Ideas of mathematical proof

Slides Week 24

Properties of logical operations. Links with set theory.
Tautology and contradiction. Proofs by contradiction.
Predicate calculus. Quantifiers.

Connectives for two statements P and Q:

conjunction $P \wedge Q$ true when both P and Q are true;

disjunction $P \vee Q$ true when P or Q is true, or both.

implication $P \Rightarrow Q$ is <u>defined</u> by the following truth table:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The implication $P \Rightarrow Q$ is not true only if P is true while Q is false.

Understanding implication

Note that $P \Rightarrow Q$ is true if P is false

whatever the value of Q:

"anything follows from a wrong statement".

This agrees with natural language:

"If condition A holds, then I will do B".

When condition A is false (does not hold),

and I do not do B, my statement is still true:

I keep my promise.

Example

Let $P(x)$ be "$x > 3$", and $Q(x)$ be "$x > 1$".

Surely, the implication $P(x) \Rightarrow Q(x)$ is always true!

For $x = 4$ we have both P and Q true.

For $x = 2$: P is false and Q is true.

For $x = 0$: $P(x)$ is false and $Q(x)$ is false.

Main thing: there are no x such that $P(x)$ is true but $Q(x)$ is false.

Necessary and sufficient conditions

Definition

In a theorem $P \Rightarrow Q$,

P is a **sufficient** condition for Q.

Or: Q holds **if** P holds.

Definition

In a theorem $P \Rightarrow Q$,

Q is a **necessary** condition for P.

Or: P holds **only if** Q holds.

Implication as a disjunction

Proposition

The statement $P \Rightarrow Q$

is logically equivalent to $\neg P \vee Q$;

in other words: $(P \Rightarrow Q) \equiv (\neg P \vee Q)$.

Proof. By truth table:

for all possible input values of P and Q,

check that the corresponding columns are the same.

Proof by truth table

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T			
T	F			
F	T			
F	F			

Proof by truth table

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T	T		
T	F	F		
F	T	T		
F	F	T		

Proof by truth table

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T	T	F	
T	F	F	F	
F	T	T	T	
F	F	T	T	

Proof by truth table

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Proof by truth table

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

We see the columns are the same,

hence, $(P \Rightarrow Q) \equiv (\neg P \vee Q)$. $\square$

Converse

Definition

The **converse** of a statement $P \Rightarrow Q$

is defined to be the statement $Q \Rightarrow P$.

Example

Let $P(x)$ be "$x > 3$", and let $Q(x)$ be "$x > 1$".

$P(x) \Rightarrow Q(x)$ is always true.

But $Q(x) \Rightarrow P(x)$ is not always true:

for $x = 2$, $Q(x)$ is true but $P(x)$ is false.

(Note: one counterexample is enough.)

Converse of Pythagoras Theorem

Example

Pythagoras Theorem: $P \Rightarrow Q$,

where for a triangle ABC,

P is "$\angle ACB = 90^\circ$" and Q is "$AC^2 + BC^2 = AB^2$".

The converse is $Q \Rightarrow P$, which is, in fact, also true:

if $AC^2 + BC^2 = AB^2$, then $\angle ACB = 90^\circ$.

Even if we prove the Pythagoras theorem itself,
the converse theorem still must be proved,
<u>it is not the same theorem</u>,
in many other cases the converse may not be true.

If and only if

Definition

We write $P \Leftrightarrow Q$ to abbreviate $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

The truth table is:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Necessary and sufficient condition

So $P \Leftrightarrow Q$ is true exactly when
the values of P and Q are the same,
either both true, or both false.

In a theorem $P \Leftrightarrow Q$,
"P is a **necessary and sufficient condition** for Q
(and vice versa)".

The same as "P holds **if and only if** Q holds".

Example

The statement $(\neg P) \Leftrightarrow (\neg Q)$

is logically equivalent to $P \Leftrightarrow Q$.

By the truth table (using truth values for $\Leftrightarrow$ as known):

P	Q	$P \Leftrightarrow Q$	$\neg P$	$\neg Q$	$\neg P \Leftrightarrow \neg Q$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

Truth values are the same, so $\neg P \Leftrightarrow \neg Q$ is logically equivalent to $P \Leftrightarrow Q$.

Example

The statement $(P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q)$

is logically equivalent to $P \Leftrightarrow Q$.

