Úvod do matematickej logiky

Lev Bukovský

Katedra matematickej informatiky, Prírodovedecká fakulta UPJŠ

Košice, 2001

Obsah

1 Výrok **2**

2 Pravdivosť **5**

3 Dôkaz vo výrokovom počte **10**

4 Matematický dôkaz **14**

5 Metódy dôkazu **18**

6 Kompaktnosť **20**

7 Úplnosť výrokového počtu **22**

8 Normálny tvar výroku **27**

9 Booleove algebry **32**

10 Výroková funkcia **34**

11 Formula **40**

12 Interpretácia jazyka **44**

13 Teória a model **48**

14 Dôkaz v predikátovom počte **51**

15 Metódy dôkazu **55**

16 Rovnosť, definícia, neprotirečivosť a model **58**

Literatúra **61**

1 Výrok

Výrok a pravdivosť je gramatická veta, ktorá je pravdivá alebo nepravdivá. Hovoríme, že výrok má pravdivostnú hodnotu: pravdivý, nepravdivý. Píšeme 1, 0 alebo P, N. Teda výrok okrem iného, musí byť oznamovacia veta.

Z daných výrokov môžeme utvoriť nové výroky pomocou logických operácií $\not\wedge$, $\vee$, $\rightarrow$, $\equiv$. Logické operátory $\not\wedge$, $\vee$, $\rightarrow$, $\equiv$ sa nazývajú aj **logické spojky**.

Ak máme výrok $\mathcal{V}$, tak jeho **negácia** je výrok $\neg\mathcal{V}$ je výrok "Neplatí $\mathcal{V}$". Ak máme výroky $\mathcal{V}$, $\mathcal{W}$, tak môžeme utvoriť nové výroky:

konjunkcia	$(\mathcal{V} \wedge \mathcal{W})$	$\mathcal{V}$ a $\mathcal{W}$.
disjunkcia	$(\mathcal{V} \vee \mathcal{W})$	$\mathcal{V}$ alebo $\mathcal{W}$.
implikácia	$(\mathcal{V} \rightarrow \mathcal{W})$	Ak $\mathcal{V}$ tak $\mathcal{W}$.
ekvivalencia	$(\mathcal{V} \equiv \mathcal{W})$	$\mathcal{V}$ vtedy a len vtedy, keď $\mathcal{W}$.

"Najvonkajšejšie" zátvorky obyčajne vynecháme, napríklad $(\mathcal{V} \wedge \mathcal{W}) \rightarrow \mathcal{Z}$.

Problematika pravdivosti výrokov sa podstatne zjednodušuje vďaka triviálnemu ale veľmi dôležitému princípu týkajúceho sa pravdivosti výrokov.

Základný postulát výrokového počtu:

Pravdivostná hodnota výroku utvoreného z iných výrokov pomocou logických operácií nezávisí od obsahu týchto výrokov, ale je jednoznačne určená pravdivostnými hodnotami týchto výrokov.

To nám umožňuje utvoriť známe tabuľky:

$\mathcal{V}$	$\mathcal{W}$	$\mathcal{V} \wedge \mathcal{W}$	$\mathcal{V} \vee \mathcal{W}$	$\mathcal{V} \rightarrow \mathcal{W}$	$\mathcal{V} \equiv \mathcal{W}$	$\neg\mathcal{V}$
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

Aspoň dva stĺpce tejto tabuľky potrebujú komentár: disjunkcia a implikácia. V hovorovej reči sa často disjunkcia $\mathcal{V}$ alebo $\mathcal{W}$ vyjadrená spojkou "alebo" rozumie vo vylučovacom zmysle (pozri [2], heslo "alebo"), teda, že platí práve jeden z výrokov $\mathcal{V}$, $\mathcal{W}$ (jeden platí, ale neplatia obidva). Matematika používa disjunkciu v nevylučovacom zmysle a spojka "alebo" znamená, že platí aspoň jeden z výrokov $\mathcal{V}$, $\mathcal{W}$ (môžu platiť aj obidva). Pre vylučovací zmysel používame spojky "Buď... alebo ... ." [1]

Druhá poznámka sa týka implikácie. V hovorovej reči "Ak $\mathcal{V}$, tak $\mathcal{W}$" sa obyčajne rozumie v kauzálnom zmysle, teda, že $\mathcal{V}$ je príčinou $\mathcal{W}$. Matematika

[1] Podľa pravidiel slovenskej gramatiky, pozri [2], heslo "alebo" a heslo "buď" sa má hovoriť "Buď... buď... .", "Alebo ... alebo ... ." alebo "Buď ... alebo ... ." Matematika len posledný tvar.

rozumie implikáciu doslova: "ak platí $\mathcal{V}$, tak platí $\mathcal{W}$ ". Teda, ak neplatí predpoklad implikácie $\mathcal{V}$, tak implikácia je pravdivá nezávisle od toho, či platí alebo neplatí jej záver $\mathcal{W}$.

V hovorovej reči logické operácie nie vždy vyjadrujeme pomocou uvedených oficiálnych spojok. Často používame iné vyjadrenie.
NEGÁCIA $\neg\mathcal{V}$: "Nie $\mathcal{V}$". "Nie je pravda $\mathcal{V}$". Často negovanú vetu gramaticky upravíme.
KONJUNKCIA $\mathcal{V} \wedge \mathcal{W}$: "$\mathcal{V}$ a súčasne $\mathcal{W}$", "$\mathcal{V}$ aj $\mathcal{W}$", "Platia obidve $\mathcal{V}$ a $\mathcal{W}$". Často napíšeme len "$\mathcal{V}$, $\mathcal{W}$". Slovenčina používa dvojitý zápor. Prejaví sa to vo vyslovení konjunkcie tvaru $\neg A \wedge \neg B$, ktorú vyjadrujeme slovami "Neplatí A ani B".
DISJUNKCIA $\mathcal{V} \vee \mathcal{W}$: Je väčšinou vyjadrená pomocou spojky "alebo" a rozumie sa v nevylučovacom zmysle, t.j. je pravdivá aj keď sú pravdivé obidva výroky $\mathcal{V}, \mathcal{W}$. Iné možné vyjadrenie: "Platí aspoň jedna z $\mathcal{V}, \mathcal{W}$".
IMPLIKÁCIA $\mathcal{V} \to \mathcal{W}$: "Za predpokladu $\mathcal{V}$ platí $\mathcal{W}$", "$\mathcal{W}$ ak $\mathcal{V}$".
EKVIVALENCIA $\mathcal{V} \equiv \mathcal{W}$: "$\mathcal{V}$ práve vtedy, keď $\mathcal{W}$". V definícii ekvivalenciu vyjadrujeme stručne "$\mathcal{V}$ ak $\mathcal{W}$".

Je potrebné rozlišovať medzi implikáciou (ekvivalenciou) ako logickou operáciou a vyslovením pravdivej implikácie (ekvivalencie). V tomto prípade implikáciu vyjadrujeme "$\mathcal{V}$ implikuje $\mathcal{W}$", "$\mathcal{W}$ vyplýva z $\mathcal{V}$", "$\mathcal{V}$ je postačujúca podmienka pre $\mathcal{W}$", "$\mathcal{W}$ je nutná podmienka pre $\mathcal{V}$". Namiesto "výrok $\mathcal{V} \to \mathcal{W}$ je pravdivý" píšeme $\mathcal{V} \Rightarrow \mathcal{W}$. Pravdivú ekvivalenciu vyjadrujeme "$\mathcal{V}$ je ekvivalentné $\mathcal{W}$", píšeme $\mathcal{V} \Leftrightarrow \mathcal{W}$.

Prejdeme k matematickému štúdiu výrokov, teda k tomu, čo sa nazýva **výrokový počet**. Znaky

$$p_0, p_1, \ldots, p_n, \ldots \tag{1.1}$$

budú označovať nejaké výroky a nazveme ich **elementárne výroky**. Z elementárnych výrokov môžeme tvoriť ďalšie výroky opakovaným použitím logických spojok. Pre nás v ďalších úvahách bude výrok len to, čo vzniklo z elementárnych výrokov uvedeným spôsobom. O niečo presnejšie môžeme definovať pojem výrok indukciou [2] takto:

a) každý elementárny výrok je výrok,

b) ak A je výrok, tak aj $\neg A$ je výrok,

c) ak A, B sú výroky, tak aj $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ a $(A \equiv B)$ sú výroky.

Pravidlo c) môžeme napísať aj takto:
c) ak A, B sú výroky, tak $(A \square B)$ je výrok, kde $\square = \wedge, \vee, \to, \equiv$[3].
Obyčajne budeme používať túto formu podmienky c).

Príklad 1.1 Nasledujúce výrazy sú výroky:

$$p_0,\ p_2,\ p_1,\ \neg p_0,\ (p_2 \vee \neg p_0),\ \neg p_1,\ (\neg p_1 \to (p_2 \vee \neg p_0)).$$

[2] hovoríme tiež, **rekurentne**
[3] Rozumieme tomu tak, že je $\wedge$ alebo $\vee$ alebo $\to$ alebo $\equiv$

Môžeme sa o tom presvedčiť postupne: prvé tri výrazy sú elementárne výroky, štvrtý výraz je negácia prvého - a to bol výrok, piaty výraz je disjunkcia výrokov na druhom a štvrtom mieste, šiesty výraz je negácia elementárneho výroku a teda výrok a konečne posledný výraz je implikácia predchádzajúceho a štvrtého výroku.

Príklad 1.2 Položíme si teraz takúto otázku: je výraz $\neg((p_2 \wedge \neg p_1) \rightarrow p_4)$ výrok? Ak chcem dať kladnú odpoveď, tak musíme ukázať, že tento výraz vznikol z nejakých elementárnych výrokov opakovaným použitím logických spojok. Napíšeme postupne výroky tak, ako sa dá uvedený výraz – výrok vytvoriť a o riadok nižšie napíšeme stručne pod každý výrok ako vznikol:

$$\begin{array}{cccccc} p_1, & \neg p_1, & p_2, & (p_2 \wedge \neg p_1), & p_4, & ((p_2 \wedge \neg p_1) \rightarrow p_4), \\ \text{a)} & \text{b)}, 1 & \text{a)} & \text{c)}, \square = \wedge, 3, 2 & \text{a)} & \text{c)}, \square = \rightarrow, 4, 5 \end{array} \quad \begin{array}{c} \neg((p_2 \wedge \neg p_1) \rightarrow p_4) \\ \text{b)}, 6 \end{array}$$

Teda napísali sme postupne, ako skúmaný výrok vznikol.

Príklad motivuje definíciu. Najprv však pripomenieme niekoľko pojmov. **Abeceda** je konečná alebo nekonečná množina $\mathcal{A}$. Prvok abecedy $\mathcal{A}$ sa nazýva **znak**. Konečná postupnosť znakov sa nazýva **slovo**. Abeceda, ktorá obsahuje znaky (1.1) a znaky

$$(\quad , \quad) \quad , \quad \neg \quad , \quad \wedge \quad , \quad \vee \quad , \quad \rightarrow \quad , \quad \equiv$$

sa nazýva **abeceda výrokového počtu**. Teda je to množina

$$\{), (, \neg, \wedge, \vee, \rightarrow, \equiv, p_0, \ldots, p_n, \ldots\}$$

Postupnosť slov $A_1, A_2, \ldots, A_n$ v abecede výrokového počtu sa nazýva **vytvárajúca postupnosť výroku**, stručne **VPV**, ak pre každý jej člen, teda pre každý index $i = 1, 2, \ldots, n$ platí aspoň jedna z nasledujúcich troch možností:

a) A_i je elementárny výrok, teda jeden zo znakov (1.1),

b) existuje index $j < i$ taký, že $A_i = \neg A_j$,

c) existujú indexy j, $k < i$ také, že $A_i = (A_j \square A_k)$, kde $\square = \wedge, \vee, \rightarrow, \equiv$.

Konečne, slovo A v abecede výrokového počtu sa nazýva **výrok**, ak existuje vytvárajúca postupnosť výroku $A_1, A_2, \ldots, A_n$ taká, že $A = A_n$.

Ak chceme overiť, že daná postupnosť je VPV, tak pod každý člen napíšeme, ktorá z podmienok a), b), c) definície je splnená. V prípade podmienky b) napíšeme hodnotu j a v prípade podmienky c) napíšeme čo je to $\square$ a hodnoty j, k. Nazveme to **komentár**. Postupnosť slov v príklade 1.2 je VPV a je pod ňou napísaný komentár. Aj postupnosť slov z príkladu 1.1 je VPV. Aby sme sa o tom presvedčili, stačí doplniť komentár:

$$\begin{array}{cccccccc} p_0, & p_2, & p_1, & \neg p_0, & (p_2 \vee \neg p_0), & \neg p_1, & (\neg p_1 \rightarrow (p_2 \vee \neg p_0)) \\ \text{a)} & \text{a)} & \text{a)} & \text{b)}, 1 & \text{c)}, \square = \vee, 1, 4 & \text{b)}, 3 & \text{c)}, 6, 5 \end{array}$$

Budeme hovoriť, že výrok A je **utvorený z elementárnych výrokov** $q_1, \ldots, q_k$, písať $A(q_1, \ldots, q_k)$, ak existuje VPV s posledným členom A a taká, že množina elementárnych výrokov, ktoré sa vyskytujú v tejto VPV, je podmnožina množiny $\{q_1, \ldots, q_k\}$. Nakoniec, budeme hovoriť, že elementárny výrok p **sa vyskytuje** vo výroku A, ak každá vytvárajúca postupnosť výroku A obsahuje elementárny výrok p.

Príklad 1.3 Môžeme povedať, že výrok $(p_2 \to (\neg p_6 \wedge p_3))$ je utvorený z elementárnych výrokov p_2, p_3, p_6. Môžeme tiež povedať, že je utvorený z elementárnych výrokov p_1, p_2, p_3, p_4, p_6, ale nemôžeme povedať, že je utvorený z elementárnych výrokov p_2, p_3. Každá vytvárajúca postupnosť výroku $(p_2 \to (\neg p_6 \wedge p_3))$ zrejme musí obsahovať elementárny výrok p_6.

2 Pravdivosť

Nech $A(q_1, \ldots, q_k)$ je výrok. **Pravdivostná tabuľka** alebo jednoducho **tabuľka** pre tento výrok je tabuľka, ktorá má 2^k riadkov obsahujúcich všetky možné kombinácie pravdivostných hodnôt elementárnych výrokov $q_1, \ldots, q_k$ a v príslušnom stĺpci odpovedajúce pravdivostné hodnoty výroku A.

Tabuľku pre zložitejší výrok môžeme utvoriť tak, že robíme spoločnú tabuľku pre jeho vytvárajúcu postupnosť a mechanicky používame tabuľky pre logické spojky.

Príklad 2.1 Chceme urobiť tabuľku pre výrok $p \to (q \to (p \wedge q))$. Jeho vytvárajúca postupnosť je

$$p, \quad q, \quad p \wedge q, \quad q \to (p \wedge q), \quad p \to (q \to (p \wedge q)). \tag{2.2}$$

Elementárne výroky sú na začiatku tejto VPV. Do prvého riadku tabuľky napíšeme VPV (2.2), elementárne výroky oddelíme zvislou čiarou a utvoríme tabuľku

		Stĺpec		
1.	2.	3.	4.	5.
p	q	$p \wedge q$	$q \to (p \wedge q)$	$p \to (q \to (p \wedge q))$
1	1	1	1	1
1	0	0	1	1
0	1	0	0	1
0	0	0	1	1

Tretí stĺpec sme vypočítali z prvého a druhého pomocou tabuľky pre konjunkciu, štvrtý stĺpec sme vypočítali z druhého a tretieho pomocou tabuľky pre implikáciu a konečne piaty stĺpec sme vypočítali z prvého a štvrtého pomocou tabuľky pre implikáciu.

Každú VPV možno upraviť tak, aby elementárne výroky, ktoré sa v nej vyskytujú, boli uvedené ako prvé členy postupnosti. Potom pravdivostnú tabuľku pre daný výrok robíme pomocou takto upravenej VPV. Elementárne výroky v takejto tabuľke sú potom spravidla oddelené zvislou čiarou, ako v predchádzajúcom príklade.

Príklad 2.2 VPV z príkladu 1.2 upravíme na VPV

$$p_1, \quad p_2, \quad p_4, \quad \neg p_1, \quad (p_2 \wedge \neg p_1), \quad ((p_2 \wedge \neg p_1) \to p_4), \quad \neg((p_2 \wedge \neg p_1) \to p_4).$$

Potom hlavička spoločnej tabuľky bude mať tvar

p_1	p_2	p_4	$\neg p_1$	$p_2 \wedge \neg p_1$	$(p_2 \wedge \neg p_1) \to p_4$	$\neg((p_2 \wedge \neg p_1) \to p_4)$

Obávam sa, že nasledujúce riadky môžu byť ťažko zrozumiteľné. Napriek tomu ich uvediem a odporúčam čitateľovi vrátiť sa k nim znovu neskoršie, po pochopení určitých vecí.

Matematika pracuje s **abstraktnými pojmami**. Pojmy "číslo, štvorec, strana štvorca" zrejme neexistujú v skutočnosti, ale sú abstrakciami nejakých skutočných javov. Tieto pojmy však majú nejaké základné vlastnosti a matematik chce poznať ďalšie vlastnosti týchto pojmov. Čo sú to ďalšie vlastnosti? Pokúsime sa to upresniť pomocou príkladov.

Grécka matematika utvorila napríklad abstraktné pojmy "bod, priamka, rovina" a abstraktné vzťahy medzi nimi "byť rovnobežný, byť kolmý, ležať na priamke, ležať v rovine, byť rôznobežný" atď. Samozrejme, abstrahovala pri tom zo skutočnosti. Hneď povedala, aké základné vlastnosti tieto pojmy majú. Napríklad, "ak priamky p, q sú rovnobežné a priamka r je kolmá na priamku p, tak priamka r je kolmá aj na priamku q; ak bod A neleží na priamke p, tak existuje jediná priamka q rovnobežná s priamkou p, na ktorej leží bod A" a pod. Tieto pojmy boli abstrahované z rozličných skutočností: priamky mohli byť myslené predĺženia styku dvoch stien v miestnosti, alebo lúč svetla. "Rovnobežné priamky" asi znamenalo, že priamky síce ležia v jednej rovine, ale sa nikdy nepretnú (nemajú spoločný bod).

Podobne matematika si vytvorila abstraktný pojem "číslo". Vie niekto, čo je to číslo? Postupne historicky matematika tvorila abstraktný pojem (v dnešnej terminológii) pojmy "prirodzené číslo, celé číslo, racionálne číslo, reálne číslo". V 18. storočí dokonca vznikol pojem "komplexné číslo". Zase, matematika týmto abstraktným pojmom prisúdila určité základné vlastnosti, odpozorované z viacerých prípadov v skutočnosti.

Pre matematiku je typický nasledujúci postup: máme abstraktné pojmy s určitými základnými vlastnosťami. Z týchto základných vlastností pomocou logiky (alebo, ak chcete, logickej úvahy) môžeme **dedukovať** ďalšie vlastnosti skúmaných abstraktných pojmov. Ak skutočnosť (možno aj iná ako tá, z ktorej sme abstrahovali), má základné vlastnosti abstrahovaných pojmov, tak táto skutočnosť musí mať aj tieto ďalšie "vydedukované" vlastnosti.

Príklad 2.3 Murár má za úlohu postaviť výťahovú šachtu. Základná požiadavka na túto stavbu spočíva v tom, že steny šachty musia byť rovnobežné: musia byť všade tak široké, aby sa výťahová kabínka medzi ne vošla a nesmie sa kolísať. Murár to urobí v podstate takto: naznačí si na zem šírku kabínky a začne stavať múr podľa týchto značiek. Pri stavbe používa olovnicu, ktorá mu zaručuje, že postavený múr je kolmý na rovinu "zem".

Uvedomme si, akú abstrakciu podvedomo murár použil. Ak dve priamky sú kolmé na tú istú rovinu, tak sú rovnobežné a teda ich "vzdialenosť" je všade rovnaká. Murár implicitne dedukoval vlastnosti múru, postaveného podľa ním zvoleného postupu.

V ďalšom budeme skúmať práve takéto situácie: ak abstrahované pojmy majú určité základné vlastnosti, ktoré ďalšie vlastnosti týchto pojmov môžeme získať?

Nech $\Delta = \{B_1, \ldots, B_m\}$ je konečná množina výrokov a A je výrok. Budeme predpokladať, že všetky tieto výroky sú utvorené z elementárnych výrokov $q_1, \ldots, q_k$. Budeme hovoriť, že **výrok A platí v Δ**, píšeme

$$\Delta \models A,$$

ak v každom riadku spoločnej tabuľky pre výroky A, B_1, …, B_m, v ktorom sú pravdivostné hodnoty 1 pod výrokmi z množiny Δ, je pravdivostná hodnota 1 aj pod výrokom A.

	$\overbrace{\qquad\qquad}^{\Delta}$	
$q_1 \cdot \cdot \cdot q_k$	$B_1 \quad . \quad . \quad . \quad B_m$	A
$Q_1 \cdot \cdot \cdot Q_k$	1 . . . 1	1!

Výrok $A(q_1, \ldots, q_k)$ sa nazýva **tautológia**, ak má pravdivostnú hodnotu 1 v každom riadku tabuľky. Zrejme výrok A je tautológia práve vtedy, keď platí v prázdnej množine predpokladov, t.j. keď $\emptyset \models A$.

Príklad 2.4 Podľa príkladu 2.1 výrok $p \to (q \to (p \wedge q))$ je tautológia. Nasledujúca tabuľka ukazuje, že výrok $(p \to q) \to p$ nie je tautológia (pri konštrukcii tabuľky sme použili upravenú vytvárajúcu postupnosť výroku):

p	q	$p \to q$	$(p \to q) \to p$
1	1	1	1
1	0	0	1
0	1	1	0
0	0	1	0

Čitateľ si ľahko overí nasledujúce

Tvrdenie 2.1 *Nech $\Delta = \{B_1, \ldots, B_m\}$ a Γ sú konečné množiny výrokov, A je výrok.*

a) *Ak $A \in \Delta$, tak $\Delta \models A$.*

b) *Ak $\Delta \models A$ a $\Delta \subseteq \Gamma$, tak $\Gamma \models A$.*

c) *Ak $\Delta \models A$ a $\Gamma \models B_1$, ..., $\Gamma \models B_m$, tak $\Gamma \models A$.*

Overenie: Tvrdenia a) a b) vyplývajú bezprostredne z definície. Overenie tretieho tvrdenia sa dá jednoducho domyslieť pomocou definície z nasledovnej tabuľky:

$q_1 \; . \; . \; . \; q_k$	Γ	$\overbrace{B_1 \; . \; . \; . \; B_m}^{\Delta}$	A
$Q_1 \; . \; . \; . \; Q_k$	$1 \; . \; . \; . \; 1$	$1! \; . \; . \; . \; 1!$	$1!!$

Uvedomte si, že tvrdenie b) vyplýva z tvrdenia c) na základe tvrdenia a)!

q.e.d.

Ak $A(p_1, \ldots, p_n)$ je výrok a $B_1, \ldots, B_n$ sú výroky, tak označíme

$$A(p_1/B_1, \ldots, p_n/B_n)$$

výrok, ktorý vznikne tak, že vo výroku A nahradíme každý výskyt elementárneho výroku p_i výrokom B_i (pre $i = 1, \ldots, n$).

Napríklad, ak $A = \neg p_2 \to (p_1 \wedge p_2)$, $B_1 = \neg p_3$, $B_1 = (p_4 \vee p_1)$, tak $A(p_1/B_1, p_2/B_2)$ je výrok $\neg(p_4 \vee p_1) \to (\neg p_3 \wedge (p_4 \vee p_1))$.

Často budeme využívať nasledujúce tvrdenie.

Tvrdenie 2.2 *Ak výrok $A(p_1, \ldots, p_n)$ je tautológia a $B_1, \ldots, B_n$ sú výroky, tak výrok $A(p_1/B_1, \ldots, p_n/B_n)$ je tiež tautológia.*

Overenie: Dáme návod na overenie. Zostrojíme najprv vytvárajúcu postupnosť výroku $A(p_1/B_1, \ldots, p_n/B_n)$ pomocou vytvárajúcich postupností výrokov (postupne) $B_1, \ldots, B_n, A$. Pomocou tejto vytvárajúcej postupnosti zostrojíme tabuľku pre výrok $A(p_1/B_1, \ldots, p_n/B_n)$.

Uvažujme ľubovoľný pevný riadok tejto tabuľky. Nech $Q_1, \ldots, Q_n$ sú pravdivostné hodnoty výrokov $B_1, \ldots, B_n$ v tomto riadku. Teraz uvažujme tabuľku pre výrok $A(p_1, \ldots, p_n)$ a nej riadok, v ktorom pravdivostné hodnoty elementárnych výrokov $p_1, \ldots, p_n$ sú $Q_1, \ldots, Q_n$. Výrok $A(p_1/B_1, \ldots, p_n/B_n)$ vznikol z výrokov $B_1, \ldots, B_n$ rovnakým spôsobom, ako výrok $A(p_1, \ldots, p_n)$ z elementárnych výrokov $p_1, \ldots, p_n$. Teda v týchto riadkoch budú pravdivostné hodnoty výrokov $A(p_1/B_1, \ldots, p_n/B_n)$ a $A(p_1, \ldots, p_n)$ rovnaké. Keďže výrok $A(p_1, \ldots, p_n)$ je tautológia, tak uvažovaná pravdivostná hodnota je 1.

q.e.d.

Budeme hovoriť, že výroky A, B **sú ekvivalentné**, ak výrok $A \equiv B$ je tautológia. Budeme písať

$$A \Longleftrightarrow B.$$

Podobne budeme hovoriť, že výrok A **implikuje** výrok B, alebo z výroku A **vyplýva** výrok B, ak výrok $A \to B$ je tautológia. Píšeme

$$A \Longrightarrow B.$$

Tvrdenie 2.3 *Nech $A(q_1, \ldots, q_n)$ je výrok. Nech $B_1, \ldots, B_n$, $C_1, \ldots, C_n$ sú výroky také, že*

$$B_1 \Longleftrightarrow C_1, \quad B_2 \Longleftrightarrow C_2, \quad . \quad . \quad . \quad , B_n \Longleftrightarrow C_n.$$

Potom

$$A(q_1/B_1, \ldots, q_n/B_n) \Longleftrightarrow A(q_1/C_1, \ldots, q_n/C_n).$$

Overenie: Najprv si uvedomíme toto: ak B, C E a F sú výroky, $B \Longleftrightarrow C$, $E \Longleftrightarrow F$, tak platí

$$\neg B \Longleftrightarrow \neg C, \qquad (B \square E) \Longleftrightarrow (C \square F), \text{ pre } \square = \wedge, \vee, \to, \equiv .$$

Nech $A_1, \ldots, A_m$ je vytvárajúca postupnosť výroku A, v ktorej sa nevyskytujú iné elementárne výroky ako $q_1, \ldots, q_n$. Matematickou indukciou bezprostredne vyplýva, že

$$A_i(q_1/B_1, \ldots, q_n/B_n) \Longleftrightarrow A_i(q_1/C_1, \ldots, q_n/C_n) \text{ pre } i = 1, \ldots, m.$$

Pre $i = m$ máme tvrdenie.

q.e.d.

