CS170: Discrete Methods in Computer Science
Spring 2025
First Order Logic

Instructor: Shaddin Dughmi[1]

[1] These slides adapt some content from similar slides by Aaron Cote.

Outline

Introduction

- In propositional logic, atomic statements were simply propositional variables which may be true or false
  - We built formulas from them using operators like $\neg, \wedge, \vee, \Rightarrow$.
- More generally in math, we want to make statements about a universe of objects
  - E.g. Integers, USC students, graphs, sets, algorithms
- We need statements that take arguments. These are predicates.
- The arguments can be constants in the universe, or variables, or more generally a term.
  - E.g. Universe is integers, $P(x)$ could be the predicate "x is even".
  - You can have statements $P(1)$, $P(x)$, $P(x+y)$, $P(x^2)$.
- We can form statements using quantifiers $\forall$ and $\exists$, in addition to the usual language of propositional logic
  - e.g. $\exists x \neg P(x)$, $\forall x P(2x)$, $\forall x \exists y P(x+y)$.

Predicates

- A predicate is a statement that takes in zero or more arguments from some universe.
  - We usually denote predicates by symbols like P, Q, . . . , followed by arguments in parentheses
  - Some predicates with special meaning can be given special symbols (e.g. $=, >, <, \ldots$)
- Examples of predicates and associated universes
  - $P(n)$ = "n is odd", over the universe of integers.
  - $P(x)$ = "x lives off campus", over the universe of USC students
  - $P(m, n)$= "$m \leq n$", over the universe of integers

Predicates

- A predicate is a statement that takes in zero or more arguments from some universe.
  - We usually denote predicates by symbols like P, Q, ..., followed by arguments in parentheses
  - Some predicates with special meaning can be given special symbols (e.g. $=, >, <, \ldots$)
- Examples of predicates and associated universes
  - $P(n)$ = "n is odd", over the universe of integers.
  - $P(x)$ = "x lives off campus", over the universe of USC students
  - $P(m, n)$= "$m \leq n$", over the universe of integers
- A predicate with zero arguments is just a proposition.
- A predicate with one or more arguments becomes a proposition when its arguments are replaced by constants in the universe.
- Can think of a predicate $P(x)$ as a subset of the universe (a.k.a. a unary relation), $Q(x, y)$ as a binary relation on the universe, etc.
  - But just like we don't assume we know the truth value of a proposition, we don't assume we know the relation.

Universe and Terms

- In first order logic, there is a universe $\mathbb{U}$ and functions on it
  - E.g. $\mathbb{U} = \mathbb{Z}$
  - There are infinitely many generic functions $f, g, \ldots$
  - Also special functions relevant to your universe like $+, -, \times, \ldots$
- A term stands for something in the universe, such as
  - A variable x, y, z, $\ldots$
  - A constant, which can be
    - a generic symbol like a,b,c,$\ldots$
    - a special symbol like 0,1, -7 for constants you know something about
  - An expression involving variables, constants, and functions, such as $x \times y - 7 \times a$, or $f((x+1) \times g(b))$.
- A predicate is allowed to take in a term for each of its arguments
  - E.g. $P(x \times y - 7 \times a, f((x+1) \times g(b)))$ for a 2-argument predicate on the integers.

Building Formulas

A first-order formula is either

- A predicate with terms as arguments (Base case)
- A combination of other formulas using propositional operators $\wedge, \vee, \neg, \Rightarrow$ (Recursive case 1)
- $\forall x F$ or $\exists x F$ for a formula F (Recursive case 2)

e.g. $P(1)$, $P(n^2)$, $\forall n \left(P(n) \Rightarrow P(n^2)\right)$, $\forall x \exists y P(x + y)$ for a unary predicate P on the integers.

Building Formulas

A first-order formula is either

- A predicate with terms as arguments (Base case)
- A combination of other formulas using propositional operators $\wedge, \vee, \neg, \Rightarrow$ (Recursive case 1)
- $\forall x F$ or $\exists x F$ for a formula F (Recursive case 2)

e.g. $P(1)$, $P(n^2)$, $\forall n \left(P(n) \Rightarrow P(n^2)\right)$, $\forall x \exists y P(x+y)$ for a unary predicate P on the integers.

