# Cvičenie 3: Dôkazy

→ **Úloha 1.** Máme dokázať, že platí
$$\sqrt{60} > \sqrt{13} + \sqrt{17}.$$
Nižšie sa nachádza pokus o dôkaz tohto tvrdenia. Na koľko ide o korektný dôkaz?

**Pokus o riešenie**

Zo školy vieme, že nerovnosti môžeme rôzne upravovať, tak poďme na to:
$$\begin{aligned}
\sqrt{60} &> \sqrt{13}+\sqrt{17} \qquad |^2\\
\left(\sqrt{60}\right)^2 &> \left(\sqrt{13}+\sqrt{17}\right)^2\\
60 &> 13 + 2\sqrt{13}\sqrt{17} + 17\\
60 &> 30 + 2\sqrt{221} \qquad | -30\\
30 &> 2\sqrt{221} \qquad | \,/2\\
15 &> \sqrt{221} \qquad |^2\\
255 &> 221
\end{aligned}$$
Takto sme sa dostali k niečomu, čo platí, takže aj pôvodná nerovnosť je pravdivá.

→ **Úloha 2.** Porovnajte dôkaz predošlého s dôkazom tvrdenia, že $\sqrt{2} > \sqrt{3}$.

**Pokus o riešenie**

Opäť na to pôjdeme rovnako ako v predošlom príklade. Teda budeme upravovať dokazovanú nerovnosť:
$$\begin{aligned}
\sqrt{2} &> \sqrt{3}, \qquad | -\sqrt{3}\\
\sqrt{2}-\sqrt{3} &> 0, \qquad |^2\\
2 - 2\cdot\sqrt{2}\cdot\sqrt{3} + 3 &> 0, \qquad | +2\cdot\sqrt{6}\\
5 &> 2\cdot\sqrt{6}, \qquad |^2\\
25 &> 24,
\end{aligned}$$
a to je pravda. Preto platí $\sqrt{2} > \sqrt{3}$.

Ak si chcete precvičiť dokazovanie na takýchto číselných úlohách bez písmeniek, tak vám zopár dávame.

**Úloha 3.** Dokážte, že platí:

a) $\sqrt{9-\sqrt{10}} < \sqrt{9+\sqrt{10}} - 1$

b) $\sqrt{4}+\sqrt{7} < \sqrt{3}+\sqrt{12}$

c) $\sqrt{60}+\sqrt{\sqrt{47}-\sqrt{46}} > \sqrt{13}+\sqrt{17}$

→ **Úloha 4.** Dokážte, že platí
$$(\forall x \in \mathbb{R}_0^+)(\forall y \in \mathbb{R}_0^+)\ \frac{x+y}{2} \geq \sqrt{xy}.$$

**Úloha 5.** Zistite, či nasledovné tvrdenia sú tautológie

→ a) $[(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)] \Rightarrow [\neg b \Rightarrow (e \vee d)]$,

→ b) $[(\neg a \Rightarrow b) \vee (c \wedge d) \vee (e \wedge \neg c \wedge \neg a)] \Rightarrow [(\neg b \wedge \neg c) \Rightarrow a]$,

c) $[(\neg a \Rightarrow b) \vee (c \wedge d) \vee (e \wedge \neg c \wedge a)] \Rightarrow [(\neg b \wedge \neg c) \Rightarrow a]$,

d) $[(a \Rightarrow b) \wedge (\neg b \vee c)] \Rightarrow [((c \Rightarrow d) \wedge a) \Rightarrow d]$

e) $(a \wedge \neg b) \vee [((\neg c \vee d) \wedge (a \vee \neg e) \wedge (f \vee \neg g)) \Rightarrow (d \vee \neg e)]$

f) $(a \wedge \neg b \wedge c) \vee (\neg b \Rightarrow (d \wedge \neg e)) \vee (\neg c \wedge d \wedge e) \vee (d \Rightarrow (\neg a \wedge c))$.

**Úloha 6.** Zistite, či nasledovné výroky sú tautológie. V prípade, že nejde o tautológiu, možno dostať tautológiu nahradením $\Leftrightarrow$ za $\Leftarrow$ alebo $\Rightarrow$?

