Úvod do diskrétnych matematických štruktúr

Daniel Olejár
Martin Škoviera

24. augusta 2007

This book was developed during the project Thematic Network 114046-CP-1-2004-1-BG-ERASMUS-TN

Typeset by LaTeX2e.

Obsah

1 Základné pojmy **5**

1.1 Výstavba matematických teórií 6

1.2 Výroky 9

1.3 Výrokové formy a kvantifikované výroky 14

1.4 Matematické dôkazy 18

1.4.1 Priamy dôkaz 19

1.4.2 Nepriamy dôkaz 20

1.4.3 Nepriame dôkazy implikácií 21

1.4.4 Rozlišovacia metóda 23

1.4.5 Princíp matematickej indukcie 23

2 Základy teórie množín **29**

2.1 Základné pojmy 29

2.2 Základné množinové operácie a vzťahy medzi množinami 32

2.3 Abeceda, slová a jazyky 35

2.4 Základné množinové identity 38

2.5 Potenčná množina 50

3 Usporiadaná dvojica a karteziánsky súčin **53**

3.1 Usporiadaná dvojica 53

3.2 Karteziánsky súčin 55

4 Binárne relácie **61**

4.1 Základné pojmy 61

4.2 Skladanie binárnych relácií 64

4.3 Množinové operácie nad binárnymi reláciami 70
4.4 Jednoznačné relácie a všade definované relácie 76

5 Zobrazenia/funkcie 81

5.1 Injektívne, surjektívne a bijektívne zobrazenia 84

6 Relácie na množine 93

6.1 Vlastnosti binárnych relácií na množine 95
6.2 Relácia ekvivalencie a rozklad množiny 100
6.3 Usporiadania 103

7 Zovšeobecnené množinové operácie 111

8 Mohutnosti a usporiadania množín 119

8.1 Spočítateľné množiny 120
8.2 Nespočítateľné množiny 124
8.3 Cantor-Bernsteinova veta 125
8.4 Kardinálne čísla 127
8.5 Aritmetika kardinálnych čísel 131
8.6 Usporiadania nekonečných množín 137
8.6.1 Zobrazenia zachovávajúce usporiadanie 137
8.6.2 Ordinálne typy 138
8.6.3 Ordinálne čísla 139
8.6.4 Transfinitná indukcia 140
8.6.5 Nasledovníci a limitné ordinálne čísla 141
8.7 Ordinálna aritmetika 141
8.8 Vzťah ordinálnych a kardinálnych čísel 148
8.9 *Historické poznámky 148

9 Výrokový počet 151

9.1 Axiomatická výstavba výrokového počtu 151
9.2 Teorémy výrokového počtu 154
9.3 Úplnosť výrokového počtu 160

9.4 Neprotirečivosť výrokového počtu 164
9.5 Nezávislosť axióm výrokového počtu 166

10 Predikátový počet **171**
10.1 Jazyk predikátového počtu 1. rádu 171
10.2 Odvodzovanie v predikátovom počte 177
10.3 Interpretácia, splniteľnosť a pravdivosť 185

11 Teórie 1. rádu **189**

12 Booleovské funkcie **195**
12.1 Základné pojmy 195
12.2 Skladanie Booleovských funkcií 199
12.3 Rozklad Booleovských funkcií podľa premenných. Normálne formy 205
12.4 Minimalizácia disjunktívnych normálnych foriem 211
12.4.1 Geometrické princípy minimalizácie DNF 213
12.4.2 Quine-McCluskeyova metóda 218
12.4.3 Karnaughove mapy 221
12.4.4 Výber pokrytia 225
12.4.5 *Odhady parametrov DNF 227
12.4.6 Neúplne určené Booleovské funkcie 229
12.5 Úplnosť a uzavretosť systému Booleovských funkcií 232
12.6 Predúplné triedy. Veta o úplnosti 237
12.6.1 Triedy T_0 a T_1 238
12.6.2 Trieda lineárnych funkcií, L 238
12.6.3 Trieda monotónnych funkcií, M 239
12.6.4 Trieda samoduálnych funkcií S 241

13 Diskrétna matematika a informatika **251**
13.1 Niektoré aplikácie funkcií v informatike 251
13.1.1 Šifrovanie informácie 251
13.1.2 Hašovacie funkcie 252

