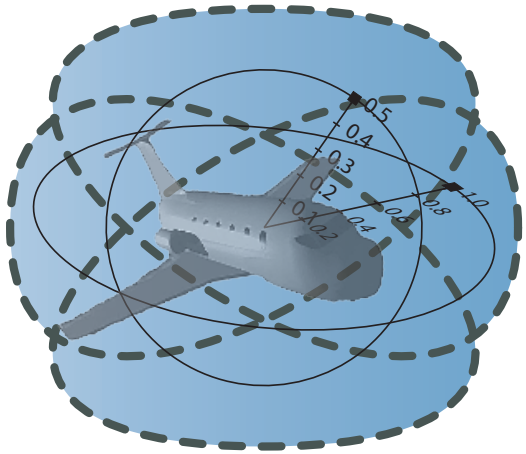
15-819/18-879: Hybrid Systems Analysis & Theorem Proving

02: Propositional and First-order Logic

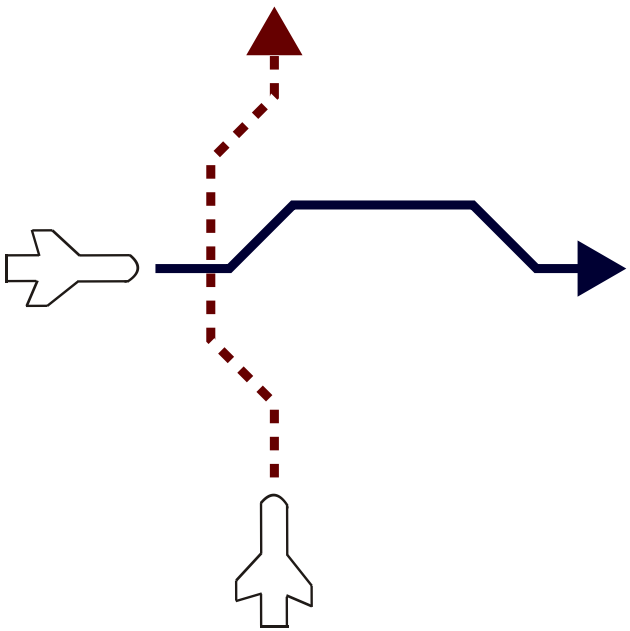
André Platzer

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



Outline

Hybrid Automaton for Collision Avoidance



Example (Property)

If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

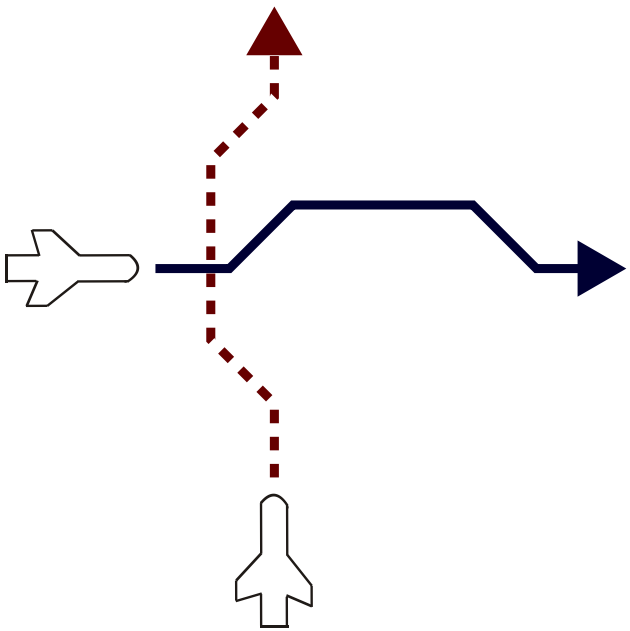
Example (Property)

If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?

Example (System behavior)

If the aircraft are coming too close and I am flying northbound, then we will initiate left evasive actions.

Hybrid Automaton for Collision Avoidance



Example (Property)

If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

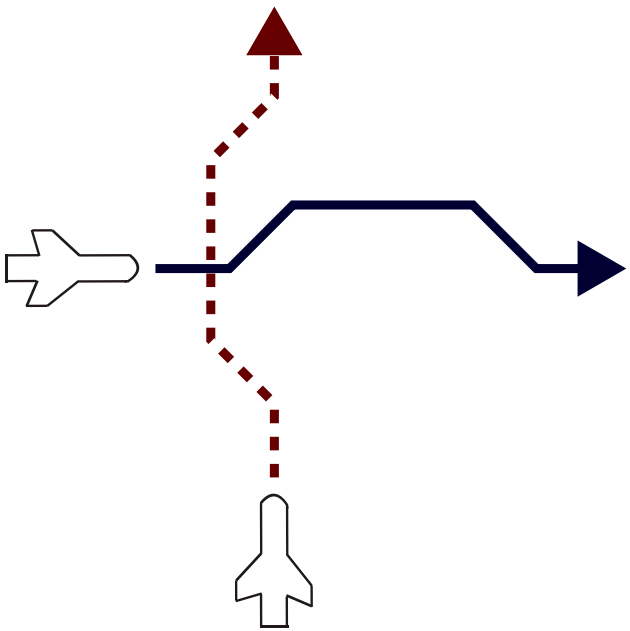
Example (Property)

If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?

Example (System behavior)

If the aircraft are coming too close and I am flying northbound, then we will initiate left evasive actions.

Hybrid Automaton for Collision Avoidance



Example (Property)

If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

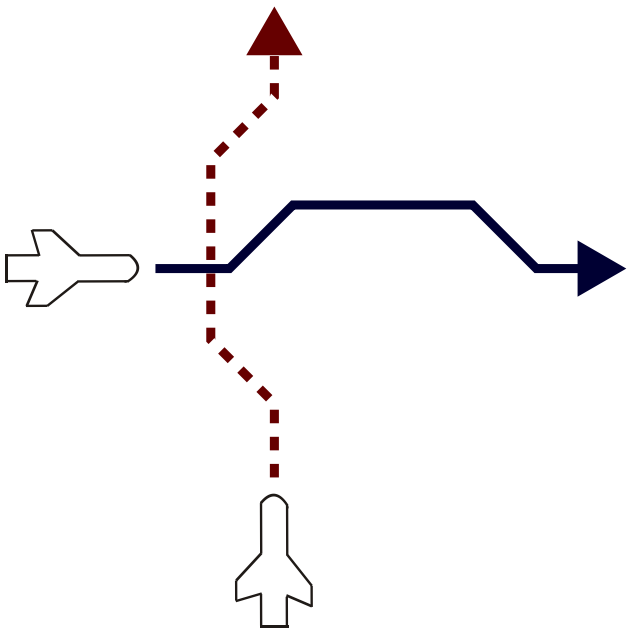
Example (Property)

If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?

Example (System behavior)

If the aircraft are coming too close and I am flying northbound, then we will initiate left evasive actions.

Hybrid Automaton for Collision Avoidance



Example (Property)

If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

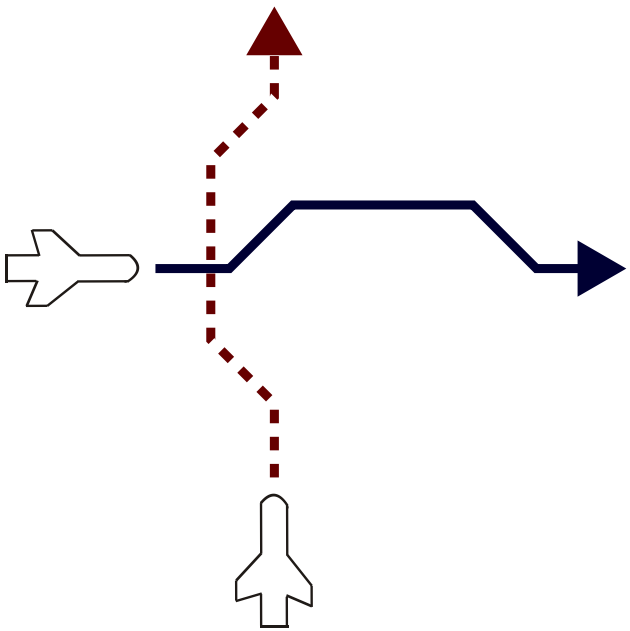
Example (Property)

If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?

