mathrm{QE}(A) \land \mathrm{QE}(B)\\
\mathrm{QE}(A \lor B) &\equiv \mathrm{QE}(A) \lor \mathrm{QE}(B)\\
\mathrm{QE}(\neg A) &\equiv \neg\,\mathrm{QE}(A)\\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A)\\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\, \mathrm{QE}(A)) && A \text{ has quantifiers}\\
\mathrm{QE}(\exists x\, (A \lor B)) &\equiv \mathrm{QE}(\exists x\, A) \lor \mathrm{QE}(\exists x\, B)\\
\mathrm{QE}(\exists x\, \neg(A \land B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \lor \neg B))\\
\mathrm{QE}(\exists x\, \neg(A \lor B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \land \neg B))\\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv \mathrm{QE}(\exists x\, A)
\end{aligned}
$$

Framework: Logical Normalization for QE

$$
\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\, \mathrm{QE}(A)) && A \text{ has quantifiers} \\
\mathrm{QE}(\exists x\, (A \vee B)) &\equiv \mathrm{QE}(\exists x\, A) \vee \mathrm{QE}(\exists x\, B) \\
\mathrm{QE}(\exists x\, \neg(A \wedge B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \vee \neg B)) \\
\mathrm{QE}(\exists x\, \neg(A \vee B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \wedge \neg B)) \\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv \mathrm{QE}(\exists x\, A) \\
\mathrm{QE}(\exists x\, (A \wedge (B \vee C))) &\equiv \\
\mathrm{QE}(\exists x\, ((A \vee B) \wedge C)) &\equiv
\end{aligned}
$$

Framework: Logical Normalization for QE

$$
\begin{aligned}
\mathrm{QE}(A \land B) &\equiv \mathrm{QE}(A) \land \mathrm{QE}(B) \\
\mathrm{QE}(A \lor B) &\equiv \mathrm{QE}(A) \lor \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\, \mathrm{QE}(A)) && \text{A has quantifiers} \\
\mathrm{QE}(\exists x\, (A \lor B)) &\equiv \mathrm{QE}(\exists x\, A) \lor \mathrm{QE}(\exists x\, B) \\
\mathrm{QE}(\exists x\, \neg(A \land B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \lor \neg B)) \\
\mathrm{QE}(\exists x\, \neg(A \lor B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \land \neg B)) \\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv \mathrm{QE}(\exists x\, A) \\
\mathrm{QE}(\exists x\, (A \land (B \lor C))) &\equiv \mathrm{QE}(\exists x\, ((A \land B) \lor (A \land C))) && \text{expensive} \\
\mathrm{QE}(\exists x\, ((A \lor B) \land C)) &\equiv \mathrm{QE}(\exists x\, ((A \land C) \lor (B \land C))) && \text{expensive}
\end{aligned}
$$

Framework: Logical Normalization for QE

Normal Form $\text{QE}(\exists x\,(A_1 \land \ldots \land A_k))$ with atomic A_i

$$
\begin{aligned}
\text{QE}(A \land B) &\equiv \text{QE}(A) \land \text{QE}(B) \\
\text{QE}(A \lor B) &\equiv \text{QE}(A) \lor \text{QE}(B) \\
\text{QE}(\neg A) &\equiv \neg\,\text{QE}(A) \\
\text{QE}(\forall x\,A) &\equiv \text{QE}(\neg\exists x\,\neg A) \\
\text{QE}(\exists x\,A) &\equiv \text{QE}(\exists x\,\text{QE}(A)) && A \text{ has quantifiers} \\
\text{QE}(\exists x\,(A \lor B)) &\equiv \text{QE}(\exists x\,A) \lor \text{QE}(\exists x\,B) \\
\text{QE}(\exists x\,\neg(A \land B)) &\equiv \text{QE}(\exists x\,(\neg A \lor \neg B)) \\
\text{QE}(\exists x\,\neg(A \lor B)) &\equiv \text{QE}(\exists x\,(\neg A \land \neg B)) \\
\text{QE}(\exists x\,\neg\neg A) &\equiv \text{QE}(\exists x\,A) \\
\text{QE}(\exists x\,(A \land (B \lor C))) &\equiv \text{QE}(\exists x\,((A \land B) \lor (A \land C))) && \text{expensive} \\
\text{QE}(\exists x\,((A \lor B) \land C)) &\equiv \text{QE}(\exists x\,((A \land C) \lor (B \land C))) && \text{expensive}
\end{aligned}
$$

