9. kapitola

Metódy matematického dôkazu – deduktívny dôkaz, základné pravidlá usudzovania, matematická indukcia

9.1 Význam dôkazu v matematike

V matematike, podobne ako aj v informatike, vystupujú do popredia dve otázky: (1) Za akých podmienok je matematický dôkaz korektný a (2) aké metódy môžu byť použité pri konštrukcii matematických dôkazov. V tejto kapitole budeme hľadať odpovede na tieto dve otázky, pričom budeme špecifikovať rôzne formy matematických dôkazov.

Veta (teorém, výrok, skutočnosť, fakt, argument, alebo výsledok) je výrok o ktorom môže byť ukázané pomocou metód logiky, že je pravdivý. V tejto súvislosti hovoríme o *dôkaze* vety, ktorý spočíva v postupnosti jednotlivých „medzikrokov“, ktoré sú odvodené buď z množiny jednoduchých postulátov, nazývaných *axiómy*, alebo z predchádzajúcich viet (pomocných viet, často nazývaných lemy) danej postupnosti. Komplikované dôkazy sú obvykle jasnejšie formulované, keď ich dôkaz je rozdelený na jednotlivé medzikroky, ktoré sú formulované ako samostatné vety. Tieto medzikroky - vety v postupnosti sú vytvárané pomocou *pravidiel odvodzovania* (*pravidiel usudzovania*), ktoré z niekoľkých pravdivých tvrdení - argumentov vytvorí nové pravdivé tvrdenie - argument.

Metódy dôkazu diskutované v tejto kapitole sú dôležité pre tvorbu korektných dôkazov viet v informatike. V teoretickej informatike sa napr. študujú rôzne metódy verifikácie korektnosti programu, alebo či operačný systém je bezpečný. V umelej inteligencii pri odvodzovaní nových faktov z danej databázy poznatkov (množiny výrokových formúl, ktorá sa vo výrokovej logike nazýva teória) je dôležité mať zabezpečené, aby daná databáza bola konzistentná (korektná), teda aby z nej súčasne nevyplýval nejaký výrok a taktiež aj jeho negácia. Môžeme teda konštatovať, že zvládnutie metód matematického dôkazu je dôležité nielen v matematike, ale aj v informatike.

Nižšie uvedená forma dôkazu sa nazýva *deduktívny dôkaz*, ktorý obsahuje:

- *systém elementárnych pojmov*, ktoré sú používané pri formulácii základných zložiek deduktívneho dôkazu
- *systém axióm* (základné elementárne poznatky, ktoré sú pokladané za evidentné),
- *pravidlá odvodzovania* (pomocou ktorých sa uskutočňuje dôkaz).
- *vety* (deduktívne poznatky - argumenty), ktoré boli odvodené z axióm pomocou pravidiel odvodzovania a ktoré podstatne zjednodušujú a skracujú dôkazy ďalších nových deduktívnych poznatkov.

Poznamenajme, že tak v matematike, ako aj v informatike, sa v ojedinelých prípadoch používa aj induktívne usudzovanie (dôkaz), ktoré je založené na pozorovaní určitých skutočností, ktoré sa často opakujú v analogických situáciách. Tieto pozorované skutočnosti sú „induktívne“ zovšeobecnené. Nové pojmy, ktoré boli zavedené týmto „induktívnym“ spôsobom sa neskoršie buď dokážu deduktívne v rámci daného systému pojmov, alebo sa postulujú ako nové špeciálne axiómy. Tieto ojedinelé situácie v dejinách matematiky

(napríklad zavedien komplexných čísel) vždy znamenali vznik nových oblastí matematiky, ktoré nie sú striktne deduktívne dokázateľné zo známych pojmov a reprezentujú akty kreatívnosti v matematike, ktoré taktiež znamenajú, že matematika nie je len veda deduktívneho charakteru, kde sa dá každý pojem odvodiť z iných jednoduchších poznatkov[1].

9.2 Pravidlá usudzovania vo výrokovej logike

Pravidlá usudzovania vo výrokovej logike tvoria schému

$$\begin{array}{|l} predpoklad_1 \\ \ldots\ldots\ldots\ldots \\ \underline{predpoklad_n} \\ záver \end{array} \tag{9.1}$$

ktorá obsahuje *n predpokladov* a jeden *záver*. Táto schéma usudzovania je totožná so symbolom *logického dôkazu* (pozri 6.1)

$$\{predpoklad_1, \ldots, predpoklad_n\} \vdash záver \tag{9.2a}$$

Tabuľka 9.1. Schémy usudzovania výrokovej logiky

Schéma usudzovania	Teorém výrokovej logiky	Názov schémy
$\begin{array}{\|l} p \\ \hline p \vee q \end{array}$	$p \Rightarrow (p \vee q)$	adícia
$\begin{array}{\|l} p \wedge q \\ \hline p \end{array}$	$(p \wedge q) \Rightarrow p$	simplifikácia (zjednodušenie)
$\begin{array}{\|l} p \\ q \\ \hline p \wedge q \end{array}$	$p \Rightarrow (q \Rightarrow (p \wedge q))$	konjunkcia
$\begin{array}{\|l} p \\ p \Rightarrow q \\ \hline q \end{array}$	$p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$	modus ponens
$\begin{array}{\|l} \neg q \\ p \Rightarrow q \\ \hline \neg p \end{array}$	$\neg q \Rightarrow ((p \Rightarrow q) \Rightarrow \neg p)$	modus tollens
$\begin{array}{\|l} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	hypotetický sylogizmus
$\begin{array}{\|l} p \vee q \\ \neg p \\ \hline q \end{array}$	$(p \vee q) \Rightarrow (\neg p \Rightarrow q)$	disjunktívny sylogizmus
$\begin{array}{\|l} p \Rightarrow q \\ \hline \neg q \Rightarrow \neg p \end{array}$	$(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$	inverzia implikácie
$\begin{array}{\|l} p \Rightarrow q \\ p \Rightarrow \neg q \\ \hline \neg p \end{array}$	$(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$	reductio ad absurdum

[1] To že matematika nie je veda čisto deduktívna má aj iné hlboké dôvody.

alebo formálne

$$\{\varphi_1,...,\varphi_n\} \vdash \varphi \tag{9.2b}$$

Táto formula logického dôkazu môže byť prepísaná do formy

$$\vdash \varphi_1 \wedge ... \wedge \varphi_n \Rightarrow \varphi \tag{9.3a}$$

alebo v ekvivalentnom tvare, kde konjunkcie sú nahradené implikáciami

$$\vdash \varphi_1 \Rightarrow \left(\varphi_2 \Rightarrow \left(\Rightarrow ... \left(\varphi_n \Rightarrow \varphi\right)\right)\right) \tag{9.3b}$$

Tabuľka 9.1 obsahuje 8 obvyklých schém usudzovania výrokovej logiky, pričom každá schéma je doprevádzaná aj zákonom (tautológiou) výrokovej logiky (v tvare formuly (9.3b)) a obvyklým historickým názvom. Hovoríme, že predpoklady sú *konzistentné* vtedy a len vtedy, ak existuje aspoň jedna interpretácia pravdivostných hodnôt výrokových premenných, pre ktorú sú všetky predpoklady pravdivé. V opačnom prípade je množina predpokladov *nekonzistentná* (*kontradiktórna*) a je charakterizovaná tým, že z nej súčasne logicky vyplýva nejaký záver a aj jeho negácia.

