Dôkazy

Jozef Rajník

Toto je nejaký predbežný môj text k dôkazom, v ktorom chcem pomerne podrobne vysvetliť, ako dokazovanie funguje.

Čo to je vlastne dôkaz? Začneme najprv jedným príbehom. Predstavme si, že sme v škole a so spolužiakmi si v rámci precvičovania riešime túto úlohu.

Úloha 0.1. V obore reálnych čísel vyriešte rovnicu

$$2x - 6 + 4 + x = 2x + 3.$$

Verím, že s takouto úlohou by ste nemali problém. Možno ste ju už vyriešili skôr ako ste začali čítať tento text. No príde náš spolužiak Seki, ktorý doteraz študoval v úplne inej krajine a predvedie nám nasledovné riešenie.

Pokus o riešenie

Pozrime sa na čísla, ktoré máme pri x-kách. Prvé x má pri sebe dvojku, druhé x nemá žiadne číslo – to zodpovedá jednotke, a posledné číslo má opäť dvojku. Sčítame $2 + 1 + 2 = 5$, čiže riešenie tejto rovnice je $x = 5$. Presvedčíme sa o tom skúškou správnosti. Ľavá strana vyjde $2 \cdot 5 - 6 + 4 + 5 = 13$ a pravá strana vyjde $2 \cdot 5 + 3 = 13$, takže skúška nám vyšla.

Čo vravíte na toto riešenie? Je správne? Úplne alebo s výhradami? Alebo je dosť mimo? Ak tvrdíte, že nie je správne, tak prečo? Asi celkom častá odpoveď, čo by sme počuli v tejto situácii je: „To nie je správne riešenie, lebo rovnice sa majú riešiť takto, lebo takto sme to robili v škole!“ Nejde náhodou o matematického génia s inovatívnym spôsobom myslenia?

Táto situácia je v matematike celkom častá a je pre všetkých zúčastnených náročná. Pri takýchto bežných typoch úloh (ako napr. rovnice) aspoň máme výhodu, že málokedy stojíme na strane vymýšľača riešení, lebo sme sa v škole učili postupy, ako sa takéto úlohy majú riešiť. No ak sa matematike venujeme viac, tak stretneme aj úlohy, ktoré nezapadajú do nejakého bežného typu. V takej situácii musíme vymýšľať vlastné riešenia. No a ľahko sa nám tu môže stať, že skončíme ako Seki. Prídeme s geniálnymi nápadmi, ako úloha funguje, ako prísť na správny výsledok, možno niekedy o tom napíšeme aj štvorstranovú esej – a dostaneme za to len zlomok bodov.

Od času napísania tejto rozprávky už ubehli nejaké roky a táto situácia sa stala ešte aktuálnejšou. Miesto spolužiaka Sekiho dnes snáď každý z nás stretáva ChatGPT a podobné iné jazykové modely, ktoré si radi vymyslia rôzne matematické dôkazy. Dostať sa k dôkazom v dnešnej dobe nie je vôbec ťažké. Ťažké však je (zatiaľ) vedieť povedať, či takto vygenerované riešenie je matematicky korektné alebo nie.

1 Základné princípy dokazovania

Začneme s dvomi jednoduchými úlohami, na ktorých si ukážeme, čo je to dôkaz. Pre pestrosť vyberieme pomerne odlišné úlohy – prvá bude z geometrie a druhá sa bude týkať čísel a odmocnín.

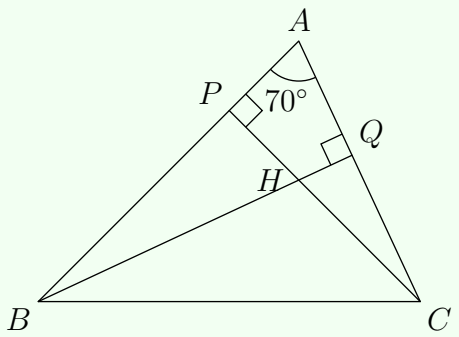
Dôkaz z geometrie

Úloha 1.1. Máme daný trojuholník ABC, kde $\alpha = 70°$, $\beta = 45°$ a $c = 6$ cm. Na strane AB zvolíme bod P tak, aby bol uhol APC pravý. Podobne na strane AC zvolíme bod Q tak, aby uhol AQH bol pravý. Priesečník úsečiek PC a QB označíme H. Dokážte, že $|\sphericalangle PHB| = 70°$.

Takýto typ dôkazovej úlohy je najľahší na pochopenie. Čo ak by úloha znela: „Určite veľkosť uhla PHB?“ Takáto úloha by nemala robiť problémy absolventovi základnej školy. V tomto prípade sa dôkazová úloha líši len v jedinej veci – prezradila nám výsledok. Skúste teda k úlohe pristúpiť takto.

Existuje viacero spôsobov, ako vieme určiť veľkosť uhla. Jedno z nich je rysovanie. Máme zadané presné rozmery trojuholníka a vieme ho narysovať štandardnou konštrukciou (usu). Potom už len narysujeme dve kolmice a odmeriame uhol medzi nimi. Viete, nakoľko je toto riešenie v poriadku? Problémom rysovania je, že nie je presné. Uhol tak nevieme určiť presne, ale len s istou presnosťou. Aj keď uhlomerom odmeriame 70°, nevieme tak vylúčiť, či skutočná veľkosť uhla nie je náhodou 70,2°, príp. nejaké iracionálne číslo. Okrem toho má rysovanie ešte jeden problém v kontexte dôkazov, ktorý ilustrujeme o kúsok neskôr.

Riešenie



Súčet vnútorných uhlov štvoruholníka $APHQ$ je 360°, preto

$$|\sphericalangle PAQ| + |\sphericalangle AQH| + |\sphericalangle QHP| + |\sphericalangle HPA| = 360°.$$

Dosadíme uhly, čo poznáme zo zadania, a máme

$$70° + 90° + |\sphericalangle QHP| + 90° = 360°,$$

čo po úprave dáva

$$|\sphericalangle QHP| = 360° - 70° - 90° - 90° = 110°.$$

Uhol BHP je susedný k uhlu QHP, preto

$$|\sphericalangle BHP| = 180° - |\sphericalangle QHP| = 180° - 110° = 70°.$$

No a takto sme dokázali, že uhol BHP má naozaj veľkosť 70°. Poznamenáme, že existujú aj iné dôkazy, napr. cez výpočet uhla ABQ. Nie každá úloha sa dá takto ľahko prerobiť na výpočtovú, ktorú poznáme. Čo s nasledujúcou úlohou?

Úloha 1.2. Máme daný ostrouhlý trojuholník ABC. Na strane AB zvolíme bod P tak, aby bol uhol APC pravý. Podobne na strane AC zvolíme bod Q tak, aby uhol AQH bol pravý. Priesečník úsečiek PC a QB označíme H. Dokážte, že $|\sphericalangle PHB| = |\sphericalangle BAC|$.

Na rozdiel od predošlej úlohy je táto *všeobecná*. To nám mimo iné zabraňuje riešenie rysovaním. My

si narysovať vieme len nejaký *konkrétny* trojuholník. V ňom vieme (približne) overiť, že uhly PHB a BAC majú rovnakú veľkosť, prípadne si vieme takto narysovať aj niekoľko ďalších trojuholníkov. Všetkých možných trojuholníkov je však nekonečne veľa. Takto teda nezískame istotu, že dokazované tvrdenie bude platiť v každom z nich.

Avšak keď sa pozrieme pozorne na predošlé riešenie, tak si môžeme všimnúť, že sme v ňom nijako nevyužili veľkosť uhla β či dĺžku strany c. Využívali sme len veľkosť uhla α. Čo ak by uhol α mal inú veľkosť? Môžete si skúsiť vyriešiť dokázať tvrdenie pre iné veľkosti uhla α (pripomíname, že zadania od nás vyžaduje len ostré uhly). Aj bez riešenia si však môžeme všimnúť, že to pôjde podobne. Výpočty z predošlého riešenia vieme totiž robiť pomocou premennej α. Pre názornejšiu ukážku uvedieme vľavo riešenie predošlej, konkrétnej úlohy a vpravo riešenie tejto všeobecnej verzie.

