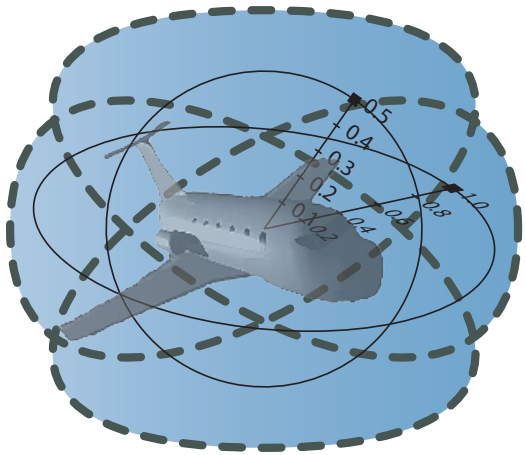
20: Virtual Substitution & Real Equations

15-424: Foundations of Cyber-Physical Systems

André Platzer

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



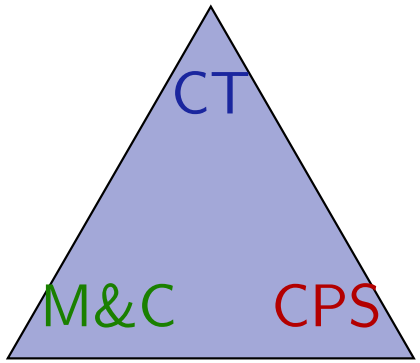
Outline

Outline

Learning Objectives

Virtual Substitution & Real Equations

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

Evaluating Real Arithmetic Formulas

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Are the following formulas valid?

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Are the following formulas valid?

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

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

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Are the following formulas valid?

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

Evaluating Real Arithmetic Formulas

When $\omega(x) = 2$

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

When $\nu(x) = -1$

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

Are the following formulas valid?

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

Framing the Miracle: Quiz

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

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

Framing the Miracle: Quiz

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

1. ✓ Propositional logic — decidable
2. FOL uninterpreted
3. $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$
4. $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$
5. $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$
6. $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$

Framing the Miracle: Quiz

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

- ✓ Propositional logic — decidable
- ✓ FOL uninterpreted — semidecidable [Gödel'30,Herbrand'30]
3. $\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$
4. $\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$
5. $\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$
6. $\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL uninterpreted	semidecidable [Gödel'30,Herbrand'30]
×	$\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$ Peano arithmetic	not semidecidable [Gödel'31]
4	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$	
5	$\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$	
6	$\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$	

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
5	$\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$	
6	$\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$	

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
×	$\text{FOL}_{\mathbb{Q}}[+,\cdot,=]$	not semidecidable [Robinson'49]
6	$\text{FOL}_{\mathbb{C}}[+,\cdot,=]$	

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
×	$\text{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	not semidecidable [Robinson'49]
✓	$\text{FOL}_{\mathbb{C}}[+,\cdot,=]$	decidable [Tarski'51,Chevalley'51]

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
×	$\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	not semidecidable [Robinson'49]
✓	$\mathrm{FOL}_{\mathbb{C}}[+,\cdot,=]$	decidable [Tarski'51,Chevalley'51]
7	$\mathrm{FOL}_{\mathbb{R}}[+,=,\wedge,\exists]$	
8	$\mathrm{FOL}_{\mathbb{R}}[+,\leq,\wedge,\exists]$	
9	$\mathrm{FOL}_{\mathbb{N}}[+,=,2\vert,3\vert,\ldots]$	
10	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$	
11	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$	

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
×	$\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	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]
8	$\mathrm{FOL}_{\mathbb{R}}[+,\leq,\wedge,\exists]$	
9	$\mathrm{FOL}_{\mathbb{N}}[+,=,2\vert,3\vert,\ldots]$	
10	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$	
11	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$	

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
×	$\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	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]
9	$\mathrm{FOL}_{\mathbb{N}}[+,=,2\vert,3\vert,\ldots]$	
10	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$	
11	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$	

Framing the Miracle: Quiz

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

✓	Propositional logic	decidable
✓	FOL 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]
×	$\text{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	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]
10	$\text{FOL}_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$	
11	$\text{FOL}_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$	

Framing the Miracle: Quiz

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

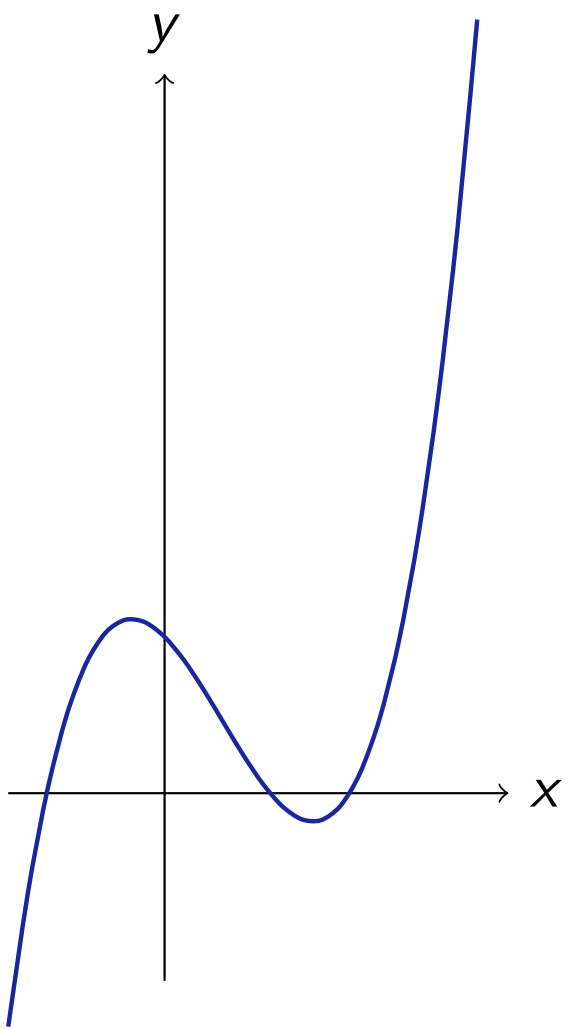
✓	Propositional logic	decidable
✓	FOL uninterpreted	semidecidable [Gödel'30,Herbrand'30]
×	$\mathrm{FOL}_{\mathbb{N}}[+,\cdot,=]$ Peano arithmetic	not semidecidable [Gödel'31]
✓	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,=,<]$	decidable [Tarski'31..51]
×	$\mathrm{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	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]
✓	$\mathrm{FOL}_{\mathbb{N}}[+,=,2\vert,3\vert,\ldots]$	decidable [Presburger'29,Skolem'31]
?	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$	unknown
11	$\mathrm{FOL}_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$	