Example (System behavior)

If the aircraft are coming too close and I am flying northbound, then we will initiate left evasive actions.

Hybrid Automaton for Collision Avoidance



Example (Property)

If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

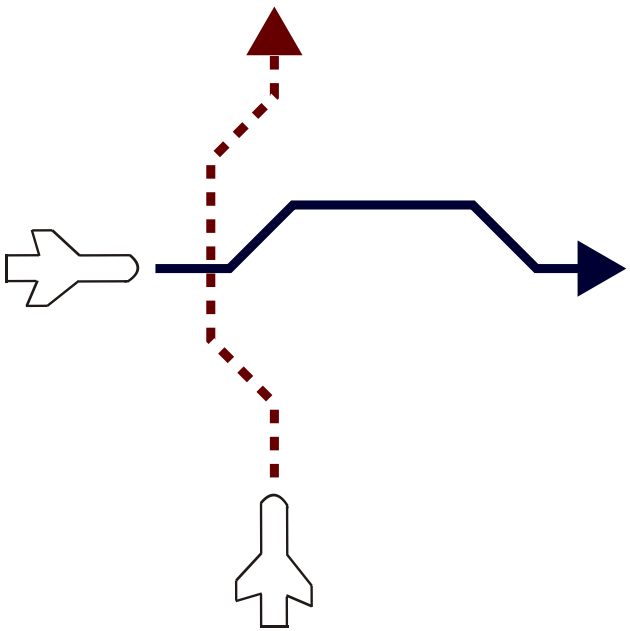
Example (Property)

If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?

Example (System behavior)

If the aircraft are coming too close and I am flying northbound, then we will initiate left evasive actions.

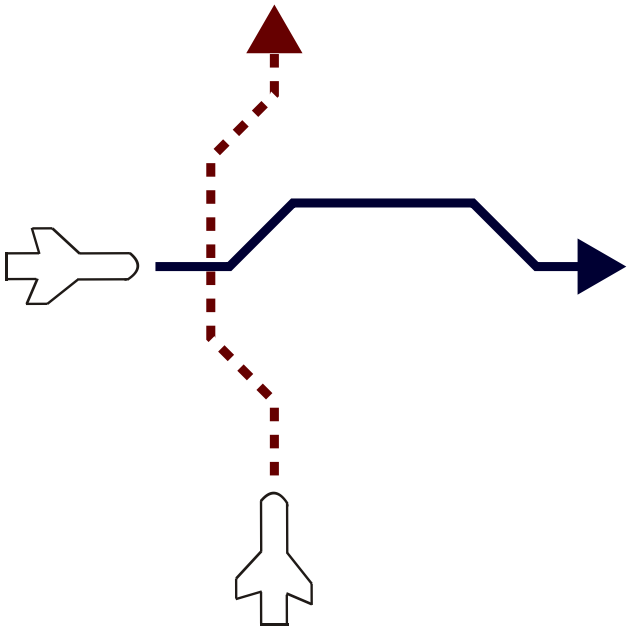
Hybrid Automaton for Collision Avoidance



Example (Informal&incomplete reasoning)

If I turn left then so will he, thus we cannot come closer. Further, he will not turn back unless we have sufficient distance. Since we do not change course early later on, we will keep the distance and can never crash.

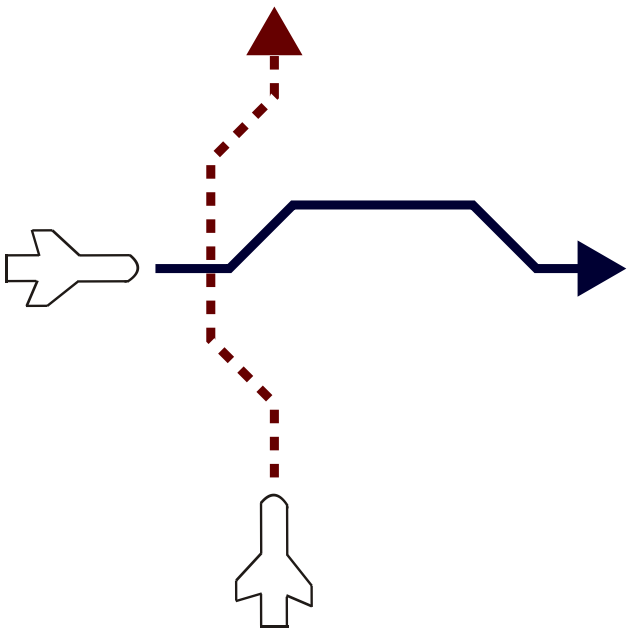
Hybrid Automaton for Collision Avoidance



Example (Informal&incomplete reasoning)

If I turn left then so will he, thus we cannot come closer. Further, he will not turn back unless we have sufficient distance. Since we do not change course early later on, we will keep the distance and can never crash.

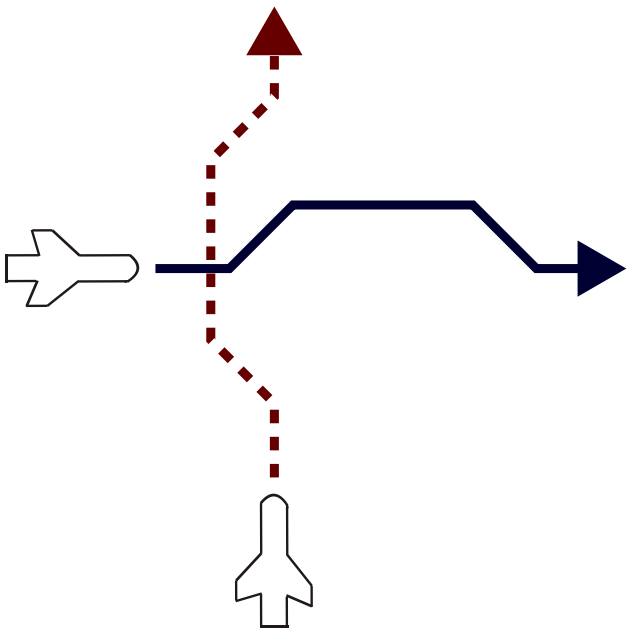
Hybrid Automaton for Collision Avoidance



Example (Informal&incomplete reasoning)

If I turn left then so will he, thus we cannot come closer. Further, he will not turn back unless we have sufficient distance. Since we do not change course early later on, we will keep the distance and can never crash.

Hybrid Automaton for Collision Avoidance



Example (Informal&incomplete reasoning)

If I turn left then so will he, thus we cannot come closer. Further, he will not turn back unless we have sufficient distance. Since we do not change course early later on, we will keep the distance and can never crash.

In hybrid systems, there is significant logical structure in the properties, the system, the reasoning, ...

Outline

Propositional Logic: Syntax

Definition (PL_0 Vocabulary V)

A set V of propositional variables / letters

Propositional Logic: Syntax

Definition (PL_0 Vocabulary V)

A set V of propositional variables / letters

Example

$$V = \{\mathsf{nb}_x, \mathsf{nb}_y, \mathsf{compat}, p_1, p_2, p_3, \dots\}$$

Propositional Logic: Syntax

Definition (PL_0 Vocabulary V)

A set V of propositional variables / letters

Definition (PL_0 Formula F, G)

$F ::=$

p	for any $p \in V$
$\neg F$	"not"
$(F \wedge G)$	"and"
$(F \vee G)$	"or"
$(F \rightarrow G)$	"implies"
$(F \leftrightarrow G)$	"equivalent/bi-implies"

Propositional Logic: Syntax

Definition (PL_0 Vocabulary V)

A set V of propositional variables / letters

Definition (PL_0 Formula F, G)

$F ::=$

p	for any $p \in V$
$\neg F$	"not"
$(F \wedge G)$	"and"
$(F \vee G)$	"or"
$(F \rightarrow G)$	"implies"
$(F \leftrightarrow G)$	"equivalent/bi-implies"

Example (Northbound flight of aircraft x and y is compatible)

$$(\text{nb}_x \wedge \text{nb}_y) \rightarrow \text{compat}$$

Quiz

Is this a propositional formula?

