4 Techniky matematických důkazů

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 „právě tehdy, když“.
* Důkazy matematickou indukcí, jejich variace a úskalí.
* Metody zesílení tvrzení a rozšíření základu v indukci.

4.1 Přehled základních důkazových technik

- *Přímé odvození.* To je způsob, o kterém jsme se dosud bavili. □
- *Kontrapozice* (také *obměnou* – „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 4.1. *Na důkaz kontrapozicí (obměnou).*

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

Důkaz *obměněného tvrzení*:
Místo uvedeného znění věty budeme 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 $p = 2 \cdot k$ není větší než 2.
- $k > 1$. Pak $p = 2 \cdot k$ není prvočíslo podle definice.

□

Příklady důkazu sporem

Příklad 4.2. *Jiný, kratší přístup k Důkazu 4.1.*

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

Důkaz *sporem*: Nechť 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). $\square$

Příklad 4.3. *Opět sporem.*

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

Důkaz *sporem*: Nechť $\sqrt{2}$ je racionální, tj. nechť existují celá kladná čísla r, s taková, že $\sqrt{2} = r/s$. Můžeme navíc předp., že r je nejmenší možné takové.

- 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 čtyřmi, tedy $r^2 = 4 \cdot m$ pro nějaké celé 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 $r' = r/2$ i $s' = s/2$ jsou celá, platí $\sqrt{2} = r/s = r'/s'$ a přitom $r' < r$, což je spor. $\square$

4.2 Věty typu „právě tehdy (když)“

- Uvažujme nyní (v matematice poměrně hojné) věty tvaru

  „Nechť platí předpoklady P.
  Pak tvrzení A platí *právě tehdy*, platí-li tvrzení B.“ □

- Příklady jiných jazykových formulací téže věty jsou:
  - Nechť platí předpoklady P. Pak tvrzení A platí *tehdy a jen tehdy*, když platí tvrzení B. □
  - 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. □

- 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 4.4. *Na důkaz typu „právě tehdy (když)".*

Věta. *Pro dvě množiny* A, B *platí, že* $2^A = 2^B$ *právě tehdy, když* $A^2 = B^2$.

Důkaz: Nezapomínáme, že našim úkolem je dokázat oba směry tvrzení (implikace zleva doprava a zprava doleva). Přitom obě implikace budeme dokazovat obměnou, symbolicky jako $2^A \neq 2^B \iff A^2 \neq B^2$.

Začneme s prvním směrem: Je-li $2^A \neq 2^B$, pak existuje množina X taková, že $X \subseteq A$ a $X \not\subseteq B$ (nebo naopak – což se řeší symetricky). $X \not\subseteq B$ přitom podle definice znamená, že pro nějaké $y \in X$ platí $y \notin B$. Zároveň však $y \in A$. Proto $(y, y) \in A^2$, ale $(y, y) \notin B^2$, neboli $A^2 \neq B^2$.

V opačném směru postupujeme z předpokladu $A^2 \neq B^2$. Zase z toho odvodíme, že existuje uspořádaná dvojice taková, že $(x, y) \in A^2$, ale $(x, y) \notin B^2$. Z posledního vyplývá, že $x \notin B$ nebo $y \notin B$. Opět bez újmy na obecnosti můžeme vzít jen případ $x \notin B$. Avšak z $(x, y) \in A^2$ vidíme, že $x \in A$. Proto $\{x\} \in 2^A$, ale $\{x\} \notin 2^B$, neboli $2^A \neq 2^B$. □

4.3 Matematická indukce

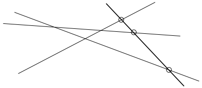
- Jde o důkazovou techniku aplikovatelnou na tvrzení tohoto typu:

  „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 $k \geq k_0$; jestliže platí $T(k)$,* *(indukční předpoklad)*
    pak platí také $T(k+1)$. *(indukční krok)*

Příklady důkazů indukcí

Příklad 4.6. *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.* □

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

Indukční krok pro $k \geq 1$: Nechť p_k^s pravděpodobnost, že při hodu k kostkami bude výsledný součet sudý, a p_k^l je pravděpodobnost lichého. Podle indukčního předpokladu je

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

□

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

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

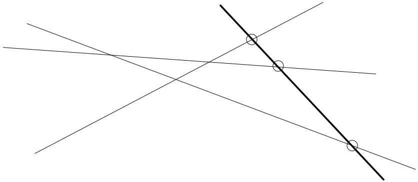
a stejně pro pravděpodobnost celkového lichého součtu. □

Příklad 4.7. *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 postačí, že $n = 0$ přímek dělí rovinu na jednu oblast. (Všimněte si také, že 1 přímka dělí rovinu na dvě oblasti.)