Príklad 9.1. Majme dva predpoklady: prvý predpoklad je výrok *´prší´* a druhý predpoklad je implikácia *´ak prší, potom je cesta mokrá´* . Použitím pravidla usudzovania modus ponens, z pravdivosti týchto dvoch predpokladov vyplýva pravdivý záver *´cesta je mokrá´*, čo môžeme formálne vyjadriť pomocou schémy

$$\left|\begin{array}{l} \textit{prší} \\ \textit{ak prší, potom cesta je mokrá} \\ \hline \textit{cesta je mokrá} \end{array}\right. .$$

Príklad 9.2. Použitím schémy usudzovania adície k pravdivému výroku *´teplota je pod bodom mrazu´* môžeme pomocou disjunkcie priradiť ľubovolný výrok (pravdivý alebo nepravdivý), napr. *´prší´*, dostaneme pravdivý záver *´teplota je pod bodom mrazu alebo prší´*

$$\left|\begin{array}{l} \textit{teplota je pod bodom mrazu} \\ \hline \textit{teplota je pod bodom mrazu alebo prší} \end{array}\right.$$

Príklad 9.3. Uvažujme dva výroky *´ak dnes bude pršať, potom sa nepôjdem kúpať"* a *´ak sa nepôjdem kúpať, potom navštívim príbuzného´*. Použitím schémy usudzovania nazvanej hypotetický sylogizmus dostaneme z týchto dvoch predpokladov záver *´ak dnes bude pršať, potom navštívim príbuzného´*

$$\left|\begin{array}{l} \textit{ak dnes bude pršať, potom sa nepôjdem kúpať} \\ \textit{ak sa nepôjdem kúpať, potom navštívim príbuzného} \\ \hline \textit{ak dnes bude pršať, potom navštívim príbuzného} \end{array}\right.$$

Túto schému môžeme sformalizovať pomocou výrokov

p=´dnes prší´
q=´kúpem sa´
r= ´navštívim príbuzného´

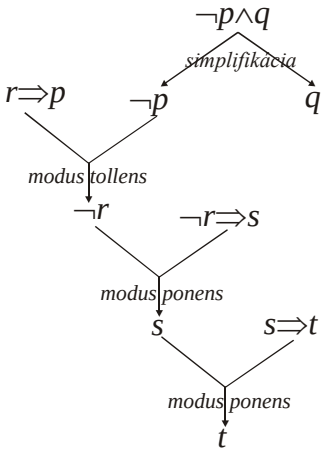
potom schéma má tento formálny tvar mierne modifikovaného hypotetického sylogizmu

$$\left|\begin{array}{l} p \Rightarrow \neg q \\ \neg q \Rightarrow r \\ \hline p \Rightarrow r \end{array}\right.$$

ktorá je odvodená z pôvodnej schémy hypotetického sylogizmu substitúciou, kde výroková premenná q je substituovaná negáciou $\neg q$.

V poslednom príklade 9.3 boli už použité výrokové premenné, ktoré nám umožnia vykonať formalizáciu celého procesu dôkazu pomocou postupnosti elementárnych krokov.

Obrátime našu pozornosť na formulu (9.2b) logického vyplývania výrokovej formuly φ z predpokladov, ktoré sú reprezentované formulami φ_1, φ_2,..., φ_n. Logické vyplývanie ilustrujeme jednoduchým príkladom.9.4.



Obrázok 9.2. Strom odvodenia pre logický dôkaz z príkladu 9.4.

Príklad 9.4. Postulujme, že množina predpokladov obsahuje tieto formuly – zložené výroky:

φ_1 = *´dnes poobede nie je slnečno a je chladnejšie ako včera´*

φ_2 = *´pôjdeme sa kúpať len vtedy, ak bude slnečno´*

φ_3 = *´ak sa nepôjdeme kúpať, potom sa budeme člnkovať na rieke´*

φ_4 = *´ak sa budeme člnkovať na rieke, potom sa vrátime domov podvečer´*

požadovaný záver má tvar

φ = *´budem doma podvečer´*

Pomocou výrokových premenných

p = ´dnes poobede je slnečno´
q = ´je chladnejšie ako včera´
r = ´ pôjdeme sa kúpať ´
s = *´ budeme člnkovať na rieke´*
t = ´ vrátime sa domov podvečer´

vykonáme formalizáciu schémy logického vyplývania do tvaru

$$\{\neg p \wedge q, r \Rightarrow p, \neg r \Rightarrow s, s \Rightarrow t\} \vdash t$$

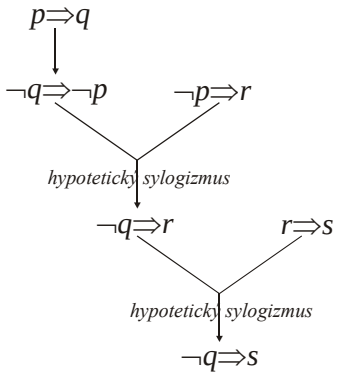
Ukážeme, že táto schéma je platná pomocou postupnosti elementárnych krokov, kde budeme používať schémy usudzovania z tab. 9.10.

1.	$\neg p \wedge q$	predpoklad$_1$
2.	$r \Rightarrow p$	predpoklad$_2$
3.	$\neg r \Rightarrow s$	predpoklad$_3$
4.	$s \Rightarrow t$	predpoklad$_4$
5.	$\neg p$	simplifikácia predpokladu$_1$
6.	q	simplifikácia predpokladu$_1$
7.	$\neg r$	medzivýsledok 5 a modus tollens na predpoklad$_2$
8.	s	medzivýsledok 7 a modus ponens na predpoklad$_3$
9.	t	medzivýsledok 8 a modus ponens na predpoklad$_4$

V úvodnej časti kapitoly 9.1 bolo poznamenané, že dôkaz je možné charakterizovať ako postupnosť formúl, kde posledná formula sa rovná požadovanému záveru, môžeme teda písať

$$(\neg p \wedge q) \to (r \Rightarrow p) \to (\neg r \Rightarrow s) \to (s \Rightarrow t) \to (\neg p) \to (q) \to (\neg r) \to (s) \to (t)$$

Túto postupnosť formúl môžeme reprezentovať aj pomocou „stromu dôkazu“ znázorneného na obr. 9.2.



Obrázok 9.3. Strom odvodenia pre logický dôkaz z príkladu 9.5.

Príklad 9.5. Nech množina predpokladov obsahuje tieto zložené výroky:

φ_1 = *´ak mi pošleš email, potom program dokončím´*

φ_2 = *´ak mi nepošleš email, potom pôjdem spať včasnejšie´*

φ_3 = *´ak pôjdem spať včasnejšie, potom sa ráno zobudím odpočinutý´*

požadovaný záver má tvar

φ = *´ak nedokončím program, potom sa ráno zobudím odpočinutý´*

Pomocou výrokových premenných

p = ´pošleš mi email ´

q = ´program dokončím´

r = ´pôjdem spať včasnejšie´

s = *´ráno sa zobudím odpočinutý´*

vykonáme formalizáciu schémy logického vyplývania do tvaru

$$\{p \Rightarrow q, \neg p \Rightarrow r, r \Rightarrow s\} \vdash \neg q \Rightarrow s$$

Pomocou postupnosti elementárnych krokov, kde budeme používať schémy usudzovania z tab. 9.1, ukážeme, že táto schéma je platná

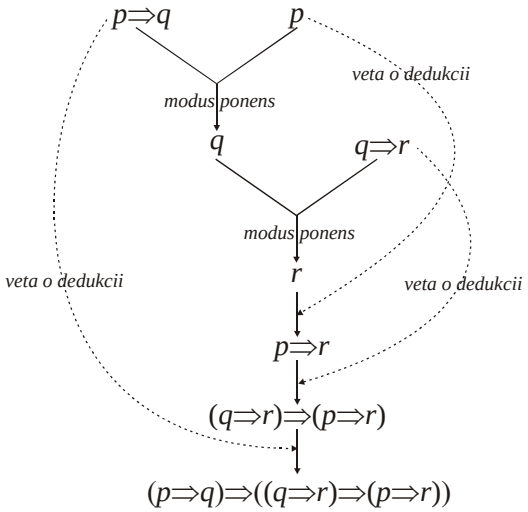
1.	$p \Rightarrow q$	predpoklad$_1$
2.	$\neg p \Rightarrow r$	predpoklad$_2$
3.	$r \Rightarrow s$	predpoklad$_3$
4.	$\neg q \Rightarrow \neg p$	inverzia implikácie na predpoklad$_1$
5.	$\neg q \Rightarrow r$	hypotetický sylogizmus na medzivýsledok 4 a predpoklad$_2$
6.	$\neg q \Rightarrow s$	hypotetický sylogizmus na medzivýsledok 5 a predpoklad$_3$

Diagramatická interpretácia tohto logického dôkazu je vykonaná pomocou stromu dôkazu znázorneného na obr. 9.3.

Uskutočnenie logického dôkazu $\{\varphi_1,...,\varphi_n\} \vdash \varphi$ môže byť podstatne zjednodušené. Ak množinu predpokladov $\{\varphi_1,...,\varphi_n\}$ rozšírime o nový „pomocný“ predpoklad ψ, potom vo výrokovej logike platí veta o dedukcii, ktorá má tvar (pozri vetu o dedukcii 4.1)

$$\left(\{\varphi_1,...,\varphi_n\}\cup\{\psi\}\vdash\varphi\right)\Rightarrow\left(\{\varphi_1,...,\varphi_n\}\vdash\left(\psi\Rightarrow\varphi\right)\right) \tag{9.4}$$

To znamená, že logický dôkaz formuly φ pomocou rozšírenej množiny predpokladov $\{\varphi_1,...,\varphi_n\}\cup\{\psi\}$ je rovnocenný logickému dôkazu formuly $\psi\Rightarrow\varphi$ pomocou pôvodnej množiny predpokladov.