Riešenie pre $\alpha = 70°$

Súčet vnútorných uhlov štvoruholníka $APHQ$ je $360°$, teda

$$70° + 90° + |\sphericalangle QHP| + 90° = 360°,$$

čo po úprave dáva

$$|\sphericalangle QHP| = 360° - 70° - 90° - 90° = 110°.$$

Zo susedných uhlov BHP a QHP:

$$|\sphericalangle BHP| = 180° - |\sphericalangle QHP| = 70°.$$

Riešenie úlohy 1.2

Nech $|\sphericalangle BAC| = \alpha$.
Súčet vnútorných uhlov štvoruholníka $APHQ$ je $360°$, teda

$$\alpha + 90° + |\sphericalangle QHP| + 90° = 360°,$$

čo po úprave dáva

$$|\sphericalangle QHP| = 360° - \alpha - 90° - 90° = 180° - \alpha.$$

Zo susedných uhlov BHP a QHP:

$$|\sphericalangle BHP| = 180° - (180° - \alpha) = \alpha.$$

Toto je častá čerta dôkazových úloh – sú väčšinou všeobecné. Zahŕňajú veľmi veľa, často až nekonečne veľa prípadov, ktoré treba pokryť. Preto pri dokazovaní takýchto tvrdení potrebujeme použiť všeobecné metódy a úvahy, čo je často sprevádzané aj použitím nejakých písmeniek, teda premenných.

Môžeme si teda všimnúť, že takéto dokazovanie sa v zásade ničím nelíši od bežného riešenia úloh – používame znalosti z matematiky, ktoré poznáme, aby sme sa dostali k tomu, čo chceme dokázať. V tejto úlohe sme využívali súčet uhlov v štvoruholníku a vlastnosti susedných uhlov.

Nerovnosti s číslami a odmocninami

Úloha 1.3. Dokážte, že platí

$$\sqrt{60} > \sqrt{13} + \sqrt{17}.$$

Oproti úlohe 1.1 máme teraz výrazne jednoduchšie zadanie. Tiež si vieme túto úlohu predstaviť ako nedôkazovú: „Ktoré z čísel $\sqrt{60}$ a $\sqrt{13} + \sqrt{17}$ je väčšie?“ Opäť nám tu formulácia úlohy prezrádza odpoveď. Vedeli by ste to zistiť? Akým postupom?

Jedna možnosť je využiť kalkulačku. To je podobný prístup ako rysovanie v geometrii – nie je presný a ťažko sa zovšeobecňuje (čo budeme neskôr potrebovať. Preto kalkulačky na chvíľu odložíme (resp. aspoň tlačidlo s odmocninou) a skúsime prísť s iným prístupom. My tiež jeden uvedieme.

Pokus o dôkaz 1

Zo školy vieme, že nerovnosti môžeme nejako 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.

Tak čo vravíte na naše riešenie? Je to podľa vás korektný dôkaz? Už druhá otázka nám napovedá, čo to asi dôkaz bude. Z jedného príkladu sa ťažko rozmýšľa, tak vám ešte pomôžeme druhým.

Úloha 1.4. Dokážeme, že $\sqrt{2} > \sqrt{3}$. V čom je tento dôkaz chybný?

Pokus o dôkaz 2

Opäť na to pôjdeme rovnako ako v predošlom dôkaze. 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 $\sqrt{2} > \sqrt{3}$.

Druhý pokus o dôkaz je zjavne nesprávny, nakoľko sme ním „dokázali“ nepravdivé tvrdenie $\sqrt{2} > \sqrt{3}$ (korektným dôkazom predsa nemôžeme dokázať nepravdivé tvrdenie). Avšak prvý pokus o dôkaz sa principiálne od druhého pokusu nelíši. Čiže tiež nebude úplne v poriadku. Poďme sa pozrieť bližšie na to, prečo je druhý pokus zlý.

Výhodou tejto úlohy je, že ľahko vieme kalkulačkou vyhodnotiť pravdivosť každého nerovnosti, ktorý sa v našom „dôkaze“ vyskytol. Problém nastáva medzi nerovnosťami

$$\sqrt{2} - \sqrt{3} > 0 \qquad \text{a} \qquad (\sqrt{2} - \sqrt{3})^2 > 0.$$

Prvý z nich neplatí a druhá platí. Problém je v tom, že nerovnosti nemôžeme len tak „nejako upravovať“. Musíme si dávať pozor na to, aké úpravy používame. Zo školy by ste si mohli pamätať, že existuje niečo také ako *ekvivalentné úpravy*. Umocňovanie na druhú vo všeobecnosti nie je ekvivalentná úprava.

Čo to ale ekvivalentné úpravy sú? Jednoducho povedané sú to také úpravy, ktoré nám nezmenia platnosť nerovnosti, resp. rovnosti. Napr. pripočítanie ľubovoľného reálneho čísla k obom stranám

nerovnosti je ekvivalentná úprava. Ak nerovnosť platí, tak ostane platiť aj potom. A ak neplatí, tak aj po pripočítaní bude neplatiť. Umocňovanie na druhú nie je ekvivalentná operácia, lebo nerovnosť $-2 < 1$ platí, ale jej umocnením dostaneme neplatnú nerovnosť $4 < 1$.

Nie je to však stratené. Ak sa však obmedzíme len na nezáporné čísla, tak umocňovanie na druhú je ekvivalentnou úpravou. Prečo? Budeme to považovať za známy fakt, ktorý vychádza z vlastností umocňovania na druhý. Nahliadnuť to môžeme napr. tým, že jeden štvorec má menšiu stranu ako druhý štvorec práve vtedy, keď má menší obsah ako druhý; alebo tiež z toho, že funkcia $y = x^2$ je na obore $\mathbb{R}^+$ rastúca.

Náš dôkaz teda vieme opraviť takto. Ekvivalentnosť úprav vieme napríklad naznačiť poznámkou na konci (alebo na začiatku) alebo aj uvedením symbolu ekvivalencie medzi riadkami. Uvedieme obe možnosti.

Dôkaz úlohy 1.3

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

Keďže pri oboch umocňovaniach sme mali na oboch stranách kladné čísla, všetky použité úpravy boli ekvivalentné.

Dôkaz úlohy 1.3

$$\begin{aligned}
\sqrt{60} &> \sqrt{13} + \sqrt{17} \qquad |^2 \\
&\Updownarrow \text{ lebo } \sqrt{60} > 0,\ \sqrt{13} + \sqrt{17} > 0 \\
\left(\sqrt{60}\right)^2 &> \left(\sqrt{13} + \sqrt{17}\right)^2 \\
&\Updownarrow \\
60 &> 13 + 2\sqrt{13}\sqrt{17} + 17 \\
&\Updownarrow \\
60 &> 30 + 2\sqrt{221} \qquad | -30 \\
&\Updownarrow \\
30 &> 2\sqrt{221} \qquad | /2 \\
&\Updownarrow \\
15 &> \sqrt{221} \qquad |^2 \\
&\Updownarrow \text{ lebo } 15 > 0,\ \sqrt{221} > 0 \\
225 &> 221
\end{aligned}$$

Upozornenie

Na používanie umocňovania na druhú ako ekvivalentnej úpravy, ak sú obidve strany nezáporné, si treba dať pozor. Nejde o štandardnú ekvivalentnú úpravu. Môže sa teda stať, že vám učiteľ v škole takýto postup neuzná (napr. pri riešení rovníc s odmocninami)

Čo sú to vlastne dôkazy?

Tvrdenia, ktoré dokazujeme, sa nazývajú v matematike *výroky*. Ide o tvrdenia, o ktorých má zmysel uvažovať, či sú pravdivé alebo nepravdivé. Spravidla majú podobu oznamovacích viet, no jeden výrok môže byť zložený aj z viacerých viet – ako v úlohe 1.1, kde do výroku treba zahrnúť celé zadanie so všetkými predpokladmi. To, či je výrok pravdivý alebo nepravdivý sa nazýva *pravdivostná hodnota*. Tá musí pri výroku byť jednoznačne určiteľná, teda musí nadobudnúť práve jednu z hodnôt pravda, nepravda.