Na záver tejto časti upresníme, čo to znamená $\Delta \models A$ v prípade nekonečnej množiny výrokov Δ. Ohraničíme sa na prípad spočítateľnej množiny

$\Pi = \{p_1, p_2, \ldots, p_n, \ldots\}$ elementárnych výrokov. Čitateľ, ktorý sledoval elementárny úvod do teórie množín určite vie, že v tomto prípade množina všetkých výrokov utvorených z elementárnych výrokov z množiny Π je tiež spočítateľná.

Najprv analyzujeme pojem $\Delta \models A$ v prípade konečnej množiny Δ. Nech Π je množina všetkých elementárnych výrokov, ktoré sa vyskytujú v niektorom výroku z množiny Δ. Množina Π je konečná. Riadok tabuľky predstavuje priradenie pravdivostných hodnôt $\{0, 1\}$ elementárnym výrokom z Π. Teda je to zobrazenie $v : \Pi \longrightarrow \{0, 1\}$. Keď sme definovali vzťah $\Delta \models A$ pre konečnú množinu $\Delta = \{B_1, \ldots, B_m\}$, tak sme predpokladali, že $\Pi = \{q_1, \ldots, q_k\}$ a naviac, ak elementárny p sa vyskytuje v niektorom z výrokov $B_1, \ldots, B_m, A$, tak $p \in \Pi$. Riadok tabuľky je zobrazenie $v : \Pi \longrightarrow \{0, 1\}$ definované vzťahom $v(q_i) = Q_i$, $i = 1, \ldots, k$ a je dodefinované pre všetky výroky utvorené z elementárnych výrokov $q_1, \ldots, q_k$. Definícia vzťahu $\Delta \models A$ sa dá preformulovať takto: pre každé $v : \Pi \longrightarrow \{0, 1\}$ také, že $v(B) = 1$ pre každý výrok $B \in \Delta$, platí aj $v(A) = 1$.

Túto formuláciu akceptujeme ako definíciu pre vzťah $\Delta \models A$ v prípade nekonečnej množiny Δ. Nech Π je množina všetkých elementárnych výrokov, ktoré sa vyskytujú v niektorom výroku z množiny Δ alebo vo výroku A. Budeme hovoriť, že A platí v Δ, písať $\Delta \models A$, ak pre každé zobrazenie $v : \Pi \longrightarrow \{0, 1\}$ také, že $v(B) = 1$ pre každé $B \in \Delta$, platí aj $v(A) = 1$.

Tvrdenie 2.1c) pre nekonečnú množinu Δ môžeme preformulovať takto:

Tvrdenie 2.4 *Ak* $\Gamma \models B$ *pre každé* $B \in \Delta$ *a* $\Delta \models A$, *tak* $\Gamma \models A$.

Príklad 2.5 Nech $\Delta = \{q_1, q_1 \to q_2, q_2 \to q_3, \ldots, q_n \to q_{n+1}, \ldots\}$. Potom pre ľubovoľné $n = 1, 2, \ldots$ platí $\Delta \models q_n$. Overte!

3 Dôkaz vo výrokovom počte

Začneme jednoduchým príkladom

Príklad 3.1 Máme overiť, či

$$\Delta \models p_4, \text{ kde } \Delta = \{p_1 \wedge p_2, p_1 \to p_3, p_3 \to p_4\}.$$

Príslušná tabuľka by mala 16 riadkov. My použijeme jednoduchú úvahu, na základe ktorej prehlásime, že je to pravda.

Uvažujme riadok tabuľky, v ktorom sú jednotky pod každým výrokom z množiny Δ. Keďže je 1 pod výrokom $p_1 \wedge p_2$, tak je 1 aj pod výrokom p_1. Ale pod výrokom $p_1 \to p_3$ je 1, tak potom aj pod výrokom p_3 je 1. Konečne, keďže je 1 pod výrokom $p_3 \to p_4$, tak musí byť aj pod výrokom p_4, čo sme chceli ukázať.

Namiesto zložitého počítania tabuľky, sme použili dedukciu – úvahu. Dedukciu používala grécka matematika a už Pytagorejci vedeli niečo o dôkaze ako forme dedukcie. Dáme presnú definíciu pojmu dôkaz vo výrokovom počte a budeme ho skúmať, hlavne jeho vzťah k dôkazu v bežnej matematike.

Každý výrok, ktorý má niektorý z nasledujúcich tvarov (A, B, C sú výroky), sa nazýva **axióma výrokového počtu**, stručne **AVP**:

$A \to A$	$A \to (B \to A)$
$(A \to B) \to ((B \to C) \to (A \to C))$	$(A \to B) \to (\neg B \to \neg A)$
$(A \to B) \to ((A \to (B \to C)) \to (A \to C))$	
$A \to (B \to (A \wedge B))$	$(A \wedge B) \to A$
$(A \wedge B) \to (B \wedge A)$	
$(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$	$A \to (A \vee B)$
$(A \vee B) \to (B \vee A)$	
$(A \to B) \to ((B \to A) \to (A \equiv B))$	$(A \equiv B) \to (A \to B)$
$(A \equiv B) \to (B \equiv A)$	
$A \vee \neg A$	$\neg\neg A \equiv A$
$(A \to B) \to ((A \to \neg B) \to \neg A)$	

Pomocou tvrdenia 2.2 si čitateľ ľahko overí

Tvrdenie 3.1 *Každá axióma výrokového počtu je tautológia.*

Zavedieme ďalšiu terminológiu tak, aby sme sa priblížili matematike. Množina výrokov Δ sa nazýva **matematická teória**, skrátene tiež **teória**. Jej prvky, teda výroky patriace do Δ, sa nazývajú **axiómy teórie** Δ.

Postupnosť výrokov $A_1, \ldots, A_n$ sa nazýva **dôkaz v tórii** Δ, ak pre každý jej člen, t.j. pre každé $i = 1, \ldots, n$ platí niektorá z nasledujúcich troch podmienok:

d1) A_i je axióma výrokového počtu,

d2) A_i je axióma teórie Δ,

d3) existujú také $k, j < i$, že A_k je výrok $A_j \to A_i$.

Podmienky d1) a d2) nepotrebujú komentár. Podmienka d3) požaduje, že sa vyskytla jedna z dvoch situácií:

$$\ldots, A_j, \ldots, \underbrace{A_j \to A_i}_{A_k}, \ldots, A_i, \ldots$$

alebo

$$\ldots, \underbrace{A_j \to A_i}_{A_k}, \ldots, A_j, \ldots, A_i, \ldots.$$

V dôkaze píšeme za sebou argumenty. Argumenty sú troch druhou: logická pravda (axióma výrokového počtu), matematická pravda[4] (axióma teórie) a konečne, ak sme mali argumenty tvaru A, $A \to B$, prípadne v opačnom poradí $A \to B$, A, tak z nich môžeme vydedukovať argument B.

Pod každý člen dôkazu, podobne ako v prípade vytvárajúcej postupnosti, budeme písať **komentár**, t.j. uvedieme, ktorá z troch podmienok d1) – d3) je splnená.

[4]možno lepšie, matematický predpoklad

Príklad 3.2 Postupnosť

$$\begin{array}{cccccccc} (p_1 \wedge p_2) \to p_1, & p_1 \wedge p_2, & p_1, & p_1 \to p_3, & p_3, & p_3 \to p_4, & p_4 \\ \text{d1)} & \text{d2)} & \text{d3) } 2,\ 1 & \text{d2)} & \text{d3) } 3,\ 4 & \text{d2)} & \text{d3) } 5,\ 6 \end{array}$$

je dôkaz v matematickej teórii

$$\Delta = \{p_1 \wedge p_2, p_1 \to p_3, p_3 \to p_4\}.$$

Porovnajte tento dôkaz s úvahou z príkladu 3.1, ktorou sme zistili, že platí

$$\{p_1 \wedge p_2, p_1 \to p_3, p_3 \to p_4\} \models p_4.$$

Výrok A je **dokázateľný v teórii** Δ, alebo A **je veta teórie** Δ, píšeme

$$\Delta \vdash A,$$

ak existuje dôkaz $A_1, \ldots, A_n$ v teórii Δ taký, že $A_n = A$.

Príklad 3.3 Nech A, B sú výroky. Ukážeme, že

$$\{A \vee B,\, \neg A\} \vdash B.$$

Stačí nájsť dôkaz v $\{A \vee B,\, \neg A\}$, ktorého posledný člen je výrok B. Zostrojíme taký dôkaz:

$$\begin{array}{cccc} 1. & 2. & 3. & 4. \\ \neg A, & \neg A \to (\neg B \to \neg A), & \neg B \to \neg A, & (\neg B \to \neg A) \to (\neg\neg A \to \neg\neg B), \\ \text{d2)} & \text{d1)} & \text{d3), } 1, 2 & \text{d1)} \end{array}$$

$$\begin{array}{cccc} 5. & 6. & 7. & 8. \\ (\neg\neg A \to \neg\neg B), & \neg\neg B \equiv B, & (\neg\neg B \equiv B) \to (\neg\neg B \to B), & (\neg\neg B \to B), \\ \text{d3), } 3, 4 & \text{d1)} & \text{d1)} & \text{d3), } 6, 7 \end{array}$$

$$\begin{array}{cc} 9. & 10. \\ (\neg\neg A \to \neg\neg B) \to ((\neg\neg B \to B) \to (\neg\neg A \to B)), & (\neg\neg B \to B) \to (\neg\neg A \to B), \\ \text{d1)} & \text{d3), } 5, 9 \end{array}$$

$$\begin{array}{cccc} 11. & 12. & 13. & 14. \\ \neg\neg A \to B, & \neg\neg A \equiv A, & (\neg\neg A \equiv A) \to (A \equiv \neg\neg A), & A \equiv \neg\neg A, \\ \text{d3), } 8, 10 & \text{d1)} & \text{d1)} & \text{d3), } 12, 13 \end{array}$$

$$\begin{array}{cc} 15. & 16. \\ (A \equiv \neg\neg A) \to (A \to \neg\neg A), & (A \to \neg\neg A) \to ((\neg\neg A \to B) \to (A \to B)), \\ \text{d1)} & \text{d1)} \end{array}$$

$$\begin{array}{ccc} 17. & 18. & 19. \\ A \to \neg\neg A, & (\neg\neg A \to B) \to (A \to B), & A \to B, \\ \text{d3), } 14, 15 & \text{d3), } 17, 16 & \text{d3), } 11, 18 \end{array}$$

$$\underset{\text{d1)}}{\overset{20.}{B \to B,}} \qquad \underset{\text{d1)}}{\overset{21.}{(A \to B) \to ((B \to B) \to ((A \vee B) \to B)),}}$$

$$\underset{\text{d3), 19, 21}}{\overset{22.}{(B \to B) \to ((A \vee B) \to B),}} \quad \underset{\text{d3), 20, 22}}{\overset{23.}{(A \vee B) \to B,}} \quad \underset{\text{d2)}}{\overset{24.}{A \vee B,}} \quad \underset{\text{d3), 24, 23}}{\overset{25.}{B.}}$$

Tvrdenie 3.2 *Nech Δ, Γ sú množiny výrokov. Potom*

a) *ak A je axióma výrokového počtu, tak $\Delta \vdash A$;*

b) *ak $A \in \Delta$, tak $\Delta \vdash A$;*

c) *ak $\Delta \subseteq \Gamma$ a $\Delta \vdash A$, tak $\Gamma \vdash A$.*

Overenie:

a) Ak A je axióma výrokového počtu, tak jednočlenná postupnosť "A" je dôkaz v Δ (komentár d1)), teda $\Delta \vdash A$.

b) Ak $A \in \Delta$, tak jednočlenná postupnosť "A" je dôkaz v Δ (komentár d2)), teda $\Delta \vdash A$.

c) Ak $\Delta \vdash A$, tak existuje dôkaz $A_1, \ldots, A_n$ v Δ taký, že $A_n = A$. Matematickou indukciou ukážeme, že pre každé $i = 1, \ldots, n$ je $\Gamma \vdash A_i$. Pre $i = n$ dostaneme tvrdenie.

Predpokladajme, že $\Gamma \vdash A_j$ pre $j < i$. Z definície dôkazu vyplýva, že výrok A_i spĺňa niektorú z troch podmienok d1)–d3). Ak spĺňa podmienku d1) alebo d2), tak podľa časti a) alebo b) je $\Gamma \vdash A_i$. Predpokladajme, že je splnená podmienka d3), teda existujú čísla $j, k < i$ také, že $A_k = (A_j \to A_i)$. Podľa indukčného predpokladu je $\Gamma \vdash A_j$ a $\Gamma \vdash A_j \to A_i$. Potom existujú dôkazy $B_1, \ldots, B_k$ a $C_1, \ldots, C_k$ v Γ také, že $B_k = A_j$ a $C_l = (A_j \to A_i)$. Postupnosť

$$\underset{\text{komentár opíš}}{\overset{A_j}{B_1, \ldots, B_k,}} \qquad \underset{\substack{\text{komentár opíš} \\ \text{indexy}+k}}{\overset{A_j \to A_i}{C_1, \ldots, C_l,}} \quad \underset{\text{m.p.},k,k+l}{A_i}$$

je dôkaz v Γ a teda $\Gamma \vdash A_i$, čo sme chceli ukázať.

q.e.d.

Tvrdenie 3.3 (Veta o korektnosti) *Ak $\Delta \vdash A$, tak $\Delta \models A$.*

Overenie: Predpokladajme, že platí $\Delta \vdash A$. Potom existuje dôkaz $A_1, \ldots, A_n$ v teórii Δ taký, že $A_n = A$. Matematickou indukciou ukážeme, že pre $i = 1, \ldots, n$ platí $\Delta \models A_i$. Potom špeciálne pre $i = n$ platí $\Delta \models A_n = A$, čo je práve overované tvrdenie.

Predpokladajme teda, že "$\Delta \models A_j$ pre každé $j < i$" a chceme ukázať, že $\Delta \models A_i$. Keďže A_i je člen dôkazu z Δ, tak spĺňa jednu z podmienok d1)–d3).

Ak A_i spĺňa podmienku d1), tak A_i je tautológia, t.j. $\emptyset \models A_i$ a podľa tvrdenia 2.1,b) aj $\Delta \models A_i$.

Ak A_i spĺňa podmienku d2), tak podľa tvrdenia 2.1,a) platí $\Delta \models A_i$.

Nech A_i spĺňa podmienku d3). Potom existujú čísla $j, k < i$ také, že platí $A_k = (A_j \to A_i)$. Uvažujme riadok príslušnej tabuľky, kde pod všetkými výrokmi z Δ sú pravdivostné hodnoty 1. Podľa indukčného predpokladu platí $\Delta \models A_j$ a $\Delta \models A_k$. Teda v tomto riadku sú pravdivostné hodnoty 1 aj pod výrokmi A_j a $A_k = (A_j \to A_i)$.

$q_1 \cdot \cdot \cdot q_k$	Δ	$\ldots A_j \ldots \overbrace{(A_j \to A_i)}^{A_k} \ldots A_i \ldots$		
		IP	IP	!
$Q_1 \cdot \cdot \cdot Q_k$	$1 \cdot \cdot \cdot 1$	1	1	1

Z pravdivostnej tabuľky pre implikáciu už ľahko vidieť, že musí byť 1 aj pod výrokom A_i.

q.e.d.

4 Matematický dôkaz

Pre matematika je primárnou otázkou, či $\Delta \models A$. Podľa vety 3.3 o korektnosti stačí ukázať, že $\Delta \vdash A$. Teda, matematika nezaujíma dôkaz v zmysle našej definície, ale ho zaujíma, či existuje dôkaz a teda, či výrok A je dokázateľný. V praxi matematik ani nekonštruuje dôkaz v zmysle definície, ale ukazuje (bez toho, aby si to explicitne uvedomil), že dôkaz v zmysle našej definície existuje a teda $\Delta \vdash A$. V ďalšom zavedieme terminológiu, ktorá predstavuje analýzu tohoto postupu.

Najprv zavedieme jeden užitočný pojem, ktorý implicitne každý pozná. Postupnosť výrokov $A_1, \ldots, A_k$; A sa nazýva **odvodzovacie pravidlo v teórii** Δ, stručne **OP v** Δ, píšeme

$$\frac{A_1, \ldots, A_k}{A} \qquad (\text{v } \Delta),$$

ak platí:

$$\text{ak } \Delta \vdash A_1, ..., \Delta \vdash A_k, \text{ tak aj } \Delta \vdash A. \tag{4.3}$$

Ak $A_1, \ldots, A_k$; A je odvodzovacie pravidlo v každom Δ, píšeme jednoducho

$$\frac{A_1, \ldots, A_k}{A}$$

a hovoríme stručne len o odvodzovacom pravidle.

Intuitívne pozadie tohoto pojmu môže vysvetliť nasledujúce. V základnej škole sme sa učili odvodzovacie pravidlá typu "k obidvom stranám rovnosti možno pripočítať to isté číslo" alebo "obidve strany rovnosti môžeme vynásobiť tým istým číslom". V tomto prípade úlohu predpokladov Δ hrajú prijaté predpoklady (axiómy) o reálnych číslach a naše odvodzovacie pravidlá môžeme napísať takto (t, t_1, t_2 označujú "číselné výrazy", Δ sú predpoklady o reálnych číslach):

$$\frac{t_1 = t_2}{t_1 + t = t_2 + t} \qquad \frac{t_1 = t_2}{t_1 \cdot t = t_2 \cdot t} \quad (\text{ v } \Delta).$$

Príklad 4.1 Najjednoduchším a súčasne najdôležitejším odvodzovacím pravidlom je odvodzovacie pravidlo **modus ponens**

$$\frac{A,\ A \to B}{B},$$

(A, B sú ľubovoľné výroky). Stručne sa naň budeme odvolávať skratkou "m.p.".

Ukážeme, že uvedená postupnosť je odvodzovacie pravidlo v ľubovoľnom Δ.

Predpokladajme, že $\Delta \vdash A$ a $\Delta \vdash A \to B$. Potom existujú dôkazy $A_1, \ldots, A_n$ a $B_1, \ldots, B_m$ v Δ také, že $A_n = A$ a $B_m = (A \to B)$. Potom postupnosť

$$\underset{\text{komentár opíš}}{A_1, \ \ldots, \ A_n,} \qquad \underset{\substack{\text{komentár opíš,}\\ \text{indexy}+n}}{\overset{A \to B}{B_1, \ \ldots, \ B_m,}} \quad \underset{\text{d3), n, n+m}}{B}$$

je dôkaz v Δ s posledným členom B. Teda platí aj $\Delta \vdash B$.

Na základe tohoto výsledku môžeme jednoducho doplniť výsledok tvrdenia 3.2 o nasledovné tvrdenie:

Tvrdenie 4.1 *Nech Δ a Γ sú množiny výrokov, A je výrok. Ak $\Gamma \vdash B$ pre každé $B \in \Delta$ a $\Delta \vdash A$, tak aj $\Gamma \vdash A$.*

Overenie: . Nech $A_1, \ldots, A_n$ je dôkaz Δ taký, že $A_n = A$. Matematickou indukciou ukážeme, že $\Gamma \vdash A_i$ pre každé $i = 1, \ldots, n$. Pre $i = n$ potom máme naše tvrdenie.

Predpokladajme, že $\Gamma \vdash A_j$ pre každé $j < i$ a chceme ukázať, že $\Gamma \vdash A_i$. Keďže A_i je člen dôkazu v Δ, tak spĺňa jednu z troch podmienok d1)–d3). Ak A_i je axióma výrokového počtu, tak podľa tvrdenie 3.2a) je $\Gamma \vdash A_i$. Ak $A_i \in \Delta$, tak $\Gamma \vdash A_i$ podľa predpokladu tvrdenia. Konečne predpokladajme, že platí podmienka d3), t.j. existujú čísla j, $k < i$ také, že $A_k = (A_j \to A_i)$. Podľa indukčného predpokladu je $\Gamma \vdash A_j$ a $\Gamma \vdash A_k = (A_j \to A_i)$. Použitím odvodzovacieho pravidla modus ponens potom dostávame $\Gamma \vdash A_i$.

q.e.d.

Príklad 4.2 Nech A, B, C sú ľubovoľné výroky. Použitím axióm výrokového počtu môžeme ľahko ukázať, že nasledujúce postupnosti výrokov (každé dostane

svoj názov, napísaný za ním) sú odvodzovacie pravidlá v ľubovoľnom Δ:

$\frac{A\to B,\, B\to C}{A\to C}$	trans $\to$	$\frac{\neg B\to\neg A}{A\to B}$	nepriamo	$\frac{A\to B}{\neg B\to\neg A}$	kontra
$\frac{A\to(B\to C)}{B\to(A\to C)}$	poradie $\to$	$\frac{A}{A\wedge A}$	idemp $\wedge$	$\frac{A\vee A}{A}$	idemp $\vee$
$\frac{A\wedge B}{B\wedge A}$	kom $\wedge$	$\frac{A,\, B}{A\wedge B}$	zav $\wedge$	$\frac{A\wedge B}{A}$	vyn $\wedge$
$\frac{A\vee B}{B\vee A}$	kom $\vee$	$\frac{A}{A\vee B}$	zav $\vee$	$\frac{A\to C,\, B\to C}{A\vee B\to C}$	vyn $\vee$
$\frac{A\equiv B}{B\equiv A}$	kom $\equiv$	$\frac{A\to B,\, B\to A}{A\equiv B}$	zav $\equiv$	$\frac{A\equiv B}{A\to B}$	vyn $\equiv$
$\frac{A\to B,\, \neg A\to B}{B}$	rozbor	$\frac{A}{\neg\neg A}$	zav $\neg\neg$	$\frac{\neg\neg A}{A}$	vyn $\neg\neg$

Čitateľ si iste domyslel, že "trans" znamená "tranzitívnosť", "poradie" znamená výmenu poradia predpokladov, "idemp" je zákon idempotencie, "zav" znamená "zavedenie", "vyn" znamená vynechanie príslušnej logickej spojky, "nepriamo" je metóda dôkazu nepriamo, "kontra" je zákon kontrapozície a "rozbor" je rozbor prípadov.

Overíme napríklad, že "trans $\to$" je OP. Nech teda A, B, C sú ľubovoľné výroky a Δ je ľubovoľná množina výrokov. Predpokladáme, že $\Delta \vdash A \to B$, $\Delta \vdash B \to C$ a chceme ukázať, že aj $\Delta \vdash A \to C$. Podľa predpokladov existujú dôkazy $A_1, \ldots, A_n$ a $B_1, \ldots, B_m$ v Δ také, že $A_n = (A \to B)$ a $B_m = (B \to C)$. Potom nasledujúca postupnosť je dôkaz v Δ:

Príklad 4.3 Odporúčame čitateľovi ako dobré cvičenie overiť, že nasledujúca postupnosť je odvodzovacie pravidlo

$$\frac{(A_1 \vee \ldots \vee A_n),\, A_1 \to B,\, \ldots,\, A_n \to B}{B}.$$

Toto odvodzovacie pravidlo je zovšeobecnením odvodzovacieho pravidla "rozbor" z príkladu 4.2.

Príklad 4.4 Ak $\Delta \vdash A$, tak

$$\frac{A_1, \ldots, A_k}{A}$$

je odvodzovacie pravidlo v Δ pre ľubovoľné výroky $A_1, \ldots, A_k$.

Naozaj, keďže $\Delta \vdash A$, tak implikácia (4.3) triviálne platí.

Ako uvidíme za chvíľu, pojem odvodzovacie pravidlo je prostriedok "na urýchlenie dôkazu". Odvodzovacie pravidlo z príkladu 4.4 však túto úlohu neplní – potrebujeme vedieť najprv to, čo je naším cieľom. Matematik potrebuje mať určitú zásobu (už overených) odvodzovacích pravidiel, aby mohol "urýchliť" dôkaz.

Zavedieme nový pojem. Postupnosť výrokov $A_1, \ldots, A_n$ sa nazýva **matematický dôkaz v teórii** Δ, ak pre každý jej člen, t.j. pre každé $i = 1, \ldots, n$ platí niektorá z nasledujúcich troch podmienok:

md1) A_i je axióma výrokového počtu,

md2) A_i je veta teórie Δ,

md3) existujú také čísla $j_1, \ldots, j_k < i$, že

$$\frac{A_{j_1}, \ldots, A_{j_k}}{A_i}$$

je odvodzovacie pravidlo v teórii Δ.

Podobne ako v prípade dôkazu, pod jednotlivé členy matematického dôkazu budeme písať komentár, ktorý bude poukazovať na to, ktorá podmienka definície je splnená.

Príklad 4.5 Postupnosť výrokov

$p_1 \wedge p_2$,	p_1	$p_1 \to p_3$,	$p_3 \to p_4$,	$p_1 \to p_4$	p_4
md1)	vyn $\wedge$, 1	md2)	md2)	trans $\to$, 3, 4	m.p., 2, 5

je matematický dôkaz v $\Delta = \{p_1 \wedge p_2, p_1 \to p_3, p_3 \to p_4\}$. Druhý riadok je príslušný komentár.

Príklad 4.6 Nech A, B sú výroky. Nasledujúca postupnosť je matematický dôkaz v $\Delta = \{A \vee B, \neg A\}$:

1.	2.	3.	4.
$\neg A$,	$\neg A \to (\neg B \to \neg A)$,	$\neg B \to \neg A$,	$A \to B$,
md1)	md1)	md3) m.p. 1, 2	md3) nepriamo 3

5.	6.	7.	8.
$B \to B$,	$(A \vee B) \to B$,	$A \vee B$,	B,
md1)	md3) vyn $\vee$ 5, 4	md2)	md3) m.p. 7, 6

Porovnajte to s príkladom 3.3.

Tvrdenie 4.2 *Ak existuje matematický dôkaz $A_1, \ldots, A_n$ v teórii Δ taký, že $A_n = A$, tak $\Delta \vdash A$.*

Overenie: Nech $A_1, \ldots, A_n$ je matematický dôkaz v Δ. Matematickou indukciou ukážeme, že pre každé $i = 1, \ldots, n$ platí $\Delta \vdash A_i$.

