Discrete Mathematics and Its Applications

Lecture 1: The Foundations: Logic and Proofs (1.3-1.5)

MING GAO

DASE @ ECNU
(for course related communications)
mgao@dase.ecnu.edu.cn

Sep. 18, 2018

Outline

Motivation

Example

There are two kinds of inhabitants in an island, knights, who always tell the truth, knaves, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B says "The two of us are opposite types"?

Motivation

Example

There are two kinds of inhabitants in an island, knights, who always tell the truth, knaves, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B says "The two of us are opposite types"?

Solution:

- p : *"A is a knight;"*
- q : *"B is a knight;"*

Motivation

Example

There are two kinds of inhabitants in an island, knights, who always tell the truth, knaves, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B says "The two of us are opposite types"?

Solution:

- p : *"A is a knight;"*
- q : *"B is a knight;"*

- If A is a knight, we have $p \wedge q \wedge ((\neg p \wedge q) \vee (p \wedge \neg q))$.

Motivation

Example

There are two kinds of inhabitants in an island, knights, who always tell the truth, knaves, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B says "The two of us are opposite types"?

Solution:

- p : *"A is a knight;"*
- q : *"B is a knight;"*

- If A is a knight, we have $p \wedge q \wedge ((\neg p \wedge q) \vee (p \wedge \neg q))$.
- If A is a knave, we have $\neg p \wedge \neg q \wedge ((p \wedge q) \vee (\neg p \wedge \neg q))$.

Motivation

Example

There are two kinds of inhabitants in an island, knights, who always tell the truth, knaves, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B says "The two of us are opposite types"?

Solution:

- p : *"A is a knight;"*
- q : *"B is a knight;"*

- If A is a knight, we have $p \wedge q \wedge ((\neg p \wedge q) \vee (p \wedge \neg q))$.
- If A is a knave, we have $\neg p \wedge \neg q \wedge ((p \wedge q) \vee (\neg p \wedge \neg q))$.

The problem is how to determine the truth value of the propositions.

Logical equivalences

Definition

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

Logical equivalences

Definition

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

- Compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology, denoted as $p \equiv q$ or $p \Leftrightarrow q$.

Logical equivalences

Definition

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

- Compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology, denoted as $p \equiv q$ or $p \Leftrightarrow q$.
- Remark: Symbol $\equiv$ is not a logical connectives, and $p \equiv q$ is not a proposition.

Logical equivalences

Definition

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

- Compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology, denoted as $p \equiv q$ or $p \Leftrightarrow q$.
- Remark: Symbol $\equiv$ is not a logical connectives, and $p \equiv q$ is not a proposition.
- One way to determine whether two compound propositions are equivalent is to use a truth table.

De Morgan's laws

Laws

$$\neg(p \land q) \equiv \neg p \lor \neg q$$
$$\neg(p \lor q) \equiv \neg p \land \neg q$$

De Morgan's laws

Laws

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

- $\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \neg \cdots \vee \neg p_n$, i.e., $\neg \bigwedge_{i=1}^{n} p_i \equiv \bigvee_{i=1}^{n} \neg p_i$.
- $\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv \neg p_1 \wedge \neg p_2 \wedge \neg \cdots \wedge \neg p_n$, i.e., $\neg \bigvee_{i=1}^{n} p_i \equiv \bigwedge_{i=1}^{n} \neg p_i$.

De Morgan's laws

Laws

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

- $\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \neg \cdots \vee \neg p_n$, i.e., $\neg \bigwedge_{i=1}^{n} p_i \equiv \bigvee_{i=1}^{n} \neg p_i$.
- $\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv \neg p_1 \wedge \neg p_2 \wedge \neg \cdots \wedge \neg p_n$, i.e., $\neg \bigvee_{i=1}^{n} p_i \equiv \bigwedge_{i=1}^{n} \neg p_i$.