13.1.3 Primitívne rekurzívne funkcie 252
13.1.4 Lexikografické usporiadanie 252

14 Prílohy **255**

14.1 Zermelo-Fraenkelov systém axióm 255

Úvod

Táto kniha je koncipovaná ako vysokoškolská učebnica venovaná vybraným častiam diskrétnej matematiky. Výber problematiky bol daný predpokladaným čitateľom, ktorým je predovšetkým študent[1] prvého ročníka univerzitného štúdia informatiky. Pre študenta informatiky sú poznatky o diskrétnych štruktúrach a metódach diskrétnej matematiky nevyhnutným predpokladom pre jeho ďalšie úspešné štúdium a to nielen matematiky, ale aj informatiky a jej aplikácií. Mnohé z toho o čom sa hovorí v tejto knihe, možno nájsť už v študijných plánoch stredných škôl a ďalšie dôležité poznatky z diskrétnej matematiky získajú študenti na prednáškach z matematickej analýzy, algebry, matematickej logiky, teórii formálnych jazykov a ďalších prednáškach. Preto je namieste otázka, či je takáto kniha vôbec potrebná. Naše pedagogické skúsenosti ukazujú, že sa nedá spoliehať na vedomosti, ktoré by študenti mali mať zo strednej školy a že na prednáškach zvyčajne nebýva dostatok času na detailnejšie opakovanie stredoškolského učiva. Na prednáškach sa nedá s výkladom čakať dovtedy, kým sa na iných predmetoch študent (popri inom) naučí narábať aj s množinami, reláciami a funkciami, dozvie sa o matematických dôkazoch a získa predstavu o matematickej logike. Na druhej strane na to, aby dokázal sledovať (napríklad) prednášku z algebry, musí mať istú predstavu o výstavbe matematických teórií, o tom, ako vyzerajú matematické tvrdenia a ako sa dokazujú. Časom by si pravdepodobne tieto predstavy vytvoril aj sám, ale stálo by ho to nemálo času a úsilia. Aby sa úvodná fáza jeho matematickej prípravy skrátila na minimum, bol do univerzitného študijného programu informatiky zaradený predmet Úvod do diskrétnych štruktúr, ktorý predstavuje akúsi matematickú propedeutiku; prehľad základných pojmov a metód diskrétnej matematiky, s ktorými sa študenti budú počas štúdia informatiky stretávať nielen na matematických ale veľmi často aj na informatických predmetoch.

Naša kniha je teda pokusom o (diskrétno-) matematickú propedeutiku pre (začínajúcich) informatikov. Jej obsah vyplynul z analýzy študijného programu informatiky, ktorá ukázala, čo by asi študent informatiky potreboval vedieť z diskrétnej matematiky na začiatku svojho štúdia, aby potom bez väčších problémov zvládol pokročilejšie matematické a informatické predmety. Nazbieralo sa toho pomerne veľa, určite viac než sa stihne odprednášať v rámci jednej prednášky. Nechceli sme napísať výkladový slovník (vybraných častí) diskrétnej matematiky, ani knihu prispôsobiť konkrétnej prednáške, a preto sme ju koncipovali širšie ako je náplň spomenutej prednášky. Predpokladáme, že sa v rámci základnej prednášky odprednášajú kapitoly venované množinám, karteziánskemu súčinu, binárnym reláciám, zobrazeniam, reláciám na množine a mohutnos-

[1] keď v tejto knihe hovoríme o študentovi, máme na mysli tak študentov ako aj študentky

tiam množín. Užitočné by bolo odprednášať aj základy výstavby matematických teórií a najmä metódy matematických dôkazov. Do knihy sme zaradili aj dve témy, ktoré sa asi do úvodného kurzu nezmestia: Booleovské funkcie a matematickú logiku. Booleovské funkcie patria medzi základné diskrétne štruktúry, bez ktorých sa informatika nezaobíde. Prednášajú sa však len okrajovo v rámci iných predmetov a v domácej literatúre chýba dostupná kniha, z ktorej by sa daná problematika dala naštudovať. Relatívne podrobne sa Booleovské funkcie študovali v Jablonského Úvode do diskrétnej matematiky [8], špeciálne otázky (realizácia Booleovských funkcií, zložitosť) sa študujú v súvislosti s návrhom logických obvodov, resp. so skúmaním výpočtovej zložitosti algoritmov, ale prehľadné zhrnutie základných vlastností ako je v [9] chýba[2]. Na podobné problémy narážame v súvislosti s matematickou logikou, ktorá však je v porovnaní s Booleovskými funkciami v podstatne lepšom postavení, pretože v študijnom programe informatiky je jej venovaná samostatná základná prednáška (Úvod do matematickej logiky). Základné poznatky z matematickej logiky však študent bude potrebovať skôr, ako absolvuje špeciálnu prednášku z matematickej logiky. V knihe sa preto zaoberáme základmi matematickej logiky: výrokovým počtom a základmi predikátového počtu; našou ambíciou je pomôcť čitateľovi vytvoriť si predstavu o axiomatickej výstavbe jednoduchej logickej teórie a naučiť ho formálne dokazovať matematické tvrdenia.

Aj keď sme pri písaní knihy mali na zreteli predovšetkým potreby študentov univerzitného štúdia informatiky, kniha nie je určená len im. Mohla by poslúžiť aj študentom vyšších ročníkov stredných škôl, stredoškolským učiteľom a iným záujemcom o diskrétnu matematiku. Zaradili sme do nej aj témy, ktoré sa na základnej prednáške nezvyknú prednášať, ktoré však môžu byť užitočné v iných predmetoch informatického vysokoškolského štúdia (napríklad minimalizácia disjunktívnych normálnych foriem v rámci predmetu Princípy počítačov). Snažili sme sa knihu napísať tak, aby dopĺňala existujúce prednášky a dala sa použiť ako materiál na samoštúdium. Preto sme do nej zaradili množstvo rozličných príkladov a najmä veľa úloh, ktoré majú čitateľovi pomôcť osvojiť si prezentovanú problematiku. Čitateľovi odporúčame, aby tieto úlohy samostatne riešil. Pre tých čitateľov, ktorí majú záujem o hlbšie poznanie uvedenej problematiky, je určená odporúčaná doplnková literatúra.