Proof by the truth table:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg P \Rightarrow \neg Q$	$(P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q)$
T	T	T	F	F	T	T
T	F	F	F	T	T	F
F	T	T	T	F	F	F
F	F	T	T	T	T	T

Truth values are the same, so $(P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q)$ is logically equivalent to $P \Leftrightarrow Q$. $\square$

Links from sets to logical statements

Recall:

Conjunction = (logical **and**) denoted by $P \wedge Q$.

Disjunction (logical **inclusive or**) denoted by $P \vee Q$.

Negation (logical **not**) denoted by $\neg P$.

Inmplication (logical **implies**) denoted by $P \Rightarrow Q$.

Links with set theory: union

Let A and B be sets.

Let $P =$ the statement "$x \in A$",

and $Q =$ "$x \in B$".

Clearly, then $P \vee Q$ means exactly $x \in A$ or $x \in B$,

that is, $x \in A \cup B$ by definition of union.

Links with set theory: intersection

Recall: A and B are sets, and

$P =$ the statement "$x \in A$",

and $Q =$ "$x \in B$".

$P \wedge Q$ means $x \in A$ and $x \in B$,

that is, $x \in A \cap B$ by definition of intersection.

Links with set theory: complement

Recall: A is a set, and

$P =$ the statement "$x \in A$".

$x \in \overline{A}$ means $x \notin A$,

that is, $x \in A$ false, that is, $\neg P$ is true.

Links with set theory: inclusion

Recall: A and B are sets, and

$P =$ the statement "$x \in A$",

and $Q =$ "$x \in B$".

$A \subseteq B$ means that $x \in A \Rightarrow x \in B$,

that is, $P \Rightarrow Q$.

Links with set theory: mnemonic rule

Thus, we have a ‘correspondence’:

$$\overline{} \quad \longleftrightarrow \quad \neg$$

$$\vee \quad \longleftrightarrow \quad \cup$$

$$\wedge \quad \longleftrightarrow \quad \cap$$

$$\Rightarrow \quad \longleftrightarrow \quad \subseteq$$

From logic to sets

Conversely, let $P(x)$ and $Q(x)$ be statements depending on some variable $x \in \mathscr{U}$.

Define the sets $A = \{x \in \mathscr{U} \mid P(x) \text{ is true}\}$ and $B = \{x \in \mathscr{U} \mid Q(x) \text{ is true}\}$.

Then the same correspondence holds:

$$A \cap B = \{x \in \mathscr{U} \mid P(x) \wedge Q(x) \text{ is true}\};$$

$$A \cup B = \{x \in \mathscr{U} \mid P(x) \vee Q(x) \text{ is true}\};$$

$$\overline{A} = \{x \in \mathscr{U} \mid \neg P(x) \text{ is true}\}.$$

Properties of logical operations

These are similar to the properties of operations on sets, having in mind the 'correspondence'

$$\overline{} \quad \longleftrightarrow \quad \neg\,; \qquad\qquad \vee \quad \longleftrightarrow \quad \cup\,; \qquad\qquad \wedge \quad \longleftrightarrow \quad \cap.$$

Namely, let P, Q, R be arbitrary statements.
Then the following hold:

1. Associativity:

   $$(P \vee Q) \vee R \equiv P \vee (Q \vee R) \qquad \text{and}$$

   $$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R).$$

2. Commutativity:

   $$P \vee Q \equiv Q \vee P \quad \text{and} \quad P \wedge Q \equiv Q \wedge P.$$

3. Distributivity:

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R) \text{ and}$$

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R).$$

4. De Morgan Laws:

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q \quad \text{and}$$

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q.$$

5. Double negation:

$$\neg(\neg P) \equiv P.$$

Proofs of laws by truth tables

All these logical equivalences can be easily proved by truth tables.

We have already proved one of the de Morgan laws in an example above.

Example

Prove (one of) the distributivity laws:

$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.