The truth table can be used to determine whether two compound propositions are equivalent.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Logical equivalence

Table of logical equivalence

equivalence	name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \wedge \neg p \equiv F$ $p \vee \neg p \equiv T$	Negation laws

Logical equivalence Cont'd

Table of logical equivalence

equivalence	name
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	Commutative laws
$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$\neg(\neg p) \equiv p$	Double negation law

Equivalence of implication

Equivalence law

$p \rightarrow q \equiv \neg p \vee q$

Equivalence of implication

Equivalence law

$p \to q \equiv \neg p \vee q$

The truth table can be used to determine whether two compound propositions are equivalent.

p	q	$p \to q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \to q \equiv \neg p \vee q$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \rightarrow q \equiv \neg p \vee q$
- $p \rightarrow q \equiv \neg q \rightarrow \neg p$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \rightarrow q \equiv \neg p \vee q$
- $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- $p \vee q \equiv \neg p \rightarrow q$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \rightarrow q \equiv \neg p \vee q$
- $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- $p \vee q \equiv \neg p \rightarrow q$
- $p \wedge q \equiv \neg(p \rightarrow \neg q)$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $p \vee q \equiv \neg p \to q$
- $p \wedge q \equiv \neg(p \to \neg q)$
- $\neg(p \to q) \equiv p \wedge \neg q$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $p \vee q \equiv \neg p \to q$
- $p \wedge q \equiv \neg(p \to \neg q)$
- $\neg(p \to q) \equiv p \wedge \neg q$
- $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $p \vee q \equiv \neg p \to q$
- $p \wedge q \equiv \neg(p \to \neg q)$
- $\neg(p \to q) \equiv p \wedge \neg q$
- $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
- $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $p \vee q \equiv \neg p \to q$
- $p \wedge q \equiv \neg(p \to \neg q)$
- $\neg(p \to q) \equiv p \wedge \neg q$
- $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
- $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
- $(p \to r) \wedge (q \to r) \equiv (p \wedge q) \to r$

Logical equivalences involving conditional statements

Table of logical equivalences involving conditional statements

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $p \vee q \equiv \neg p \to q$
- $p \wedge q \equiv \neg(p \to \neg q)$
- $\neg(p \to q) \equiv p \wedge \neg q$
- $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
- $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
- $(p \to r) \wedge (q \to r) \equiv (p \wedge q) \to r$
- $(p \to r) \vee (q \to r) \equiv (p \vee q) \to r$

Logical equivalences involving biconditional statements

Table of logical equivalences involving biconditional statements

- $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

Logical equivalences involving biconditional statements

Table of logical equivalences involving biconditional statements

- $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

Logical equivalences involving biconditional statements

Table of logical equivalences involving biconditional statements

- $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
- $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

Logical equivalences involving biconditional statements

Table of logical equivalences involving biconditional statements

- $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
- $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
- $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Logical equivalences involving biconditional statements

Table of logical equivalences involving biconditional statements

- $p \leftrightarrow q \equiv (p \rightarrow q) \land (q \rightarrow p)$
- $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
- $p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$
- $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Show that $\neg(p \leftrightarrow q)$ and $p \leftrightarrow \neg q$ are logically equivalent.

$$
\begin{aligned}
\neg(p \leftrightarrow q) &\equiv \neg((\neg p \lor q) \land (\neg q \lor p)) \\
&\equiv (p \land \neg q) \lor (q \land \neg p) \\
&\equiv (p \lor (q \land \neg p)) \land (\neg q \lor (q \land \neg p)) \\
&\equiv ((p \lor q) \land (p \lor \neg p)) \land ((\neg q \lor q) \land (\neg q \lor \neg p)) \\
&\equiv (\neg(\neg q) \lor p) \land (\neg p \lor \neg q)) \\
&\equiv (\neg q \rightarrow p) \land (p \rightarrow \neg q)) \equiv p \leftrightarrow \neg q \qquad (1)
\end{aligned}
$$

Propositional satisfiability

Definition

A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true.

Propositional satisfiability

Definition

A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true.

Determine whether each of the compound propositions $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$.

Propositional satisfiability

Definition

A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true.

Determine whether each of the compound propositions $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$.

$$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \equiv (q \rightarrow p) \wedge (r \rightarrow q) \wedge (p \rightarrow r)$$

Propositional satisfiability

Definition

A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true.

Determine whether each of the compound propositions $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$.

$$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \equiv (q \rightarrow p) \wedge (r \rightarrow q) \wedge (p \rightarrow r)$$

Note that $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ is true when the three variable p, q, and r have the same truth value.

Propositional satisfiability

Definition

A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true.

Determine whether each of the compound propositions $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$.

$$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \equiv (q \rightarrow p) \wedge (r \rightarrow q) \wedge (p \rightarrow r)$$

Note that $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ is true when the three variable p, q, and r have the same truth value.
Hence, it is satisfiable as there is at least one assignment of truth values for p, q, and r that makes it true.

