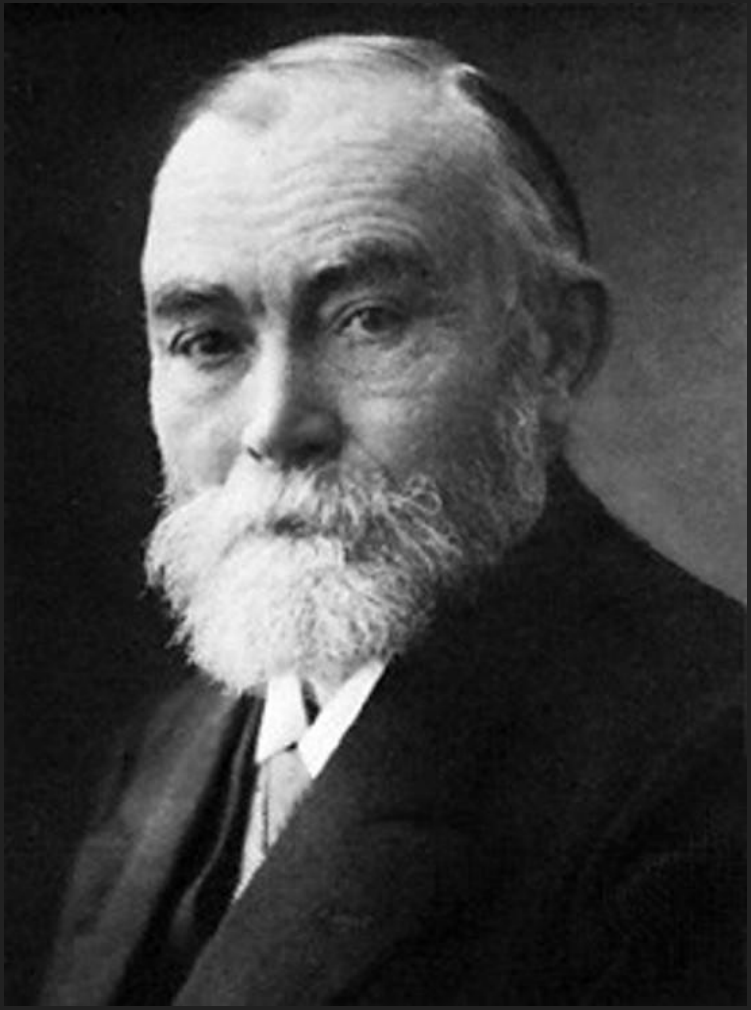
First Order Logic

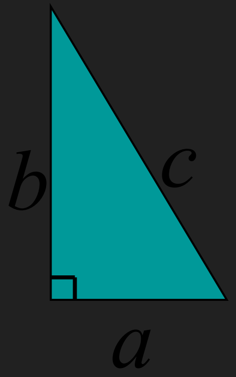


Limitation of Propositional Logic

Propositional logic – logic of simple statements

$$\neg, \wedge, \vee, \longrightarrow, \longleftrightarrow$$

How to formulate Pythagoreans' theorem using propositional logic?



How to formulate the statement that there are infinitely many primes?

Predicates

Predicates are propositions with variables

The **domain** of a variable is the set of all values that may be substituted in place of the variable.

Example: $P(x,y) ::= x + 2 = y$

$x = 1$ and $y = 3$: $P(1,3)$ is true

$x = 1$ and $y = 4$: $P(1,4)$ is false

$\neg P(1,4)$ is true

Set

R	Set of all real numbers
Z	Set of all integers
Q	Set of all rational numbers

$x \in A$ means that x is an element of *A*

$x \notin A$ means that x is not an element of *A*

Sets can be defined directly:

e.g. {1,2,4,8,16,32,...},

{CSC222,CSC222,...}

Truth Set

Sets can be defined by a predicate

Given a predicate P(x) and x has domain D, the truth set of P(x) is the set of all elements of D that make P(x) true.

$$\{x \in D \mid P(x)\}$$

e.g. Let P(x) be “n is the square of a number”,
and the domain D of x is set of positive integers.

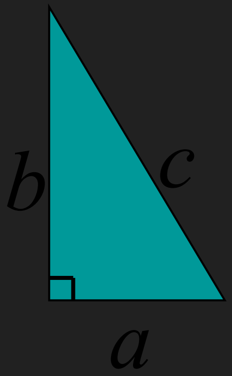
e.g. Let P(x) be “n is a prime number”,
and the domain D of x is set of positive integers.