1. $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
2. $A \rightarrow (B \wedge (\neg F \leftrightarrow$
3. $x > y \leftrightarrow x - y > 0$
4. $A \rightarrow B \vee (\neg B \wedge C)$

Quiz

Is this a propositional formula?

1. ✓ $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
2. $A \rightarrow (B \wedge (\neg F \leftrightarrow$
3. $x > y \leftrightarrow x - y > 0$
4. $A \rightarrow B \vee (\neg B \wedge C)$

Quiz

Is this a propositional formula?

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

× $A \rightarrow (B \wedge (\neg F \leftrightarrow$

3. $x > y \leftrightarrow x - y > 0$
4. $A \rightarrow B \vee (\neg B \wedge C)$

Quiz

Is this a propositional formula?

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

× $A \rightarrow (B \wedge (\neg F \leftrightarrow$

× $x > y \leftrightarrow x - y > 0$

4. $A \rightarrow B \vee (\neg B \wedge C)$

Quiz

Is this a propositional formula?

- ✓ $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $A \rightarrow (B \wedge (\neg F \leftrightarrow$
- × $x > y \leftrightarrow x - y > 0$
- ✓ $A \rightarrow B \vee (\neg B \wedge C)$

Propositional Logic: Semantics

Definition (PL_0 Truth-assignment I)

Assignment $I : V \rightarrow \{true, false\}$ of truth-values to propositional variables

Propositional Logic: Semantics

Definition (PL_0 Truth-assignment I)

Assignment $I : V \rightarrow \{true, false\}$ of truth-values to propositional variables

Example

v	nb_x	nb_y	compat
$I(v)$	*false*	*true*	*true*

Propositional Logic: Semantics

Definition (PL_0 Truth-assignment I)

Assignment $I : V \to \{true, false\}$ of truth-values to propositional variables

Definition (PL_0 Interpretation $[\![\cdot]\!]_I$)

$[\![\cdot]\!]_I$ is inductively defined as

$$
\begin{aligned}
[\![p]\!]_I &= I(p) \text{ for any } p \in V \\
[\![\neg F]\!]_I &= true \text{ iff } [\![F]\!]_I = false \\
[\![F \wedge G]\!]_I &= true \text{ iff } [\![F]\!]_I = true \text{ and } [\![G]\!]_I = true \\
[\![F \vee G]\!]_I &= true \text{ iff } [\![F]\!]_I = true \text{ or } [\![G]\!]_I = true \\
[\![F \to G]\!]_I &= true \text{ iff } [\![F]\!]_I = false \text{ or } [\![G]\!]_I = true \\
[\![F \leftrightarrow G]\!]_I &= true \text{ iff, either, } [\![F]\!]_I = true \text{ and } [\![G]\!]_I = true \\
&\qquad \text{or, instead, } [\![F]\!]_I = false \text{ and } [\![G]\!]_I = false
\end{aligned}
$$

Propositional Logic: Semantics

Example (Truth tables)

$I(\text{nb}_x)$	$I(\text{nb}_y)$	$I(\text{compat})$	$[\![\text{nb}_x \wedge nb_y]\!]_I$

Propositional Logic: Semantics

Example (Truth tables)

$I(\text{nb}_x)$	$I(\text{nb}_y)$	$I(\text{compat})$	$[\![\text{nb}_x \wedge nb_y]\!]_I$	$[\![\text{nb}_x \wedge nb_y \rightarrow \text{compat}]\!]_I$
true	*true*	*true*	*true*	

Propositional Logic: Semantics

Example (Truth tables)

$I(\text{nb}_x)$	$I(\text{nb}_y)$	$I(\text{compat})$	$[\![\text{nb}_x \wedge nb_y]\!]_I$	$[\![\text{nb}_x \wedge nb_y \rightarrow \text{compat}]\!]_I$
true	*true*	*true*	*true*	*true*
true	*true*	*false*	*true*	

Example (Truth tables)

$I(\text{nb}_x)$	$I(\text{nb}_y)$	$I(\text{compat})$	$[\![\text{nb}_x \wedge nb_y]\!]_I$	$[\![\text{nb}_x \wedge nb_y \rightarrow \text{compat}]\!]_I$
true	*true*	*true*	*true*	*true*
true	*true*	*false*	*true*	*false*
true	*false*	*true*	*false*	

Propositional Logic: Semantics

Example (Truth tables)

$I(\text{nb}_x)$	$I(\text{nb}_y)$	$I(\text{compat})$	$[\![\text{nb}_x \wedge nb_y]\!]_I$	$[\![\text{nb}_x \wedge nb_y \rightarrow \text{compat}]\!]_I$
true	*true*	*true*	*true*	*true*
true	*true*	*false*	*true*	*false*
true	*false*	*true*	*false*	*true*
true	*false*	*false*	*false*	

Example (Truth tables)

$I(\text{nb}_x)$	$I(\text{nb}_y)$	$I(\text{compat})$	$[\![\text{nb}_x \wedge nb_y]\!]_I$	$[\![\text{nb}_x \wedge nb_y \rightarrow \text{compat}]\!]_I$
true	*true*	*true*	*true*	*true*
true	*true*	*false*	*true*	*false*
true	*false*	*true*	*false*	*true*
true	*false*	*false*	*false*	*true*
false	*true*	*true*	*false*	*true*
false	*true*	*false*	*false*	*true*
false	*false*	*true*	*false*	*true*
false	*false*	*false*	*false*	

Validity

Definition (Validity / Tautology)

Formula F is *valid* iff $[\![F]\!]_I = \mathit{true}$ for all assignments I, otherwise *invalid*

Example

Is this formula valid: $\mathrm{nb}_x \wedge \mathit{nb}_y \rightarrow \mathrm{separate}$?

Validity

Definition (Validity / Tautology)

Formula F is *valid* iff $[\![F]\!]_I = \mathit{true}$ for all assignments I, otherwise *invalid*

Example

Is this formula valid: $A \rightarrow (B \vee C \leftrightarrow (B \rightarrow \neg C \vee A))$?

Validity

Definition (Validity / Tautology)

Formula F is *valid* iff $[\![F]\!]_I = \mathit{true}$ for all assignments I, otherwise *invalid*

Example

Is this formula valid: F ?

Validity

Definition (Validity / Tautology)

Formula F is *valid* iff $[\![F]\!]_I = \mathit{true}$ for all assignments I, otherwise *invalid*

Example

Is this formula valid: F ?

Problem

How do you check validity of a formula?

Validity

Definition (Validity / Tautology)

Formula F is *valid* iff $[\![F]\!]_I = \mathit{true}$ for all assignments I, otherwise *invalid*

Example

Is this formula valid: F ?

Problem

How do you check validity of a formula?

Proposition

Validity and satisfiability for propositional logic are decidable (by exhaustive enumeration) in exponential time.

Validity

Definition (Validity / Tautology)

Formula F is *valid* iff $[\![F]\!]_I = \mathit{true}$ for all assignments I, otherwise *invalid*

Example

Is this formula valid: F ?

Problem

How do you check validity of a formula?

Proposition

Validity and satisfiability for propositional logic are decidable (by exhaustive enumeration) in exponential time. Better: SAT solving!