Obrázok 9.4. Strom odvodenia pre logický dôkaz z príkladu 9.6.

Príklad 9.6. Pomocou logického dôkazu založeného na (9.4) dokážeme zákon hypotetického sylogizmu výrokovej logiky

$$\{p\Rightarrow q,q\Rightarrow r\}\cup\{p\}\vdash r$$

kde množina $\{p\Rightarrow q,q\Rightarrow r\}$ obsahujúca pôvodné predpoklady je rozšírená o pomocný predpoklad p.

1.	$p\Rightarrow q$	predpoklad$_1$
2.	$q\Rightarrow r$	predpoklad$_2$
3.	p	pomocný predpoklad
4.	q	modus ponens na predpoklad$_1$ a pomocný predpoklad
5.	r	modus ponens na predpoklad$_2$ a medzivýsledok 4
6.	$p\Rightarrow r$	použitie (1.4) na výsledok 5 a pomocný predpoklad
7.	$(q\Rightarrow r)\Rightarrow(p\Rightarrow r)$	použitie (9.4) na výsledok 6 a predpoklad$_2$
8.	$(p\Rightarrow q)\Rightarrow((q\Rightarrow r)\Rightarrow(p\Rightarrow r))$	použitie (9.4) na výsledok 7 a predpoklad$_1$

V krokoch 7 a 8 sme opakovane použili vzťah (9.4), kde sme z množiny predpokladov vždy vyeliminovali jeden predpoklad. Finálny výsledok už platí pre prázdnu množinu predpokladov, čo znamená, že formula je zákonom (tautológiou) výrokovej logiky.

V kapitole 9.1 bolo zdôraznené postavenie viet vo formálnom logickom systéme ako efektívnej skratky logických dôkazov, kde sa už nemusí opakovať to, čo už raz bolo dokázané. Tento prístup výstavby formálnych systémov pomocou viet a ich využívania patrí medzi základné črty formálnych systémov, ktorých výstavba sa uskutočňuje hlavne pomocou prepojenej siete viet, ktoré sú dokazované pomocou už dokázaných viet v predošlých krokoch.

Nech ψ je veta (tautológia) , potom logický dôkaz $\{\varphi_1,...,\varphi_n\} \vdash \varphi$ môže byť rozšírený o vetu ψ takto

$$\left(\{\varphi_1,...,\varphi_n\} \vdash \varphi\right) \Rightarrow \left(\{\varphi_1,...,\varphi_n\} \cup \{\psi\} \vdash \varphi\right) \tag{9.5}$$

Význam tohto rozšírenia spočíva v tom, že zahrnutie vhodnej vety môže podstatne zjednodušiť dôkaz vety.

Príklad 9.7. Dokážte zákon rezolventy

$$(p \vee q) \Rightarrow \left((\neg p \vee r) \Rightarrow (q \vee r)\right)$$

pomocou zákona hypotetického sylogizmu

$$(p \Rightarrow q) \Rightarrow \left((q \Rightarrow r) \Rightarrow (p \Rightarrow r)\right)$$

a pomocou vety o disjunktnom tvare implikácie

$$(p \Rightarrow q) \equiv (\neg p \vee q)$$

formálne

$$\left\{(p \Rightarrow q) \Rightarrow \left((q \Rightarrow r) \Rightarrow (p \Rightarrow r)\right)\right\} \cup \left\{(p \Rightarrow q) \equiv (\neg p \vee q)\right\} \vdash \left((p \vee q) \Rightarrow \left((\neg p \vee r) \Rightarrow (q \vee r)\right)\right)$$

Logický dôkaz pozostáva z tejto postupnosti medzivýsledkov:

1.	$(p \Rightarrow q) \Rightarrow \left((q \Rightarrow r) \Rightarrow (p \Rightarrow r)\right)$	predpoklad$_1$
2.	$(p \Rightarrow q) \equiv (\neg p \vee q)$	pomocný predpoklad - veta
3.	$(\neg p \vee q) \Rightarrow \left((\neg q \vee r) \Rightarrow (\neg p \vee r)\right)$	prepis 1 pomocou vety 2
4.	$(\neg q \vee p) \Rightarrow \left((\neg p \vee r) \Rightarrow (\neg q \vee r)\right)$	prepis 3 pomocou zámeny $p \rightleftarrows q$
5.	$(p \vee q) \Rightarrow \left((\neg p \vee r) \Rightarrow (q \vee r)\right)$	prepis 4 pomocou substitúcie $\neg q/q$

Úplne analogickým spôsobom by sme mohli dokázať, že zákon rezolventy je možné prepísať na zákon hypotetického sylogizmu, z čoho plynie, že tieto dva zákony sú navzájom ekvivalentné

$$\left((p \Rightarrow q) \Rightarrow \left((q \Rightarrow r) \Rightarrow (p \Rightarrow r)\right)\right) \equiv \left((p \vee q) \Rightarrow \left((\neg p \vee r) \Rightarrow (q \vee r)\right)\right)$$

9.2.1 Chybné pravidlá usudzovania

Existujú jednoduché modifikácie schém usudzovania modus ponens a modus tollens, ktoré nie sú korektné. Prvá nekorektná schéma sa nazýva *potvrdenie dôsledku*

$$\left|\begin{array}{l} q \\ \underline{p \Rightarrow q} \\ p \end{array}\right. \tag{9.6a}$$

Druhá sa nazýva *popretie predpokladu*

$$\left|\begin{array}{l} \neg p \\ \underline{p \Rightarrow q} \\ \neg q \end{array}\right. \tag{9.6b}$$

Prvá schéma „popretie predpokladu“ je ilustrovaná príkladom

$$\frac{\begin{array}{l}\textit{vydala som sa}\\ \textit{ak som pekná, tak sa vydám}\end{array}}{\textit{som pekná}}$$

Záver nie je korektný, môže sa vydať aj vtedy, keď nie je pekná. Druhá schéma „potvrdenie dôsledku“ môže byť ilustrovaná podobným príkladom

$$\frac{\begin{array}{l}\textit{nie som pekná}\\ \textit{ak som pekná, tak sa vydám}\end{array}}{\textit{nevydám sa}}$$

Chyba v usudzovaní je podobná ako v predchádzajúcom príklade. O nekorektnosti schém usudzovania (9.6a-b) sa ľahko presvedčíme tak, že im priradíme formuly výrokovej logiky

$$q \Rightarrow \big((p \Rightarrow q) \Rightarrow p\big) \tag{9.7a}$$

$$\neg p \Rightarrow \big((p \Rightarrow q) \Rightarrow \neg q\big) \tag{9.7b}$$

Pre prvú formulu existuje interpretácia premenných $\tau = (p/0, q/1)$, pre ktorú má prvá formula (9.7a) pravdivostnú hodnotu ´0´. Táto interpretácia môže byť použitá aj pre druhú formulu (9.7b) k ukázaniu, že formula má pravdivostnú hodnotu ´0´. To znamená, že obe formuly (9.7a-b) nie sú tautológie, čiže nemôžu byť zákonmi výrokovej logiky.

Ako svedčia mnohé kognitívno-psychologické výskumy [xx], obe tieto schémy, aj keď sú chybné, sa často využívajú v bežnom usudzovaní, možno ich teda pokladať za „klasické chyby“ nášho každodenného uvažovania.

9.3 Pravidlá usudzovania v predikátovej logike

Predikátová logika môže byť chápaná ako zovšeobecnenie výrokovej logiky o tzv. kvantifikátory (všeobecný a existenčný). Základné schémy usudzovania v predikátovej logike sú uvedené v tab. 9.2.