Framing the Miracle: Quiz

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

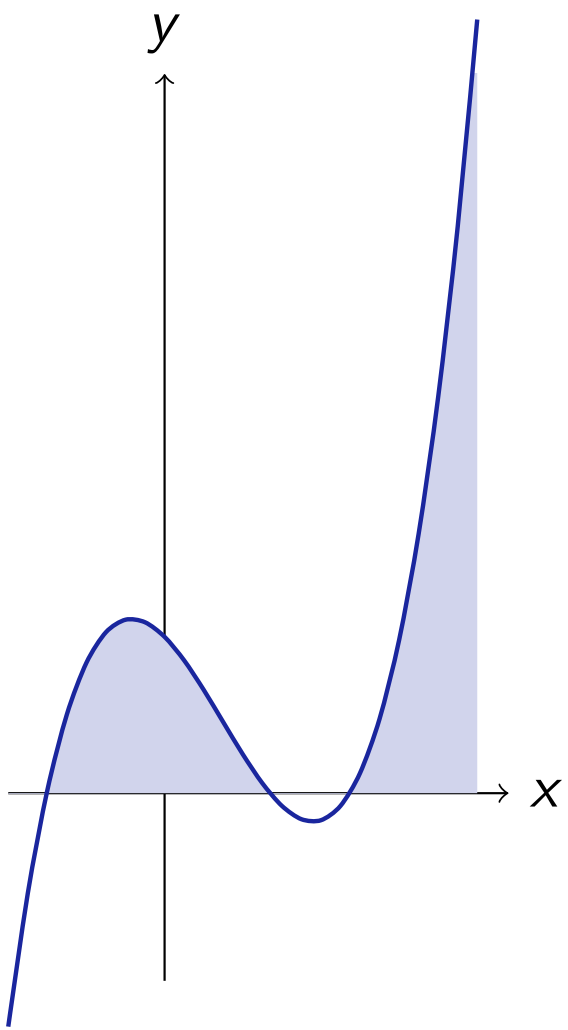
✓	Propositional logic	decidable
✓	FOL uninterpreted	semidecidable [Gödel'30,Herbrand'30]
×	$\text{FOL}_{\mathbb{N}}[+,\cdot,=]$ Peano arithmetic	not semidecidable [Gödel'31]
✓	$\text{FOL}_{\mathbb{R}}[+,\cdot,=,<]$	decidable [Tarski'31..51]
×	$\text{FOL}_{\mathbb{Q}}[+,\cdot,=]$ $\sqrt{2} \notin \mathbb{Q}$	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]
?	$\text{FOL}_{\mathbb{R}}[+,\cdot,\mathit{exp},=,<]$	unknown
×	$\text{FOL}_{\mathbb{R}}[+,\cdot,\mathit{sin},=,<]$	not semidecidable

Quantifier Elimination $\Leftrightsquigarrow$ Projection



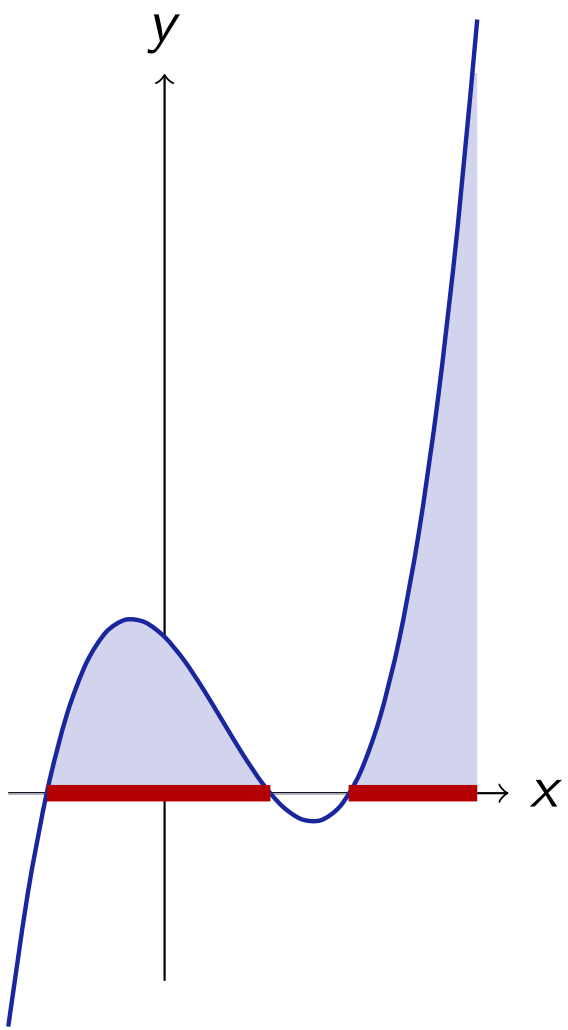
$$F \equiv \exists y\,(y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$