Okrem toho, že dokazujeme výroky, tak aj v samotných našich dôkazov sa objavilo viacero výrokov, napr. $|\sphericalangle QHP| = 110°$ či $60 > 30 + 2\sqrt{221}$. Za výroky teda môžeme považovať naše jednotlivé kroky dokazovania. Aby sme mohli hovoriť o dôkaze, tak nemôžeme tieto výroky písať len tak halabala. Dôležité sú vzťahy medzi nimi (ako sme poukázali už pri ekvivalentných a neekvivalentných úpravách). Tieto vzťahy možno vyjadriť rôznymi *výrokovými spojkami*. Tie vieme umiesť medzi dva výroky a vytovríme tak zložený výrok:

„a“

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

„alebo“

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

„ak ..., tak“

A	B	$A \Rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

„práve vtedy, keď“

A	B	$A \Leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Pomocou týchto logických spojok vieme aj poukázať na problém nesprávneho dôkazu tvrdenia $\sqrt{2} > \sqrt{3}$. Problém bol medzi výrokmi $\sqrt{2}-\sqrt{3} > 0$ a $(\sqrt{2}-\sqrt{3})^2 > 0$. V akom vzťahu sú tieto dva výroky? Akú logickú operáciu či úvahu sme použili? Vzťah tam máme nasledovný:

$$\sqrt{2} - \sqrt{3} > 0 \Rightarrow (\sqrt{2} - \sqrt{3})^2 > 0.$$

Keď sa nad tým zamyslíme kus všeobecnejšie, túto implikáciu vieme chápať aj nasledovne: „Ak máme kladné číslo, tak jeho druhá mocnina je tiež kladná.“ (Pomocou symbolov by sme toto tvrdenie vedeli zapísať ako $\forall x \in \mathbb{R}\colon x > 0 \Rightarrow x^2 > 0$. – k takýmto zápisom je viac nižšie.)

Problém je však ten, že táto implikácia pripúšťa, že z nepravdy vyplýva pravda. Keď vieme, že platí $(\sqrt{2} - \sqrt{3})^2 > 0$, tak to nám nič nehovorí o tom, či platí $\sqrt{2} - \sqrt{3} > 0$ (pozriete si riadok $0 \Rightarrow 1$ v tabuľke pre implikáciu).

Pri dokazovaní nerovnosti sme hovorili o ekvivalentných úpravách. Ekvivalencia dvoch výrokov znamená, že majú rovnakú pravdivostnú hodnotu. O výroku $225 > 221$ vieme, že je pravdivý. Pomocou ekvivalencií vieme tak túto pravdivosť dostať až k dokazovanému výroku $\sqrt{60} > \sqrt{13} + \sqrt{17}$. Využili sme teda, že tento výrok je ekvivalentný pravdivému výroku, a preto musí byť aj on sám pravdivý.

Avšak ekvivalentné úpravy nie sú až tak nutné. Pozrime sa na to, ako sme dospeli k záveru, že dokazovaný výrok je pravdivý? Jeho pravdivosť sme preniesli od zjavne pravdivého výroku $255 > 221$ k dokazovanému výroku. A pri tomto „prenose pravdy“ nám stačí, aby sme mali všade len implikácie. A práve tak funguje *priamy dôkaz*: ide o sériu implikácií od pravdivého výroku k dokazovanému výroku. Pri dôkaze nám teda stačí skontrolovať, či smerom „zdola nahor“ platia všetky implikácie. Dôkaz vieme zapísať teda tak ako v riešení vľavo. Ak by sme však chceli byť poriadni, tak dôkaz zapíšeme v poradí, ktoré rešpektuje smer implikácií.

Dôkaz podľa smeru implikácií

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

S takýmito dôkazmi sa vieme často stretnúť v matematických textoch. Ako plot twist z veľkolepého seriálu, často nás dôkaz začiatku prekvapí náhodným tvrdením typu $225 > 221$, ktoré na prvý pohľad vôbec nesúvisí s dokazovaným tvrdením.

Dôkaz 3: písaný opačným smerom s vyznačenými implikáciami

$$
\begin{aligned}
\sqrt{60} &> \sqrt{13} + \sqrt{17} \qquad |^2 \\
&\Uparrow \text{lebo } \sqrt{60} > 0,\ \sqrt{13} + \sqrt{17} > 0 \\
\left(\sqrt{60}\right)^2 &> \left(\sqrt{13} + \sqrt{17}\right)^2 \\
&\Uparrow \\
60 &> 13 + 2\sqrt{13}\sqrt{17} + 17 \\
&\Uparrow \\
60 &> 30 + 2\sqrt{221} \qquad | -30 \\
&\Uparrow \\
30 &> 2\sqrt{221} \qquad | /2 \\
&\Uparrow \\
15 &> \sqrt{221} \qquad |^2 \\
&\Uparrow \text{lebo } 255 > 0,\ 221 > 0 \\
255 &> 221
\end{aligned}
$$

Úpravy naznačené za zvislou čiarou nie sú napísané zrovna najkorektnejšie. Korektnejšie by bolo písať opačné úpravy, ktoré robíme zdola nahor. Resp. môžeme si ich aj úplne odpustiť a nepísať ich. Nejde však o žiadnu tragédiu.

Na záver si teda zhrnieme, ako by po takejto stránke mal vyzerať dôkaz, resp. takáto základná forma dôkazu, ktorá sa nazýva *priamy dôkaz*. Neskôr sa zoznámime aj s inými typmi dôkazov.

Priamy dôkaz

Priamy dôkaz výroku V je konečná postupnosť výrokov, ktorá sa končí výrokom V a pre každý výrok tejto postupnosti platí niektorý z nasledovných bodov:

(i) je axióma,

(ii) je všeobecne známe alebo už dokázané tvrdenie,

(iii) vyplýva (je logickým dôsledkom) z predchádzajúcich výrokov tejto postupnosti.

V exaktnej matematickej logike sa bod (ii) vynecháva. Formálne vzaté musí každý dôkaz začínať axiómami. Potom sú však dôkazy dlhé. V praxi preto často nezachádzame až k axiómam. Napokon, každý takýto neporiadny dôkaz vieme prerobiť tak, že ku každému známemu tvrdeniu pridáme jeho dôkaz.

Ako na dôkaz nerovnosti kalkulačkou – dá sa to aj bez ekvivalentných úprav

Pozrieme sa ešte na pár ďalších pokusov o dôkaz. Na počítanie odmocnín máme predsa kalkulačku, tak to do nej naťukáme! Ako však takýto postup správne zapísať? Sú nasledovné dva postupy korektné?

Pokus o riešenie 3

Pomocou kalkulačky vypočítame:
$\sqrt{60} = 7{,}74596669$
$\sqrt{13} = 3{,}60555128$
$\sqrt{17} = 4{,}12310563$
Teda $\sqrt{13} + \sqrt{17} = 3{,}60555128 + 4{,}12310563 = 7{,}72865691$

Pokus o riešenie 4

Pomocou kalkulačky vypočítame: $\sqrt{60} \doteq 7{,}74596669$
$\sqrt{13} \doteq 3{,}60555128$
$\sqrt{17} \doteq 4{,}12310563$
Teda $\sqrt{13} + \sqrt{17} \doteq 3{,}60555128 + 4{,}12310563 = 7{,}72865691$

V pokuse 3 by mal byť problém zjavný: predsa $\sqrt{60} = 7{,}74596669$ nie je pravdivý výrok, nie je to presná hodnota $\sqrt{60}$, ale len približná. Tento problém je už opravený v pokuse 4, kde naozaj je pravda $\sqrt{60} \doteq 7{,}74596669$. Problém je tu však v tom, že čo znamená $\sqrt{60} \doteq 7{,}74596669$? Vieme, že symbol $\doteq$ znamená *približne sa rovná*, ale vieme, čo presne tento pojem znamená po matematickej stránke? Alebo vieme, ako a či vôbec môžeme približné čísla sčítavať? Problém je práve v sčítavaní: pri našom chápaní znaku $\doteq$ ako zaokrúhľovania na dve desatinné miesta platí $\sqrt{13} \doteq 3{,}61$ a $\sqrt{30} = 5{,}48$. Na základe našej úvahy o sčítavaní (ktorú sme použili na konci pokusu 4) by sme tak dostali $\sqrt{13} + \sqrt{30} \doteq 9{,}09$. To však nie je pravda, lebo $\sqrt{13} + \sqrt{30} \doteq 9{,}08$ (overte si všetko na kalkulačke).

Upozorníme, že toto je častý problém pri mnohých dôkazoch, ktorý spočítava v tom, že používame pojmy alebo symboly, ktorým poriadne nerozumieme alebo nie sú jasne definované. V tomto prípade ide len o technický detail, no sú situácie, kedy takéto riešenia majú ďaleko od poriadneho dôkazu, hoci po intuitívnej stránke vyzerajú veľmi presvedčivo.