Fill the truth table giving all 8 possible combinations of inputs for P, Q, R:

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T				
T	T	F	T				
T	F	T	T				
T	F	F	F				
F	T	T	T				
F	T	F	T				
F	F	T	T				
F	F	F	F				

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T			
T	T	F	T	T			
T	F	T	T	T			
T	F	F	F	F			
F	T	T	T	F			
F	T	F	T	F			
F	F	T	T	F			
F	F	F	F	F			

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T		
T	T	F	T	T	T		
T	F	T	T	T	F		
T	F	F	F	F	F		
F	T	T	T	F	F		
F	T	F	T	F	F		
F	F	T	T	F	F		
F	F	F	F	F	F		

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	
T	T	F	T	T	T	F	
T	F	T	T	T	F	T	
T	F	F	F	F	F	F	
F	T	T	T	F	F	F	
F	T	F	T	F	F	F	
F	F	T	T	F	F	F	
F	F	F	F	F	F	F	

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

We see that the columns for $P \wedge (Q \vee R)$ and $(P \wedge Q) \vee (P \wedge R)$ are the same, as required,

so $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$. $\square$

Tautology statements

Definition

A compound logical statement is a **tautology** if its truth value is TRUE for any input values of constituents.

Example

$P \vee \neg P$ is clearly always true, no matter what the value of P is: P is true $\Rightarrow$ disjunction true, or P is false and then $\neg P$ is true $\Rightarrow$ disjunction true.

By truth table:

P	$\neg P$	$P \vee \neg P$
T	F	T
F	T	T

Only T in that column — so is a tautology.

Example

Prove that $(P \wedge Q) \Rightarrow (P \vee Q)$ is a tautology.

Proof by truth table:

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \Rightarrow (P \vee Q)$
T	T			
T	F			
F	T			
F	F			

Example

Prove that $(P \wedge Q) \Rightarrow (P \vee Q)$ is a tautology.

Proof by truth table:

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \Rightarrow (P \vee Q)$
T	T	T		
T	F	F		
F	T	F		
F	F	F		

Example

Prove that $(P \wedge Q) \Rightarrow (P \vee Q)$ is a tautology.

Proof by truth table:

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \Rightarrow (P \vee Q)$
T	T	T	T	
T	F	F	T	
F	T	F	T	
F	F	F	F	

Example

Prove that $(P \wedge Q) \Rightarrow (P \vee Q)$ is a tautology.

Proof by truth table:

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \Rightarrow (P \vee Q)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

Last column has T only, so this is a tautology. $\square$

Tautology properties

Notation

Any tautology is denoted by T.

Properties

$T \wedge P \equiv P$ for any statement P;

$T \vee P \equiv T$ for any statement P.

Proof. By truth table:

P	T	$T \wedge P$	$T \vee P$
T	T		
F	T		

Tautology properties

Notation

Any tautology is denoted by T.

Properties

$T \wedge P \equiv P$ for any statement P;

$T \vee P \equiv T$ for any statement P.

Proof. By truth table:

P	T	$T \wedge P$	$T \vee P$
T	T	T	
F	T	F	

Tautology properties

Notation

Any tautology is denoted by T.

Properties

$T \wedge P \equiv P$ for any statement P;

$T \vee P \equiv T$ for any statement P.

Proof. By truth table:

P	T	$T \wedge P$	$T \vee P$
T	T	T	T
F	T	F	T

We see that the columns are as required. $\square$

Contradiction statements

Definition

A compound statement that is always false,

for all input data, is called a **contradiction**.

Any such statement is denoted by F.

Example

$2 = 5$ is a contradiction, has truth value F.

Example

$(a > 5) \wedge (a^2 < 9)$ is a contradiction, $\equiv F$.

Example

$P \wedge \neg P \equiv F$ for any statement P:

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

This is a typical situation how contradiction appears in proofs by contradiction, as we shall see later.

Example

Prove that $(P \Rightarrow \neg Q) \wedge (P \wedge Q) \equiv F$

for any statements P, Q.

P	Q	$\neg Q$	$P \Rightarrow \neg Q$	$P \wedge Q$	$(P \Rightarrow \neg Q) \wedge (P \wedge Q)$
T	T				
T	F				
F	T				
F	F				

Example

Prove that $(P \Rightarrow \neg Q) \wedge (P \wedge Q) \equiv F$

for any statements P, Q.

P	Q	$\neg Q$	$P \Rightarrow \neg Q$	$P \wedge Q$	$(P \Rightarrow \neg Q) \wedge (P \wedge Q)$
T	T	F			
T	F	T			
F	T	F			
F	F	T			

Example

Prove that $(P \Rightarrow \neg Q) \wedge (P \wedge Q) \equiv F$

for any statements P, Q.