Quantifier Elimination $\leftrightsquigarrow$ Projection



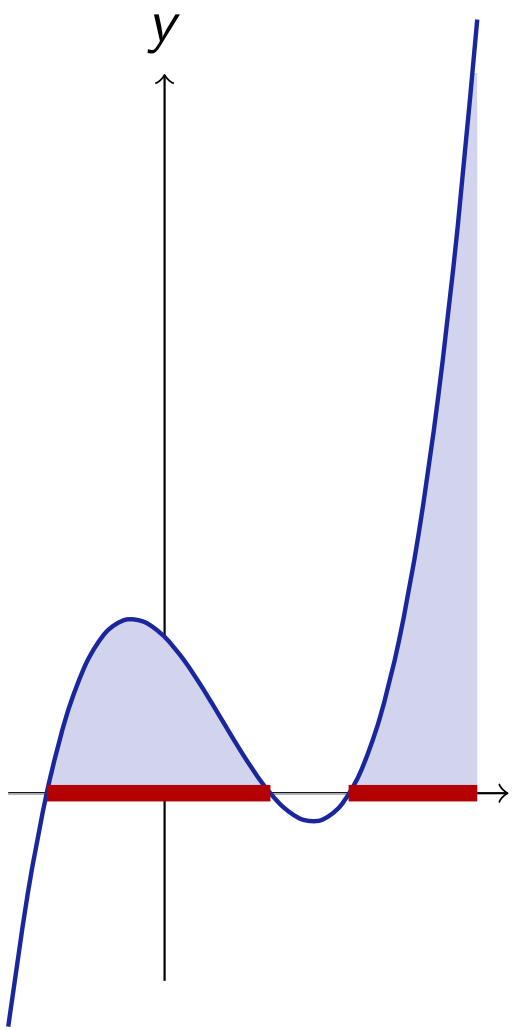
$$F \equiv \exists y\,(y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$

Quantifier Elimination $\Longleftrightarrow$ Projection



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

Quantifier Elimination ⟺ Projection



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

QE

$\mathrm{QE}(F) \equiv 0.75 < x \wedge x < 0.68 \vee x > 1.17$

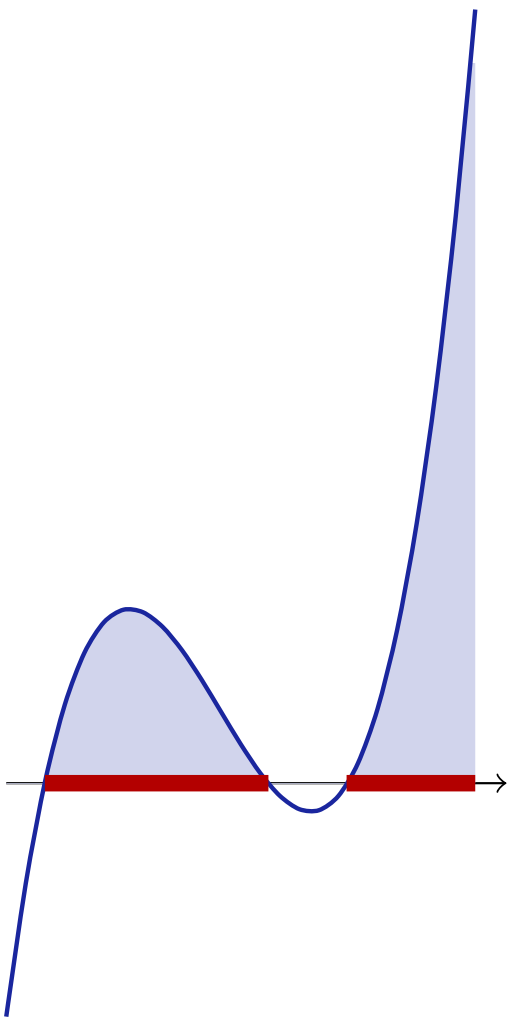
Quantifier Elimination $\leftsquigarrow$ Projection