Tento pokus o dôkaze by sme vedeli opraviť, ak správne použijeme pravidlá pre počítanie s približnými číslami. No netreba vôbec používať takýto overkill. Ukážeme si jednoduchšie riešenie. Hlavná myšlienka spočíva v tom, že problematický vzťah $\doteq$ nahradíme jasnými vzťahmi porovnávania, s ktorými vieme pracovať.

Dôkaz 4

1. $60 > 59{,}9076$ (zjavná pravda)
2. $\sqrt{60} > 7{,}74$ (odmocnenie 1.)
3. $13{,}0321 > 13$ (zjavná pravda)
4. $3{,}61 > \sqrt{13}$ (odmocnenie 3.)
5. $17{,}0569 > 17$ (zjavná pravda)
6. $4{,}13 > \sqrt{17}$ (odmicnenie 5.)
7. $7{,}74 = 3{,}61 + 4{,}13 > \sqrt{13} + \sqrt{17}$, lebo je to súčet 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 $\forall a, b, c \in \mathbb{R}$).

Pri tomto dôkaze pekne vidíme, že dôkazy vôbec nemusia byť lineárne. Nové tvrdenie v dôkazovej postupnosti nemusí vyplývať iba z predošlého, ale môže vyplývať aj z ľubovoľných už dokázaných tvrdení. Stále platí, že takto vieme „preniesť“ pravdu od zjavne pravdivých tvrdení (tvrdenia 1., 3., 5,) postupne k všetkým ostatným a teda aj k dokazovanému tvrdeniu.

Ako takéto dôkazy zapisovať? 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.

Dôkaz 5

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

Úloha 1.5. Dokážte, že platí:

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

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

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

Nerovnosť s písmenkami

A opäť si vyskúšame všeobecnejšiu verziu predošlej úlohy

Úloha 1.6. Dokážte, že pre každé nezáporné reálne číslo x platí

$$\sqrt{4x+8} > \sqrt{x} + \sqrt{x+4}.$$

Toto je pomerne typický dôkaz, s ktorým sa stretneme v matematike – máme dokázať, že niečo platí pre *všetky* čísla z nejakej množiny (teraz všetky nezáporné reálne čísla). Ako niečo také dokázať? „Jednoduchá“ predstava je, že vyskúšame všetky hodnoty premennej. Teda $x = 0$, $x = 9$, $x = 13$ (takto dostaneme priamo úlohu 1.3), ale aj také hodnoty ako $x = \sqrt{2}$, $x = \pi$ a ešte divokejšie. Samozrejme, vyskúšať nekonečne veľa čísel nie je v našich silách. No predstava takéhoto skúšania nám niekedy vie pomôcť.

Pozrime sa na dôkaz tvrdenia pre $x = 13$, teda na riešenie úlohy 1.3. Napravo od neho ponecháme premennú x v našej nerovnosti a pokúsime sa robiť rovnaké úpravy s touto premennou.

$$\begin{aligned}
\sqrt{60} &> \sqrt{13} + \sqrt{17} \qquad |^2 \\
&\Uparrow \text{ lebo } \sqrt{60} > 0,\ \sqrt{13} + \sqrt{17} > 0 \\
\left(\sqrt{60}\right)^2 &> \left(\sqrt{13} + \sqrt{17}\right)^2 \\
&\Uparrow \\
60 &> 13 + 2\sqrt{13}\sqrt{17} + 17 \\
&\Uparrow \\
60 &> 30 + 2\sqrt{221} \qquad | -30 \\
&\Uparrow \\
30 &> 2\sqrt{221} \qquad | /2 \\
&\Uparrow \\
15 &> \sqrt{221} \qquad |^2 \\
&\Uparrow \text{ lebo } 255 > 0,\ 221 > 0 \\
255 &> 221
\end{aligned}$$

$$\begin{aligned}
\sqrt{4x+8} &> \sqrt{x} + \sqrt{x+4} \qquad |^2 \\
&\Uparrow \text{ lebo } \sqrt{4x+8} > 0,\ \sqrt{x} + \sqrt{x+4} > 0 \\
\left(\sqrt{4x+8}\right)^2 &> \left(\sqrt{x} + \sqrt{x+4}\right)^2 \\
&\Uparrow \\
4x+8 &> x + 2\sqrt{x}\sqrt{x+4} + x + 4 \\
&\Uparrow \\
4x+8 &> 2x + 4 + 2\sqrt{221} \qquad | -(2x+4) \\
&\Uparrow \\
2x+4 &> 2\sqrt{x(x+4)} \qquad | /2 \\
&\Uparrow \\
x+2 &> \sqrt{x(x+4)} \qquad |^2 \\
&\Uparrow \text{ lebo } x(x+4) > 0,\ x+2 > 0 \\
(x+2)^2 &> x(x+4)
\end{aligned}$$

To vyzerá celkom sľubne. Podarilo sa nám dopracovať k pomerne jednoduchej nerovnosti. Narozdiel od čísel, tu nevidíme priamo, či táto nerovnosť platí alebo nie. Ale môžeme ju ďalej upravovať:

$$\begin{gathered}
(x+2)^2 > x(x+4) \\
\Uparrow \\
x^2 + 4x + 4 > x^2 + 4x \\
\Uparrow \\
4 > 0
\end{gathered}$$

A takto sme sa už dostali k niečomu, čo platí. A čo je dôležité, nerovnosť $4 > 0$ platí pre každé nezáporné reálne číslo x (resp. inak povedané, platí nezávisle na hodnote reálneho čísla x). Týmto sme všeobecne dokázali dokazované tvrdenie. A ani to nebolelo. Robili sme vlastne to isté, ako keby tam bolo číslo. Dôležité bolo, že sme používali úpravy, ktoré nezávisia na presnej hodnote premenných, nanajvýš na ich nezápornosti, čo sme vo všetkých prípadoch vedeli zaručiť, keďže x bolo podľa zadania nezáporné. Pre porovnanie, dôkaz s odhadovaním odmocnín by šlo zovšeobecniť ťažko – čo by sme napísali miesto $\sqrt{60} > 7{,}74$? (Napriek tomu to nie je nemožné. Aj rôzne odhady výrazov inými sa pri dôkazoch využívajú.)

Dôkaz z deliteľnosti

Pre pestrosť zájdeme do ďalšej oblasti a skúsime dokázať tvrdenie o deliteľnosti.

Úloha 1.7. Dokážte, že pre každé prirodzené číslo n je číslo $n^3 - n$ deliteľné a) dvomi, b) tromi, c) šiestimi.

Tálesova kružnica

Pre lepšiu pestrosť si ukážeme podobný prístup na úlohe z geometrie. Pri nej zabudneme na to, že poznáme vlastnosti Tálesovej kružnice.

Úloha 1.8. Máme danú úsečku AB dlhú 6 cm. V jej strede S spravíme kružnicu s polomerom 3 cm. Na kružnici k zvolíme bod C tak, aby $|\sphericalangle CAB| = 40°$. Dokážte, že uhol ACB je pravý.

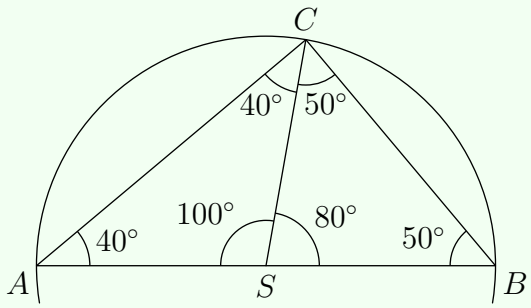
Poznámka

Aký výrok dokazujeme v tejto úlohe? Žeby výrok „Uhol ACB je pravý“? Toto nie je výrok, lebo nevieme, čo sú body A, B, C. V skutočnosti je týmto výrokom skoro celé zadanie, teda napr.: „Máme danú úsečku AB dlhú 6 cm. V jej strede S spravíme kružnicu s polomerom 3 cm. Na kružnici k zvolíme bod C tak, aby $|\sphericalangle CAB| = 40°$. Potom uhol ACB je pravý.“ Toto je príklad toho, že definícia „Výrok je oznamovacia veta...“ nie je presná. V tejto situácii sme totiž výrok vyjadrili viacerými vetami. A toto sa bežne deje aj inde v matematike, nakoľko matematici bežne pracujú aj s výrokmi na niekoľko riadkov.

