

## 2 Důkazové techniky, Indukce

Náš hlubší úvod do matematických formalismů pro informatiku začneme základním přehledem technik matematických důkazů. Z nich pro nás asi nejdůležitější je technika důkazů *matematickou indukcí*, která je svou podstatou velmi blízká počítačovým programům (jako iterace cyklů).



### Stručný přehled lekce

- \* Základní důkazové techniky: přímé, nepřímé a sporem. Důkazy „tehdy a jen tehdy“.
- \* Důkazy matematickou indukcí, jejich variace a úskalí.
- \* Metody zesílení tvrzení a rozšíření základu v indukci.

## 2.1 Přehled základních důkazových technik

- *Přímé odvození*. To je způsob, o kterém jsme se dosud bavili. □

- *Kontrapozice* (také *obrácením* či *nepřímý důkaz*). Místo věty

„Jestliže platí **předpoklady**, pak platí **závěr**.“

budeme dokazovat ekvivalentní větu

„Jestliže neplatí **závěr**, pak neplatí alespoň jeden z **předpokladů**.“ □

- *Důkaz sporem*. Místo věty

„Jestliže platí **předpoklady**, pak platí **závěr**.“

budeme dokazovat větu

„Jestliže platí **předpoklady** a platí **opak závěru**, pak platí...“

- nějaké **zjevně nepravdivé tvrzení**, nebo případně
- **závěr** (tj. opak jeho opaku) či opak jednoho z předpokladů. □

- *Matematická indukce*. Pokročilá technika. . .

## Příklad důkazu kontrapozicí

**Definice:** *Prvočíslo* je celé číslo  $p > 1$ , které nemá jiné dělitele než 1 a  $p$ .

**Příklad 2.1.** *Na důkaz kontrapozicí (obrácením).*

**Věta.** *Jestliže  $p$  je prvočíslo větší než 2, pak  $p$  je liché.* □

**Důkaz *obráceného tvrzení:*** Budeme místo uvedeného znění věty dokazovat, že je-li  $p$  sudé, pak  $p$  není větší než 2 nebo  $p$  není prvočíslo.

Připomínáme, že podle definice je  $p$  sudé, právě když lze psát  $p = 2 \cdot k$ , kde  $k$  je celé. Jsou jen dvě snadno řešitelné možnosti:

- $k \leq 1$ . Pak  $p = 2k$  není větší než 2.
- $k > 1$ . Pak  $p = 2 \cdot k$  není prvočíslo podle definice.

□

## Příklady důkazu sporem

**Příklad 2.2.** *Jiný, kratší přístup k Důkazu 2.1.*

**Věta.** *Jestliže  $p$  je prvočíslo větší než 2, pak  $p$  je liché.* □

**Důkaz sporem:** Necht' tedy  $p$  je prvočíslo větší než 2, které je sudé. Pak  $p = 2 \cdot k$  pro nějaké  $k > 1$ , tedy  $p$  není prvočíslo, **spor** (s předpokladem, že  $p$  je prvočíslo). □

**Příklad 2.3.** *Opět sporem.*

**Věta.** *Číslo  $\sqrt{2}$  není racionální.* □

**Důkaz sporem:** Necht' tedy  $\sqrt{2}$  je racionální, tj. necht' existují nesoudělná celá kladná čísla  $r, s$  taková, že  $\sqrt{2} = r/s$ . □

- Pak  $2 = r^2/s^2$ , tedy  $r^2 = 2 \cdot s^2$ , proto  $r^2$  je dělitelné dvěma. Z toho plyne, že i  $r$  je dělitelné dvěma (proč?). □
- Jelikož  $r$  je dělitelné dvěma, je  $r^2$  dělitelné dokonce čtyřmi, tedy  $r^2 = 4 \cdot m$  pro nějaké  $m$ . Pak ale také  $4 \cdot m = 2 \cdot s^2$ , tedy  $2 \cdot m = s^2$  a proto  $s^2$  je dělitelné dvěma. □
- Z toho plyne, že  $s$  je také dělitelné dvěma. Celkem dostáváme, že  $r$  i  $s$  jsou dělitelné dvěma, jsou tedy soudělná a to je **spor**. □

„Nevíte-li, jak nějakou větu dokázat, zkuste důkaz sporem. . . “

## 2.2 Věty typu „tehdy a jen tehdy“

- Uvažujme nyní (v matematice poměrně hojně) věty tvaru  
„Nechť platí předpoklady P. Pak tvrzení A platí *tehdy a jen tehdy*,  
platí-li tvrzení B.“□
- Příklady jiných jazykových formulací téže věty jsou:
  - \* Za předpokladů P je tvrzení B *nutnou a postačující* podmínkou pro platnost tvrzení A.□
  - \* Za předpokladů P je tvrzení A nutnou a postačující podmínkou pro platnost tvrzení B.□
  - \* Nechť platí předpoklady P. Pak tvrzení A platí *právě tehdy* když platí tvrzení B.□
- **Plný důkaz** vět tohoto tvaru má vždy **dvě části(!)**. Je třeba dokázat:
  - \* Jestliže platí předpoklady P a tvrzení A, pak platí tvrzení B.
  - \* Jestliže platí předpoklady P a tvrzení B, pak platí tvrzení A.