$\mathrm{QE}(F) \equiv 0.75 < x \wedge x < 0.68 \vee x > 1.17$

Quantifier Elimination ⟺ Projection

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

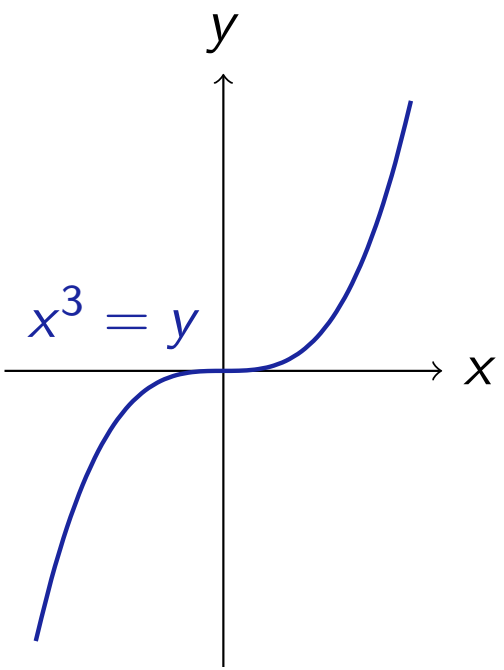
QE

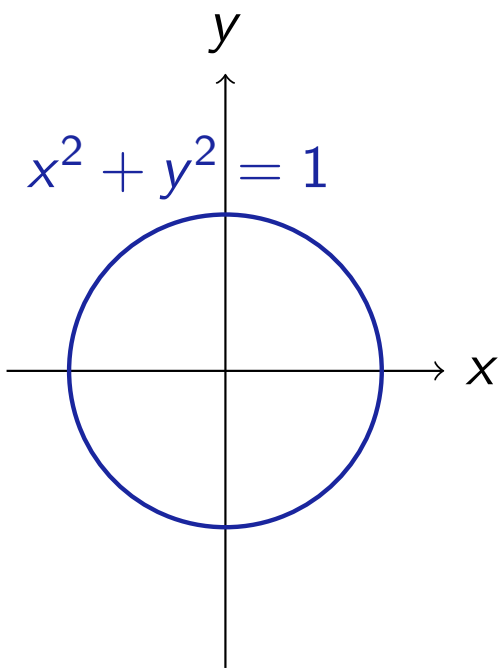


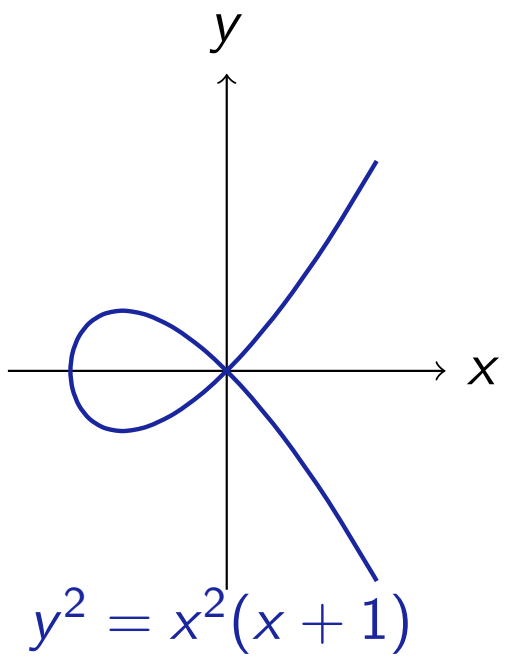
$$\mathrm{QE}(F) \equiv 0.75 < x \wedge x < 0.68 \vee x > 1.17$$

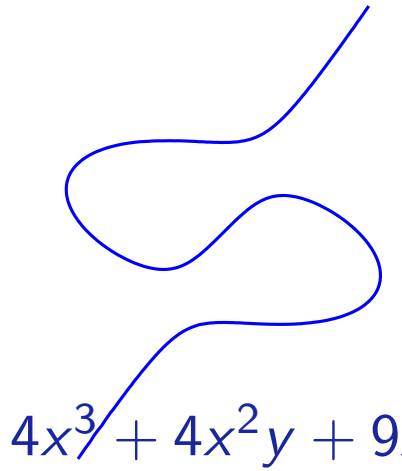
If all but one variable fixed: Finite union of intervals.
Univariate polynomials have finitely many roots.