Tabuľka 9.2. Schémy usudzovania predikátovej logiky

Schéma usudzovania	Teorém predikátovej logiky	Názov schémy
$\dfrac{\forall x\, P(x)}{P(c)}$	$\big(\forall x\, P(x)\big) \Rightarrow P(c)$	Konkretizácia univerzálneho Kvantifikátora
$\dfrac{P(c)\ \textit{pre každé } c}{\forall x\, P(x)}$	$P(c) \Rightarrow \big(\forall x\, P(x)\big)$	Zovšeobecnenie pomocou univerzálneho kvantifikátora
$\dfrac{\exists x\, P(x)}{P(c)\ \textit{pre nejaký element } c}$	$\big(\exists x\, P(x)\big) \Rightarrow P(c)$	Konkretizácia existenčného Kvantifikátora
$\dfrac{P(c)\ \textit{pre nejaký element } c}{\exists x\, P(x)}$	$P(c) \Rightarrow \big(\exists x\, P(x)\big)$	Zovšeobecnenie pomocou existenčného kvantifikátora

Konkretizácia univerzálneho kvantifikátora.
Ak nejakú vlastnosť $P(x)$ je pravdivá pre každý objekt (indivíduum) z konečného univerza U, potom $\forall x\, P(x)$, potom túto vlastnosť musí mať aj ľubovoľný konkrétny objekt c z tohto univerza,

$$\left(\forall x\, P(x)\right) \Rightarrow P(c) \tag{9.8}$$

Táto formula je priamym dôsledkom intuitívnej interpretácie univerzálneho kvantifikátora ako konjunkcie vlastnosti $P(x)$ pre každý objekt x z konenčného univerza

$$\forall x\, P(x) =_{def} \bigwedge_{x \in U} P(x) = P(a) \wedge P(b) \wedge ... \wedge P(u) \tag{9.9}$$

Ak na túto formulu (predpoklad) použijeme schému usudzovania simplifikácie z tab. 9.1, potom vlastnosť P má menovite každý objekt z U

$$\left|\begin{array}{l} \forall x\, P(x) \\ \hline P(a) \\ P(b) \\ ..... \\ P(c) \\ ..... \end{array}\right. \tag{9.10}$$

Potom musí platiť aj implikácia (9.8). Ako ilustračný príklad tejto vlastnosti univerzálneho kvantifikátora uvedieme klasický príklad konkretizácie zo stredovekej logiky

$$\left|\begin{array}{l} \textit{každý človek je smrteľný} \\ \textit{Sokrates je človek} \\ \hline \textit{Sokrates je smrteľný} \end{array}\right.$$

kde Sokrates patrí do univerza U (obsahujúceho všetkých ľudí) platnosti kvantifikátora $\forall$. Toto schéma usudzovanie môžeme zovšeobecniť takto

$$\left|\begin{array}{l} \forall (x \in U) P(x) \\ c \in U \\ \hline P(c) \end{array}\right. \tag{9.11}$$

Zovšeobecnenie pomocou univerzálneho kvantifikátora
Ak sa nám podarí dokázať, že vlastnosť P má každý objekt z nejakého univerza U, potom vzhľadom k tomuto univerzu môžeme definovať univerzálny kvantifikátor $\forall$

$$P(a) \wedge ... \wedge P(c) \wedge ... = \bigwedge_{x \in U} P(x) =_{def} \forall x\, P(x) \tag{9.12}$$

Ak použijeme na túto formulu schému usudzovania konjunkcie z tab. 9.1, potom

$$\left|\begin{array}{l} P(a) \\ ..... \\ P(c) \\ ..... \\ \hline \forall x\, P(x) \end{array}\right. \tag{9.13}$$

potom musí platiť aj

$$P(t) \Rightarrow \left(\forall x\, P(x)\right) \tag{9.14}$$

s poznámkou, že t je ľubovoľný objekt z univerza U. Zovšeobecnenie pomocou univerzálneho kvantifikátora sa často používa v matematike implicitne, pretože dôkaz vlastnosti $P(c)$ bol vykonaný pre ľubovoľný objekt c a nie len pre určitý špecifický objekt.

V mnohých prípadoch mimo matematiku použitie zovšeobecnenia podľa schémy usudzovania (9.13) (alebo predikátovej formuly (9.14)) tvorí základ tzv. *induktívneho*

zovšeobecnia, v ktorom sa snažíme parciálne poznatky zovšeobecniť pre každý objekt postulovaného univerza *U*. V tejto súvislosti potom vystupuje do popredia podľa rakúsko-anglického filozofa Karla Poppera problém falzifikácie všeobecného výroku $\forall x\, P(x)$. Stačí nájsť jeden objekt $o \in U$ pre ktorý neplatí vlastnosť *P*, $\neg P(o)$, potom všeobecný výrok $\forall x\, P(x)$ je neplatný, $\neg \forall x\, P(x)$.

Ako ilustračný príklad budeme študovať univerzum U , ktoré obsahuje všetky labute na našej planéte. Experimentálnym pozorovaním zistíme, že pre veľkú podmnožinu $U' \subset U$ platí, že každá labuť z nej je biela (túto vlastnosť označíme predikátom *B*). Túto skutočnosť môžeme „poctivo“ zovšeobecniť pomocou univerzálneho kvantifikátora $\forall'$ definovaného vzhľadom k „poduniverzu“ U'

$$\forall' x\, B(x) =_{def} \bigwedge_{x \in U'} B(x)$$

V dôsledku určitej netrpezlivosti, pozorovateľ zovšeobecní tento poznatok pre celé univerzum *U*, postuluje platnosť formuly $\forall x\, B(x)$. Falzifikácia tejto vlastnosti spočíva v tom, že nájdeme takú labuť (napr. pod skleneným mostom v Piešťanoch alebo ori vyšehradskom v Prahe), ktorá je čierna, potom automaticky platí $\neg \forall x\, B(x)$.

V tejto súvislosti môžeme hovoriť aj o verifikácii vlastnosti $\forall' x\, B(x)$, ďalšími a ďalšími pozorovaniami rozširujeme univerzum U' o ďalšie objekty *x*, ktoré majú vlastnosť *B*(*x*). Avšak je potrebné poznamenať, že toto rozširovanie platnosti $\forall' x\, B(x)$ o ďalšie objekty nám neprináša nový poznatok, neustále platí, že „labute sú biele“, len máme stále rozsiahlejšie vedomosti o evidentnosti tohto poznatku. Preto falzifikácia, na rozdiel od verifikácie, je zásadne dôležitá pre induktívne zovšeobecňovanie, napomáha nám pri vzniku nových poznatkov (čo ako prvý zdôraznil Karl Popper).

Konkretizácia existenčného kvantifikátora

Ak nejaká vlastnosť platí pre niektoré objekty z univerza *U*, potom musí platiť aj implikácia

$$\left(\exists x\, P(x)\right) \Rightarrow P(e) \tag{9.15}$$

alebo pomocou schémy uvažovania

$$\left| \begin{array}{l} \exists x\, P(x) \\ \hline P(e) \text{ pre nejaký element } e \end{array} \right. \tag{9.16}$$

Táto vlastnosť konkretizácie existenčného kvantifikátora vyplýva priamo z jeho intuitívnej interpretácie pomocou disjunkcie predikátov nad konečným univerzom

$$\exists x\, P(x) =_{def} \bigvee_{x \in U} P(x) = P(a) \vee \ldots \vee P(c) \vee \ldots \tag{9.17}$$

Disjunkcia výrokov je pravdivá vtedy a len vtedy, ak aspoň jeden jej výrok je pravdivý, potom existuje aspoň jeden objekt *c* pre ktorý je výrok *P*(*c*) pravdivý, t.j. platí implikácia (9.15).

Zovšeobecnenie pomocou existenčného kvantifikátora

Podľa tejto „skromnej“ schémy usudzovania, ak nejaká vlastnosť *P* platí aspoň pre jeden objekt *c* z univerza *U*, potom túto skutočnosť môžeme zovšeobecniť pomocou existenčného kvantifikátora $\exists$

$$P(e) \Rightarrow \bigvee_{x \in U} P(x) =_{def} \exists x\, P(x) \tag{9.18}$$

kde sme použili schému usudzovania s názvom adícia z tab. 9.1. Túto implikáciu môžeme vyjadriť pomocou schémy usudzovania

$$\frac{P(e) \text{ pre nejaký element } e}{\exists x\, P(x)} \tag{9.19}$$

Spojením (1.15) a (1.18) dostaneme

$$P(e) \equiv \exists x\, P(x) \tag{9.20}$$

Podľa tejto formuly, pravdivosť výroku P(e) je ekvivalentná pravdivosti výroku s existenčným kvantifikátorom $\exists x\, P(x)$.

Príklad 9.8. Ukážte, že predpoklady a záver

$\varphi 1$ = ‘každý kto navštevuje prednášky z diskrétnej matematiky je študentom informatiky‘

φ_2 = ‘Mária navštevuje prednášky z diskrétnej matematiky’

φ = ‘Mária je študentom informatiky’

sú správne.