Applications of satisfiability

Sudoku puzzle

For each cell with a given value, we assert $p(i,j,n)$ when the cell in row i and column j has the given value n.

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

Applications of satisfiability

Sudoku puzzle

For each cell with a given value, we assert $p(i, j, n)$ when the cell in row i and column j has the given value n.

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

- For every row, we assert: $\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$;

Applications of satisfiability

Sudoku puzzle

For each cell with a given value, we assert $p(i, j, n)$ when the cell in row i and column j has the given value n.

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

- For every row, we assert: $\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$;
- For every column, we assert: $\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$;

Applications of satisfiability

Sudoku puzzle

For each cell with a given value, we assert $p(i,j,n)$ when the cell in row i and column j has the given value n.

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

- For every row, we assert: $\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i,j,n)$;
- For every column, we assert: $\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i,j,n)$;
- For every block, we assert it contains every number: $\bigwedge_{r=0}^{2} \bigwedge_{s=0}^{2} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r+i, cs+j, n)$;

Applications of satisfiability

Sudoku puzzle

For each cell with a given value, we assert $p(i, j, n)$ when the cell in row i and column j has the given value n.

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

- For every row, we assert: $\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$;
- For every column, we assert: $\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$;
- For every block, we assert it contains every number: $\bigwedge_{r=0}^{2} \bigwedge_{s=0}^{2} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r + i, cs + j, n)$;
- To assert that no cell contains more than one number, we take the conjunction over all values of n, $n^{'}$, i, and j where each variable ranges from 1 to 9 and $n \neq n^{'}$ of $p(i, j, n) \rightarrow \neg p(i, j, n^{'})$.

Motivation I

In many cases, the statement we are interested in contains variables.

Example

"e is even", "p is prime", or "s is a student".

Motivation I

In many cases, the statement we are interested in contains variables.

Example

"e is even", "p is prime", or "s is a student".
As we previously did with propositions, we can use variables to represent these statements.

- $E(x)$: "x is even";

Motivation I

In many cases, the statement we are interested in contains variables.

Example

"e is even", "p is prime", or "s is a student".
As we previously did with propositions, we can use variables to represent these statements.

- $E(x)$: "x is even";
- $P(y)$: "y is prime";

Motivation I

In many cases, the statement we are interested in contains variables.

Example

"e is even", "p is prime", or "s is a student".
As we previously did with propositions, we can use variables to represent these statements.

- $E(x)$: "x is even";
- $P(y)$: "y is prime";
- $S(w)$: "w is a student".

Motivation I

In many cases, the statement we are interested in contains variables.

Example

"e is even", "p is prime", or "s is a student".

As we previously did with propositions, we can use variables to represent these statements.

- $E(x)$: "x is even";
- $P(y)$: "y is prime";
- $S(w)$: "w is a student".

You can think of $E(x)$, $P(y)$ and $S(w)$ as statements that may be true of false depending on the values of its variables.

Motivation II

Example

- *"Every computer connected to the university network is functioning properly."*
  No rules of propositional logic allow us to conclude the truth of the statement
  "$MATH_3$ is functioning properly, if $MATH_3$ is one of the computers connected to the university network."

Motivation II

Example

- *"Every computer connected to the university network is functioning properly."*
  No rules of propositional logic allow us to conclude the truth of the statement
  "$MATH_3$ is functioning properly, if $MATH_3$ is one of the computers connected to the university network."
- Likewise, we cannot use the rules of propositional logic to conclude from the statement
  "CS_2 is under attack by an intruder, and CS_2 is a computer on the university network."
  We can conclude the truth of *"There is a computer on the university network that is under attack by an intruder."*

Motivation II

Example

- *"Every computer connected to the university network is functioning properly."*
  No rules of propositional logic allow us to conclude the truth of the statement
  "$MATH_3$ is functioning properly, if $MATH_3$ is one of the computers connected to the university network."
- Likewise, we cannot use the rules of propositional logic to conclude from the statement
  "CS_2 is under attack by an intruder, and CS_2 is a computer on the university network."
  We can conclude the truth of *"There is a computer on the university network that is under attack by an intruder."*

Predicate logic is a more powerful type of logic theory.

Predicates

Definition

"x is greater than 3" has two parts: variable x (the subject of the statement), and *predicate P* "is greater than 3", denoted as $P(x) : x > 3$.

Predicates

Definition

"x is greater than 3" has two parts: variable x (the subject of the statement), and *predicate P* "is greater than 3", denoted as $P(x) : x > 3$.