Note

- We use parentheses for clarity whenever it is helpful
- It is common to always allow the special predicate $=$ on the universe (makes life easier)
- A variable in a formula may be free or bound

Free and Bound Variables

- An occurence of a variable x in a formula can be free or bound
- Bound: There is a quantifier that tells us whether we should be checking the formula for all x or only for some x
- Free: There is no such quantifier, so it's a "loose reference"
- A formula with no free variables has a definite truth value (whether you know it or not), otherwise it does not.
  - We call those formulas closed.

Free and Bound Variables

- An occurence of a variable x in a formula can be free or bound
- Bound: There is a quantifier that tells us whether we should be checking the formula for all x or only for some x
- Free: There is no such quantifier, so it's a "loose reference"
- A formula with no free variables has a definite truth value (whether you know it or not), otherwise it does not.
  - We call those formulas closed.

Examples

Which variables are free or bound in the following examples, with Odd(x) representing the predicate "x is odd".

- Odd(x)
- $\forall x$ Odd(x)
- $\forall x\,(\text{Odd}(x) \Rightarrow \text{Odd}(x+y))$
- $\forall x \exists y\,(\text{Odd}(x) \Rightarrow \text{Odd}(x+y))$

Outline

Example

Let $P(x)$ be "x is mortal" over the universe of all humans

- Socrates is mortal: $P(\text{Socrates})$.
- All humans are mortal: $\forall x P(x)$
- Not all humans are mortal: $\neg\forall x P(x)$
- There is an immortal human: $\exists x \neg P(x)$

Example

Let $P(x)$ be "x is mortal" over the universe of all humans

- Socrates is mortal: $P(\text{Socrates})$.
- All humans are mortal: $\forall x P(x)$
- Not all humans are mortal: $\neg \forall x P(x)$
- There is an immortal human: $\exists x \neg P(x)$

The last two are logically equivalent

Generally

Can push a negation through a quantifier, in either direction, while flipping the quantifier

- $\neg \exists x P(x) \equiv \forall x \neg P(x)$
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$

Example

Let $E(x)$ be "x is an elephant" and $P(x)$ be "x is pink", over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$:

Example

Let $E(x)$ be "x is an elephant" and $P(x)$ be "x is pink", over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$: All animals are pink elephants.

Example

Let $E(x)$ be "x is an elephant" and $P(x)$ be "x is pink", over the universe of animals at the zoo.

- $\forall x(E(x) \land P(x))$: All animals are pink elephants.
- $\exists x(E(x) \land P(x))$:

Example

Let $E(x)$ be "x is an elephant" and $P(x)$ be "x is pink", over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$: All animals are pink elephants.
- $\exists x(E(x) \wedge P(x))$: There is a pink elephant.

Example

Let $E(x)$ be "x is an elephant" and $P(x)$ be "x is pink", over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$: All animals are pink elephants.
- $\exists x(E(x) \wedge P(x))$: There is a pink elephant.
- $\forall x(E(x) \Rightarrow P(x))$:

Example

Let $E(x)$ be “x is an elephant” and $P(x)$ be “x is pink”, over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$: All animals are pink elephants.
- $\exists x(E(x) \wedge P(x))$: There is a pink elephant.
- $\forall x(E(x) \Rightarrow P(x))$: All elephants are pink.

Example

Let $E(x)$ be “x is an elephant” and $P(x)$ be “x is pink”, over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$: All animals are pink elephants.
- $\exists x(E(x) \wedge P(x))$: There is a pink elephant.
- $\forall x(E(x) \Rightarrow P(x))$: All elephants are pink.
- $\exists x(E(x) \Rightarrow P(x))$:

Example

Let $E(x)$ be “x is an elephant” and $P(x)$ be “x is pink”, over the universe of animals at the zoo.

- $\forall x(E(x) \wedge P(x))$: All animals are pink elephants.
- $\exists x(E(x) \wedge P(x))$: There is a pink elephant.
- $\forall x(E(x) \Rightarrow P(x))$: All elephants are pink.
- $\exists x(E(x) \Rightarrow P(x))$: If all animals are elephants, then there must be a pink one.

