ALGEBRA A DISKRÉTNE MATEMATIKA

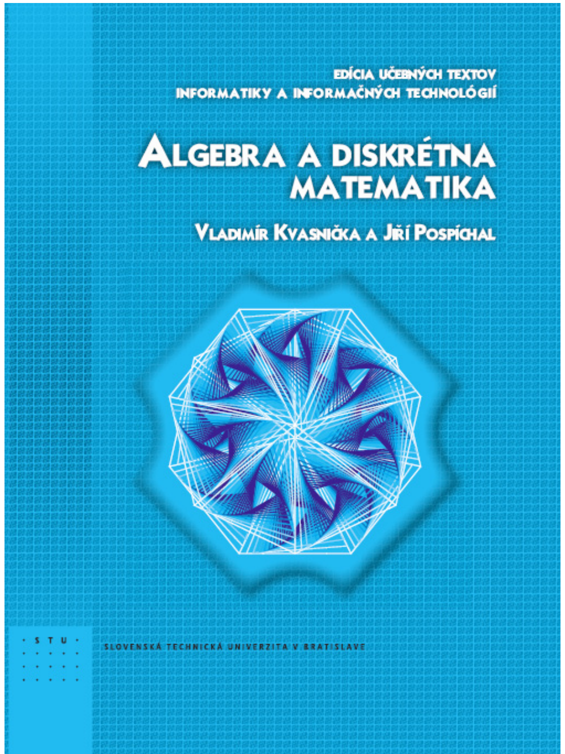
rozsah: 3-2-0

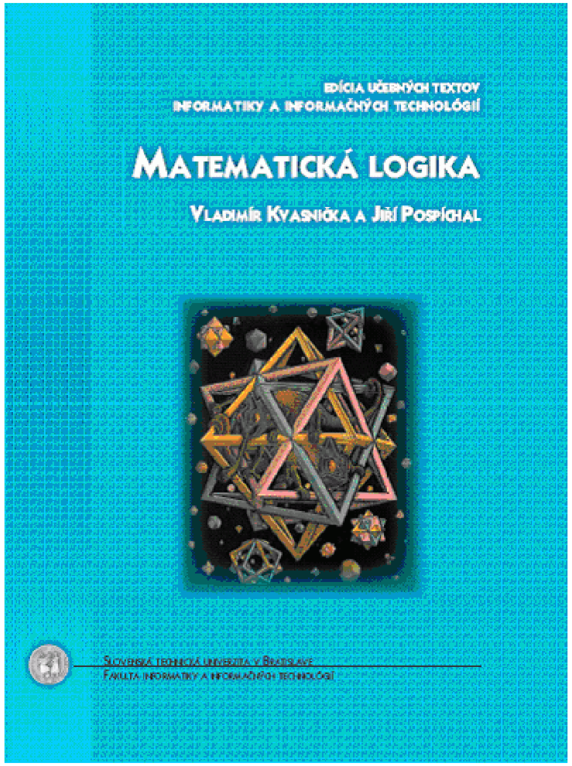
prednáška **cvičenie**

Prednáška: štvrtok 10.00-13.00 hod. v BC300
piatok 9.00-12.00 hod. v DE300

prednášajú: prof. Ing. Vladimír Kvasnička, DrSc.
prof. RNDr. Jiří Pospíchal, DrSc.

Vyšli knihy vo Vydavateľstve STU





Na web stránke sú priesvitky ku každej knihy v PDF formáte

Rozvrh cvičení z predmetu ADM, zimný semester, akad. rok 2011-12

#	deň	čas	dvojkrúžok	miestnosť	cvičiaci
1	utorok	7-9	17,18	BC35	Varga
2	utorok	9-11	11,12	BC35	Varga
3	utorok	11-13	111,112	BC35	Chalupa
4	streda	13-15	13,14	BC35	Chalupa
5	streda	15-17	121,122	CD35	Kovárová
6	streda	17-19	123,124	BC35	Pospíchal (Pálfy)
7	streda	13-15	19,110	CD35	Kovárová
8	streda	15-17	15,16	BC35	Pospíchal (Pálfy)
9	štvrtok	13-15	119,120	C201	Kobza
10	štvrtok	15-17	113,114	C201	Kobza
11	štvrtok	17-19	117,118	C201	Clementis
12	štvrtok	19-21	115,116	C201	Clementis

Predmet je totálne transparentný!!