Do knihy sme zámerne nezaradili kombinatoriku a teóriu grafov. Predpokladáme, že táto problematika bude spracovaná v samostatnej knihe.

Kniha nie je zatiaľ úplná. Text, ktorý je zverejnený predstavuje cca 80% toho, čo je pripravené. (Základom je náš starší učebný text [15], ktorý prepracovávame a dopĺňame.) Základný text plánujeme dokončiť v priebehu akademického roku 2006/2007, zverejniť ho na webe a po roku sa k nemu vrátiť, opraviť zistené chyby a zapracovať pripomienky. Ďalší osud tohto textu závisí od pracovného zaťaženia autorov a možnosti jeho použitia. Kniha je určená len pre interné použitie. Študenti si pre vlastné použitie môžu text vytlačiť. Na iné použitie textu sa vzťahujú obmedzenia uvedené v deklarácii autorských práv.

[2] s ľútosťou sme zavrhli možnosť prezentovať čitateľovi v kapitole o Booleovských funkciách použitie Booleovských funkcií v kryptológii a vlastné výsledky o kryptograficky silných Booleovských funkciách.

Autori ďakujú všetkým, ktorí svojimi pripomienkami prispeli k odstráneniu nedostatkov a zlepšeniu obsahovej a formálnej úrovne tejto knihy.

V Bratislave 24. augusta 2007

Daniel Olejár

Kapitola 1

Základné pojmy

God wrote the universe in the language of mathematics.
Galileo

Matematika vznikla pôvodne na základe praktických potrieb ľudí (meranie a počítanie reálnych objektov a skúmanie ich vlastností). Skoro sa však ukázalo, že medzi veľmi rozdielnymi objektami existujú podobné (číselne vyjadriteľné vzťahy) a to v matematike podnietilo štúdium abstraktných idealizovaných objektov. Prechod z reálneho do idealizovaného sveta umožnil matematike dosiahnuť výsledky, ktoré by sa jej pri štúdiu reálnych objektov nikdy nebolo podarilo dosiahnuť. Idealizácia a abstrakcia však vzdialili predmet skúmania matematiky od reálneho sveta a znemožnili jej používať na skúmanie také metódy ako pozorovanie a experiment. (Premeranie dĺžok strán miliónov pravouhlých trojuholníkov nestačí na dôkaz Pytagorovej vety; pretože (1) merania nie sú presné a (2) z toho, že milión objektov má nejakú vlastnosť ešte nijako nevyplýva, že túto vlastnosť majú všetky objekty.) Matematika si musela vytvoriť primeraný aparát, ktorý by jej umožnil korektne popísať idealizované objekty (na ktoré sa nevzťahujú obmedzenia reálneho sveta) a skúmať ich vlastnosti. Hľadanie adekvátneho aparátu nebol jednoduchý ani priamočiary proces[1], a riešenie tejto na prvý pohľad technickej otázky výrazne prispelo k pochopeniu možností aj obmedzení samotnej matematiky [11]. Matematici dlho hľadali univerzálny základ, na ktorom by mohli vybudovať matematiku bez protirečení a paradoxov. Nejaký čas sa zdalo, že týmto základom môže byť matematická logika, ale Gödelove výsledky túto možnosť definitívne zavrhli. Hoci matematická logika nie je matematickým *kameňom mudrcov*[2], úspešne sa používa (zohľadňujúc obmedzenia vyplývajúce z Gödelových viet) ako základ súčasných matematických teórií.

V tejto kapitole sa najprv pozrieme na to, ako vyzerajú matematické teórie, potom sa pozrieme na matematickú logiku a napokon sa budeme zaoberať spôsobmi dokazovania matematických tvrdení; t.j. matematickými dôkazmi.

[1] ktorý nie je uzavretý ani dnes
[2] či skôr Leibnitzovým *characteristica universalis* a *ars iudicandi*

1.1 Výstavba matematických teórií

Matematická teória nevzniká okamžite. Keď sa objaví nejaká nová oblasť (matematického) poznania, nejaký čas trvá, kým sa určia jej základné objekty a preskúmajú vzťahy medzi nimi; až po nejakom čase sa potom tieto poznatky spracujú do podoby ucelenej formálnej teórie.

Výstavbu matematickej teórie a význam jej formalizácie ilustrujeme na dobre známej teórii množín [4], [3].