Tieto tri výroky prepíšeme do tvaru

$$\frac{\begin{array}{l}\varphi_1 = \forall x \left(P(x) \Rightarrow I(x)\right) \\ \varphi_2 = P(Maria)\end{array}}{\varphi = I(Maria)}$$

kde $P(x)$ je predikát ‘objekt x navštevuje prednášku z diskrétnej matematiky’ a $I(x)$ je predikát ‘objekt x je študentom informatiky’. Korektnosť riešenia overíme postupnosťou formúl

1.	$\forall x \left(P(x) \Rightarrow I(x)\right)$	predpoklad$_1$
2.	$P(Maria)$	predpoklad$_2$
3.	$P(Maria) \Rightarrow I(Maria)$	konkretizácia 1
4.	$I(Maria)$	modus ponens na 2 a 3

Príklad 9.9. Ukážte, že dva predpoklady a záver

φ_1 = ‘*niektorí študenti navštevujúci prednášku nečítali predpísanú učebnicu* ‘

φ_2 = ‘*každý študent navštevujúci prednášku vykonal skúšku*’

φ = ‘*niektorí študenti, ktorí vykonali skúšku, nečítali predpísanú učebnicu*’

sú správne.

Tieto tri výroky prepíšeme do tvaru

$$\frac{\begin{array}{l}\varphi_1 = \exists x \left(P(x) \wedge \neg N(x)\right) \\ \varphi_2 = \forall x \left(P(x) \Rightarrow S(x)\right)\end{array}}{\varphi = \exists x \left(S(x) \wedge \neg N(x)\right)}$$

kde $P(x)$ je predikát *´objekt x navštevuje prednášku´*, $N(x)$ je predikát *´objekt x čítal predpísanú učebnicu´*, $S(x)$ je predikát *´objekt x vykonal skúšku´*. Korektnosť riešenia overíme postupnosťou formúl

1.	$\exists x\left(P(x)\wedge\neg N(x)\right)$	predpoklad$_1$
2.	$\forall x\left(P(x)\Rightarrow S(x)\right)$	predpoklad$_2$
3.	$P(c)\wedge\neg N(c)$	konkretizácia predpokladu$_1$
4.	$P(c)$	simplifikácia 3
5.	$\neg N(c)$	simplifikácia 3
6.	$P(c)\Rightarrow S(c)$	konkretizácia predpokladu$_2$
7.	$S(c)$	modus ponens na 4 a 6
8.	$S(c)\wedge\neg N(c)$	konjunkcia 5 a 7
9.	$\exists x\left(S(x)\wedge\neg N(x)\right)$	zovšeobecnie 8 pomocou existenčného kvantifikátora

Ako vidieť z uvedených príkladov, dôkazy formúl obsahujúcich kvantifikátory sú zmesou aplikácií schém usudzovania tak z výrokovej, ako aj predikátovej logiky. Táto skutočnosť vyplýva z faktu, že predikátová logika je vlastne zovšeobecnením výrokovej logiky, ktorá je „vnorená“ do predikátovej logiky; všetky zákony výrokovej logiky sú aj zákonmi predikátovej logiky.

9.4 Metódy dôkazu viet

Dôkaz vety je vo všeobecnosti obtiažny a netriviálny problém, ktorý len v ojedinelých prípadoch môže byť vykonaný priamočiarym mechanickým postupom. Preto v matematike vznikli rôzne metódy dôkazu viet, z ktorých uvedieme najdôležitejšie: priamy dôkaz, nepriamy dôkaz, dôkaz sporom a dôkaz vymenovaním prípadov.

Priamy dôkaz

Implikácia $p\Rightarrow q$ môže byť dokázaná tak, že ukážeme, že z predpokladu pravdivosti výroku p vyplýva taktiež aj pravdivosť výroku q. Túto jednoduchú formuláciu priameho dôkazu môžeme upresniť tak, že pri dôkaze vychádzame z axióm a z už dokázaných viet $\{\psi_1,...,\psi_m\}$, potom dôkaz $p\Rightarrow q$ môžeme charakterizovať vzťahom logického dôkazu

$$\{\varphi_1,...,\varphi_n\}\cup\{\psi_1,...,\psi_m\}\cup\{p\}\vdash q \qquad (9.21)$$

V tejto schéme máme na ľavej strane všetky axiómy systému, dokázané potrebné vety (tautológie) a predpoklad p, použitím pravidiel odvodzovania (modus ponens, pravidlá substitúcie,...) z týchto „predpokladov“ odvodíme dôsledok q.

Príklad 9.10. Dokáže vetu „ak n je nepárne prirodzené číslo, potom n^2 je taktiež nepárne číslo“.

Požadovanú vetu zformalizujeme pomocou implikácie

$$\underbrace{\left(n\ je\ nepárne\ číslo\right)}_{p}\Rightarrow\underbrace{\left(n^2\ \ je\ nepárne\ číslo\right)}_{q}$$

Použijeme techniku priameho dôkazu, z predpokladu pravdivosti p dokážeme pravdivosť dôsledku q.

Nech n je nepárne prirodzené číslo, potom existuje také nezáporné celé číslo k , že $n = 2k+1$. Pre kvadrát čísla n platí

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{l} + 1 = 2l + 1$$

čiže aj kvadrát n^2 je nepárne číslo. Týmto sme dokázali platnosť implikácie $p \Rightarrow q$.

Nepriamy dôkaz

Technika nepriameho dôkazu je založená na ekvivalencii (nazývanej zákon inverzie implikácie) $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$, podľa ktorej, ak v implikácii vymeníme poradie jej členov, potom musíme negovať aj jej jednotlivé členy. Z tohto zákona vyplýva, že dôkaz implikácie $(p \Rightarrow q)$ je ekvivalentný dôkazu „inverznej“ implikácie $\neg q \Rightarrow \neg p$.

Príklad 9.11. Dokážte vetu „ak $3n+2$ je nepárne číslo, potom aj n je nepárne číslo“.

Vetu upravíme do tvaru implikácie

$$\underbrace{(3n+2 \ \textit{je nepárne číslo})}_{p} \Rightarrow \underbrace{(n \ \textit{je nepárne číslo})}_{q}$$

Budeme dokazovať inverznú implikáciu

$$\underbrace{(n \ \textit{je párne číslo})}_{\neg q} \Rightarrow \underbrace{(3n+2 \ \textit{je párne číslo})}_{\neg p}$$

Nech n je párne číslo, potom existuje také nezáporné celé číslo k, že $n = 2k$. Pre takto špecifikované číslo n dostaneme $3n+2 = 3(2k)+2 = 2(3k+1)$, ktoré je párne. Týmto sme dokázali inverznú implikáciu $\neg q \Rightarrow \neg p$, čiže musí platiť aj „pôvodná“ implikácia $p \Rightarrow q$.

Dôkaz sporom

Tento typ dôkazu je založený na schéme „reductio ad absurdum“ z tab. 9.1

$$\left|\begin{array}{l} p \Rightarrow q \\ \underline{p \Rightarrow \neg q} \\ \neg p \end{array}\right. \tag{9.22}$$

založenej na zákone výrokovej logiky

$$(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p) \tag{9.23}$$

Túto schému usudzovania môžeme interpretovať tak, že ak z predpokladu p súčasne odvodíme q a $\neg q$, potom musí byť pravdivá negácia $\neg p$ východieho predpokladu.

Príklad 9.12. Dokážte, že $\sqrt{2}$ je iracionálne číslo.

Predpokladajme, že $\sqrt{2}$ je racionálne číslo, tento výrok označime

$$p = '\sqrt{2} \ \textit{je racionálne číslo}'$$

Z tohto výroku vyplýva, že číslo $\sqrt{2}$ má tvar α/β, kde α a β sú celé nesúdeliteľné čísla, tento výrok označíme

$$q = '\sqrt{2} = \alpha/\beta, \textit{kde } \alpha,\beta \textit{ sú celé nesúdeliteľné čísla}' .$$

t. j. platí implikácia $p \Rightarrow q$. Úpravou matematického výrazu z výroku q dostaneme formulu $\alpha^2 = 2\beta^2$, z ktorej vyplýva, že číslo $\alpha^2 = 2k$ je párne. V príklade 9.10 bola dokázaná veta, že ak celé číslo n je nepárne, potom aj jeho kvadrát n^2 je nepárne číslo. Obrátením tejto implikácie dostaneme, že ak n^2 je párne číslo, potom aj n je párne číslo. Z tejto vety vyplýva, že číslo α je párne. Potom taktiež platí $\beta^2 = 2k^2$, t. j. β^2 je párne číslo, čiže aj β je párne číslo. Týmto sme dokázali, že α, β sú párne čísla, čiže sú súdeliteľné

$$\neg q = '\sqrt{2} = \alpha/\beta, kde\ \alpha,\beta\ sú\ celé\ súdeliteľné\ čísla'$$

t.j. platí implikácia $p \Rightarrow \neg q$. Týmto sme dokázali, že súčasne platia implikácie $p \Rightarrow q$ a $p \Rightarrow \overline{q}$, použitím schémy „reductio ad absurdum“ (9.22) dostaneme, že platí negácia ich predpokladu

$$\neg p = '\sqrt{2}\ \ je\ iracionálne\ číslo'$$

čo bolo potrebné dokázať.