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y \; K(x, y)$:

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y \ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y \ K(x, y)$:

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \land (x \neq y)$:

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$:

Example

Let $K(x, y)$ be “x knows y” over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody
- $\exists x \forall y\ K(x, y)$:

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody
- $\exists x \forall y\ K(x, y)$: Somebody knows everybody

Example

Let $K(x,y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y \; K(x,y)$: All students know each other (and themselves)
- $\exists x \exists y \; K(x,y)$: Some student knows a student (possibly himself)
- $\exists x \exists y \; K(x,y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y \; K(x,y)$: Everybody knows somebody
- $\exists x \forall y \; K(x,y)$: Somebody knows everybody
- $\exists y \forall x \; K(x,y)$:

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody
- $\exists x \forall y\ K(x, y)$: Somebody knows everybody
- $\exists y \forall x\ K(x, y)$: Somebody is known by everybody

Example

Let $K(x, y)$ be "x knows y" over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody
- $\exists x \forall y\ K(x, y)$: Somebody knows everybody
- $\exists y \forall x\ K(x, y)$: Somebody is known by everybody
- $\forall y \exists x\ K(x, y)$:

Example

Let $K(x, y)$ be “x knows y” over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody
- $\exists x \forall y\ K(x, y)$: Somebody knows everybody
- $\exists y \forall x\ K(x, y)$: Somebody is known by everybody
- $\forall y \exists x\ K(x, y)$: Everybody is known by somebody

Example

Let $K(x, y)$ be “x knows y” over the universe of students in this class.

- $\forall x \forall y\ K(x, y)$: All students know each other (and themselves)
- $\exists x \exists y\ K(x, y)$: Some student knows a student (possibly himself)
- $\exists x \exists y\ K(x, y) \wedge (x \neq y)$: Some student knows a different student

Note

Can switch the order of quantifiers if they are both $\exists$ or both $\forall$, without changing the meaning

- $\forall x \exists y\ K(x, y)$: Everybody knows somebody
- $\exists x \forall y\ K(x, y)$: Somebody knows everybody
- $\exists y \forall x\ K(x, y)$: Somebody is known by everybody
- $\forall y \exists x\ K(x, y)$: Everybody is known by somebody

Note

Switching the order of different quantifiers changes the meaning.

Example

Let $H(x, y)$ be “x has y” when x is a dog and y is a tail.

- Every dog has a tail: $\forall x \exists y H(x, y)$ (when universe(x) and universe(y) established in advance)
- Alternatively: $\forall x \ (Dog(x) \Rightarrow \exists y \ (tail(y) \wedge H(x, y)))$ (too cumbersome)
- A better alternative: $\forall x \in Dogs \ \exists y \in Tails \ H(x, y)$

Example

Let $Q(x, y, z)$ be $x + y = z$ over the universe of integers. Which of the following is true, given what we know about integer arithmetic.

- $\forall x \forall y \exists z \; Q(x, y, z)$
- $\exists x \exists y \forall z \; Q(x, y, z)$
- $\exists x \forall y \forall z \; Q(x, y, z)$
- $\forall x \exists y \exists z \; Q(x, y, z)$
- $\exists x \forall y Q(x, y, y)$

Example

Let $Q(x, y, z)$ be $x + y = z$ over the universe of integers. Which of the following is true, given what we know about integer arithmetic.

- $\forall x \forall y \exists z \; Q(x, y, z)$
- $\exists x \exists y \forall z \; Q(x, y, z)$
- $\exists x \forall y \forall z \; Q(x, y, z)$
- $\forall x \exists y \exists z \; Q(x, y, z)$
- $\exists x \forall y Q(x, y, y)$

Implicitly, we are proving these starting from everything we know about about integer arithmetic as our premises.