V teórii množín sa pracuje s pojmami ako *množina, prvok množiny*; zavádzajú operácie s množinami (prienik, zjednotenie, rozdiel, doplnok), vyberajú sa z (rozličných) množín prvky a vytvárajú z nich nové množiny (dvojice, karteziánske súčiny, relácie, zobrazenia) a pod. Množiny a operácie s nimi sú na prvý pohľad zrejmé a vzniká tak prirodzená otázka, na čo vlastne potrebujeme budovať formálnu teóriu množín? Skutočne, keď pracujeme s konkrétnymi množinami, problémy sa neobjavujú. Tieto vznikajú, keď vytvárame „veľké množiny“. Zakladateľ teórie množín Cantor chápal množinu intuitívne; ako súbor objektov, spĺňajúcich nejakú vlastnosť. Skoro sa však ukázalo, že takéto chápanie je až príliš voľné a vedie k paradoxom. Russel ukázal, že „množina“ všetkých množín, ktoré neobsahujú seba samé ako svoje prvky nemôže byť množinou.[3] Ak sa chceme v teórii množín vyhnúť podobným problémom, musíme intuitívnu Cantorovu teóriu množín upresniť, formalizovať. Formalizáciu budeme robiť postupne. Najprv vyberieme najjednoduchšie pojmy, z ktorých bude možno odvodiť ostatné pojmy teórie. Všetky vlastnosti základných pojmov uvedieme ako predpoklady (t.j. niečo, čoho platnosť predpokladáme bez toho, aby sme to dokazovali), ktoré budeme nazývať *axiómami*. V ďalšom budeme teóriu (množín) rozvíjať tak, že zo základných objektov budeme vytvárať nové objekty a potom skúmať ich vlastnosti. Vlastnosti nových objektov budeme formulovať v podobe matematických tvrdení, viet, ktoré budeme dokazovať. Dokazovanie viet sa riadi presnými pravidlami, stanovenými matematickou logikou. Na výstavbu teórie (množín) používame jazyk, ktorého základom je prirodzený jazyk (v našom prípade slovenčina), rozšírený o nové špeciálne pojmy (množinové). Problém, na ktorý pri výstavbe matematickej teórie (v tomto prípade teórie množín) narážame, spočíva v tom, že prirodzený jazyk umožňuje formulovať tvrdenia dvoch odlišných úrovní:

- tvrdenia o objektoch teórie (napríklad „množina A je prázdna“);
- tvrdenia o samotnej teórii (napríklad „tvrdenie $\mathcal{T}$ sa v teórii množín nedá dokázať“).

V prvom tvrdení vystupuje prirodzený jazyk ako *jazyk teórie* v druhom ako jazyk vyššej úrovne, *metajazyk*. Vo väčšine matematických teórií sa prirodzený jazyk používa tak vo funkcii jazyka ako aj vo funkcii metajazyka teórie bez toho, aby to spôsobovalo problémy. V teórii množín (a iných matematických teóriách) je však potrebné obe úrovne odlišovať, aby sme sa vyhli tzv. *sémantickým paradoxom*, vyplývajúcim zo zmiešavania oboch úrovní jazyka. To sa dá dosiahnuť tým, že sa vytvorí nový (formálny) jazyk teórie a prirodzený jazyk sa bude používať len vo funkcii metajazyka. Slová (tvrdenia) vyjadrené v jazyku teórie budú mať podobu postupnosti symbolov. Tak ako v prirodzenom jazyku,

[3] k Russelovmu paradoxu sa vrátime neskôr, keď budeme mať k dispozícii potrebný aparát.

aj zmysluplné slová a tvrdenia v jazyku teórie sa vytvárajú podľa istých gramatických (syntaktických) pravidiel.

Keď budeme skúmať formálnu teóriu množín (prípadne sa pozrieme na iné matematické teórie) z obsahového hľadiska, zistíme, že v matematickej teórii sa vyskytujú (používajú sa) tvrdenia dvojakého druhu: tvrdenia o vlastných objektoch teórie a všeobecné (logické) tvrdenia. Tvrdenia prvého druhu sa dali očakávať - ak by ich teória neobsahovala, ako by popisovala vzťahy medzi objektami teórie (napr. množinami)? Aká je však úloha logických tvrdení v matematickej teórii? Logické tvrdenia tvoria[4] tzv. *logické základy matematickej teórie*; logickú teóriu, ktorú daná matematická teória používa. Logické základy matematickej teórie sú všeobecné, hovoria v podstate o tom, ako z pravdivých tvrdení odvodzovať pravdivé tvrdenia, musia mať výrazové prostriedky na popis objektov a vzťahov danej matematickej teórie, ale nehovoria nič o obsahu tvrdení prvého druhu (ani o obsahu samotnej matematickej teórie). Logické základy teórie ani nemusia byť formulované explicitne, matematici však obvykle vedia, akú logiku treba na výstavbu danej matematickej teórie použiť. Mnohé matematické teórie majú rovnaké požiadavky na logickú teóriu a preto môžu mať aj rovnaké logické základy. Aby sme si vytvorili konkrétnejšiu predstavu o tom, ako vyzerajú logické základy matematických teórií, predpokladajme, že logickým základom matematickej teórie je výroková logika (Podrobnejšie budeme o výrokovom a predikátovom počte hovoriť v kapitolách 9 a 10.) Výroková logika je teória, ktorá popisuje, ako z jednoduchých tvrdení (výrokov) vytvárať zložitejšie a ako dokazovať pravidovosť (zložitých) výrokov. Výrokovú logiku popíšeme formálne (zadáme „gramatiku“ zložitých výrokov a popíšeme pravidlá dokazovania ich správnosti). Výroková logika ako formálna teória (axiomatický výrokový počet) je zadaná