### Příklad 2.4. Na důkaz typu „tehdy a jen tehdy“.

**Věta.** Pro každá dvě celá č.  $a, b$  platí, že  $a < b$  právě tehdy, když  $2^a < 2^b$ .

□

**Důkaz:** Nezapomínáme, že našim úkolem je dokázat oba směry tvrzení (implikace zleva doprava a zprava doleva). Začneme s prvním: Předpoklad  $a < b$  je definičně ekvivalentní tomu, že  $b = a + k$  pro nějaké přirozené  $k > 0$ . Potom  $2^b = 2^{a+k} = 2^a \cdot 2^k = \ell \cdot 2^a$  pro nějaké přirozené  $\ell = 2^k \geq 2$ , a tudíž

$$2^b - 2^a = (\ell - 1) \cdot 2^a \geq 1 \cdot 2^a > 0.$$

Tím je první část důkazu hotova. □

V opačném směru postupujeme z předpokladu  $2^a < 2^b$ . Vydělením obou stran nerovnosti kladným číslem  $2^a$  získáme

$$2^b / 2^a = 2^{b-a} > 1. \square$$

Dále postupujeme sporem. Nechť tedy  $a \geq b$ , neboli  $a - b = m \geq 0$ . Potom máme  $2^{a-b} = \underbrace{2 \cdot \dots \cdot 2}_{m \times} \geq 1$ . Avšak celkově  $1 = 2^0 = 2^{a-b} \cdot 2^{b-a} > 1 \cdot 1 = 1$  je

sporné. Proto zbývá jen požadovaný závěr  $a < b$ . □

## 2.3 Matematická indukce

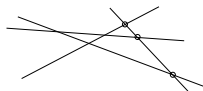
- Jde o důkazovou techniku aplikovatelnou na tvrzení tohoto typu:

„Pro každé přirozené (celé)  $n \geq k_0$  platí  $T(n)$ .“

Zde  $k_0$  je nějaké pevné přir. číslo a  $T(n)$  je tvrzení parametrizované čís.  $n$ . □

Příkladem je třeba tvrzení:

Pro každé  $n \geq 0$  platí, že  $n$  přímek dělí rovinu nejvýše na  $\frac{1}{2}n(n+1) + 1$  oblastí. □



- **Princip matematické indukce** říká (coby axiom), že k důkazu věty

„Pro každé přirozené (celé)  $n \geq k_0$  platí  $T(n)$ .“

stačí ověřit platnost těchto dvou tvrzení:

- \*  $T(k_0)$  (tzv. **báze** neboli základ indukce)
- \* Pro každé  $n \geq k_0$ ; jestliže platí  $T(n)$ , (indukční předpoklad)  
pak platí také  $T(n+1)$ . (indukční krok) □

## Příklady důkazů indukcí

**Příklad 2.6.** *Velmi jednoduchá a přímočará indukce.*

**Věta.** *Pro každé přiroz.  $n \geq 1$  je stejná pravděpodobnost, že při současném hodu  $n$  kostkami bude výsledný součet sudý, jako, že bude lichý.  $\square$*

**Důkaz:** *Základ indukce* je zde zřejmý: Na jedné kostce (pochvě!) jsou tři lichá a tři sudá čísla, takže obě skupiny padají se stejnou pravděpodobností.  $\square$

*Indukční krok* pro  $n \geq 1$ : Necht'  $p_n^s$  pravděpodobnost, že při hodu  $n$  kostkami bude výsledný součet sudý, a  $p_n^l$  je pravděpodobnost lichého. Podle indukčního předpokladu je

$$p_n^s = p_n^l = \frac{1}{2}.$$

$\square$

Hoďme navíc  $(n + 1)$ -ní kostkou. Podle toho, zda na ní padne liché nebo sudé číslo, je pravděpodobnost celkového sudého součtu rovna

$$\frac{3}{6}p_n^l + \frac{3}{6}p_n^s = \frac{1}{2}$$

a stejně pro pravděpodobnost celkového lichého součtu.  $\square$

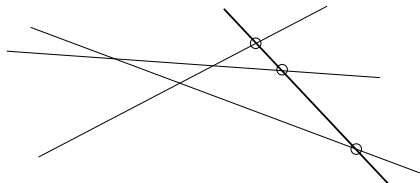


**Příklad 2.7.** Ukázka skutečné důkazové „síly“ principu matematické indukce.

**Věta.** Pro každé  $n \geq 0$  platí, že  $n$  přímek dělí rovinu nejvýše na

$$\frac{1}{2}n(n+1) + 1$$

oblastí.