Dôkaz vymenovaním prípadov

Naším cieľom je dokázať implikáciu

$$(p_1 \vee ... \vee p_n) \Rightarrow q \tag{9.24}$$

Jednoduchými ekvivalentnými úpravami môžeme túto implikáciu prepísať do ekvivalentného tvaru

$$((p_1 \vee ... \vee p_n) \Rightarrow q) \equiv ((p_1 \Rightarrow q) \wedge ... \wedge (p_n \Rightarrow q)) \tag{9.25}$$

1.	$(p_1 \vee ... \vee p_n) \Rightarrow q$	
2.	$\neg(p_1 \vee ... \vee p_n) \vee q$	prepis 1 pomocou disjunktívneho tvaru implikácie
3.	$(\neg p_1 \wedge ... \wedge \neg p_n) \vee q$	použitie De Morganovho zákona 2
4.	$(\neg p_1 \vee q) \wedge ... \wedge (\neg p_n \vee q)$	použitie distributívneho zákona na 3
5.	$(p_1 \Rightarrow q) \wedge ... \wedge (p_n \Rightarrow q)$	prepis 4 pomocou disjunktívneho tvaru implikácie

Formulu (9.25) môžeme prepísať do tvaru schémy usudzovania

$$\begin{array}{|l} (p_1 \Rightarrow q) \\ ..... \\ (p_n \Rightarrow q) \\ \hline (p_1 \vee ... \vee p_n) \Rightarrow q \end{array} \tag{9.26}$$

Túto schému usudzovania (dôkaz vymenovaním prípadov) používame vtedy, ak výrok q je dôsledok rôznych prípadov p_1,..., p_n.

Príklad 9.13. Dokážte identitu

$$max\{a, min\{b,c\}\} = min\{max\{a,b\}, max\{a,c\}\}$$

kde *a*, *b* a *c* sú čísla.

Dôkaz tejto identity vykonáme tak, že vykonáme verifikáciu identity pre všetkých 6 rôznych prípadov:

(1) Prípad $a < b < c$

$$max\left\{a, \underbrace{min\{b,c\}}_{b}\right\} = min\left\{\underbrace{max\{a,b\}}_{b}, \underbrace{max\{a,c\}}_{c}\right\}$$

$$\underbrace{max\{a,b\}}_{b} = \underbrace{min\{b,c\}}_{b}$$

$$b = b$$

(2) Prípad $b < a < c$

$$max\left\{a, \underbrace{min\{b,c\}}_{b}\right\} = min\left\{\underbrace{max\{a,b\}}_{a}, \underbrace{max\{a,c\}}_{c}\right\}$$

$$\underbrace{max\{a,b\}}_{a} = \underbrace{min\{a,c\}}_{a}$$

$$a = a$$

Podobným spôsobom by sme preskúmali aj ostatné štyri možnosti vzájomného usporiadania čísel *a, b* a *c*. Týmto spôsobom sme dokázali 6 nezávislých implikácií

$$(a < b < c) \Rightarrow \left(max\{a, min\{b,c\}\} = b\right) \wedge \left(min\{max\{a,b\}, max\{a,c\}\} = b\right)$$

$$(b < a < c) \Rightarrow \left(max\{a, min\{b,c\}\} = a\right) \wedge \left(min\{max\{a,b\}, max\{a,c\}\} = a\right)$$

.....

$$(c < b < a) \Rightarrow \left(max\{a, min\{b,c\}\} = a\right) \wedge \left(min\{max\{a,b\}, max\{a,c\}\} = a\right)$$

Týmto „enumeratívnym“ spôsobom sme dokázali danú algebraickú identitu tak, že sme separátne preskúmali všetky možné usporiadania čísel *a, b* a *c*.

Príklad 9.14. Dokážte identitu $|a-b| \le |a| + |b|$, kde *a, b* sú ľubovolné reálne čísla a $|.|$ je absolútna hodnota.

(1) $a < b < 0$, potom $a - b < 0$, $a < 0$ a $b < 0$, dokazovaná nerovnosť má tvar $-(a-b) \le -a - b$, alebo $b \le 0$, čo je pravdivý výrok (pre $b = 0$ nerovnosť automaticky platí) .

(2) $a < 0 < b$, potom $a - b < 0$, $a < 0$ a $b > 0$, dokazovaná nerovnosť má tvar $-(a-b) \le -a + b$, čo je pravdivý výrok.

(3) $0 < a < b$, potom $a - b < 0$, $a > 0$ a $b > 0$, dokazovaná nerovnosť má tvar $-(a-b) \le a + b$, alebo $a \ge 0$, čo je pravdivý výrok (pre $a = 0$ nerovnosť automaticky platí).

Podobným spôsobom by sa dokázali aj ostatné tri možnosti ($b < a < 0, b < 0 < a$ a $0 < b < a$).

Nutnosť použitia metódy dôkazu vymenovaním všetkých prípadov sa môže stať v niektorých špeciálnych situáciách limitujúcim faktorom uskutočnenia dôkazu, keď počet možných prípadov je veľké číslo. Potom môžeme prenechať hlavná ťarcha dôkazu počítaču, ktorý systematicky preverí všetky možné prípady. Podobná situácia sa vyskytla počiatkom

90-tych rokov minulého storočia, keď matematik Andrew Wiles po dlhoročnom úsilí dokázal veľkú Fermatovu vetu[2].

9.5 Matematická indukcia

Stojíme pred problémom dokázať $\forall n\, P(n)$, podľa ktorej vlastnosť $P(n)$ platí pre každé prirodzené číslo. Dôkaz vety je možné vykonať metódou matematickej indukcie, ktorá je založená na dvoch východzích predpokladoch $P(1)$ a $\forall n\left(P(n) \Rightarrow P(n+1)\right)$. Ukážeme, že z týchto dvoch predpokladov vyplýva formula $\forall n\, P(n)$.

1.	$P(1)$	
2.	$\forall n\left(P(n) \Rightarrow P(n+1)\right)$	
3.	$P(1) \Rightarrow P(2)$	konkretizácia 2 pre $n = 1$
4.	$P(2) \Rightarrow P(3)$	konkretizácia 2 pre $n = 2$
.....	.....	
5.	$P(n) \Rightarrow P(n+1)$	konkretizácia 2 pre $n = n$
.....	.....	
6.	$P(2)$	modus ponens na 1 a 3
7.	$P(3)$	modus ponens na 6 a 4
.....	.....	
8.	$P(n+1)$	modus ponens na predchádzajúci riadok a 5
.....	.....	
9.	$\forall n\, P(n)$	zovšeobecnenie pomocou $\forall$

Tento výsledok môže byť prezentovaný ako schéma usudzovania matematickej indukcie

$$\begin{array}{|l} P(1) \\ \forall n\left(P(n) \Rightarrow P(n+1)\right) \\ \hline \forall n\, P(n) \end{array} \qquad (9.27)$$

Metóda matematickej indukcie bola známa už počiatkom novoveku talianskemu matematikovi F. Maurolico (1494 – 1575), ktorý ju používal k dôkazu niektorých vlastností celých čísel (napr. dokázal, že suma kvadrátov prvých n prirodzených nepárnych čísel sa rovná n^2). V modernej matematike a logike matematická indukcia bola využitá talianskym matematikom a logikom G. Peanom (1858 - 1932) pri formulácii jeho axiomatického systému aritmetiky celých čísel.

Príklad 9.15. Dokážte, že suma prvých n nepárnych prirodzených čísel sa rovná n^2.

[2] Veľká Fermatova veta tvrdí, že rovnica $x^n + y^n = z^n$ nemá celočíselné riešenie pre x, y a z, pričom $xyz \neq 0$ a n je celé číslo, pričom $n > 2$. Wilesov článok, v ktorom podal dôkaz tejto vety, "Modular Elliptic Curves and Fermat's Last Theorem" bol publikovaný v r. 1995 v časopise *Annals of Mathematics.* Článok je doprevádzaný vysoko technickou publikáciou jeho doktoranda Richarda Taylora, v ktorom boli enumeratívnym spôsobom preštudované na počítači vlastnosti špeciálnej Heckeho algebry, ktorej použitie hrá kľúčovú úlohu v celom dôkaze.