Web stránka predmetu je na adrese

http://www2.fiit.stuba.sk/~kvasnicka/DiskretnaMatematika

Čo vás čaká v priebehu semestra?

- **dve kontrolné písomky (2x20 = 40 bodov), na zápočet je potrebné získať min. 18 bodov**
- **záverečná písomná skúška (60 bodov), na absolvovanie predmetu je potrebné získať min. 56 bodov**

1. prednáška

Metódy matematického dôkazu

- **deduktívny dôkaz**
- **základné pravidlá usudzovania**
- **matematická indukcia.**

Význam dôkazu v matematike

V matematike, podobne ako aj v informatike, vystupujú do popredia dve otázky:

(1) Za akých podmienok je matematický argument korektný a
(2) aké metódy môžu byť použité pri konštrukcii matematických argumentov.

- ***Veta*** (teorém, výrok, skutočnosť, fakt, alebo výsledok) je výrok o ktorom môže byť ukázané, že je pravdivý.

- ***Dôkaz*** vety – je postupnosť argumentov, ktoré sú odvodené buď z množiny jednoduchých argumentov – postulátov, nazývaných *axiómy*, alebo z predchádzajúcich argumentov (pomocných viet, často nazývané lemy) danej postupnosti.

- Postupnosť argumentov môže byť podstatne ***skrátená***, keď bude obsahovať už dokázané vety, ktoré sú založené na rovnakej množine axióm.

Deduktívny dôkaz

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

Induktívne usudzovanie (dôkaz)

- Používa sa v informatike a v matematike len ***ojedinele***.

- Jej použitie je založené na ***pozorovaní*** určitých skutočností, na ich častom opakovaní 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 zaznamená v dejinách matematiky vždy znamenali ***vznik nových oblastí matematiky***, ktoré nie sú striktne deduktívne dokázateľné zo známych pojmov a reprezentujú akty kreatívnosti v matematike.

Ilustračný príklad axiomatického systému

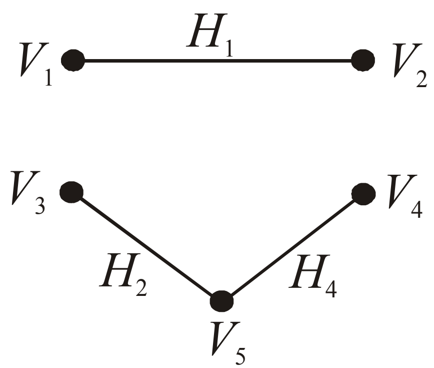
Uvažujme jednoduchý axiomatický systém, ktorý obsahuje tri *elementárne pojmy* – ´vrchol´, ´hrana´, ´ležať na´ a dve *axiómy*

A_1. Každý vrchol leží aspoň na jednej hrane.
A_2. Pre každú hranu existujú práve dva vrcholy, ktoré ležia na nej.
A_3. Máme práve 5 vrcholov.

Použitá terminológia navodzuje zavedenie modelu *grafu*, kde vrchol je bod a hrana je čiara obsahujúca na svojich koncoch dva vrcholy.

Veta 1. Každý graf má aspoň tri hrany.

Veta 2. Každý graf má jeden vrchol, ktorý leží aspoň na dvoch hranách.



Deduktívny systém rozšírime o nový elementárny pojem „komponenta“, ktorý popisuje takú časť grafu, z ktorej vrcholy z druhej časti nie sú spojené cestou pozostávajúcou z postupnosti hrán.

Veta 3. Ak má graf dve komponenty, potom jedna z komponent obsahuje len jednu hranu.

Pravidlá usudzovania vo výrokovej logike

Pravidlá usudzovania vo výrokovej logike tvoria schému

$$\begin{array}{|l}
predpoklad_1 \\
\ldots\ldots\ldots\ldots\ldots \\
predpoklad_n \\
\hline
záver
\end{array}$$

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

$$\{predpoklad_1, \ldots, predpoklad_n\} \vdash záver$$

Schémy usudzovania výrokovej logiky

Schéma usudzovania	Teorém výrokovej logiky	Názov schémy
$\dfrac{p}{p \vee q}$	$p \Rightarrow (p \vee q)$	adícia
$\dfrac{p \wedge q}{p}$	$(p \wedge q) \Rightarrow p$	simplifikácia (zjednodušenie)
$\dfrac{p \quad q}{p \wedge q}$	$p \Rightarrow (q \Rightarrow (p \wedge q))$	konjunkcia
$\dfrac{p \quad p \Rightarrow q}{q}$	$p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$	modus ponenes
$\dfrac{\neg q \quad p \Rightarrow q}{\neg p}$	$\neg q \Rightarrow ((p \Rightarrow q) \Rightarrow \neg p)$	modus tollens