- Statement $P(x)$ is the value of the propositional function P at x;

Predicates

Definition

"x is greater than 3" has two parts: variable x (the subject of the statement), and *predicate P* "is greater than 3", denoted as $P(x) : x > 3$.

- Statement $P(x)$ is the value of the propositional function P at x;
- Once variable x is fixed, statement $P(x)$ becomes a proposition and has a truth value. e.g., $P(4)$ (true) and $P(2)$ (false)

Predicates

Definition

"x is greater than 3" has two parts: variable x (the subject of the statement), and *predicate P* "is greater than 3", denoted as $P(x) : x > 3$.

- Statement $P(x)$ is the value of the propositional function P at x;
- Once variable x is fixed, statement $P(x)$ becomes a proposition and has a truth value. e.g., $P(4)$ (true) and $P(2)$ (false)
- Let $A(x)$ denote "Computer x is under attack by an intruder". Assume that CS_2 in the campus is currently under attack by intruders. What are truth values of $A(CS_1)$, and $A(CS_2)$?

Predicates

Definition

"x is greater than 3" has two parts: variable x (the subject of the statement), and *predicate P* "is greater than 3", denoted as $P(x) : x > 3$.

- Statement $P(x)$ is the value of the propositional function P at x;
- Once variable x is fixed, statement $P(x)$ becomes a proposition and has a truth value. e.g., $P(4)$ (true) and $P(2)$ (false)
- Let $A(x)$ denote "Computer x is under attack by an intruder". Assume that CS_2 in the campus is currently under attack by intruders. What are truth values of $A(CS_1)$, and $A(CS_2)$?
- Let $Q(x, y)$ denote the statement "x = y + 3". What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Predicates

Definition

"x is greater than 3" has two parts: variable x (the subject of the statement), and *predicate P* "is greater than 3", denoted as $P(x) : x > 3$.

- Statement $P(x)$ is the value of the propositional function P at x;
- Once variable x is fixed, statement $P(x)$ becomes a proposition and has a truth value. e.g., $P(4)$ (true) and $P(2)$ (false)
- Let $A(x)$ denote "Computer x is under attack by an intruder". Assume that CS_2 in the campus is currently under attack by intruders. What are truth values of $A(CS_1)$, and $A(CS_2)$?
- Let $Q(x, y)$ denote the statement "x = y + 3". What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

In general, a statement involving n variables $x_1, x_2, \cdots, x_n$ can be denoted by $P(x_1, x_2, \cdots, x_n)$, where P is also called an n-place predicate or a n-ary predicate, and $x_1, x_2, \cdots, x_n$ is a n-tuple.

Quantifiers

Quantification

Quantification expresses the extent to which a predicate is true over a range of elements. In general, all values of a variable is called the *domain of discourse* (or *universe of discourse*), just referred to as *domain*.

Quantifiers

Quantification

Quantification expresses the extent to which a predicate is true over a range of elements. In general, all values of a variable is called the *domain of discourse* (or *universe of discourse*), just referred to as *domain*.

1. The *universal quantification* of $P(x)$ is the statement "$P(x)$ for all values of x in the domain". Notation $\forall x P(x)$ denotes the universal quantification of $P(x)$, where $\forall$ is called the universal quantifier. An element for which $P(x)$ is false is called a counterexample of $\forall x P(x)$.

Quantifiers

Quantification

Quantification expresses the extent to which a predicate is true over a range of elements. In general, all values of a variable is called the *domain of discourse* (or *universe of discourse*), just referred to as *domain*.

1. The *universal quantification* of $P(x)$ is the statement "$P(x)$ for all values of x in the domain". Notation $\forall x P(x)$ denotes the universal quantification of $P(x)$, where $\forall$ is called the universal quantifier. An element for which $P(x)$ is false is called a counterexample of $\forall x P(x)$.
2. The *existential quantification* of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$". Notation $\exists x P(x)$ denotes the existential quantification of $P(x)$, where $\exists$ is called the existential quantifier.

Quantifiers

Quantification

Quantification expresses the extent to which a predicate is true over a range of elements. In general, all values of a variable is called the *domain of discourse* (or *universe of discourse*), just referred to as *domain*.