Polynomial Equations ⇜⇝ Algebraic Varieties

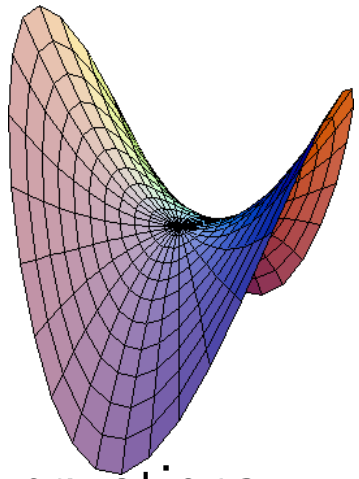






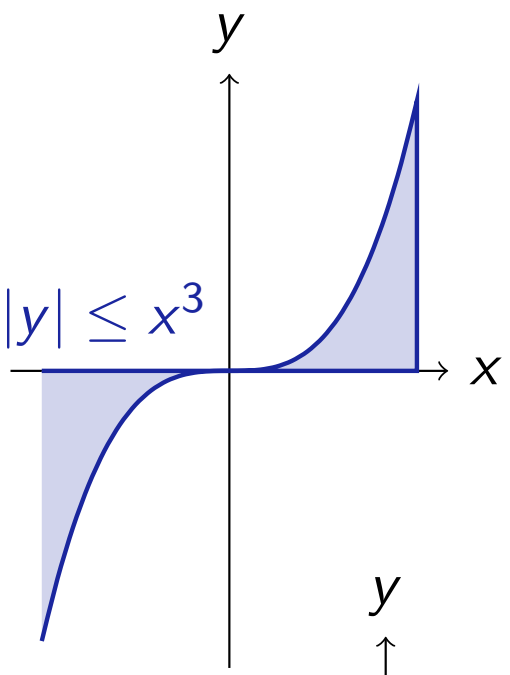


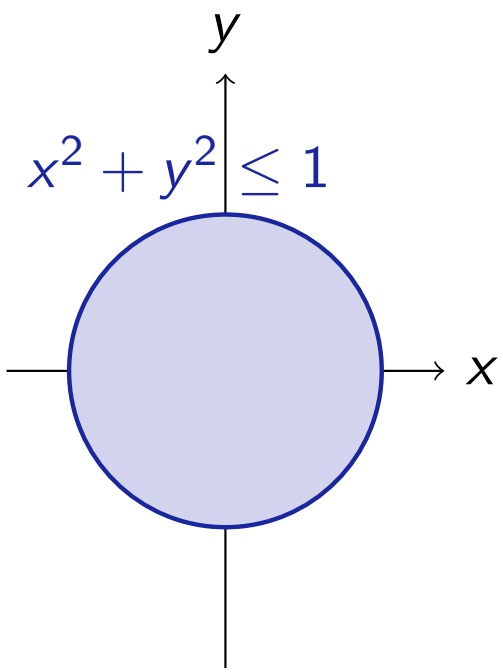
$z = x^2 - y^2$

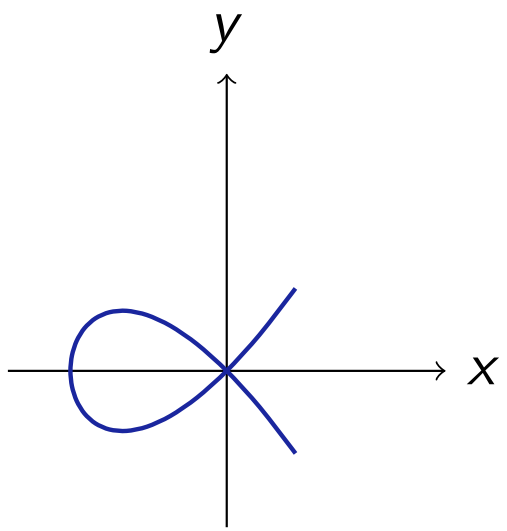


Algebraic variety: defined by conjunction of polynomial equations

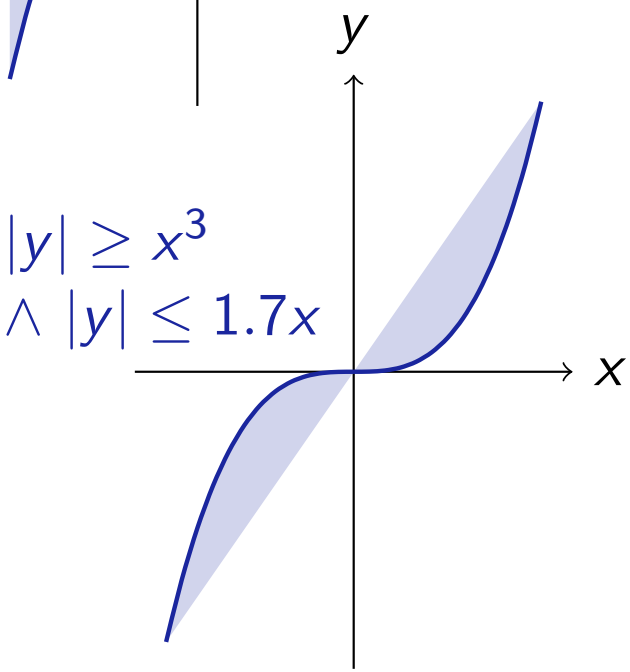
Polynomial Inequalities ⟺ Semialgebraic Sets



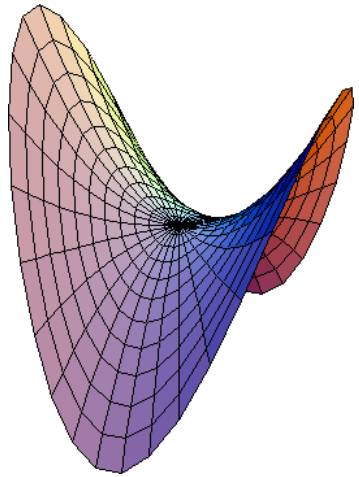




$y^2 = x^2(x+1)$
$\wedge\ x \leq 0.44$



$z = x^2 - y^2$



Quantifier Elimination in Real Arithmetic

Theorem (Tarski'31)

First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e. with each formula ϕ, a quantifier-free formula $\mathsf{QE}(\phi)$ can be associated effectively that is equivalent, i.e. $\phi \leftrightarrow \mathsf{QE}(\phi)$ 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. with each formula ϕ, a quantifier-free formula $\mathsf{QE}(\phi)$ can be associated effectively that is equivalent, i.e. $\phi \leftrightarrow \mathsf{QE}(\phi)$ is valid.

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).*

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

Quantifier Elimination Examples

- $\mathsf{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5))$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\ \mathrm{QE}(\exists x\,(2x^2 + y \leq 5))$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\ \mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\,(y \leq 5))$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\ \mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\,(y \leq 5)) \equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\ \mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\,(y \leq 5)) \equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \mathit{false}$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\ \mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\,(y \leq 5)) \equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \mathit{false}$
- $\mathrm{QE}(\exists x\,(a = b + x^2)) \equiv$

Quantifier Elimination Examples

- $\mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv y \leq 5$
- $\mathrm{QE}(\forall y\,\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\ \mathrm{QE}(\exists x\,(2x^2 + y \leq 5)) \equiv \mathrm{QE}(\forall y\,(y \leq 5)) \equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \mathit{false}$
- $\mathrm{QE}(\exists x\,(a = b + x^2)) \equiv a \geq b$

Framework: Logical Normalization for QE

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

A not quantifier-free

Framework: Logical Normalization for QE

$$\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\ \mathrm{QE}(A)) \qquad A \text{ not quantifier-free}
\end{aligned}$$

Framework: Logical Normalization for QE

$$\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\ \mathrm{QE}(A)) \qquad A \text{ not quantifier-free} \\
\mathrm{QE}(\exists x\, (A \vee B)) &\equiv \\
\mathrm{QE}(\exists x\, \neg(A \wedge B)) &\equiv \\
\mathrm{QE}(\exists x\, \neg(A \vee B)) &\equiv \\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv
\end{aligned}$$

Framework: Logical Normalization for QE

$$
\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\ \mathrm{QE}(A)) && A \text{ not quantifier-free} \\
\mathrm{QE}(\exists x\, (A \vee B)) &\equiv \mathrm{QE}(\exists x\, A) \vee \mathrm{QE}(\exists x\, B) \\
\mathrm{QE}(\exists x\, \neg(A \wedge B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \vee \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\, \neg(A \vee B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \wedge \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv \mathrm{QE}(\exists x\, A)
\end{aligned}
$$

