First Order Logic

This Lecture

Last time we talked about propositional logic, i.e., logics on simple statements.

This time we will talk about first order logic, i.e., logics on quantified statements.

First order logic is much more expressive than propositional logic.

The topics on first order logic are:

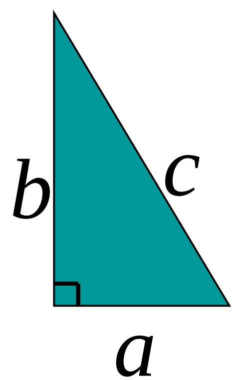
- Quantifiers
- Negation
- Multiple quantifiers
- Arguments of quantified statements

Limitation of Propositional Logic

Propositional logic – logic of simple statements

$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$$

How to formulate Pythagorean theorem using propositional logic?



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

Predicates

Predicates are propositions (i.e. statements) with variables.

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

When there is a variable, we need to specify what to put in the variables.

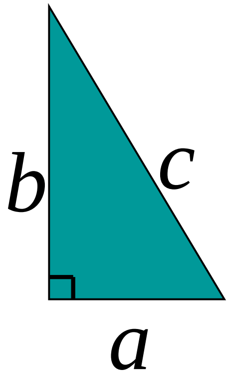
The **domain** of a variable is the set of all values that may be substituted in place of the variable.

The Universal Quantifier

The universal quantifier $\forall x$ for ALL x

Example: $\forall x \in Z^{+}$ $P(x)$ means $P(1) \wedge P(2) \wedge P(3) \wedge \ldots$

Example: $\forall x \in Z \; \forall y \in Z,\; x + y = y + x.$



Pythagorean theorem

$\forall$ right – angled triangle $a^2 + b^2 = c^2$

Example: $\forall x \quad x^2 \geq x$

This statement is true if the domain is Z, but not true if the domain is R.

The truth of a predicate depends on the domain.

The Existential Quantifier

$\exists y$ There EXISTS some y

$\exists y \in Z^+ \; P(y)$ means $P(1) \vee P(2) \vee P(3) \vee \ldots$

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 Z	T
positive integers Z^+	T
negative integers Z^-	F
negative reals R^-	T

Translating Mathematical Theorem

Translate to a logical formula?

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

Three IMPORTANT elements:

- **Conditions:** $a^n + b^n \neq c^n$
- **Variables:** a, b, c, n
- **Domains:** $a \in Z^+$, $b \in Z^+$, $c \in Z^+$, $n \in Z$, $n > 2$

Last step: Add quantifiers & reconcile the order

$$\forall a, b, c \in \mathbb{Z}^+, (n \leq 2) \vee (n \notin \mathbb{Z}) \vee (a^n + b^n \neq c^n)$$

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

Translating Mathematical Theorem

Goldbach's conjecture: Every positive even number is a sum of two primes.

Suppose we already have predicates prime(x), even(x), odd(x).

1. **Conditions:** p+q=n
2. **Variables:** p, q, n
3. **Domains:** prime(p), prime(q), even(n), $n \in Z^+$
4. **Add quantifiers and reconcile the order:**

$$\forall n \in \mathbb{Z}^+, \mathrm{odd}(n) \vee (\exists p, q \in \mathbb{Z}, \mathrm{prime}(p) \wedge \mathrm{prime}(q) \wedge (p + q = n))$$

Translating Mathematical Theorem

How to write prime(p)?

A **prime number** (or a **prime**) is a natural number greater than 1 that has no positive divisors other than 1 and itself.

1. **Conditions:** p≠a·b
2. **Variables:** p, a, b
3. **Domains:** p,a,b>1; $p, a, b \in \mathbb{Z}$
4. **Add quantifiers and reconcile the order:**

$$(p > 1) \land (p \in \mathbb{Z}) \land (\forall a, b \in \mathbb{Z}^+, (p \neq a \cdot b) \lor (a = 1) \lor (a = p))$$

- Quantifiers
- Negation
- Multiple quantifiers
- Arguments of quantified statements

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.

$$\begin{aligned} \neg \forall x P(x) &\equiv \neg(P(1) \wedge P(2) \wedge P(3)) \\ &\equiv \neg(P(1) \wedge P(2)) \vee \neg P(3) \\ &\equiv \neg P(1) \vee \neg P(2) \vee \neg P(3) \quad \equiv \exists x \neg P(x) \end{aligned}$$

The same idea can be used to prove for any number of variables.