1. The *universal quantification* of $P(x)$ is the statement "$P(x)$ for all values of x in the domain". Notation $\forall x P(x)$ denotes the universal quantification of $P(x)$, where $\forall$ is called the universal quantifier. An element for which $P(x)$ is false is called a counterexample of $\forall x P(x)$.
2. The *existential quantification* of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$". Notation $\exists x P(x)$ denotes the existential quantification of $P(x)$, where $\exists$ is called the existential quantifier.

Statement	When True?	When False?
$\forall x P(x)$	$P(x)$ is true for every x	$\exists x$ for which $P(x)$ is false
$\exists x P(x)$	$\exists x$ for which $P(x)$ is true	$P(x)$ is false for every x

Examples

Universal quantification

1. Let $P(x)$ be "$x+1>x$". What is the truth value of $\forall x P(x)$ for $\forall x \in R$?

   Note that if the domain is empty, then $\forall x P(x)$ is true for any propositional function $P(x)$ because there are no elements x in the domain for which $P(x)$ is false.

2. Let $P(x)$ be "$x^2>0$". What is the truth value of $\forall x P(x)$ for $\forall x \in Z$? (Note that $x=0$ is a counterexample because $x^2=0$.)

Examples

Universal quantification

1. Let $P(x)$ be "$x + 1 > x$". What is the truth value of $\forall x P(x)$ for $\forall x \in R$?

   Note that if the domain is empty, then $\forall x P(x)$ is true for any propositional function $P(x)$ because there are no elements x in the domain for which $P(x)$ is false.

2. Let $P(x)$ be "$x^2 > 0$". What is the truth value of $\forall x P(x)$ for $\forall x \in Z$? (Note that $x = 0$ is a counterexample because $x^2 = 0$.)

Existential quantification

1. Let $P(x)$ denote "$x > 3$". What is the truth value of $\exists x P(x)$ for $\forall x \in R$?
2. Let $P(x)$ be "$x^2 > 0$". What is the truth value of $\exists x P(x)$ for $\forall x \in Z$?

Remarks

When all the elements in the domain can be listed as $x_1, x_2, \cdots, x_n$

Universal quantification

$\forall x P(x)$ is the same as conjunction

$$P(x_1) \wedge P(x2) \wedge \cdots \wedge P(x_n),$$

because this conjunction is true if and only if $P(x_1)$, $P(x_2), \cdots, P(x_n)$ are all true.

Remarks

When all the elements in the domain can be listed as $x_1, x_2, \cdots, x_n$

Universal quantification

$\forall x P(x)$ is the same as conjunction

$$P(x_1) \wedge P(x2) \wedge \cdots \wedge P(x_n),$$

because this conjunction is true if and only if $P(x_1)$, $P(x_2), \cdots, P(x_n)$ are all true.

Existential quantification

$\exists x P(x)$ is the same as disjunction

$$P(x_1) \vee P(x2) \vee \cdots \vee P(x_n),$$

since the disjunction is true if and only if at least one of $P(x_1)$, $P(x_2), \cdots, P(x_n)$ is true.

Quantifiers with restricted domains

Example

What do the statements $\forall x < 0(x^2 > 0)$ and $\exists y > 0(y^2 = 2)$ mean, where the domain in each case consists of the real numbers?

Quantifiers with restricted domains

Example

What do the statements $\forall x < 0(x^2 > 0)$ and $\exists y > 0(y^2 = 2)$ mean, where the domain in each case consists of the real numbers?

1. The statement $\forall x < 0(x^2 > 0)$ states that for every real number x with $x < 0, x^2 > 0$, i.e., it states "The square of a negative real number is positive". This statement is the same as $\forall x(x < 0 \rightarrow x^2 > 0)$.

Quantifiers with restricted domains

Example

What do the statements $\forall x < 0(x^2 > 0)$ and $\exists y > 0(y^2 = 2)$ mean, where the domain in each case consists of the real numbers?

1. The statement $\forall x < 0(x^2 > 0)$ states that for every real number x with $x < 0, x^2 > 0$, i.e., it states "The square of a negative real number is positive". This statement is the same as $\forall x(x < 0 \rightarrow x^2 > 0)$.
2. The statement $\exists y > 0(y^2 = 2)$ states "There is a positive square root of 2", i.e., $\exists y(y > 0 \wedge y^2 = 2)$.

Quantifiers with restricted domains

Example

What do the statements $\forall x < 0(x^2 > 0)$ and $\exists y > 0(y^2 = 2)$ mean, where the domain in each case consists of the real numbers?