Predpokladajme, že pre každé $j < i$ platí $\Delta \vdash A_j$. Chceme ukázať, že aj $\Delta \vdash A_i$. $A_1, \ldots, A_n$ je matematický dôkaz v Δ a preto A_i spĺňa jednu z troch podmienok md1) – md3).

Ak A_i spĺňa podmienku md1), tak podľa tvrdenia 3.2a) je $\Delta \vdash A_i$.

Ak A_i spĺňa podmienku md2), tak podľa definície je $\Delta \vdash A_i$.

Predpokladajme, že A_i spĺňa podmienku md3). Potom podľa definície existujú čísla $j_1, \ldots, j_k < i$ také, že

$$\frac{A_{j_1}, \ldots, A_{j_k}}{A_i}$$

je odvodzovacie pravidlo v Δ. Keďže $j_1, \ldots, j_k < i$, tak podľa indukčného predpokladu platí $\Delta \vdash A_{j_1}, \ldots, \Delta \vdash A_{j_k}$ a odtiaľ bezprostredne z definície odvodzovacieho pravidla dostávame $\Delta \vdash A_i$.

Pre $i = n$ dostávame naše tvrdenie.

q.e.d.

Dôsledok 4.1 *Ak $A_1, \ldots, A_n = A$ je matematický dôkaz v Δ, tak $\Delta \models A$.*

Príklad 4.7 Na základe výsledku príkladu 4.6 máme

$$\{A \vee B, \neg A\} \models B$$

pre ľubovoľné výroky A, B.

5 Metódy dôkazu

Matematici matematický dôkaz prezentovaný v predchádzajúcej časti obyčajne nazývajú **priamy dôkaz**. V svojich úvahách však viac ako 2500 rokov používajú aj iné metódy dôkazu. Začneme s tou najjednoduchšou metódou, ktorá sa používa najčastejšie, bez toho, aby si to bežný matematik uvedomoval. Najprv jedna konvencia. Namiesto $\Delta \cup \{A\} \vdash B$ budeme jednoduchšie písať $\Delta, A \vdash B$.

Ak má matematik dokázať implikáciu $A \to B$, tak obyčajne začne slovami "Nech platí A". Teda výrok A pridá medzi predpoklady Δ a v skutočnosti dokazuje výrok B za predpokladov $\Delta \cup \{A\}$. Nasledujúca veta tvrdí, že je to v poriadku, že naozaj ukázal, že $\Delta \vdash A \to B$.

Tvrdenie 5.1 (Veta o dedukcii) *Nech Δ je množina výrokov, A, B sú výroky. Potom $\Delta \vdash A \to B$ vtedy a len vtedy ak $\Delta, A \vdash B$.*

Overenie: Jednoduchšia je implikácia zľava doprava. Predpokladajme, že $\Delta \vdash A \to B$. Potom $\Delta, A \vdash A \to B$ a $\Delta, A \vdash A$. Pomocou odvodzovacieho pravidla modus ponens dostávame $\Delta, A \vdash B$.

Nech teraz $\Delta, A \vdash B$. Potom existuje dôkaz $A_1, \ldots, A_n$ v teórii Δ, A taký, že $A_n = B$. Matematickou indukciou ukážeme, že pre $i = 1, \ldots, n$ platí $\Delta \vdash A \to A_i$. Špeciálne pre $i = n$ dostaneme potom naše tvrdenie.

Predpokladáme teda, že pre každé $j < i$ platí $\Delta \vdash A \to A_j$ a chceme ukázať, že aj $\Delta \vdash A_i$. Keďže A_i je člen dôkazu v Δ, A, tak platí jedna z troch podmienok definície dôkazu.

Ak A_i je axióma výrokového počtu, tak postupnosť

$$\begin{array}{lll} A_i, & A_i \to (A \to A_i), & A \to A_i \\ \text{d1)} & \text{d1)} & \text{d3), 1, 2} \end{array}$$

je dôkaz v Δ a teda $\Delta \vdash A \to A_i$.

Ak $A_i \in \Delta \cup \{A\}$, tak máme dve možnosti. Ak $A_i \in \Delta$, tak postupnosť

$$\begin{array}{lll} A_i, & A_i \to (A \to A_i), & A \to A_i \\ \text{d2)} & \text{d1)} & \text{d3), 1, 2} \end{array}$$

je dôkaz v Δ a teda $\Delta \vdash A \to A_i$.

Ak $A_i = A$, tak jednoprvková postupnosť $A \to A$ je dôkaz v Δ a teda $\Delta \vdash A \to A_i$.

Predpokladajme, že platí tretia možnosť, t.j. existujú čísla $j, k < i$ také, že $A_k = (A_j \to A_i)$. Podľa indukčného predpokladu potom $\Delta \vdash A \to A_j$ a $\Delta \vdash A \to (A_j \to A_i)$ a teda existujú dôkazy $E_1, \ldots, E_k$ a $F_1, \ldots, F_l$ v Δ také, že $E_k = (A \to A_j)$ a $F_l = (A \to (A_j \to A_i)$. Potom nasledujúca postupnosť je dôkaz v Δ

$$\underset{\text{komentár opíš}}{E_1, \quad . \quad . \quad . \quad ,} \overbrace{E_n}^{A \to A_j}, \quad \underset{\text{d1)}}{(A \to A_j) \to ((A \to (A_j \to A_i)) \to (A \to A_i))},$$

$$\underset{\text{d3),}n,n+1}{(A \to (A_j \to A_i)) \to (A \to A_i)}, \quad \underset{\text{komentár opíš}}{F_1, \quad . \quad . \quad . \quad ,} \overbrace{F_m}^{A \to (A_j \to A_i)}, \quad \underset{\substack{\text{d3),}n+m+1,\\ n+m+2}}{A \to A_i}$$
$$\text{index}+n+2$$

a teda $\Delta \vdash A \to A_i$.

q.e.d.

Pytagorejci v 6. storočí pred nar. Kr. poznali metódu dôkazu sporom. Dokázali pomocou nej im nepríjemné tvrdenie o nesúerateľnosti strany a uhlopriečky štvorca (inými slovami, iracionálnosť $\sqrt{2}$). Táto metóda nazvaná neskôr latinsky **reductio ad absurdum** je v matematike veľmi často používaná a spočíva v nasledujúcom tvrdení.

Tvrdenie 5.2 (Reductio ad absurdum) *Nech Δ je množina výrokov, A a B sú výroky.*

a) *Ak $\Delta, \neg A \vdash B$ a $\Delta, \neg A \vdash \neg B$, tak $\Delta \vdash A$.*

b) *Ak $\Delta, A \vdash B$ a $\Delta, A \vdash \neg B$, tak $\Delta \vdash \neg A$.*

Overenie: Predpokladajme, Δ, $\neg A \vdash B$ a Δ, $\neg A \vdash \neg B$. Pomocou odvodzovacieho pravidla"zav $\neg\neg$" z prvého dostaneme Δ, $\neg A \vdash \neg\neg B$. Podľa vety o dedukcii dostaneme $\Delta \vdash \neg A \to \neg\neg B$ a $\Delta \vdash \neg A \to \neg B$. Pomocou odvodzovacieho pravidla "nepriamo" potom máme $\Delta \vdash \neg B \to A$ a $\Delta \vdash B \to A$. Pomocou odvodzovacieho pravidla "rozbor" dostávame $\Delta \vdash A$.

V prípade b) predpokladáme Δ, $A \vdash B$ a Δ, $A \vdash \neg B$. Podľa vety o dedukcii potom $\Delta \vdash A \to B$ a $\Delta \vdash A \to \neg B$. Pomocou odvodzovacieho pravidla "kontra" dostaneme $\Delta \vdash \neg B \to \neg A$ a $\Delta \vdash \neg\neg B \to \neg A$. Podľa odvodzovacieho pravidla "rozbor" potom $\Delta \vdash \neg A$.

q.e.d.

Dvojica výrokov C a $\neg C$ sa nazýva **spor v teórii** Δ, ak súčasne platí $\Delta \vdash C$ a $\Delta \vdash \neg C$. Teda metóda dôkazu sporom spočíva v tom, že ak chceme dokázať za predpokladov Δ výrok A, tak medzi predpoklady pridáme výrok $\neg A$ a dokážeme nejaký spor. Oproti priamemu dôkazu to má tú výhodu, že nemáme dopredu

striktne daný cieľ. Ak robíme priamy dôkaz výroku A, t.j. konštruujeme matematický dôkaz, tak musíme skončiť výrokom A, teda dopredu máme stanovený pevný cieľ, ktorý môže byť ťažké dosiahnuť. Pri dôkaze sporom máme určitú voľnosť. Naším cieľom je **nejaký** spor. Pri dôkaze výroku tvaru implikácie sa často kombinuje veta o dedukcii s odvodzovacím pravidlom nepriamo alebo s metódou dôkazu sporom.

Tvrdenie 5.3 *Ak* $\Delta, \neg B \vdash \neg A$*, tak* $\Delta \vdash A \to B$*.*

Overenie: Ak Ak $\Delta, \neg B \vdash \neg A$, tak podľa vety o dedukcii $\Delta \vdash \neg B \to \neg A$ a odtiaľ pomocou odvodzovacieho pravidla "nepriamo" $\Delta \vdash A \to B$.

q.e.d.

Tvrdenie 5.4 *Ak* $\Delta, \neg B, A \vdash C$*,* $\Delta, \neg B, A \vdash \neg C$*, tak* $\Delta \vdash A \to B$*.*

Overenie: Ak $\Delta, \neg B, A \vdash C$, $\Delta, \neg B, A \vdash \neg C$, tak podľa tvrdenia o dôkaze sporom $\Delta, \neg B \vdash \neg A$. Podľa vety o dedukcii potom $\Delta \vdash \neg B \to \neg A$ a použitím odvodzovacieho pravidla "nepriamo" dostávame $\Delta \vdash A \to B$.

q.e.d.

6 Kompaktnosť

V predchádzajúcich úvahách sme neupresnili, či množina Δ je konečná alebo nie. Všetky prezentované výsledky platia aj pre nekonečné množiny Δ.

Ľahko sa vidí, že dokázateľnosť sa vzťahuje len "na konečne mnoho výrokov". Vyjadruje to nasledujúci výsledok.

Tvrdenie 6.1 (Veta o kompaktnosti) *Nech* Δ *je množina výrokov a* A *je výrok. Potom* $\Delta \vdash A$ *vtedy a len vtedy, keď existuje konečná množina* $\Delta_0 \subseteq \Delta$ *taká, že* $\Delta_0 \vdash A$*.*

Overenie: Predpokladajme, že $\Delta \vdash A$. Potom existuje dôkaz $A_1, \ldots, A_n$ v Δ, ktorého posledný člen je $A_n = A$. Nech Δ_0 je množina tých členov dôkazu, ktoré sú prvkom množiny Δ, teda

$$\Delta_0 = \{B \in \Delta; \text{existuje } i = 1, \ldots, n \text{ také, že } B = A_i\}.$$

Potom postupnosť $A_1, \ldots, A_n$ aj dôkazom v konečnej množine $\Delta_0 \subseteq \Delta$. Teda $\Delta_0 \vdash A$.

Naopak, ak existuje konečná množina $\Delta_0 \subseteq \Delta$ taká, že $\Delta_0 \vdash A$, tak podľa tvrdenia 3.2c) je $\Delta \vdash A$.

q.e.d.

Podobné výsledky platia aj pre vzťahy pravdivosti. Platí toto:

Tvrdenie 6.2 (Sémantická veta o kompaktnosti) *Nech* Δ *je množina výrokov a* A *je výrok. Potom* $\Delta \models A$ *vtedy a len vtedy, keď existuje konečná množina* $\Delta_0 \subseteq \Delta$ *taká, že* $\Delta_0 \models A$*.*

Overenie je však zložitejšie a vo všeobecnosti využíva určité dosť silné výsledky teórie množín. My overíme jeho platnosť v prípade spočítateľnej množiny Δ. Najprv však zavedieme jeden užitočný pojem.

Nech Δ je množina výrokov, A je výrok. Nech Π je množina všetkých elementárnych výrokov, ktoré sa vyskytujú v niektorom výroku z množiny Δ alebo vo výroku A. Budeme hovoriť, že výrok A **je splniteľný v** Δ, ak existuje zobrazenie $v : \Pi \longrightarrow \{0,1\}$ ("riadok tabuľky") také, že $v(B) = 1$ pre každý výrok $B \in \Delta$ a $v(A) = 1$.

Podľa definície pravdivostnej hodnoty platí, že $v(A) = 1$ vtedy a len vtedy, keď $v(\neg A) = 0$. Teda

$$\Delta \models A \text{ vtedy a len vtedy, keď } \neg A \text{ nie je splniteľné v } \Delta. \tag{6.4}$$

Použitím tejto ekvivalencie ľahko vidieť, že sémantická veta o kompaktnosti vyplýva (a je aj ekvivalentná) z nasledujúceho tvrdenia:

Tvrdenie 6.3 (Veta o splniteľnosti) *Výrok A je splniteľný v Δ vtedy a len vtedy, keď je splniteľný v každej konečnej podmnožine $\Delta_0 \subseteq \Delta$.*

Overenie: Implikácia zľava doprava je triviálne pravdivá.

Overíme implikáciu sprava doľava pre spočítateľnú množinu Δ. Nech teda $\Delta = \{B_0, B_1, \ldots, B_n, \ldots\}$ je spočítateľná množina výrokov. Predpokladáme, že pre každú konečnú množinu $\Delta_0 \subseteq \Delta$ je výrok A splniteľný v Δ_0. Potom výrok A je splniteľný v každej množine $\{B_0, \ldots, B_n\}$. Nech Π_n je množina

$$\{p \text{ elementárny výrok}; p \text{ sa vyskytuje v niektorom z výrokov } B_0, \ldots, B_n, A\}.$$

Zrejme pre každé n je $\Pi_n \subseteq \Pi_{n+1}$. Nech $\Pi = \bigcup_{n=0}^{\infty} \Pi_n$. Pre každé n označíme

$$V_n = \{v : \Pi_n \longrightarrow \{0,1\}; v(B_1) = \ldots = v(B_n) = v(A) = 1\}, \qquad V = \bigcup_{n=0}^{\infty} V_n.$$

Podľa predpokladu každá množina V_n je neprázdna.

Máme dve možnosti: množina Π je konečná alebo nekonečná.

Uvažujme najprv prípad, keď množina Π je konečná. Potom existuje také n_0, že pre každé $n > n_0$ je $\Pi_n = \Pi_{n_0} = \Pi$. Potom aj

$$V_n \subseteq {}^{\Pi_n}\{0,1\} = {}^{\Pi}\{0,1\} \text{ pre } n \geq n_0.$$

Zrejme platí $V_{n+1} \subseteq V_n$ pre $n \geq n_0$. Keďže množina ${}^{\Pi}\{0,1\}$ je konečná, tak existuje také $n_1 \geq n_0$ že $V_n = V_{n_1}$ pre $n > n_1$. Keďže $V_{n_1} \neq \emptyset$, tak existuje $v \in V_{n_1}$ a potom platí $v(B) = 1$ pre každé $B \in \Delta$, $v(A) = 1$, čo sme chceli ukázať.

Nech teraz množina Π je nekonečná. Ak $v, w \in {}^{\Pi}\{0,1\}$, tak $v \sqsubseteq w$ znamená toto[5]:

$$\mathcal{D}(v) \subseteq \mathcal{D}(w),\ v(B) = w(B) \text{ pre každé } B \in \mathcal{D}(v).$$

[5] $\mathcal{D}(f)$ je definičný obor funkcie f.

Poznamenajme, že

$$\text{ak } w \in V,\ v \sqsubseteq w,\ \text{tak } \ \in V. \tag{6.5}$$

Zostrojíme postupnosť $v_n \in V_n$, $n = 0, 1, \ldots, n, \ldots$ takú, že pre každé n je $v_n \sqsubseteq v_{n+1}$.

Pre $v \in V_n$ označíme $W_v = \{w \in V; v \sqsubseteq w\}$. Ľahko sa overí, že platí

$$\text{ak } v \in V_n,\ \text{tak } W_v = \bigcup \{W_w; w \in V_{n+1}, v \sqsubseteq w\}. \tag{6.6}$$

Naviac, $V = \bigcup_{v \in V_0} W_v$. Teraz už ľahko zostrojíme postupnosť v_n, $n \in \mathbb{N}$. Keďže množina V je nekonečná, množina V_0 je konečná, tak existuje také $v_0 \in V_0$, že množina W_{v_0} je nekonečná. Ak už máme zostrojené $v_n \in V_n$ také, že množina W_n je nekonečná, tak podľa (6.6) existuje $v_{n+1} \in V_{n+1}$ také, že $v_n \sqsubseteq v_{n+1}$ a množina $W_{v_{n+1}}$ je nekonečná.

Zobrazenie $\mu : \Pi \longrightarrow \{0, 1\}$ definované predpisom

$$\mu(q) = v_n(q) \text{ ak } q \in \Pi_n \subseteq \Pi$$

je "riadok tabuľky", ktorý spĺňa množinu Δ a výrok A.

q.e.d.

7 Úplnosť výrokového počtu

V tejto časti ukážeme tvrdenie, ktoré hovorí o tom, že dôkaz je dostatočne široký prostriedok pre overovanie pravdivosti, menovite

Tvrdenie 7.1 (Veta o úplnosti)

$$\textit{Ak } \Delta \models A, \textit{ tak } \Delta \vdash A.$$

Overenie tohoto tvrdenia sa rozdelí fakticky na tri časti: najprv ho overíme pre $\Delta = \emptyset$, potom pre Δ konečné a nakoniec využijeme sémantickú vetu o kompaktnosti, aby sme ukázali tvrdenie pre nekonečné (spočítateľné) Δ.

Relatívne najzložitejší je prvý prípad. Začneme s dôležitým pomocným tvrdením. Najprv označenie. Ak Q označuje možnú pravdivostnú hodnotu 0 alebo 1 výroku A, tak $(Q)A$ označuje výrok A ak $Q = 1$ a výrok $\neg A$ ak $Q = 0$.

Tvrdenie 7.2 (Churchova lema[6]) *Nech A je výrok utvorený z elementárnych výrokov $q_1 \ldots, q_n$. Nech Q je pravdivostná hodnota výroku A v riadku tabuľky, v ktorom $Q_1, \ldots, Q_n$ sú pravdivostné hodnoty elementárnych výrokov $q_1, \ldots, q_n$[7]. Potom*

$$(Q_1)q_1, \ldots, (Q_n)q_n \vdash (Q)A. \tag{7.7}$$

[6] Alonzo Church (1900–1970) bol významný americký matematik, ktorý získal dôležité výsledky v matematickej logike.

[7] Teda $Q = v(A)$ v "riadku" tabuľky, v ktorom $v(q_1) - Q_1, \ldots, v(q_n) = Q_n$

Príklad 7.1 Ilustrujeme tvrdenie na príklade. Nech $A = (q_2 \to (q_1 \vee \neg q_2))$.

Ak $Q_1 = Q_2 = 0$, tak je $Q = 1$. Potom $(Q_1)q_1 = \neg q_1$, $(Q_2)q_2 = \neg q_2$ a $(Q)A = A$. Churchova lema tvrdí, že

$$\neg q_1, \neg q_2 \vdash A.$$

Ak $Q_1 = 0$ a $Q_2 = 1$, tak je $Q = 0$ a Churchova lema tvrdí, že

$$\neg q_1, q_2 \vdash \neg A.$$

Overenie:

V celom overení $Q_1, \ldots, Q_n$ sú ľubovoľné ale pevné pravdivostné hodnoty elementárnych výrokov $q_1, \ldots, q_n$. Kvôli jednoduchosti označíme

$$\Delta_0 = \{(Q_1)q_1, \ldots, (Q_n)q_n\}.$$

Nech $A_1, \cdots, A_m$ je vytvárajúca postupnosť výroku A. Môžeme predpokladať, že v tejto postupnosti sa nevyskytnú iné elementárne výroky ako $q_1, \ldots, q_n$. Nech $R_1, \ldots, R_m$ sú pravdivostné hodnoty výrokov $A_1, \ldots, A_m$ v tom riadku tabuľky, v ktorom sú pod elementárnymi výrokmi $q_1, \ldots, q_n$ pravdivostné hodnoty $Q_1, \ldots, Q_n$[8]. Matematickou indukciou ukážeme, že pre každé $i = 1, \ldots, m$ platí

$$\Gamma \vdash (R_i)A_i.$$

Pre $i = n$ dostaneme tvrdenie.

Predpokladajme, že pre každé $j < i$ platí $\Gamma \vdash (R_j)A_j$ a chceme ukázať, že $\Gamma \vdash (R_i)A_i$.

Keďže A_i je člen VPV, tak platí jedna z troch podmienok:

a) A_i je elementárny výrok,

b) existuje index $j < i$ taký, že $A_i = \neg A_j$,

c) existujú indexy j, $k < i$ také, že $A_i = (A_j \square A_k)$, kde $\square = \wedge, \vee, \to, \equiv$.

Musíme overiť 19 prípadov: prípad a) je 1, v prípade b) musíme rozlíšiť, či R_j je 0 alebo 1, teda 2 prípady a konečne v každom zo štyroch prípadov c) (podľa toho, čo je $\square$), musíme ešte rozlíšiť štyri možné kombinácie pravdivostných hodnôt R_j a R_k, teda 16 prípadov.

Začneme prípadom a). Podľa predpokladu, A_i je niektorý z elementárnych výrokov $q_1, \ldots, q_n$, teda existuje $l \leq n$ také, že $A_i = q_l$. Potom $R_i = Q_l$ a $(R_i)A_i = (Q_l)q_l \in \Gamma$. Teda $\Gamma \vdash (R_i)A_i$.

Uvažujme prípad b), t.j. $A_i = \neg A_j$, $j < i$. Ak $R_j = 0$, tak $R_i = 1$ a $(R_i)A_i = A_i = \neg A_j = (R_j)A_j$. Podľa indukčného predpokladu $\Gamma \vdash (R_j)A_j$ a teda aj $\Gamma \vdash (R_i)A_i$. Ak $R_j = 1$, tak $R_i = 0$ a $(R_i)A_i = \neg\neg A_j$. Podľa indukčného predpokladu $\Gamma \vdash A_j$. Pomocou odvodzovacieho pravidla "zav $\neg\neg$" dostávame $\Gamma \vdash \neg\neg A_j$ a teda $\Gamma \vdash (R_i)A_i$.

[8]Teda $R_j = v(A_j)$, $j = 1, \ldots, m$, kde $v(q_i) = Q_i$ pre $i = 1, \ldots, n$

Nech platí podmienka c). Na ilustráciu predvedieme prípady.

Nech $\square = \wedge$, $R_j = 1$ a $R_k = 0$. Potom $A_i = (A_j \wedge A_k)$ a $A_i = 0$. Podľa indukčného predpokladu máme $\Gamma \vdash A_j$, $\Gamma \vdash \neg A_k$ a chceme ukázať $\Gamma \vdash \neg A_i$. Využijeme metódu dôkazu sporom. Postupnosť

$$\begin{array}{ccc} A_j \wedge A_k, & A_k \wedge A_j, & A_k \\ md2) & md3)\ \text{kom}\ \wedge & md3)\ \text{vyn}\ \wedge \end{array}$$

je matematický dôkaz v Γ, A_i, teda $\Gamma, A_i \vdash A_k$. Z indukčného predpokladu máme $\Gamma, A_i \vdash \neg A_k$. Odtiaľ podľa tvrdenia 5.2b) dostávame $\Gamma \vdash \neg A_i$.

Nech teraz $\square = \vee$, $R_j = 0$ a $R_i = 0$. Potom $A_i = (A_j \vee A_k)$ a $R_i = 0$. Podľa indukčného predpokladu máme $\Gamma \vdash \neg A_j$, $\Gamma \vdash \neg A_k$ a chceme ukázať $\Gamma \vdash \neg A_i$. Postupnosť

$$\begin{array}{cccccc} A_j \to A_j, & \neg A_k \to (\neg A_j \to \neg A_k), & \neg A_k, & \neg A_j \to \neg A_k, & A_k \to A_j, \\ md1) & md1) & md2) & md3)\ \text{m.p.} & md3)\ \text{nepriamo} \end{array}$$

$$\begin{array}{ccccc} (A_j \vee A_k) \to A_j, & \neg A_j \to \neg(A_j \vee A_k), & \neg A_j, & \neg(A_j \vee A_k) \\ md3)\ \text{rozbor} & md3)\ \text{kontra} & md2) & md3)\ \text{m.p.} \end{array}$$

je matematický dôkaz v Γ a teda $\Gamma \vdash \neg A_i$.

Nech $\square = \to$, $R_j = 0$ a $R_k = 0$. Potom $A_i = (A_j \to A_k)$ a $R_i = 1$. Podľa indukčného predpokladu $\Gamma \vdash \neg A_j$ a $\Gamma \vdash \neg A_k$. Chceme $\Gamma \vdash (A_j \to A_k)$. Zase napíšeme matematický dôkaz v Γ:

$$\begin{array}{cccc} \neg A_j \to (\neg A_k \to \neg A_j), & \neg A_j, & \neg A_k \to \neg A_j, & A_j \to A_k, \\ md1) & md2) & md3)\ \text{m.p.} & md3)\ \text{nepriamo} \end{array}$$

Konečne uvažujme prípad $\square = \equiv$, $R_j = 1$ a $R_k = 0$. Potom $A_i = (A_j \equiv A_k$ a $R_i = 0$. Podľa indukčného predpokladu máme $\Gamma \vdash A_j$, $\Gamma \vdash \neg A_k$ a chceme $\Gamma \vdash \neg(A_j \equiv A_k)$. Použijeme metódu dôkazu sporom. Postupnosť

$$\begin{array}{ccccccc} A_j \equiv A_k, & (A_j \equiv A_k) \to (A_j \to A_k), & A_j \to A_k, & A_j, & A_k \\ md2) & md1) & md3)\ \text{m.p.} & md2) & md3)\ \text{m.p.} \end{array}$$

je matematický dôkaz v $\Gamma, (A_j \equiv A_k)$. Teda $\Gamma, (A_j \equiv A_k) \vdash A_k$. Podľa druhého indukčného predpokladu máme však $\Gamma, (A_j \equiv A_k) \vdash \neg A_k$ a teda podľa vety 5.2b) je $\Gamma \vdash \neg(A_j \equiv A_k)$.

Ostatných 12 prípadov možno ukázať podobne.

q.e.d.

Myšlienku nasledujúceho tvrdenia najprv ilustrujeme na jeho špeciálnom prípade.

