Logic

pondělí 9. září 2024 20:11

1. Logic

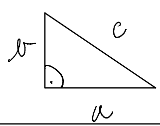
structure of mathematical reasoning:

assumption $\Longrightarrow$ conclusion

what we pay

what we get

Theorem (Pythagoras)



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

Theorem: For all $a, b \in \mathbb{R}$ we have

$$\frac{|a| + |b|}{2} \geq \sqrt{|a| \cdot |b|}$$

Literary style of mathematical text

- Theorem
- Proposition
- Lemma (technical)
- Corollary (consequence)
- Claim
- Fact
- Observation

importance

formally

$A \Rightarrow B$

$A \Leftrightarrow B$

1.1. Propositional logic

- informal definition:
  Proposition is a statement that is true or false
  " Sky is blue"

- In formal system proposition is a basic entity (like points, sets ...)
  What is more important are operations with propositions.

- If P is a proposition
  Thruth function

$$\mu(P) = \begin{cases} 0 & F \\ 1 & T \end{cases}$$

Basic logical operations
logical connectivness

NEGOTION : $\neg P$ truth table

P	$\neg P$
0	1
1	0

CONJUCTION

"P and Q"

$P \wedge Q$ truth table

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

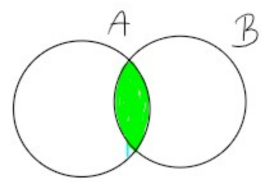
- $P \wedge Q$ is true exactly when both P and Q is true

- model

$P \equiv x \in A$

$Q \equiv x \in B$

$P \wedge Q \equiv x \in A \cap B$



DISJUNCTION

"P or Q"

$P \vee Q$

truth table

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

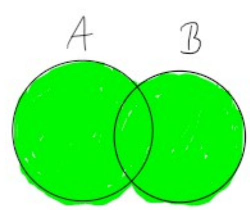
- $P \vee Q$ is true exactly when at least one statement is true

- model

$P \equiv x \in A$

$Q \equiv x \in B$

$P \vee Q \equiv x \in A \cup B$



IMPLICATION

$P \Rightarrow Q$

"P implies Q" ; "if P, then Q"

"Q if P" "P only if Q"

"P is sufficient for Q"

"Q is necessary for P"

truth table

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

- $P \Rightarrow Q$ is false exactly when P is true and Q is not true

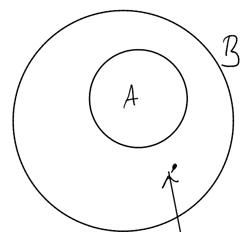
- model:

  $P \equiv x \in A$

  $Q \equiv x \in B$

  $P \Rightarrow Q \quad \equiv \quad A \subset B$

  (for all x)



- Comments:

  "false may imply truth"

  $5 = 3 \mid 0 \Rightarrow 0 \cdot 5 = 3 \cdot 0$

  $0 = 0$ ✓

- Slogan: $P \Rightarrow Q$

  P is a sufficient condition for Q

  Q is a necessary condition for P

- Example: "If I walk tomorrow, then there will be no rain"

  logical not casual consequence

  It is not true if "I walk" and "it is raining"

  rephrase: "I will walk only if it is not raining"

  "not raining" is necessary for walk

EQUIVALENCE

$P \Leftrightarrow Q$

"P is equivalent to Q"

"P if, and only if Q"

"P is sufficient and necessary for Q"

truth table

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

- $P \Leftrightarrow Q$ is true exactly when P and Q has the same truth value

- model

  $P \equiv x \in A$

  $Q \equiv x \in B$

  $P \Leftrightarrow Q$ corresponds to $A = B$
for all x

- Starting with a set of propositions $P_1, P_2, \ldots, P_n$ ≡ logical variables we built more complicated logical expressions (formulas).

We use ( ) for indication priority
negation has automatic priority.
Thruth value can be extended using tables of $\underbrace{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow}_{\text{basic}}$
in a consequtive way.

Formal definition

Definition Let A be a non-empty set whose elements will be called logical variables

We define propositional formulas as follows

- Any logical variable is a propositional formula
- If R and S are propositional formulas then $(\neg R)$, $(R \wedge S)$, $(R \vee S)$, $(R \Rightarrow S)$, $(R \Leftrightarrow S)$ are propositional formulas as well

A truth valuation is a function

$$u : A \to \{0,1\}.$$

It is extended to all formulas based on the tables above

More precisely, if R is a formula involving logical variables $p_1, p_2, \ldots, p_n$ then u is a map from the set of sequences of 0's and 1's into $\{0,1\}$.