Toto je opäť príklad úlohy, v ktorej sa dá dôkazový rozmer ľahko odstrániť – stačí sa spýtať otázku: „Zistite veľkosť uhla ACB.“ Opäť nám dôkazová formulácia úlohy prezradila výsledok. Aj túto úlohu si vieme ľahko predstaviť. Zadanie hovorí totiž o jedinečnej konfigurácii. Nie je problém si túto situáciu narysovať. V nej dokonca môžeme odmerať veľkosť uhla ACB a takto sa presvedčiť o pravdivosti tvrdenia. Avšak nie dokázať ho, lebo rysovanie nie je presné (je ešte menej presné ako kalkulačka). No nie je náročné prísť aj s presným riešením.

Riešenie

Keďže body A, B, C ležia na kružnici k, tak $|SA| = |SB| = |SC|$.
Trojuholník ASC je tak rovnoramenný, teda $|\sphericalangle ACS| = |\sphericalangle CAB| = 40°$.
$|\sphericalangle ASC| = 180° - |\sphericalangle SCA| - |\sphericalangle CAS| = 180° - 40° - 40° = 100°$ (súčet uhlov v trojuholníku ASC).
$|\sphericalangle CSB| = 180° - 100° = 80°$ (susedný uhol).
$|\sphericalangle SCB| = |\sphericalangle SBC| = (180° - 80°)/2 = 50°$ (z rovnoramenného trojuholníka SBC).
$|\sphericalangle ACB| = |\sphericalangle ACS| + |\sphericalangle SCB| = 40° + 50° = 90°$.



Porovnajte si štruktúru tohto dôkazu s tým, čo už viete o priamom dôkaze. Vychádzame z toho, o čom vieme, že už platí. Teraz sú to veci, ktoré máme v zadaní (napr. že body A, B, C, ležia na kružnici) a z nich odvodzujeme postupne ďalšie a ďalšie tvrdenia. Skončíme pritom, čo máme dokázať, teda že $|\sphericalangle ACB| = 90°$. Dokonca v tomto prípade je prirodzené tvoriť dôkaz v jeho správnom smere.

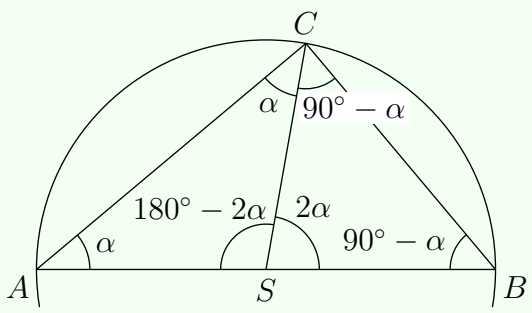
Čo ak by sme však mali dokázať o niečo všeobecnejšie tvrdenie? Priamočiara vec je, že môžeme vypustiť dĺžku úsečky AB. Avšak dokonca ani veľkosť uhla CAB nepotrebujeme.

Úloha 1.9. Máme danú úsečku AB dlhú 6 cm. V jej strede S spravíme kružnicu s polomerom 3 cm. Na kružnici k zvolíme ľubovoľný bod C rôzny od bodov A, B. Dokážte, že uhol ACB je pravý.

Slovíčkom *ľubovoľný* v zadaní hovoríme, že tvrdenie máme dokázať pre všetky také body C. Aj v tomto prípade tak vieme spraviť pomerne priamočiarou úpravou konkrétneho dôkazu. Ak poznáme uhol CAB, tak dôkaz ide ľahko. Ak ho nepoznáme, tak si ho vieme označiť a pracovať s týmto označením.

Riešenie

Nech $\alpha = |\sphericalangle CAB|$. Keďže body A, B, C ležia na kružnici k, tak $|SA| = |SB| = |SC|$.
Trojuholník ASC je tak rovnoramenný, teda $|\sphericalangle ACS| = |\sphericalangle CAB| = \alpha$.
$|\sphericalangle ASC| = 180° - |\sphericalangle SCA| - |\sphericalangle CAS| = 180° - \alpha - \alpha = 180° - 2\alpha$ (súčet uhlov v trojuholníku ASC).
$|\sphericalangle CSB| = 180° - (180° - 2\alpha) = 2\alpha$ (susedný uhol).
$|\sphericalangle SCB| = |\sphericalangle SBC| = (180° - 2\alpha)/2 = 90° - \alpha$ (z rovnoramenného trojuholníka SBC).
$|\sphericalangle ACB| = |\sphericalangle ACS| + |\sphericalangle SCB| = \alpha + (90° - \alpha) = 90°$.



2 Výrokové formy a kvantifikátory

Na predošlých príkladoch sme videli, že dokazovať všeobecné tvrdenie nie je až také strašné. Stačí robiť to isté, čo by sme robili s číslami, len to robíme s písmenkami. Toto však boli len isté typy dôkazov. Dôkazy s písmenkami sa však niekedy vedia celkom zamotať.

Celkom typická matematická vec s písmenkami môže vyzerať napríklad takto:

$$x > 5.$$

Alebo slovne: *Číslo x je väčšie ako* 5. O čo ide z pohľadu výrokovej logiky? Je to veta, ale jej pravdivostnú hodnotu určiť nevieme – bráni nám v tom premenná. Nejde teda o výrok. Vo výrokovej logike sa niečo takéto volá *výroková formula*. Ide o vetu, ktorá obsahuje premenné (jednu alebo viac), za ktoré keď dosadíme, tak dostaneme výrok. V tomto prípade napr. dosadením môžeme dostať napr. výroky $6 > 5$, $2 > 5$, $-9 > 5$ či $\pi + \sqrt{3 - \log_7 3} > 5$.

Výroková forma však potrebuje však ešte jednu vec. Musíme špecifikovať, čo za premenné do nej môžeme dosadzovať. Lebo veta $\heartsuit > 5$ asi nie je výrokom (aj keď pri trochu inom prístupe by sme ju mohli prehlásiť za nepravdivý výrok).

Výrokové formuly budeme označovať malým písmenkom, za ktoré do zátvorky napíšeme, ktoré premenné obsahuje. Napríklad:

- $a(x) \equiv x > 5$, $x \in \mathbb{R}$;
- $b(y) \equiv 6 \mid y$, $y \in \mathbb{N}$;
- $c(k, l) \equiv \mathrm{NSD}(a, b) = 1$, $a, b \in \{2, 3, 4, 5, 6, 7, 8, 10\}$;
- $d(x, y) \equiv x$ je otcom y, x, y sú ľudia;
- $e(x, y, z) \equiv x^2 + 2y^4 - \sqrt{5z} = 47xy$, $x, y \in \mathbb{R}$, $z \in \mathbb{R}^+$.

Okrem dosadenia však existuje ďalší spôsob, ako z výrokovej formy $p(x)$ spraviť výrok. Ide o *kvantifikovanie*. V matematike poznáme dva základné spôsoby, ako môžeme kvantifikovať. Vieme tak dostať výrok

- „Pre všetky x z množiny M platí $p(x)$.“ – symbolicky zapisujeme $\forall x \in M : p(x)$.
- „Existuje x z množiny M platí $p(x)$.“ – symbolicky zapisujeme $\exists x \in M : p(x)$.

Pri kvantifikácii je dôležité uviesť množinu, cez ktorú kvantifikujeme.Predsa len $\forall x \in \mathbb{Z}^+ : 2x > x$ je niečo iné ako $\forall x \in \mathbb{R} : 2x > x$. Tieto výroky môžeme prečítať slovne aj nasledovne: „Dvojnásobok ľubovoľného *prirodzeného* čísla je väčší ako číslo samotné“ a „Dvojnásobok ľubovoľného *reálneho* čísla je väčší ako číslo samotné“. Tu vidíme aj to, že pri čítaní takýchto výrokov, nemusíme dodržať presnú formuláciu „Pre všetky...“ – niekedy tak dostaneme výrok ľahší na pochopenie.

Poznámka

Uvádzanie množín pri kvantifikátoroch má svoje výnimky. Môžete sa stretnúť aj zo zápismi štýlu $\forall x : p(x)$, kde žiadnu množinu neuvádzame. Toto možno interpretovať dvomi spôsobmi. Prvým vysvetlením je, že týmto zápisom myslíme kvantifikovanie cez všetky x, pre ktoré je výroková formula $p(x)$ definovaná. Druhým kontextom, kde môžete takýto zápis stretnúť je, keď je na inom mieste dané, v akej množine prvkov pracujeme. Ak máme povedané, že pracujeme iba s celými číslami, tak každý kvantifikátor $\forall x$ či $\exists x$ bez množiny kvantifikuje cez množinu celých čísel.