1. The statement $\forall x < 0(x^2 > 0)$ states that for every real number x with $x < 0, x^2 > 0$, i.e., it states "The square of a negative real number is positive". This statement is the same as $\forall x(x < 0 \to x^2 > 0)$.
2. The statement $\exists y > 0(y^2 = 2)$ states "There is a positive square root of 2", i.e., $\exists y(y > 0 \land y^2 = 2)$.

- Note that the restriction of a universal quantification is the same as the universal quantification of a conditional statement.

Quantifiers with restricted domains

Example

What do the statements $\forall x < 0(x^2 > 0)$ and $\exists y > 0(y^2 = 2)$ mean, where the domain in each case consists of the real numbers?

1. The statement $\forall x < 0(x^2 > 0)$ states that for every real number x with $x < 0, x^2 > 0$, i.e., it states "The square of a negative real number is positive". This statement is the same as $\forall x(x < 0 \to x^2 > 0)$.
2. The statement $\exists y > 0(y^2 = 2)$ states "There is a positive square root of 2", i.e., $\exists y(y > 0 \wedge y^2 = 2)$.

- Note that the restriction of a universal quantification is the same as the universal quantification of a conditional statement.
- On the other hand, the restriction of an existential quantification is the same as the existential quantification of a conjunction.

Precedence of quantifiers and binding variables

Precedence of quantifiers

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.

- $\forall x P(x) \wedge Q(x) \equiv (\forall x P(x)) \wedge Q(x)$, rather than $\forall x (P(x) \wedge Q(x))$.
- $\exists x P(x) \vee Q(x) \equiv (\exists x P(x)) \vee Q(x)$.

Precedence of quantifiers and binding variables

Precedence of quantifiers

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.

- $\forall x P(x) \wedge Q(x) \equiv (\forall x P(x)) \wedge Q(x)$, rather than $\forall x(P(x) \wedge Q(x))$.
- $\exists x P(x) \vee Q(x) \equiv (\exists x P(x)) \vee Q(x)$.

Bound and free

In statement $\exists x(x + y = 1)$, variable x is bound by the existential quantification $\exists x$, but variable y is free because it is not bound by a quantifier and no value is assigned to this variable. This illustrates that in the statement, x is *bound*, but y is *free*.

The part of a logical expression to which a quantifier is applied is called the *scope* of this quantifier. Consequently, a variable is free if it is outside the scope of all quantifiers in the formula that specify this variable.

Logical equivalences involving quantifiers

Definition

Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional functions. We use the notation $S \equiv T$ to indicate that two statements S and T involving predicates and quantifiers are logically equivalent.

Logical equivalences involving quantifiers

Definition

Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional functions. We use the notation $S \equiv T$ to indicate that two statements S and T involving predicates and quantifiers are logically equivalent.

Table of logical equivalence

equivalence	name
$\forall x(P(x) \land Q(x)) \equiv \forall xP(x) \land \forall xQ(x)$	Distributive law
$\neg\forall xP(x) \equiv \exists x\neg P(x)$ $\neg\exists xP(x) \equiv \forall x\neg P(x)$	Negation law
$\neg\forall x(P(x) \rightarrow Q(x)) \equiv \exists x(P(x) \land \neg Q(x))$	

Quantifiers in system specifications

Example

Use predicates and quantifiers to express the system specifications "Every mail message larger than one megabyte will be compressed" and "If a user is active, at least one network link will be available."

Quantifiers in system specifications

Example

Use predicates and quantifiers to express the system specifications "Every mail message larger than one megabyte will be compressed" and "If a user is active, at least one network link will be available."

- Let $S(m, y)$ be "Mail message m is larger than y megabytes," where variable x has the domain of all mail messages and variable y is a positive real number, and let $C(m)$ denote "Mail message m will be compressed." Then "Every mail message larger than one megabyte will be compressed" can be represented as $\forall m(S(m, 1) \rightarrow C(m))$.

Quantifiers in system specifications

Example

Use predicates and quantifiers to express the system specifications "Every mail message larger than one megabyte will be compressed" and "If a user is active, at least one network link will be available."

- Let $S(m, y)$ be "Mail message m is larger than y megabytes," where variable x has the domain of all mail messages and variable y is a positive real number, and let $C(m)$ denote "Mail message m will be compressed." Then "Every mail message larger than one megabyte will be compressed" can be represented as $\forall m(S(m, 1) \rightarrow C(m))$.
- Let $A(u)$ represent "User u is active," where variable u has the domain of all users, let $S(n, x)$ denote "Network link n is in state x," where n has the domain of all network links and x has the domain of all possible states for a network link. Then "If a user is active, at least one network link will be available" can be represented by $\exists u A(u) \rightarrow \exists n S(n, available)$.