Normal Form $\mathrm{QE}(\exists x\,(p_1 \sim_i 0 \land \ldots \land p_k \sim_k 0))$ and $\sim_i \in \{>,=,\geq,\neq\}$

$$
\begin{aligned}
p = q &\equiv p - q = 0\\
p \geq q &\equiv p - q \geq 0\\
p > q &\equiv p - q > 0\\
p \neq q &\equiv p - q \neq 0\\
p \leq q &\equiv q - p \geq 0\\
p < q &\equiv q - p > 0\\
\neg(p \geq q) &\equiv p < q\\
\neg(p > q) &\equiv p \leq q\\
\neg(p = q) &\equiv p \neq q\\
\neg(p \neq q) &\equiv p = q
\end{aligned}
$$

Virtual Substitution

$$\exists x\, F \leftrightarrow \bigvee_{t \in T} A_t \land F_x^t$$

where terms T substituted (virtually) into F depend on F
where A_t are quantifier-free additional compatibility conditions

Scalability requires simplifier for intermediate results

Quantifier Elimination by Virtual Substitution

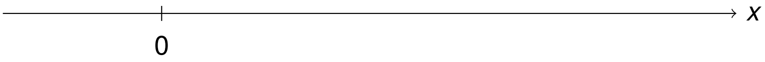
Virtual Substitution

Quantifier $\exists x\, F \leftrightarrow \bigvee_{t \in T} A_t \wedge F_x^t$ Quantifier-free

where terms T substituted (virtually) into F depend on F
where A_t are quantifier-free additional compatibility conditions

Scalability requires simplifier for intermediate results

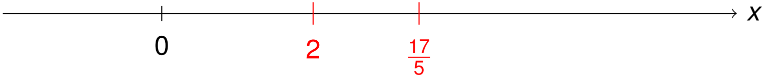
Naïve Virtual Substitution by Example



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

$$\exists x \left(x > 2 \land x < \frac{17}{5} \right)$$

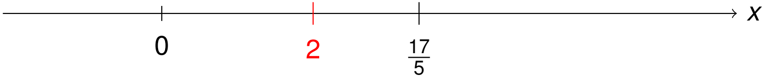
Naïve Virtual Substitution by Example



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

$$\exists x (x > 2 \land x < \frac{17}{5})$$

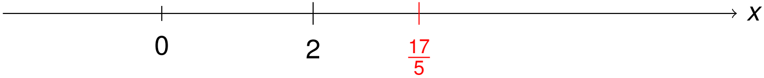
Naïve Virtual Substitution by Example



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

$$
\begin{aligned}
& \exists x\,(x > 2 \land x < \tfrac{17}{5}) \\
\equiv \quad & (2 > 2 \land 2 < \tfrac{17}{5}) \qquad \text{boundary case “}x = 2\text{”}
\end{aligned}
$$

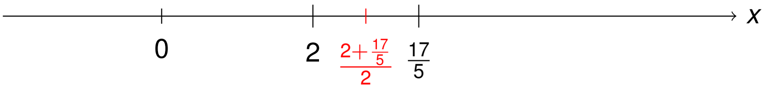
Naïve Virtual Substitution by Example



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

$$
\begin{array}{lll}
 & \exists x\,(x > 2 \land x < \frac{17}{5}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{5}) & \text{boundary case “}x = 2\text{”} \\
\lor & (\frac{17}{5} > 2 \land \frac{17}{5} < \frac{17}{5}) & \text{boundary case “}x = \frac{17}{5}\text{”}
\end{array}
$$

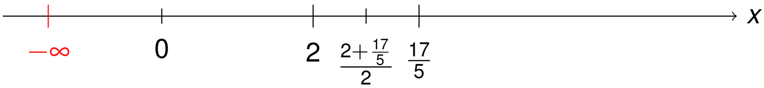
Naïve Virtual Substitution by Example



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

$$
\begin{array}{lll}
 & \exists x (x > 2 \land x < \frac{17}{5}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{5}) & \text{boundary case "} x = 2 \text{"} \\
\lor & (\frac{17}{5} > 2 \land \frac{17}{5} < \frac{17}{5}) & \text{boundary case "} x = \frac{17}{5} \text{"} \\
\lor & (\frac{2+\frac{17}{5}}{2} > 2 \land \frac{2+\frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case "} x = \frac{2+\frac{17}{5}}{2} \text{"}
\end{array}
$$