Okrem toho sa zápisy kvantifikátorov bez množín používajú aj pri poriadnom štúdiu výrokovej logiky. Tento prístup slúži hlavne na oddelenie výrokov a množín, aby sa nám nemiešali matematické oblasti. S týmto sa môžete stretnúť napr. keď si pozriete ľubovoľnú sadu axióm k nejakej matematickej teórii, napr. Zermelovu-Fraenkelovu sadu axióm k teórii množín – ako by sme v nich kvantifikovali cez množiny, keďže pomocou týchto axióm definujeme samotné množiny? Existuje vlastne množina všetkých množín, cez ktorú by sme tu mohli kvantifikovať?

Dôkazy kvantifikovaných výrokov

Teraz sa pozrieme na to, ako dokazovať pravdivosť alebo nepravdivosť výrokov. Teda, pozrieme sa rovno na zisťovanie pravdivostnej hodnoty. No hoci úlohy budú o zisťovaní, budeme v nich chcieť úplné riešenie vrátane dôkazu.

Úloha 2.1. Určte pravdivostnú hodnotu výroku

$$\exists x \in \mathbb{R} \colon 3x + 2 > 2x + 5.$$

Opäť vám ponúkame dva pokusy o riešenie.

Pokus o riešenie 1

Nerovnosť

$$3x + 2 > 2x + 5$$

si odčítaním $2x$ a odčítaním 2 ekvivalentne upravíme na

$$x > 3.$$

Toto, a teda aj nerovnosť $3x + 2 > 2x + 4$ platí pre všetky reálne čísla väčšie ako 3, teda výrok je pravdivý.

Pokus o riešenie 2

Sčítame všetky čísla v zadaní:

$$3 + 2 + 2 + 5 = 12.$$

Dosadáme $x = 12$, čím máme na ľavej strane $3 \cdot 12 + 2 = 38$ a na pravej strane $2 \cdot 12 + 5 = 29$. Vyšlo nám $38 > 29$, čo je pravda, teda také $x \in \mathbb{R}$, pre ktoré platí $3x + 2 > 2x + 5$ existuje. Výrok teda platí.

Možno vás teraz prekvapíme, ale správne sú teraz obe riešenia. A možno vás ešte prekvapíme aj tým, keď povieme, že druhý pokus je o niečo lepší. Spomeňme si, že dôkaz slúži na presvedčenie čitateľa o pravdivosti nášho tvrdenia. A ako niekoho presvedčíme o existencii niečoho? Najjednoduchšie tak, že mu to ukážeme.

Prvé riešenie je zbytočne zložité. Možno je to tým, že keď vidíme nerovnicu, tak máme nutkanie ju vyriešiť zaužívaným školským postupom. Takto si však pridávame prácu a tiež zvyšujeme šancu na to, že sa niekde pomýlime. Isto, teraz nám to príde banálne a irelevantné. No táto poznámka bude relevantná hlavne pri zložitejších úlohách.

Ideálne riešenie takejto úlohy teda obsahuje len posledné dva riadky. Dokonca ich vieme skrátiť do nasledovného tvaru.

Riešenie úlohy 2.1

Pre $x = 12$ máme $38 > 29$, teda výrok platí.

Objavili sme tak v podstate najjednoduchšiu formu dôkazu, ktorú vieme zhrnúť asi takto.

Dôkaz existenčného výroku

Pravdivosť tvrdenia tvaru $\exists x \in M \colon p(x)$ dokazujeme tak, že uvedieme príklad konkrétneho prvku x z množiny M a dokážeme, že pre tento prvok platí $p(x)$. Pri dôkaze je ideálne dodržať štruktúru (c nahradíme konkrétnym prvkom):

Nech $x = c$. Potom … [dôkaz $p(c)$].

Hoci tento typ dôkazu vyzerá jednoducho, nemusí tomu byť vždy tak. Aj po dosadení konkrétnej

hodnoty do $p(x)$ môžeme dostať nejaký výrok, ktorého pravdivosť nebude triviálne dokázať – pozrite sa na nejaké náročné dôkazy z predošlej sekcie.

Teraz by ste mohli túto úlohu zvládnuť vyriešiť.

Úloha 2.2. Určte pravdivostnú hodnotu výroku

$$\forall x \in \mathbb{R}\colon 3x + 2 > 2x + 5.$$

Riešenie úlohy 2.2

Dosadením $x = 0$ dostaneme $2 > 5$, čo neplatí. Preto je výrok zo zadania nepravdivý.

Čiže v prípade, že všeobecný výrok neplatí, tak dôkaz máme tiež jednoduchý.

Vyvrátenie všeobecného výroku

Nepravdivosť tvrdenia tvaru $\forall x \in M\colon p(x)$ dokazujeme tak, že uvedieme príklad konkrétneho prvku x z množiny M a dokážeme, že pre tento prvok neplatí $p(x)$.

Čo sa týka dokazovania všeobecných výrokov, tak to sme už videli pri úlohe 1.6.

Dôkaz všeobecného výroku

Pravdivosť tvrdenia tvaru $\forall x \in M\colon p(x)$ dokazujeme tak, že uvedieme príklad konkrétneho prvku x z množiny M a dokážeme, že pre tento prvok neplatí $p(x)$. Dôkaz môže mať štruktúru:

Nech $x \in M$. Potom ... [dôkaz $p(x)$, pri ktorom využívame premennú x].

A pre úplnosť, vyvrátiť existenčný výrok $\exists x \in M\colon p(x)$ znamená dokázať jeho negáciu, teda výrok $\forall x \in M\colon \neg p(x)$, čo vieme spraviť podľa schémy vyššie.

Striedanie kvantifikátorov

Úloha 2.3. Rozhodnite o pravdivosti nasledovných tvrdení:

a) $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\colon x + y = 0$,

b) $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\colon x + y = 0$,

c) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon x + y = 0$,

d) $\exists x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon x + y = 0$,

Riešenia úloh sú zoradené podľa ich náročnosti.

Riešenie

a) Neplatí, lebo pre $x = 1$, $y = 2$ neplatí $1 + 2 = 0$.

d) Platí, lebo pre $x = 3$, $y = -3$ platí $3 + (-3) = 0$.

c) Platí, lebo pre ľubovoľné $x \in \mathbb{R}$ a pre $y = -x$ platí $x + (-x) = 0$.

b) Neplatí, lebo pre ľubovoľné $x \in \mathbb{R}$ zvolíme $y = 1 - x$ (čo je zjavne reálne číslo), pre ktoré

máme $1 + (1 - x) = 1 \neq 0$, teda výrok $1 + (1 - x) = 0$ neplatí.

Uvedomme si, že v podúlohe b) sme vlastne dokazovali negáciu tvrdenia, ktorý vyzerá: $\forall x \in \mathbb{R} \exists y \in \mathbb{R}\colon x + y \neq 0$. Preto sme použili takúto štruktúru – začali sme dokazovať všeobecný výrok „Pre ľubovoľné $x \in \mathbb{R}\ldots$“ a pre toto všeobecné x sme začali dokazovať existenčný výrok, čo sme začali voľbou y. Po prejdení kvantifikátorov sme dokazovali, že platí $x + y \neq 0$.

Výroky b) a c) ilustrujú, že na poradí kvantifikátorov záleží. To môžeme ilustrovať aj rôznymi slovnými významami výrokov b) a c):

b) Existuje reálne číslo, ktoré dáva súčet 0 s ľubovoľným reálnym číslom.

c) Každé reálne číslo dáva súčet 0 s nejakým reálnym číslom.

Na podúlohe c) si ešte rozoberieme štruktúru dôkazu podľa toho, čo sme si povedali vyššie. Dôkaz sa začína za slovom lebo, teda je to veta: „Pre ľubovoľné $x \in \mathbb{R}$ a pre $y = -x$ platí $x + (-x) = 0$.“

- Pre ľubovoľné $x \in \mathbb{R}$: Takto sa začína dôkaz všeobecného výroku. Ďalej teda nasleduje dôkaz tvrdenia $\exists y \in \mathbb{R}\colon x + y = 0$.
- pre $y = -x$: Teraz dokazujeme existenčné tvrdenie, a toto je jeho začiatok. Všimnite si, že narozdiel o riadku vyššie teraz uvádzame konkrétnu hodnotu premennej y. Teda konkrétnu v kontexte dokazovania $\exists y \in \mathbb{R}\colon x + y = 0$, kedy sme už (v odrážke vyššie) zaviedli do dôkazu premennú x.
- platí $x+(-x) = 0$: Ostalo nám dokázať $x+(-x)$, čo vyplýva z jednoduchej algebraickej úpravy.