→ a) $(\forall x)a(x) \Rightarrow (\exists x)a(x)$

→ b) $(\exists x)a(x) \Rightarrow (\forall x)a(x)$

→ c) $(\forall x)(a(x) \wedge b(x)) \Leftrightarrow ((\forall x)a(x) \wedge (\forall x)b(x))$

→ d) $(\forall x)(a(x) \vee b(x)) \Leftrightarrow ((\forall x)a(x) \vee (\forall x)b(x))$

e) $(\exists x)(a(x) \wedge b(x)) \Leftrightarrow ((\exists x)a(x) \wedge (\exists x)b(x))$

f) $(\exists x)(a(x) \vee b(x)) \Leftrightarrow ((\exists x)a(x) \vee (\exists x)b(x))$

→ g) $(\forall x)(a(x) \Rightarrow b(x)) \Leftrightarrow ((\forall x)a(x) \Rightarrow (\forall x)b(x))$

h) $(\exists x)(a(x) \Rightarrow b(x)) \Leftrightarrow ((\forall x)a(x) \Rightarrow (\exists x)b(x))$

i) $((\forall x)a(x) \Rightarrow (\exists x)b(x)) \Leftrightarrow (\exists x)(a(x) \Rightarrow b(x))$

**Úloha 7.** Dokážte nasledovné tvrdenia:

a) $(\forall n \in \mathbb{N})(7 \nmid 47n \Rightarrow 7 \nmid n)$

b) $(\forall a, b \in \mathbb{N})[(22 \mid a \wedge 33 \mid b) \Rightarrow 11 \mid (a+b)]$

c) $\sqrt{3}$ je iracionálne číslo.

d) $\log_2 3$ je iracionálne číslo.

e) $(\forall n \in \mathbb{N}^+)(2^n < n! \Rightarrow 2^{n+1} < (n+1)!)$

f) $(\forall a, b \in \mathbb{N})[(a \bmod 7 = 4 \wedge b \bmod 7 = 5) \Rightarrow ab \bmod 7 = 6]$

g) Pre každé prvočíslo $p$ je $\sqrt{p}$ iracionálne číslo.

→ **Úloha 8.** Rozhodnite o platnosti nasledovných výrokov:

a) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((x \notin \mathbb{Q} \wedge y \notin \mathbb{Q}) \Rightarrow x + y \notin \mathbb{Q})$

b) $(\exists c \in \mathbb{R})(\forall n \in \mathbb{N})(47n^5 + 42n^3 + 17n^2 - 9 \leq cn^5)$

c) $(\exists c \in \mathbb{R})(\forall n \in \mathbb{N})(n^2 + 47 \leq cn)$

d) $(\exists K \in \mathbb{R})(\forall x \in \mathbb{R})(x \geq K \Rightarrow x^7 - 50x^6 - 47x^5 - 42x^3 - 17x^2 + 18x - 9 \geq 0)$

## Úlohy na ďalšie precvičenie dôkazov

**Úloha 9.** Dokážte:

a) $(\forall n \in \mathbb{N})(5 \mid n^2 + 1 \Rightarrow 10 \nmid n)$

b) Ak prirodzené číslo $n$ nie je deliteľné tromi, tak $n^2$ dáva po delení tromi zvyšok 1.

c) Ak súčet reálnych čísel $a$, $b$, $c$, $d$, $e$ je nula, tak aspoň jedno z nich je nezáporné.

d) Súčet tretích mocnín troch za sebou idúcich čísel je deliteľný deviatimi.

e) $(\forall a, b \in \mathbb{R}^+)\left(\dfrac{a+b}{2} \leq \dfrac{2(a^2+ab+b^2)}{3(a+b)}\right)$

**Úloha 10.** Dokážte, že ak $a$, $b$ sú racionálne čísla, tak aj $a \cdot b$ je racionálne číslo.

**Úloha 11.** Dokážte, že ak súčin dvoch reálnych čísel $x$ a $y$ je iracionálne číslo, musí byť aspoň jedno z čísel $x$ a $y$ iracionálne.

