Matematické důkazy

Struktura matematiky a typy důkazů

Petr Liška

Masarykova univerzita

18.9.2014

Motto:

Matematika je tvořena z 50 procent formulemi, z 50 procent důkazy a z 50 procent představivostí.

Euklidovská geometrie

Jedná se (nejspíše) o první ucelený systém matematické teorie (viz *Základy*, asi 300 př.n.l.; Eukleides, asi 325–260 př.n.l).
Byla založena na 5 postulátech:

1) každé dva různé body spojuje jediná přímka
2) každou úsečku lze prodloužit na přímku
3) lze sestrojit kružnici s libovolným poloměrem a se středem v libovolném bodě
4) všechny pravé úhly jsou shodné
5) jestliže přímka p protíná další přímky q, r a vytváří s nimi na své jedné straně vnitřní úhly, jejichž součet je menší dva úhly pravé, pak se na této straně přímky p přímky q, r protínají.

Na základě těchto postulátů lze logicky odvodit celou řadu známých tvrzení.
Jsou všechny axiomy nutné?

Motto:

Nejkrásnější chvíle v životě matematika jsou ty po dokončení důkazu, avšak předtím než objeví chybu.

Struktura matematic- kého textu

- axióm
  - definice
    - věta
    - tvrzení
    - lemma
    - důsledek

    } důkaz
    - poznámka
    - příklad

Axiom

matematický výrok, který je považován za pravdivý a nedokazuje se (v matematice též *postulát*, v řecké matematice se tyto pojmy rozlišovaly)

Věta

pravdivý (netriviální) výrok, který je odvozen na základě axiomů, definic a dříve dokázaných vět (slabší výroky: tvrzení, lemma, důsledek, . . .)

Důkaz

posloupnost "formulí" taková, že každý člen této posloupnosti je buď *axiomem* nebo *tautologií*
Tautologie: vždy pravdivý složený výrok ($P \Leftrightarrow P$; $P \vee \neg P$; $\neg\neg P \Leftrightarrow P$)
Kontradikce (oxymóron): vždy nepravdivý složený výrok (kulatý čtverec; Karel Hynek Mácha /Máj/: "Mrtvé milenky cit, zbortěné harfy tón.")

Tvary matematických vět

- *obecná věta* „$\forall x \in M : V(x)$“
- *existenční věta* „$\exists x \in M : V(x)$“ (příp. „$\exists! \, x \in M : V(x)$“)
- *implikace* „$\forall x \in M : A(x) \Rightarrow B(x)$“ ($A$...předpoklad, B...závěr; A...nutná podmínka, B...postačující podmínka)
- *ekvivalence* „$A(x) \Leftrightarrow B(x)$“ neboli „$A(x) \Rightarrow B(x) \wedge A(x) \Leftarrow B(x)$“ (často věty typu: „Jestliže platí P, pak tvrzení $A_1, A_2, \ldots A_n$ jsou ekvivalentní“; důkaz obvykle $A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_n \Rightarrow A_1$, přičemž nezáleží na pořadí)

Metody matematických důkazů

- *přímý důkaz* (T.: $A \Rightarrow B$. D.: $A \Rightarrow A_1 \Rightarrow \cdots \Rightarrow B$)
- *nepřímý důkaz*
  - *obměna* (kontrapozice): $A \Rightarrow B \iff \neg B \Rightarrow \neg A$
  - *spor*: $A \Rightarrow B \iff \neg(A \wedge \neg B)$
- matematická indukce

Přímý důkaz

Přímý důkaz

Důkaz tvrzení $A \Rightarrow B$ pomocí posloupnosti přijatých axiomů a/nebo vět ve tvaru

$$A_i \Rightarrow A_{i+1}, \quad i = 0, \ldots, n,$$

kde $A_0 = A$ a $A_{n+1} = B$, tj.

$$A = A_0 \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow A_n \Rightarrow A_{n+1} = B.$$

Je tedy potřeba najít „jednodušší tvrzení“ (mezikroky). Taková metoda uvažování se nazývá *deduktivní*.

Příklad

Věta: Nechť $m \in \mathbb{Z}$ je sudé a $p \in \mathbb{Z}$. Potom součin $mp \in \mathbb{Z}$ je sudé číslo.

Příklad

Věta: Pro každé $n \in \mathbb{N}$ platí

$$\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}.$$

Příklad

Dokažte, že v každém čtverci s rozměry $10 \times 10\,\text{cm}$, kde je zakresleno 101 různých bodů, existuje trojúhelník o obsahu $1\,\text{cm}^2$, který obsahuje alespoň dva z daných bodů.

Nepřímý důkaz

$A \Rightarrow B$

- obrácená (opačná) implikace
- obměněná implikace (kontrapozice)

Opačné tvrzení

Uvažujme tvrzení $P: \ A \Rightarrow B$ (tj.: jestliže platí předpoklad A, pak je splněn závěr B). *Opačné tvrzení* k P je výrok $B \Rightarrow A$, které zaměňuje předpoklad a závěr tvrzení.