**Důkaz:** □ Pro bázi indukce stačí, že 0 přímek dělí rovinu na jednu část. (Všimněte si také, že 1 přímka dělí rovinu na dvě části, jen pro lepší pochopení důkazu.)

Mějme nyní rovinu rozdělenou  $n$  přímkami na nejvýše  $\frac{1}{2}n(n+1) + 1$  částí. □ Další,  $(n+1)$ -ní přímka je rozdělena průsečíky s předchozími přímkami na nejvýše  $n+1$  úseků a každý z nich oddělí novou část roviny. □ Celkem tedy bude rovina rozdělena našimi přímkami na nejvýše tento počet oblastí:

$$\frac{1}{2}n(n+1) + 1 + (n+1) = \frac{1}{2}n(n+1) + \frac{1}{2} \cdot 2(n+1) + 1 = \frac{1}{2}(n+1)(n+2) + 1$$

□

## Příklad 2.8. Další indukční důkaz rozepsaný v podrobných krocích.

**Věta.** Pro každé  $n \geq 0$  platí  $\sum_{j=0}^n j = \frac{n(n+1)}{2}$ .  $\square$

**Důkaz indukcí** vzhledem k  $n$ .

- **Báze:** Zde musíme dokázat „ $T(0)$ “, což je v tomto případě rovnost  $\sum_{j=0}^0 j = \frac{0(0+1)}{2}$ . Tato rovnost (zjevně) platí.  $\square$
- **Indukční krok:** Musíme dokázat, že pro každé  $n \geq 0$  platí „z  $T(n)$  vyplývá  $T(n+1)$ “, což je konkrétně následující tvrzení:

Jestliže  $\sum_{j=0}^n j = \frac{n(n+1)}{2}$ , pak platí  $\sum_{j=0}^{n+1} j = \frac{(n+1)(n+1+1)}{2}$ .  $\square$

**Předpokládejme** tedy, že  $\sum_{j=0}^n j = \frac{n(n+1)}{2}$  a pokusme se dokázat, že pak také

$\sum_{j=0}^{n+1} j = \frac{(n+1)(n+1+1)}{2} = \frac{(n+1)(n+2)}{2}$ .  $\square$  To už plyne úpravou:

$$\sum_{j=0}^{n+1} j = \sum_{j=0}^n j + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \square$$

Podle principu matematické indukce je celý důkaz hotov.  $\square$

## 2.4 Komentáře k matematické indukci

Pro správné a úspěšné použití indukce v dokazování je vhodné si zapamatovat několik cenných rad:

- Základní trik všech důkazů matematickou indukcí je vhodná *reformulace* tvrzení  $T(n+1)$  tak, aby se „odvolávalo“ na tvrzení  $T(n)$ .
  - \* Dobře se vždy podívejte, v čem se liší tvrzení  $T(n+1)$  od tvrzení  $T(n)$ . Tento „rozdíl“ budete muset v důkaze zdůvodnit. □
- Pozor, občas je potřeba „*zesílit*“ tvrzení  $T(n)$ , aby indukční krok správně „fungoval“. □
- Často se chybí v důkazu indukčního kroku, neboť ten bývá většinou výrazně obtížnější než báze, ale o to *zrádnější* jsou chyby v samotné zdánlivě snadné bázi!
  - \* Dejte si dobrý pozor, od které hodnoty  $n \geq k_0$  je indukční krok univerzálně platný a jestli báze nezahrnuje více než jednu hodnotu. . .