**Úloha 12.** Nech $a$, $b$ sú kladné celé čísla. Dokážte, že ak nemožno krátiť zlomok $\frac{a}{b}$, tak nemožno krátiť ani zlomok $\dfrac{a-b}{a+b}$.

**Úloha 13.** Máme reálne čísla $a$, $b$, $c$ také, že čísla

$$\frac{1}{b+c}, \qquad \frac{1}{c+a}, \qquad \frac{1}{a+b}$$

tvoria aritmetickú postupnosť. Dokážte, že aj čísla $a^2$, $b^2$, $c^2$ tvoria aritmetickú postupnosť.

**Úloha 14.** Dokážte, že ak existuje nekonečne veľa prvočísel $p$, pre ktoré je aj $p + 2$ prvočíslo, tak potom existuje nekonečne veľa prvočísel $p$, pre ktoré je $p + 2$ prvočíslo a navyše $p + 1$ je deliteľné 6-timi.

**Úloha 15.** Dokážte, že ak $e$ (eulerova konštanta) nie je riešením polynomiálnej rovnice s celočíselnými koeficientmi, tak ani $2e$ nie je.

**Úloha 16.** O čísle $\pi$ vieme, že je iracionálne. Dokážte, že číslo

$$\frac{47}{\sqrt[3]{\pi} + 42}$$

je tiež iracionálne.

**Úloha 17.** Dokážte, že pre každé prvočíslo $p$ je $\sqrt{p}$ iracionálne číslo.

**Úloha 18.** Je číslo $\sqrt{2} + \sqrt{3}$ racionálne?

**Úloha 19.** Dokážte, že ak $\sqrt{a} + \sqrt{b} \in \mathbb{Q}$ pre nejaké racionálne čísla $a$, $b$, tak aj $\sqrt{a} \in \mathbb{Q}$, aj $\sqrt{b} \in \mathbb{Q}$.

**Úloha 20.** Dokážte, že pre každé celé čísla $x$, $y$ platí

$$31 \mid 6x + 11y \Leftrightarrow 31 \mid x + 7y.$$

**Úloha 21.** Nech $a$, $b$, $c$ sú reálne čísla, pre ktoré platí $a + b + c = 0$. Dokážte, že

$$\frac{a}{b} + \frac{b}{a} + \frac{a}{c} + \frac{c}{a} + \frac{b}{c} + \frac{c}{b} = -3.$$

**Úloha 22.** Rozhodnite o platnosti nasledovných výrokov:

a) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((x \notin \mathbb{Q} \wedge y \notin \mathbb{Q} \Rightarrow x + y \notin \mathbb{Q}))$

b) $(\exists c \in \mathbb{R})(\forall n \in \mathbb{N})(47n^5 + 42n^3 + 17n^2 - 9 \leq nc^5)$

c) $(\exists c \in \mathbb{R})(\forall n \in \mathbb{N})(n^2 + 47 \leq cn)$

d) $(\exists K \in \mathbb{R})(\forall x \in \mathbb{R})(x \geq K \Rightarrow x^7 - 50x^6 - 47x^5 - 42x^3 - 17x^2 + 18x - 9 \geq 0)$

Pri riešení nevyužívajte vysokoškolskú matematiku (limity, derivácie, ...).

**Úloha 23.** (*) Dokážte, že pre každé prirodzené číslo $n$ je číslo 2 najväčším spoločným deliteľom čísel $2n + 6$, $4n + 10$.

**Úloha 24.** (*) Dokážte, že ak existuje nekonečne veľa palindromických prvočísel (čítajú sa rovnako spredu aj odzadu), tak existuje aj nekonečne veľa palindromických prvočísel, ktoré majú nepárny počet cifier.

## Ako správne písať dôkazy

V tejto časti ilustrujeme zopár príkladov správneho zápisu dôkazov. Všetky riešenia sú písané pomerne minimalisticky, len s nevyhnutnými komentármi. Ak si však pri riešení nie ste istí, odporúčame vám písať do riešenia aj slovné komentáre, ktoré popisujú vaše zdôvodnenia a argumenty.