Quiz

1. Example for a valid formula?
2. Example for an invalid formula?
3. Example for an unsatisfiable formula?

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

1. $A \rightarrow (B \rightarrow A)$
2. $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
3. $A \rightarrow B \vee (\neg B \wedge C)$
4. $(A \rightarrow (\neg A \rightarrow B)) \rightarrow B$
5. $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
6. $x < 0 \rightarrow x^2 > 0$
7. $\big(A \rightarrow (B \rightarrow C)\big) \leftrightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

1. ✓ $A \to (B \to A)$
2. $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
3. $A \to B \vee (\neg B \wedge C)$
4. $(A \to (\neg A \to B)) \to B$
5. $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
6. $x < 0 \to x^2 > 0$
7. $\big(A \to (B \to C)\big) \leftrightarrow \big((A \to B) \to (A \to C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

1. ✓ $A \rightarrow (B \rightarrow A)$
2. ✓ $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
3. $A \rightarrow B \vee (\neg B \wedge C)$
4. $(A \rightarrow (\neg A \rightarrow B)) \rightarrow B$
5. $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
6. $x < 0 \rightarrow x^2 > 0$
7. $\big(A \rightarrow (B \rightarrow C)\big) \leftrightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

✓ $A \to (B \to A)$

✓ $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

× $A \to B \vee (\neg B \wedge C)$

4. $(A \to (\neg A \to B)) \to B$
5. $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
6. $x < 0 \to x^2 > 0$
7. $\big(A \to (B \to C)\big) \leftrightarrow \big((A \to B) \to (A \to C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

1. ✓ $A \rightarrow (B \rightarrow A)$
2. ✓ $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
3. × $A \rightarrow B \vee (\neg B \wedge C)$
4. × $(A \rightarrow (\neg A \rightarrow B)) \rightarrow B$
5. $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
6. $x < 0 \rightarrow x^2 > 0$
7. $\big(A \rightarrow (B \rightarrow C)\big) \leftrightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

- ✓ $A \to (B \to A)$
- ✓ $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
- × $A \to B \vee (\neg B \wedge C)$
- × $(A \to (\neg A \to B)) \to B$
- ✓ $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
- 6. $x < 0 \to x^2 > 0$
- 7. $\big(A \to (B \to C)\big) \leftrightarrow \big((A \to B) \to (A \to C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

- ✓ $A \to (B \to A)$
- ✓ $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
- × $A \to B \vee (\neg B \wedge C)$
- × $(A \to (\neg A \to B)) \to B$
- ✓ $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
- × $x < 0 \to x^2 > 0$
- 7. $\big(A \to (B \to C)\big) \leftrightarrow \big((A \to B) \to (A \to C)\big)$

Quiz

Is this a valid/invalid/satisfiable/unsatisfiable propositional formula?

- ✓ $A \rightarrow (B \rightarrow A)$
- ✓ $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
- × $A \rightarrow B \vee (\neg B \wedge C)$
- × $(A \rightarrow (\neg A \rightarrow B)) \rightarrow B$
- ✓ $\big((A \leftrightarrow B) \leftrightarrow C\big) \leftrightarrow \big(A \leftrightarrow (B \leftrightarrow C)\big)$
- × $x < 0 \rightarrow x^2 > 0$
- ✓ $\big(A \rightarrow (B \rightarrow C)\big) \leftrightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$

Outline

First-order Logic: Syntax

Definition (FOL Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities

First-order Logic: Syntax

Definition (FOL Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities

Example (Aircraft vocabulary)

$$\Sigma = \{\text{cruise}/1, \text{separate}/2, \text{faster}/2, \text{ground}/1\} \cup \{\ldots\}$$

First-order Logic: Syntax

Definition (FOL Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities

Definition (FOL Term t)

$t ::=$

x	for variable $x \in V$
$f(t_1, \ldots, t_n)$	for function $f/n \in \Sigma$ of arity $n \geq 0$

First-order Logic: Syntax

Definition (FOL Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities

Definition (FOL Formula F, G)

$F ::=$

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

First-order Logic: Syntax

Definition (FOL Signature Σ)

Countable set of predicate or function symbols along with natural numbers as arities

Example (Aircraft vocabulary)

$$\Sigma = \{\text{cruise}/1, \text{separate}/2, \text{faster}/2, \text{ground}/1\} \cup \{\dots\}$$

Example (Cruising aircraft cannot crash)

$$(\forall x\, \text{cruise}(x)) \rightarrow \neg\exists x\, \exists y\, (\neg\text{separate}(x, y))$$

Quiz

Is this a first-order formula?

1. $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
2. $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
3. $\forall x\,\exists y\,p(x \rightarrow f(y))$
4. $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
5. $\forall x\,(\mathrm{human}(x) \rightarrow \mathrm{mortal}(x)) \wedge \mathrm{human}(\mathit{Sokrates}) \rightarrow \mathrm{mortal}(\mathit{Sokrates})$
6. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

1. ✓ $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
2. $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
3. $\forall x\,\exists y\,p(x \rightarrow f(y))$
4. $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
5. $\forall x\,(\mathrm{human}(x) \rightarrow \mathrm{mortal}(x)) \wedge \mathrm{human}(\mathit{Sokrates}) \rightarrow \mathrm{mortal}(\mathit{Sokrates})$
6. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

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

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

3. $\forall x\,\exists y\,p(x \rightarrow f(y))$
4. $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
5. $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
6. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

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

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

× $\forall x\,\exists y\,p(x \rightarrow f(y))$

4. $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
5. $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
6. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

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

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

× $\forall x\,\exists y\,p(x \rightarrow f(y))$

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

5. $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
6. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

- ✓ $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- ✓ $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- × $\forall x\,\exists y\,p(x \rightarrow f(y))$
- × $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
- 6. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
- 7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

- ✓ $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- ✓ $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- × $\forall x\,\exists y\,p(x \rightarrow f(y))$
- × $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
- ✓ $\forall x\,(\mathrm{human}(x) \rightarrow \mathrm{mortal}(x)) \wedge \mathrm{human}(\mathit{Sokrates}) \rightarrow \mathrm{mortal}(\mathit{Sokrates})$
- × $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
- 7. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Quiz

Is this a first-order formula?

- ✓ $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- ✓ $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- × $\forall x\,\exists y\,p(x \rightarrow f(y))$
- × $\forall x\,\forall y\,(x > y \leftrightarrow x - y > 0)$
- ✓ $\forall x\,(\mathrm{human}(x) \rightarrow \mathrm{mortal}(x)) \wedge \mathrm{human}(\mathit{Sokrates}) \rightarrow \mathrm{mortal}(\mathit{Sokrates})$
- × $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(r(x) \wedge p(x) \leftrightarrow p(y)))$
- ✓ $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$

Semantics of Formulas

Example (Cruising aircraft cannot crash)

$$(\forall x\, \text{cruise}(x)) \rightarrow \neg\exists x\, \exists y\, (\neg\text{separate}(x, y))$$

Is this formula true over the following signature?

Example (Aircraft vocabulary)

$$\Sigma = \{\text{cruise}/1, \text{separate}/2\} \cup \emptyset$$

Truth depends on the interpretation of symbols

First-order Logic: Semantics

Definition (FOL Interpretation I)

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

First-order Logic: Semantics

Definition (FOL Interpretation I)

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

Definition (FOL Variable Assignment β)

Assignment $\beta : V \to D$ of an element in domain D to each variable in V

Definition (FOL Valuation of terms $[\![\cdot]\!]_{I,\beta}$)

$[\![\cdot]\!]_{I,\beta}$ is inductively defined as

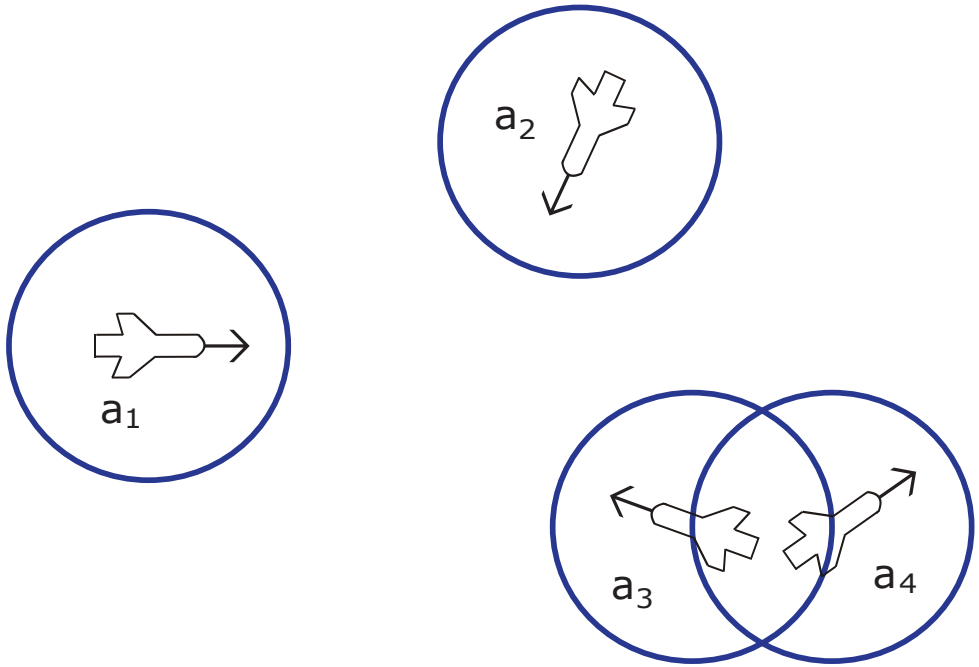
$$[\![x]\!]_{I,\beta} = \beta(x) \text{ for variable } x \in V$$
$$[\![f(t_1, \ldots, t_n)]\!]_{I,\beta} = I(f)([\![t_1]\!]_{I,\beta}, \ldots, [\![t_n]\!]_{I,\beta})$$