**Příklad 2.9.** Kdy je vhodné (a v zásadě také nutné) indukční krok zesílit. . .

**Věta.** Pro každé  $n \geq 1$  platí

$$s(n) = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} < 1.$$

**Důkaz:**  $\square$  *Báze indukce* je zřejmá, neboť  $\frac{1}{1 \cdot 2} < 1$ .

Co však *indukční krok*? Předpoklad  $s(n) < 1$  je sám o sobě „příliš slabý“ na to, aby bylo možno tvrdit  $s(n+1) = s(n) + \frac{1}{(n+1)(n+2)} < 1$ .  $\square$

Neznamená to ještě, že by tvrzení nebylo platné, jen je potřeba náš indukční předpoklad *zesílit*. Budeme dokazovat

„Pro každé přirozené  $n \geq 1$  platí  $s(n) \leq 1 - \frac{1}{n+1} < 1$ .“  $\square$

To platí pro  $n = 1$  a dále už úpravou jen dokončíme zesílený indukční krok:

$$\begin{aligned} s(n+1) &= s(n) + \frac{1}{(n+1)(n+2)} \leq 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} = \\ &= 1 + \frac{-(n+2) + 1}{(n+1)(n+2)} = 1 - \frac{1}{n+2} \end{aligned}$$

$\square$

## Rozšíření báze a předpokladu

Mimo zesilování tvrzení indukčního kroku jsme někdy okolnostmi nuceni i k **rozšiřování** samotné báze indukce a s ní indukčního předpokladu na více než jednu hodnotu parametru  $n$ . □

- Můžeme například předpokládat platnost (parametrizovaných) tvrzení  $T(n)$  i  $T(n + 1)$  **zároveň**, a pak odvozovat platnost  $T(n + 2)$ .

Toto lze samozř. zobecnit na jakýkoliv počet předpokládaných parametrů. □

- Můžeme dokonce předpokládat platnost tvrzení  $T(j)$  **pro všechna**  $j = k_0, k_0 + 1, \dots, n$  najednou a dokazovat  $T(n + 1)$ .

Toto typicky využijeme v případech, kdy indukční krok „rozdělí“ problém  $T(n + 1)$  na dvě menší části a z nich pak odvodí platnost  $T(n + 1)$ . □

**Fakt:** Obě prezentovaná „rozšíření“ jsou v konečném důsledku jen speciálními instancemi základní matematické indukce; použité rozšířené možnosti pouze zjednodušují formální zápis důkazu.

**Příklad 2.10.** *Když je nutno rozšířit bázi a indukční předpoklad. . .*

**Věta.** *Nechť funkce  $f$  pro každé  $n \geq 0$  splňuje vztah*

$$f(n+2) = 2f(n+1) - f(n).$$

*Pokud platí  $f(0) = 1$  a zároveň  $f(1) = 2$ , tak platí  $f(n) = n + 1$  pro všechna přirozená  $n \geq 0$ . □*

**Důkaz:** Už samotný pohled na daný vztah  $f(n+2) = 2f(n+1) - f(n)$  naznačuje, že bychom měli rozšířit indukční předpoklad (a krok) zhruba takto:

*Pro každé  $n \geq 0$ ; jestliže platí  $T(n)$ ; neboli  $f(n) = n + 1$ , a zároveň platí  $T(n+1)$ ;  $f(n+1) = n + 2$ , pak platí také  $T(n+2)$ ;  $f(n+2) = n + 3$ .*

**Báze indukce** – □ pozor, zde už musíme ověřit dvě hodnoty

$$f(0) = 0 + 1 = 1, \quad f(1) = 1 + 1 = 2. \square$$

Náš **indukční krok** tak nyní může využít celého rozšířeného předpokladu, znalosti hodnot  $f(n)$  i  $f(n+1)$ , pro ověření

$$f(n+2) = 2f(n+1) - f(n) = 2 \cdot (n+1+1) - (n+1) = n+3 = n+2+1. \square$$

## Závěrem malý „problém“

**Příklad 2.11.** *Aneb jak snadno lze v matematické indukci udělat chybu.*

**Věta.** („nevěta“)

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

**Důkaz** indukcí vzhledem k  $n$ .

**Báze:** Ve stádu o jednom koni mají všichni koně stejnou barvu.  $\square$

**Indukční krok:** Necht'  $S = \{K_1, \dots, K_{n+1}\}$  je stádo o  $n+1$  koních. Dokážeme, že všichni koně mají stejnou barvu. Uvažme dvě menší stáda:

- $S' = \{K_1, \underline{K_2}, \dots, K_n\}$
- $S'' = \{\underline{K_2}, \dots, K_n, K_{n+1}\}$   $\square$

Podle indukčního předpokladu mají všichni koně ve stádu  $S'$  stejnou barvu  $B'$ . Podobně všichni koně ve stádu  $S''$  mají podle indukčního předpokladu stejnou barvu  $B''$ .  $\square$  Dokážeme, že  $B' = B''$ , tedy že všichni koně ve stádu  $S$  mají stejnou barvu. To ale plyne z toho, že koně  $K_2, \dots, K_n$  patří jak do stáda  $S'$ , tak i do stáda  $S''$ .  $\square$

$\square$

Ale to už je podvod! Vidíte, kde?