P	Q	$\neg Q$	$P \Rightarrow \neg Q$	$P \wedge Q$	$(P \Rightarrow \neg Q) \wedge (P \wedge Q)$
T	T	F	F		
T	F	T	T		
F	T	F	T		
F	F	T	T		

Example

Prove that $(P \Rightarrow \neg Q) \wedge (P \wedge Q) \equiv F$

for any statements P, Q.

P	Q	$\neg Q$	$P \Rightarrow \neg Q$	$P \wedge Q$	$(P \Rightarrow \neg Q) \wedge (P \wedge Q)$
T	T	F	F	T	
T	F	T	T	F	
F	T	F	T	F	
F	F	T	T	F	

Example

Prove that $(P \Rightarrow \neg Q) \wedge (P \wedge Q) \equiv F$

for any statements P, Q.

P	Q	$\neg Q$	$P \Rightarrow \neg Q$	$P \wedge Q$	$(P \Rightarrow \neg Q) \wedge (P \wedge Q)$
T	T	F	F	T	F
T	F	T	T	F	F
F	T	F	T	F	F
F	F	T	T	F	F

We see that the last column (for our statement) contains only F, so this is a contradiction. $\square$

Remark. Note that $F \Rightarrow P$ is a tautology for any P:

F	P	$F \Rightarrow P$
F	T	T
F	F	T

"Anything follows from a wrong statement"

Contradiction properties

Properties

1. $F \wedge P \equiv F$ for any statement P;
2. $F \vee P \equiv P$ for any statement P;
3. $\neg T \equiv F$;
4. $\neg F \equiv T$.

Proof: By truth table:

T	F	P	$F \wedge P$	$F \vee P$	$\neg T$	$\neg F$
T	F	T				
T	F	F				

Contradiction properties

Properties

1. $F \wedge P \equiv F$ for any statement P;
2. $F \vee P \equiv P$ for any statement P;
3. $\neg T \equiv F$;
4. $\neg F \equiv T$.

Proof: By truth table:

T	F	P	$F \wedge P$	$F \vee P$	$\neg T$	$\neg F$
T	F	T	F			
T	F	F	F			

Contradiction properties

Properties

1. $F \wedge P \equiv F$ for any statement P;
2. $F \vee P \equiv P$ for any statement P;
3. $\neg T \equiv F$;
4. $\neg F \equiv T$.

Proof: By truth table:

T	F	P	$F \wedge P$	$F \vee P$	$\neg T$	$\neg F$
T	F	T	F	T		
T	F	F	F	F		

Contradiction properties

Properties

1. $F \wedge P \equiv F$ for any statement P;
2. $F \vee P \equiv P$ for any statement P;
3. $\neg T \equiv F$;
4. $\neg F \equiv T$.

Proof: By truth table:

T	F	P	$F \wedge P$	$F \vee P$	$\neg T$	$\neg F$
T	F	T	F	T	F	
T	F	F	F	F	F	

Contradiction properties

Properties

1. $F \wedge P \equiv F$ for any statement P;
2. $F \vee P \equiv P$ for any statement P;
3. $\neg T \equiv F$;
4. $\neg F \equiv T$.

Proof: By truth table:

T	F	P	$F \wedge P$	$F \vee P$	$\neg T$	$\neg F$
T	F	T	F	T	F	T
T	F	F	F	F	F	T

We see that columns are as required. $\square$

Remark. In the analogy with sets:

$$\overline{} \quad \longleftrightarrow \quad \neg \, ; \qquad \cup \quad \longleftrightarrow \quad \vee \, ; \qquad \cap \quad \longleftrightarrow \quad \wedge$$

we can now add

$$\mathscr{U} \quad \longleftrightarrow \quad T \, ; \qquad \varnothing \quad \longleftrightarrow \quad F \, .$$

Simplifying logical expressions by using the properties.

This type of tasks are similar to those for expressions with sets.

Recap of the properties

Let P, Q, R be arbitrary statements. Then the following hold:

1. Associativity:

   $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ and

   $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$.

2. Commutativity:

   $P \vee Q \equiv Q \vee P$ and $P \wedge Q \equiv Q \wedge P$.