Položíme

$$P\left(n=2k-1\right)=1+3+5+...+\left(2k-1\right)=\sum_{i=1}^{k}\left(2i-1\right)=k^2$$

Ľahko sa presvedčíme, že platí P(1) = 1. Budeme študovať $P(n+1)$

$$P\left(n=2k+1\right)=1+3+5+...+\left(2k+1\right)=\sum_{i=1}^{k+1}\left(2i-1\right)=\sum_{i=1}^{k}\left(2i-1\right)+\left(2k+1\right)$$

$$=k^2+\left(2k+1\right)=\left(k+1\right)^2$$

Týmto sme dokázali, že platnosť formule $P(n)$ implikuje formulu $P(n+1)$, pre každé prirodzené číslo n, potom použitím zovšeobecnenia pomocou univerzálneho kvantifikátora dostaneme $\forall n\left(P\left(n\right)\Rightarrow P\left(n+1\right)\right)$. Použitím schémy matematickej indukcie dostaneme

$$\forall n\, P\left(n=2k-1\right)=k^2$$

čím sme zavŕšili dôkaz vety špecifikujúcej sumu prvých n nepárnych prirodzených čísel.

Príklad 9.16. Dokážte, že pre každé prirodzené číslo n platí $n<2^n$.

Nech $P(n)$ je predikát ´ $n<2^n$ ´, potom $P(1)$ je pravdivý predikát. Budeme študovať $P(n+1)$

$$\left(n+1\right)<2^{n+1}\Rightarrow\left(n\right)<\left(2^n\cdot 2\right)-1\Rightarrow\left(n\right)<2^n\cdot 2$$

kde sme použili indukčný predpoklad $n<2^n$ a ktorá evidentne platí už pre $n\geq 2$. Týmto sme dokázali, že pre každé prirodzené číslo n platí implikácia $P\left(n\right)\Rightarrow P\left(n+1\right)$, alebo $\forall n\left(P\left(n\right)\Rightarrow P\left(n+1\right)\right)$. Týmto sme vlastne dokázali platnosť $\forall n\left(n<2^n\right)$

Príklad 9.17. Pomocou matematickej indukcie dokážte platnosť zovšeobecneného De Morganovho vzťahu z teórie množín

$$\overline{\bigcap_{i=1}^{n}A_i}=\bigcup_{i=1}^{n}\overline{A_i}$$

pre $n\geq 2$.

Položme

$$P\left(n\right)=\overline{\bigcap_{i=1}^{n}A_i}=\bigcup_{i=1}^{n}\overline{A_i}$$

Pre n = 2 dostaneme

$$P\left(2\right)=\overline{A_1\cap A_2}=\overline{A}_1\cup\overline{A}_2$$

čo je štandardná verzia De Morganovho zákona pre negáciu prieniku dvoch množín. Študujme

$$P\left(n+1\right)=\overline{\bigcap_{i=1}^{n+1}A_i}=\overline{\bigcap_{i=1}^{n}A_i\cap A_{n+1}}=\overline{\bigcap_{i=1}^{n}A_i}\cup\overline{A_{n+1}}=\bigcup_{i=1}^{n}\overline{A_i}\cup\overline{A_{n+1}}=\bigcup_{i=1}^{n+1}\overline{A_i}$$

Týmto sme dokázali implikáciu zovšeobecnenú pomocou univerzálneho kvantifikátora

$$\forall\left(n\geq 2\right)\left(P\left(n\right)\Rightarrow P\left(n+1\right)\right)$$

čím sme dokázali pomocou matematickej indukcie zovšeobecnenie De Morganovho vzťahu pre negáciu prieniku dvoch a viac množín.

9.5.1 Silná matematická indukcia

Špeciálna forma matematickej indukcie je keď platnosť vlastnosti P(n+1) je implikovaná konjunkciou všetkých predchádzajúcich vlastností $P(1) \wedge P(2) \wedge ... \wedge P(n) \Rightarrow P(n+1)$, postulujme, že táto vlastnosť je splnená pre každé $n \geq 1$, potom $\forall n \left(P(1) \wedge ... \wedge P(n) \Rightarrow P(n+1) \right)$. Zostrojme zovšeobecnenú schému usudzovania matematickej indukcie

$$\frac{\begin{array}{l} P(1) \\ \forall n \left(P(1) \wedge P(2) \wedge ... \wedge P(n) \Rightarrow P(n+1) \right) \end{array}}{\forall n \, P(n)}$$

Nebudeme dokazovať túto schému usudzovania, jej dôkaz je úplne analogický dôkazu schémy usudzovania matematickej indukcie (9.27).

Príklad 9.18. Dokážte, že ľubovolné prirodzené číslo $n > 1$ môže byť vyjadrené ako súčin prvočísiel.

Nech vlastnosť $P(n)$ má tvar

$$P(n) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} ....$$

kde p_1, p_2, p_3, ... sú prvé prvočísla (2, 3, 5,...) a α_1, α_2, α_3, ...sú nezáporné celé čísla. Táto formula je pravdivá pre $P(2)$, kde α_1=1, $\alpha_2 = \alpha_3 = ... = 0$, potom $P(2) = 2$. Predpokladajme, že $P(j)$ je pravdivé pre každé prirodzené $j \leq n$. Ukážeme, že z tohto predpokladu vyplýva platnosť $P(n + 1)$. Bude rozlišovať dva prípady:

1. *prípad* – $P(n+1)$ je prvočíslo p, potom P(n+1) = p .
2. *prípad* – $P(n+1)$ nie je prvočíslo, potom môže byť písané ako súčin dvoch prirodzených čísel $2 < a \leq b < n+1$. Každé z týchto dvoch čísel môže byť vyjadrené ako súčin prvočísiel (indukčný predpoklad)

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} ....$$
$$a = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k} ....$$

potom ich súčin má tvar

$$P(n+1) = a \cdot b = p_1^{\alpha_1 + \beta_1} p_2^{\alpha_2 + \beta_2} ... p_k^{\alpha_k + \beta_k} ....$$

Cvičenie

Cvičenie 9.1. Aké pravidlo usudzovania bolo použité pri dôkaze záverov?

(a) Mária je študentom informatiky. Preto, je Mária študentom informatiky alebo študentom telekomunikácií.
(b) Jaroslav študuje informatiku a elektrotechnológiu. Preto, Jaroslav študuje informatiku.
(c) Ak prší, potom plaváreň je zatvorená. Preto, ak plaváreň je otvorená, potom neprší.
(d) Ak dnes sneží, kino bude uzavreté. Kino dnes nie je uzavreté. Preto, dnes nesneží.
(e) Ak dnes pôjdem plávať, potom ráno skoro vstanem. Ak ráno skoro vstanem, potom pôjdem do obchodu kúpiť čerstvé pečivo. Preto, ak dnes pôjdem plávať, potom pôjdem do obchodu kúpiť čerstvé pečivo.

Cvičenie 9.2. Aké pravidlo usudzovania bolo použité pri dôkaze záverov?

(a) Dnes bude teplo alebo bude smog v ovzduší. Dnes nebolo teplo. Preto, dnes bude smog v ovzduší.

(b) Eva vynikajúco pláva. Ak Eva je vynikajúci plavec, potom môže pracovať ako plavčík. Preto, Eva môže pracovať ako plavčík.
(c) Stano bude pracovať v počítačovej firme ABC. Ak Stano dokončí štúdium na FIIT, potom nebude pracovať v počítačovej firme ABC. Preto, Stano nedokončil štúdium na FIIT.
(d) Ak budem intenzívne pracovať na projekte, potom zvládnem teóriu logických obvodov. Ak zvládnem teóriu logických obvodov, potom úspešne dokončím bakalárske štúdium. Preto, ak budem intenzívne pracovať na projekte, potom úspešne dokončím bakalárske štúdium.