Framework: Logical Normalization for QE

$$\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\ \mathrm{QE}(A)) && A \text{ not quantifier-free} \\
\mathrm{QE}(\exists x\, (A \vee B)) &\equiv \mathrm{QE}(\exists x\, A) \vee \mathrm{QE}(\exists x\, B) \\
\mathrm{QE}(\exists x\, \neg(A \wedge B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \vee \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\, \neg(A \vee B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \wedge \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv \mathrm{QE}(\exists x\, A) \\
\mathrm{QE}(\exists x\, (A \wedge (B \vee C))) &\equiv \\
\mathrm{QE}(\exists x\, ((A \vee B) \wedge C)) &\equiv
\end{aligned}$$

Framework: Logical Normalization for QE

$$
\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) && \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) && \\
\mathrm{QE}(\neg A) &\equiv \neg\, \mathrm{QE}(A) && \\
\mathrm{QE}(\forall x\, A) &\equiv \mathrm{QE}(\neg \exists x\, \neg A) && \\
\mathrm{QE}(\exists x\, A) &\equiv \mathrm{QE}(\exists x\ \mathrm{QE}(A)) && A \text{ not quantifier-free} \\
\mathrm{QE}(\exists x\, (A \vee B)) &\equiv \mathrm{QE}(\exists x\, A) \vee \mathrm{QE}(\exists x\, B) && \\
\mathrm{QE}(\exists x\, \neg(A \wedge B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \vee \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\, \neg(A \vee B)) &\equiv \mathrm{QE}(\exists x\, (\neg A \wedge \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\, \neg\neg A) &\equiv \mathrm{QE}(\exists x\, A) && \\
\mathrm{QE}(\exists x\, (A \wedge (B \vee C))) &\equiv \mathrm{QE}(\exists x\, ((A \wedge B) \vee (A \wedge C))) && \text{if need be} \\
\mathrm{QE}(\exists x\, ((A \vee B) \wedge C)) &\equiv \mathrm{QE}(\exists x\, ((A \wedge C) \vee (B \wedge C))) && \text{if need be}
\end{aligned}
$$

Framework: Logical Normalization for QE

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

$$\begin{aligned}
\mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\
\mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\
\mathrm{QE}(\neg A) &\equiv \neg\,\mathrm{QE}(A) \\
\mathrm{QE}(\forall x\,A) &\equiv \mathrm{QE}(\neg\exists x\,\neg A) \\
\mathrm{QE}(\exists x\,A) &\equiv \mathrm{QE}(\exists x\ \mathrm{QE}(A)) && A \text{ not quantifier-free} \\
\mathrm{QE}(\exists x\,(A \vee B)) &\equiv \mathrm{QE}(\exists x\,A) \vee \mathrm{QE}(\exists x\,B) \\
\mathrm{QE}(\exists x\,\neg(A \wedge B)) &\equiv \mathrm{QE}(\exists x\,(\neg A \vee \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\,\neg(A \vee B)) &\equiv \mathrm{QE}(\exists x\,(\neg A \wedge \neg B)) && \text{with cost} \\
\mathrm{QE}(\exists x\,\neg\neg A) &\equiv \mathrm{QE}(\exists x\,A) \\
\mathrm{QE}(\exists x\,(A \wedge (B \vee C))) &\equiv \mathrm{QE}(\exists x\,((A \wedge B) \vee (A \wedge C))) && \text{if need be} \\
\mathrm{QE}(\exists x\,((A \vee B) \wedge C)) &\equiv \mathrm{QE}(\exists x\,((A \wedge C) \vee (B \wedge C))) && \text{if need be}
\end{aligned}$$

Framework: Arithmetical Normalization for QE

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

$$p = q \equiv p - q = 0$$
$$p \geq q \equiv p - q \geq 0$$
$$p > q \equiv p - q > 0$$
$$p \neq q \equiv p - q \neq 0$$
$$p \leq q \equiv q - p \geq 0$$
$$p < q \equiv q - p > 0$$
$$\neg(p \geq q) \equiv p < q$$
$$\neg(p > q) \equiv p \leq q$$
$$\neg(p = q) \equiv p \neq q$$
$$\neg(p \neq q) \equiv p = q$$

Quantifier Elimination by Virtual Substitution

Virtual Substitution

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

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

Needs simplifier for intermediate results

Quantifier Elimination by Virtual Substitution

Virtual Substitution

Quantifier

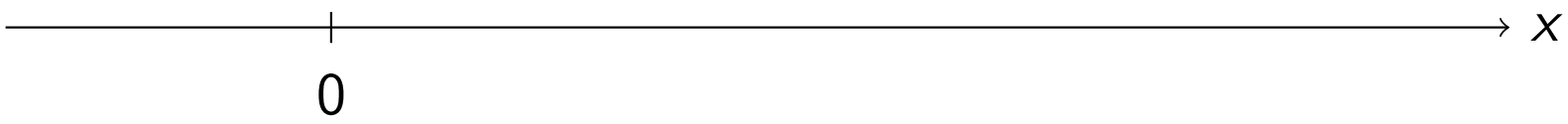
$$\exists x\, F \leftrightarrow \bigvee_{t \in T} A_t \wedge F_x^t$$