### Dôkaz nerovnosti z úlohy 1

Uvedené riešenie vieme opraviť dvomi spôsobmi

**1. spôsob riešenia**

$$\begin{aligned}
255 &> 221 \qquad \big| \sqrt{\phantom{x}} \text{( obe strany kladné)}\\
15 &> \sqrt{221}\\
30 &> 2\sqrt{221}\\
60 &> 30 + 2\sqrt{221}\\
60 &> 13 + 2\sqrt{13}\sqrt{17} + 17\\
\left(\sqrt{60}\right)^2 &> \left(\sqrt{13}+\sqrt{17}\right)^2\\
\left|\sqrt{60}\right| &> \left|\sqrt{13}+\sqrt{17}\right|\\
\sqrt{60} &> \sqrt{13}+\sqrt{17}
\end{aligned}$$

**2. spôsob riešenia**

$$\begin{aligned}
\sqrt{60} &> \sqrt{13}+\sqrt{17} \qquad |^2\\
&\Uparrow\\
\left(\sqrt{60}\right)^2 &> \left(\sqrt{13}+\sqrt{17}\right)^2\\
&\Uparrow\\
60 &> 13 + 2\sqrt{13}\sqrt{17} + 17\\
&\Uparrow\\
60 &> 30 + 2\sqrt{221} \qquad | -30\\
&\Uparrow\\
30 &> 2\sqrt{221} \qquad | /2\\
&\Uparrow\\
15 &> \sqrt{221} \qquad |^2\\
&\Uparrow\\
255 &> 221
\end{aligned}$$

V skutočnosti však dôkazy vôbec nemusia byť lineárne. Nové tvrdenie v dôkazovej postupnosti nemusí vyplývať iba z predošlého, ale môže vyplývať aj z ľubovoľných už dokázaných tvrdení. Takýmto štýlom vieme zostaviť dôkaz, ktorý je založený na výpočtoch, resp. presnejšie, odhadoch.

**3. spôsob riešenia**

1. $60 > 59,9076$ (zjavná pravda)
2. $\sqrt{60} > 7,74$ (lebo 1.)
3. $13,0321 > 13$ (zjavná pravda)
4. $3,61 > \sqrt{13}$ (lebo 3.)
5. $17,0569 > 17$ (zjavná pravda)
6. $4,13 > \sqrt{17}$ (lebo 3.)
7. $7,74 = 3,61 + 4,13 > \sqrt{13} + \sqrt{17}$, lebo 4. a 5.
8. $\sqrt{60} > \sqrt{13} + \sqrt{17}$, lebo 2. a 6.

V 6. kroku sme využili, že ak platí $a < c$ a zároveň $b < d$, tak platí aj $a + b < c + d$, pre ľubovoľné reálne čísla $a$, $b$, $c$, $d$. V 7. kroku sme zas využili, že ak platí $a < b$ a zároveň $b < c$, tak platí aj $a < c$ (pre $\forall a, b, c \in \mathbb{R}$).

V tomto prípade sme jednotlivé kroky dôkazu písali pod seba a slovne sme naznačili, na základe čoho sme tvrdenie dostali. Zdôvodnenia v zátvorkách možno vynechať. Taktiež tieto zdôvodnenia možno zaznačiť aj inak. Jedným z ďalších spôsobov je využitie šípok / implikácií, čo z čoho vyplýva.

**4. spôsob riešenia**

$$\left.\begin{array}{r} \left.\begin{array}{r} 13,0321 > 13 \Rightarrow 3,61 > \sqrt{13} \\ 17,0569 > 17 \Rightarrow 4,13 > \sqrt{17} \end{array}\right\} \Rightarrow 7,74 > \sqrt{13} + \sqrt{17} \\ 60 > 59,9076 \Rightarrow \sqrt{60} > 7,74 \end{array}\right\} \Rightarrow \sqrt{60} > \sqrt{13} + \sqrt{17}$$

## Dôkaz tautológie 5 a)

**Zápis riešenie cez postupnosť tvrdení**

Výrok je tautológia. Dôkaz sporom.