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another.

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another. For example, $\forall x \exists y(x + y = 0)$. Note that everything within the scope of a quantifier can be thought of as a propositional function. $\forall x \exists y(x + y = 0)$ is the same thing as $\forall x Q(x)$, where $Q(x)$ is $\exists y P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Please translate following nested quantifiers into statements

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another. For example, $\forall x \exists y(x + y = 0)$. Note that everything within the scope of a quantifier can be thought of as a propositional function. $\forall x \exists y(x + y = 0)$ is the same thing as $\forall x Q(x)$, where $Q(x)$ is $\exists y P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Please translate following nested quantifiers into statements

- $\forall x \forall y(x + y = y + x)$ for $\forall x, y \in R$.

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another. For example, $\forall x \exists y(x + y = 0)$. Note that everything within the scope of a quantifier can be thought of as a propositional function. $\forall x \exists y(x + y = 0)$ is the same thing as $\forall x Q(x)$, where $Q(x)$ is $\exists y P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Please translate following nested quantifiers into statements

- $\forall x \forall y(x + y = y + x)$ for $\forall x, y \in R$.
- $\forall x \exists y(x + y = 0)$ for $\forall x, y \in R$.

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another. For example, $\forall x \exists y(x + y = 0)$. Note that everything within the scope of a quantifier can be thought of as a propositional function. $\forall x \exists y(x + y = 0)$ is the same thing as $\forall x Q(x)$, where $Q(x)$ is $\exists y P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Please translate following nested quantifiers into statements

- $\forall x \forall y(x + y = y + x)$ for $\forall x, y \in R$.
- $\forall x \exists y(x + y = 0)$ for $\forall x, y \in R$.
- $\forall x \forall y \forall z((x + y) + z = x + (y + z))$ for $\forall x, y, z \in R$.

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another. For example, $\forall x \exists y(x + y = 0)$. Note that everything within the scope of a quantifier can be thought of as a propositional function. $\forall x \exists y(x + y = 0)$ is the same thing as $\forall x Q(x)$, where $Q(x)$ is $\exists y P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Please translate following nested quantifiers into statements

- $\forall x \forall y(x + y = y + x)$ for $\forall x, y \in R$.
- $\forall x \exists y(x + y = 0)$ for $\forall x, y \in R$.
- $\forall x \forall y \forall z((x + y) + z = x + (y + z))$ for $\forall x, y, z \in R$.
- $\forall x \forall y((x > 0) \wedge (y > 0) \rightarrow (xy < 0))$ for $\forall x, y \in R$.

Nested quantifiers

Definition

Nested quantifiers is one quantifier within the scope of another. For example, $\forall x \exists y(x + y = 0)$. Note that everything within the scope of a quantifier can be thought of as a propositional function. $\forall x \exists y(x + y = 0)$ is the same thing as $\forall x Q(x)$, where $Q(x)$ is $\exists y P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Please translate following nested quantifiers into statements

- $\forall x \forall y(x + y = y + x)$ for $\forall x, y \in R$.
- $\forall x \exists y(x + y = 0)$ for $\forall x, y \in R$.
- $\forall x \forall y \forall z((x + y) + z = x + (y + z))$ for $\forall x, y, z \in R$.
- $\forall x \forall y((x > 0) \wedge (y > 0) \rightarrow (xy < 0))$ for $\forall x, y \in R$.
- $\forall \epsilon > 0 \exists \delta > 0 \forall x(0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)$.

Order of quantifiers

Order is important

It is important to note that the order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.

Order of quantifiers

Order is important

It is important to note that the order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.

Statement	When True?	When False?
$\forall x \forall y P(x,y)$ $\forall y \forall x P(x,y)$	$P(x,y)$ is true for every pair x, y	There is a pair x, y for which $P(x,y)$ is false
$\forall x \exists y P(x,y)$	For every x, there is a y for which $P(x,y)$ is true	There is an x such that $P(x,y)$ is false for $\forall y$
$\exists x \forall y P(x,y)$	There is an x for which $P(x,y)$ is true for every y	For every x, there is a y for which $P(x,y)$ is false
$\exists x \exists y P(x,y)$ $\exists y \exists x P(x,y)$	There is a pair x, y for which $P(x,y)$ is true	$P(x,y)$ is false for every pair x, y

Applications of nested quantifiers

Nested quantifiers translation

$$\forall x(C(x) \vee \exists y(C(y) \wedge F(x,y)))$$

- $C(x)$: x has a computer;
- $F(x,y)$: x and y are friends;
- Domain for both x and y consists of all students in your school.