Quantifier-free

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

Needs simplifier for intermediate results

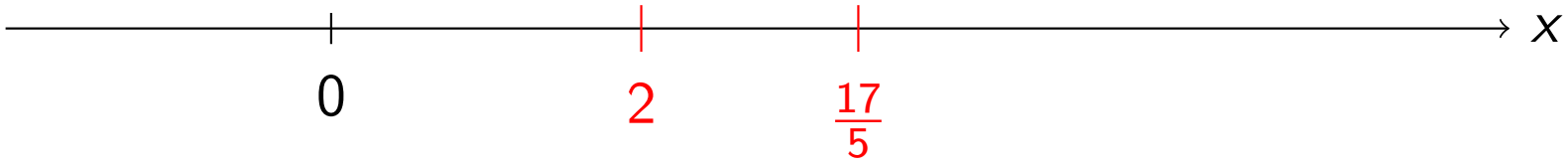
Virtual Substitution by Example



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

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

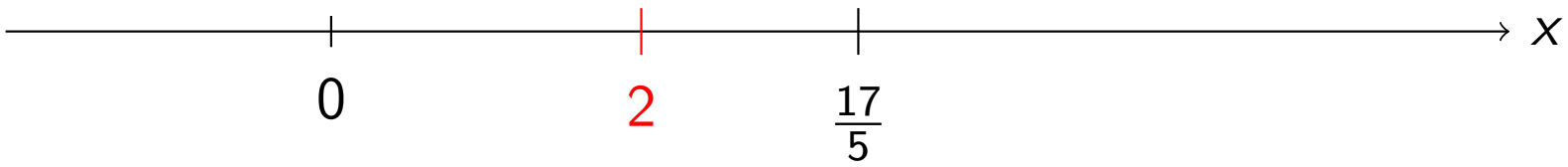
Virtual Substitution by Example



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

$$\exists x(x > 2 \wedge x < \tfrac{17}{5})$$

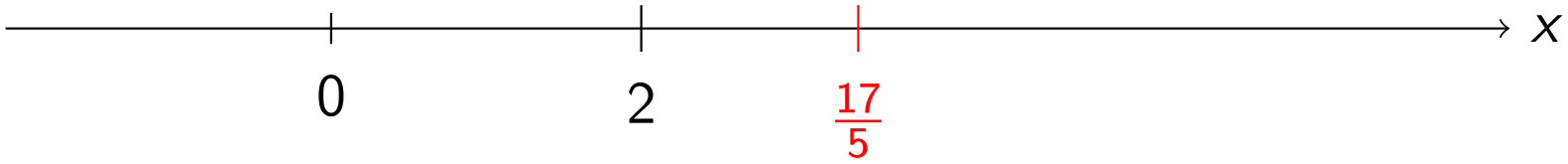
Virtual Substitution by Example



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

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

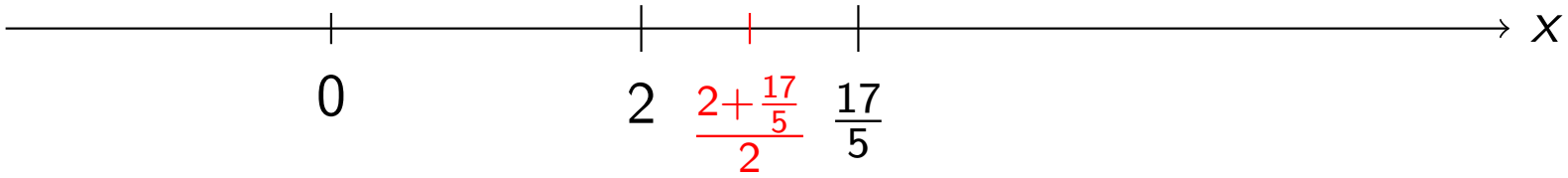
Virtual Substitution by Example



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

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

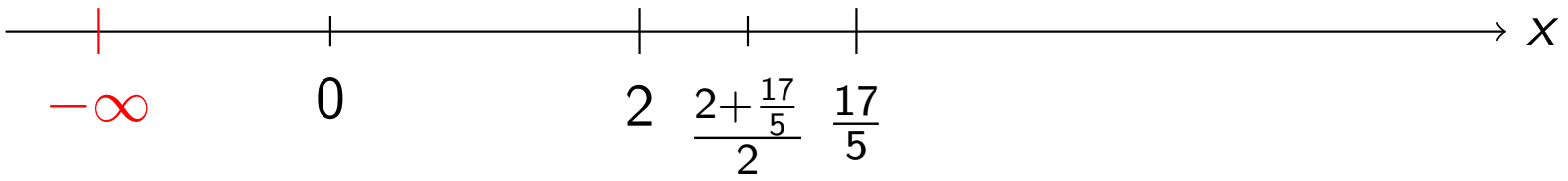
Virtual Substitution by Example



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

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

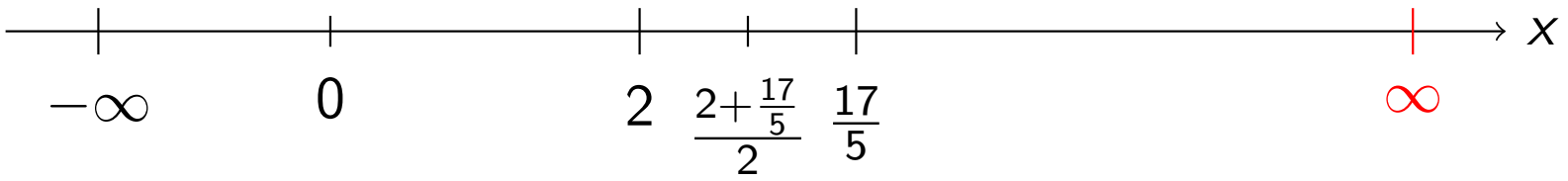
Virtual Substitution by Example



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

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

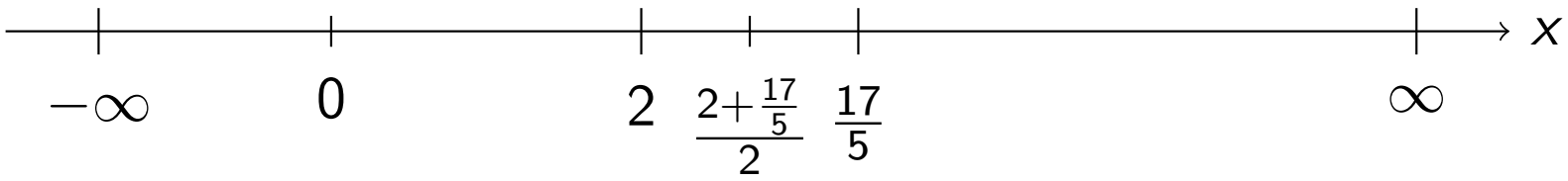
Virtual Substitution by Example



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

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

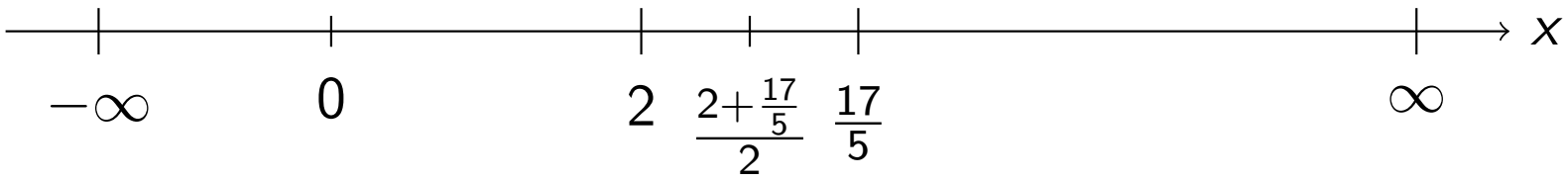
Virtual Substitution by Example



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

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

Virtual Substitution by Example



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

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

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

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

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

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

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

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

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

Linear Virtual Substitution

Theorem (Virtual Substitution: Linear Equation)

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

Linear Virtual Substitution

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

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

Linear Virtual Substitution

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

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

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

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

Quadratic Virtual Substitution

Theorem (Virtual Substitution: Quadratic Equation)

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

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

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

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

Quadratic Virtual Substitution

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

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

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

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

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

Quadratic Virtual Substitution

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

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

1. Quantifier-free equivalent

Quadratic Virtual Substitution

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

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

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

Quadratic Virtual Substitution

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

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

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 $-c/b$

Quadratic Virtual Substitution

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

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

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 $x \notin a, b, c$)

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

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 ... it's merely equivalent

Quadratic Virtual Substitution

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

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

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 ... it's merely equivalent
5. $\exists r\,(r^2 = c)$ would do it for $\sqrt{c}$

Quadratic Virtual Substitution

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

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

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 ... it's merely equivalent
5. $\exists r\,(r^2 = c)$ would do it for $\sqrt{c}$ but that's going in circles

Outline

Quadratic Virtual Substitution

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

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

Square Root Expression Algebra

Virtual Substitution into Polynomial

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

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

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

Square Root Expression Algebra

Virtual Substitution into Polynomial

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

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

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

Square Root Expression Algebra

Virtual Substitution into Polynomial

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

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