1. súborom základných logických objektov (výrokové premenné - predstavujúce z obsahovej stránke elementárne výroky, zo syntaktickej - atomické/elementárne formuly),
2. súborom logických operátorov (logických spojok) a pomocných symbolov (interpunkčné znamienka, zátvorky)),
3. súborom pravidiel na vytváranie nových objektov (formúl, zložených výrokov) výrokovej logiky,
4. súborom vybraných formúl - základných logických právd (axióm),
5. súborom odvodzovacích pravidiel.

Na čo jednotlivé súbory objektov a pravidiel slúžia? Výroková logika má dve stránky - syntaktickú a sémantickú. Základné pojmy výrokovej logiky a pravidlá na vytváranie nových objektov (v prípade výrokovej logiky formúl) určujú syntax výrokovej logiky, axiómy a odvodzovacie pravidlá definujú sémantiku výrokovej logiky. Vo výrokovej logike sú dané elementárne syntakticky správne objekty. Pravidlá na vytváranie nových objektov sú akési gramatické pravidlá, ktoré určujú, čo je vo výrokovej logike formálne správne a čo nie. Umožňujú vytvárať z formálne správnych objektov nové formálne

[4] samozrejme spolu s príslušnými axiómami a odvodzovacími pravidlami, pozri kapitoly 9 a 10

správne objekty výrokovej logiky. Formálne správne vytvorený objekt výrokovej logiky však ešte nemusí mať nijaký zmysel. Zmysel (význam, sémantika) výroku (formuly) je daná jeho pravdivostnou hodnotou. Pojem pravdivosti sa do výrokovej logiky vnáša pomocou vybraných formúl (výrokov), ktoré sa definujú ako základné pravdivé tvrdenia (výroky)—axiómy. Asi by nebolo efektívne budovať matematickú teóriu ako donekonečna sa predlžujúci zoznam pravdivých tvrdení. Schodnejšia cesta je odhaliť základné pravdy a nájsť spôsob, ako porovnávať nové tvrdenia so základnými pravdami. Odvodzovacie pravidlá sú nástrojom na riešenie tohto problému. Sú to presné predpisy, ktoré umožňujú z pravdivých výrokov (zapísaných pomocou formúl) odvodiť ďalšie pravdivé výroky. Neskôr uvidíme, že všetky pravdivé výroky výrokovej logiky možno odvodiť z relatívne malého počtu axióm pomocou jediného odvodzovacieho pravidla, čo zjednodušene povedané znamená, že všetky pravdy výrokovej logiky sú obsiahnuté v malom počte axióm a odvodzovacích pravidlách výrokového počtu. Ako sme už povedali, samotné logické základy teórie hovoria o tom, ako možno od pravdivých tvrdení prejsť k pravdivým tvrdeniam, ale neobsahujú žiadne poznatky o množinách. Aby sme vybudovali teóriu množín, musíme k logickým pojmom pridať pojmy vlastnej matematickej teórie, ako sú množina, prvok množiny, byť prvkom množiny, zjednotenie a prienik množín a pod. Pojmy vlastnej matematickej teórie sa delia na dve skupiny: na základné pojmy a odvodené pojmy. Základné pojmy matematickej teórie zavádzame bez toho aby sme ich popisovali (napr. v teórii množín sú to pojmy množina, prvok množiny a byť prvkom množiny). Odvodené pojmy sú definované pomocou základných pojmov (napríklad pojem podmnožina). Vlastnosti objektov a vzťahy medzi nimi popisujeme v matematickej teórií pomocou tvrdení. Tvrdenia matematickej teórie majú podobu formúl logickej teórie (výrokovej, predikátovej alebo inej logiky) ktorá bola použitá ako logický základ matematickej teórie. V matematickej teórii existuje niekoľko tvrdení popisujúcich základné vlastnosti objektov alebo vzťahy medzi objektami danej matematickej teórie. Tieto tvrdenia nazývame vlastnými axiómami danej matematickej teórie. Výber vlastných axióm matematickej teórie nebýva jednoznačný. Existujú však (našťastie) kritériá, ktoré umožňujú posúdiť, či bol výber vlastných axióm „dobrý“ alebo nie. Podrobnosti možno nájsť v kapitolách 9 a 10.

V matematickej teórii teda máme dva druhy axióm: *axiómy logickej teórie* tvoriace logický základ danej matematickej teórie (nazývané logickými axiómami) a *vlastné axiómy*, ktoré popisujú objekty vlastnej matematickej teórie a vzťahy medzi nimi. Niekedy sa medzi logické axiómy zaraďujú aj axiómy, ktoré nie sú celkom „bezobsažné“ ako axiómy logickej teórie, ale nehovoria nič o objektoch vlastnej matematickej teórie. Typickým príkladom takýchto axióm sú *axiómy rovnosti*.