1. Nech platí $\neg[[(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)] \Rightarrow [\neg b \Rightarrow (e \vee d)]]$
2. $(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)$ (z 1.)

3. $\neg[\neg b \Rightarrow (e \vee d)]$ (z 1.)
4. $\neg b$ (z 3.)
5. $\neg(e \vee d)$ (z 3.)
6. $\neg e$ (z 5.)
7. $\neg d$ (z 5.)
8. $a \Rightarrow b$ (z 2.)
9. $\neg a$ (z 4. a 8.)
10. $(c \vee d)$ (z 2.)
11. $c$ (z 7. a 11.)
12. $(\neg a \wedge c) \Rightarrow e$ (z 2.)
13. $\neg a \wedge c$ (z 9. a 11.)
14. $e$ (z 12. a 13.) – to je spor s 6.

Pri dôkaze sporom je potrebné napísať, že ideme dokazovať sporom (kľudne aj jedným slovom. A následne označiť, čo je s čím v spore (v našom prípade 6. a 14.). Pri takýchto riešeniach často hovoríme o tom, že nejaký výrok platí alebo neplatí. To sa dá značiť viacerými spôsobmi.

- Pravdivé výroky môžeme písať len tak ako krok (napr. body 2., 8., 10., 14.), nepravdivé vieme písať formou, že platí ich negácia (napr. body 1., 3., 4, 5.). (Toto je použité aj v riešení)
- Pravdivosť vieme vyjadriť ekvivalenciou s pravdivostnou hodnotou, napr.
  1. $[[(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)] \Rightarrow [\neg b \Rightarrow (e \vee d)]] \Leftrightarrow 0$
  4. $b \Leftrightarrow 0$
  8. $(a \Rightarrow b) \Leftrightarrow 1$
  14. $e \Leftrightarrow 1$

  Pritom si však dávajte pozor, aby to nevyzeralo ako dosadenie pravdivostnej hodnoty za elementárny výrok.
- Použiť ohodnotenie / valuáciu výrokov $v$:
  1. $v([(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)] \Rightarrow [\neg b \Rightarrow (e \vee d)]) = 0$
  14. $v(e) = 1$

  Tento spôsob sa často používa pri hlbšom štúdiu matematickej logiky. Na tomto predmete však nie je nutné sa ním zaobrať.

Ešte si ukážeme, že dôkazy sa dajú zapisovať aj ako text. Tento text zároveň aj detailnejšie vysvetľuje, čo sa deje v predšlom symbolickom dôkaze. Záver je mierne odlišný.

**Zápis riešenia textom**

Sporom. Nech neplatí $[(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)] \Rightarrow [\neg b \Rightarrow (e \vee d)]$. Potom $(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)$ platí a výrok $\neg b \Rightarrow (e \vee d)$ neplatí. Z neskoršieho dostávame, že $\neg b$ je pravda, teda $b \Leftrightarrow 0$; a tiež $e \vee d$ neplatí, teda $e \Leftrightarrow 0$ a $d \Leftrightarrow 0$. Z pravdivého výroku $(a \Rightarrow b) \wedge (c \vee d) \wedge ((\neg a \wedge c) \Rightarrow e)$ vieme, že $(a \Rightarrow b)$ platí. Preto keďže $b \Leftrightarrow 0$, tak aj $a \Leftrightarrow 0$. Tiež nám platí $(c \vee d)$, z čoho vďaka $d \Leftrightarrow 0$ máme, že $c \Leftrightarrow 1$. Napokon nám platí aj $(\neg a \wedge c) \Rightarrow e$. Keď tam však dosadíme určené pravdivostné hodnoty, tak nám vyjde $(1 \wedge 1) \Rightarrow 0$, čo však pravda nie je, a to je spor.

### Dôkaz ne-tautológie 5 b)

Ak chceme dokázať, že zložený výrok nie je tautológia, máme to jednoduché – stačí nám uviesť jeden prípad, kedy nám vyjde nepravda + vyhodnotiť (resp. aspoň naznačiť vyhodnotenie výroku).