Príklad 7.2 Ilustrujeme najprv myšlienku overenia na špeciálnom prípade. Nech A je výrok – tautológia, zostrojený z dvoch elementárnych výrokov q_1, q_2. Keďže výrok A je tautológia, tak pre ľubovoľné pravdivostné hodnoty Q_1, Q_2

elementárnych výrokov q_1, q_2, pravdivostná hodnota výroku A je $Q = 1$. Podľa Churchovej lemy máme

$$\begin{aligned} q_1, q_2 &\vdash A, \\ q_1, \neg q_2 &\vdash A, \\ \neg q_1, q_2 &\vdash A, \\ \neg q_1, \neg q_2 &\vdash A. \end{aligned}$$

Podľa vety o dedukcii postupne dostaneme

$$\begin{aligned} q_1 &\vdash q_2 \to A, \\ q_1 &\vdash \neg q_2 \to A, \\ \neg q_1 &\vdash q_2 \to A, \\ \neg q_1 &\vdash \neg q_2 \to A. \end{aligned}$$

Pomocou odvodzovacieho pravidla "rozbor" z prvých dvoch riadkov dostaneme

$$q_1 \vdash A$$

a z druhých dvoch riadkov dostaneme

$$\neg q_1 \vdash A.$$

Zase, podľa vety o dedukcii postupne dostaneme

$$\emptyset \vdash q_1 \to A, \qquad \emptyset \vdash \neg q_1 \to A$$

a opätovným použitím odvodzovacieho pravidla "rozbor" konečne dostaneme

$$\emptyset \vdash A.$$

Nasledujúce tvrdenie, dôležité samo o sebe, sa overí rovnako.

Tvrdenie 7.3 (Postova veta o dokázateľnosti tautológie)
Ak výrok A je tautológia, tak $\emptyset \vdash A$

Overenie: Predpokladajme, A je utvorený z elementárnych výrokov $q_1, \ldots, q_n$. Keďže výrok A je tautológia, pre ľubovoľné pravdivostné hodnoty $Q_1, \ldots, Q_n$ elementárnych výrokov $q_1, \ldots, q_n$ pravdivostná hodnota Q výroku A je 1. Teda podľa Churchovej lemy pre ľubovoľné $Q_1, \ldots, Q_n$ platí

$$(Q_1)q_1, \ldots, (Q_n)q_n \vdash A. \tag{7.8}$$

Špeciálne, pre ľubovoľné $Q_1, \ldots, Q_{n-1}$ a $Q_n = 0$ máme

$$(Q_1)q_1, \ldots, (Q_{n-1})q_{n-1}, \neg q_n \vdash A$$

a pre ľubovoľné $Q_1, \ldots, Q_{n-1}$ a $Q_n = 1$ máme

$$(Q_1)q_1, \ldots, (Q_{n-1})q_{n-1}, q_n \vdash A.$$

Podľa vety o dedukcii potom

$$(Q_1)q_1, \ldots, (Q_{n-1})q_{n-1} \vdash \neg q_n \to A, \quad (Q_1)q_1, \ldots, (Q_{n-1})q_{n-1} \vdash q_n \to A.$$

Použitím odvodzovacieho pravidla "rozbor" dostávame

$$(Q_1)q_1, \ldots, (Q_{n-1})q_{n-1} \vdash A$$

pre ľubovoľné pravdivostné hodnoty $Q_1, \ldots, Q_{n-1}$.

Zopakujeme tento postup $n-1$ krát a dostaneme

$$(Q_1)q_1 \vdash A$$

pre ľubovoľné Q_1. Zase, špecifikáciou Q_1 dostaneme

$$\neg q_1 \vdash A, \qquad q_1 \vdash A$$

a podľa vety o dedukcii

$$\emptyset \vdash \neg q_1 \to A, \qquad \emptyset \vdash q_1 \to A.$$

Odtiaľ použitím odvodzovacieho pravidla "rozbor" dostaneme

$$\emptyset \vdash A,$$

čo sme mali ukázať.

q.e.d.

Najprv overíme pomocné tvrdenie, ktoré využijeme pri overení vety o úplnosti.

Tvrdenie 7.4 (Sémantická veta o dedukcii)
Nech Γ je množina výrokov, A, B sú výroky. Ak $\Gamma, B \models A$, tak $\Gamma \models B \to A$.

Overenie: Predpokladajme, že $\Gamma, B \models A$.

Uvažujme riadok spoločnej tabuľky pre všetky výroky z Γ a výroky A, B, v ktorom sú pod výrokmi z Γ jednotky. Máme dve možnosti.

Pod výrokom B je jednotka. Potom podľa predpokladu je jednotka aj pod výrokom A a teda aj pod výrokom $B \to A$.

Pod výrokom B je nula. Potom pod výrokom $B \to A$ je jednotka.

q.e.d.

Dôsledok 7.1 *Ak $\{B_1, \ldots, B_m\} \models A$, tak výrok*

$$B_1 \to (B_2 \to (\ldots (B_m \to A) \ldots))$$

je tautológia.

Overenie vety o úplnosti: Nech $\Delta \models A$. Podľa sémantickej vety o kompaktnosti potom existuje konečná množina $\Delta_0 \subseteq \Gamma$ taká, že $\Delta_0 \models A$. Nech

$$\Delta_0 = \{B_1 \ \ldots, B_m\}.$$

Podľa dôsledku 7.1 výrok $B_1 \to (B_2 \to (\ldots (B_m \to A) \ldots))$ je tautológia. Podľa tvrdenie 7.3 platí

$$\emptyset \vdash B_1 \to (B_2 \to (\ldots (B_m \to A) \ldots)).$$

m– násobným použitím odvodzovacieho pravidla modus ponens potom postupne dostaneme

$$\begin{aligned} \{B_1\} &\vdash B_2 \to (B_3 \to (\ldots (B_m \to A) \ldots)) \\ \{B_1, B_2\} &\vdash B_3 \to (B_4 \to (\ldots (B_m \to A) \ldots)) \\ \vdots \qquad & \qquad \vdots \\ \Delta_0 = \{B_1, B_2, \ldots, B_m\} &\vdash A. \end{aligned}$$

Potom platí aj $\Delta \vdash A$.

q.e.d.

Príklad 7.3 Postovu vetu 7.3 o dokázateľnosti tautológie môžeme výhodne využiť. Dáme jeden jednoduchý príklad. Ľahko sa zistí, že nasledujúce výroky sú tautológie

$$\begin{gathered} (A \to C) \to ((B \to D) \to ((A \wedge B) \to (C \wedge D))), \\ (A \to C) \to ((B \to D) \to ((A \vee B) \to (C \vee D))), \\ (A \to (B \to C)) \to ((A \wedge B) \to C), \\ ((A \wedge B) \to C) \to ((A \to (B \to C)). \end{gathered}$$

Teda sú dokázateľné z prázdnych predpokladov a môžeme ich použiť na overenie toho, že nasledujúce postupnosti sú odvodzovacie pravidlá:

$$\frac{A \to C,\ B \to D}{(A \wedge B) \to (C \wedge D)}, \qquad \frac{A \to C,\ B \to D}{(A \vee B) \to (C \vee D)},$$

$$\frac{A \to (B \to C)}{(A \wedge B) \to C}, \qquad \frac{(A \wedge B) \to C}{A \to (B \to C)}.$$

Navrhujeme čitateľovi, aby – ako dobré cvičenie – zostrojil dôkazy uvedených tautológií.

8 Normálny tvar výroku

Výrok tvaru

$$A_1 \vee \ldots \vee A_n$$

sa nazýva **elementárna disjunkcia**, ak každý z výrokov A_i, $i = 1, \ldots, n$ je elementárny výrok alebo negácia elementárneho výroku a, okrem prípadu $q \vee \neg q$, žiadny elementárny výrok sa v nej nevyskytuje dvakrát. Podobne, výrok tvaru

$$A_1 \wedge \ldots \wedge A_n$$

sa nazýva **elementárna konjunkcia**, ak každý z výrokov A_i, $i = 1, \ldots, n$ je elementárny výrok alebo negácia elementárneho výroku a, okrem prípadu $q \wedge \neg q$, žiadny elementárny výrok sa v nej nevyskytuje dvakrát. Naviac elementárny výrok alebo jeho negácia je jednočlenná elementárna konjunkcia aj disjunkcia. Ak $B_1, \ldots, B_m$ sú elementárne disjunkcie, tak hovoríme, že výrok

$$B_1 \wedge \ldots \wedge B_m$$

je v **normálnom konjunktívnom tvare**. Podobne, ak $B_1, \ldots, B_m$ sú elementárne konjunkcie, tak hovoríme, že výrok

$$B_1 \vee \ldots \vee B_m$$

je v **normálnom disjunktívnom tvare**. Ako vyššie, môže byť $m = 1$, teda elementárna disjunkcia je výrok v konjunktívnom normálnom tvare a elementárna konjunkcia je výrok v disjunktívnom normálnom tvare. Ak naviac všetky elementárne konjunkcie (disjunkcie) obsahujú tie isté elementárne výroky, tak príslušný normálny tvar sa nazýva **úplný**.

Pre výrok v disjunktívnom normálnom tvare sa ľahko zostrojí pravdivostná tabuľka. Totiž elementárna konjunkcia je pravdivá práve vtedy, keď sú pravdivé všetky jej členy. Ak je výrok v úplnom disjunktívnom tvare, tak každá jeho elementárna konjunkcia je pravdivá práve v jednom riadku tabuľky.

Príklad 8.1 Uvažujme výrok v úplnom disjunktívnom normálnom tvare

$$(q_1 \wedge \neg q_2 \wedge q_3) \vee (q_1 \wedge q_2 \wedge q_3) \vee (\neg q_1 \wedge q_2 \wedge q_3). \tag{8.9}$$

Tento výrok je pravdivý, ak je pravdivá aspoň jedna z elementárnych konjunkcií. Naviac, každá elementárna konjunkcia je pravdivá práve v jednom riadku tabuľky, lebo obsahuje všetky elementárne výroky, z ktorých je výrok utvorený. Teda výrok (8.9) má pravdivostnú hodnotu 1 len v troch riadkoch tabuľky:

q_1	q_2	q_3	$(q_1 \wedge \neg q_2 \wedge q_3) \vee (q_1 \wedge q_2 \wedge q_3) \vee (\neg q_1 \wedge q_2 \wedge q_3)$
1	0	1	1
1	1	1	1
0	1	1	1

V ostatných riadkoch tabuľky má výrok (8.9) pravdivostnú hodnotu 0.

Výrok $(q_1 \wedge \neg q_3) \vee (\neg q_1 \wedge q_2)$ má pravdivostnú hodnotu 1 v tých riadkoch tabuľky, kde

q_1	q_2	q_3	$(q_1 \wedge \neg q_3) \vee (\neg q_1 \wedge q_2)$
1		0	1
0	1		1

Teda po doplnení dostávame

q_1	q_2	q_3	$(q_1 \wedge \neg q_3) \vee (\neg q_1 \wedge q_2)$
1	1	0	1
1	0	0	1
0	1	1	1
0	1	0	1

Musíme dať pozor pri dopĺňaní riadkov, lebo niektoré sa môžu opakovať. Ak urobíme podobným spôsobom tabuľku pre výrok $(q_1 \wedge \neg q_3) \vee (q_1 \wedge \neg q_2)$, tak 2. a 4. riadok sú rovnaké – opakujú sa:

q_1	q_2	q_3	$(q_1 \wedge \neg q_3) \vee (q_1 \wedge \neg q_2)$
1	1	0	1
1	0	0	1
1	0	1	1
1	0	0	1

Na základe de Morganových pravidiel

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B), \qquad \neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$$

z výroku v disjunktívnom normálnom tvare negovaním dostaneme výrok v konjunktívnom normálnom tvare a naopak. Dôležitý je nasledovný výsledok.

Tvrdenie 8.1 *Pre každý výrok existuje ekvivalentný výrok v úplnom konjunktívnom normálnom tvare a ekvivalentný výrok v úplnom disjunktívnom normálnom tvare.*

Overenie: Nech $A(q_1, \ldots, q_n)$ je výrok. Dáme návod na konštrukciu výroku v úplnom disjunktívnom normálnom tvare, ktorý je ekvivalentný výroku A.

Najprv zostrojíme pravdivostnú tabuľku pre výrok A. Ak v žiadnom riadku tabuľky nie je pravdivostná hodnota 1, tak výrok A je ekvivalentný výroku $q_1 \wedge \neg q_1$, ktorý je v disjunktívnom normálnom tvare.

Predpokladajme teda, že aspoň v jednom riadku tabuľky má výrok A pravdivostnú hodnotu 1. Pre každý riadok tabuľky, v ktorom výrok A má pravdivostnú hodnotu 1 a elementárne výroky $q_1, \ldots, q_n$ majú pravdivostné hodnoty $Q_1, \ldots, Q_n$, utvoríme elementárnu konjunkciu $(Q_1)q_1 \wedge \ldots \wedge (Q_n)q_n$. Nech B je disjunkcia elementárnych konjunkcií utvorených pre všetky tie riadky tabuľky,

v ktorých má výrok A pravdivostnú hodnotu 1. Ľahko vidieť, že výrok B je v úplnom disjunktívnom normálnom tvare. Keďže tabuľky výrokov A a B sú rovnaké, tak výroky A, B sú ekvivalentné.

Ak C je výrok v disjunktívnom normálnom tvare a je ekvivalentný výroku $\neg A$, tak negáciu výroku C vieme ľahko previesť do konjunktívneho normálneho tvaru a táto bude ekvivalentná výroku A.

q.e.d.

Budeme hovoriť, že výrok B je disjunktívny normálny tvar výroku A.

Príklad 8.2 Nájdeme výrok v disjunktívnom normálnom tvare ekvivalentný výroku

$$(q_1 \vee \neg q_2) \to (q_2 \wedge q_3). \tag{8.10}$$

Zostrojíme najprv pravdivostnú tabuľku:

q_1	q_2	q_3	$(q_1 \vee \neg q_2) \to (q_2 \wedge q_3)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

Vytvoríme elementárne konjunkcie pre 1., 5. a 6. riadok a spojíme ich disjunkciami

$$(q_1 \wedge q_2 \wedge q_3) \vee (\neg q_1 \wedge q_2 \wedge q_3) \vee (\neg q_1 \wedge q_2 \wedge \neg q_3). \tag{8.11}$$

Tento výrok je v úplnom disjunktívnom normálnom tvare a je ekvivalentný výroku (8.10). Ľahko sa zistí, že aj výrok

$$(\neg q_1 \wedge q_2) \vee (q_2 \wedge q_3) \tag{8.12}$$

je v disjunktívnom normálnom tvare a je ekvivalentný výroku (8.10). Tento výrok však nie je v úplnom normálnom tvare.

Výrok v disjunktívnom normálnom tvare ľahko upravíme na výrok v úplnom disjunktívnom normálnom tvare. Ak v elementárnej konjunkcii $A_1 \wedge \ldots \wedge A_n$

chýba elementárny výrok q, tak túto konjunkciu nahradíme ekvivalentnou disjunkciou

$$(A_1 \wedge \ldots \wedge A_n \wedge q) \vee (A_1 \wedge \ldots \wedge A_n \wedge \neg q).$$

Tak pokračujeme dovtedy, kým nedostaneme úplný normálny tvar. Opakujúce sa elementárne konjunkcie vynecháme. Podobný postup môžeme použiť pre konjunktívny normálny tvar.

Príklad 8.3 Výrok (8.12) upravíme na úplný disjunktívny tvar postupne takto:

$$((\neg q_1 \wedge q_2 \wedge q_3) \vee (\neg q_1 \wedge q_2 \wedge \neg q_3)) \vee ((q_2 \wedge q_3 \wedge q_1) \vee (q_2 \wedge q_3 \wedge \neg q_1)),$$

$$(\neg q_1 \wedge q_2 \wedge q_3) \vee (\neg q_1 \wedge q_2 \wedge \neg q_3) \vee (q_1 \wedge q_2 \wedge q_3).$$

Dostali sme výrok (8.11).

Uvedieme aj iný spôsob získania ekvivalentného výroku v disjunktívnom alebo konjunktívnom normálnom tvare. Využijeme nasledujúce ekvivalencie:

$$\begin{array}{ll}
(e1) & (A \to B) \Leftrightarrow (\neg A \vee B) \\
(e2) & (A \equiv B) \Leftrightarrow ((\neg A \vee B) \wedge (A \vee \neg B)) \\
(e3) & \neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B) \\
(e4) & \neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B) \\
(e5) & \neg\neg A \Leftrightarrow A \\
(e6) & (A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C)) \\
(e7) & (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C)) \\
(e8) & (A \vee B) \Leftrightarrow (B \vee A) \\
(e9) & (A \wedge B) \Leftrightarrow (B \wedge A) \\
(e10) & (A \vee A) \Leftrightarrow A \\
(e11) & (A \wedge A) \Leftrightarrow A
\end{array}$$

Ak chceme nájsť ekvivalentný výrok v disjunktívnom normálnom tvare, tak postupujeme nasledovne:
1. použitím (e1) a (e2) nahradíme implikáciu a ekvivalenciu disjunkciami, konjunkciami a negáciami;
2. použitím (e3) a (e4) prenesieme negácie pred elementárne výroky;
3. použitím (e5) odstránime viacnásobné negácie;
4. použitím distributívneho zákona (e6) upravíme konjunkcie tak, aby sme mali disjunkcie zátvoriek, v ktorých sú len konjunkcie elementárnych výrokov alebo ich negácií;
5. použitím (e9) a (e11) odstránime opakované elementárne výroky alebo ich negácie;
6. ak sa niekde vyskytne konjunkcia elementárneho výroku a jeho negácie, tak príslušnú zátvorku vynecháme; ak sú všetky zátvorky také, tak celý výrok je ekvivalentný výroku $q \wedge \neg q$.

Príklad 8.4 Nájdeme disjunktívny normálny tvar výroku

$$\neg((p \to \neg q) \vee (q \equiv r)).$$

Postupne dostávame:

$$\neg((\neg p \vee \neg q) \vee ((\neg q \vee r) \wedge (\neg r \vee q))),$$
$$\neg(\neg p \vee \neg q) \wedge \neg((\neg q \vee r) \wedge (\neg r \vee q)),$$
$$(\neg\neg p \wedge \neg\neg q) \wedge (\neg(\neg q \vee r) \vee \neg(\neg r \vee q)),$$
$$(\neg\neg p \wedge \neg\neg q) \wedge ((\neg\neg q \wedge \neg r) \vee (\neg\neg r \wedge \neg q)),$$
$$(p \wedge q) \wedge ((q \wedge \neg r) \vee (r \wedge \neg q)),$$
$$((p \wedge q) \wedge (q \wedge \neg r)) \vee ((p \wedge q) \wedge (r \wedge \neg q)),$$
$$(p \wedge q \wedge \neg r) \vee (q \wedge q \wedge r \wedge \neg q)),$$
$$(p \wedge q \wedge \neg r).$$

Pre nájdenie konjunktívneho normálneho tvaru postupujeme podobne, len v 4. kroku použijeme ekvivalenciu (e7), v 5. kroku používame ekvivalencie (e8) a (e10) a konečne v 6. kroku vynecháme zátvorku, v ktorej je disjunkcia výroku a jeho negácie.

Použitím ekvivalencií (e1), (e2) a

$$(e12) \qquad (A \vee B) \Leftrightarrow \neg(\neg A \wedge \neg B)$$
$$(e13) \qquad (A \wedge B) \Leftrightarrow \neg(\neg A \vee \neg B)$$

sa dá ku každému výroku nájsť ekvivalentný výrok, ktorý neobsahuje iné logické spojky ako $\neg$ a $\vee$, alebo ekvivalentný výrok, ktorý obsahuje len spojky $\neg$ a $\wedge$. Teda stačia dve logické spojky.

Vzniká prirodzená otázka, či existuje logická spojka, ktorá jediná stačí na vyjadrenie všetkých logických spojok. Odpoveď je klasicky známa. Logická spojka $A|B$, tak zvaná **Shefferova čiarka**, ktorá sa dá opísať ekvivalenciou

$$A|B \Leftrightarrow \neg(A \wedge B),$$

má požadovanú vlastnosť. Zrejme je $\neg A$ ekvivalentné výroku $A|A$ a $A \vee B$ je ekvivalentné výroku $(A|A)|(B|B)$. Zostrojte pravdivostnú tabuľku pre Shefferovu čiarku a overte uvedené ekvivalencie. Existuje ešte jedna logická operácia s uvedenou vlastnosťou, ktorá sa volá **Peirceova operácia** a je ekvivalentná operácii $\neg(A \vee B)$. Ukážte, že iné binárne spojky s uvedenou vlastnosťou neexistujú (koľko je všetkých možných binárnych logických spojok?).

9 Booleove algebry

Ak na množine B sú dané dve binárne operácie $\wedge$, $\vee$, jedna unárna operácia $-$ a dva špeciálne prvky $0, 1 \in B$, tak štruktúra $\langle B, \wedge, \vee, -, 0, 1\rangle$ sa nazýva **Booleova algebra**, ak platí:

a) operácie $\wedge, \vee$ sú asociatívne, komutatívne a idempotentné, t.j.

$$x \wedge x = x \vee x = x,$$

b) platia distributívne zákony

$$x \wedge (y \vee z) = (x \vee y) \wedge (x \vee z), \qquad x \vee (y \wedge z) = (x \wedge y) \vee (x \wedge z),$$

c) platia de Morganove pravidlá

$$-(x \wedge y) = (-x) \vee (-y), \qquad -(x \vee y) = (-x) \wedge (-y),$$

d) $x \vee 0 = x, \quad x \vee 1 = 1, \quad x \wedge 0 = 0, \quad x \wedge 0 = 0,$

e) $- - x = x, \quad -0 = 1.$

Operácia $\vee$ sa nazýva **spojenie**, operácia $\wedge$ sa nazýva **prienik** a $-$ je **komplement**. Booleovu algebru môžeme čiastočne usporiadať reláciou

$$x \leq y \equiv x \vee y = y.$$

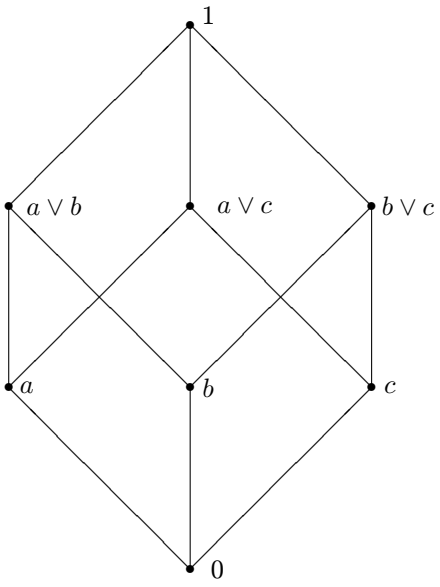
$x < y$ znamená $x \leq y \wedge x \neq y$. Prvok 1 je potom najväčší prvok a prvok 0 je najmenší prvok množiny B.

Booleovu algebru môžeme definovať aj ako čiastočne usporiadanú množinu $B, \leq$ s najmenším a najväčším prvkom 0, 1, každá dvojprvková $\{x, y\} \subseteq B$ množina má supremum $x \vee y$ a infimum $x \wedge y$, platia distributívne zákony b) a pre každý prvok $x \in B$ existuje jeho komplement, t.j. prvok $y \in B$ taký, že $x \vee y = 1$ a $x \wedge y = 0$.

Najjednoduchšia Booleova algebra je dvojprvková $\{0, 1\}$, kde operácie sú definované predpismi $x \vee y = \max\{0, 1\}$, $x \wedge y = \min\{0, 1\}$ a $-0 = 1$.

Príklad 9.1 Nech X je pevná neprázdna množina. Ak $B = \mathcal{P}(X)$ je množina všetkých podmnožín množiny X, spojenie je zjednotenie, prienik je množinový prienik a komplement je komplement v množine X, tak $\langle \mathcal{P}(X), \cap, \cup, \setminus, \emptyset, X \rangle$ je Booleova algebra.

Príklad 9.2 Osemprvková Booleova algebra má takýto Hasseho diagram:



Príklad 9.3 Uvažujme teraz množinu $\mathcal{L}(q_1, \ldots, q_n)$ všetkých výrokov, ktoré možno utvoriť pomocou daných elementárnych výrokov $q_1, \ldots, q_n$. Dva ekvivalentné výroky budeme pokladať za ten istý výrok. Nech prienik dvoch výrokov je ich konjunkcia, spojenie je ich disjunkcia a komplement výtoku je jeho negácia. Potom $\mathcal{L}(q_1, \ldots, q_n)$ (presnejšie, triedy ekvivalentných výrokov) je Booleova algebra s najväčším prvkom tautológia a s najmenším prvkom negácia tautológie. Koľko prvkov má táto Booleova algebra? Podľa vety 8.1 každý výrok je ekvivalentný s výrokom v úplnom disjunktívnom normálnom tvare, v ktorom vystupujú len elementárne výroky $q_1, \ldots, q_n$. Existuje 2^n elementárnych konjunkcií z týchto elementárnych výrokov. Ak výrok je negácia tautológie, tak sme za jeho normálnu formu vzali výrok $q_1 \wedge \neg q_1$. Každý iný výrok je ekvivalentný disjunkcii určitého nenulového počtu elementárnych konjunkcií. Teda všetkých úplných disjunktívnych normálnych tvarov (včítane prvého) je 2^{2^n}.

Prvok $x \in B$ Booleovej algebry sa nazýva **atóm**, ak $x \neq 0$ a neexistuje prvok $y \in B$ taký, že $0 < y < x$. Teda atóm je minimálny prvok množiny $B \setminus \{0\}$. Booleova algebra B sa nazýva **atomická**, ak pre každé $x \in B \setminus \{0\}$ existuje atóm $y \leq x$. Použitím princípu minima sa ľahko vidí, že každá konečná Booleova algebra je atomická. Ak $\langle B, \wedge, \vee, -, 0, 1\rangle$ je konečná Booleova algebra a X je množina jej atómov, tak B je izomorfná Booleovej algebre $\langle \mathcal{P}(X), \cap, \cup, \setminus, \emptyset, X\rangle$.

Príklad 9.4 Elementárna konjunkcia obsahujúca výroky $q_1, \ldots, q_n$ alebo ich negácie je atóm Booleovej algebry $\mathcal{L}(q_1, \ldots, q_n)$. Naopak, každý atóm tejto Booleovej algebry je takáto elementárna konjunkcia. Disjunkcia atómov je prvok tejto Booleovej algebry a každý prvok (ak negáciu tautológie považujeme za prázdnu disjunkciu) má takýto tvar.