Z vlastných i logických axióm matematickej teórie možno potom pomocou odvodzovacích pravidiel odvodzovať tvrdenia, ktorých pravdivosť je rovnaká ako pravdivosť východiskových axióm. Tieto tvrdenia sa nazývajú teorémami danej matematickej teórie. Matematickú teóriu tvoria potom základné pojmy (logické i vlastné), odvodzovacie pravidlá, axiómy (logické i vlastné) a teorémy danej matematickej teórie.

Vybudovať axiomaticky nejakú matematickú teóriu nie je ľahká úloha[5]. Axiomatická výstavba, resp. axiomatizácia matematických teórií je predmetom štúdia matema-

[5]A to nehovoríme o problémoch s úplnosťou a bezospornosťou matematických teórií, vyplývajúcich z Godelových teorém

tickej logiky a ďaleko presahuje rámec tejto knihy. Naviac, väčšina matematických teórií sa najmä kvôli čitateľnosti podáva v menej formálnej[6] podobe. Preto sa uspokojíme s tým, že čitateľa naučíme pracovať s tvrdeniami matematických teórií; t.j. naučíme ho rozpoznávať logickú štruktúru matematických tvrdení a základné typy matematických dôkazov. Čitateľovi, ktorý by sa o axiomatických teóriách chcel dozvedieť viac, odporúčame po preštudovaní kapitol 9 a 10 siahnuť po práci [14].

My sa teraz pozrieme detailnejšie na logický aparát matematických teórií. Začneme najjednoduchšou logickou teóriou, výrokovým počtom. V nasledujúcich častiach budeme budovať výrokový počet pomocou pravdivostných tabuliek, budeme skúmať pravdivostné hodnoty formúl a konštruovať všeobecne pravdivé formuly – tautológie. Axiomatickej výstavbe výrokového počtu je venovaná kapitola 9, v ktorej na záver ukážeme, že oba prístupy (odvodzovanie z axióm a konštrukcia tautológií) umožňujú vytvoriť tú istú teóriu.

1.2 Výroky

Výrok je tvrdenie, o ktorého pravdivosti alebo nepravdivosti má význam uvažovať. Výrok je buď pravdivý, alebo je nepravdivý (*princíp dvojhodnotovosti*); t.j. nemôže byť súčasne aj pravdivý aj nepravdivý (*zákon o vylúčení sporu*) ale platí aspoň jedna z týchto dvoch možností (*zákon vylúčenia tretieho*). Pravdivostná hodnota *pravdivý* sa označuje symbolmi 1 alebo T (z anglického true); pravdivostná hodnota *nepravdivý* sa označuje symbolmi 0 alebo F (z anglického false). Pri rozhodovaní o tom, či má nejaké tvrdenie pravdivostnú hodnotu 0 alebo 1; t.j. či tvrdenie je výrokom z hľadiska výrokového počtu nezáleží na tom, akým spôsobom určíme pravdivostnú hodnotu tohto tvrdenia, ba dokonca ani na tom, či pravdivostnú hodnotu tvrdenia vieme určiť. Preto tvrdenia

1. V roku 2017 pristanú ľudia na Marse.
2. Každé párne číslo väčšie ako 2 možno rozložiť na súčet dvoch prvočísel (Goldbachova domnienka).
3. Číslo $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right)$ je iracionálne číslo.

sú výrokmi aj keď o ich pravdivosti nevie zatiaľ nikto rozhodnúť. Všimnite si, že nerozhodnuteľnosť prvého tvrdenia má iný charakter ako nerozhodnuteľnosť ostatných. Na druhej strane tvrdenia tohto typu

1. Modrá je dobrá.
2. Súčasný kráľ USA je černoch.

sú nezmyselné, a preto nie sú výrokmi. Výrokmi však nie sú ani nasledujúce tvrdenia

1. Táto veta je nepravdivá.

[6] aj keď čitatelia môžu mať iný dojem

2. Všetci Kréťania vždy klamú.

pretože im nemožno priradiť pravdivostnú hodnotu. Porozmýšľajte nad tým, čo vyjadruje tvrdenie (1) ak je pravdivé/nepravdivé a čo sa dá povedať o druhom tvrdení v prípade, ak ho vyslovil Kréťan.

Výroky budeme označovať malými písmenami abecedy: $p, q, r, \ldots$. Symboly $p, q, r, \ldots$ používané na označovanie výrokov sa nazývajú výrokovými premennými. Pravdivostnú hodnotu výroku p budeme označovať symbolom $h(p)$. Pripomenieme, že ak je výrok p pravdivý, tak $h(p) = 1$, v opačnom prípade (t.j. ak je výrok p nepravdivý), jeho pravdivostná hodnota je $h(p) = 0$.