Outline

Some Examples

Are the following true or false:

Some Examples

Are the following true or false:

1. $\forall x(P(x) \wedge Q(x)) \models \forall x P(x)$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \wedge Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \land Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)

Some Examples

Are the following true or false:

1. $\forall x(P(x) \wedge Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \wedge Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$
4. $\forall x(P(x) \vee Q(x)) \models (\forall x P(x)) \vee (\forall x Q(x))$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \wedge Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$
4. $\forall x(P(x) \vee Q(x)) \models (\forall x P(x)) \vee (\forall x Q(x))$
5. $\exists x(P(x) \vee Q(x)) \equiv (\exists x P(x)) \vee (\exists x Q(x))$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \land Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \land Q(x)) \equiv (\forall x P(x)) \land (\forall x Q(x))$
4. $\forall x(P(x) \lor Q(x)) \models (\forall x P(x)) \lor (\forall x Q(x))$
5. $\exists x(P(x) \lor Q(x)) \equiv (\exists x P(x)) \lor (\exists x Q(x))$
6. $\exists x(P(x) \land Q(x)) \equiv (\exists x P(x)) \land (\exists x Q(x))$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \land Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \land Q(x)) \equiv (\forall x P(x)) \land (\forall x Q(x))$
4. $\forall x(P(x) \lor Q(x)) \models (\forall x P(x)) \lor (\forall x Q(x))$
5. $\exists x(P(x) \lor Q(x)) \equiv (\exists x P(x)) \lor (\exists x Q(x))$
6. $\exists x(P(x) \land Q(x)) \equiv (\exists x P(x)) \land (\exists x Q(x))$
7. $\forall x \exists y Q(x, y) \models \exists y \forall x Q(x, y)$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \wedge Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$
4. $\forall x(P(x) \vee Q(x)) \models (\forall x P(x)) \vee (\forall x Q(x))$
5. $\exists x(P(x) \vee Q(x)) \equiv (\exists x P(x)) \vee (\exists x Q(x))$
6. $\exists x(P(x) \wedge Q(x)) \equiv (\exists x P(x)) \wedge (\exists x Q(x))$
7. $\forall x \exists y Q(x,y) \models \exists y \forall x Q(x,y)$
8. $\exists x \forall y Q(x,y) \models \forall y \exists x Q(x,y)$

Some Examples

Are the following true or false:

1. $\forall x(P(x) \land Q(x)) \models \forall x P(x)$
2. $\forall x P(x) \models \exists x P(x)$ (we only consider non-empty universes)
3. $\forall x(P(x) \land Q(x)) \equiv (\forall x P(x)) \land (\forall x Q(x))$
4. $\forall x(P(x) \lor Q(x)) \models (\forall x P(x)) \lor (\forall x Q(x))$
5. $\exists x(P(x) \lor Q(x)) \equiv (\exists x P(x)) \lor (\exists x Q(x))$
6. $\exists x(P(x) \land Q(x)) \equiv (\exists x P(x)) \land (\exists x Q(x))$
7. $\forall x \exists y Q(x, y) \models \exists y \forall x Q(x, y)$
8. $\exists x \forall y Q(x, y) \models \forall y \exists x Q(x, y)$
9. $\forall x \exists y P(x, y), \forall x \forall y \forall z(P(x, y) \land P(y, z) \Rightarrow P(x, z))$
   $\models \forall x \exists y \exists z P(x, y) \land P(y, z) \land P(x, z)$

Syntax vs Semantics

- Semantics of propositional logic center on truth assignments
  - When we give "meaning" to variables, we explicitly or implicitly assign them a True/False value
  - A formula can be thought of as a truth table, or as the family of truth assignments which satisfy the formula
  - One or more premises semantically entail a conclusion if every truth assignment which satisfies permises also satisfies conclusion.
  - We denoted semantic entailment with $\models$. For example, we write $A, B \models C$ if every truth assignment satisfying A and B also satisfies C.
- Syntax described valid formulas, and inference rules
  - If you can prove a conclusion from some premises using rules of inference, we say premises syntactically entail the conclusion.
  - It is traditional to write use the symbol $\vdash$ for syntactic entailment. E.g., we write $A, B \vdash C$ if there is a proof of C from A and B.