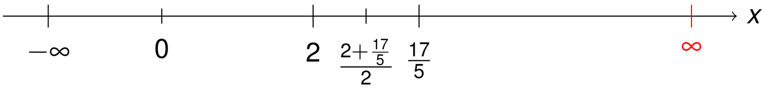
Naïve Virtual Substitution by Example



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

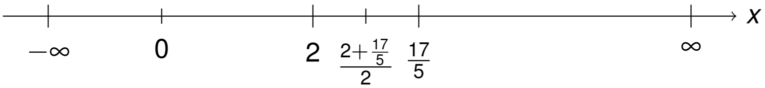
$$
\begin{array}{lll}
 & \exists x (x > 2 \land x < \frac{17}{5}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{5}) & \text{boundary case “}x = 2\text{”} \\
\lor & (\frac{17}{5} > 2 \land \frac{17}{5} < \frac{17}{5}) & \text{boundary case “}x = \frac{17}{5}\text{”} \\
\lor & (\frac{2+\frac{17}{5}}{2} > 2 \land \frac{2+\frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case “}x = \frac{2+\frac{17}{5}}{2}\text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{5}) & \text{extremal case “}x = -\infty\text{”}
\end{array}
$$

Naïve Virtual Substitution by Example



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

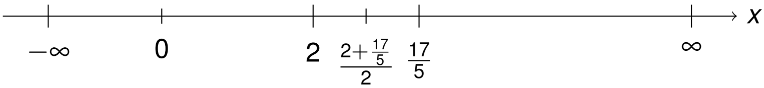
$$
\begin{array}{cll}
 & \exists x\,(x > 2 \land x < \frac{17}{5}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{5}) & \text{boundary case “}x = 2\text{”} \\
\lor & (\frac{17}{5} > 2 \land \frac{17}{5} < \frac{17}{5}) & \text{boundary case “}x = \frac{17}{5}\text{”} \\
\lor & (\frac{2+\frac{17}{5}}{2} > 2 \land \frac{2+\frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case “}x = \frac{2+\frac{17}{5}}{2}\text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{5}) & \text{extremal case “}x = -\infty\text{”} \\
\lor & (\infty > 2 \land \infty < \frac{17}{5}) & \text{extremal case “}x = \infty\text{”}
\end{array}
$$



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

$$
\begin{array}{rll}
 & \exists x\,(x > 2 \land x < \frac{17}{5}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{5}) & \text{boundary case “}x = 2\text{”} \\
\lor & (\frac{17}{5} > 2 \land \frac{17}{5} < \frac{17}{5}) & \text{boundary case “}x = \frac{17}{5}\text{”} \\
\lor & (\frac{2+\frac{17}{5}}{2} > 2 \land \frac{2+\frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case “}x = \frac{2+\frac{17}{5}}{2}\text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{5}) & \text{extremal case “}x = -\infty\text{”} \\
\lor & (\infty > 2 \land \infty < \frac{17}{5}) & \text{extremal case “}x = \infty\text{”} \\
\equiv & \mathit{true} & \text{evaluate}
\end{array}
$$

Naïve Virtual Substitution by Example



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

$$
\begin{array}{cll}
 & \exists x\,(x > 2 \land x < \frac{17}{5}) & \\
\equiv & (2 > 2 \land 2 < \frac{17}{5}) & \text{boundary case “}x = 2\text{”} \\
\lor & (\frac{17}{5} > 2 \land \frac{17}{5} < \frac{17}{5}) & \text{boundary case “}x = \frac{17}{5}\text{”} \\
\lor & (\frac{2+\frac{17}{5}}{2} > 2 \land \frac{2+\frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case “}x = \frac{2+\frac{17}{5}}{2}\text{”} \\
\lor & (-\infty > 2 \land -\infty < \frac{17}{5}) & \text{extremal case “}x = -\infty\text{”} \\
\lor & (\infty > 2 \land \infty < \frac{17}{5}) & \text{extremal case “}x = \infty\text{”} \\
\equiv & \mathit{true} & \text{evaluate}
\end{array}
$$

- ∞ is not in $\mathrm{FOL}_{\mathbb{R}}$
- Interior points aren't always terms in $\mathrm{FOL}_{\mathbb{R}}$ if nonlinear
- Substituting them into formulas requires attention