$\dfrac{p \Rightarrow q \quad q \Rightarrow r}{p \Rightarrow r}$	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	hypotetický sylogizmus
$\dfrac{p \vee q \quad \neg p}{q}$	$(p \vee q) \Rightarrow (\neg p \Rightarrow q)$	disjunktívny sylogizmus
$\dfrac{p \Rightarrow q}{\neg q \Rightarrow \neg p}$	$(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$	inverzia implikácie
$\dfrac{p \Rightarrow q \quad p \Rightarrow \neg q}{\neg p}$	$(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$	reductio ad absurdum

Schémy usudzovania píšeme alternatívne takto

$$\{\varphi_1, \ldots, \varphi_n\} \vdash \varphi$$

$$\vdash \varphi_1 \wedge \ldots \wedge \varphi_n \Rightarrow \varphi$$

$$\vdash \varphi_1 \Rightarrow \left(\varphi_2 \Rightarrow \left(\Rightarrow \ldots \left(\varphi_n \Rightarrow \varphi\right)\right)\right)$$

Príklad

Prvý predpoklad je výrok ´*prší*´
Druhý predpoklad je implikácia ´*ak prší, potom je cesta mokrá*´ .

Použitím *modus ponens* dostaneme záver ´*cesta je mokrá*´,

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

$$\begin{array}{|l} p \\ \underline{p \Rightarrow q} \\ q \end{array}$$

Príklad

k pravdivému výroku ´*teplota je pod bodom mrazu*´

Použitím schémy usudzovania *adície* dostaneme pravdivý záver ´*teplota je pod bodom mrazu alebo prší*´

$$\left| \frac{\textit{teplota je pod bodom mrazu}}{\textit{teplota je pod bodom mrazu alebo prší}} \right.$$

$$\left| \frac{p}{p \vee q} \right.$$

Príklad

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

Túto schému môžeme sformalizovať pomocou štyroch výrokov

$$p = \text{´}dnes\ prší\text{´}$$
$$q = \text{´}kúpem\ sa\text{´}$$
$$r = \text{´}navštívim\ príbuzného\text{´}$$