Definition (FOL Valuation of formulas $[\![\cdot]\!]_{I,\beta}$)

$[\![\cdot]\!]_{I,\beta}$ is inductively defined as

$$
\begin{aligned}
[\![p(t_1,\ldots,t_n)]\!]_{I,\beta} &= \mathit{true} \text{ iff } ([\![t_1]\!]_{I,\beta},\ldots,[\![t_n]\!]_{I,\beta}) \in I(p) \text{ for pred. } p \in \Sigma \\
[\![\neg F]\!]_{I,\beta} &= \mathit{true} \text{ iff } [\![F]\!]_{I,\beta} = \mathit{false} \\
[\![F \wedge G]\!]_{I,\beta} &= \mathit{true} \text{ iff } [\![F]\!]_{I,\beta} = \mathit{true} \text{ and } [\![G]\!]_{I,\beta} = \mathit{true} \\
[\![F \vee G]\!]_{I,\beta} &= \mathit{true} \text{ iff } [\![F]\!]_{I,\beta} = \mathit{true} \text{ or } [\![G]\!]_{I,\beta} = \mathit{true} \\
[\![F \rightarrow G]\!]_{I,\beta} &= \mathit{true} \text{ iff } [\![F]\!]_{I,\beta} = \mathit{false} \text{ or } [\![G]\!]_{I,\beta} = \mathit{true} \\
[\![\forall x\, F]\!]_{I,\beta} &= \mathit{true} \text{ iff } [\![F]\!]_{I,\beta'} = \mathit{true} \text{ for all } \beta' \text{ that are like } \beta \\
&\qquad \text{except for the value of } x \\
[\![\exists x\, F]\!]_{I,\beta} &= \mathit{true} \text{ iff } [\![F]\!]_{I,\beta'} = \mathit{true} \text{ for some } \beta' \text{ that is like } \beta \\
&\qquad \text{except for the value of } x
\end{aligned}
$$

One Example for an Interpretation



Example (Cruising aircraft cannot crash)

$$(\forall x\, \text{cruise}(x)) \rightarrow \neg\exists x\, \exists y\, (\neg\text{separate}(x, y))$$

$$I_4(\text{cruise}) = \{a_1, a_3, a_4\}$$
$$I_4(\text{separate}) = \{(a_1, a_2), (a_1, a_3), (a_1, a_4), (a_2, a_3), (a_2, a_4)\}$$

Quiz

Is this a valid first-order formula?

1. $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
2. $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
3. $\forall x\,(\mathrm{human}(x) \rightarrow \mathrm{mortal}(x)) \wedge \mathrm{human}(\mathit{Sokrates}) \rightarrow \mathrm{mortal}(\mathit{Sokrates})$
4. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
5. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
6. $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

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

2. $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
3. $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
4. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
5. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
6. $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

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

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

3. $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
4. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
5. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
6. $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

- × $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
4. $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
5. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
6. $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

- × $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
- × $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
5. $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
6. $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

- × $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
- × $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
- ✓ $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
- 6 $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

- × $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
- × $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
- ✓ $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
- × $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$

Quiz

Is this a valid first-order formula?

- × $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
- × $\forall x\,\forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
- ✓ $\forall x\,e(f(f(x)),x) \rightarrow \exists y\,e(f(f(f(y))),f(y))$
- × $\forall x\,(x > 0 \rightarrow \exists y\,x > y^2)$
- 7. $\forall x\,(r(x,0) \rightarrow \exists y\,r(x,p(x,2)))$

Quiz

Is this a valid first-order formula?

- × $F \vee (G \wedge (H \leftrightarrow \neg F) \rightarrow J)$
- × $\forall x\,(p(x) \rightarrow \exists y\,(p(y) \wedge \exists x\,\neg r(x,y)))$
- ✓ $\forall x\,(\text{human}(x) \rightarrow \text{mortal}(x)) \wedge \text{human}(\mathit{Sokrates}) \rightarrow \text{mortal}(\mathit{Sokrates})$
- × $\forall x \forall y\,(e(x,y) \leftrightarrow \forall p\,(p(x) \leftrightarrow p(y)))$
- ✓ $\forall x\, e(f(f(x)),x) \rightarrow \exists y\, e(f(f(f(y))),f(y))$
- × $\forall x\,(x > 0 \rightarrow \exists y\, x > y^2)$
- × $\forall x\,(r(x,0) \rightarrow \exists y\, r(x,p(x,2)))$

Outline

Interpreted First-order Logic

- In a formula like

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

how do we get "+" and "−" and "^2" and ">" to mean what we want?

Interpreted First-order Logic

- In a formula like

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

  how do we get "$+$" and "$-$" and "^2" and "$>$" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.

Interpreted First-order Logic

- In a formula like

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

  how do we get "+" and "−" and "^2" and ">" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.
- Interpreted first-order logic is like first-order logic, except that some symbols have a fixed semantics (all interpretations agree on the semantics of those symbols).

Interpreted First-order Logic

- In a formula like

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

  how do we get "+" and "−" and "^2" and ">" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.
- Interpreted first-order logic is like first-order logic, except that some symbols have a fixed semantics (all interpretations agree on the semantics of those symbols).
- Our primary focus: first-order real arithmetic $\text{FOL}_{\mathbb{R}}$

Interpreted First-order Logic

- In a formula like

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

how do we get "+" and "−" and "^2" and ">" to mean what we want?

Interpreted First-order Logic

- In a formula like

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

  how do we get "$+$" and "$-$" and "^2" and "$>$" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.

Interpreted First-order Logic

- In a formula like

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

  how do we get "+" and "−" and "^2" and ">" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.
- Interpreted first-order logic is like first-order logic, except that some symbols have a fixed semantics (all interpretations agree on the semantics of those symbols).

Interpreted First-order Logic

- In a formula like

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

  how do we get "+" and "−" and "^2" and ">" to mean what we want?
- Fix their meaning in the semantics and analyze the resulting logic.
- Interpreted first-order logic is like first-order logic, except that some symbols have a fixed semantics (all interpretations agree on the semantics of those symbols).
- Our primary focus: first-order real arithmetic $\text{FOL}_{\mathbb{R}}$

Interpreted First-order Logic: Syntax

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

$t ::=$

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

Interpreted First-order Logic: Syntax

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

$t ::=$

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

Interpreted First-order Logic: Syntax

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

$F ::=$

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

Interpreted First-order Logic: Syntax

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

$F ::=$

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

Quiz

Is this a formula of first-order real arithmetic?

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

✓ $x < y \wedge \exists z\,x > z^2$

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

✓ $x < y \wedge \exists z\,x > z^2$

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

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

✓ $x < y \wedge \exists z\, x > z^2$

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

× $\forall x \exists y\, x > x^y$

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

✓ $x < y \wedge \exists z\, x > z^2$

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

× $\forall x \exists y\, x > x^y$

? $\exists x \forall y\, x > y + \pi$

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

Quiz

Is this a formula of first-order real arithmetic?