Syntax vs Semantics

- Semantics of propositional logic center on truth assignments
  - When we give "meaning" to variables, we explicitly or implicitly assign them a True/False value
  - A formula can be thought of as a truth table, or as the family of truth assignments which satisfy the formula
  - One or more premises semantically entail a conclusion if every truth assignment which satisfies permises also satisfies conclusion.
  - We denoted semantic entailment with $\models$. For example, we write $A, B \models C$ if every truth assignment satisfying A and B also satisfies C.
- Syntax described valid formulas, and inference rules
  - If you can prove a conclusion from some premises using rules of inference, we say premises syntactically entail the conclusion.
  - It is traditional to write use the symbol $\vdash$ for syntactic entailment. E.g., we write $A, B \vdash C$ if there is a proof of C from A and B.
- We mentioned that for propositional logic with the rules of inference I showed you, $\models$ and $\vdash$ are the same relation!
  - Soundness and completeness.

Syntax vs Semantics

- First order logic is the same way, except we also have a universe and functions on it!
- Semantics:
  - Specify a non-empty universe and functions on it, plus truth value for every proposition ($P(a)$, $L(a, b)$, etc)
    - This is often called a model, structure, or interpretation.
  - Premises semantically entail conclusion, in sense of $\models$, if every model satisfying premises also satisfies conclusion.
- Syntax: Valid formulas, and inference rules
  - Similarly, syntactic entailment $\vdash$ describes what you can prove using the rules of inference.

Useful Notation for Inference Rules

- A formula F can involve multiple variables, constants, etc. Variables may be free or bound.
- When x is a variable, F is a formula involving x, and t is a term, we use $F(t/x)$ to denote replacing free occurrences of x in F with t.
- Examples:
  - $F = P(x) \wedge (\forall x\, Q(x, y))$
  - $F(a/x) = P(a) \wedge (\forall x\, Q(x, y))$
  - $F(b/y) = P(x) \wedge (\forall x\, Q(x, b))$
  - $F((y + 7)/x) = P(y + 7) \wedge (\forall x\, Q(x, y))$

Useful Notation for Inference Rules

- A formula F can involve multiple variables, constants, etc. Variables may be free or bound.
- When x is a variable, F is a formula involving x, and t is a term, we use $F(t/x)$ to denote replacing free occurrences of x in F with t.
- Examples:
  - $F = P(x) \wedge (\forall x\, Q(x, y))$
  - $F(a/x) = P(a) \wedge (\forall x\, Q(x, y))$
  - $F(b/y) = P(x) \wedge (\forall x\, Q(x, b))$
  - $F((y + 7)/x) = P(y + 7) \wedge (\forall x\, Q(x, y))$
- Caveat: Avoid variable capture, which is when a free variable in t becomes bound after substitution $F(t/x)$
  - Not legal: $F(x/y) = P(x) \wedge (\forall x\, Q(x, x))$
  - Instead, rename the quantified variable with fresh symbol first: $F(x/y) = P(x) \wedge (\forall z\, Q(z, x))$

Inference Rules of First-Order Logic

- Inference rules of propositional logic: (see corresponding lecture)
- Reorder Quantifiers:

$$\forall x \forall y F \equiv \forall y \forall x F$$

$$\exists x \exists y F \equiv \exists y \exists x F$$

- Quantifier Negation:

$$\neg \forall x F \equiv \exists x \neg F$$

$$\neg \exists x F \equiv \forall x \neg F$$

- Change of Variables: If F has x as a free variable but not y

$$\exists x F \equiv \exists y F(y/x)$$

$$\forall x F \equiv \forall y F(y/x)$$

- Scope change: If F involves free variable x but G does not

$$\exists x (F \vee G) \equiv (\exists x F) \vee G$$

$$\forall x (F \vee G) \equiv (\forall x F) \vee G$$

$$\exists x (F \wedge G) \equiv (\exists x F) \wedge G$$

$$\forall x (F \wedge G) \equiv (\forall x F) \wedge G$$

Inference Rules of First-Order Logic

- Universal Instantiation:

$$\forall x\ F \vdash F(t/x)$$

  for any term t (can include variables, constants, functions, etc).
- Existential Instantiation:

$$\exists x\ F \vdash F(a/x)$$

  for a fresh (i.e., new, never seen before) constant symbol a.
- Universal Generalization: If F involves free variable x

$$F \vdash \forall x F$$

  Requirement: x must not appear free in the assumptions.
- Existential Generalization: If F involves a free variable x, and t is a constant term (i.e., does not involve any variables)

$$F(t/x) \vdash \exists x F$$

Example of a Formal Proof

1. Premise: $\forall x\,(P(x) \Rightarrow Q(x))$
2. Premise: $\exists x P(x)$

6. Conclusion: $\exists x Q(x)$

Example of a Formal Proof

1. Premise: $\forall x\,(P(x) \Rightarrow Q(x))$
2. Premise: $\exists x P(x)$
3. $P(a)$ (Existential instantiation, 2)

6. Conclusion: $\exists x Q(x)$

Example of a Formal Proof

1. Premise: $\forall x\,(P(x) \Rightarrow Q(x))$
2. Premise: $\exists x P(x)$
3. $P(a)$ (Existential instantiation, 2)
4. $P(a) \Rightarrow Q(a)$ (Universal instantiation, 1)

6. Conclusion: $\exists x Q(x)$

Example of a Formal Proof

1. Premise: $\forall x \, (P(x) \Rightarrow Q(x))$
2. Premise: $\exists x P(x)$
3. $P(a)$ (Existential instantiation, 2)
4. $P(a) \Rightarrow Q(a)$ (Universal instantiation, 1)
5. $Q(a)$ (Modus Ponens, 3 and 4)
6. Conclusion: $\exists x Q(x)$

Example of a Formal Proof

1. Premise: $\forall x\,(P(x) \Rightarrow Q(x))$
2. Premise: $\exists x P(x)$
3. $P(a)$ (Existential instantiation, 2)
4. $P(a) \Rightarrow Q(a)$ (Universal instantiation, 1)
5. $Q(a)$ (Modus Ponens, 3 and 4)
6. Conclusion: $\exists x Q(x)$ (Existential Generalization, 5)

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \wedge P(y, z) \wedge P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \land P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \land P(y, z) \land P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \land P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \land P(y, z) \land P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \land P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \land P(y, z) \land P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \wedge P(y, z) \wedge P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)
7. $P(x, a) \wedge P(a, b)$ (Conjunction, 4 and 6)

12. Conclusion: $\forall x \exists y \exists z \left(P(x, y) \wedge P(y, z) \wedge P(x, z)\right)$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)
7. $P(x, a) \wedge P(a, b)$ (Conjunction, 4 and 6)
8. $P(x, a) \wedge P(a, b) \Rightarrow P(x, b)$ (Universal instantiation$\times 3$, 2)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \wedge P(y, z) \wedge P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)
7. $P(x, a) \wedge P(a, b)$ (Conjunction, 4 and 6)
8. $P(x, a) \wedge P(a, b) \Rightarrow P(x, b)$ (Universal instantiation$\times 3$, 2)
9. $P(x, b)$ (Modus Ponens, 7 and 8)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \wedge P(y, z) \wedge P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)
7. $P(x, a) \wedge P(a, b)$ (Conjunction, 4 and 6)
8. $P(x, a) \wedge P(a, b) \Rightarrow P(x, b)$ (Universal instantiation$\times 3$, 2)
9. $P(x, b)$ (Modus Ponens, 7 and 8)
10. $P(x, a) \wedge P(a, b) \wedge P(x, b)$ (Conjunction, 7 and 9)

12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \wedge P(y, z) \wedge P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \land P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)
7. $P(x, a) \land P(a, b)$ (Conjunction, 4 and 6)
8. $P(x, a) \land P(a, b) \Rightarrow P(x, b)$ (Universal instantiation$\times 3$, 2)
9. $P(x, b)$ (Modus Ponens, 7 and 8)
10. $P(x, a) \land P(a, b) \land P(x, b)$ (Conjunction, 7 and 9)
11. $\exists y \exists z P(x, y) \land P(y, z) \land P(x, z)$ (Existential Generalization$\times 2$, 10)
12. Conclusion: $\forall x \exists y \exists z \, (P(x, y) \land P(y, z) \land P(x, z))$