Z výrokov možno pomocou logických operácií vytvárať nové výroky. *Logická operácia* je predpis, ktorý jednému alebo niekoľkým výrokom priradí nejaký výrok. Výrok, ktorý bol vytvorený z iných výrokov pomocou nejakej logickej operácie, sa nazýva *zložený výrok*. Výrok, ktorý nie je zložený, sa nazýva *elementárny výrok*. V konečnom dôsledku teda možno všetky zložené výroky redukovať na elementárne výroky pospájané pomocou logických operácií. Existuje viacero logických operácií, na tomto mieste sa budeme zaoberať len niektorými z nich, ktoré sa používajú v matematických dôkazoch.

Najjednoduchší spôsob, ako za daného výroku p vytvoriť nový výrok je poprieť skutočnosť, ktorú výrok p tvrdí, t.j. vyjadriť súhlas s protikladnou (*kontradiktorickou*) skutočnosťou. Výrok q, ktorý je protikladom výroku p nazveme *negáciou výroku* p a budeme ho označovať symbolom $\neg p$. (Negácia sa označuje aj inými spôsobmi, napríklad $p', \overline{p}, \sim p$, non p, v programovacích jazykoch NOT p alebo dokonca aj ako $!p$.) Keďže výrok môže nadobúdať len dve hodnoty (pravdivý 1 a nepravdivý 0), môžeme popísať pravdivostné hodnoty výroku a jeho negácie pomocou tzv. pravdivostnej tabuľky 1.1.[7] *Konjunkcia*

p	$\neg p$
0	1
1	0

Tabuľka 1.1: Pravdivostné hodnoty negovaného výroku

spája výroky p, q do nového výroku p a q. Konjunkciu výrokov p, q zapisujeme $p\&q$. Niekedy sa konjunkcia výrokov p, q nazýva aj *logickým súčinom* a zapisuje sa ako $p.q$ alebo pq. V programovacích jazykoch sa konjunkcia výrokov p, q zapisuje v podobe p AND q, p && q. Konjunkcia $p\&q$ je pravdivá práve vtedy, ak sú pravdivé oba výroky p a q. Pravdivostná tabuľka konjunkcie $p\&q$ je uvedená spolu s pravdivostnými tabuľkami ďalších základných logických operácií v tabuľke 1.2. *Disjunkciu* výrokov p, q zapisujeme výrazom $p \vee q$ (v programovacích jazykoch p OR q alebo $p||q$). Výrok $p \vee q$ čítame ako p alebo q. Disjunkcia $p \vee q$, v technickej literatúre nazývaná aj *logickým súčtom* je pravdivá práve vtedy, ak je pravdivý aspoň jeden z výrokov p, q. Okrem disjunkcie sa niekedy používa aj tzv. *alternatíva* (výlučné alebo, XOR, sčítanie podľa modulo 2, nonekvivalencia). Alternatívu výrokov p, q budeme zapisovať pomocou výrazu $p \oplus q$ a interpretovať nasledovne:„buď platí výrok p, alebo platí výrok q, ale výroky p, q neplatia súčasne.“ Alternatíva $p \oplus q$ je teda pravdivá práve vtedy, ak je pravdivý práve jeden z výrokov p, q.

[7] Kvôli zjednodušeniu označovania sa v záhlaví pravdivostných tabuliek uvádzajú výroky (p) a nie pravdivostné hodnoty výrokov ($h(p)$)

p	q	p&q	$p \vee q$	$p \Rightarrow q$	$p \oplus q$	$p \Leftrightarrow q$
0	0	0	0	1	0	1
0	1	0	1	1	1	0
1	0	0	1	0	1	0
1	1	1	1	1	0	1

Tabuľka 1.2: Pravdivostná tabuľka základných zložených výrokov

V matematických dôkazoch zohráva dôležitú úlohu ďalšia základná logická operácia, implikácia. *Implikácia výrokov* p, q sa zapisuje výrazom $p \Rightarrow q$ a číta sa nasledovne: „ak (platí výrok) p, tak (platí výrok) q“, „z p vyplýva q“ alebo jednoducho „p implikuje q“. Výrok p v implikácii $p \Rightarrow q$ sa nazýva *predpoklad (premisa)* a výrok q je *uzáver (conclusio)* alebo *dôsledok*, ktorý sa v matematike nazýva *tvrdením*. Implikácia je nepravdivá v prípade, keď je pravdivý predpoklad implikácie a nepravdivý jej uzáver. Vo všetkých ostatných prípadoch je implikácia pravdivá. Pozri pravdivostnú tabuľku implikácie 1.2.