3. Distributivity:

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R) \quad \text{and}$$

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R).$$

4. De Morgan Laws:

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q \quad \text{and}$$

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q.$$

5. Double negation:

$$\neg(\neg P) \equiv P.$$

6. Tautology and contradiction laws:

$P \vee \neg P \equiv T \quad \text{and} \quad P \wedge \neg P \equiv F$
for any statement P;

$T \wedge P \equiv P \quad \text{and} \quad T \vee P \equiv T$
for any statement P;

$F \wedge P \equiv F \quad \text{and} \quad F \vee P \equiv P$
for any statement P;

$\neg T \equiv F \quad \text{and} \quad \neg F \equiv T.$

7. Implication law:

$$P \Rightarrow Q \equiv \neg P \vee Q.$$

8. Absorption laws:

$$P \vee (P \wedge Q) \equiv P;$$

$$P \wedge (P \vee Q) \equiv P.$$

9. Idempotent laws:

$$P \vee P \equiv P;$$

$$P \wedge P \equiv P.$$

Example

Simplify:

$$
\begin{aligned}
\neg((P \vee \neg Q) \wedge Q) &\equiv \neg(P \vee \neg Q) \vee \neg Q \quad \text{de Morgan} \\
&\equiv (\neg P \wedge \neg\neg Q) \vee \neg Q \quad \text{de Morgan} \\
&\equiv (\neg P \wedge Q) \vee \neg Q \quad \text{double negation} \\
&\equiv (\neg P \vee \neg Q) \wedge (Q \vee \neg Q) \quad \text{distributivity} \\
&\equiv (\neg P \vee \neg Q) \wedge T \quad \text{tautology law} \\
&\equiv \neg P \vee \neg Q \quad \text{tautology law}
\end{aligned}
$$

Example

Simplify:

$$
\begin{aligned}
P \wedge ((P \wedge Q) \vee \neg P) &\equiv (P \wedge P \wedge Q) \vee (P \wedge \neg P) \text{ distrib.} \\
&\equiv (P \wedge Q) \vee (P \wedge \neg P) \text{ idempotent} \\
&\equiv (P \wedge Q) \vee F \text{ contradiction law} \\
&\equiv P \wedge Q \text{ contradiction law}
\end{aligned}
$$

Proofs by contradiction

Proofs by contradiction are based on

Theorem

We have the logical equivalence $(\neg P \Rightarrow F) \equiv P$.

Proof: By truth table:

P	F	$\neg P$	$\neg P \Rightarrow F$
T	F	F	T
F	F	T	F

last column is the same as for P, as required. $\square$

This means: P is true exactly when $\neg P \Rightarrow F$ is true.

Proofs by contradiction

Hence, we have the following rule.

Proof by contradiction

To prove a statement P *is the same*

as to prove that $\neg P \Rightarrow F$,

i. e. that the negation causes (=implies, leads to)

a contradiction.

(Does not mean one has to always use proof by contradiction...)

Example

Suppose that k is an integer such that k^2 is even. Prove that k is even. (Let $P =$ "k is even".)

Proof. We "argue by contradiction": suppose $\neg P$: that is, k is not even, that is, $k = 2m + 1$ for an integer m.

Then $k^2 = (2m+1)^2 = 4m^2 + 4m + 1$
$= 2 \cdot (2m^2 + 2m) + 1$, which is odd.

This is a contradiction: we know that k^2 is even, and at the same time obtained that k^2 is odd.

This contradiction shows that our assumption (that k is not even) must be false, that is, k is even, as required. $\square$

Again: the scheme was: P meant "k is even".

We assumed $\neg P$: "k is odd".

Then we obtained a contradiction: $\cdots \Rightarrow Q \wedge \neg Q \equiv F$, where Q means "k^2 is even" (as given beforehand) and $\neg Q =$ "k^2 is odd".

So we have $\neg P \Rightarrow F$ is true, which means P is true.

Example

Prove that $\sqrt{2}$ is irrational, i. e., $\sqrt{2} \notin \mathbb{Q}$.

Proof by contradiction:

Suppose the negation ("the opposite"), that is, $\sqrt{2} \in \mathbb{Q}$, that is, $\sqrt{2} = m/n$ for $m, n \in \mathbb{Z}$.
We can choose a reduced fraction, so we assume that m/n is a reduced fraction, g.c.d.$(m, n) = 1$.

Square: $2 = m^2/n^2$; $2n^2 = m^2$ is even.
Then by preceding example, m is even: $m = 2k$.

Substitute: $2n^2 = (2k)^2 = 4k^2$; $n^2 = 2k^2$ is even.
Hence by preceding example, n is also even.