Příklad

Zcela přirozeně platí, že, je-li tvrzení P pravdivé, pak opačný výrok *nemusí* být splněn. Např.:
A: studuji na ESF MU (n je prvočíslo větší než 2)
B: mám přístup do IS MU (n je liché číslo)
Pak tvrzení $A \Rightarrow B$ je pravdivé, ale opačné tvrzení $B \Rightarrow A$ již pravdivé být nemusí.

Nepřímý důkaz

Ekvivalence

Jestliže tvrzení $A \Rightarrow B$ i opačné tvrzení $B \Rightarrow A$ jsou obě pravdivá, řekneme, že A platí *tehdy a jen tehdy, když* (právě tehdy, když) platí B (nebo „A je ekvivalentní B“), a píšeme $A \Leftrightarrow B$.

Příklad

A: n je sudé prvočíslo
B: $n = 2$

Příklad

Dokažte, že číslo $n \in \mathbb{N}$ je sudé právě tehdy, když číslo n^2 je sudé.

Nepřímý důkaz

Obměna

Tvrzení $\neg B \Rightarrow \neg A$ se nazývá *obměnou* (též kontrapozicí) tvrzení $A \Rightarrow B$.

Z výrokové logiky plyne, že $(A \Rightarrow B) \iff (\neg B \Rightarrow \neg A)$

Příklad

Tvrzení: Jestliže mám uspět u zkoušky z mikroekonomie, věnuji svoji pozornost i matematice.

Obměna: Jestliže nevěnuji svoji pozornost i matematice, neuspěji u zkoušky z mikroekonomie.

Příklad

Jestliže $p \in \mathbb{N}$ je prvočíslo větší než 2, pak p je liché.

Příklad

Pro libovolné prvočíslo p platí: $p \mid n^2 \Rightarrow p \mid n$.

Nepřímý důkaz

Spor

Obměnou jsme ukázali, že tvrzení $A \Rightarrow B$ je platné právě tehdy, když tvrzení $\neg B \Rightarrow \neg A$ je platné. Tuto myšlenku můžeme rozšířit:pravdivost závěru B můžeme potvrdit tak, že budeme uvažovat všechny alternativy k B. Pokud všechna taková tvrzení povedou ke sporu se základními axiomy nebo známými tvrzeními, musí být závěr B pravdivý. Takovému způsobu se říká *důkaz sporem* (reductio ad absurdum). Chceme vlastně ukázat, že neplatí $A \wedge \neg B$ (tj. $A \Rightarrow B \Longleftrightarrow \neg(A \wedge \neg B)$).

Příklad

Neexistuje nejmenší kladné racionální číslo.

Příklad

Číslo $\sqrt{2}$ je iracionální.

Příklad

Jestliže číslo p je prvočíslo větší než 2, pak číslo p je liché.

Matematická indukce

Motivace

Uvažujme skupinu 100 mužů seřazených za sebou do řady. Každý zašeptá své jméno muži za sebou, přičemž my víme pouze dvě věci:

$(*)$ první muž v řadě se jmenuje David

$(+)$ přímo za každým mužem, který se jmenuje David, stojí jiný muž se jménem David.

Z toho můžeme vyvodit, že všichni muži mají jméno David. Proč?

Dle $(*)$ víme, že první muž je David $\overset{(+)}{\Longrightarrow}$ za ním stojí také David $\overset{(+)}{\Longrightarrow} \ldots \overset{(+)}{\Longrightarrow}$ poslední muž v řade je David.

I kdyby byl počet mužů v řadě nekonečný a výroky $(*)$, $(+)$ by byly pravdivé, mohli bychom stále tvrdit, že všichni muži se jmenují David.

Matematická indukce

Jak to funguje?

Uvažujme řadu výroků očíslovanou přirozenými čísly tak, že první tvrzení je $P(1)$, druhé tvrzení je $P(2)$, ..., n-té tvrzení je $P(n)$. Předpokládejme, že o těchto výrocích můžeme dokázat:

1) výrok $P(1)$ je splněn (tzv. *báze* nebo *základ indukce*)
2) kdykoli je platné tvrzení $P(k)$ pro nějaké $k \in \mathbb{N}$ (tzv. *indukční předpoklad*), pak platí také $P(k+1)$ (tzv. *indukční krok*).

   Chceme vlastně ukázat, že z platnosti výroků $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ plyne $P(k+1)$

Potom můžeme snadno dospět k závěru, že všechna tvrzení jsou pravdivá.

Matematická indukce

Příklad

Pro $n \in \mathbb{N}$ platí: $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Příklad

Součet prvních n lichých přirozených čísel je n^2, tj.

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Příklad

Pro každé $n \geq 1$ je při současném hodu n kostkami stejná pravděpodobnost toho, že výsledný součet bude sudý nebo lichý.

Příklad

Každé přirozené číslo větší než 1 může být vyjádřeno jako součin prvočísel.

Příklad

V každém stádu o $n \geq 1$ koních mají všichni koně stejnou barvu.