Another Example of a Formal Proof

1. Premise: $\forall x \exists y P(x, y)$
2. Premise: $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$
3. $\exists y P(x, y)$ (Universal instantiation, 1)
4. $P(x, a)$ (Existential instantiation, 3)
5. $\exists y P(a, y)$ (Universal instantiation, 1)
6. $P(a, b)$ (Existential instantiation, 5)
7. $P(x, a) \wedge P(a, b)$ (Conjunction, 4 and 6)
8. $P(x, a) \wedge P(a, b) \Rightarrow P(x, b)$ (Universal instantiation$\times 3$, 2)
9. $P(x, b)$ (Modus Ponens, 7 and 8)
10. $P(x, a) \wedge P(a, b) \wedge P(x, b)$ (Conjunction, 7 and 9)
11. $\exists y \exists z P(x, y) \wedge P(y, z) \wedge P(x, z)$ (Existential Generalization$\times 2$, 10)
12. Conclusion: $\forall x \exists y \exists z \left(P(x, y) \wedge P(y, z) \wedge P(x, z)\right)$
    (Universal Generalization, 11)

The Role of Formal Proofs

- In the real world, we don't usually write fully formal proofs using inference rules for purposes of discovering or communicating mathematical ideas.
  - Too tedious to write or read.
- Instead, we write proofs in common language, along with math terminology and notation, that strike a balance between rigor and convenience/legibility.
  - Like we've been doing most of the class.
- Exceptions: Computer-aided theorem proving, particularly for results that are controversial and/or groundbreaking.

The Role of Formal Proofs

- Ideally, your reader should be able to convert your common proofs to fully formal ones with a lot of tedious work, but without ingenuity.
- Therefore, it's good to see these fully formal proofs once or twice in your life, and that's what we're doing.
  - You can rest assured I won't expect too much of you in this regard.
- Also, knowing how formal proofs work helps us understand how math is built up, and why it all sits on solid ground.

Soundness and Completeness

Recall the following two properties of a logic with rules of inference.

- Soundness: If there is a proof that starts with a set of assumptions and derives a conclusion, then every model satisfying the assumptions also satisfies the conclusion.
  - IOW: Syntactic entailment ($\vdash$) implies semantic entailment ($\models$).
  - Informally: "Everything you prove is in fact guaranteed to be true."
- Completeness: If a conclusion holds in every model satisfying the assumptions, then there is a proof which starts with those assumptions and derives the conclusion.
  - IOW: Semantic entailment ($\models$) implies syntactic entailment ($\vdash$).
  - Informally: "Everything guaranteed to be true has a proof."

Soundness and Completeness

Just like in propositional logic, we have

Theorem

First-Order Logic, with the inference rules I showed you, is both sound and complete.

In other words: The conclusions you can prove are precisely those guaranteed to hold in every model satisfying your assumptions.

Soundness and Completeness

Just like in propositional logic, we have

Theorem

First-Order Logic, with the inference rules I showed you, is both sound and complete.

In other words: The conclusions you can prove are precisely those guaranteed to hold in every model satisfying your assumptions.

Note

Not to be confused with the Gödel's Incompleteness Theorems (which you may or may not have heard of). Those are different!

We will get back to this fascinating story later …

Outline

Formalizing Mathematics

- We now have this logical system, first-order logic (FOL) with some inference rules, which seems to check checks all the boxes
  - Kinda simple and natural
  - Sound
  - Complete
- We build theories on top of it to describe various areas of math
  - Natural numbers and arithmetic on them (addition, multiplication)
  - Calculus
  - Linear Algebra
  - Probability and statistics
  - Computation
  - ...