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

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

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

✓ $x < y \wedge \exists z\, x > z^2$

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

× $\forall x \exists y\, x > x^y$

? $\exists x \forall y\, x > y + \pi$

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

Interpreted First-order Logic: Semantics

Definition ($FOL_{\mathbb{R}}$ Interpretation I)

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

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

Quiz

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

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

Quiz

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

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

Quiz

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

✓ PL_0 decidable

? FOL undecidable but semidecidable

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

Quiz

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

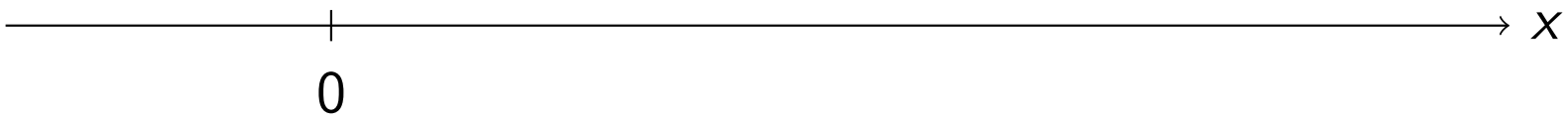
- ✓ PL_0 decidable
- ? FOL undecidable but semidecidable
- × $\mathsf{FOL}_{\mathbb{N}}[+,\cdot,=]$ not even semidecidable "Peano arithmetic" [Gödel'31]
4. $\mathsf{FOL}_{\mathbb{R}}[+,\cdot,=,<]$
5. $\mathsf{FOL}_{\mathbb{Q}}[+,\cdot,=]$
6. $\mathsf{FOL}_{\mathbb{C}}[+,\cdot,=]$

Quiz

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

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

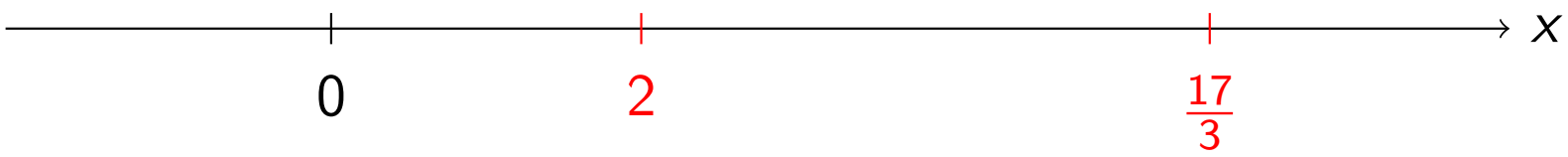
Quantifier Elimination by Example



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

$$\exists x(x > 2 \wedge x < \tfrac{17}{3})$$

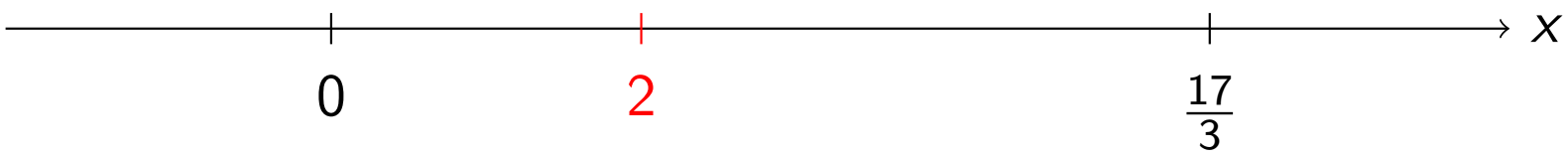
Quantifier Elimination by Example



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

$$\exists x(x > 2 \wedge x < \tfrac{17}{3})$$

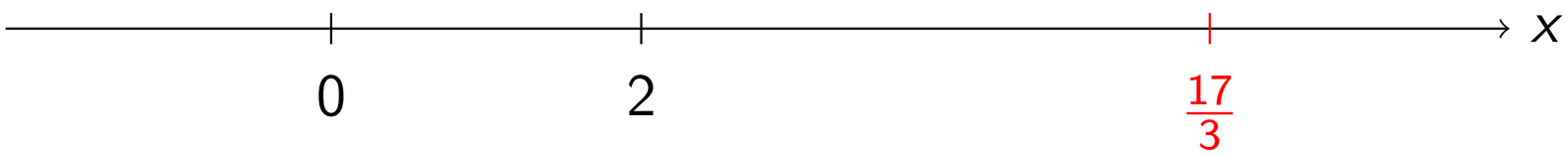
Quantifier Elimination by Example



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

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

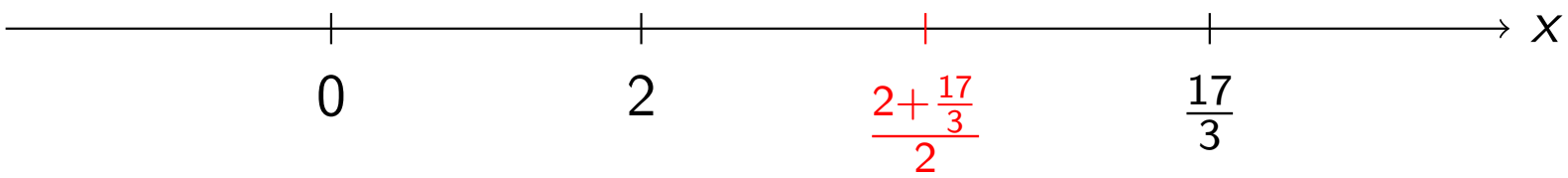
Quantifier Elimination by Example



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

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

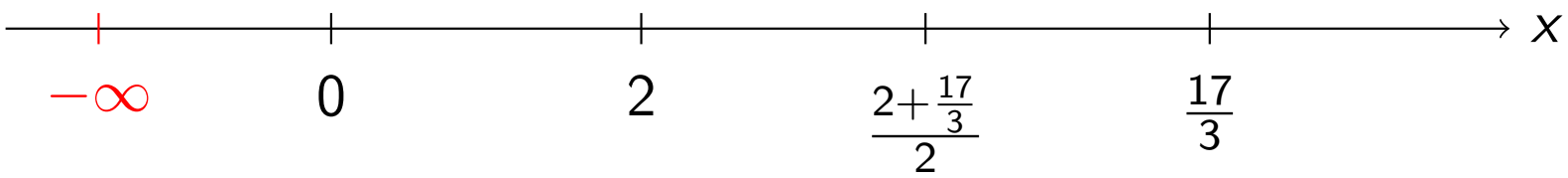
Quantifier Elimination by Example



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

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

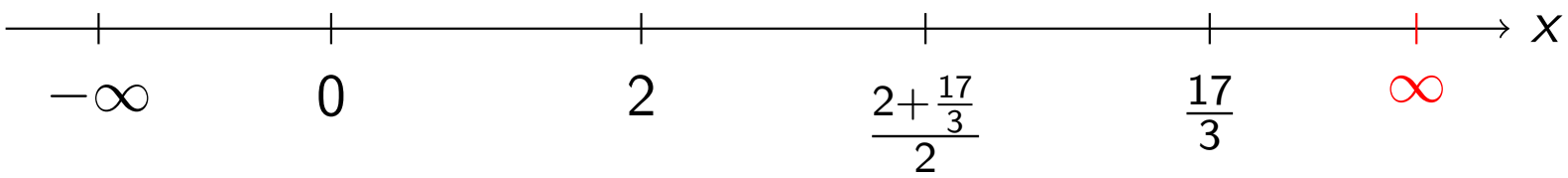
Quantifier Elimination by Example



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

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

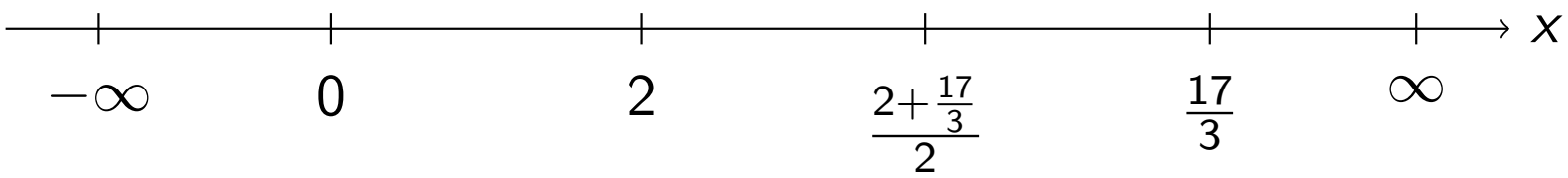
Quantifier Elimination by Example



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

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

Quantifier Elimination by Example



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

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

Quantifier Elimination in Real-Closed Fields

Definition (Quantifier elimination)