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

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

A toto je přesně naše tvrzení pro $n = k+1$, takže jsme hotovi. □

Příklad 4.8. *Další indukční důkaz rozepsaný v podrobných krocích.*

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

Důkaz *indukcí* vzhledem k n.

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

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

Předpokládejme tedy, že $\sum_{j=0}^{k} j = \frac{k(k+1)}{2}$ a pokusme se dokázat, že pak také $\sum_{j=0}^{k+1} j = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2}$. □ To už plyne přímočarou úpravou:

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

Podle principu matematické indukce je celý důkaz hotov. □

4.4 Komentáře k matematické indukci

- 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. □

- Dokud se matematickou indukci teprve učíte, používejte následující.

  Zaveďte si další proměnnou k a formulujte svá tvrzení a úpravy stylem „platí-li naše tvrzení $T(n)$ pro $n := k$, pak bude platit i pro $n := k + 1$“. □

- Pozor, občas je potřeba *zesílit* tvrzení $T(n)$, aby indukční krok správně „fungoval“ (a jsou situace, kde tento trik velmi pomáhá).□

- Často se chybuje 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 4.9. *Kdy je vhodné (a v zásadě také nutné) indukční tvrzení zesílit...*

Věta. *Pro každé* $n \geq 1$ *platí*

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

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

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

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

„Pro každé přirozené $n \geq 1$ platí $s(n) \leq 1 - \frac{1}{2^n} < 1\,.$"

To platí pro bázi $n = 1$, neboť $\frac{1}{2} \leq 1 - \frac{1}{2}$, a dále už úpravou jen dokončíme zesílený indukční krok:

$$s(n+1) \;=\; s(n) + \frac{1}{2^{n+1}} \;\leq\; 1 - \frac{1}{2^n} + \frac{1}{2^{n+1}} = 1 - \frac{1}{2^{n+1}}$$

□

Rozšíření předpokladu; silná indukce

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 tři i více předpokládaných parametrů.□

- Můžeme dokonce předpokládat platnost tvrzení $T(j)$ pro všechna $j = k_0, k_0+1, \dots, n$ najednou a dokazovat $T(n+1)$ (vznešeně se této variantě indukce říká *silná indukce*).

  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; nejsou o nic „silnější“ ve striktním matematickém smyslu a použité rozšířené možnosti pouze zjednodušují formální zápis důkazu.

Příklad 4.10. *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 přirozené $k \geq 0$; jestliže platí $f(n) = n+1$ pro $n := k$ a zároveň pro $n := k+1$, pak $f(n) = n+1$ platí také pro $n := k+2$.

Báze indukce – pozor, zde už musíme ověřit dvě hodnoty pro $n := 0$ a $n := 1$:

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

Náš *indukční krok* tak nyní může využít celého rozšířeného předpokladu, znalosti hodnot $f(k)$ i $f(k+1)$, pro ověření požadovaného vztahu pro $n := k+2$

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

□

Příklad 4.11. *Ukázka s vhodným použitím silné indukce:*

> **Věta**. *Každé přirozené číslo $n \geq 2$ lze zapsat jako součin prvočísel (může být jen jednoho a prvočísla nemusí být různá).*

Důkaz: *Báze indukce*. Nechť $n = 2$, pak n je prvočíslem a součinem jednoho prvočísla.

Indukční krok. Pokud nemá n vlastní dělitele, je n prvočíslem vzhledem k předpokladu $n \geq 2$, což je shodné s bází.

Jinak napíšeme $n = a \cdot b$, kde platí $a, b \geq 2$ a zároveň $a, b < n$, a proto lze na obě čísla a, b použít indukční předpoklad. Tudíž každé z nich lze napsat jako součin prvočísel a jelikož ta nemusí být různá, prostě oba součiny sloučíme do jednoho, jehož výsledkem je $a \cdot b = n$. $\square$

Závěrem malý „problém“

Příklad 4.12. *Aneb jak snadno lze v matematické indukci udělat chybu.*

Věta. *(„nevěta“)*
V každém stádu o $n \geq 1$ koních mají všichni koně stejnou barvu. □

Důkaz indukcí vzhledem k n.

Báze: Ve stádu o jednom koni mají všichni koně stejnou barvu. □

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

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

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''. □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''. □

□

Ale to už je podvod! Vidíte, kde?