Example $A = \{P, Q, R\}$

logical variables

$S = (P \Rightarrow Q) \vee (R \wedge P)$

computing truth table

order based on dyadic expansions

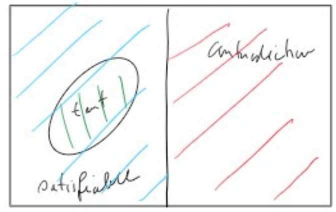
	P	Q	R	$P \Rightarrow Q$	$R \wedge P$	S
0	0	0	0	1	0	1
1	0	0	1	1	0	1
2	0	1	0	1	0	1
3	0	1	1	1	0	1
4	1	0	0	0	0	0
5	1	0	1	0	1	1
6	1	1	0	1	0	1
7	1	1	1	1	1	1

Definition Formula R is called tautology if its truth function is constant one.

In symbols: $\models R$

Formula R is satisfiable if its truth function is not constant 0

Formula R is a contradiction if its truth function is constant zero



- Observe: $\models R \Leftrightarrow \neg R$ is a contradiction

---

<u>Example</u>: $\models P \vee \neg P$

$P \wedge \neg P$ is a contradiction

<u>Definition</u> Two formulas (on the same set of logical variables) R and S are **tautologically equivalent** if $\models (R \Leftrightarrow S)$.

(i.e. R and S has same truth function)

In symbols: $R \dashv\vDash S$

<u>Example</u> $(P \Rightarrow Q) \vee (R \wedge P) \dashv\vDash \neg P \vee Q \vee R$

$\downarrow$

this is false if and only if

$u(P) = 0$

$u(Q) = 1$

$u(R) = 1$

and see example above.

Some important tautologies

- de Morgan law

$\neg(P \vee Q) \dashv\vDash \neg P \wedge \neg Q$

$\neg(P \wedge Q) \dashv\vDash \neg P \vee \neg Q$

- <u>distributivity law</u>

$(P \vee Q) \wedge R \dashv\vDash (P \wedge R) \vee (Q \wedge R)$

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

- $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ contraposition

- transitivity of $\Rightarrow$
  $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow P \Rightarrow R$ (tautology)

---

contraposition :

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Fact

$$\boxed{P \Rightarrow Q \equiv \neg P \vee Q}$$

LHS : false if and only if

P	Q
1	0

RHS : false if and only if

$\neg P$	Q
0	0

Exercise: Using basic rules express $\neg(P \Rightarrow Q)$ in terms of $\neg, \wedge, \vee$

Solution : $P \Rightarrow Q \equiv \neg P \vee Q$

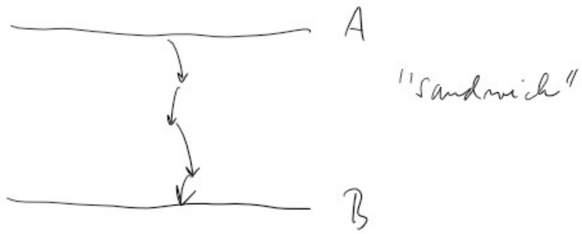
$\downarrow$ de Morgan

$\neg(P \Rightarrow Q) \equiv \neg(\neg P \vee Q) = P \wedge \neg Q$

1.2. Techniques of proofs

How to prove
$$A \Rightarrow B$$

- **direct proof** ... chain of implications



Theorem If x is an odd integer then $x+5$ is even.

Proof $x = 2k+1$, where k is an integer

$$x+5 = 2k+1+5 = 2k+6 = \underbrace{2(k+3)}_{\text{even}}$$

- **Proof by counterpositive**

we are proving
$$\neg B \Rightarrow \neg A \quad \text{(by direct proof)}$$

Theorem If the sum of two integers is even, then they have the same parity.

Proof We prove

x and y have different parities

$\Downarrow$

$x+y$ is odd

Suppose **WLOG = without loss of generality**

that $x = 2k+1$

$y = 2l$

for k, l integers

Then $x+y = 2k+1+2l = 2(k+l)+1$
$\downarrow$
this is odd

- **Proof by contradiction**

$$\left.\begin{array}{l} A \text{ holds} \\ \neg B \text{ holds} \end{array}\right\} \Rightarrow \text{contradiction}$$

Based on $\neg(A \Rightarrow B) \vdash A \wedge B^{\perp}$

<u>Theorem</u>: Let a, b be real numbers
Then $ab = 0 \Rightarrow a = 0$ or $b = 0$.