**Riešenie**

Nejde o tautológiu, lebo pre $a \Leftrightarrow 0$, $b \Leftrightarrow 0$, $c \Leftrightarrow 0$, $d \Leftrightarrow 1$, $e \Leftrightarrow 1$ vyjde nepravda:

$$\underbrace{\underbrace{[(\neg a \Rightarrow b) \vee (c \wedge d) \vee \underbrace{(e \wedge \neg c \wedge \neg a)}_{1}]}_{1} \Rightarrow \underbrace{[\underbrace{(\neg b \wedge \neg c)}_{1} \Rightarrow \underbrace{a}_{0}]}_{0}}_{0}$$

Upozorňujeme, na časté nesprávne (neúplné riešenie)

**Nesprávne riešenie**

Pre spor predpokladajme, že výrok neplatí

1. $\neg[[(\neg a \Rightarrow b) \vee (c \wedge d) \vee (e \wedge \neg c \wedge \neg a)] \Rightarrow [(\neg b \wedge \neg c) \Rightarrow a]]$
2. $(\neg b \wedge \neg c) \Rightarrow a$ (z 1.)
3. $(\neg b \wedge \neg c)$ (z 2.)
4. $\neg b$ (z 3.)
5. $\neg c$ (z 3.)
6. $\neg a$ (z 2.)
7. $(\neg a \Rightarrow b) \vee (c \wedge d) \vee (e \wedge \neg c \wedge \neg a)$ (z 1.)
8. $\neg(\neg a \Rightarrow b)$ (z 4. a 6.)
9. $\neg(c \wedge d)$ (z 5.)
10. $e \wedge \neg c \wedge \neg a$ (z 7., lebo prvé dva výroky v disjunkcii sú nepravdivé, tak musí platiť tretí)
11. $e$ (z 10.)

Dostali sme ohodnotenie elementárnych výrokov, kedy platí $a \Leftrightarrow 0$, $b \Leftrightarrow 0$, $c \Leftrightarrow 0$, $e \Leftrightarrow 1$ ($d$ môže byť aj pravda, aj nepravda). Teda výrok nie je tautológia.

Hoci takto zrejme budete riešiť takéto úlohy, toto nie je dôkaz – vychádzame totiž z predpokladu, že zložený výrok neplatí a tak nemôžeme dokázať, že naozaj neplatí. Dokonca v takejto situácii môžeme dojsť aj nesprávnemu záveru (teda by výrok bol tautológiou) – to, že sa nám nepodarilo dostať ku sporu, neznamená, že tam niekde skrytý nie je.

V takejto situácii potrebujeme overiť, že pre nami nájdené ohodnotenie elementárnych výrokov nám vyjde naozaj nepravda (alebo to iným spôsobom zdôvodniť, ale overenie je najjednoduchšie a najistejšie). Je to rovnaká situácia, ako keď pri riešení rovnice (či sústavy rovníc) nám nestačí dospieť k tomu, že $x = 17$, $y = 42$ a $z = 47$, ale potrebujeme ešte vykonať skúšku správnosti (alebo iným spôsobom odargumentovať, že nami nájdené riešenie vyhovuje).

## Ako dokazovať kvantifikované tautológie

Ilustrujeme si to na modifikácii úlohy 6g), kde dokážeme, že

$$(\forall x)(a(x) \Rightarrow b(x)) \Rightarrow ((\forall x)a(x) \Rightarrow (\forall x)b(x))$$

je tautológia.

**Priamy dôkaz**

1. Nech platí $(\forall x)(a(x) \Rightarrow b(x))$.
Dokážeme, že platí $(\forall x)a(x) \Rightarrow (\forall x)b(x)$:

2. Nech platí $(\forall x)a(x)$.
Dokážeme, že platí $(\forall x)b(x)$:

Pre každé $x$ platí:

3. $a(x)$ (lebo 2.)
4. $a(x) \Rightarrow b(x)$ (lebo 1.)
5. $b(x)$ (lebo 3. a 4.)

Teda platí $(\forall x)b(x)$.