Thus, both m and n are even
– a contradiction with the fact that g.c.d.$(m, n) = 1$.

Thus, $\sqrt{2} \in \mathbb{Q}$ (negation) $\Rightarrow$ contradiction,

so the assertion $\sqrt{2} \notin \mathbb{Q}$ is true.

Or simply:

"...this contradiction proves the assertion." $\square$

Predicate calculus

Definition

A **predicate** is a (possibly compound) logical expression

$P(x)$ depending on a variable x

from some universal set $x \in \mathscr{U}$

called **universe of discourse**.

When we substitute a particular value for x,

the predicate becomes a statement,

which is either true or false.

Examples of predicates

Predicates are not statements!

become statements for values of variables substituted (or with quantifiers – later).

Example

Let $P(x)$ be $x > 2$, with $\mathscr{U} = \mathbb{R}$.

Then $P(3)$ is true, while $P(1)$ is false.

Example

Let $P(x)$ be "x is divisible by 3" and $\mathscr{U} = \mathbb{Z}$.

Then $P(12)$ is true, $P(17)$ is false,

and $P(3.5)$ makes no sense (since $3.5 \notin \mathscr{U}$).

Examples of predicates

Example

Let $P(x)$ be $x > 5$ and $Q(x)$ be $x^2 > 9$.

Consider the compound predicate $R(x) = P(x) \wedge Q(x)$.

Then $R(6)$ is true,

since both $P(6)$ and $Q(6)$ are true,

but $R(-4)$ is false:

$P(-4)$ is false and $Q(-4)$ is true,

conjunction is then false.

Examples of predicates

Example

Let $P(x)$ be $x > 4$ and $Q(x)$ be $x^2 > 16$.

Then $P(x) \Rightarrow Q(x)$ is always true, for all x.

Indeed, if $x > 4$, then $x^2 > 16$.

E.g. $x = 6$: $P(x)$ true and $Q(x)$ true.

For $x = 1$: $P(x)$ false and $Q(x)$ false.

For $x = -5$: $P(x)$ false and $Q(x)$ true.

(Note that when $P(x)$ is false,

the implication $P(x) \Rightarrow Q(x)$ is true regardless of $Q(x)$.)

Predicates in several variables

Example

Let $P(x, y)$ be $x^2 + y^2 = 1$, with $\mathscr{U} = \mathbb{R}$.

Then $P(1, 0)$ is true, while $P(1, 1)$ is false.

Example

Let $P(x, y)$ be $x > y$ and $Q(x)$ be $x < 2$.

Find truth value of $\neg(P(x, y) \wedge Q(x))$ for $x = 3$, $y = 1$.

Easy by truth table:

$P(3,1)$	$Q(3)$	$P(3,1) \wedge Q(3)$	$\neg(P(3,1) \wedge Q(3))$
T	F	F	T

Quantifiers

Universal quantifier.

Many statements in maths begin with

"For all x..",

or "For every x...",

or "For any x...",

or "For each x...", etc., ... (something holds true).

(which all mean the same).

Universal quantifier

Definition

Given a **predicate** with one variable $P(x)$ for $x \in \mathscr{U}$,

a **statement** $\forall x\, P(x)$ is formed: by definition,

$\forall x\, P(x)$ is true if $P(a)$ is true for all $a \in \mathscr{U}$.

The symbol $\forall$ is called the **universal quantifier**.

So $\forall x\, P(x)$ is false if it is not true for some $a \in \mathscr{U}$,

that is, false if there is at least one $a \in \mathscr{U}$

such that $P(a)$ is false.

Dependence on universe

Example

Let $P(x)$ be $(x+1)^2 > x^2$, and $\mathscr{U} = \mathbb{R}$.

Then $\forall x\, P(x)$ is false: for example, $P(-1)$ is false.

Different universe:

Example

Let $P(x)$ be $(x+1)^2 > x^2$ and $\mathscr{U} = \mathbb{N}$.

Then $\forall x\, P(x)$ is true:

since $(a+1)^2 = a^2 + 2a + 1 > a^2$

for any positive integer a.

Universal quantifier for several variables

Similar definitions for predicates with many variables: universal quantifiers can turn them into statements.

$\forall x \, \forall y \, R(x, y)$ is true if $\forall y \, R(x, y)$ is true for all x, which, for given $x = x_0$, is true if $R(x_0, y)$ is true for all y.