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.

$$\begin{aligned}
\neg \exists x P(x) &\equiv \neg(P(1) \vee P(2) \vee P(3)) \\
&\equiv \neg(P(1) \vee P(2)) \wedge \neg P(3) \\
&\equiv \neg P(1) \wedge \neg P(2) \wedge \neg P(3) \\
&\equiv \forall x \neg P(x)
\end{aligned}$$

The same idea can be used to prove for any number of variables.

- Quantifiers
- Negation
- **Multiple quantifiers**
- Arguments of quantified statements

Order of Quantifiers

Anti-virus programs kill all 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 ...

$\forall\exists$ is expensive!

Order of Quantifiers

There is an anti-virus program killing all 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!

Order of Quantifiers

Let's say we have an array A of size 6x6.

$$\forall \text{ row } x \; \exists \text{ column } y \quad A[x, y] = 1$$

1					
	1	1		1	
		1			
		1		1	
			1		
		1			

Then this table satisfies the statement.

Order of Quantifiers

Let's say we have an array A of size 6x6.

$$\exists \text{ row } x \; \forall \text{ column } y \quad A[x,y] = 1$$

1					
	1	1		1	
		1			
		1		1	
			1		
		1			

But if the order of the quantifiers are changes,
then this table no longer satisfies the new statement.

Order of Quantifiers

Let's say we have an array A of size 6x6.

$$\exists \text{ row } x \; \forall \text{ column } y \quad A[x,y] = 1$$

1	1	1	1	1	1

To satisfy the new statement, there must be a row with all ones.

Questions

Are these statements equivalent?

$$\forall \text{ row } x \ \forall \text{ column } y \quad A[x,y] = 1$$

$$\forall \text{ column } y \ \forall \text{ row } x \quad A[x,y] = 1$$

Are these statements equivalent?

$$\exists \text{ row } x \ \exists \text{ column } y \quad A[x,y] = 1$$

$$\exists \text{ column } y \ \exists \text{ row } x \quad A[x,y] = 1$$

Yes, in general, you can change the order of two "forall"s, and you can change the order of two "exist"s.

More Negations

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

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

What is the negation of the above 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.

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

2. There is no smallest positive real number.

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

In words, there is always a smaller positive real number.

Exercises

3. There are infinitely many prime numbers.

This sentence contains two meanings:

There exists a prime. **+** There is no largest prime.

$$(\exists\, p \in \mathbb{Z}, prime(p)) \wedge (\forall\, p \in \mathbb{Z}^{+}, \neg prime(p) \vee (\exists q \in \mathbb{Z}, prime(q) \wedge (q > p)))$$

Formulating sentences using first order logic is useful in logic programming and database queries.

- Quantifiers
- Negation
- Multiple quantifiers
- Arguments of quantified statements

Predicate Calculus Validity

Propositional logic	**First order logic**
A tautology is true ***no matter what*** the truth values of A and B are.	A tautology is true ***no matter what*** the domain of x,y,z is, or P,Q are.
E.g., (A -> B) V (B -> A)	E.g., $\forall z, [Q(z) \wedge P(z)] \rightarrow [\forall x, Q(x) \wedge \forall y, P(y)]$

Generalizing the propositional logic,

A **quantified argument** (i.e. arugment with variables, quantifiers) is *valid* if the conclusion is true whenever the assumptions are true.

Arguments with Quantified Statements

Universal instantiation:

$$\forall x, P(x)$$
$$\therefore\ P(a)$$

Universal modus ponens:

$$\forall x, P(x) \rightarrow Q(x)$$
$$P(a)$$
$$\therefore\ Q(a)$$

Universal modus tollens:

$$\forall x, P(x) \rightarrow Q(x)$$
$$\neg Q(a)$$
$$\therefore\ \neg P(a)$$

Universal Generalization

valid rule

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

providing c is independent of *A*

Informally, if we could prove that R(c) is true for an arbitrary c
(in a sense, c is a "variable"), then we could prove the statement for all values.