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

$$\exists x\,(bx + c = 0 \land F) \;\leftrightarrow$$

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

$$\exists x\,(bx + c = 0 \land F) \;\leftrightarrow\; F_x^{-c/b}$$

Linear solution

Theorem (Virtual Substitution: Linear Equation)

$$\exists x \, (bx + c = 0 \land F) \; \leftrightarrow \; b \neq 0 \land F_x^{-c/b}$$

Don't divide by 0

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

$$b \neq 0 \rightarrow \left(\exists x\,(bx + c = 0 \land F) \;\leftrightarrow\; b \neq 0 \land F_x^{-c/b}\right)$$

Only actually linear solution if $b \neq 0$

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation $x \notin b, c$)

$$b \neq 0 \rightarrow \left(\exists x\,(bx + c = 0 \land F) \leftrightarrow b \neq 0 \land F_x^{-c/b}\right) \quad \textit{if } x \notin b, c$$

Only linear if no x in b, c

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation $x \notin b, c$)

$$b \neq 0 \rightarrow \big(\exists x\,(bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b}\big) \quad \textit{if } x \notin b, c$$

Conditional equivalence, so conditions may need to be checked or case-split

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation $x \notin b, c$)

$$b \neq 0 \rightarrow \big(\exists x\,(bx + c = 0 \land F) \leftrightarrow b \neq 0 \land F_x^{-c/b}\ \big) \quad \text{if } x \notin b, c$$

Lemma (Uniform substitution of linear equations)

The linear equation axiom is sound (b, c are arity 0 function symbols):

$$\exists lin \quad b \neq 0 \rightarrow \big(\exists x\,(b \cdot x + c = 0 \land q(x)) \leftrightarrow q(-c/b)\big)$$

$$\exists x\,(\underbrace{(y^2+4)}_{b} \cdot x + \underbrace{(yz-1)}_{c} = 0 \land x^3 + x \geq 0) \leftrightarrow \left(-\frac{yz-1}{y^2+4}\right)^3 + \left(-\frac{yz-1}{y^2+4}\right) \geq 0$$

Outline

1. Learning Objectives
2. Framing the Miracle
3. Quantifier Elimination
   - Homomorphic Normalization for QE
   - Term Substitutions for Linear Equations
4. Square Root $\sqrt{\cdot}$ Virtual Substitution for Quadratics
   - Square Root Algebra
   - Virtual Substitutions of Square Roots
   - Example
5. Summary

Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$

$$F_x^{(-b+\sqrt{b^2-4ac})/(2a)}$$

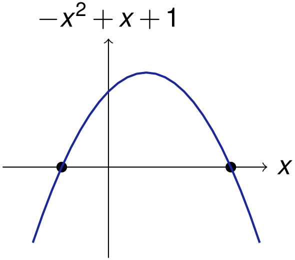
Quadratic solution

Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x\,(ax^2+bx+c=0 \land F) \leftrightarrow$$

$$\left(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\right)$$

Or negative square root solution



Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$

$$a \neq 0 \land \qquad \left(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\right)$$

Don't divide by 0

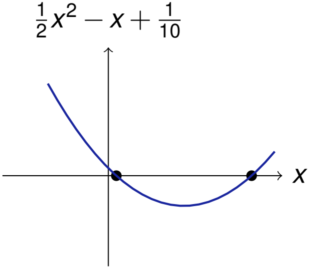
Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x\, (ax^2 + bx + c = 0 \land F) \leftrightarrow$$

$$a \neq 0 \land b^2 - 4ac \geq 0 \land \left(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\right)$$

Real solution if $\sqrt{\cdot}$ exists by discriminant



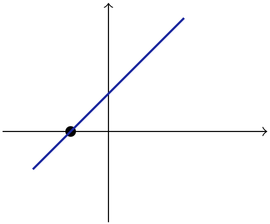
Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$

$$a = 0 \land b \neq 0 \land F_x^{-c/b}$$

$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \left(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\right)$$

Instead linear solution if $a = 0$ (may case-split)



Theorem (Virtual Substitution: Quadratic Equation)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_x^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

Only equivalent if not all 0 which gives trivial equation (else use F)

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_x^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