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

Táto schéma je jemne modifikovaný hypotetický sylogizmus substitúciu

Príklad

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*´

Výrokové premenné

p = ´*dnes poobede nie je slnečno*´

q = ´*je chladnejšie ako včera*´

r = ´ *pôjdeme sa kúpať* ´

s = ´ *budeme člnkovať na rieke*´

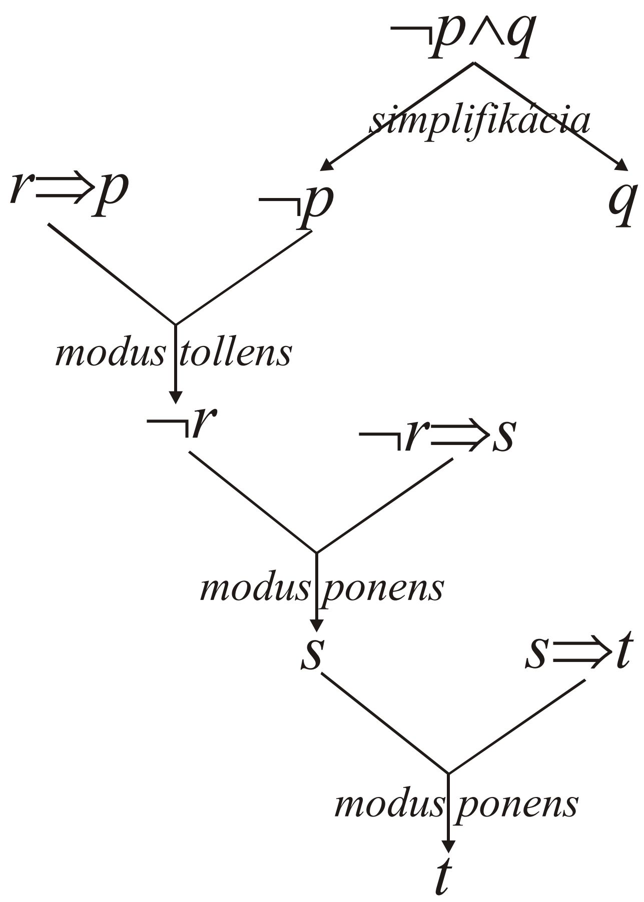
t = ´ *vrátime domov podvečer*´

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

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 preddpoklad$_2$
8.	s	medzivýsledok 7 a modus ponens na predpoklad$_3$
9.	t	medzivýsledok 8 a modus ponens na predpoklad$_4$

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

Diagramatická reprezentácia príkladu



Príklad

Množina predpokladov obsahuje tieto formuly – zložené výroky:

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

φ_2 = ´*ak mi nepošleš email, potom pôjdeme 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* ´

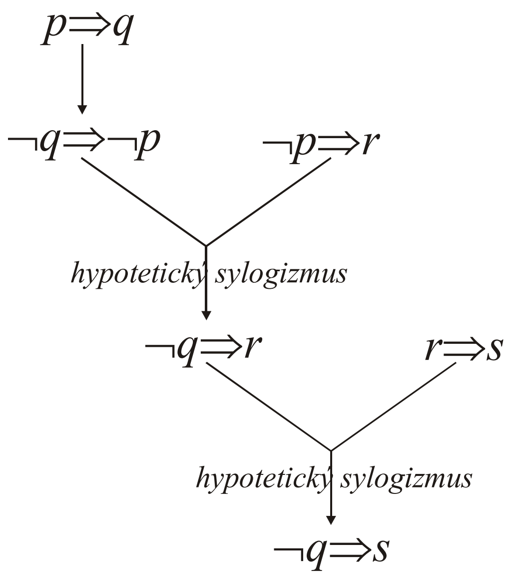
q = ´*program dokončím*´

r = ´*pôjdeme spať včasnejšie*´

s = ´*sa ráno zobudím odpočinutý*´

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

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 predpokladu$_2$
6.	$\neg q \Rightarrow s$	hypotetický sylogizmus na medzivýsledok 5 a preddpoklad$_3$



Veta o dedukcii

Uskutočnenie logického dôkazu $\{\varphi_1,\ldots,\varphi_n\} \vdash \varphi$ môže byť podstatne zjednodušené ak množinu predpokladov $\{\varphi_1,\ldots,\varphi_n\}$ rozšírime o nový predpoklad ψ, potom

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

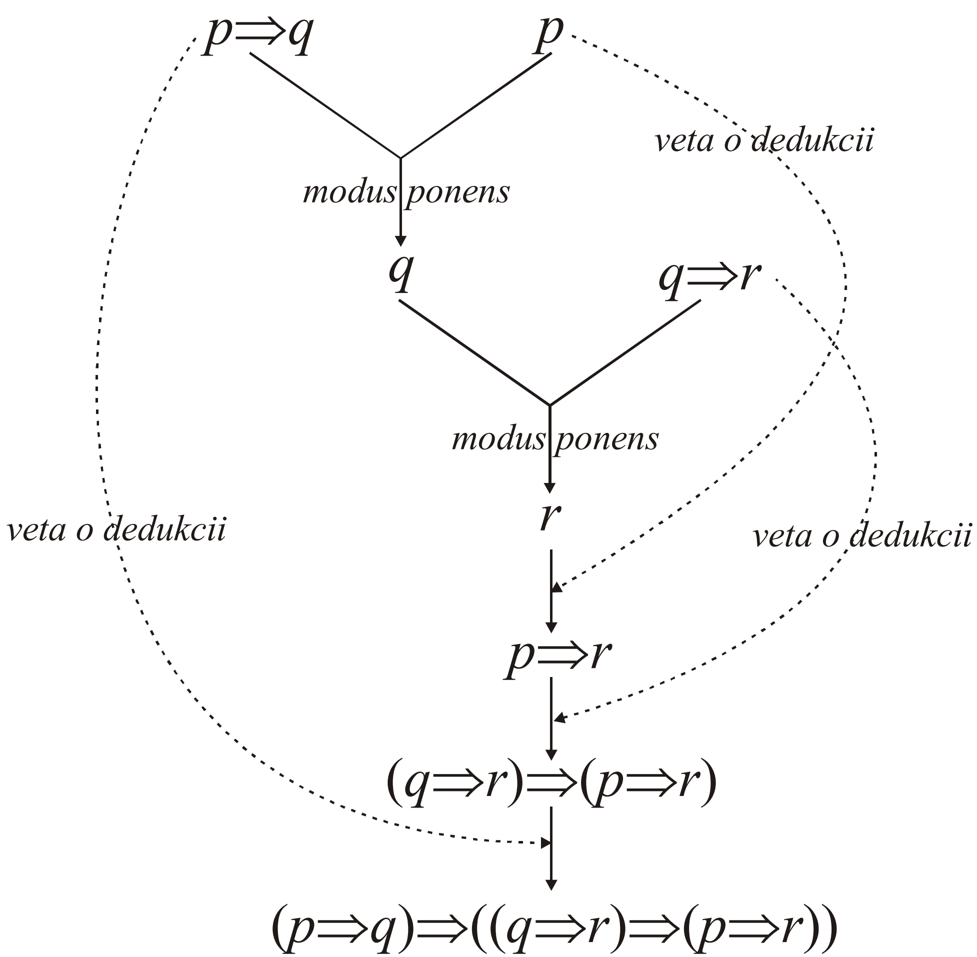
Logický dôkaz formuly φ pomocou rozšírenej množiny predpokladov $\{\varphi_1,\ldots,\varphi_n\} \cup \{\psi\}$ je rovnocenný logickému dôkazu formuly $\psi \Rightarrow \varphi$ pomocou pôvodnej množiny predpokladov.