Úloha 2.4. Rozhodnite o pravdivosti nasledovných tvrdení:

a) $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\colon xy = 0$,

b) $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\colon xy = 0$,

c) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon xy = 0$,

d) $\exists x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon xy = 0$.

Riešenie

a) Neplatí, lebo pre $x = 4$ a $y = 2$: $4 \cdot 2 \neq 0$.

b) Platí, lebo pre $x = 0$ platí $\forall y \in \mathbb{R}\colon 0 \cdot y = 0$

c) Platí, lebo pre každé $x \in \mathbb{R}$ platí: pre $y = 0$ dostaneme $x \cdot 0 = 0$.

d) Platí, lebo pre $x = 0$ a $y = -17$ platí $0 \cdot (-17) = 0$.

Úloha 2.5. Rozhodnite, ktoré výroky sú pravdivé.

a) $\exists x \in \mathbb{R}\colon x \cdot 1 = x$

b) $\forall x \in \mathbb{R}\colon x \cdot 1 = x$

c) $\exists x \in \mathbb{R}\colon x \cdot x = 1$

d) $\forall x \in \mathbb{R}\colon x \cdot x = 1$

e) $\exists x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon x \cdot y = 1$

f) $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\colon x \cdot y = 1$

g) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\colon x \cdot y = 1$

h) $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\colon x \cdot y = 1$

Úloha 2.6. Rozhodnite, ktoré výroky sú pravdivé.

a) $\exists n \in \mathbb{N}\ \exists k \in \mathbb{N}\colon k > n$

b) $\forall n \in \mathbb{N}\ \exists k \in \mathbb{N}\colon k > n$

c) $\exists n \in \mathbb{N}\ \forall k \in \mathbb{N}\colon k > n$

d) $\exists n \in \mathbb{N}\ \exists k \in \mathbb{N}\colon k \mid n$

e) $\forall n \in \mathbb{N}\ \exists k \in \mathbb{N}\colon k \mid n$

f) $\exists n \in \mathbb{N}\ \forall k \in \mathbb{N}\colon k \mid n$

Úloha 2.7. Dokážte, že súčet ľubovoľných dvoch celých čísel deliteľných tromi je deliteľný tromi.

Začneme tým, že si najprv dokazovaný výrok symbolicky zapíšeme:

$$\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\colon (3 \mid a \wedge 3 \mid b) \Rightarrow 3 \mid (a+b).$$

Teraz detailne rozpíšeme dôkaz spolu s úvahami, ktoré počas neho robíme.

Krok dôkazu	Jeho vysvetlenie
1. Nech a, $b \in \mathbb{Z}$	Dokazujeme všeobecný výrok. Zahodíme kvantifikátory, zavedieme premenné a vo zvyšku dôkazu dokazujeme $(3 \mid a \wedge 3 \mid b) \Rightarrow 3 \mid (a+b)$
2. Nech platí $3 \mid a \wedge 3 \mid b$	Dokazujeme výrok v tvare implikácie. Skúšame priamy dôkaz, teda predpokladáme, že ľavá strana implikácie platí a naším cieľom je dokázať $3 \mid (a+b)$
3. $3 \mid a$ (lebo 2.)	Využili sme, že platí konjunkcia $3 \mid a \wedge 3 \mid b$ a odvodili sme z toho, že platí jej člen $3 \mid a$ (teda využili sme tautológiu $(p \wedge q) \Rightarrow p$)
4. $\exists k \in \mathbb{Z}\colon a = 3k$ (lebo 3.)	Využili sme definíciu deliteľnosti.
5. $a = 3r$ pre nejaké $r \in \mathbb{Z}$ (lebo 4.)	V kroku 4. vieme, že existuje nejaké celé číslo s istou vlastnosťou. Toto celé číslo si vieme označiť a ďalej pracovať s týmto označením. Pre jeho označenie sme zvolili r.
6. $3 \mid b$ (lebo 2.)	To isté robíme pre druhý člen konjunkcie z bodu 2.
7. $\exists k \in \mathbb{Z}\colon a = 3k$ (lebo 3.)	
8. $b = 3s$ pre nejaké $s \in \mathbb{Z}$ (lebo 7.)	Opäť robíme to isté, len si musíme dať pozor. Pre označenie „onoho čísla, ktoré existuje v bode 6“ musíme použiť nové označenie. Premennú r už máme použitú, preto sme použili s.
9. $a + b = 3r + 3s$ (lebo 5. a 8.)	Sčítali sme odvodené rovnosti
10. $a + b = 3(r+s)$ (lebo 9.)	Na tvrdenie z bodu 8. sme použili distributívny zákon.
11. $r + s \in \mathbb{Z}$ (lebo $r \in \mathbb{Z} \wedge s \in \mathbb{Z}$)	Využívame, že súčet celých čísel je celé číslo.
12. $\exists k \in \mathbb{Z}\colon a + b = 3k$ (lebo 10. a 11.)	V bode 9 máme nájdené celé číslo, konkrétne číslo $k = r + s$, pre ktoré platí $a + b = 3k$.
13. $3 \mid (a+b)$ (lebo 12.)	Teraz sme opäť použili definíciu deliteľnosti, len teraz opačným smerom ako na začiatku.

Najčastejšou chybou pri dôkazoch tohto typu je zlé pomenovanie premennej v kroku 8. Je potrebné si uvedomiť, že keď odstraňujeme existenčný kvantifikátor, musíme jeho lokálnu premennú nahradiť novou premennou. Okrem toho sa chyták môže skrývať aj v bode 11. Keď dokazujeme existenčné tvrdenie príkladom, je potrebné overiť, že náš príklad naozaj patrí do kvantifikovanej množiny. Vo väčšine úloh je toto tvrdenie triviálne, no môže sa objaviť výnimka. Napr. ak by nám vyšlo $a + b = 3(\sqrt{r} + 2s/(r + \sqrt{3}))$, kedy vôbec nie je jasné, že v zátvorke máme celé číslo.

Zapisovať dôkazy takto podrobne nie je potrebné. Mnohé úvahy sa dajú spojiť do jednej, čím vieme dôkaz skrátiť. Týmto dlhým zápisom sme chceli len ilustrovať úvahy, ktoré sa pri dokazovaní dejú. Keď aj tieto úvahy nebudete písať, mali by ste ich robiť vo svojej hlave.

3 Dôkaz sporom

Poďme sa pozrieť na nasledovnú dôkazovú úlohu. Skúste si dokázať toto tvrdenie.

Úloha 3.1. Majme tri reálne čísla so súčtom 0. Dokážte, že aspoň jedno z týchto čísel je nezáporné.

Keď máte tvrdenie dokázané, skúste sa zamyslieť nad tým, ako presne ste sa presvedčili, že dokazovaný výrok je pravdivý.

Pokus o riešenie

Ak by boli všetky tri čísla záporné, tak aj ich súčet by bol záporný, lebo súčet záporných čísel je záporný. Preto niektoré z nich musí byť nezáporné.

Možno niekoho zmätie slovný zápis riešia. To nie je problém. Mnoho dôkazov je písaných slovne (v učebniciach, vzorových riešeniach MO, ...). Môže nám pomôcť prepísať si ho symbolicky. Na to si najprv musíme zapísať symbolicky samotné dokazované tvrdenie. To sa dá napríklad ako

$$\forall x, y, z \in \mathbb{R}, x + y + z = 0 \colon x \geq 0 \vee y \geq 0 \vee z \geq 0.$$

Miesto spojok alebo si môžeme pomôcť aj existenčným kvantifikátorom, napr. $\exists w \in \{x, y, z\} \colon w \geq 0$. Skúmaný dôkaz by potom môže vyzerať takto.