Výklad o výrokoch, ktorý sme prezentovali, sa obyčajne nazýva **výrokový počet**. Často sa mu pridáva epiteton **klasický**. Chce sa tým zdôrazniť to, že sme prijali tie tabuľky pravdivostných hodnôt pre jednotlivé logické spojky, ktoré sme prijali a že sme definovali dôkaz (teda hlavne axiómy výrokového počtu a odvodzovacie pravidlo modus ponens) tak, ako sme to urobili. Existujú aj iné neklasické výrokové počty, ktoré sa líšia hlavne inými tabuľkami pravdivostných hodnôt, iným dôkazom a niekedy aj ďalšími logickými spojkami. Najjednoduchšia neklasická logika je viachodnotová logika s hodnotami v Booleovej algebre. Klasická logika je potom jej špeciálny prípad, keď Booleova algebra má len dva prvky.

10 Výroková funkcia

Gramatická veta "Študent čítal knihu." sa síce podobá na výrok, ale nevieme povedať, či je pravdivá alebo nepravdivá. Študent X.Y. čítal Zámok Franza Kafku, ale študent U.V. nečítal Mor Alberta Camusa. Aby sme mohli povedať, či uvedená veta je pravdivá alebo nie, musíme špecifikovať, ktorého študenta a ktorú knihu myslíme. Slovo "študent" v uvedenej vete je "premenná", ktorá nám len oznamuje, že ide o človeka, ktorý študuje na nejakej škole. Podobne,

slovo "kniha" v uvedenej vete je premenná, ktorá oznamuje, že čítanie študenta sa vzťahuje na písomnosť, ktorú nazývame kniha. Z uvedenej vety dostaneme výrok, ak upresníme, ktorého konkrétneho študenta slovo "študent" v tejto vete označuje a ktorú konkrétnu knihu slovo "kniha" v tejto vete označuje. Inými slovami, za premenné "študent" a "kniha" musíme dosadiť konkrétne (dovolené) objekty a dostaneme tak výrok. [9]

Podobným príkladom je veta "Číslo $x \cdot y$ je kladné.", skrátene "$x \cdot y > 0$". Aby sme dostali výrok, musíme za premenné x, y dosadiť konkrétne reálne čísla.

Veta uvedeného typu sa nazýva **výroková funkcia**. Teda, výroková funkcia je veta, v ktorej sa vyskytujú premenné. Keď za tieto premenné dosadíme dovolené konkrétne objekty, dostaneme výrok. Kvôli jednoduchosti aj výrok pokladáme za výrokovú funkciu, ktorá obsahuje nula premenných.

Ešte si vysvetlíme epiteton "dovolené". Určite v prvom príklade za slovo "študent" nemôžeme dosadiť "funkcia sínus". Podobne za slovo "kniha" nemôžeme dosadiť "Dalajláma". Obidva objekty sú síce konkrétne, ale nie sú dovolené. Slovo "študent" nám zreteľne dáva najavo, čo za neho môžeme dosadiť: (meno) človeka, ktorý študuje na nejakej škole. Podobne slovo "kniha" nám dáva dostatočne presnú informáciu o tom, čo môžeme dosadiť. V druhom príklade za premenné x, y môžeme dosadzovať len konkrétne reálne čísla, nie konkrétne priamky a ani knihy.

Výrokovú funkciu, ktorá obsahuje premenné $x_1, \ldots, x_n$ označíme napríklad $\mathcal{V}(x_1, \ldots, x_n)$. Hovoríme tiež, že táto výroková funkcia **závisí** od premenných $x_1, \ldots, x_n$. Ak uvažujeme viac výrokových funkcií súčasne, bolo by vhodné, keby záviseli od tých istých premenných. To dosiahneme tak, že budeme pokladať výrokovú funkciu závislú aj od premennej, od ktorej de facto nezávisí. Takú premennú nazveme **fiktívna**. Teda, ak výroková funkcia $\mathcal{V}$ závisí od premenných $x_1, \ldots, x_n$, tak píšeme $\mathcal{V}(x_1, \ldots, x_n)$. Ak máme ďalšie premenné $y_1, \ldots, y_m$, tak môžeme a budeme písať aj $\mathcal{V}(x_1, \ldots, x_n, y_1, \ldots, y_m)$. Napríklad, výroková funkcia $x \cdot y > 0$ závisí od premenných x, y. Môžeme ju označiť $\mathcal{V}(x, y)$. Ale môžeme zaviesť aj fiktívnu premennú (ak za ňu dosadíme, nič sa nestane!) z a písať $\mathcal{V}(x, y, z)$.

Z výrokových funkcií môžeme utvoriť nové výrokové funkcie pomocou logických spojok rovnako, ako sme z výrokov utvorili nové výroky. Ak máme výrokové funkcie $\mathcal{V}_1(x_1, \ldots, x_n)$ a $\mathcal{V}_2(x_1, \ldots, x_n)$, tak môžeme z nich utvoriť nové výrokové funkcie

$$\mathcal{V}_1(x_1, \ldots, x_n) \vee \mathcal{V}_2(x_1, \ldots, x_n), \qquad \mathcal{V}_1(x_1, \ldots, x_n) \wedge \mathcal{V}_2(x_1, \ldots, x_n),$$

$$\mathcal{V}_1(x_1, \ldots, x_n) \to \mathcal{V}_2(x_1, \ldots, x_n), \qquad \mathcal{V}_1(x_1, \ldots, x_n) \equiv \mathcal{V}_2(x_1, \ldots, x_n),$$

ktoré nazveme podobne ako v prípade výrokov postupne disjunkcia, konjunkcia,

[9] V záujme zrozumiteľnosti a zjednodušenia sa dopúšťame určitej nepresnosti. Za premennú "študent" nedosadzujeme študenta Marcela Mrkvičku (ten v tej chvíli sa môže vyskytovať na inom mieste), dosadzujeme jeho názov, t.j. meno. Podobne je to v prípade premennej "kniha". Nedosadili sme konkrétny výtlačok Camusovho "Moru", ale jeho názov. Podobná situácia bude aj v ostatných prípadoch.

implikácia a ekvivalencia. Samozrejme môžeme utvoriť negáciu

$$\neg\mathcal{V}(x_1,\ldots,x_n).$$

Pre používanie zátvoriek platia rovnaké dohody ako v prípade výrokov.

Existujú aj iné možnosti, ako utvoriť z výrokovej funkcie novú výrokovú funkciu. Môžeme použiť **veľký** alebo **všeobecný kvantifikátor** $\forall$ a **malý** alebo **existenčný kvantifikátor** $\exists$. Ak $\mathcal{V}(x,y_1,\ldots,y_n)$ je výroková funkcia, tak môžeme utvoriť výrokovú funkciu

$$(\forall x)\,\mathcal{V}(x,y_1,\ldots,y_n), \tag{10.13}$$

ktorú čítame "Pre každé x platí $\mathcal{V}(x,y_1,\ldots,y_n)$." Táto výroková funkcia už nezávisí od premennej x. Tú istú výrokovú funkciu môžeme vyjadriť aj vetou "Pre každé u platí $\mathcal{V}(u,y_1,\ldots,y_k)$". Naviac, ak do výrokovej funkcie (10.13) môžeme za premenné $y_1,\ldots,y_k$ dosadiť nejaké konkrétne objekty, za premennú x nemôžeme dosadzovať.

Podobne môžeme utvoriť výrokovú funkciu

$$(\exists x)\,\mathcal{V}(x,y_1,\ldots,y_k), \tag{10.14}$$

ktorú čítame "Existuje x také, že platí $\mathcal{V}(x,y_1,\ldots,y_k)$." Ani táto výroková funkcia nezávisí od premennej x a za túto premennú do výrokovej funkcie (10.14) nemôžeme dosadzovať.

Matematici často šetria písanie a nepíšu zátvorky okolo kvantifikátorov. Je to vec individuálnej dohody, pokiaľ to nevedie k nedorozumeniu (najčastejšie k nejednoznačnosti). Výrokové funkcie (10.13) a (10.14) sa často skrátene píšu napríklad takto:

$$\forall x:\ \mathcal{V}(x,y_1,\ldots,y_k), \qquad \exists x:\ \mathcal{V}(x,y_1,\ldots,y_k).$$

Uvažujme číselný výraz

$$\sum_{i=n}^{m} i^2. \tag{10.15}$$

Tento výraz závisí od čísiel n, m a nezávisí od premennej i. Naviac, za premenné n, m môžeme dosadiť nejaké konkrétne prirodzené (alebo celé) čísla. Za premennú i nemôžeme dosadzovať. Premennú i môžeme vo všetkých jej výskytoch premenovať a výraz sa nezmení:

$$\sum_{i=n}^{m} i^2 = \sum_{j=n}^{m} j^2 = \sum_{\square=n}^{m} \square^2 = \sum_{\heartsuit=n}^{m} \heartsuit^2.$$

Číselný výraz (10.15) vieme opísať aj bez použitia premennej i, napríklad takto: "(10.15) je súčet druhých mocnín čísiel od n po m". Podobne je to aj s premenou x vo výraze

$$\int_a^b x^2\,dx.$$

Hovoríme, že premenná x (v prípade výrazu (10.15) premenná i) je viazaná.

Podobne je to aj s kvantifikátormi. Premenná, ktorá je bezprostredne za kvantifikátorom, je v danej výrokovej funkcii **viazaná**. [10] Premenné, ktoré sa vyskytujú vo výrokovej funkcii a nie sú viazané, sú **voľné**. Kvantifikátor premennú **viaže**, teda mení ju z voľnej na viazanú. Ak viazanú premennú vo všetkých jej výskytoch nahradíme premennou, ktorá sa ešte v danej situácii nevyskytla, tak sa výroková funkcia nezmení. Za viazanú premennú nemôžeme dosadzovať. Výroková funkcia závisí od voľných premenných, nezávisí od viazaných premenných.

Príklad 10.1 Ak nahradíme každý výskyt premennej x premennou z, tak sa daný výraz alebo výroková funkcia nezmení:

$$\int_0^1 x^2\,dx, \qquad \sum_{x=0}^{n} \frac{1}{x^2}, \qquad (\forall x)\, x^2 \geq 0, \qquad (\forall x)(\exists y)\, x + y = a$$

$$\int_0^1 z^2\,dz, \qquad \sum_{z=0}^{n} \frac{1}{z^2}, \qquad (\forall z)\, z^2 \geq 0, \qquad (\forall z)(\exists y)\, z + y = a$$

Naproti tomu dosadenie za viazanú premennú dáva nezmysel:

$$\int_0^1 7^2\,d7, \qquad \sum_{3=0}^{n} \frac{1}{3^2}, \qquad (\forall 1)\, 1^2 \geq 0, \qquad ,(\forall 0)(\exists y)\, 0 + y = a$$

Príklad 10.2 Ak urobíme konjunkciu výrokových funkcií

$$x^2 > 3, \qquad (\forall x)(\exists y)\,(x + y < z)$$

tak vo výrokovej funkcii

$$x^2 > 3 \wedge (\forall x)(\exists y)\,(x + y < z) \tag{10.16}$$

premenná x sa vyskytuje dvojako: pred spojkou $\wedge$ je voľná a po spojke $\wedge$ je viazaná. Môže to spôsobiť nedorozumenie a preto sa takejto kolízii vyhýbame. Podľa potreby viazané premenné najprv premenujeme a až potom utvoríme konjunkciu. Výrokovú funkciu (10.16) môžeme bez kolízie premenných vyjadriť napríklad takto:

$$x^2 > 3 \wedge (\forall u)(\exists y)\,(u + y < z).$$

Všeobecný kvantifikátor $(\forall x)$ často vyjadrujeme slovami: "pre ľubovoľné x", "pre všetky x", "pre akékoľvek x". Ak nasleduje záporná veta, tak slovenčina si vyžaduje vyjadrenie "pre žiadne x".

Existenčný kvantifikátor $(\exists x)$ často vyjadrujeme slovami: "pre nejaké x", "nájde sa také x, že", "aspoň pre jedno x".

[10] Presnejšie, je viazaná vo výrokovej funkcii, pred ktorú sme napísali kvantifikátor. Ak potom urobíme napríklad konjunkciu takejto výrokovej funkcie s inou výrokovou funkciou, tak v tej inej sa môže inkriminovaná premenná vyskytovať voľne. Budeme sa však takejto situácii vyhýbať, pozri príklad 10.2.

Gramaticky správne vyjadrenie všeobecného kvantifikátora v zápornom prípade slovami "pre nijaké x" nie je vhodné, lebo je ľahko zameniteľné so svojím opakom "pre nejaké x". Nie je tam žiadna redundancia informácie[11]!

Ak výroková funkcia začína jedným alebo viacerými veľkými kvantifikátormi za sebou a za nimi nasleduje výroková funkcia bez kvantifikátorov, tak matematici obyčajne tieto kvantifikátory **zamlčia**. Napríklad, ak matematik chce povedať, že "Pre každé x, y, z, ak $x < y$ a $y < z$, tak $x < z$.", tak povie skrátene "Ak $x < y$ a $y < z$, tak $x < z$." Hovoríme tomu **interpretácia všeobecnosti**. Podobne to platí aj pri vyjadrení implikácie alebo ekvivalencie. Ak chceme povedať, že "Výroková funkcia $(\forall x)\,(\mathcal{V}(x) \to \mathcal{W}(x))$ je pravdivá", povieme obyčajne "Platí $\mathcal{V}(x) \to \mathcal{W}(x)$". Podobne pre ekvivalenciu. Nesmieme to urobiť, ak výroková funkcia obsahuje malý kvantifikátor. Mohlo by to viesť k nedorozumeniu.

Matematika často používa kvantifikátory s podmienkou. **Veľký kvantifikátor s podmienkou**

$$(\forall x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$$

je skratka výrokovej funkcie

$$(\forall x)\,(\mathcal{V}(x) \to \mathcal{W}(x, y_1, \ldots, y_k))$$

a **malý kvantifikátor s podmienkou**

$$(\exists x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$$

je skratka výrokovej funkcie

$$(\exists x)\,(\mathcal{V}(x) \wedge \mathcal{W}(x, y_1, \ldots, y_k)).$$

Príklad 10.3 Definícia limity postupnosti, by mala byť formulovaná takto:

$$\lim_{n\to\infty} a_n = a \text{ ak } (\forall \varepsilon)\,(\varepsilon > 0 \to (\exists n_0)(\forall n)\,(n > n_0 \to |a_n - a| < \varepsilon)).$$

Táto neprehľadná forma sa dá prehľadnejšie napísať pomocou kvantifikátorov s podmienkou takto:

$$\lim_{n\to\infty} a_n = a \text{ ak } (\forall \varepsilon, \varepsilon > 0)(\exists n_0)(\forall n, n > n_0)\,(|a_n - a| < \varepsilon).$$

Matematici to napíšu spravidla ešte jednoduchšie

$$\lim_{n\to\infty} a_n = a \text{ ak } (\forall \varepsilon > 0)(\exists n_0)(\forall n > n_0)\,(|a_n - a| < \varepsilon).$$

Podobne, ako v prípade výrokov, existujú výrokové funkcie, ktoré sú pravdivé vďaka svojmu tvaru pre ľubovoľné hodnoty premenných. Najjednoduchšími

[11] Redundancia znamená nadbytočnosť, ktorá je potrebná k tomu, aby sme si mohli pri šume – nedobrom vyslovení alebo zlom počutí – domyslieť správnu informáciu.

príkladmi takýchto výrokových funkcií sú výrokové funkcie, ktoré vznikli z výrokov – tautológií, napríklad

$$(\mathcal{V}_1(x) \to \mathcal{V}_3(x)) \to ((\mathcal{V}_2(x) \to \mathcal{V}_3(x)) \to ((\mathcal{V}_1(x) \vee \mathcal{V}_2(x)) \to \mathcal{V}_3(x))).$$

Existujú aj iné výrokové funkcie, ktoré sú takto pravdivé, napríklad

$$(\forall x)\,\mathcal{V}(x) \to \mathcal{V}(y), \quad \neg(\forall x)\,\mathcal{V}(x) \equiv (\exists x)\,\neg\mathcal{V}(x), \quad \neg(\exists x)\,\mathcal{V}(x) \equiv (\forall x)\,\neg\mathcal{V}(x).$$

Budeme hovoriť, že takéto výrokové funkcie sú **logicky pravdivé**. Podobne ako v prípade výrokov, budeme hovoriť, že výrokové funkcie $\mathcal{V}$ a $\mathcal{W}$ sú **ekvivalentné**, ak výroková funkcia $\mathcal{V} \equiv \mathcal{W}$ je logicky pravdivá.

Negácia výrokovej funkcie

$$\neg(\forall x)\,\mathcal{V}(x, y_1, \ldots, y_k)$$

je ekvivalentná výrokovej funkcii

$$(\exists x)\,\neg\mathcal{V}(x, y_1, \ldots, y_k).$$

Podobne, negácia výrokovej funkcie

$$\neg(\exists x)\,\mathcal{V}(x, y_1, \ldots, y_k)$$

je ekvivalentná výrokovej funkcii

$$(\forall x)\,\neg\mathcal{V}(x, y_1, \ldots, y_k).$$

Teda výroková funkcia

$$\neg(\forall x)(\exists y)(\exists u)(\forall v)\,\mathcal{V}(x, y, u, v)$$

je ekvivalentná výrokovej funkcii

$$(\exists x)(\forall y)(\forall u)(\exists v)\,\neg\mathcal{V}(x, y, u, v).$$

Ľahko sa overí, že negácie výrokových funkcií začínajúcich kvantifikátorom s podmienkou

$$(\forall x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k), \qquad (\exists x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$$

sú postupne ekvivalentné

$$(\exists x, \mathcal{V}(x))\,\neg\mathcal{W}(x, y_1, \ldots, y_k), \qquad (\forall x, \mathcal{V}(x))\,\neg\mathcal{W}(x, y_1, \ldots, y_k).$$

Napríklad, výroková funkcia $(\forall x, \mathcal{V}(x))\,\mathcal{W}(x, y_1, \ldots, y_k)$ s kvantifikátorom s podmienkou je skratkou pre výrok $(\forall x)\,(\mathcal{V}(x) \to \mathcal{W}(x, y_1, \ldots, y_k))$. Negáciou tejto výrokovej funkcie je výroková funkcia $(\exists x)\,\neg(\mathcal{V}(x) \to \mathcal{W}(x, y_1, \ldots, y_k))$. Negácia implikácie je ekvivalentná výrokovej funkcii $\mathcal{V}(x) \wedge \neg\mathcal{W}(x, y_1, \ldots, y_k))$, teda skúmaná negácia je ekvivalentná výrokovej funkcii $(\exists x)\,(\mathcal{V}(x) \wedge \neg\mathcal{W}(x, y_1, \ldots, y_k))$. My sme sa dohodli, že túto výrokovú funkciu skrátene označíme

$$(\exists x, \mathcal{V}(x))\,\neg\mathcal{W}(x, y_1, \ldots, y_k).$$

Podobne by sme postupovali pre negovanie malého kvantifikátora s podmienkou. Teda, kvantifikátory s podmienkou negujeme rovnako, ako kvantifikátory bez podmienky.

Príklad 10.4 Výroková funkcia $\neg(\lim_{n\to\infty} a_n = a)$ je ekvivalentná výrokovej funkcii

$$(\exists\varepsilon > 0)(\forall n_0)(\exists n > n_0)\,(|a_n - a| \geq \varepsilon).$$

11 Formula

Aby sme získali základné výsledky výrokového počtu, museli sme pojem výroku formalizovať. Dohodli sme sa, že máme nejaké elementárne výroky a uvažovali sme len výroky utvorené z týchto elementárnych výrokov. Podobne budeme postupovať aj v prípade výrokových funkcií. V tomto prípade je však štruktúra zložitejšia.

Výroková funkcia závisí od nejakých premenných, za ktoré môžeme dosadzovať dovolené objekty. Dá sa ľahko dosiahnuť to, že za všetky premenné vo výrokovej funkcii môžeme dosadzovať tie isté dovolené objekty, inými slovami, dovolené objekty sú spoločné pre všetky premenné. Obyčajne je daná množina a dovolené objekty sú prvky tejto množiny. Napríklad, ak výroková funkcia závisí od prirodzených čísiel, tak dovolené objekty sú prvky množiny $\mathbb{N}$ všetkých prirodzených čísiel. Alebo, ak výroková funkcia závisí od reálnych čísiel, tak dovolené objekty sú prvky množiny $\mathbb{R}$. Pre výrokovú funkciu "Študent čítal knihu" sú dvojaké dovolené objekty. Formálne to môžeme vyriešiť tak (a to sa obyčajne tak aj robí), že za množinu dovolených objektov považujeme množinu všetkých študentov a všetkých kníh. Ak na prvom mieste dosadíme názov knihy alebo na druhom mieste dosadíme meno študenta, tak sa dohodneme, že dostaneme nepravdivý výrok, napr. "Študent Camusov Mor čítal Marcela Mrkvičku." je nepravdivý výrok.

Podobne, ako sme utvorili výroky z elementárnych výrokov pomocou logických spojok, výrokové funkcie vytvoríme pomocou logických spojok a kvantifikátorov z nejakých elementárnych výrokových funkcií. Ak sa pozrieme na štruktúru niektorých najjednoduchších výrokových funkcií o prirodzených alebo reálnych číslach, tak zistíme, že úlohu elementárnych výrokov hrajú výrokové funkcie tvaru $t_1 = t_2$, $t_1 < t_2$, kde t_1, t_2 by sme mohli nazvať číselné výrazy. Napríklad, výroková funkcia "Číslo n je prvočíslo" sa dá napísať takto:

$$(\forall m)(((\exists k)\, k \cdot m = n) \to (m = 1 \vee m = n)).$$

Výroková funkcia "Ak $x > y > 0$ tak $\sqrt{x} > \sqrt{y}$" sa dá napísať ako

$$((x > y \wedge y > 0) \to (\forall u)(\forall v)\,((u > 0 \wedge v > 0 \wedge u^2 = x \wedge v^2 = y) \to u > v).$$

Vystupujú v nich číselné výrazy m, n, 1, $k \cdot m$, x, y, 0, u, v, u^2, v^2. Ako sme utvorili číselný výraz? Začali sme s premennými alebo konkrétnymi reálnymi (alebo prirodzenými) číslami a postupne sme požili operácie sčítania, násobenia a podobne. Operácia druhej odmocniny je problematická, lebo je definovaná len pre nezáporné reálne čísla. To bol dôvod, prečo sme výrokovú funkciu "Ak $x > y > 0$ tak $\sqrt{x} > \sqrt{y}$" prepisovali do tvaru bez použitia druhej odmocniny.

Ukazuje sa, že toto je naozaj typická štruktúra elementárnych výrokov: do nejakej základnej výrokovej funkcie dosadíme "číselné výrazy". Táto predbežná

analýza situácie sa stane základom pre formalizáciu teórie výrokových funkcií. Táto teória sa nazýva **predikátový počet**.[12]

Najprv predstavíme **jazyk** predikátového počtu. Jazyk bude obsahovať nasledujúce znaky:

premenné:	$\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$, ... , $\mathbf{x}_n$, ...
logické spojky"	$\neg$, $\wedge$, $\vee$, $\rightarrow$, $\equiv$,
kvantifikátory"	$\forall$, $\exists$,
zátvorky:	(,),
predikáty:	$\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$, ...
individuálne konštanty:	$\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, ...
názvy operácií:	$\mathbf{f}$, $\mathbf{g}$, $\mathbf{h}$, ...

U každého predikátu a názvu operácie je udaná **árnosť**, t.j. počet miest, do ktorých sa dosadzuje. Konkrétny jazyk sa bude prispôsobovať situácii, ktorú chceme skúmať. Znaky uvedené v prvých štyroch riadkoch sú povinné: bude ich obsahovať každý jazyk a nebudeme ich explicitne uvádzať. Preto budeme písať

$$\mathcal{L} = \{\mathbf{P}, \mathbf{Q}, \mathbf{R}, \ldots, \mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots, \mathbf{f}, \mathbf{g}, \mathbf{h}, \ldots\}.$$

Budeme predpokladať, že jazyk obsahuje aspoň jeden predikát. Budeme mať jazyky bez individuálnych konštánt a/alebo názvov operácií. Samotné označenie chce naznačiť, že premenných máme vždy nekonečne mnoho, zatiaľ čo ostatných nemusí byť nekonečne mnoho. Dokonca mnohokrát ich bude len niekoľko málo. Kvôli jednoduchosti budeme používať na označenie premenných aj znaky $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, $\mathbf{u}$, $\mathbf{v}$, ...

Uvedené znaky jazyka predikátového počtu budú niečo označovať. Prezradíme dopredu, že čo. Premenná označuje bližšie neurčený prvok množiny M dovolených objektov. Predikát je nástroj na výrobu relácie na množine dovolených objektov. Árnosť predikátu určuje árnosť relácie. Individuálna konštanta označuje konkrétny prvok množiny dovolených objektov. Konečne názov k-árnej operácie označuje k-árnu operáciu na množine M, t.j. zobrazenie z M^k do M.

Príklad 11.1 Jazyk $\mathcal{L}_{okruh}$ pre teóriu okruhov okrem povinných znakov bude obsahovať binárny predikát $\underset{\smile}{=}$, dve individuálne konštanty $\mathbf{0}$, $\mathbf{1}$ a tri názvy binárnych operácií $\underset{\smile}{+}$, $\underset{\smile}{-}$, $\underset{\smile}{\cdot}$. Teda

$$\mathcal{L}_{okruh} = \{\underset{\smile}{=}, \mathbf{0}, \mathbf{1}, \underset{\smile}{+}, \underset{\smile}{-}, \underset{\smile}{\cdot}\}.$$

Jazyk pre teóriu grúp obsahuje jeden binárny predikát $\underset{\smile}{=}$, jednu individuálnu konštantu $\mathbf{e}$ a jeden názov binárnej operácie $\underset{\smile}{\circ}$:

$$\mathcal{L}_{grupa} = \{\underset{\smile}{=}, \underset{\smile}{\circ}, \mathbf{e}\}.$$

[12] Niekedy sa zdôrazňuje, že predikátový počet prvého rádu, lebo poznáme aj predikátové počty vyšších rádov.

Jazyk pre teóriu grafov bude mať dva binárne predikáty $\underset{\smile}{=}$, $\mathbf{H}$ a žiadne individuálne konštanty ani názvy operácií.

Potrebujeme pojem, ktorý bude predstavovať niečo ako názov "číselného výrazu". Tento pojem sa nazýva **term**. Definícia termu (indukciou) je nasledujúca:

t1) každá premenná je term,

t2) každá individuálna konštanta je term,

t3) ak $\mathbf{t}_1, \ldots, \mathbf{t}_k$ sú termy, $\mathbf{f}$ je názov k-árnej operácie, tak $\mathbf{f}(\mathbf{t}_1, \ldots, \mathbf{t}_k)$ je term.