Teda platí $(\forall x)a(x) \Rightarrow (\forall x)b(x)$

Teda platí $(\forall x)(a(x) \Rightarrow b(x)) \Rightarrow ((\forall x)a(x) \Rightarrow (\forall x)b(x))$

*Komentár.* Dokazovaná tautológia má formu implikácie. Tú dokazujeme priamo tak, že predpokladáme pravdivosť ľavej strany a ukážeme, že platí aj pravá strana. Keďže na pravej strane je opäť implikácia, tak tento postup zopakujeme. Dôkazy týchto dvoch implikácií sú v červených rámčekoch. Dostaneme sa k dokazovaniu výroku v tvare všeobecného kvantifikátora (modrý rámček). Ten dokazujeme tak, že napíšeme dôkaz kvantifikovanej výrokovej formy všeobecne za pomoci premennej (zlený rámček). Všimnite si, že vnútri zeleného rámčeka nemáme žiadne kvantifikátory. Do vašich riešení nemusíte písať tento komentár. Tiež môžete vypustiť aj závery „Teda platí. . . “

**Dôkaz sporom**

Pre spor predpokladajme, že (pre nejaké univerzum a nejaké výrokové formy $a(x)$, $b(x)$ na ňom definované) platí negácia, teda:

1. $\neg[(\forall x)(a(x) \Rightarrow b(x)) \Rightarrow ((\forall x)a(x) \Rightarrow (\forall x)b(x))]$
2. $(\forall x)(a(x) \Rightarrow b(x)) \wedge \neg[(\forall x)a(x) \Rightarrow (\forall x)b(x)]$ (negácia 1.)
3. $(\forall x)(a(x) \Rightarrow b(x))$ (lebo 2.)
4. $(\exists x)(a(x) \wedge \neg b(x))$ (lebo 2. + negácia)
5. $a(c) \wedge \neg b(c)$ pre nejaký prvok $c$ (lebo 4.) (tu sme zaviedli do nášho dôkazu **novú** premennú $c$, ktorou sme označili prvok univerza, ktorého existenciu zaručuje výrok 4.)
6. $a(c) \Rightarrow b(c)$ (lebo 2. platí pre všetky prvky univerza, teda aj pre naše $c$)
7. $\neg(a(c) \Rightarrow b(c))$ (negácia 5.) – SPOR s tvrdením 6.

Časti písané šedou slúžia pre lepšie objasnenie, do riešenia takto podrobne netreba písať.

Celé tvrdenie z úlohy 6g) nie je tautológia. To vieme dokázať dosadením, kedy nám vyjde nepravda:

**Riešenie**

Na doméne $\{1, 2\}$ definujme $a(x) \Leftrightarrow x = 1$, $b(x) \Leftrightarrow x = 2$. Po dosadení dostávame výrok

$$\underbrace{(\forall x \in \{1,2\})(x = 1 \Rightarrow x = 2)}_{\text{0, lebo neplatí pre } x=1} \Leftrightarrow (\underbrace{(\forall x \in \{1,2\})(x = 1)}_{\text{0, lebo neplatí pre x = 2}} \Rightarrow \underbrace{(\forall x \in \{1,2\})(x = 2)}_{\text{0, lebo neplatí pre } x=1},$$

ktorého pravdivostná hodnota je 0.

Ako vieme na takéto dosadenie prísť? Výrokové formy si vieme predstaviť ako tabuľky, kde pre každý prvok univerza máme napísané pravdivostnú hodnotu, teda tabuľku s hlavičkou

| $x$ | $a(x)$ | $b(x)$ |
|---|---|---|
| | | |

Poďme teda nájsť také výrokové formy, pre ktoré nebude platiť $(\forall x)(a(x) \Rightarrow b(x)) \Rightarrow ((\forall x)a(x) \Rightarrow (\forall x)b(x))$. Keďže ide o ekvivalenciu. Máme dve možnosti: $1 \Leftrightarrow 0$ alebo $0 \Leftrightarrow 1$. Pri prvej možnosti sa nám dariť nebude (možno aj dôjdeme k sporu a dokážeme, že ide o tautológiu, ako vyššie). Preto skúsime druhú možnosť:

$$\underbrace{(\forall x)(a(x) \Rightarrow b(x))}_{0} \Rightarrow \underbrace{((\forall x)a(x) \Rightarrow (\forall x)b(x))}_{1}$$