The Universal Quantifier

$\forall$
x

For ALL x

$\forall\ x \in\ Z\ \ \forall\ y \in\ Z,\ x + y = y +$
$x.$



$\forall$ right − angled triangle

$$a^2 + b^2 = c^2$$

The Existential Quantifier

$\exists y$ There EXISTS some y

e.g. $\exists y, y^2 = y$

The truth of a predicate depends on the domain.

$$\forall x \exists y.\ x < y$$

Domain	Truth value
integers □	T
positive integers $□^+$	T
negative integers $□^-$	F
negative reals $□^-$	T

Translating Mathematical Theorem

Fermat (1637): If an integer n is greater than 2,
then the equation $a^n + b^n = c^n$ has no solutions in non-zero integers a, b, and c.

$$\forall n > 2 \ \forall a \in Z^+ \ \forall b \in Z^+ \ \forall c \in Z^+ \quad a^n + b^n \neq c^n$$

Andrew Wiles (1994) http://en.wikipedia.org/wiki/Fermat's_last_theorem

Translating Mathematical Theorem

Goldbach's conjecture: Every even number is the sum of two prime numbers.

Suppose we have a predicate prime(x) to determine if x is a prime number.

$$\forall n \in Z \ \text{even}(n) \rightarrow$$

$$\exists p \in Z \ \exists q \in Z \ \text{prime}(p) \ \wedge \ \text{prime}(q) \ \wedge \ p+q=n$$

How to write prime(p)?

$$\text{prime}(p) \quad :=$$

$$(p>1) \wedge (\forall a \in Z \ \forall b \in Z \ (a>1 \wedge b>1 \rightarrow a \cdot b \neq p))$$

Negations of Quantified Statements

Everyone likes football.

What is the negation of this statement?

Not everyone likes football = There exists someone who doesn't like football.

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

(generalized) DeMorgan's Law

Say the domain has only three values.

$$\neg\forall x P(x) \equiv \neg(P(1) \wedge P(2) \wedge P(3))$$

$$\equiv \neg P(1) \vee \neg P(2) \vee \neg P(3)$$

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

Negations of Quantified Statements

There is a plant that can fly.

What is the negation of this statement?

Not exists a plant that can fly = every plant cannot fly.

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

(generalized) DeMorgan's Law

Say the domain has only three values.

$$\neg \exists x P(x) \equiv \neg (P(1) \vee P(2) \vee P(3))$$

$$\equiv \neg P(1) \wedge \neg P(2) \wedge \neg P(3)$$

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

Order of Quantifiers

There is an anti-virus program killing every computer virus.

How to interpret this sentence?

For every computer virus, there is an anti-virus program that kills it.

$$\forall V \ \exists P, \mathsf{kill}(P, V)$$

- For every attack, I have a defense:
- against **MYDOOM**, use Defender
- against **ILOVEYOU**, use Norton
- against **BABLAS**, use Zonealarm …

□□ is expensive!

Order of Quantifiers

There is an anti-virus program killing every computer virus.

How to interpret this sentence?

There is one single anti-virus program that kills all computer viruses.

$$\exists P \ \forall V, \mathsf{kill}(P, V)$$

I have *one* defense good against every attack.

Example: P is CSE-antivirus,
protects against *ALL* viruses

That's much better!

Order of quantifiers is very important!

More Negations

There is an anti-virus program killing every computer virus.

$$\exists P\ \forall V, \mathsf{kill}(P, V)$$

What is the negation of this sentence?

$$\neg(\exists P\ \forall V, \mathsf{kill}(P, V))$$

$$\equiv \forall P\ \neg(\forall V, \mathsf{kill}(P, V))$$

$$\equiv \forall P \exists V \neg \mathsf{kill}(P, V))$$

For every program, there is some virus that it can not kill.

Exercises

1. There is a smallest positive integer.
2. There is no smallest positive real number.
3. There are infinitely many prime numbers.

Exercises

1. There is a smallest positive integer.

$$\exists s \in Z^{+} \ \forall x \in Z^{+} \ \ s \leq x$$

2. There is no smallest positive real number.

$$\forall r \in R^{+} \ \exists x \in R^{+} \ \ x < s$$

3. There are infinitely many prime numbers.

$$\forall p \in Z \ \exists q \in Z \ \ prime(p) \wedge prime(q) \wedge q > p$$

Predicate Calculus Validity

Propositional validity

$$(A \rightarrow B) \vee (B \rightarrow A)$$

True ***no matter what*** the truth values of *A* and *B* are

Predicate calculus validity

$$\forall z\, [Q(z) \;\square\; P(z)] \rightarrow [\forall x.Q(x) \;\square\; \forall y.P(y)]$$

True ***no matter what***

- the Domain is,
- or the predicates are.