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

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

Remark: Universal generalization is often difficult to prove, we will introduce mathematical induction to prove the validity for all values.

Valid Rule?

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

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

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

but $\forall x.Q(x) \vee \forall y.P(y)$ 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 $\forall z\, [Q(z) \vee P(z)]$ 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 $\forall x.Q(x) \vee \forall y.P(y)$ is not true.

Valid Rule?

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

Proof: Assume $\forall z\ [Q(z) \wedge P(z)]$ is true.

So $Q(z) \wedge P(z)$ is true for all z in the domain D.

Now let c be some element in the domain D.

So $Q(c) \wedge P(c)$ is true (by instantiation), and thus $Q(c)$ is true.

But c could be any element in the domain D.

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

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

$\forall x.Q(x) \wedge \forall y.P(y)$ is ture. QED.

Summary

This finishes the introduction to logic. We shall use logic to do mathematical proofs.

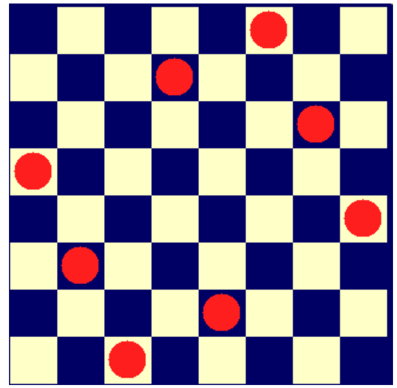
At this point, you should be able to:

- Express (quantified) statements using logical formulas
- Use simple logic rules (e.g. DeMorgan, contrapositive, etc)
- Fluent with arguments and logical equivalence

Applications of Logic

Logic programming

solve problems by logic

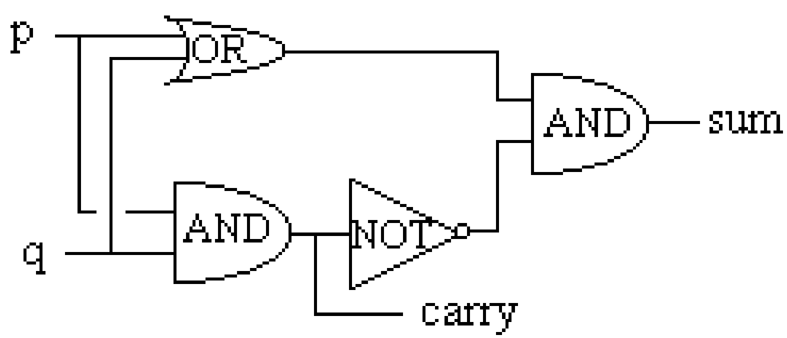


	1		6		7			4
	4	2						
8	7		3			6		
	8			7			2	
			8	9	3			
	3			6			1	
		8			6		4	5
						1	7	
4			9		8		6	

Database

making queries, data mining

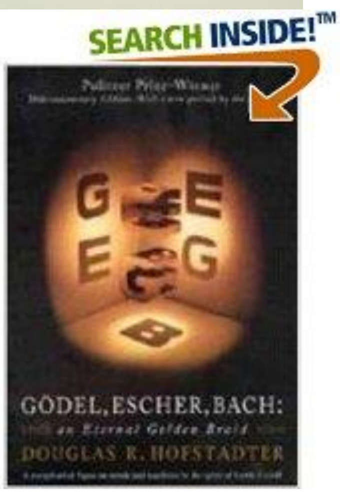
Digital circuit



p	q	sum	carry
1	1	0	1
1	0	1	0
0	1	1	0
0	0	0	0

(Optional) More About Logic

Ideally, we can come up with a "perfect" logical system, which is consistent (not having contradictions) and is powerful (can derive everything that is true).



But Gödel proved that there is no perfect logical system.

This is called the Gödel's incompleteness theorem.

It is an important and surprising result in mathematics.

The ideas in his proof are also influential in computer science,

to prove that certain problem is not computable,

e.g. it is impossible to write a program to check whether

another program will loop forever on a particular input

(see Halting Problem in Note 2.1).