<u>Proof</u>: By contradiction. Suppose $ab = 0$
and $a \neq 0 \wedge b \neq 0$.

Then $ab = 0 \,/\, \frac{1}{a}$
$\Downarrow$
$b = 0$ contradiction

- **Proof by induction**

$\mathbb{N}$ - set of positive integers
$= \{1, 2, 3, \dots\}$

$P(n)$ is some property depending on n

$$\left.\begin{array}{l} \cdot\ P(1) \text{ holds} \\ \cdot\ P(n) \Rightarrow P(n+1) \\ \quad \text{holds for all } n \end{array}\right\} \Rightarrow P(n) \text{ holds for all } n$$

<u>Exercise</u> Prove that any polynomial of degree n has at most n roots

polynomial of degree n: $p_n(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n$
$a_0, a_1, \dots a_n$ - real numbers
$a_0 \neq 0$

- $n=1$: $p(x) = a_0 x + a_1 \quad a_0 \neq 0$
  the root is just one : $x_0 = -\frac{a_1}{a_0}$

$P(1)$ ✓

- $P(n) \Rightarrow P(n+1)$

Suppose that each polynomial of degree $n > 0$ has at most n roots

Take polynomial $p_{n+1}(x)$ of degree $n+1$

If it has no root then $P(n+1)$ holds for p_{n+1}

Suppose $p_{n+1}(x)$ has a root α

Then algebra says

$$p_{n+1}(x) = (x-\alpha) \underbrace{q_n(x)}_{\text{polynomial of degree } n}$$

$q_n(x)$ has at most n roots

If $p_{n+1}(\beta) = 0$ → $\beta = \alpha$ / → β is a root of $q_n(x)$ } see exercise above

So $p_{n+1}(x)$ has at most $n+1$ roots

---

1. 3. Quantifiers

a propositional function is a proposition depending on some variable

$\forall$ ≡ for all ≡ universal quantifier

$\boxed{\forall x \ P(x)}$ ≡ for all x $P(x)$ holds

Example: $\forall$ real number x $x^2+1 \neq 0$

$\exists$ ≡ there exists ≡ existencial quantifier

$\exists$ ≡ there exists ≡ existencial quantifier
(at least one)

$\boxed{\exists x \ P(x)}$ ≡ there exists x such that $P(x)$ holds

Example There exists a real number x such that $x^2 = 5$

- Often more variables are involved
$\forall x, y \in \mathbb{R} \quad x^2 + y^2 \geq 0$

How to negate $\forall$ and $\exists$?

$$\boxed{\begin{array}{l} \forall x \ P(x) \xrightarrow{\text{negation}} \exists x \ \neg P(x) \\ \exists x \ P(x) \xrightarrow{\text{negation}} \forall x \ \neg P(x) \end{array}}$$

Example: Every polynomial (with real coefficient) of degree at least 1 has a root

$\downarrow$ negation

There is a real polynomial $p(x)$ such that $p(x) \neq 0$ for all $x \in \mathbb{R}$

Usually we have two or more quantifiers

- $\lim\limits_{n \to \infty} x_n = x$
$\equiv \forall \varepsilon > 0 \ \exists n_0 \ \forall n \geq n_0 \quad |x_n - x| < \varepsilon$

- $\lim\limits_{n\to\infty} x_n = x$

$$\equiv \forall \varepsilon>0\ \exists n_0\ \forall n\geq n_0\ |x_n - x|<\varepsilon$$

depends

- x is not a limit of $(x_n)_{n=1}^{\infty}$:

$$\exists \varepsilon_0>0\ \forall n_0\ \exists n\geq n_0\ |x_n-x|\geq\varepsilon_0$$

- Order of quantifiers matters

$\forall x\in\mathbb{R}\setminus\{0\}\ \exists y\in\mathbb{R}\ xy=1$ (true $y=\frac{1}{x}$)

$\exists y\in\mathbb{R}\ \forall x\in\mathbb{R}\setminus\{0\}\ xy=1$ (not true
$\nexists$ $xy=1$
$\Rightarrow (2x)y=2$)