Z toho, že $(\forall x)(a(x) \Rightarrow b(x))$ neplatí máme, že platí $(\exists x)(a(x) \land \neg b(x))$, teda existuje riadok tabuľky, v ktorom máme 1 a 0.

| $x$ | $a(x)$ | $b(x)$ |
|---|---|---|
| | 1 | 0 |

Keďže $b(x)$ je už niekedy 0, tak výrok $(\forall x)b(x)$ neplatí. Avšak má platiť $(\forall x)a(x) \Rightarrow (\forall x)b(x)$, preto $(\forall x)a(x)$ tiež neplatí. Teda v niektorom riadku musí mať $a(x)$ nulu.

| $x$ | $a(x)$ | $b(x)$ |
|---|---|---|
| | 1 | 0 |
| | 0 | |

Prešli sme už všetko. Tak nám už ostáva len dokončiť tabuľku – voľné miesto v $b(x)$ vyplníme ľubovoľne a nejako si pomenujeme prvky $x$ univerza, napr. 42 a 47. Dostávame teda výrokové formy definované na $\{42, 47\}$ ako:

| $x$ | $a(x)$ | $b(x)$ |
|---|---|---|
| 42 | 1 | 0 |
| 47 | 0 | 0 |

Pre tie už ľahko overíme, že nám vyjde nepravdivý výrok.

## Niekoľko rád ako dokazovať výroky podľa ich typu

Tu je prehľad základných štruktúr dôkazu podľa typu výroku, ktorý máme dokazovať. Defaultne tak dostaneme priamy dôkaz, ale nič nám nebraní pred dokazovaním si dokazované tvrdenie upraviť na iné (nepriamym dôkazom či matematickou indukciou).

$A \land B$: Dokážme $A$ a potom dokážeme $B$.

$A \lor B$: Rozdelíme dôkaz na dva prípady (napr. ak je nejaké číslo párne alebo nepárne). Z jedného dokážeme $A$ a zdruhého dokážeme $B$.

$A \Rightarrow B$: Predpokladáme, že $A$ platí a dokážeme $B$.

$A \Leftrightarrow B$: Dokážeme $A \Rightarrow B$ a $B \Rightarrow A$.

⋄ V niektorých prípadoch je možné nájsť postupnosť ekvivalentých úprav od výroku $A$ k $B$. Tu však treba byť obozretný, či naozaj všetky sú ekvivalentné. Pre lepšiu kontrolu odporúčame skontrolovať, či sú všetky úvahy správne jedným aj druhým smerom.

$(\forall x)a(x)$: Dokážeme $a(x)$ za použitia premennej $x$.

$(\exists x)a(x)$: Ukážeme platnosť $a(x)$ pre jednu konkrétnu voľbu premennej $x$ (napr. dokážeme $a(47)$). Pri voľbe $x$ môžeme použiť aj premenné, ale iba ak už v našom dôkaze nejaké máme definované (a nesmú byť „zakryté“ kvantifikátorom).

A tu je prehľad základných logických krokov, ktoré vieme počas dokazovania robiť. Opäť pre každý z najčastejších typov výrokov uvádzame, čo z neho možno odvodiť.

$A \wedge B$: Vieme odvodiť platnosť $A$, rovnako aj platnosť $B$.

$A \vee B$: Vieme rozdeliť dôkaz na dve časti, v jednej predpokladáme platnosť $A$ a v druhej platnosť $B$ (vhodné pri dokazovaní výrokov so spojkou alebo).

$A \Rightarrow B$: Ak máme už dokázané $A$, vieme odvodiť platnosť $B$

$A \Leftrightarrow B$: Rovnako ako pri $A \Rightarrow B$, príp. $B \Rightarrow A$.

$(\forall x)a(x)$: Vieme za $x$ dosadiť honotu a odvodiť pre ňu platnosť výroku (napr. $a(47)$, ak sme v celých číslach).

$(\exists x)a(x)$: Zavedieme **novú** premennú, napr. $c$, a odvodíme platnosť $a(c)$.