Only linear or quadratic if no x in a, b, c

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$
\begin{aligned}
& a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow \\
& \quad \Big(\exists x \, (ax^2 + bx + c = 0 \land F) \leftrightarrow \\
& \qquad a = 0 \land b \neq 0 \land F_x^{-c/b} \\
& \quad \lor a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)} \big) \Big)
\end{aligned}
$$

1. Quantifier-free equivalent

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_x^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

1. Quantifier-free equivalent
2. Just not a formula . . .

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow \Big(\exists x \,(ax^2 + bx + c = 0 \land F) \leftrightarrow a = 0 \land b \neq 0 \land F_x^{-c/b} \lor a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

1. Quantifier-free equivalent
2. Just not a formula ...
3. $(-b + \sqrt{b^2 - 4ac})/(2a)$ is not in $\mathrm{FOL}_{\mathbb{R}}$ and neither is $-c/b$

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_x^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

1. Quantifier-free equivalent
2. Just not a formula . . .
3. $(-b+\sqrt{b^2-4ac})/(2a)$ is not in $\mathrm{FOL}_{\mathbb{R}}$ and neither is $-c/b$
4. Virtual substitution $F_{\bar{x}}^{(a+b\sqrt{c})/d}$ acts as if it were to substitute $(a+b\sqrt{c})/d$ for x in F

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\, (ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

1. Quantifier-free equivalent
2. Just not a formula ...
3. $(-b + \sqrt{b^2 - 4ac})/(2a)$ is not in $\mathrm{FOL}_{\mathbb{R}}$ and neither is $-c/b$
4. Virtual substitution $F_{\bar{x}}^{(a+b\sqrt{c})/d}$ acts as if it were to substitute $(a + b\sqrt{c})/d$ for x in F ... but it's merely equivalent

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

1. Quantifier-free equivalent
2. Just not a formula ...
3. $(-b + \sqrt{b^2 - 4ac})/(2a)$ is not in $\mathrm{FOL}_{\mathbb{R}}$ and neither is $-c/b$
4. Virtual substitution $F_{\bar{x}}^{(a+b\sqrt{c})/d}$ acts as if it were to substitute $(a + b\sqrt{c})/d$ for x in F ... but it's merely equivalent
5. $\exists r\,(r^2 = c)$ would do it for $\sqrt{c}$

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \left(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\right)\Big)$$

1. Quantifier-free equivalent
2. Just not a formula . . .
3. $(-b+\sqrt{b^2-4ac})/(2a)$ is not in $\mathrm{FOL}_{\mathbb{R}}$ and neither is $-c/b$
4. Virtual substitution $F_{\bar{x}}^{(a+b\sqrt{c})/d}$ acts as if it were to substitute $(a+b\sqrt{c})/d$ for x in F . . . but it's merely equivalent
5. $\exists r\,(r^2 = c)$ would do it for $\sqrt{c}$ but that's going in circles

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$
\begin{aligned}
&a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow \\
&\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow \\
&\qquad a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b} \\
&\quad \lor a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)
\end{aligned}
$$

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=}$$

Convention: On this slide c' is not a derivative but just another name ...

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a+b\sqrt{c})/d)$$

Convention: On this slide c' is not a derivative but just another name ...

Square Root Algebra

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a+b\sqrt{c})/d) \quad \text{by algebraic evaluation of } +, \cdot$$

Convention: On this slide c' is not a derivative but just another name ...

Square Root Algebra

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a+b\sqrt{c})/d) \quad \text{by algebraic evaluation of } +, \cdot$$

$\sqrt{c}$-algebra

Algebra of terms $(a+b\sqrt{c})/d$ with polynomials $a,b,c,d \in \mathbb{Q}[x_1,..,x_n]$:

$$((a+b\sqrt{c})/d)+((a'+b'\sqrt{c})/d') =$$
$$((a+b\sqrt{c})/d)\cdot((a'+b'\sqrt{c})/d') =$$

Convention: On this slide c' is not a derivative but just another name ...

Square Root Algebra

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a+b\sqrt{c})/d) \quad \text{by algebraic evaluation of } +, \cdot$$

$\sqrt{c}$-algebra

Algebra of terms $(a+b\sqrt{c})/d$ with polynomials $a,b,c,d \in \mathbb{Q}[x_1,..,x_n]$:

$$((a+b\sqrt{c})/d)+((a'+b'\sqrt{c})/d') = ((ad'+da')+(bd'+db')\sqrt{c})/(dd')$$

$$((a+b\sqrt{c})/d)\cdot((a'+b'\sqrt{c})/d') =$$

Convention: On this slide c' is not a derivative but just another name ...