Prenechávame na čitateľa, aby podľa vzoru definície výroku, túto definíciu upresnil zavedením pojmu **vytvárajúca postupnosť termu**. Potom slovo v jazyku predikátového počtu je term, ak existuje vytvárajúca postupnosť termu taká, že toto slovo je jej posledný člen. Term **závisí** od premenných, ktoré sa v ňom vyskytujú, alebo inými slovami, ktoré sme potrebovali na jeho vytvorenie.

Príklad 11.2 Ak $\mathbf{t}_1$, $\mathbf{t}_2$ sú termy v jazyku teórie okruhov $\mathcal{L}_{okruh}$, tak termy $\underset{\smile}{+}(\mathbf{t}_1, \mathbf{t}_2)$, $\underset{\smile}{-}(\mathbf{t}_1, \mathbf{t}_2)$, $\underset{\smile}{\cdot}(\mathbf{t}_1, \mathbf{t}_2)$, budeme písať $(\mathbf{t}_1 \underset{\smile}{+} \mathbf{t}_2)$, $(\mathbf{t}_1 \underset{\smile}{-} \mathbf{t}_2)$, $(\mathbf{t}_1 \underset{\smile}{\cdot} \mathbf{t}_2)$. Vonkajšie zátvorky obyčajne nepíšeme. Rovnako postupujeme aj v prípade podobných jazykov.

Nasledujúce slová sú termy v tomto jazyku:

$$(\mathbf{x} \underset{\smile}{\cdot} \mathbf{x}) + (\mathbf{y} \underset{\smile}{\cdot} \mathbf{y}),\ ((\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} \mathbf{x}) \underset{\smile}{+} \mathbf{z},\ ((\mathbf{x} \underset{\smile}{\cdot} \mathbf{x}) \underset{\smile}{-} ((\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} (\mathbf{x} \underset{\smile}{\cdot} \mathbf{y}))) \underset{\smile}{+} (\mathbf{y} \underset{\smile}{\cdot} \mathbf{y}).$$

Ich vytvárajúce postupnosti sú nasledujúce postupnosti

$$\mathbf{x},\ \mathbf{x} \underset{\smile}{\cdot} \mathbf{x},\ \mathbf{y},\ \mathbf{y} \underset{\smile}{\cdot} \mathbf{y},\ (\mathbf{x} \underset{\smile}{\cdot} \mathbf{x}) \underset{\smile}{+} (\mathbf{y} \underset{\smile}{\cdot} \mathbf{y});$$

$$\mathbf{x},\ \mathbf{z},\ \mathbf{1},\ \mathbf{1} \underset{\smile}{+} \mathbf{1},\ (\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} \mathbf{x},\ ((\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} \mathbf{x}) \underset{\smile}{+} \mathbf{z};$$

$$\mathbf{x},\ \mathbf{x} \underset{\smile}{\cdot} \mathbf{x},\ \mathbf{y},\ \mathbf{1},\ \mathbf{1} \underset{\smile}{+} \mathbf{1},\ \mathbf{x} \underset{\smile}{\cdot} \mathbf{y},\ (\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} (\mathbf{x} \underset{\smile}{\cdot} \mathbf{y}),\ (\mathbf{x} \underset{\smile}{\cdot} \mathbf{x}) \underset{\smile}{-} ((\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} (\mathbf{x} \underset{\smile}{\cdot} \mathbf{y})),$$

$$\mathbf{y} \underset{\smile}{\cdot} \mathbf{y},\ ((\mathbf{x} \underset{\smile}{\cdot} \mathbf{x}) \underset{\smile}{-} ((\mathbf{1} \underset{\smile}{+} \mathbf{1}) \underset{\smile}{\cdot} (\mathbf{x} \underset{\smile}{\cdot} \mathbf{y}))) \underset{\smile}{+} (\mathbf{y} \underset{\smile}{\cdot} \mathbf{y}).$$

Prvý a tretí term závisí od premenných $\mathbf{x}$, $\mathbf{y}$ a druhý od premenných $\mathbf{x}$, $\mathbf{z}$.

V jazyku pre teóriu grafov jediné termy sú premenné.

Môžeme pristúpiť k definícii ďalšieho dôležitého pojmu – k pojmu formula, ktorá je formalizáciou pojmu "výroková funkcia". Ak $\mathbf{t}_1, \ldots, \mathbf{t}_k$ sú termy a $\mathbf{P}$ je k–árny predikát, tak $\mathbf{P}(\mathbf{t}_1, \ldots, \mathbf{t}_k)$ je **atomická formula**. Pojem **formula** definujeme indukciou nasledovne:

f1) každá atomická formula je formula,

f2) ak φ je formula, tak $\neg\varphi$ je formula,

f3) ak φ_1, φ_2 sú formuly, tak $(\varphi_1 \square \varphi_2)$ je formula, $\square = \wedge, \vee, \rightarrow, \equiv$,

f4) ak φ je formula, tak $(\mathbf{Q}\mathbf{x})\,\varphi$ je formula, kde $\mathbf{Q} = \forall, \exists$ a $\mathbf{x}$ je premenná.

Mohli by sme podať formálnu zložitú definíciu pojmu "premenná je voľná" a "premenná je viazaná" v danej formule. Zhruba povedané: atomická formula

obsahuje voľné premenné, od ktorých závisia termy, ktoré sa v nej vyskytujú. Kvantifikátor mení voľnú premennú na viazanú. Predpokladáme, že intuitívne vysvetlenie tohoto pojmu bolo dostatočné a tento pojem nemusíme podrobne definovať. Prijmeme rovnaké konvencie o voľných a viazaných premenných vo formulách, aké sme robili v prípade výrokových funkcií.

Príklad 11.3 Ak $\mathbf{t}_1$, $\mathbf{t}_2$ sú termy v jazyku teórie okruhov $\mathcal{L}_{okruh}$, tak atomickú formulu $=(\mathbf{t}_1, \mathbf{t}_2)$ budeme písať $(\mathbf{t}_1 = \mathbf{t}_2)$. Vonkajšie zátvorky obyčajne nepíšeme. Rovnako postupujeme aj v prípade podobných jazykov.

Nasledujúce slová sú atomické formuly v tomto jazyku:

$$((\mathbf{x} \dot{\cdot} \mathbf{x}) \dot{+} (\mathbf{y} \dot{\cdot} \mathbf{y})) \dot{=} (\mathbf{1} \dot{+} \mathbf{1}),\ (((\mathbf{x} \dot{\cdot} \mathbf{x}) \dot{-} ((\mathbf{1} \dot{+} \mathbf{1}) \dot{\cdot} (\mathbf{x} \dot{\cdot} \mathbf{y}))) \dot{+} (\mathbf{y} \dot{\cdot} \mathbf{y})) \dot{=} \mathbf{0}.$$

Tieto atomické formuly obsahujú voľné premenné $\mathbf{x}$, y.

Nasledujúce slovo je formula tohoto jazyka:

$$(\exists \mathbf{x})\,(((\mathbf{x} \dot{\cdot} \mathbf{x}) \dot{+} (\mathbf{y} \dot{\cdot} \mathbf{y})) \dot{=} (\mathbf{1} \dot{+} \mathbf{1})).$$

Premenná $\mathbf{x}$ je viazaná a premenná $\mathbf{y}$ je voľná v tejto formule.

Ak φ je formula, tak zápis $\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ znamená, že φ neobsahuje iné voľné premenné ako $\mathbf{x}_1, \ldots, \mathbf{x}_n$. Dohody o fiktívnych premenných sú rovnaké, ako v prípade výrokových funkcií. Formula, ktorá neobsahuje žiadnu voľnú premennú, sa nazýva **uzavretá**. Ak formula φ obsahuje voľné premenné (a žiadne iné) $\mathbf{x}_1, \ldots, \mathbf{x}_n$, tak formulu

$$(\forall \mathbf{x}_1) \ldots (\forall \mathbf{x}_n)\, \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$$

budeme značiť jednoducho $(\forall \ldots)\, \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ alebo jednoducho $(\forall \ldots)\, \varphi$ a budeme ju nazývať **univerzálny uzáver formuly** φ. Univerzálny uzáver formuly je uzavretá formula.

Predpokladali sme, že v každom jazyku $\mathcal{L}$ je aspoň jeden predikát. Nech je to k-árny predikát $\mathbf{P}$. Potom

$$(\forall \mathbf{x}_1) \ldots (\forall \mathbf{x}_k)\, \mathbf{P}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$$

je uzavretá formula jazyka $\mathcal{L}$. Teda, v každom jazyku existuje aspoň jedna uzavretá formula.

Kvantifikátor s podmienkou definujeme podobne ako pre výrokové funkcie. Ak $\psi(\mathbf{x})$, φ sú formuly, tak formuly s kvantifikátorom s podmienkou

$$(\forall \mathbf{x},\, \psi(\mathbf{x}))\, \varphi, \qquad (\exists \mathbf{x},\, \psi(\mathbf{x}))\, \varphi$$

sú skratkou pre formuly

$$(\forall \mathbf{x})\, (\psi(\mathbf{x}) \to \varphi), \qquad (\exists \mathbf{x})\, (\psi(\mathbf{x})) \wedge \varphi).$$

12 Interpretácia jazyka

Teraz opíšeme postup opačný k formalizácii. Uvažujme jazyk predikátového počtu

$$\mathcal{L} = \{\mathbf{P}, \ldots, \mathbf{a}, \ldots, \mathbf{f}, \ldots\}.$$

Štruktúra[13]

$$\mathfrak{M} = \langle M, P, \ldots, a, \ldots, f, \ldots\rangle$$

sa nazýva **interpretácia jazyka** $\mathcal{L}$, ak platí:

1) M je neprázdna množina,

2) ak $\mathbf{P}$ je k–árny predikát, tak P je k–árna relácia na množine M, t.j. $P \subseteq M^k$,

3) $a \in M$,

4) ak $\mathbf{f}$ je názov k–árnej operácie, tak f je k–árna operácia na množine M, t.j. $f : M^k \longrightarrow M$.

Teda povieme, čo označujú premenné: prvky množiny M. Z predikátu $\mathbf{P}$ sa stane elementárna výroková funkcia $[x_1, \ldots, x_k] \in P$. Individuálna konštanta označuje pevný prvok a množiny M. Konečne, $\mathbf{f}$ je názov k–árnej operácie $f : M^k \longrightarrow M$.

Príklad 12.1 Štruktúra

$$\mathfrak{R} = \langle \mathbb{R}, =, 0, 1, +, -, \cdot\rangle$$

je interpretácia jazyka $\mathcal{L}_{okruh}$. Iné interpretácie toho istého jazyka sú

$$\mathfrak{Q} = \langle \mathbb{Q}, =, 0, 1, +, -, \cdot\rangle, \qquad \mathfrak{N} = \langle \mathbb{N}, =, 0, 1, +, -, \cdot\rangle.$$

Môžeme zostrojiť aj neprirodzenú interpretáciu tohoto jazyka

$$\mathfrak{R}^\star = \langle \mathbb{R}, =, 0, 1, \cdot, +, -\rangle$$

Čitateľ iste pozná aj ďalšiu interpretáciu jazyka $\mathcal{L}_{okruh}$. Nech $p > 1$ je pevné prirodzené číslo. Potom štruktúra

$$\mathfrak{Z}_p = \langle \mathbb{Z}, \equiv \bmod p, 0, 1, +, -, \cdot\rangle$$

je interpretácia tohoto jazyka.

Jazyk $\mathcal{L}_{grupa}$ má napríklad tieto interpretácie

$$\mathcal{G}_1 = \langle \mathbb{R}, =, +, 0\rangle, \qquad \mathcal{G}_2 = \langle \mathbb{R} \setminus \{0\}, =, \cdot, 1\rangle$$
$$\mathcal{G}_3 = \langle \mathbb{Z}, \equiv \bmod p, +, 0\rangle \qquad \mathcal{G}_4 = \langle \{1, \ldots, p\}, \equiv \bmod p, \cdot, 1\rangle$$

V interpretácii sa z formuly "stane" výroková funkcia. Najprv však musíme povedať, čo sa stane z termu.

[13] Ak čitateľ nevie, čo je to štruktúra, tak pre naše účely stačí náš opis. Je to postupnosť uvedených objektov.

Nech Prem je množina premenných jazyka predikátového počtu

$$\text{Prem} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n, \ldots\}.$$

Nech

$$\mathfrak{M} = \langle M, P, \ldots, a, \ldots, f, \ldots\rangle$$

je interpretácia jazyka predikátového počtu

$$\mathcal{L} = \{\mathbf{P}, \ldots, \mathbf{a}, \ldots, \mathbf{f}, \ldots\}.$$

a $v : \text{Prem} \longrightarrow M$ je **ohodnotenie** premenných v tejto interpretácii. Indukciou definujeme $v(\mathbf{t}) \in M$ pre každý term $\mathbf{t}$ jazyka $\mathcal{L}$. Ak $\mathbf{x}$ je premenná, tak $v(\mathbf{x})$ je už definované. Ak $\mathbf{a}$ je individuálna konštanta, tak položíme $v(\mathbf{a}) = a$. Konečne nech $\mathbf{t} = \mathbf{f}(\mathbf{t}_1, \ldots, \mathbf{t}_k)$, kde $\mathbf{t}_1, \ldots, \mathbf{t}_k$ sú termy, pre ktoré hodnoty $v(\mathbf{t}_1), \ldots, v(\mathbf{t}_1)$ sú už definované a $\mathbf{f}$ je názov k-árnej operácie. Položíme

$$v(\mathbf{f}(\mathbf{t}_1, \ldots, \mathbf{t}_1)) = f(v(\mathbf{t}_1), \ldots, v(\mathbf{t}_1)).$$

Musíme dávať pozor na jednu skutočnosť. Hodnota termu $v(\mathbf{t})$ nezávisí len od ohodnotenia v (a teda od množiny M), ale od celej interpretácie $\mathfrak{M}$. V zápise $v(\mathbf{t})$ to nie je zachytené.

Príklad 12.2 Uvažujme interpretáciu $\mathfrak{Q}$ jazyka $\mathcal{L}_{okruh}$. Nech ohodnotenie premenných $v : \text{Prem} \longrightarrow \mathbb{Q}$ je také, že $v(\mathbf{x}) = 4$, $v(\mathbf{y}) = -3$ a $v(\mathbf{z}) = 2$. Potom hodnota termu

$$\mathbf{t} = \mathbf{x} \mathbin{\underset{\smile}{+}} (\mathbf{y} \mathbin{\underset{\smile}{\cdot}} (\mathbf{z} \mathbin{\underset{\smile}{+}} \mathbf{1}))$$

v tomto ohodnotení je

$$v(\mathbf{x} \mathbin{\underset{\smile}{+}} (\mathbf{y} \mathbin{\underset{\smile}{\cdot}} (\mathbf{z} \mathbin{\underset{\smile}{+}} \mathbf{1}))) = 4 + (-3 \cdot (2 + 1)) = -5.$$

Ak však uvažujeme interpretáciu $\mathfrak{R}^\star$ tak pri ohodnotení $v : \text{Prem} \longrightarrow \mathbb{R}$, ktoré nadobúda tie isté hodnoty v premenných $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, tento term má hodnotu

$$v(\mathbf{t}) = 4 \cdot (-3 - (2 \cdot 1)) = -20.$$

V danej interpretácii $\mathfrak{M}$ jazyka $\mathcal{L}$ sa z formuly $\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ stane výroková funkcia, ktorú na chvíľu označíme (píšeme úvodzovky, lebo podobná formula bez úvodzoviek bude v budúcnosti označovať niečo iné):

$$\text{"}\mathfrak{M} \models \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)\text{"}. \tag{12.17}$$

Pri danom ohodnotení premenných sa táto výroková funkcia zmení na výrok, ktorý je pravdivý alebo nepravdivý. Indukciou podľa štruktúry formúl to definujeme.

Uvažujme teda jazyk $\mathcal{L}$, jeho interpretáciu $\mathfrak{M}$ a ohodnotenie premenných $v : \text{Prem} \longrightarrow M$. Indukciou definujeme vzťah

$$\mathfrak{M} \models_v \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n).$$

Nech $\mathbf{P}$ je n-árny predikát, $\mathbf{t}_1, \ldots, \mathbf{t}_n$ sú termy. Potom

$$\mathfrak{M} \models_v \mathbf{P}(\mathbf{t}_1, \ldots, \mathbf{t}_n) \text{ vtedy a len vtedy, keď } [v(\mathbf{t}_1), \ldots, v(\mathbf{t}_n)] \in P.$$

Ak φ, φ_1, φ_2 sú formuly, tak definujeme

$$\mathfrak{M} \models_v \neg\varphi \text{ vtedy a len vtedy, keď neplatí } \mathfrak{M} \models_v \varphi,$$

$$\mathfrak{M} \models_v (\varphi_1 \wedge \varphi_2) \text{ vtedy a len vtedy, keď } \mathfrak{M} \models_v \varphi_1 \text{ a } \mathfrak{M} \models_v \varphi_2,$$

$$\mathfrak{M} \models_v (\varphi_1 \vee \varphi_2) \text{ vtedy a len vtedy, keď } \mathfrak{M} \models_v \varphi_1 \text{ alebo } \mathfrak{M} \models_v \varphi_2.$$

$$\mathfrak{M} \models_v (\varphi_1 \to \varphi_2) \text{ vtedy a len vtedy, keď z } \mathfrak{M} \models_v \varphi_1 \text{ vyplýva } \mathfrak{M} \models_v \varphi_2.$$

Podobne definujeme pre ekvivalenciu. O niečo zložitejšia je definícia pre kvantifikátory:

$\mathfrak{M} \models_v (\forall \mathbf{x})\, \varphi$ vtedy a len vtedy, ak pre každé ohodnotenie premenných w také, že $w(\mathbf{y}) = v(\mathbf{y})$ pre každú premennú $\mathbf{y}$ rôznu od $\mathbf{x}$, platí $\mathfrak{M} \models_w \varphi$.

Podobne pre malý kvantifikátor

$\mathfrak{M} \models_v (\exists \mathbf{x})\, \varphi$ vtedy a len vtedy, ak existuje ohodnotenie premenných w také, že $w(\mathbf{y}) = v(\mathbf{y})$ pre každú premennú $\mathbf{y}$ rôznu od $\mathbf{x}$, a platí $\mathfrak{M} \models_w \varphi$.

Preformulujeme poslednú definíciu. $\mathfrak{M} \models_v (\exists \mathbf{x})\, \varphi$ práve vtedy, keď existuje také $x \in M$, že $\mathfrak{M} \models_w \varphi$, kde ohodnotenie w je rovnaké ako ohodnotenie v, okrem hodnoty $w(\mathbf{x}) = x$.

Príklad 12.3 Uvažujme jazyk $\mathcal{L}_{okruh}$ a jeho interpretáciu $\mathfrak{R}$. Ak v je ohodnotenie premenných, tak $\mathfrak{R} \models_v \mathbf{x} \dot{\cdot} \mathbf{x} \dot{=} \mathbf{y}$ práve vtedy, keď $v(\mathbf{x})^2 = v(\mathbf{y})$. Ak $v(\mathbf{y}) \geq 0$, tak

$$\mathfrak{R} \models_v (\exists \mathbf{x})\, \mathbf{x} \dot{\cdot} \mathbf{x} \dot{=} \mathbf{y};$$

stačí položiť $w(\mathbf{z}) = v(\mathbf{z})$ pre $\mathbf{z}$ rôzne od $\mathbf{x}$ a $w(\mathbf{x}) = \sqrt{v(\mathbf{y})}$.

Ak uvažujeme interpretáciu $\mathfrak{Q}$ a ohodnotenie premenných v je také, že $v(\mathbf{y}) = 2$, tak $\mathfrak{Q} \models_v (\exists \mathbf{x})\, \mathbf{x} \dot{\cdot} \mathbf{x} \dot{=} \mathbf{y}$ podľa definície znamená, že existuje také ohodnotenie premenných w, že (okrem iného) $w(\mathbf{y}) = v(\mathbf{y}) = 2$ a $(w(\mathbf{x}))^2 = v(\mathbf{y}) = 2$. Hodnoty ohodnotenia w majú byť racionálne čísla a teda také ohodnotenie neexistuje. Takže dostávame

$$\mathfrak{Q} \models_v \neg(\exists \mathbf{x})\, \mathbf{x} \dot{\cdot} \mathbf{x} \dot{=} \mathbf{y}.$$

Nech $\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ je formula, ktorá obsahuje len vyznačené voľné premenné. Pozorným prezretím definície možno ľahko zistiť, že pravdivosť vzťahu

$$\mathfrak{M} \models_v \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n)$$

závisí len od hodnôt ohodnotenia v v premenných $\mathbf{x}_1, \ldots, \mathbf{x}_n$. Inými slovami, ak w je také ohodnotenie premenných, že $w(\mathbf{x}_1) = v(\mathbf{x}_1)$, ... , $w(\mathbf{x}_n) = v(\mathbf{x}_n)$, tak

$$\mathfrak{M} \models_v \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n) \text{ práve vtedy, keď } \mathfrak{M} \models_w \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_n).$$

Špeciálne, ak φ je uzavretá formula, tak vzťah $\mathfrak{M} \models_v \varphi$ nezávisí od ohodnotenie premenných v, t.j. je buď pravdivý pre všetky ohodnotenia v alebo nepravdivý pre všetky ohodnotenia v. V prvom prípade budeme jednoducho písať

$$\mathfrak{M} \models \varphi$$

a hovoriť, že formula φ **platí v interpretácii** $\mathfrak{M}$. V súlade s dohodami o zamlčaní veľkého kvantifikátora, v prípade neuzavretej formuly φ budeme písať

$$\mathfrak{M} \models \varphi,$$

ak

$$\mathfrak{M} \models (\forall \ldots)\, \varphi.$$

To bol dôvod, prečo sme v (12.17) písali úvodzovky.

Nech $A(q_1, \ldots, q_n)$ je výrok utvorený z elementárnych výrokov $q_1, \ldots, q_n$ a $\varphi_1, \ldots, \varphi_n$ sú formuly v jazyku $\mathcal{L}$. Nech $\mathfrak{M}$ je interpretácia jazyka $\mathcal{L}$ a v je ohodnotenie premenných. Indukciou podľa vytvárajúcej postupnosti výroku A z definície vzťahu $\models_v$ bezprostredne vyplýva, že

$$\mathfrak{M} \models_v A(q_1/\varphi_1, \ldots, q_n/\varphi_n) \text{ vtedy a len vtedy, keď platí výrok}$$

$$A(q_1/\mathfrak{M} \models_v \varphi_1, \ldots, q_n/\mathfrak{M} \models_v \varphi_n).$$

Špeciálne, ak výrok A je tautológia, tak pre ľubovoľné ohodnotenie v platí

$$A(q_1/\mathfrak{M} \models_v \varphi_1, \ldots, q_n/\mathfrak{M} \models_v \varphi_n)$$

a teda pre ľubovoľnú interpretáciu $\mathfrak{M}$ jazyka $\mathcal{L}$ platí

$$\mathfrak{M} \models A(q_1/\varphi_1, \ldots, q_n/\varphi_n).$$

Príklad 12.4 Výrok $A(p, q) = (p \to (q \to (p \wedge q)))$ je tautológia. Ak φ, ψ sú ľubovoľné formuly v jazyku $\mathcal{L}$, tak $A(p/\varphi, q/\psi)$ je formula $\varphi \to (\psi \to (\varphi \wedge \psi))$. Nech $\mathfrak{M}$ je interpretácia jazyka $\mathcal{L}$, v je ohodnotenie premenných. Potom výrok $A(p/\mathfrak{M} \models_v \varphi, q/\mathfrak{M}_v \models \psi)$ je výrok

$$\text{Ak } \mathfrak{M} \models_v \varphi \text{ tak, ak platí } \mathfrak{M} \models_v \psi \text{ tak platí aj } \mathfrak{M} \models_v \varphi \text{ a } \mathfrak{M} \models_v \psi.$$

Posledný výrok je tautológia. Teda

$$\mathfrak{M} \models \varphi \to (\psi \to (\varphi \wedge \psi)).$$

13 Teória a model

Nech $\mathcal{L}$ je jazyk predikátového počtu. Množina $\mathbf{T}$ (konečná alebo nekonečná) uzavretých formúl jazyka $\mathcal{L}$ sa nazýva **teória** alebo **matematická teória** alebo **formalizovaná teória** v jazyku $\mathcal{L}$. Formula, ktorá je prvok množiny $\mathbf{T}$ sa nazýva **axióma teórie T**. Ak každý znak jazyka $\mathcal{L}$ sa vyskytuje v niektorej axióme teórie $\mathbf{T}$, tak budeme hovoriť, že $\mathcal{L}$ je **jazyk teórie T**.

Matematika používa nasledujúcu konvenciu. Ak φ je formula, ktorá neobsahuje kvantifikátory, tak hovoríme, že φ je axióma teórie $\mathbf{T}$, ak $(\forall \ldots)\,\varphi$ je axióma teórie $\mathbf{T}$. To je v súlade s konvenciou o zamlčaní veľkého kvantifikátora.