Príklad

Pomocou logického dôkazu založeného na vete o dedukcii dokážte zákon hypotetického sylogizmu výrokovej logiky

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

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.	$p \Rightarrow r$	veta o dedukcii na výsledok 5 a pomocný predpoklad
7.	$(q \Rightarrow r) \Rightarrow (p \Rightarrow r)$	veta o dedukcii na výsledok 6 a predpoklad$_2$
8.	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$	veta o dedukcii



$p \Rightarrow q$
p
modus ponens
veta o dedukcii
q
$q \Rightarrow r$
modus ponens
r
veta o dedukcii
veta o dedukcii
$p \Rightarrow r$
$(q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$

- Vety majú významné 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

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

Príklad

Dokážte zákon rezolventy

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

pomocou zákona hypotetického sylogizmu

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

a pomocou vety o disjunktnom tvare implikácie

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

formálne

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

$$\vdash ((p \vee q) \Rightarrow ((\neg p \vee r) \Rightarrow (q \vee r)))$$

Logický dôkaz pozostáva z tejto postupnosti medzivýsledkov:

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

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

Chybné pravidlá usudzovania

Prvá nekorektná schéma sa nazýva ***potvrdenie dôsledku***

$$\begin{array}{|l} q \\ p \Rightarrow q \\ \hline p \end{array}$$

Druhá nekorektná schéma sa nazýva ***popretie predpokladu***

$$\begin{array}{|l} \neg p \\ p \Rightarrow q \\ \hline \neg q \end{array}$$

Prvá schéma „popretie predpokladu“ je ilustrovaná príkladom

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

Druhá schéma „potvrdenie dôsledku môže byť ilustrovaná podobným príkladom

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

O nekorektnosti týchto dvoch schém usudzovania sa ľahko presvedčíme tak, že im priradíme formuly výrokovej logiky, ktoré nie sú tautológie

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

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

Pravidlá usudzovania v predikátovej logike

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

Konkretizácia univerzálneho kvantifikátora

Ak nejaká vlastnosť $P(x)$ platí pre každý objekt (indivíduum) z univerza U, $\forall x\, P(x)$, potom túto vlastnosť musí mať aj ľubovoľný konkrétny objekt c z tohto univerza,

$$\left(\forall x\, P(x)\right) \Rightarrow P(c)$$

Táto vlastnosť je priamym dôsledkom interpretácia univerzálneho kvantifikátora

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

$$\begin{array}{|l} \forall x\, P(x) \\ \hline P(a) \\ P(b) \\ \ldots\ldots\ldots \\ P(c) \\ \ldots\ldots\ldots \end{array}$$

Príklad

Príklad konkretizácie zo stredovekej logiky

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

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

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

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 $\forall$

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

$$\begin{array}{|l} P(a) \\ \ldots\ldots\ldots \\ P(c) \\ \ldots\ldots\ldots \\ \hline \forall x\, P(x) \end{array}$$

$$P(c) \Rightarrow \left(\forall x\, P(x)\right)$$

- V mnohých prípadoch mimo matematiku použitie zovšeobecnenia podľa tejto schémy usudzovania tvorí základ tzv. ***induktívneho zovšeobecnia***, v ktorom sú parciálne poznatky zovšeobecnené 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, $\neg \forall x\, P(x)$.