Square Root Algebra

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a+b\sqrt{c})/d) \quad \text{by algebraic evaluation of } +, \cdot$$

$\sqrt{c}$-algebra

Algebra of terms $(a+b\sqrt{c})/d$ with polynomials $a, b, c, d \in \mathbb{Q}[x_1, .., x_n]$:

$$((a+b\sqrt{c})/d) + ((a'+b'\sqrt{c})/d') = ((ad'+da') + (bd'+db')\sqrt{c})/(dd')$$

$$((a+b\sqrt{c})/d) \cdot ((a'+b'\sqrt{c})/d') = ((aa'+bb'c) + (ab'+ba')\sqrt{c})/(dd')$$

Convention: On this slide c' is not a derivative but just another name ...

Square Root Algebra

Virtual Substitution into Polynomial

Virtually substitute $(a+b\sqrt{c})/d$ into a polynomial p:

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a+b\sqrt{c})/d) \quad \text{by algebraic evaluation of } +,\cdot$$

$\sqrt{c}$-algebra

Algebra of terms $(a+b\sqrt{c})/d$ with polynomials $a,b,c,d \in \mathbb{Q}[x_1,..,x_n]$:
where $c \geq 0, d, d' \neq 0$

$$((a+b\sqrt{c})/d) + ((a'+b'\sqrt{c})/d') = ((ad'+da') + (bd'+db')\sqrt{c})/(dd')$$
$$((a+b\sqrt{c})/d) \cdot ((a'+b'\sqrt{c})/d') = ((aa'+bb'c) + (ab'+ba')\sqrt{c})/(dd')$$

Convention: On this slide c' is not a derivative but just another name ...

Virtual Substitution into Comparisons

Virtually substitute $(a+b\sqrt{c})/d$ into a comparison $p \sim 0$:

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv$$

Virtual Substitution into Comparisons

Virtually substitute $(a+b\sqrt{c})/d$ into a comparison $p \sim 0$:

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0)$$

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

Virtually substitute $(a+b\sqrt{c})/d$ into a comparison $p \sim 0$:

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0)$$

$\sqrt{c}$-comparisons $\quad d \neq 0 \wedge c \geq 0$

$$(a+0\sqrt{c})/d = 0 \equiv$$

$$(a+0\sqrt{c})/d \leq 0 \equiv$$

$$(a+0\sqrt{c})/d < 0 \equiv$$

$$(a+b\sqrt{c})/d = 0 \equiv$$

$$(a+b\sqrt{c})/d \leq 0 \equiv$$

$$(a+b\sqrt{c})/d < 0 \equiv$$

Virtual Substitution into Comparisons

Virtually substitute $(a+b\sqrt{c})/d$ into a comparison $p \sim 0$:

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0)$$

$\sqrt{c}$-comparisons $\quad d \neq 0 \wedge c \geq 0$

$$(a+0\sqrt{c})/d = 0 \equiv a = 0$$

$$(a+0\sqrt{c})/d \leq 0 \equiv ad \leq 0$$

$$(a+0\sqrt{c})/d < 0 \equiv ad < 0$$

$$(a+b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2c = 0$$

$$(a+b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \wedge a^2 - b^2c \geq 0 \vee bd \leq 0 \wedge a^2 - b^2c \leq 0$$

$$(a+b\sqrt{c})/d < 0 \equiv ad < 0 \wedge a^2 - b^2c > 0$$
$$\vee\, bd \leq 0 \wedge (ad < 0 \vee a^2 - b^2c < 0)$$

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

Virtually substitute $(a+b\sqrt{c})/d$ into a comparison $p \sim 0$:

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0) \quad \text{accordingly for } \wedge, \vee, \ldots$$

$\sqrt{c}$-comparisons $\qquad d \neq 0 \wedge c \geq 0$

$$(a+0\sqrt{c})/d = 0 \equiv a = 0$$

$$(a+0\sqrt{c})/d \leq 0 \equiv ad \leq 0$$

$$(a+0\sqrt{c})/d < 0 \equiv ad < 0$$

$$(a+b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2 c = 0$$

$$(a+b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \wedge a^2 - b^2 c \geq 0 \vee bd \leq 0 \wedge a^2 - b^2 c \leq 0$$

$$(a+b\sqrt{c})/d < 0 \equiv ad < 0 \wedge a^2 - b^2 c > 0$$
$$\vee\, bd \leq 0 \wedge (ad < 0 \vee a^2 - b^2 c < 0)$$