Príklad 13.1 Teória okruhov $\mathbf{T}_{okruh}$ je nasledujúca množina formúl v jazyku $\mathcal{L}_{okruh}$[14]:

$$\mathbf{x} \doteq \mathbf{x} \qquad \mathbf{x} \doteq \mathbf{y} \to \mathbf{y} \doteq \mathbf{x} \qquad \mathbf{x} \doteq \mathbf{y} \to (\mathbf{y} \doteq \mathbf{z} \to \mathbf{x} \doteq \mathbf{z})$$

$$(\mathbf{x} \doteq \mathbf{u} \wedge \mathbf{y} \doteq \mathbf{v}) \to (\mathbf{x} \dot{+} \mathbf{y} \doteq \mathbf{u} \dot{+} \mathbf{v}) \qquad (\mathbf{x} \doteq \mathbf{u} \wedge \mathbf{y} \doteq \mathbf{v}) \to (\mathbf{x} \dot{-} \mathbf{y} \doteq \mathbf{u} \dot{-} \mathbf{v})$$

$$(\mathbf{x} \doteq \mathbf{u} \wedge \mathbf{y} \doteq \mathbf{v}) \to (\mathbf{x} \mathbin{\dot{\cdot}} \mathbf{y} \doteq \mathbf{u} \mathbin{\dot{\cdot}} \mathbf{v}) \qquad \neg \mathbf{0} \doteq \mathbf{1}$$

$$\mathbf{x} \dot{+} (\mathbf{y} \dot{+} \mathbf{z}) \doteq (\mathbf{x} \dot{+} \mathbf{y}) \dot{+} \mathbf{z} \qquad \mathbf{x} \mathbin{\dot{\cdot}} (\mathbf{y} \mathbin{\dot{\cdot}} \mathbf{z}) \doteq (\mathbf{x} \mathbin{\dot{\cdot}} \mathbf{y}) \mathbin{\dot{\cdot}} \mathbf{z}$$

$$\mathbf{x} \dot{+} \mathbf{y} \doteq \mathbf{y} \dot{+} \mathbf{x} \qquad \mathbf{x} \mathbin{\dot{\cdot}} \mathbf{y} \doteq \mathbf{y} \mathbin{\dot{\cdot}} \mathbf{x}$$

$$\mathbf{x} \mathbin{\dot{\cdot}} (\mathbf{y} \dot{+} \mathbf{z}) \doteq (\mathbf{x} \mathbin{\dot{\cdot}} \mathbf{y}) \dot{+} (\mathbf{x} \mathbin{\dot{\cdot}} \mathbf{z}) \qquad \mathbf{x} \dot{+} (\mathbf{y} \dot{-} \mathbf{x}) \doteq \mathbf{x}$$

$$\mathbf{x} \dot{+} \mathbf{0} \doteq \mathbf{x} \qquad \mathbf{x} \mathbin{\dot{\cdot}} \mathbf{0} \doteq \mathbf{0} \qquad \mathbf{x} \mathbin{\dot{\cdot}} \mathbf{1} \doteq \mathbf{x}$$

Teória polí $\mathbf{T}_{pole}$ má tie isté axiómy a naviac axiómu

$$(\forall \mathbf{x} \neq \mathbf{0})(\exists \mathbf{y})\, \mathbf{x} \mathbin{\dot{\cdot}} \mathbf{y} \doteq \mathbf{1}.$$

Podobne, teória oborov integrity $\mathbf{T}_{oborintegrity}$ má tie isté axiómy ako teória okruhov a naviac axiómu

$$(\forall \mathbf{x}, y)\, (\mathbf{x} \mathbin{\dot{\cdot}} \mathbf{y} \doteq \mathbf{0} \to (\mathbf{x} \doteq \mathbf{0}) \vee (\mathbf{y} \doteq \mathbf{0})). \tag{13.18}$$

Všetky tri uvedené teórie sú v jazyku $\mathcal{L}_{okruh}$.

Teória grúp $\mathbf{T}_{grupa}$ je teória v jazyku $\mathcal{L}_{grupa}$ a má nasledujúce axiómy:

$$\mathbf{x} \doteq \mathbf{x} \qquad \mathbf{x} \doteq \mathbf{y} \to \mathbf{y} \doteq \mathbf{x} \qquad \mathbf{x} \doteq \mathbf{y} \to (\mathbf{y} \doteq \mathbf{z} \to \mathbf{x} \doteq \mathbf{z})$$

$$(\mathbf{x} \doteq \mathbf{u} \wedge \mathbf{y} \doteq \mathbf{v}) \to (\mathbf{x} \circ \mathbf{y} \doteq \mathbf{u} \circ \mathbf{v}) \qquad \mathbf{x} \circ (\mathbf{y} \circ \mathbf{z}) \doteq (\mathbf{x} \circ \mathbf{y}) \circ \mathbf{z}$$

$$\mathbf{x} \circ \mathbf{e} \doteq \mathbf{x} \qquad \mathbf{e} \circ \mathbf{x} \doteq \mathbf{x} \qquad (\forall \mathbf{x})(\exists \mathbf{y})\, \mathbf{x} \circ \mathbf{y} \doteq \mathbf{e}.$$

[14] Ak φ neobsahuje kvantifikátory, tak v súlade s uvedenou konvenciou namiesto $(\forall \ldots)\,\varphi$ píšeme jednoducho φ.

Nech $\mathbf{T}$ je teória v jazyku $\mathcal{L}$. Interpretácia $\mathfrak{M}$ jazyka $\mathcal{L}$ sa nazýva **model teórie $\mathbf{T}$**, ak každá axióma teórie $\mathbf{T}$ platí v interpretácii $\mathfrak{M}$, t.j. ak

$$\mathfrak{M} \models \varphi \text{ pre každé } \varphi \in \mathbf{T}.$$

Pripomeňme si definíciu pojmu "okruh" v algebre. Definícia bola približne takáto: Nech na množine M je daná binárna relácia rovnosti $=$, tri binárne operácie $+$, $-$, $\cdot$ a dva prvky 0, 1. Ak sú splnené podmienky

$x = x$, $x = y \to y = x$, $x = y \to (y = z \to x = z)$,
$(x = u \wedge y = v) \to (x + y = u + v)$, $(x = u \wedge y = v) \to (x - y = u - v)$,
$(x = u \wedge y = v) \to (x$
$cdoty = u \cdot v)$, $\neg 0 = 1$,
$x + (y + z) = (x + y) + z$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
$x + y = y + x$, $x \cdot y = y \cdot x$,
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, $x + (y - x) = x$,
$x + 0 = x$, $x \cdot 0 = 0$, $x \cdot 1 = x$,

tak štruktúra $\langle M, =, +, -, \cdot, 0, 1\rangle$ sa nazýva **okruh**.

Veta "Nech na množine M je daná binárna relácia rovnosti $=$, tri binárne operácie $+$, $-$, $\cdot$ a dva prvky 0, 1." je ekvivalentná tvrdeniu, že štruktúra

$$\langle M, =, +, -, \cdot, 0, 1\rangle$$

je interpretácia jazyka $\mathcal{L}_{okruh}$. Splnenie uvedených podmienok je to isté, ako žiadať, že uvedená interpretácia je model teórie $\mathbf{T}_{okruh}$.

Teda, môžeme zhrnúť: okruh je model teórie okruhov $\mathbf{T}_{okruh}$.

Ak si pripomenieme definície pojmov pole, obor integrity a grupa z algebry, tak ľahko zistíme, že pole je model teórie polí $\mathbf{T}_{pole}$, obor integrity je model teórie oborov integrity $\mathbf{T}_{oborint}$ a grupa je model teórie grúp $\mathbf{T}_{grupa}$.

Príklad 13.2 Na základe poznatkov z algebry vieme, že interpretácie $\mathfrak{R}$, $\mathfrak{Q}$ z príkladu 12.3 sú modely teórií $\mathbf{T}_{okruh}$, $\mathbf{T}_{pole}$ a $\mathbf{T}_{oborint}$. Interpretácia $\mathfrak{Z}_p$ je model teórie $\mathbf{T}_{okruh}$ pre každé prirodzené číslo $p > 1$ a je model teórií $\mathbf{T}_{pole}$ a $\mathbf{T}_{oborint}$, ak p je prvočíslo. Interpretácie $\mathfrak{N}$ a $\mathfrak{R}^\star$ nie sú modelom žiadnej z uvedených teórií. Prečo?

Interpretácie $\mathfrak{G}_1$, $\mathfrak{G}_2$ a $\mathfrak{G}_3$ jazyka $\mathcal{L}_{grupa}$ sú modely teórie $\mathbf{T}_{grupa}$. Interpretácia $\mathfrak{G}_4$ je model teórie $\mathbf{T}_{grupa}$ práve vtedy, keď p je prvočíslo.

Nech $\mathbf{T}$ je matematická teória v jazyku $\mathcal{L}$, φ je formula v tomto jazyku. Budeme hovoriť, že formula φ **platí v teórii $\mathbf{T}$**, písať $\mathbf{T} \models \varphi$, ak v každom modeli $\mathfrak{M}$ teórie $\mathbf{T}$ je $\mathfrak{M} \models \varphi$.

Príklad 13.3 Ak φ je axióma teórie $\mathbf{T}$, tak $\mathbf{T} \models \varphi$. Naozaj, ak $\mathfrak{M}$ je model teórie $\mathbf{T}$, tak podľa definície modelu je $\mathfrak{M} \models \varphi$.

Porovnáme situáciu s výrokovým počtom. Formálny výrok $A(q_1, \ldots, q_k)$ bol utvorený z elementárnych výrokov $q_1, \ldots, q_k$. Ak sme chceli z formálneho výroku A dostať výrok (ktorý je pravdivý alebo nepravdivý) tak sme museli povedať, čo označujú elementárne výroky $q_1, \ldots, q_k$, z ktorých je výrok A utvorený.

Vzhľadom na základný postulát výrokového počtu stačilo povedať, ktorý z elementárnych výrokov $q_1, \ldots, q_k$ je pravdivý a ktorý je nepravdivý. To je práve riadok pravdivostnej tabuľky: pod každým elementárnym výrokom $q_1, \ldots, q_k$ je napísaná jeho pravdivostná hodnota $Q_1, \ldots, Q_k$. Teda, riadok tabuľky je to, čo sme v predikátovom počte nazvali interpretácia jazyka. Mohli by sme pokračovať v analógii. Nech Δ je množina výrokov. Riadok tabuľky nazveme **model teórie** Δ, ak pod každým výrokom množiny Δ je v tomto riadku pravdivostná hodnota 1. Potom definícia vzťahu $\Delta \models A$ dostane tvar "V každom modeli teórie Δ platí výrok A".

Výrok $A(q_1, \ldots, q_n)$ sme nazvali tautológia, ak $\emptyset \models A$. Bol to výrok, ktorý platil nezávisle od toho, čo označovali elementárne výroky $q_1, \ldots, q_n$. Formula φ, pre ktorú platí $\emptyset \models \varphi$, teda formula ktorá platí v ľubovoľnej interpretácii, je formalizácia výrokovej funkcie, ktorú sme neformálne nazvali logicky pravdivou.

Na základe úvah uvedených na konci časti 12, dostávame

Tvrdenie 13.1 *Ak $A(q_1, \ldots, q_n)$ je výrok tautológia, $\varphi_1, \ldots, \varphi_n$ sú formuly, tak*

$$\emptyset \models A(q_1/\varphi_1, \ldots, q_n/\varphi_n).$$

Ak $\mathbf{T}_1 \subseteq \mathbf{T}_2$, t.j. ak každá axióma teórie $\mathbf{T}_1$ je aj axiómou teórie $\mathbf{T}_2$, tak každý model teórie $\mathbf{T}_2$ je aj model teórie $\mathbf{T}_1$. V uvedenom tvrdení je určitá nepresnosť. Tvrdenie je pravdivé, ak obidve teórie sú v tom istom jazyku. Ak nie, tak jazyk teórie $\mathbf{T}_1$ je časťou jazyka teórie $\mathbf{T}_2$ a treba vynechať "interpretáciu" tých pojmov, ktoré sa v prvom jazyku nevyskytujú.

Príklad 13.4 Teória komutatívnych grúp vznikne z teórie grúp $\mathbf{T}_{grupa}$ pridaním axiómy

$$(\forall \mathbf{x})(\forall \mathbf{y})(\mathbf{x} \circ \mathbf{y} = \mathbf{y} \circ \mathbf{x}).$$

Býva zvykom v jazyku teórie komutatívnych grúp označovať grupovú operáciu $+$ a nie $\circ$ a individuálnu konštantu $\mathbf{0}$ a nie $\mathbf{e}$. Nech teda teória $\mathbf{T}_{komgrupa}$ vznikne z reórie $\mathbf{T}_{grupa}$ pridaním uvedenej axiómy, premenovaním názvu operácie $\circ$ na $+$ a zámenou individuálnej konštanty $\mathbf{e}$ konštantou $\mathbf{0}$.

Potom platí $\mathbf{T}_{komgrupa} \subseteq \mathbf{T}_{okruh}$. Jazyk teórie komutatívnych grúp $\{=, \mathbf{0}, +\}$ je časťou jazyka $\mathcal{L}_{okruh} = \{=, \mathbf{0}, 1, +, -, \cdot\}$. Ak

$$\mathfrak{M} = \langle M, =, 0, 1, +, -, \cdot \rangle$$

je okruh, teda model teórie $\mathbf{T}_{okruh}$, tak po vynechaní interpretácie názvov operácií $-$, $\cdot$ a interpretácie individuálnej konštanty $\mathbf{1}$ dostaneme model

$$\langle M, =, 0, + \rangle$$

teórie komutatívnych grúp $\mathbf{T}_{komgrupa}$.

Príklad 13.5 Z kurzu algebry čitateľ pozná tvrdenie "Pole je obor integrity." V tejto formulácii sme, ako obyčajne, zamlčali veľký kvantifikátor. Chceli sme povedať, že "Každé pole je obor integrity". Analyzujme, čo toto tvrdenie znamená a čo potrebujeme overiť.

Pole je model teórie polí. Obor integrity je model teórie oborov integrity. Teda tvrdenie hovorí, že v každom modeli teórie $\mathbf{T}_{pole}$ platia všetky axiómy teórie $\mathbf{T}_{oborint}$. Každá axióma teórie $\mathbf{T}_{oborint}$ je axiómou teórie $\mathbf{T}_{pole}$, okrem axiómy (13.18). Teda potrebujeme a stačí ukázať, že

v každom poli platí axióma (13.18).

Doslova, mali by sme vyskúšať, či v každom poli platí (13.18). Ale my nemáme prehľad o všetkých poliach. Poznáme všetky polia? Stačí nám ten v tomto prípade negatívny poznatok, že existuje nekonečne mnoho polí: pre každé prvočíslo p interpretácia $\mathfrak{Z}_p$ je pole. Takže už overovanie platnosti (13.18) v týchto nekonečne mnoho poliach by bolo "nekonečné".

Samozrejme, v algebre sme to tak nerobili. Urobili sme niečo iné. V teórii $\mathbf{T}_{pole}$ "sme dokázali" formulu (13.18) a využili sme poznatky o vzťahu dôkazu a pravdivosti. Spomeňte si, že vo výrokovom počte sme mali vetu o korektnosti, ktorá tvrdila, že ak výrok je dokázateľný z predpokladov Δ, tak platí za predpokladov Δ. Podobne to bude aj v predikátovom počte.

14 Dôkaz v predikátovom počte

Podobne ako vo výrokovom počte definujeme pojem dôkaz. Postupnosť formúl

$$\varphi_1, \ldots, \varphi_n$$

sa nazýva **dôkaz v teórii T**, ak pre každý člen tejto postupnosti, t.j. pre každé $i = 1, \ldots, n$ platí jedna z podmienok

D1) φ_i je axióma predikátového počtu,

D2) φ_i je axióma teórie $\mathbf{T}$,

D3) existujú také $k, j < i$, že φ_k je formula $\varphi_j \to \varphi_i$,

D4) existuje také $j < i$ a formuly φ, ψ, formula ψ neobsahuje premennú $\mathbf{x}$, také, že φ_j je $\psi \to \varphi(\mathbf{x}, \ldots)$ a φ_i je formula $\psi \to (\forall \mathbf{x})\, \varphi(\mathbf{x}, \ldots)$,

D5) existuje také $j < i$ a formuly φ, ψ, formula ψ neobsahuje premennú $\mathbf{x}$, také, že φ_j je $\varphi(\mathbf{x}, \ldots) \to \psi$ a φ_i je formula $(\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots) \to \psi$.

Samozrejme, musíme povedať. čo je to **axióma predikátového počtu**, skrátene **APP**. Budeme mať tri skupiny axióm predikátového počtu. Axiómy prvej skupiny budeme často nazývať axiómy výrokového počtu. Dôvod je zrejmý. Ak

φ, ψ, σ sú formuly, tak nasledujúce formuly sú APP:

$$\varphi \to \varphi \qquad \varphi \to (\psi \to \varphi)$$
$$(\varphi \to \psi) \to ((\psi \to \sigma) \to (\varphi \to \sigma)) \qquad (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$$
$$(\varphi \to \psi) \to ((\varphi \to (\psi \to \sigma)) \to (\varphi \to \sigma))$$
$$\varphi \to (\psi \to (\varphi \wedge \psi)) \qquad (\varphi \wedge \psi) \to \varphi$$
$$(\varphi \wedge \psi) \to (\psi \wedge \varphi)$$
$$(\varphi \to \sigma) \to ((\psi \to \sigma) \to ((\varphi \vee \psi) \to \sigma)) \qquad \varphi \to (\varphi \vee \psi)$$
$$(\varphi \vee \psi) \to (\psi \vee \varphi)$$
$$(\varphi \to \psi) \to ((\psi \to \varphi) \to (\varphi \equiv \psi)) \qquad (\varphi \equiv \psi) \to (\varphi \to \psi)$$
$$(\varphi \equiv \psi) \to (\psi \equiv \varphi)$$
$$\varphi \vee \neg\varphi \qquad \neg\neg\varphi \equiv \varphi$$
$$(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$$

Túto skupinu axióm môžeme opísať aj takto: ak $D(p, q, r)$ je axióma výrokového počtu ($A = p$, $B = q$, $C = r$) a φ, ψ, σ sú formuly, tak $D(p/\varphi, q/\psi, r/\sigma)$ je axióma predikátového počtu.

Druhá skupina tvoria axiómy o vynechaní veľkého kvantifikátora a zavedení malého kvantifikátora. Ak $\varphi(\mathbf{x}, \ldots)$ je formula, $\mathbf{t}$ je term, ktorý neobsahuje premennú $\mathbf{x}$, tak nasledujúce formuly sú APP:

$$(\forall \mathbf{x})\, \varphi(\mathbf{x}, \ldots) \to \varphi(\mathbf{t}, \ldots),$$
$$\varphi(\mathbf{t}, \ldots) \to (\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots).$$

Prvú axiómu môžeme nazvať "vynechanie $\forall$" a druhú "zavedenie $\exists$".

Tretia skupina axióm predikátového počtu sú tzv. de Morganove pravidlá pre negovanie kvantifikátorov. Ak φ je formula, tak nasledujúce formuly sú APP:

$$\neg(\forall \mathbf{x})\, \varphi \equiv (\exists \mathbf{x})\, \neg\varphi, \qquad \neg(\exists \mathbf{x})\, \varphi \equiv (\forall \mathbf{x})\, \neg\varphi.$$

Podmienka D3) predstavuje nám známe odvodzovacie pravidlo modus ponens. Podmienky D4) a D5) opisujú použitie odvodzovacích pravidiel

$$\frac{\psi \to \varphi(\mathbf{x}, \ldots)}{\psi \to (\forall \mathbf{x})\, \varphi(\mathbf{x}, \ldots)} \quad \text{zav } \forall, \qquad \frac{\varphi(\mathbf{x}, \ldots) \to \psi}{(\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots) \to \psi} \quad \text{vyn } \exists,$$

za predpokladu, že formula ψ neobsahuje premennú $\mathbf{x}$.

Ak existuje dôkaz $\varphi_1, \ldots, \varphi_n$ v teórii $\mathbf{T}$ taký, že $\varphi_n = \varphi$, tak hovoríme, že formula φ **je dokázateľná v teórii T**, píšeme $\mathbf{T} \vdash \varphi$.

Tvrdenie 14.1 *Ak φ je APP, tak $\emptyset \models \varphi$.*

Overenie: Pre prvú skupinu axióm tvrdenie vyplýva z tvrdenia 13.1, lebo každá axióma výrokového počtu je tautológia.

Overíme tvrdenie pre axiómu zavedenie $\exists$. Nech φ je formula v jazyku $\mathcal{L}$, $\mathbf{t}$ je term v tomto jazyku a $\mathfrak{M}$ je ľubovoľná interpretácia jazyka $\mathcal{L}$. Nech v je ohodnotenie premenných. Predpokladajme, že platí $\mathfrak{M} \models_v \varphi(\mathbf{t}, \ldots)$. Nech w je

ohodnotenie premenných také, že $w(\mathbf{y}) = v(\mathbf{y})$ pre každú premennú $\mathbf{y} \neq \mathbf{x}$ a $w(\mathbf{x}) = v(\mathbf{t})$. Potom $\mathfrak{M} \models_w (\exists)\, \varphi(\mathbf{x}, \ldots)$. Teda

$$\emptyset \models \varphi(\mathbf{t}, \ldots) \to (\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots).$$

Ostatné prípady sú dobrým cvičením na pochopenie príslušných definícií.

q.e.d.

Podobne ako pre výroky, platí

Tvrdenie 14.2 (Veta o korektnosti)
Ak $\mathbf{T}$ *je teória,* φ *je formula v jazyku tejto teórie a* $\mathbf{T} \vdash \varphi$*, tak* $\mathbf{T} \models \varphi$.

Overenie: Nech $\varphi_1, \ldots, \varphi_n$ je dôkaz v teórii $\mathbf{T}$ taký, že $\varphi_n = \varphi$. Matematickou indukciou ukážeme, že pre každé $i = 1, \ldots, n$ platí $\mathbf{T} \models \varphi_i$.

Predpokladajme, že $\mathbf{T} \models \varphi_j$ pre každé $j < i$. Keďže φ_i je člen dôkazu v teórii $\mathbf{T}$, tak spĺňa jednu z podmienok D1) – D5).

Ak spĺňa podmienku D1) alebo D2), tak tvrdenie vyplýva z príkladu 13.3 a tvrdenia 14.1.

Na ilustráciu ukážeme prípad, keď je splnená podmienka D5). Nech teda existuje také $j < i$ a formuly φ, ψ, formula ψ neobsahuje premennú $\mathbf{x}$, také, že φ_j je $\varphi(\mathbf{x}, \ldots) \to \psi$ a φ_i je formula $(\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots) \to \psi$. Nech $\mathfrak{M}$ je interpretácia teórie $\mathbf{T}$ a v ohodnotenie premenných. Predpokladajme, že

$$\mathfrak{M} \models_v (\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots).$$

Teda existuje také ohodnotenie premenných w, že $w(\mathbf{y}) = v(\mathbf{y})$ pre každú premennú $\mathbf{y}$ rôznu od premennej $\mathbf{x}$ a $\mathfrak{M} \models_w \varphi(\mathbf{x}, \ldots)$. Podľa indukčného predpokladu $\mathbf{T} \models \varphi_j$. Potom $\mathfrak{M} \models_w \varphi_j$, t.j. $\mathfrak{M} \models_w \varphi(\mathbf{x}, \ldots) \to \psi$. Podľa definície vzťahu $\models_w$ pre implikáciu dostávame $\mathfrak{M} \models_w \psi$. Keďže formula ψ neobsahuje premennú $\mathbf{x}$, tak platí aj $\mathfrak{M} \models_v \psi$. Potom podľa definície vzťahu $\models_v$ pre implikáciu dostaneme

$$\mathfrak{M} \models_v (\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots) \to \psi.$$

q.e.d.

Platí aj obrátené tvrdenie. Jeho overenie je však podstatne zložitejšie a presahuje rámec tohoto kurzu. Uvedomte si, že overenie vety o úplnosti výrokového počtu bolo pomerne komplikované. Teraz nám ešte pribudli kvantifikátory.

Tvrdenie 14.3 (Gödelova veta o úplnosti predikátového počtu)
Ak $\mathbf{T}$ *je teória,* φ *je formula v jazyku tejto teórie a* $\mathbf{T} \models \varphi$*, tak* $\mathbf{T} \vdash \varphi$.

Rovnako ako v časti 4 môžeme definovať pojem **odvodzovacie pravidlo v teórii T**. 0Ak odvodzovacie pravidlo je odvodzovacím pravidlom v ľubovoľnej teórii, tak podobne ako vo výrokovom počte, budeme stručne hovoriť len o odvodzovacom pravidle.

Podmienkam D3) – D5) definície dôkazu v predikátovom počte odpovedajú pravidlo modus ponens (známe z výrokového počtu) a už spomenuté odvodzovacie pravidlá zavedenie $\forall$ a vynechanie $\exists$.

Ak v odvodzovacom pravidle výrokového počtu (ktoré je OP v ľubovoľnej množine Δ) nahradíme výroky formulami, tak dostaneme odvodzovacie pravidlo (v ľubovoľnej teórii). Napríklad, ak výroky A, B, C v odvodzovacích pravidlách príkladu 4.2 nahradíme formulami φ, ψ, σ, tak dostaneme odvodzovacie pravidlá:

$\frac{\varphi\to\psi,\ \psi\to\sigma}{\varphi\to\sigma}$	trans $\to$	$\frac{\neg\psi\to\neg\varphi}{\varphi\to\psi}$	nepriamo	$\frac{\varphi\to\psi}{\neg\psi\to\neg\varphi}$	kontra
$\frac{\varphi\to(\psi\to\sigma)}{\psi\to(\varphi\to\sigma)}$	poradie $\to$	$\frac{\varphi}{\varphi\wedge\varphi}$	idemp $\wedge$	$\frac{\varphi\vee\varphi}{\varphi}$	idemp $\vee$
$\frac{\varphi\wedge\psi}{\psi\wedge\varphi}$	kom $\wedge$	$\frac{\varphi,\ \psi}{\varphi\wedge\psi}$	zav $\wedge$	$\frac{\varphi\wedge\psi}{\varphi}$	vyn $\wedge$
$\frac{\varphi\vee\psi}{\psi\vee\varphi}$	kom $\vee$	$\frac{\varphi}{\varphi\vee\psi}$	zav $\vee$	$\frac{\varphi\to\sigma,\ \psi\to\sigma}{\varphi\vee\psi\to\sigma}$	vyn $\vee$
$\frac{\varphi\equiv\psi}{\psi\equiv\varphi}$	kom $\equiv$	$\frac{\varphi\to\psi,\ \psi\to\varphi}{\varphi\equiv\psi}$	zav $\equiv$	$\frac{\varphi\equiv\psi}{\varphi\to\psi}$	vyn $\equiv$
$\frac{\varphi\to\psi,\ \neg\varphi\to\psi}{\psi}$	rozbor	$\frac{\varphi}{\neg\neg\varphi}$	zav $\neg\neg$	$\frac{\neg\neg\varphi}{\varphi}$	vyn $\neg\neg$

Podobným postupom aplikovaným na príklad 7.3 dostaneme odvodzovacie pravidlá

$$\frac{\varphi\to\sigma,\ \psi\to\rho}{(\varphi\wedge\psi)\to(\sigma\wedge\rho)},\qquad \frac{\varphi\to\sigma,\ \psi\to\rho}{(\varphi\vee\psi)\to(\sigma\vee\rho)},$$

$$\frac{\varphi\to(\psi\to\sigma)}{(\varphi\wedge\psi)\to\sigma},\qquad \frac{(\varphi\wedge\psi)\to\sigma}{\varphi\to(\psi\to\sigma)}.$$

Podobne ako vo výrokovom počte formula φ sa nazýva **veta teórie T**, ak $\mathbf{T}\vdash\varphi$. Postupnosť formúl $\varphi_1,\dots,\varphi_n$ sa nazýva **matematický dôkaz v teórii T**, ak pre každý jej člen, t.j. pre každé $i=1,\dots,n$ platí niektorá z nasledujúcich troch podmienok:

MD1) φ_i je axióma predikátového počtu,

MD2) φ_i je veta teórie $\mathbf{T}$,

MD3) existujú také čísla $j_1,\dots,j_k<i$, že

$$\frac{A_{j_1},\dots,A_{j_k}}{A_i}$$

je odvodzovacie pravidlo v teórii $\mathbf{T}$.