Príklad

- Univerzum U 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) , 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 $B(x)$.
- Toto rozširovanie platnosti $\forall' x\, B(x)$ o ďalšie objekty nám neprináša žiadnu zásadne nový poznatok, neustále platí, že „labute sú biele“, len máme o tejto skutočnosti stále rozsiahlejšie vedomosti o evidentnosti tohto poznatku.
- Preto, ako prvý zdôraznil Karl Popper, falzifikácia na rozdiel od verifikácie, je zásadne dôležitá pre induktívne zovšeobecňovanie, napomáha nám pri vzniku nových poznatkov.

Konkretizácia existenčného kvantifikátora

$$\left(\exists x\, P(x)\right) \Rightarrow P(c)$$

$$\begin{array}{|l} \exists x\; P(x) \\ \hline P(c)\ \textit{pre nejaký element } c \end{array}$$

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

Zovšeobecnenie pomocou existenčného kvantifikátora

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

$$\begin{array}{|l} P(c)\ \textit{pre nejaký element } c \\ \hline \exists x\, P(x) \end{array}$$

$$P(c) \equiv \exists x\, P(x)$$

Príklad

Predpoklady:

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

φ_2 = ‘Mária navštevuje prednášky z diskrétnej matematiky’

Záver:

φ = ‘Mária je študentom informatiky’

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

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

Predpoklady:

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

φ_2 = '*každý študent navštevujúci prednášku vykonal skúšku*'

Záver:

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

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

1.	$\exists x \left(P(x) \wedge \neg N(x) \right)$	prepdoklad$_1$
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

Metódy dôkazu viet

Priamy dôkaz

Implikácia $p \Rightarrow q$ je dokázaná tak, že z predpokladu pravdivosti p vyplýva pravdivosť výroku q.

$$\underbrace{\{\varphi_1,\ldots,\varphi_n\}}_{axi\acute{o}my} \cup \underbrace{\{\psi_1,\ldots,\psi_m\}}_{vety} \cup \underbrace{\{p\}}_{predpoklad} \vdash \underbrace{q}_{d\hat{o}sledok}$$

Príklad

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

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

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

čiže aj kvadrát n^2 je nepárne číslo.

Nepriamy dôkaz

Implikácie $(p \Rightarrow q)$ je dokázaná pomocou priameho dôkazu „inverznej“ implikácie $\neg q \Rightarrow \neg p$.

Príklad

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

Budeme dokazovať inverznú implikáciu

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

Nech n je párne číslo, potom $n = 2k$, potom $3n+2=3(2k)+2=2(3k+1)$, čo je párne číslo. Týmto sme dokázali inverznú implikáciu $\neg q \Rightarrow \neg p$, čiže musí platiť aj „pôvodná“ implikácia $p \Rightarrow q$.

Dôkaz sporom

Ak z predpokladu p súčasne odvodíme q a $\neg q$, potom musí byť pravdivá negácia $\neg p$ východiskového predpokladu.

Tento typ dôkazu je založený na schéme „reductio ad absurdum“

$$\begin{array}{|l} p \Rightarrow q \\ p \Rightarrow \neg q \\ \hline \neg p \end{array}$$

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

Príklad

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

(1) implikácia $p \Rightarrow q$

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

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

(2) implikácia $p \Rightarrow \neg q$

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

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

$$\Downarrow$$

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

Dôkaz vymenovaním prípadov

Dôkaz vymenovaním prípadov používame vtedy, ak výrok q je dôsledok rôznych prípadov $p_1,\ldots,p_n$.

$$\left(p_1 \vee \ldots \vee p_n\right) \Rightarrow q$$

$$\left(\left(p_1 \vee \ldots \vee p_n\right) \Rightarrow q\right) \equiv \left(\left(p_1 \Rightarrow q\right) \wedge \ldots \wedge \left(p_n \Rightarrow q\right)\right)$$

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

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

Príklad

Dokážte identitu

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

(1) Prípad $a<b<c$

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

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

(2) Prípad $b<a<c$

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

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

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

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

....