Applications of nested quantifiers

Nested quantifiers translation

$$\forall x(C(x) \vee \exists y(C(y) \wedge F(x, y)))$$

- $C(x)$: x has a computer;
- $F(x, y)$: x and y are friends;
- Domain for both x and y consists of all students in your school.

Solution:

The statement says that for every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends.

Applications of nested quantifiers

Nested quantifiers translation

$$\forall x(C(x) \vee \exists y(C(y) \wedge F(x, y)))$$

- $C(x)$: x has a computer;
- $F(x, y)$: x and y are friends;
- Domain for both x and y consists of all students in your school.

Solution:

The statement says that for every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends.

That is, every student in your school has a computer or has a friend who has a computer.

Applications of nested quantifiers Cont'd

Sentence translation I

"If a person is female and is a parent, then she is someones mother".

Solution:

$\forall x((F(x) \wedge P(x)) \rightarrow \exists y M(x, y))$

- $F(x)$: x is female;
- $P(x)$: x is a parent;
- $M(x, y)$: x is the mother of y;

Applications of nested quantifiers Cont'd

Sentence translation I

"If a person is female and is a parent, then she is someones mother".

Solution:

$\forall x((F(x) \wedge P(x)) \rightarrow \exists y M(x, y))$

- $F(x)$: x is female;
- $P(x)$: x is a parent;
- $M(x, y)$: x is the mother of y;

Sentence translation II

"There is a woman who has taken a flight on every airline in the world".

Solution:

$\exists w \forall a \exists f(P(w, f) \wedge Q(f, a))$

- $P(w, f)$: w has taken f;
- $Q(f, a)$: f is a flight on a;

Or

$\exists w \forall a \exists f R(w, f, a)$

- $R(w, f, a)$: w has taken f on a.

Negation of nested quantifiers

Example

Use quantifiers to express the statement that "There does not exist a woman who has taken a flight on every airline in the world"

$$\neg \exists w \forall a \exists f (P(w, f) \land Q(f, a))$$

- $P(w, f)$: w has taken f;
- $Q(f, a)$: f is a flight on a;

Negation of nested quantifiers

Example

Use quantifiers to express the statement that "There does not exist a woman who has taken a flight on every airline in the world"

$$\neg\exists w \forall a \exists f (P(w,f) \wedge Q(f,a))$$

- $P(w,f)$: w has taken f;
- $Q(f,a)$: f is a flight on a;

$$\begin{aligned}
\neg\exists w \forall a \exists f (P(w,f) \wedge Q(f,a)) &\equiv \forall w \neg\forall a \exists f (P(w,f) \wedge Q(f,a)) \\
&\equiv \forall w \exists a \neg\exists f (P(w,f) \wedge Q(f,a)) \\
&\equiv \forall w \exists a \forall f \neg(P(w,f) \wedge Q(f,a)) \\
&\equiv \forall w \exists a \forall f (\neg P(w,f) \vee \neg Q(f,a))
\end{aligned}$$

Negation of nested quantifiers

Example

Use quantifiers to express the statement that "There does not exist a woman who has taken a flight on every airline in the world"

$$\neg\exists w \forall a \exists f (P(w, f) \land Q(f, a))$$

- $P(w, f)$: w has taken f;
- $Q(f, a)$: f is a flight on a;

$$\begin{aligned}
\neg\exists w \forall a \exists f (P(w, f) \land Q(f, a)) &\equiv \forall w \neg\forall a \exists f (P(w, f) \land Q(f, a)) \\
&\equiv \forall w \exists a \neg\exists f (P(w, f) \land Q(f, a)) \\
&\equiv \forall w \exists a \forall f \neg(P(w, f) \land Q(f, a)) \\
&\equiv \forall w \exists a \forall f (\neg P(w, f) \lor \neg Q(f, a))
\end{aligned}$$

"For every woman there is an airline such that for all flights, this woman has not taken that flight or that flight is not on this airline."

Take-aways

Conclusion

- Logic equivalences
- Propositional satisfiability
- Predicates
- Quantifiers
- Applications of predicates and quantifiers
- Nested quantifiers