Clearly, this is the same as:

Definition

$\forall x \, \forall y \, R(x, y)$ is true if $R(x, y)$ is true for all x, y.

Example

Let $P(x,y)$ be $x^2 = y^2$

and $Q(x,y)$ be $x + y = 0$, with $x, y \in \mathscr{U} = \mathbb{R}$.

Prove that $\forall x\, \forall y\, (Q(x,y) \Rightarrow P(x,y))$ is true.

Indeed, whenever $a + b = 0$, we have $a = -b$, whence $a^2 = b^2$.

Example

Is $\forall x\, \forall y\, (P(x,y) \Rightarrow Q(x,y))$ true?

This is false: e.g. $x = 1$, $y = 1$.

Note that the universe of discourse can be defined differently for x, y.

In other words, it can be defined as 'universe of pairs' (x, y) involved in $P(x, y)$.

Example

Let the universe of discourse be $\mathbb{C} \times \mathbb{N}$,

Consider $\forall x \, \forall y \, (|x + y| \leq |x| + y)$.

True or false? True (special case of triangle inequality).

Existential quantifier

Definition

Given a **predicate** with one variable $P(x)$ for $x \in \mathscr{U}$,

a **statement** $\exists x\, P(x)$ is formed: by definition,

$\exists x\, P(x)$ is true if $P(a)$ is true for some $a \in \mathscr{U}$.

In other words,

$\exists x\, P(x)$ is true if there exists (at least one) $a \in \mathscr{U}$

such that $P(a)$ is true.

So it is false if there are no such $a \in \mathscr{U}$.

The symbol $\exists$ is called the **existential quantifier**.

Existence statements

$\exists x$ corresponds to: "There is x..", or "There exists x.."
usually followed by "such that...' (something holds);
Or simply "For some x . . . " (something holds).

Example

Let $P(x)$ be $(x-1)^2 > x^2$, and $\mathscr{U} = \mathbb{R}$.

Then $\exists x\, P(x)$ is true: for example, $P(0)$ is true.

Dependence on universe

Choice of the universe of discourse $\mathscr{U}$ is important.

Example

Let $P(x)$ be $x^2 = 2$ with $\mathscr{U} = \mathbb{R}$.

Then $\exists x\, P(x)$ is true: e.g. $(\sqrt{2})^2 = 2$.

The same statement with a different universe:

Example

Let $P(x)$ be $x^2 = 2$ with $\mathscr{U} = \mathbb{Q}$.

Then $\exists x\, P(x)$ is false,

as there is no rational square root of 2, as we know.

Existence with several variables

Definition

$\exists x\, \exists y\, P(x, y)$ is true if there exist $a, b \in \mathscr{U}$

such that $P(a, b)$ is true.

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\exists x\, \exists y\, ((x^2 > y^2) \wedge (x < y))$

is true: e.g. $x = -2$, $y = 1$.

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\exists x\, \exists y\, ((x > 2y^2) \wedge (x < 0))$

is false: no such pairs x, y.

Mixing different quantifiers

For predicates with many variables, universal and existential quantifiers can be mixed, to make them into statements.

Each quantifier always comes with a variable to which it refers.

The **order** in which they are placed **is important**.

Notation.

When a quantifier $\forall x$ or $\exists x$ is placed before a formula, it is applied to the whole formula on the right.

Extra brackets are not used: e.g. $\forall x (\exists y \, P(x, y))$ is written simply as $\forall x \, \exists y \, P(x, y)$.

Brackets with quantifiers

If we want a quantifier to be applied to a part of the formula, then brackets are used:

e.g. $(\forall x\, P(x)) \Rightarrow \exists x Q(x)$ means that

if $P(x)$ is true for all x,

then $Q(x)$ is true for some x.

Without brackets $\forall x\, P(x) \Rightarrow Q(x)$ the meaning is different: $P(x)$ implies $Q(x)$ for all x.

...But no harm in using brackets to avoid ambiguity: $\forall x\, (P(x) \Rightarrow Q(x))$.

Example

Let $P(x, y)$ mean "x likes y"

with x in the set of students of UoL,

and y in the set of songs by Beatles.

Then $\forall x \, \exists y \, P(x, y)$

means that every student likes some (at least one) song (may be different for different students).