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

Quantifier Elimination in Real-Closed Fields

Definition (Quantifier elimination)

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

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

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

Quantifier Elimination in Real-Closed Fields

Definition (Quantifier elimination)

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

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

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

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

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

Quiz

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

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

Quiz

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

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

Quiz

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

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

Quiz

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

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

Quiz

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

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

Quiz

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

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

Quiz

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

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

QE Tools

- QEPCAD [Hoon Hong, George Collins]
- QEPCAD B [Chris Brown,...]
- Redlog [Volker Weispfenning,...]
- Mathematica [Wolfram]: Reduce function

- SyNRAC for Maple [Hitoshi Yanami, Hirokazu Anai]
- ATP implementation [John Harrison, Sean McLaughlin]

QE Tools

- QEPCAD [Hoon Hong, George Collins]
- QEPCAD B [Chris Brown,...]
- Redlog [Volker Weispfenning,...]
- Mathematica [Wolfram]: Reduce function

$$Reduce[x/y = z \leftrightarrow (x = y \cdot z \wedge y \neq 0)]$$

- SyNRAC for Maple [Hitoshi Yanami, Hirokazu Anai]
- ATP implementation [John Harrison, Sean McLaughlin]

QE Tools

- QEPCAD [Hoon Hong, George Collins]
- QEPCAD B [Chris Brown,...]
- Redlog [Volker Weispfenning,...]
- Mathematica [Wolfram]: Reduce function

$$Reduce[x/y = z \leftrightarrow (x = y \cdot z \wedge y \neq 0)] \text{ not true}$$

- SyNRAC for Maple [Hitoshi Yanami, Hirokazu Anai]
- ATP implementation [John Harrison, Sean McLaughlin]

QE Tools

- QEPCAD [Hoon Hong, George Collins]
- QEPCAD B [Chris Brown,...]
- Redlog [Volker Weispfenning,...]
- Mathematica [Wolfram]: Reduce function

$$Reduce[x/y = z \leftrightarrow (x = y \cdot z \wedge y \neq 0)] \text{ not true}$$
$$Reduce[(x/y = z \wedge y \neq 0) \leftrightarrow (x = y \cdot z \wedge y \neq 0)]$$

- SyNRAC for Maple [Hitoshi Yanami, Hirokazu Anai]
- ATP implementation [John Harrison, Sean McLaughlin]

QE Tools

- QEPCAD [Hoon Hong, George Collins]
- QEPCAD B [Chris Brown,...]
- Redlog [Volker Weispfenning,...]
- Mathematica [Wolfram]: Reduce function

$$\mathit{Reduce}[x/y = z \leftrightarrow (x = y \cdot z \wedge y \neq 0)] \text{ not true}$$
$$\mathit{Reduce}[(x/y = z \wedge y \neq 0) \leftrightarrow (x = y \cdot z \wedge y \neq 0)] \text{ true}$$

- SyNRAC for Maple [Hitoshi Yanami, Hirokazu Anai]
- ATP implementation [John Harrison, Sean McLaughlin]

Axioms of Reals

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

First-order Axioms of Reals

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

First-order Axioms of Reals

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

Theorem (downward Skolem-Löwenheim'1915-20)

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

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

"first-order logic cannot distinguish different infinities"

First-order Axioms of Reals

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

Theorem (downward Skolem-Löwenheim'1915-20)

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

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

"first-order logic cannot distinguish different infinities"

Corollary

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

First-order Axioms of Reals

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

Theorem (downward Skolem-Löwenheim'1915-20)

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

Corollary

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

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

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed
✓		dense in $\mathbb{R}$	

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed
✓		dense in $\mathbb{R}$	
	×	$\mathrm{FOL}_{\mathbb{Q}}$ undecidable	$\mathrm{FOL}_{\mathbb{R}}$ decidable

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed
✓		dense in $\mathbb{R}$	
	×	$\mathrm{FOL}_{\mathbb{Q}}$ undecidable	$\mathrm{FOL}_{\mathbb{R}}$ decidable

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, any of the following equivalent conditions holds:

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

Real-Closed Fields

Definition (Real-closed field)

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

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

Real-Closed Fields beyond the Reals

Example (Real-Closed Fields)

- Real numbers $\mathbb{R}$.

Real-Closed Fields beyond the Reals

Example (Real-Closed Fields)

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

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

Real-Closed Fields beyond the Reals

Example (Real-Closed Fields)

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

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

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

Real-Closed Fields beyond the Reals

Example (Real-Closed Fields)

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

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

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

Real-Closed Fields beyond the Reals

Example (Real-Closed Fields)

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

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

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

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

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

First-Order Axiom Schemes of Real-Closed Fields

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

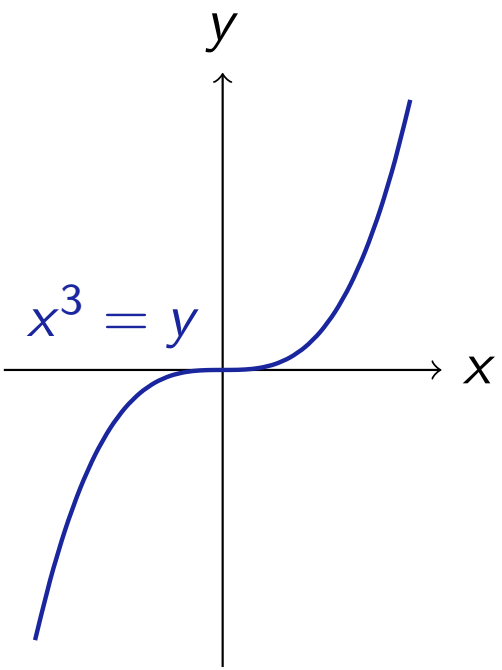
Definition (Real Affine Algebraic Variety)

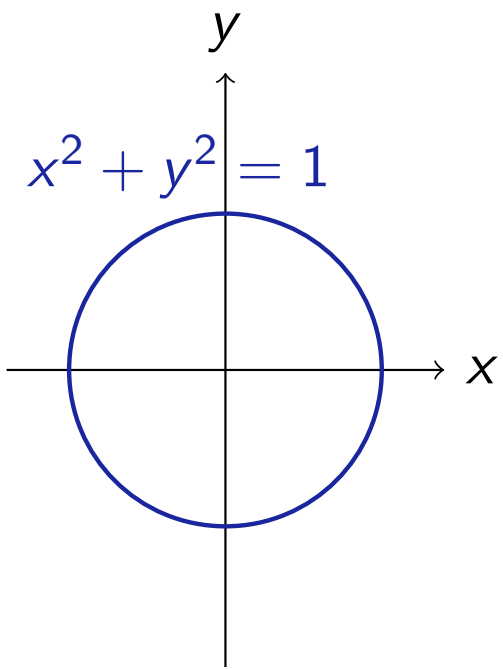
$V \subseteq \mathbb{R}^n$ is an *affine variety* iff, for some set $F \subseteq \mathbb{R}[X_1, \ldots, X_n]$ of polynomials over $\mathbb{R}$:

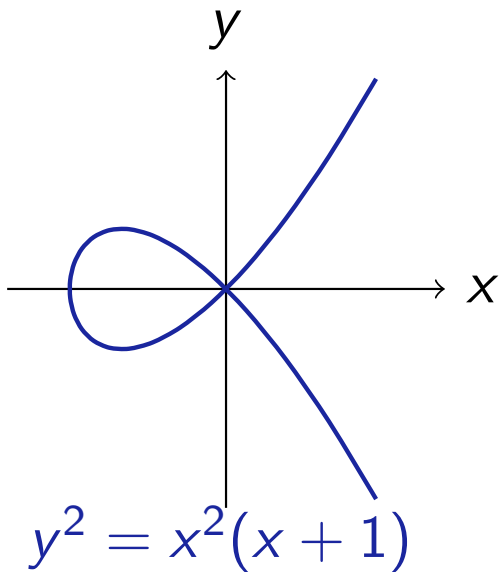
$$V = V(F) := \{x \in \mathbb{R}^n \ : \ f(x) = 0 \text{ for all } f \in F\}$$

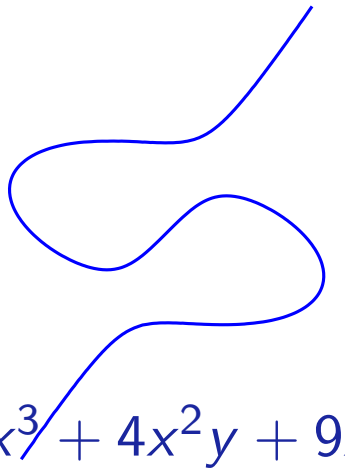
i.e., affine varieties are subsets of $\mathbb{R}^n$ that are definable by a set of polynomial equations.

Algebraic Variety Examples

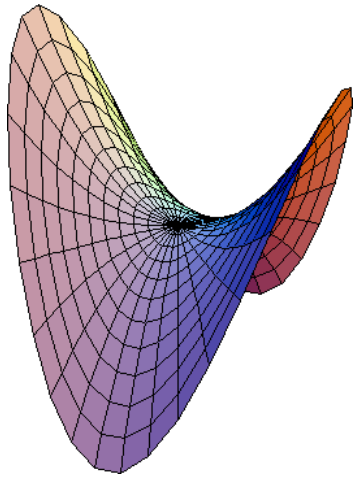








$z = x^2 - y^2$



Definition (Semialgebraic Set)

$S \subseteq \mathbb{R}^n$ is an *semialgebraic set* iff it is defined by a finite intersection of polynomial equations and inequalities or any finite union of such sets.

$$S = \bigcup_{i=1}^{t} \bigcap_{j=1}^{s} \{x \in \mathbb{R}^n \ : \ p(x) \sim 0\} \quad \text{with any } \sim \in \{=, \geq, >\}$$

Definition (Semialgebraic Set)

$S \subseteq \mathbb{R}^n$ is an *semialgebraic set* iff it is defined by a finite intersection of polynomial equations and inequalities or any finite union of such sets.

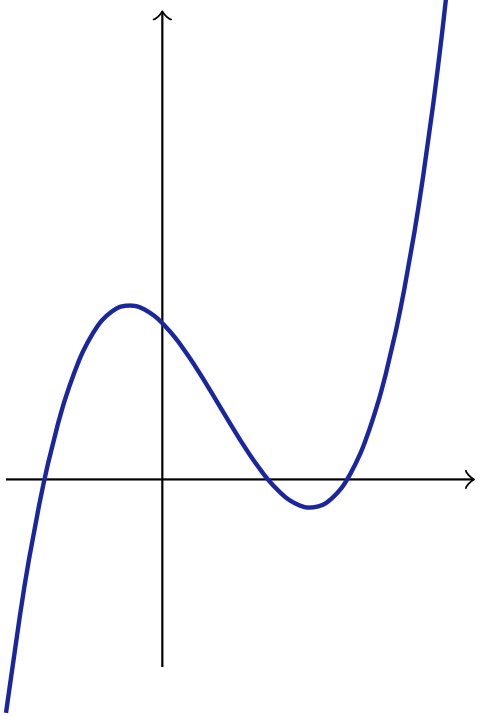
$$S = \bigcup_{i=1}^{t} \bigcap_{j=1}^{s} \{x \in \mathbb{R}^n \ : \ p(x) \sim 0\} \quad \text{with any } \sim \in \{=, \geq, >\}$$

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

Semialgebraic sets are closed under finite unions, finite intersections, complements and projection to linear subspaces.

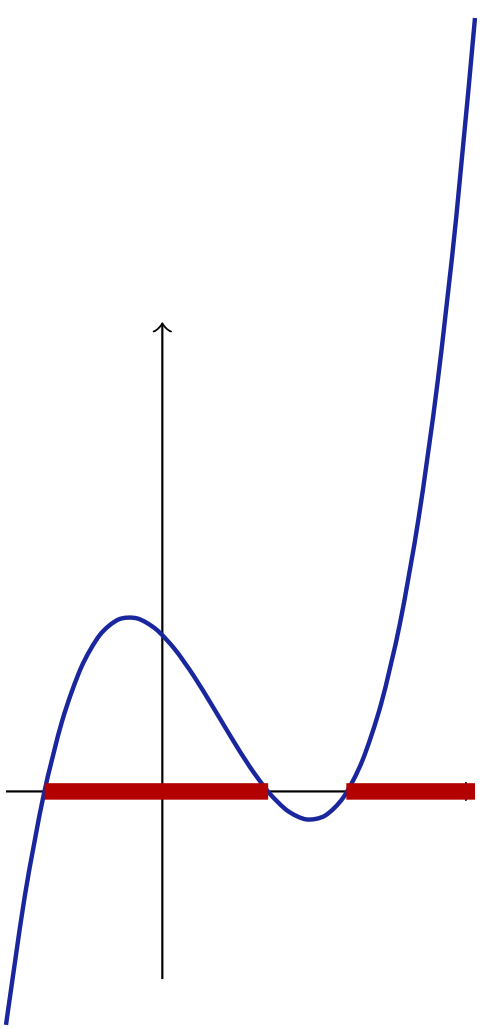
Quantifier Elimination and Projection

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



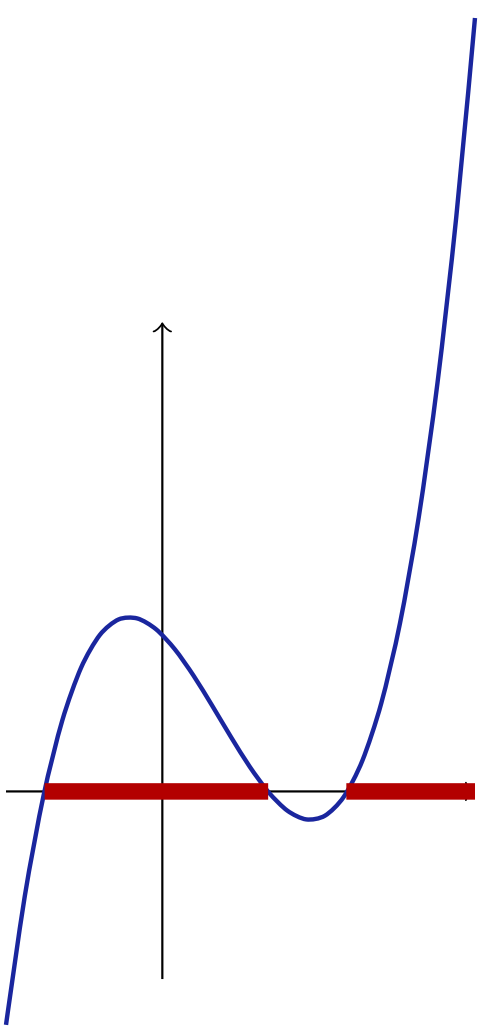
Quantifier Elimination and Projection

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



Quantifier Elimination and Projection

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



$$0.75 < x \wedge x < 0.68 \vee x > 1.17$$


P. B. Andrews.
An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof.
Kluwer, 2nd edition, 2002.


S. Basu, R. Pollack, and M.-F. Roy.
Algorithms in Real Algebraic Geometry.
Springer, 2nd edition, 2006.


M. Fitting.
First-Order Logic and Automated Theorem Proving.
Springer, New York, 2nd edition, 1996.


J. Harrison.
Handbook of Practical Logic and Automated Reasoning.
Cambridge Univ. Press, 2009.


R. M. Smullyan.
First-Order Logic.
Dover, 1995.