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

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

Matematická indukcia

Metóda matematickej indukcie dokazuje $\forall n\, P(n)$ pomocou dvoch východiskových predpokladov $P(1)$ a $\forall n\left(P(n) \Rightarrow P(n+1)\right)$z ktorých vyplýva formula $\forall n\, P(n)$.

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

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

Príklad

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

Nech

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

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

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

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

Týmto sme dokázali, že platnosť implikácie $\forall n\left(P\left(n\right)\Rightarrow P\left(n+1\right)\right)$, použitím schémy matematickej indukcie dostaneme $\forall n\, P\left(n=2k-1\right)=k^2$.

Príklad

Dokážte, že pre každé kladné celé číslo n platí $n < 2^n$.

Nech $P(n) = \left(n < 2^n\right)$, $P(1)$ je pravdivý predikát.

Budeme študovať $P(n+1)$

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

$$\Rightarrow (n) < 2^n \cdot 2 \Rightarrow 1 < 2$$

kde sme použili indukčný predpoklad $n < 2^n$. Týmto sme dokázali platnosť implikácie $\forall n \left(P(n) \Rightarrow P(n+1)\right)$, potom musí platiť $\forall n \left(n < 2^n\right)$.

Príklad

Pomocou matematickej indukcie dokážte platnosť zovšeobecneného De Morganovho vzťahu z výrokovej logiky

$$\neg\left(\bigwedge_{i=1}^{n} p_i\right) \equiv \left(\bigvee_{i=1}^{n} \neg p_i\right)$$

$$\neg\left(\bigvee_{i=1}^{n} p_i\right) \equiv \left(\bigwedge_{i=1}^{n} \neg p_i\right)$$

pre $n \geq 2$.

Nech

$$P(n) = \neg\left(\bigwedge_{i=1}^{n} p_i\right) \equiv \left(\bigvee_{i=1}^{n} \neg p_i\right)$$

Pre n = 2 dostaneme

$$P(2) = \neg(p_1 \wedge p_2) = \neg p_1 \vee \neg p_2$$

čo je štandardná verzia De Morganovho zákona pre negáciu konjunkcie dvoch výrokov.

$$P(n+1) = \neg\left(\bigwedge_{i=1}^{n+1} p_i\right) = \neg\left(\bigwedge_{i=1}^{n} p_i \wedge p_{n+1}\right) = \neg\left(\bigwedge_{i=1}^{n} p_i\right) \vee \neg p_{n+1} = \left(\bigvee_{i=1}^{n} \neg p_i\right) \vee \neg p_{n+1}$$

$$= \left(\bigvee_{i=1}^{n+1} \neg p_i\right)$$

Týmto sme dokázali implikáciu zovšeobecnenú pomocou univerzálneho kvantifikátora

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

čím sme dokázali pomocou matematickej indukcie zovšeobecnenie De Morganovho vzťahu pre negáciu konjunkcie dvoch a viacerých výrokov.

Silná matematická indukcia

Metóda silnej matematickej indukcie dokazuje $\forall n\, P(n)$ pomocou dvoch východiskových predpokladov $P(1)$ a $\forall n\left(P(1)\wedge\ldots\wedge P(n)\Rightarrow P(n+1)\right)$ z ktorých vyplýva formula $\forall n\, P(n)$.

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

Príklad

Dokážte, že každé celé číslo $n > 1$ môže byť vyjadrené ako súčin prvočísiel.

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

kde $p_1, p_2, p_3, \ldots$ sú prvé tri prvočísla (2, 3, 5,...) a $\alpha_1, \alpha_2, \alpha_3, \ldots$sú nezáporné celé čísla.

Formula je pravdivá pre $P(2)$, kde $\alpha_1=1$, $\alpha_2 = \alpha_3 = \ldots = 0$, potom $P(2) = 2$.

Predpokladajme, že $P(j)$ je pravdivé pre každé prirodzené $j \leq n$.

Ukážeme, že z tohto predpokladu vyplýva platnosť $P(n + 1)$:

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 ≤ b < n+1. Každé z týchto dvoch čísel môže byť vyjadrené ako súčin prvočísiel (indukčný predpoklad)

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

potom ich súčin má tvar

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