For different order the meaning is quite different:

$\exists y \, \forall x \, P(x, y)$ means that

there is a song that is liked by all students.

As we already did, predicates given by formulae are often used without names (like $P(x, y)$).

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\exists x \, \forall y \, (x \neq y)$

is false: for any x take $y = x$;

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\forall x \, \exists y \, (x \neq y)$

is true: for any x take $y = x + 1$.

Equivalence of statements with quantifiers

Recall: two statements are logically equivalent

if they have the same truth values for all inputs.

The same for statements with quantifiers.

Negation and quantifiers

Two additional basic rules:

Theorem (Negation for quantified statements)

For any predicate $P(x)$,

(a) $\neg(\forall x\, P(x)) \equiv \exists x\, \neg P(x)$;

(b) $\neg(\exists x\, P(x)) \equiv \forall x\, \neg P(x)$.

(Mnemonic rule: "transfer/carry negation sign from left to right over quantifiers changing $\forall \leftrightarrow \exists$ until landing on unquantified statement".)

Proofs for negation with quantifiers

...follow directly from the definition of truth values for quantified statements.

Proof of $\neg(\forall x\, P(x)) \equiv \exists x\, \neg P(x)$

L.H.S. is true when $\forall x\, P(x)$ is false,

that is, it is false that $P(x)$ is true for all x,

that is, there is x_0 such that $P(x_0)$ is false,

that is, $\neg P(x_0)$ is true,

that is, there is x_0 such that $\neg P(x_0)$ is true,

which means R.H.S. is true.

Thus, L.H.S. is true exactly when R.H.S. is true.

Proofs for negation with quantifiers

Proof of $\neg(\exists x\, P(x)) \equiv \forall x\, \neg P(x)$**.**

L.H.S. is true when $\exists x\, P(x)$ is false,

that is, there is no x such that $P(x)$ is true,

that is, for all x we have $P(x)$ is false,

that is, $\neg P(x)$ is true for all x,

that is, $\forall x\, \neg P(x)$ is true,

which means R.H.S. is true.

Thus, L.H.S. is true exactly when R.H.S. is true. $\square$

Example

We saw that $\exists x\,(x^2 = 2)$ is false for $\mathscr{U} = \mathbb{Q}$.

Then the negation must be true:

$$\begin{aligned} \neg(\exists x\,(x^2 = 2)) &\equiv \forall x\,\neg(x^2 = 2) \\ &\equiv \forall x\,(x^2 \neq 2) \;\text{ is true} \end{aligned}$$

(That is, $x^2 \neq 2$ for any $x \in \mathbb{Q}$.)

Example

Let $P(x, y)$ mean "x likes y"
with x in the set of students of UoL,
and y in the set of songs by Beatles.

$\exists y \, \forall x \, P(x, y)$ means there is a song that is liked by all students.

What is the negation? By the above rules we transform:

$$\begin{aligned} \neg(\exists y \, \forall x \, P(x, y)) &\equiv \forall y \, \neg(\forall x \, P(x, y)) \\ &\equiv \forall y \, \exists x \, \neg P(x, y). \end{aligned}$$

In words: for every song there is a student who does not not like this song, precisely the negation: there is no song that is liked by all students.

More examples

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\forall x\, \forall y\, (x^2 + y^2 = (x+y)^2)$

is false: e.g. for $x = 1, y = 1$.

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\forall x\, \exists y\, (x^2 + y^2 = (x+y)^2)$

is true: e.g. for any x choose $y = 0$.

Example

Let $\mathscr{U} = \mathbb{R}$. Then $\exists x\, \forall y\, (x^2 + y^2 = (x+y)^2)$

is true: e.g. for $x = 0$.

Example

Let $\mathscr{U} = \mathscr{P}(\mathbb{R})$, the set of all subsets of $\mathbb{R}$.

Is

$$\forall X \, \forall Y \, \forall Z \;\; (X \cap Y) \cup Z = X \cap (Y \cup Z)$$

true or false?

It is false: as usual, just one example is enough to ruin a 'universal' statement:

e.g. take $X = \varnothing$, then r.h.s is empty,

and if $Z \neq \varnothing$, the l.h.s. is non-empty as it contains Z.

Say, $X = \varnothing$, $Y = \{1\}$, $Z = \{1\}$:

l.h.s. $\{1\} \quad \neq \quad$ r.h.s. $\varnothing$.