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a,b,c$)

$$
\begin{aligned}
& a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow \\
& \quad \big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow \\
& \qquad a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b} \\
& \quad \lor a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\big)
\end{aligned}
$$

Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$)

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \big(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)$$

Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$)

Extended logic

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

$FOL_{\mathbb{R}}$

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$

$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$

$$a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b}$$

$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \left(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\right)\Big)$$

Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$)

Extended logic $\quad F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d} \quad$ $FOL_{\mathbb{R}}$

$$\omega_x^r \in [\![F]\!] \textit{ iff } \omega \in [\![F_{\bar{x}}^{(a+b\sqrt{c})/d}]\!] \textit{ where } r = (\omega[\![a]\!] + \omega[\![b]\!]\sqrt{\omega[\![c]\!]})/(\omega[\![d]\!]) \in \mathbb{R}$$

Example: Quadratic Curiosity

$$a \neq 0 \rightarrow (\exists x\,(ax^2+bx+c=0 \land ax^2+bx+c \leq 0) \leftrightarrow b^2-4ac \geq 0 \land true)$$

$$
\begin{aligned}
&(ax^2+bx+c)_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)}\\
=&a((-b+\sqrt{b^2-4ac})/(2a))^2+b((-b+\sqrt{b^2-4ac})/(2a))+c\\
=&a((b^2+b^2-4ac+(-b-b)\sqrt{b^2-4ac})/(4a^2))+(-b^2+b\sqrt{b^2-4ac})/(2a)+c\\
=&(ab^2+ab^2-4a^2c+(-ab-ab)\sqrt{b^2-4ac})/(4a^2)+(-b^2+2ac+b\sqrt{b^2-4ac})/(2a)\\
=&((ab^2+ab^2-4a^2c)2a+(-b^2+2ac)4a^2+((-ab-ab)2a+b4a^2)\sqrt{b^2-4ac})/(8a^3)\\
=&(\cancel{2a^2b^2}+\cancel{2a^2b^2}-\cancel{8a^3c}-\cancel{4a^2b^2}+\cancel{8a^3c}+(-\cancel{2a^2b}-\cancel{2a^2b}+\cancel{4a^2b})\sqrt{b^2-4ac})/(8a^3)\\
=&(0+0\sqrt{b^2-4ac})/(8a^3)=(0+0\sqrt{..})/1=0
\end{aligned}
$$

$$(ax^2+bx+c=0)_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \equiv ((0+0\sqrt{..})/1=0) \equiv (0\cdot 1=0) \equiv true$$

$$(ax^2+bx+c\leq 0)_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \equiv (\underbrace{(0+0\sqrt{..})/1}_{0} \leq 0) \equiv (0\cdot 1 \leq 0) \equiv true$$

Example: Nonnegative Roots of Quadratic Polynomials

$$a \neq 0 \to \big(\exists x\,(ax^2+bx+c=0 \land x \geq 0)$$
$$\leftrightarrow b^2-4ac \geq 0 \land \big(2ba \leq 0 \land 4ac \geq 0 \lor -2a \leq 0 \land 4ac \leq 0$$
$$\lor 2ba \leq 0 \land 4ac \geq 0 \lor 2a \leq 0 \land 4ac \leq 0)\big)$$

$$-(-b+\sqrt{b^2-4ac})/(2a) = ((-1+0\sqrt{b^2-4ac})/1)\cdot((-b+\sqrt{b^2-4ac})/(2a)$$
$$= (b-\sqrt{b^2-4ac})/(2a)$$

$$(-x \leq 0)_{\bar{x}}^{(b-\sqrt{b^2-4ac})/(2a)}$$
$$\equiv b2a \leq 0 \land \cancel{b^2}-(-1)^2(\cancel{b^2}-4ac) \geq 0 \lor -1\cdot 2a \leq 0 \land \cancel{b^2}-(-1)^2(\cancel{b^2}-4ac) \leq 0$$
$$\equiv 2ba \leq 0 \land 4ac \geq 0 \lor -2a \leq 0 \land 4ac \leq 0$$

$$(-x \leq 0)_{\bar{x}}^{(b+\sqrt{b^2-4ac})/(2a)}$$
$$\equiv b2a \leq 0 \land \cancel{b^2}-1^2(\cancel{b^2}-4ac) \geq 0 \lor 1\cdot 2a \leq 0 \land \cancel{b^2}-1^2(\cancel{b^2}-4ac) \leq 0$$
$$\equiv 2ba \leq 0 \land 4ac \geq 0 \lor 2a \leq 0 \land 4ac \leq 0$$