Mathematical Theories

- Theory: A logical system (e.g. FOL), plus some axioms that describe the objects you want to study

Mathematical Theories

- Theory: A logical system (e.g. FOL), plus some axioms that describe the objects you want to study

Example: Theory of natural number arithmetic

Designate special functions $+$ and $\times$, special constants 0 and 1.
Axioms:

- Anything plus zero is itself: $\forall x\ 0 + x = x$
- Anything times 1 is itself: $\forall x\ 1 \times x = x$
- Addition is commutative: $\forall x \forall y\ x + y = y + x$
- Multiplication distributes across addition: $\forall x \forall y \forall z\ x \times (y + z) = x \times y + x \times z$
- A dozen or so more …
- Induction: For every predicate P: $(P(0) \wedge \forall x (P(x) \Rightarrow P(x + 1))) \Rightarrow (\forall x P(x))$
  Technically a schema of infinitely many axioms, but that's OK.

Mathematical Theories

- Theory: A logical system (e.g. FOL), plus some axioms that describe the objects you want to study
- There are many other theories: Linear algebra, group theory, computability theory, set theory, ...
- Usually the axioms are self evident, needing no further justification.
- Furthermore, we ideally want axioms that are
  - Consistent: Don't have inherent contradictions
  - Effective: Not too many, or at least can be "enumerated" by an algorithm
  - Complete (different meaning of the word): Fully describe the objects you want to study, so that every statement can proven either true or false.

Incompleteness of Mathematical Theories

Sadly, we are out of luck. . . ,

Gödel's Incompleteness Theorem

Any theory which is consistent, effective, and powerful enough to express arithmetic on the natural numbers, must be incomplete!

Incompleteness of Mathematical Theories

Sadly, we are out of luck. . . ,

Gödel's Incompleteness Theorem

Any theory which is consistent, effective, and powerful enough to express arithmetic on the natural numbers, must be incomplete!

- Kills a lot of theories you would want, since other areas of math include arithmetic inside (e.g. computability, linear algebra, etc)

Incompleteness of Mathematical Theories

Sadly, we are out of luck. . . ,

Gödel's Incompleteness Theorem

Any theory which is consistent, effective, and powerful enough to express arithmetic on the natural numbers, must be incomplete!

- Kills a lot of theories you would want, since other areas of math include arithmetic inside (e.g. computability, linear algebra, etc)
- How to reconcile this with soundness & completeness of FOL?
    - You can't ever write a long enough list of axioms in FOL to "narrow things down" to the "true" model of natural numbers.
    - Therefore, there will be statements that are true in some model of your theory but false in another
    - Therefore, by soundness, you can't prove the statement or its negation from the axioms of your theory

Incompleteness of Mathematical Theories

Sadly, we are out of luck. . . ,

Gödel's Incompleteness Theorem

Any theory which is consistent, effective, and powerful enough to express arithmetic on the natural numbers, must be incomplete!

- Kills a lot of theories you would want, since other areas of math include arithmetic inside (e.g. computability, linear algebra, etc)
- How to reconcile this with soundness & completeness of FOL?
  - You can't ever write a long enough list of axioms in FOL to "narrow things down" to the "true" model of natural numbers.
  - Therefore, there will be statements that are true in some model of your theory but false in another
  - Therefore, by soundness, you can't prove the statement or its negation from the axioms of your theory
- What if we upgrade to more powerful logic, e.g. second-order logic or higher-order logic?
  - Those logics don't have completeness of inference rules, so you lose in a different way!

ZFC Set Theory

- Zermelo-Fraenkel set theory, with the axiom of Choice
- Built on First-order Logic
- Universe is universe of Sets
  - When you say $\forall x$ or $\exists x$, x is a set
- ZFC Axioms: A somewhat short-ish list of properties of sets which mathematicians have found the most useful
  - Look it up if interested.
- Can encode arithmetic, and pretty much any other math theory
  - E.g. The number 3 can be encoded by a set with 3 elements.
  - Properties of numbers can be viewed through properties of the sets encoding them.
  - This can be extended to calculus, linear algebra, CS, probability, ...
- All of modern math is built on ZFC.
  - Sets can encode pretty much any other mathematical object.
  - Using this encoding, can prove properties of that object in ZFC.
- Since different areas of math now have a shared foundation, can safely port insights and discoveries from one to the other.
- By incompleteness, this is imperfect, but it's the best we've got!