Čitateľ môže modifikovať overenie z výrokového počtu, ktoré dáva

Tvrdenie 14.4 *Ak $\varphi_1,\dots,\varphi_n$ je matematický dôkaz v teórii $\mathbf{T}$, tak $\mathbf{T}\vdash\varphi_n$.*

Samozrejme, existujú odvodzovacie pravidlá, ktoré nemôžeme získať z odvodzovacích pravidiel výrokového počtu, lebo súvisia s kvantifikátormi.

Príklad 14.1 Ak $\varphi(\mathbf{x},\ldots)$ je formula, $\mathbf{t}$ je term, ktorý neobsahuje premennú $\mathbf{x}$, tak nasledujúce postupnosti sú odvodzovacie pravidlá:

$$\frac{(\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)}{\varphi(\mathbf{t},\ldots)}\ \text{vyn}\ \forall \qquad \frac{\varphi(\mathbf{t},\ldots)}{(\exists\mathbf{x})\,\varphi(\mathbf{x},\ldots)}\ \text{zav}\ \exists$$

$$\frac{(\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)}{(\forall\mathbf{y})\,\varphi(\mathbf{y},\ldots)}\ \text{zámena prem} \qquad \frac{\varphi(\mathbf{x},\ldots)}{(\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)}\ \text{zovš}$$

Prvé dve odvodzovacie pravidlá sa overia jednoducho použitím axió predikátového počtu druhej skupiny.

Overíme, že tretia postupnosť (prvá v druhom riadku) je odvodzovacie pravidlo. Nech $\mathbf{T}$ je teória a $\mathbf{T} \vdash (\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)$. Nech σ je ľubovoľná uzavretá formula, ktorá neobsahuje premenné $\mathbf{x}$ a $\mathbf{y}$. Potom formula $\sigma = (\psi \to \psi)$ je APP. Potom nasledujúca postupnosť je matematický dôkaz v teórii $\mathbf{T}$

$$(\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots),\quad (\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)\to\varphi(\mathbf{y},\ldots),\quad \varphi(\mathbf{y},\ldots)\to(\psi\to\varphi(\mathbf{y},\ldots)),$$
$$\varphi(\mathbf{y},\ldots),\quad \psi\to\varphi(\mathbf{y},\ldots),\quad \psi\to(\forall\mathbf{y})\,\varphi(\mathbf{y},\ldots),\quad \psi,\quad (\forall\mathbf{y})\,\varphi(\mathbf{y},\ldots)$$

a teda $\mathbf{T} \vdash (\forall\mathbf{y})\,\varphi(\mathbf{y},\ldots)$.

mm

Podobne, predpokladajme, že $\mathbf{T} \vdash \varphi(\mathbf{x},\ldots)$ a ψ je vyššie zostrojená formula. Potom postupnosť

$$\varphi(\mathbf{x},\ldots),\quad \varphi(\mathbf{x},\ldots)\to(\psi\to\varphi(\mathbf{x},\ldots)),\quad \psi\to\varphi(\mathbf{x},\ldots),$$
$$\psi\to(\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots),\quad \psi,\quad (\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)$$

je matematický dôkaz v teórii $\mathbf{T}$ a teda $\vdash(\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)$.

Dôležitým dôsledkom príkladu, konkrétne posledného odvodzovacieho pravidla je ekvivalencia

$$\mathbf{T} \vdash \varphi \text{ vtedy a len vtedy, keď } \mathbf{T} \vdash (\forall\ldots)\,\varphi.$$

15 Metódy dôkazu

Podobne ako vo výrokovom počte platí

Tvrdenie 15.1 (Veta o dedukcii) *Nech $\mathbf{T}$ je teória, φ, ψ sú uzavreté formuly v jazyku tejto teórie. Ak $\mathbf{T} + \psi \vdash \varphi$, tak $\mathbf{T} \vdash \psi \to \varphi$.*

Overenie: Nech $\varphi_1,\ldots,\varphi_n$ je dôkaz v teórii $\mathbf{T} + \varphi$, $\varphi_n = \varphi$. Matematickou indukciou ukážeme, že $\mathbf{T} \vdash \psi \to \varphi_i$ pre $i = 1,\ldots,n$.

Predpokladajme, že $\mathbf{T} \vdash \psi \to \varphi_j$ pre $j < i$ a chceme ukázať, že $\mathbf{T} \vdash \psi \to \varphi_i$. Keďže je člen dôkazu v teórii $\mathbf{T} + \psi$, tak platí jedna z podmienok D1) – D5). Ak platí niektorá z podmienok D1) – D3), tak postupujeme rovnako ako pri overovaní tvrdenia 5.1.

Predpokladajme, že platí podmienka D4), t.j. existuje také $j < i$ a formuly σ, ρ, formula σ neobsahuje premennú $\mathbf{x}$, také, že φ_j je $\sigma \to \rho$ a φ_i je formula $\sigma \to (\forall \mathbf{x})\, \rho$. Podľa indukčného predpokladu je

$$\mathbf{T} \vdash \psi \to (\sigma \to \rho.$$

Potom nasledujúca postupnosť je matematický dôkaz v teórii $\mathbf{T}$

$$\psi \to (\sigma \to \rho),\ (\psi \wedge \sigma) \to \rho,\ (\psi \wedge \sigma) \to (\forall \mathbf{x})\, \rho,\ \psi \to (\sigma \to (\forall \mathbf{x})\, \rho$$

a teda $\mathbf{T} \vdash \psi \to \varphi_i$.

Ak platí podmienka D4), tak existuje také $j < i$ a formuly σ, ρ, formula σ neobsahuje premennú $\mathbf{x}$, také, že φ_j je $\rho \to \sigma$ a φ_i je formula $(\exists \mathbf{x})\, \rho \to \sigma$. Podľa indukčného predpokladu $\mathbf{T} \vdash \psi \to \varphi_j$. Potom postupnosť

$$\psi \to (\rho \to \sigma),\ \rho \to (\psi \to \sigma),\ (\forall \mathbf{x})\, \rho \to (\psi \to \sigma),\ \psi \to ((\forall \mathbf{x})\, \rho \to \sigma)$$

je matematický dôkaz v teórii $\mathbf{T}$.

q.e.d.

Podobne ako vo výrokovom počte, z tohoto tvrdenia dostávame

Tvrdenie 15.2 (Reductio ad absurdum) *Nech $\mathbf{T}$ je teória, φ a ψ sú uzavreté formuly.*

a) *Ak $\mathbf{T} + \neg\varphi \vdash \psi$ a $\mathbf{T} + \neg\varphi \vdash \neg\psi$, tak $\mathbf{T} \vdash \varphi$.*

b) *Ak $\mathbf{T} + \varphi \vdash \psi$ a $\mathbf{T} + \varphi \vdash \neg\psi$, tak $\mathbf{T} \vdash \neg\varphi$.*

Rovnako môžeme utvoriť najrôznejšie kombinácie používané pri dôkaze formuly tvaru implikácie.

Kvantifikátory si však vyžadujú ďalšie metódy dôkazu. Uvedieme dve najdôležitejšie.

Tvrdenie 15.3 (Metóda pomocnej konštanty)
Nech $\mathbf{T}$ je matematická teória, $\varphi(\mathbf{x}, \ldots)$, $\psi(\mathbf{x}, \ldots)$ sú formuly v jej jazyku. Nech $\mathbf{c}$ je individuálna konštanta, ktorá sa nevyskytuje v žiadnej axióme teórie $\mathbf{T}$. Ak

$$\mathbf{T} + \varphi(\mathbf{c}, \ldots) \vdash \psi(\mathbf{c}, \ldots),$$

tak

$$\mathbf{T} \vdash (\forall \mathbf{x})\, (\varphi(\mathbf{x}, \ldots) \to \psi(\mathbf{x}, \ldots)).$$

Overenie: Nech platí

$$\mathbf{T} + \varphi(\mathbf{c}, \ldots) \vdash \psi(\mathbf{c}, \ldots).$$

Podľa vety o dedukcii 15.1 potom

$$\mathbf{T} \vdash \varphi(\mathbf{c}, \ldots) \to \psi(\mathbf{c}, \ldots).$$

Teda existuje dôkaz

$$\varphi_1(\mathbf{c}, \ldots), \ldots, \varphi_n(\mathbf{c}, \ldots) \tag{15.19}$$

v teórii $\mathbf{T}$ taký, že $\varphi_n(\mathbf{c},\ldots) = (\varphi(\mathbf{c},\ldots) \to \psi(\mathbf{c},\ldots))$[15]. Nech $\mathbf{z}$ je premenná, ktorá sa nevyskytuje v žiadnom člene tohoto dôkazu. Tvrdíme, že postupnosť

$$\varphi_1(\mathbf{z},\ldots),\ldots,\varphi_n(\mathbf{z},\ldots) \tag{15.20}$$

je dôkaz v teórii $\mathbf{T}$.

Keďže postupnosť (15.19) je dôkaz v teórii $\mathbf{T}$, tak každý člen musí spĺňať jednu z podmienok D1) – D5). Ak $\varphi_i(\mathbf{c},\ldots)$ je APP, tak zrejme aj $\varphi_i(\mathbf{z},\ldots)$ je APP. Ak $\varphi_i(\mathbf{c},\ldots)$ je axióma teórie $\mathbf{T}$, tak podľa predpokladu (konštanta $\mathbf{c}$ sa nevyskytuje v žiadnej axióme teórie $\mathbf{T}$) platí $\varphi_i(\mathbf{c},\ldots) = \varphi_i(\mathbf{z},\ldots)$. Ak v (15.19) platí podmienka D3), tak sa ľahko vidí, že $\varphi_i(\mathbf{z},\ldots)$ spĺňa túto podmienku v (15.20).

Nech $\varphi_i(\mathbf{c},\ldots)$ spĺňa podmienku D4). Potom existuje také $j < i$ a formuly φ, ψ, formula ψ neobsahuje premennú $\mathbf{x}$, také, že φ_j je $\psi \to \varphi(\mathbf{x},\ldots)$ a φ_i je formula $\psi \to (\forall\mathbf{x})\,\varphi(\mathbf{x},\ldots)$. Keďže premenná $\mathbf{z}$ sa nevyskytuje v dôkaze (15.19), tak podmienka D4) bude splnená aj pre formulu $\varphi_i(\mathbf{z},\ldots)$ v dôkaze (15.20).

Podobný argument platí v prípade splnenia podmienky D5).

q.e.d.

Uvedenú metódu matematici veľmi často používajú. Ak máme dokázať implikáciu $(\forall x)\,(\mathcal{V}(x,\ldots) \to \mathcal{W}(x,\ldots)$, tak dôkaz začneme slovami "nech x je ľubovoľné pevné také, že platí $\mathcal{V}(x,\ldots)$." Čo to znamená? Medzi matematické predpoklady sme pridali nový predpoklad $\mathcal{V}(x,\ldots)$, teda k matematickej teórii sme pridali novú axiómu. Pritom sme však urobili na premennú x určité ohraničenia. Slovo "ľubovoľné" chce vyjadriť tú skutočnosť, že na x sme doteraz neurobili žiadny predpoklad okrem práve urobeného $\mathcal{V}(x,\ldots)$. Slovo "pevné" zase chce povedať, že počas dôkazu nemôžeme premennú x kvantifikovať, t.j. musí sa správať ako individuálna konštanta. Podľa požiadavky "ľubovoľná", táto individuálna konštanta sa nesmie vyskytovať v žiadnej axióme teórie $\mathbf{T}$.

V matematickej analýze máte často ukázať, že

$$(\forall\varepsilon)(\varepsilon > 0 \to \ \ldots\ ).$$

Dôkaz začneme slovami "Nech ε je ľubovoľné pevné kladné číslo". Teda je to typická situácia vety 15.3.

Matematici v dôkaze často používajú nasledujúci postup. Vieme už, že existuje x také, že $\mathcal{V}(x)$. Povieme: "nech x je také, že $\mathcal{V}(x)$". Tento postup je oprávnený na základe nasledujúceho tvrdenia, ktoré bezprostredne vyplýva z vety 15.3 o pomocnej konštante.

Tvrdenie 15.4 (Také, ktoré existuje)
Nech $\mathbf{T}$ je matematická teória, $\varphi(\mathbf{x},\ldots)$, ψ sú formuly v jej jazyku, formula ψ neobsahuje premennú $\mathbf{x}$. Nech $\mathbf{c}$ je individuálna konštanta, ktorá sa nevyskytuje v žiadnej axióme teórie $\mathbf{T}$. Ak

$$\mathbf{T} + \varphi(\mathbf{c},\ldots) \vdash \psi,$$

[15]Silne využívame konvenciu o fiktívnych premenných. Individuálna konštanta $\mathbf{c}$ sa nemusí vôbec vyskytovať v uvedených formulách.

tak

$$\mathbf{T} \vdash (\exists \mathbf{x})\, \varphi(\mathbf{x}, \ldots) \to \psi.$$

Overenie: Podľa tvrdenia o pomocnej konštante 15.3 platí $\mathbf{T} \vdash (\forall \mathbf{x})\, (\varphi(\mathbf{x}) \to \psi)$. Teda aj

$$\mathbf{T} \vdash (\forall \mathbf{x})\, (\neg\varphi(\mathbf{x}) \vee \psi)$$

a teda

$$\mathbf{T} \vdash ((\forall \mathbf{x})\, \neg\varphi(\mathbf{x})) \vee \psi.$$

Posledné však znamená

$$\mathbf{T} \vdash (\exists \mathbf{x})\, \varphi(\mathbf{x}) \to \psi.$$

q.e.d.

Mnohé výhodné odvodzovacie pravidlá sú viazané na konkrétnu teóriu.

Príklad 15.1 Nech $\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}_3, \mathbf{t}_4$ sú termy v jazyku $\mathcal{L}_{okruh}$. Potom nasledujúce postupnosti

$$\frac{\mathbf{t}_1 \mathrel{\dot{=}} \mathbf{t}_2 \qquad \mathbf{t}_3 \mathrel{\dot{=}} \mathbf{t}_4}{\mathbf{t}_1 \mathbin{\dot{+}} \mathbf{t}_3 \mathrel{\dot{=}} \mathbf{t}_2 \mathbin{\dot{+}} \mathbf{t}_4} \qquad \frac{\mathbf{t}_1 \mathrel{\dot{=}} \mathbf{t}_2 \qquad \mathbf{t}_3 \mathrel{\dot{=}} \mathbf{t}_4}{\mathbf{t}_1 \mathbin{\dot{\cdot}} \mathbf{t}_3 \mathrel{\dot{=}} \mathbf{t}_2 \mathbin{\dot{\cdot}} \mathbf{t}_4}$$

sú odvodzovacie pravidlá v teóriách $\mathbf{T}_{okruh}$, $\mathbf{T}_{pole}$ a $\mathbf{T}_{oborintegrity}$.

Predpokladajme, že $\mathbf{T}_{okruh} \vdash \mathbf{t}_1 \mathrel{\dot{=}} \mathbf{t}_2$ a $\mathbf{T} \vdash \mathbf{t}_3 \mathrel{\dot{=}} \mathbf{t}_4$. Štvornásobným použitím axiómy vynechanie $\forall$ a štvrtej axiómy teórie $\mathbf{T}_{okruh}$ (pozor, zamlčali sme veľké kvantifikátory) dostaneme

$$\mathbf{T} \vdash \mathbf{t}_1 \mathbin{\dot{+}} \mathbf{t}_3 \mathrel{\dot{=}} \mathbf{t}_2 \mathbin{\dot{+}} \mathbf{t}_4$$

Podobne v druhom prípade.

16 Rovnosť, definícia, neprotirečivosť a model

Pozorný čitateľ si už iste všimol, že prvé tri axiómy teórie $\mathbf{T}_{okruh}$ a $\mathbf{T}_{grupa}$ sú rovnaké. Naviac, 4. až 6. axióma teórie $\mathbf{T}_{okruh}$ a 4. axióma teórie $\mathbf{T}_{grupa}$ sú si veľmi podobné. Ak sa ešte pozriete na axiomatizáciu teórie množín, tak zistíte, že aj tam boli veľmi podobné axiómy pre reálne čísla. Nie je to náhoda? Nie, totiž v matematike jedným zo základných predikátov je predikát rovnosti a ten musí spĺňať určité axiómy. Musí byť reflexívny, symetrický a tranzitívny (to sú práve spomenuté prvé tri axiómy dvoch teórií). Naviac, musí dovoliť dosadzovať. Inými slovami, rovnaké termy po matematických operáciách alebo dosadeniach do predikátov musia dať rovnaké výsledky. To je dôvod, prečo matematici uvažujú predikátový počet s rovnosťou. Dokonca, axiómy tejto teórie, ktoré uvedieme, matematika často pokladá za samozrejmosť.

Nech

$$\mathcal{L} = \{\underset{\smile}{=}, \mathbf{P}, \ldots, \mathbf{a}, \ldots, \mathbf{f}, \ldots\}.$$

je jazyk obsahujúci predikát rovnosti $\underset{\smile}{=}$. **Predikátový počet s rovnosťou** v jazyku $\mathcal{L}$ okrem axióm APP má tieto ďalšie axiómy:

r1) $\mathbf{x} \underset{\smile}{=} \mathbf{x}, \qquad \mathbf{x} \underset{\smile}{=} \mathbf{y} \to \mathbf{y} \underset{\smile}{=} \mathbf{x}, \qquad \mathbf{x} \underset{\smile}{=} \mathbf{y} \to (\mathbf{y} \underset{\smile}{=} \mathbf{z} \to \mathbf{x} \underset{\smile}{=} \mathbf{z})$,

r2) ak $\mathbf{P} \in \mathcal{L}$ je k–árny predikát, tak nasledujúca formula je axióma:

$$(\mathbf{x}_1 = \mathbf{y}_1 \wedge \ldots \wedge \mathbf{x}_k = \mathbf{y}_k) \to (\mathbf{P}(\mathbf{x}_1, \ldots, \mathbf{x}_k) \to \mathbf{P}(\mathbf{y}_1, \ldots, \mathbf{y}_k)),$$

r3) ak $\mathbf{f} \in \mathcal{L}$ je názov k–árnej operácie, tak nasledujúca formula je axióma:

$$(\mathbf{x}_1 = \mathbf{y}_1 \wedge \ldots \wedge \mathbf{x}_k = \mathbf{y}_k) \to \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_k) \underset{\smile}{=} \mathbf{f}(\mathbf{y}_1, \ldots, \mathbf{y}_k).$$

Venujme pozornosť inej problematike. Matematika má rada definície. Čo je to definícia? Zjednodušená odpoveď je krátka: definícia je skratka. Upresníme toto tvrdenie. Musíme rozlíšiť definíciu pojmu, konkrétneho objektu a definíciu operácie.

V matematickej analýze namiesto toho, aby sme hovorili, že

$$(\forall \varepsilon > 0)(\exists \delta)(\forall x)(|x - a| < \delta \to |f(x) - f(a)| < \varepsilon$$

hovoríme, že **funkcia f je spojitá v bode** a. To je definícia. Čo sa stalo z hľadiska logiky? Do jazyka našej teórie reálnych čísiel a funkcií sme pridali nový predikát "funkcia je spojitá v bode". K teórii sme pridali novú axiómu

$$f \text{ je spojitá v bode } a \equiv (\forall \varepsilon > 0)(\exists \delta)(\forall x)(|x - a| < \delta \to |f(x) - f(a)| < \varepsilon).$$

Zovšeobecníme tento postup. Ak $\mathbf{R}$ je k–árny predikát, ktorý nepatrí do jazyka $\mathcal{L}$ teórie $\mathbf{T}$ a $\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ je formula jazyka $\mathcal{L}$, tak definícia nového pojmu $\mathbf{R}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ znamená pridanie k teórii $\mathbf{T}$ novej axiómy

$$\mathbf{R}(\mathbf{x}_1, \ldots, \mathbf{x}_k) \equiv \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k).$$

Nech $\mathbf{T}$ je teória v predikátovom počte s rovnosťou. Ak $\varphi(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_k)$ je taká formula, že v $\mathbf{T}$ je dokázateľné

$$(\forall \mathbf{x}_1) \ldots (\forall \mathbf{x}_k)(\exists \mathbf{y})\, \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}), \tag{16.21}$$

$$(\forall \mathbf{x}_1) \ldots (\forall \mathbf{x}_k)(\forall \mathbf{y})(\forall \mathbf{z})\, ((\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}) \wedge \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{z})) \to \mathbf{y} \underset{\smile}{=} \mathbf{z}), \tag{16.22}$$

tak k teórii $\mathbf{T}$ pridáme novú axiómu, definíciu názvu operácie $\mathbf{g}$:

$$g(\mathbf{x}_1, \ldots, \mathbf{x}_k) \underset{\smile}{=} \mathbf{y} \equiv \varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}).$$

Dvojica formúl (16.21) sa niekedy stručne zapisuje

$$(\forall \mathbf{x}_1) \dots (\forall \mathbf{x}_k)(\exists! \mathbf{y})\, \varphi(\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{y}).$$

Kvantifikátor $\exists!$ sa číta *existuje jediné*.

Teória $\mathbf{T}$ sa nazýva **protirečivá**, ak sa v nej dá dokázať spor, t.j. keď existuje uzavretá formula φ taká, že $\mathbf{T} \vdash \varphi$ a $\mathbf{T} \vdash \neg\varphi$. V opačnom prípade je teória **neprotirečivá**. Teda tvrdenie o metóde dôkazu sporom môžeme sformulovať takto: ak teória $\mathbf{T} + \neg\varphi$ je protirečivá, tak $\mathbf{T} \vdash \varphi$.

Ľahko vidieť, že ak máme dve teorie $\mathbf{T}_1 \subseteq \mathbf{T}_2$ a teória $\mathbf{T}_2$ je neprotirečivá, tak je taká aj teória $\mathbf{T}_1$.

Tvrdenie 16.1 *Teória* $\mathbf{T}$ *je neprotirečivá vtedy a len vtedy, keď existuje formula* φ *taká, že* $\mathbf{T} \nvdash \varphi$.

Overenie: Nech φ je ľubovoľná uzavretá formula jazyka teórie $\mathbf{T}$. Keďže teória $\mathbf{T}$ je neprotirečivá, tak aspoň jedn a z formúl φ a $\neg\varphi$ nie je dokázateľná v teórii $\mathbf{T}$.

Naopak, ak $\mathbf{T}$ je protirečivá, tak existuje uzavretá formula ψ taká, že $\mathbf{T} \vdash \psi$ a $\mathbf{T} \vdash \neg\psi$. Nech φ je ľubovoľná formula jazyka teórie $\mathbf{T}$. Potom $\mathbf{T} \vdash \neg\varphi \to \psi$ a $\mathbf{T} \vdash \neg\varphi \to \neg\psi$. Použitím poslednej axiómy prvej skupiny APP

$$(\neg\varphi \to \psi) \to ((\neg\varphi \to \neg\psi) \to \neg\neg\varphi)$$

dostaneme $\mathbf{T} \vdash \varphi$.

q.e.d.

Z vety o úplnosti ľahko dostaneme

Tvrdenie 16.2 *Teória* $\mathbf{T}$ *je neprotirečivá vtedy a len vtedy, keď existuje model teórie* $\mathbf{T}$.

Overenie: Predpokladajme, že teória $\mathbf{T}$ je neprotirečivá. Nech φ je ľubovoľná uzavretá formula jej jazyka. Potom napríklad $\mathbf{T} \nvDash \varphi$. Podľa vety o úplnosti 14.3 existuje model $\mathfrak{M}$ teórie $\mathbf{T}$ taký, že $\mathfrak{M} \not\models \varphi$. Teda existuje model teórie $\mathbf{T}$.

Naopak, nech existuje model $\mathfrak{M}$ teórie $\mathbf{T}$. Keby $\mathbf{T} \vdash \varphi$ a $\mathbf{T} \vdash \neg\varphi$, tak podľa vety o korektnosti 14.2 dostávame $\mathfrak{M} \models \varphi$ a $\mathfrak{M} \models \neg\varphi$, čo nie je možné podľa definície vzťahu $\models$.

q.e.d.

Tvrdenie 16.3 (Veta o lokalizácii) *Nech* $\mathbf{T}$ *je teória a* φ *je formula v jej jazyku. Ak* $\mathbf{t} \vdash \varphi$, *tak existuje konečná množina* $\mathbf{T}_0 \subseteq \mathbf{T}$ *taká, že* $\mathbf{T}_0 \vdash \varphi$.

Overenie: Postupujeme podobne, ako vo výrokovom počte. Ak $\mathbf{t} \vdash \varphi$, tak existuje existuje dôkaz $\varphi_1, \dots, \varphi_n$ v teórii $\mathbf{T}$ taký, že $\varphi_n = \varphi$. Nech

$$\mathbf{T}_0 = \{\psi \in \mathbf{T}; \psi \text{ je člen dôkazu } \varphi_1, \dots, \varphi_n\}.$$

Potom $\mathbf{T}_0 \subseteq \mathbf{T}$ je konečná množina a $\varphi_1, \dots, \varphi_n$ je dôkaz v teórii $\mathbf{T}_0$. Teda $\mathbf{T}_0 \vdash \varphi$.

q.e.d.

Tvrdenie 16.4 (Veta o kompaktnosti) *Teória* $\mathbf{T}$ *je neprotirečivá vtedy a len vtedy, keď každá konečná podteória* $\mathbf{T}_0 \subseteq \mathbf{T}$ *je neprotirečivá.*

Overenie: Ak teória $\mathbf{T}$ je neprotirečivá, tak zrejme aj každá jej podteória je taká.

Nech naopak, teória $\mathbf{T}$ je protirečivá. Teda exstuje uzavretá formula φ taká, že $\mathbf{T} \vdash \varphi$ a $\mathbf{T} \vdash \neg\varphi$. Podľa vety o lokalizácii existujú konečné podteórie $\mathbf{T}_1 \subseteq \mathbf{T}$ a $\mathbf{T}_2 \subseteq \mathbf{T}$ také, že $\mathbf{T}_1 \vdash \varphi$ a $\mathbf{T}_2 \vdash \neg\varphi$. Potom konečná teória $\mathbf{T}_0 = \mathbf{T}_1 \cup \mathbf{T}_2$ je protirečivá.

q.e.d.

Literatúra

[1] Bukovský L., *Množiny a všeličo okolo nich,* Alfa, Bratislava 1985

[2] Kačala J. a kolektív, *Krátky slovník slovenského jazyka,* Veda, Bratislava 1989

[3] Kleene S. C.,*Introduction to Mathematical Logic,* Wiley&Sons, New York 1967, ruský preklad, Mir, Moskva 1973

[4] Sochor A., *Klasická matematická logika,* Karolinum, Praha 2001