Outline

1. Learning Objectives
2. Framing the Miracle
3. Quantifier Elimination
   - Homomorphic Normalization for QE
   - Term Substitutions for Linear Equations
4. Square Root $\sqrt{\cdot}$ Virtual Substitution for Quadratics
   - Square Root Algebra
   - Virtual Substitutions of Square Roots
   - Example
5. Summary

$\sqrt{\cdot}$ Square Root Algebra

Virtual Substitution of $(a+b\sqrt{c})/d$ into Comparisons

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0) \quad \text{accordingly for } \land, \lor, \ldots$$

$\sqrt{c}$-algebra $\qquad d \neq 0 \land c \geq 0$

$$((a+b\sqrt{c})/d) + ((a'+b'\sqrt{c})/d') = ((ad'+da') + (bd'+db')\sqrt{c})/(dd')$$

$$((a+b\sqrt{c})/d) \cdot ((a'+b'\sqrt{c})/d') = ((aa'+bb'c) + (ab'+ba')\sqrt{c})/(dd')$$

$\sqrt{c}$-comparisons $\qquad d \neq 0 \land c \geq 0$

$$(a+b\sqrt{c})/d = 0 \equiv ab \leq 0 \land a^2 - b^2c = 0$$

$$(a+b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \land a^2 - b^2c \geq 0 \lor bd \leq 0 \land a^2 - b^2c \leq 0$$

$$(a+b\sqrt{c})/d < 0 \equiv ad < 0 \land a^2 - b^2c > 0$$
$$\lor bd \leq 0 \land (ad < 0 \lor a^2 - b^2c < 0)$$

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$)

$$a \neq 0 \lor b \neq 0 \lor c \neq 0 \rightarrow$$
$$\Big(\exists x\,(ax^2 + bx + c = 0 \land F) \leftrightarrow$$
$$a = 0 \land b \neq 0 \land F_{\bar{x}}^{-c/b}$$
$$\lor\, a \neq 0 \land b^2 - 4ac \geq 0 \land \left(F_{\bar{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \lor F_{\bar{x}}^{(-b-\sqrt{b^2-4ac})/(2a)}\right)\Big)$$

Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$)

Extended logic

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

$FOL_{\mathbb{R}}$

$$\omega_x^r \in [\![F]\!] \text{ iff } \omega \in [\![F_{\bar{x}}^{(a+b\sqrt{c})/d}]\!] \text{ where } r = (\omega[\![a]\!] + \omega[\![b]\!]\sqrt{\omega[\![c]\!]})/(\omega[\![d]\!]) \in \mathbb{R}$$

André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Switzerland, 2018.
URL: http://www.springer.com/978-3-319-63587-3, doi:10.1007/978-3-319-63588-0.

Volker Weispfenning.
Quantifier elimination for real algebra — the quadratic case and beyond.
Appl. Algebra Eng. Commun. Comput., 8(2):85–101, 1997.
doi:10.1007/s002000050055.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.

Jacek Bochnak, Michel Coste, and Marie-Francoise Roy.
Real Algebraic Geometry, volume 36 of *Ergeb. Math. Grenzgeb.*
Springer, Berlin, 1998.
doi:10.1007/978-3-662-03718-8.

Saugata Basu, Richard Pollack, and Marie-Françoise Roy.
Algorithms in Real Algebraic Geometry.
Springer, Berlin, 2nd edition, 2006.
doi:10.1007/3-540-33099-2.

Alfred Tarski.
A Decision Method for Elementary Algebra and Geometry.
University of California Press, Berkeley, 2nd edition, 1951.
doi:10.1007/978-3-7091-9459-1_3.

George E. Collins.
Quantifier elimination for real closed fields by cylindrical algebraic decomposition.
In H. Barkhage, editor, *Automata Theory and Formal Languages*, volume 33 of *LNCS*, pages 134–183, Berlin, 1975. Springer.
doi:10.1007/3-540-07407-4_17.