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

Square Root Expression Algebra

Virtual Substitution into Polynomial

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

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

$\sqrt{c}$-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 Expression Algebra

Virtual Substitution into Polynomial

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

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

$\sqrt{c}$-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 Expression Algebra

Virtual Substitution into Polynomial

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

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

$\sqrt{c}$-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 Expression Algebra

Virtual Substitution into Polynomial

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

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

$\sqrt{c}$-algebra

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

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

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

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

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

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

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

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

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

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

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

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

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

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

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

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

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

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

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

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

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

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

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

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

Quadratic Virtual Substitution

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

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

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 $x \notin a, b, c$)

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

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

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

Quadratic Virtual Substitution

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

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

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

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

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

Example: Curiosity

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

$$(ax^2+bx+c)^{(-b+\sqrt{b^2-4ac})/(2a)}_{\bar{x}}$$

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

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

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

$$= ((ab^2+ab^2-4a^2c)2a + (-b^2+2ac)4a^2 + ((-ab-ab)2a+b4a^2)\sqrt{b^2-4ac})/(4a^2)$$

$$= (\cancel{2a^2b^2} + \cancel{2a^2b^2} - \cancel{8a^3c} - \cancel{4a^2b^2} + \cancel{8a^3c} + (-\cancel{2a^2b} - \cancel{2a^2b} + \cancel{4a^2b})\sqrt{b^2-4ac})/(4a^2$$

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

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

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

Example: Nonnegative Roots

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

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

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

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

Outline

Square Root Expression Algebra

Virtual Substitution into Polynomial

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

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

$\sqrt{c}$-algebra

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

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

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

Virtual $\sqrt{\cdot}$ Substitution

Virtual Substitution into Comparisons

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

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

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

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

Quadratic Virtual Substitution

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

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

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

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

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


André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2016.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps16.html.


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


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


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


Jacek Bochnak, Michel Coste, and Marie-Francoise Roy.
Real Algebraic Geometry, volume 36 of *Ergeb. Math. Grenzgeb.* Springer, 1998.


Alfred Tarski.
A Decision Method for Elementary Algebra and Geometry.
University of California Press, Berkeley, 2nd edition, 1951.


George E. Collins.
Hauptvortrag: 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. Springer, 1975.