Cvičenie 9.3. Aké závery vyplývajú z množiny výrokov?
(a) „Ak jem korenenú stravu, potom mám hrozné sny“, „ak hrmí keď spím, potom mám hrozné sny“, „nemám hrozné sny“.
(b) „Ja som chytrý alebo mám šťastie“, „nemám šťastie“, „ak mám šťastie, potom zvíťazím v lotérii“.
(c) „Každý študent informatiky vlastní notebook“, „Rudo nevlastní notebook“, „Ana vlastní notebook“.
(d) „Čo je dobré pre našu firmu, je dobré aj pre Slovensko“, „čo je dobré pre Slovensko, je dobré aj pre teba“, „ak si nemôžeš kúpiť auto, potom to nie je pre teba dobré“.
(e) „Všetci hlodavce hryzú potravu“, „myš je hlodavec“, „pes nehryzie potravu“, „netopier nie je hlodavec“.

Cvičenie 9.4. Vysvetlite, ktorá schéma usudzovania bola použitá v ktorom kroku.
(a) „Eva je študentka nášho krúžku a vlastní červené auto“, „každý, kto vlastní červené auto dostal aspoň jednu pokutu za prekročenie rýchlosti“, „preto, niekto z nášho krúžku dostal pokutu za prekročenie rýchlosti“.
(b) „Všetci moji priatelia Mária, Adolf, Rudolf, Viera a Karol, si zapísali do indexu prednášku z diskrétnej matematiky“, „každý študent, ktorý si zapísal do indexu prednášku z diskrétnej matematiky, môže si nasledujúci akademický rok zapísať aj prednášku z algoritmov“, „preto, všetci moji priatelia Mária, Adolf, Rudolf, Viera a Karol, môžu si nasledujúci akademický rok zapísať do indexu prednášku z algoritmov“.
(c) „Všetky filmy s Charlie Chaplinom sú vynikajúce“, „Charlie Chaplin hral v nemých filmoch“, „preto, niektoré vynikajúce filmy sú nemé“.

Cvičenie 9.5. Vysvetlite prečo uvedené závery sú korektné alebo nekorektné.
(a) „Všetci študenti v tomto krúžku ovládajú logiku“, „Jano je študentom tohto krúžku“, „preto, Jano ovláda logiku“.
(b) „Každý študent informatiky má zapísanú v indexe prednášku z diskrétnej matematiky“, „Viera má zapísanú prednášku z diskrétnej matematiky“, „preto, Viera je študentom informatiky“.
(c) „Každý kôň má rád ovocie“, „môj pes nie je kôň“, „preto, môj pes nemá rád ovocie“.
(d) „Každý, kto má rád ovsené vločky je zdravý“, „Lenka nie je zdravá“, „preto, Lenka nemá rada ovsené vločky“.

Cvičenie 9.6. Určite, ktorá veta je pravdivá. Ak je uvedený záver korektný, určite, ktorá schéma usudzovania bola použitá pri jeho dôkaze.
(a) Ak x je reálne číslo také, že $x>1$, potom $x^2>1$. Predpokladajte, že $x^2>1$, potom $x>1$.

(b) Číslo $log_2 3$ je iracionálne vtedy, ak sa nedá vyjadriť ako podiel dvoch celých nesúdeliteľných čísel. Pretože číslo $log_2 3$ nie je vyjadriteľné ako p/q, kde p a q sú celé nesúdeliteľné čísla, potom je číslo $log_2 3$ iracionálne.

(c) Ak x je reálne číslo, ktoré spĺňa podmienku $x > 3$, potom $x^2 > 9$. Nech $x^2 \leq 9$, potom $x \leq 3$.

(d) Ak x je reál ne číslo, ktoré spĺňa podmienku $x > 2$, potom $x^2 > 4$. Nech $x \leq 2$, potom $x^2 \leq 4$.

Cvičenie 9.7. Určite, či uvedené výroky sú korektné, ak nie, prečo?

(a) Ak x^2 je iracionálne, potom x je iracionálne. Preto, ak x je iracionálne, potom x^2 je iracionálne.

(b) Ak x^2 je iracionálne, potom x je iracionálne. Číslo $x = \pi^2$ je iracionálne. Preto, číslo $x = \pi$ je iracionálne.

Cvičenie 9.8. Prečo tieto výroky sú nekorektné?

(a) Nech $H(x)$ je predikát s významom „x je štastný“. Nech platí $\exists x\, H(x)$. Preto, Eva je šťastná.

(b) Nech $S(x,y)$ je predikát s významom „x je menší ako y“. Nech platí implikácia $\exists s\, S(s,Max) \Rightarrow S(Max,Max)$.

Cvičenie 9.9. Dokážte, keď sa dajú dokázať, tieto výroky:

(a) Dokážte výrok $P(0)$, kde $P(n)$ je výrok „ak n je kladné celé číslo väčšie ako 1, potom $n^2 > n$. Ktorú schému usudzovania sme použili?

(b) Dokáže výrok $P(1)$, kde $P(n)$ je výrok „Ak n je kladné celé číslo, potom $n^2 > n$. Ktorú schému usudzovania sme použili?

(c) Nech $P(n)$ je výrok „ak a a b sú kladné reálne čísla, potom $(a+b)^n \geq a^n + b^n$“. Dokážte, že P(1) je pravdivý výrok.

(d) Dokážte, že kvadrát párneho čísla je párne číslo použitím priameho dôkazu.

(e) Dokážte, že ak n je celé číslo a $n^3 + 5$ je nepárne číslo, potom n je párne číslo použitím nepriameho dôkazu.

(f) Dokážte, že suma dvoch nepárnych čísel je párne číslo.

(g) Dokážte, že súčin dvoch nepárnych čísel je nepárne číslo.

(h) Dokáže, že ak x je iracionálne nenulové číslo, potom $1/x$ je iracionálne číslo.

Cvičenie 9.10. Dokážte metódou vymenovaním prípadov tieto vlastnosti:

(a) $max\{x,y\} + min\{x,y\} = x + y$, kde x, y sú reálne čísla.

(b) $min\{a,min\{b,c\}\} = min\{min\{a,b\},c\}$

(c) Kvadráty celých čísel sú reprezentované dekadickými číslicami, ktoré končia 0, 1, 4, 5, 6, alebo 9.

(d) Štvrté mocniny celých čísel sú reprezentované dekadickými číslami, ktoré končia 0, 1, 5, alebo 6.

Cvičenie 9.11. Dokážte tieto vlastnosti:

(a) Ak n je kladné celé číslo, potom n je párne vtedy a len vtedy, ak $7n+4$ je párne.

(b) Ak n je kladné celé číslo, potom n je nepárne vtedy a len vtedy, ak $5n+6$ je nepárne.

(c) $m^2 = n^2$ platí vtedy a len vtedy, ak $m = n$, alebo $m = -n$.

(d) Dokážte, že tieto tri výroky sú ekvivalentné: (1) $a \le b$, (2) priemer a a b je väčší ako a, $(a+b)/2 > a$, (3) priemer a a b je menší ako b, $(a+b)/2 < b$.

Cvičenie 9.12. Pomocou matematickej indukcie dokážte:

(a) Suma prvých n prirodzených čísel je

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

(b) Dokážte formulu

$$3+3\cdot 5+3\cdot 5^2+\ldots+3\cdot 5^n=\frac{1}{4}3\left(5^{n+1}-1\right)$$

(c) Nájdite formulu pre

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{n(n+1)}$$

(d) Dokážte formulu

$$1^2+2^2+3^2+\ldots+n^2=\frac{1}{6}n(n+1)(2n+1)$$

(e) Dokážte formulu

$$1^3+2^3+3^3+\ldots+n^3=\frac{1}{4}n^2(n+1)^2$$

(f) Dokážte formulu $n! < n^n$, pre $n > 1$.

(g) Dokážte formulu pre prvú deriváciu funkcie $f(x)=x^n$, $f'(x)=nx^{n-1}$.

(h) Nech $\boldsymbol{A}$ a $\boldsymbol{B}$ sú štvorcové matice, ktoré komutujú, $\boldsymbol{AB} = \boldsymbol{BA}$, dokážte $\boldsymbol{AB}^n = \boldsymbol{B}^n\boldsymbol{A}$.

(i) Dokážte

$$\overline{\bigcup_{i=1}^{n} A_i}=\bigcap_{i=1}^{n}\overline{A_i}$$

(j) Dokážte zovšeobecnené distributívne formuly z výrokovej logiky

$$(p_1\vee p_2\vee\ldots\vee p_n)\wedge q\equiv(p_1\wedge q)\vee(p_2\wedge q)\vee\ldots\vee(p_n\wedge q)$$

$$(p_1\wedge p_2\wedge\ldots\wedge p_n)\vee q\equiv(p_1\vee q)\wedge(p_2\vee q)\wedge\ldots\wedge(p_n\vee q)$$