That is, logically correct, independent of the specific content.

Arguments with Quantified Statements

Universal instantiation:

$$\begin{array}{rl} & \forall x, P(x) \\ \therefore & P(a) \end{array}$$

Universal modus ponens:

$$\begin{array}{rl} & \forall x, P(x) \rightarrow Q(x) \\ & P(a) \\ \therefore & Q(a) \end{array}$$

Universal modus tollens:

$$\begin{array}{rl} & \forall x, P(x) \rightarrow Q(x) \\ & \neg Q(a) \\ \therefore & \neg P(a) \end{array}$$

Universal Generalization

valid rule

$$\frac{A \rightarrow R(c)}{A \rightarrow \forall x. R(x)}$$

providing *c* is independent of *A*

e.g. given any number c, 2c is an even number

=> for all x, 2x is an even number.

Not Valid

$\forall z\,[Q(z) \square P(z)] \rightarrow [\forall x.Q(x) \square \forall y.P(y)]$

Proof: Give ***countermodel***, where

$\forall z\,[Q(z) \square P(z)]$ is true,

but $\forall x.Q(x) \square \forall y.P(y)$ is false.

Find a domain, and a predicate.

In this example, let domain be integers,

$Q(z)$ be true if z is an even number, i.e. Q(z)=even(z)

$P(z)$ be true if z is an odd number, i.e. P(z)=odd(z)

Then $\forall z\,[Q(z) \square P(z)]$ is true, because every number is either even or odd.

But $\forall x.Q(x)$ is not true, since not every number is an even number.

Similarly $\forall y.P(y)$ is not true, and so $\forall x.Q(x) \square \forall y.P(y)$ is not true.

Validity

$\forall z \in D\ \ [Q(z) \ \square\ P(z)] \rightarrow [\forall x \in D\ Q(x) \ \square\ \forall y \in D\ P(y)]$

Proof: Assume $\forall z\ [Q(z) \square P(z)]$.
So $Q(z) \square P(z)$ holds for all z in the domain D.

Now let c be some element in the domain D.

So $Q(c) \square P(c)$ holds (by instantiation), and therefore $Q(c)$ by itself holds.

But c could have been any element of the domain D.

So we conclude $\forall x.Q(x)$. (by generalization)

We conclude $\forall y.P(y)$ similarly (by generalization). Therefore,

$\forall x.Q(x) \ \square\ \forall y.P(y)$ QED.

Mathematical Proof

We prove mathematical statement by using logic.

$$\frac{P \rightarrow Q,\ Q \rightarrow R,\ R \rightarrow P}{P \wedge Q \wedge R}$$

not valid

To prove something is true, we need to assume some **axioms**!

This is invented by Euclid in 300 BC,
who begins with 5 assumptions about geometry,

and derive many theorems as logical consequences.

http://en.wikipedia.org/wiki/Euclidean_geometry

(see page 18 of the notes for the ZFC axioms for set theory)

Ideal Mathematical World

What do we expect from a logic system?

- What we prove is true. (soundness)
- What is true can be proven. (completeness)

Hilbert's program

- To resolve foundational crisis of mathematics (e.g. paradoxes)
- Find a finite, complete set of axioms,
  and provide a proof that these axioms were consistent.

http://en.wikipedia.org/wiki/Hilbert's_program

Power of Logic

Good news: Gödel's Completeness Theorem

Only need to know a few axioms & rules, to prove *all* validities.

That is, starting from a few propositional & simple predicate validities, every valid assertions can be proved using just universal generalization and *modus ponens* repeatedly!

modus ponens

$$\frac{P \to Q, P}{Q}$$

Limits of Logic

Gödel's *In*completeness Theorem for Arithmetic

For any "reasonable" theory that proves basic arithemetic truth, an arithmetic statement that is true, but not provable in the theory, can be constructed.

(very very brief) proof idea:

Any theory "expressive" enough can express the sentence

"This sentence is not provable."

If this is provable, then the theory is inconsistent.

So it is not provable.

Limits of Logic

Gödel's Second Incompleteness Theorem for Arithmetic

For any "reasonable" theory that proves basic arithemetic truth, it cannot prove its consistency.

No hope to find a complete and consistent set of axioms?!