Symbolicky zapísané riešenie

$x < 0 \wedge y < 0 \wedge z < 0$
$x + y < 0$, lebo $x < 0 \wedge y < 0$
$x + y + z < 0$, lebo $x + y < 0 \wedge z < 0$
Dostali sme, že $x + y + z < 0$, ale podľa zadania $x + y + z = 0$. V oboch krokoch sme využili známe pravidlo $\forall a, b, c, d \in \mathbb{R} \colon (a < b \wedge c < d) \Rightarrow a + c < b + d$

Či sa už pozeráme na textový alebo symbolický dôkaz, obe z nich sa líšia od priameho dôkazu. Pozeráme si v nich na situáciu, kedy dokazovaný výrok V neplatí. Vychádzame teda z predpokladu $\neg V$. Dopracovali sme sa k niečomu nepravdivému – že súčet $a + b + c$ je 0, ale zároveň má byť aj záporný. A to je problém, niečo také sa nemôže stať. Preto sa nemôže stať ani to, že platí $\neg V$. Takýto princíp dokazovania sa volá dôkaz sporom. Z pohľadu výrokov sme dokázali implikáciu $\neg V \Rightarrow N$, kde N je nepravdivý výrok. Keďže implikácia $\neg V \Rightarrow N$ je pravdivá (lebo sme ju korektne odvodili), tak aj výrok $\neg V$ musí neplatiť. Pripomeňme si pravdivostnú tabuľku implikácie.

a	b	$a \Rightarrow b$
0	0	1
0	1	1
1	0	0
1	1	1

Dôkaz sporom

Výrok V dokážme sporom nasledovne. Predpokladáme, že platí jeho negácia $\neg V$. Z tohto predpokladu odvodíme (napr. ako pri priamom dôkaze) platnosť nepravdivého tvrdenia. Teda dokážeme

$$V' \Rightarrow N,$$

kde N je nepravdivé tvrdenie.Jeho štruktúra vyzerá zväčša nasledovne:

Kostra dôkazu sporom

Tvrdenie V dokážme sporom. Nech platí V'. Potom
... *(Reťazec úvah ako pri priamom dôkaze)*
Teda platí N, čo je v spor.

Spor často dostávame tým, že postupne dokážeme nejaké tvrdenie, aj jeho negáciu. Napríklad:

> Tvrdenie V dokážme sporom. Nech platí V'. Potom
> ...
> Preto n je párne číslo
> ...
> Teda n je nepárne číslo, čo je v spor tým, že je párne.

V takomto prípade, keď sme v závere nedostali tvrdenie, ktoré je samo o sebe nepravdivé (napr. n je nepárne číslo – to kľudne môže byť pravda), je odporúčané dopísať, s čím je toto tvrdenie v spore (alebo naznačiť šípkou).

Poriadny zápis dôkazu z úlohy 3.1 môže teda vyzerať takto.

Dôkaz úlohy 3.1 sporom

Sporom. Nech sú všetky tri čísla záporné. Potom aj ich súčet je záporný, lebo súčet záporných čísel je záporný. To je ale spor s tým, že súčet týchto čísel je 0.

Na tomto dôkaze si ešte môžeme všimnúť, že spor sme dostali s tým, čo sme v zadaní. Dokazované tvrdenie možno tiež vyjadriť ako implikáciu

$$\forall x, y, z \in \mathbb{R}\colon x + y + z = 0 \Rightarrow (x \geq 0 \vee y \geq 0 \vee z \geq 0).$$

Vtedy dostávame spor s ľavou stranou implikácie. Takýto dôkaz sa nazýva aj *nepriamy dôkaz*.

Nepriamy dôkaz

Tvrdenie vo forme implikácie $A \Rightarrow B$ dokážeme nepriamo tak, že miesto implikácie $A \Rightarrow B$ dokážeme implikáciu $\neg B \Rightarrow \neg A$, ktorá sa nazýva *obmena implikácie*.

Nepriamy dôkaz je založený na fakte, že implikácie $A \Rightarrow B$ a $\neg B \Rightarrow A$ majú rovnaké pravdivostné hodnoty. Samotnú obmenu potom dokazujeme priamo (môžeme aj inak, ale iné techniky nepoznáme a dokazovať obmenou alebo sporom nemá zmysel). Obmena tvrdenia z úlohy 3.1 je

$$\forall x, y, z \in \mathbb{R}\colon (x < 0 \wedge y < 0 \wedge z \geq 0) \Rightarrow x + y + z \neq 0.$$

Nepriamy dôkaz teda môže vyzerať nasledovne. Uvedieme stručnú verziu.

Dôkaz úlohy 3.1 nepriamo

Nepriamo. Nech $x < 0 < y < 0 < z$. Potom $x + y + z < 0$ (lebo súčet záporných čísel je záporný), teda $x + y + z \neq 0$.

Dávame do pozornosti, že pokiaľ nepoužívame priamy dôkaz, je dobré napísať, aký dôkaz používame. Aspoň minimalisticky slovíčkom *sporom* alebo *nepriamo*.

4 Prehľad dokazovania

Typy dôkazov podľa spôsobu uvažovania

Priamy dôkaz

Priamy dôkaz výroku V je konečná postupnosť výrokov, ktorá sa končí výrokom V a pre každý výrok tejto postupnosti platí niektorý z nasledovných bodov:

(i) je axióma,

(ii) je všeobecne známe alebo už dokázané tvrdenie,

(iii) vyplýva (je logickým dôsledkom) z predchádzajúcich výrokov tejto postupnosti.

Dôkaz sporom

Výrok V dokážme sporom nasledovne. Predpokladáme, že výrok platí negácia výroku V. Z tohto predpokladu odvodíme (napr. ako pri priamom dôkazov) platnosť nepravdivého tvrdenia. Teda dokážeme

$$V' \Rightarrow N,$$

kde N je nepravdivé tvrdenie. Jeho štruktúra vyzerá zväčša nasledovne:

> Tvrdenie V dokážme sporom. Nech platí V'. Potom
> ... *(Reťaze úvah ako pri priamom dôkaze)*
> Teda platí N, čo je v spor.

Spor často dostávame tým, že postupne dokážeme nejaké tvrdenie, aj jeho negáciu. Napríklad:

> Tvrdenie V dokážme sporom. Nech platí V'. Potom
> ...
> Preto n je párne číslo
> ...
> Teda n je nepárne číslo, čo je v spor tým, že je párne.

V takomto prípade, keď sme v závere nedostali tvrdenie, ktoré je samo o sebe nepravdivé (napr. n je nepárne číslo – to kľudne môže byť pravda), je odporúčané dopísať, s čím je toto tvrdenie v spore (alebo naznačiť šípkou).

Dokazovanie kvantifikovaných výrokov

Dôkaz existenčného výroku

Výrok tvaru $\exists x \in M : v(x)$ najľahšie dokážeme tak, že nájdeme jedno x z množiny M, pre ktoré platí výroková forma $v(x)$. Takýto dôkaz má štruktúru

Pre $x = 9$ platí $v(9)$, lebo $\langle$*Dôkaz výroku* $v(9)\rangle$.

Samozrejme, miesto 9 zvolíme správne číslo alebo prvok. Dokonca môžeme použiť aj výraz s premennými, ak dokazujeme len výrokovú formu vnútri zložitejšieho výroku.

Dôkaz všeobecného výroku

Výrok tvaru $\forall x \in M : v(x)$ najľahšie dokážeme tak, že spravíme dôkaz „výroku“ $v(x)$, v ktorom budeme používať premennú x.

Nech x je ľubovoľný prvok M. Potom platí $\langle$*Dôkaz výroku* $v(x)\rangle$.

Samozrejme, existujú aj iné typy dôkazov. Obzvlášť pri existenčných tvrdeniach je viacero dôkazov, ktoré nezačínajú určením hľadanej hodnoty.

Prehľad dokazovania výrokov podľa štruktúry

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).

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

$A \vee B$: 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).

Prehľad logických úsudkov podľa štruktúry výroku

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 $a(c)$.

5 Ako robiť dôkazy tautológií

Dôkaz nekvantifikovanej tautológie

Úloha 5.1. Rozhodnite, či zložený výrok

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

je tautológia.

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

Úloha 5.2. Rozhodnite, či nasledovný zložený výrok je tautológia

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

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).

Kvantifikované tautológie

Úloha 5.3. Dokážte, že výrok

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

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.

Úloha 5.4. Rozhodnite, či výrok

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

je tautológia.

Oproti predošlej úlohe sme teraz implikáciu nahradili ekvivalenciou. Tým však už výrok tautológiou neostane. 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 $(\exists x)(a(x) \wedge \neg b(x))$, 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.