Poslednou zo základných logických operácií je *ekvivalencia*. Ekvivalenciu výrokov p, q zapisujeme výrazom $p \Leftrightarrow q$ ($p \sim q$, $p \equiv q$) a čítame ako „p je ekvivalentné s q“, „p (platí) práve vtedy keď (platí) q“, „p (platí) vtedy a len vtedy keď (platí) q“. Ekvivalencia $p \Leftrightarrow q$ platí práve vtedy, keď majú oba výroky p a q rovnakú pravdivostnú hodnotu; t.j. keď sú oba súčasne pravdivé, alebo oba súčasne nepravdivé. Výroky p, q, ktoré majú rovnakú pravdivostnú hodnotu sa nazývajú *logicke rovnocenné (ekvivalentné)*. To, že výroky majú rovnakú pravdivostnú hodnotu, znamená, že jeden z nich môže byť napríklad v nejakom zloženom výroku nahradený druhým bez toho, aby sa pravdivostná hodnota zloženého výroku zmenila. To že sú nejaké dva výroky logicky ekvivalentné, nemusí ešte znamenať, že majú rovnaký (sémantický) význam. Napríklad výroky „4. júla 2004 bola nedeľa“ a „$\pi > 3$“ sú pravdivé a teda sú to ekvivalentné výroky, ktoré však na prvý pohľad majú rozličný zmysel. Ekvivalencia výrokov má význam pri úpravách výrokov. Napríklad pri zisťovaní pravdivostnej hodnoty nejakého veľmi zložitého výroku môžeme postupne nahrádzať výroky z ktorých pozostáva, ekvivalentnými jednoduchšími výrokmi, až sa nakoniec dostaneme k výroku, ktorého pravdivostnú hodnotu vieme určiť.

Predpokladáme, že vieme určiť pravdivostné hodnoty elementárnych výrokov. Pravdivostné hodnoty zložených výrokov je potom možné určiť na základe pravdivostných hodnôt elementárnych výrokov, z ktorých daný zložený výrok pozostáva. Podľa toho, aké pravdivostné hodnoty nadobúda výrok, rozlišujeme tri možnosti:

1. výroky, ktoré nadobúdajú obe pravdivostné hodnoty 1 a 0. Takéto výroky nemajú špeciálne pomenovanie.

2. Výroky, ktoré pre všetky možné pravdivostné hodnoty svojich elementárnych výrokov nadobúdajú pravdivostnú hodnotu 1. Takéto výroky sa nazývajú *tautológie*.

3. Výroky, ktoré pre všetky možné pravdivostné hodnoty svojich elementárnych výrokov nadobúdajú pravdivostnú hodnotu 0. Takéto výroky sa nazývajú *kontradikcie*.

Pri matematických dôkazoch nás budú zaujímať najmä tautológie, resp. podmienky, za ktorých budú výroky nadobúdať pravdivostnú hodnotu 1. Uvedieme teraz niektoré

významné tautológie, ktoré budeme v ďalšom výklade používať. Predpokladáme, že p, q, r označujú ľubovoľné výroky (výrokové premenné); symbol 0 označuje ľubovoľnú kontradikciu a symbol 1 ľubovoľnú tautológiu. Za týchto predpokladov sú nasledujúce výroky tautológie

1. $(p \vee p) \equiv p$ idempotentosť (rovnomocnosť) disjunkcie
2. $(p\&p) \equiv p$ idempotentosť (rovnomocnosť) konjunkcie
3. $(p\&q) \equiv (q\&p)$ komutatívnosť
4. $(p \vee q) \equiv (q \vee p)$
5. $(p \equiv q) \equiv (q \equiv p)$
6. $(p \vee (q \vee r)) \equiv ((p \vee q) \vee r)$ asociatívnosť disjunkcie
7. $(p\&(q\&r)) \equiv ((p\&q)\&r)$ asociatívnosť konjunkcie
8. $(p \vee (q\&r)) \equiv ((p \vee q)\&(p \vee r))$ distributívne zákony
9. $(p\&(q \vee r)) \equiv ((p\&q) \vee (p\&r))$
10. $(p\&(p \vee r)) \equiv p)$ absorbčné zákony
11. $(p \vee (p\&r)) \equiv p)$
12. $(\neg\neg p) \equiv p$ zákon dvojitej negácie
13. $p \vee (\neg p)$ zákon vylúčenia tretieho
14. $\neg(p\&(\neg p))$ vylúčenie sporu
15. $\neg(p\&q) \equiv ((\neg p) \vee (\neg q))$ de Morganov zákon
16. $\neg(p \vee q) \equiv ((\neg p)\&(\neg q))$ de Morganov zákon
17. $(\neg p \Rightarrow \neg q) \equiv (q \Rightarrow p)$ kontrapozícia negácie
18. $(p \equiv q) \equiv ((p \Rightarrow q)\&(q \Rightarrow p))$
19. $(p\&q) \equiv \neg((\neg p) \vee (\neg q))$
20. $(p \vee q) \equiv \neg((\neg p)\&(\neg q))$
21. $(p \Rightarrow q) \equiv ((\neg p) \vee q)$
22. $p \Rightarrow (p \Rightarrow q)$
23. $((\neg p) \Rightarrow p) \Rightarrow p$ reductio ad absurdum
24. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
25. $(\neg p \Rightarrow \neg q) \Rightarrow ((\neg p \Rightarrow q) \Rightarrow p)$

26. $(p\&q) \Rightarrow p$
27. $(p\&q) \Rightarrow q$
28. $p \Rightarrow (p \vee q)$
29. $q \Rightarrow (p \vee q)$
30. $(p \Rightarrow q) \Rightarrow ((p \Rightarrow r) \Rightarrow (p \Rightarrow (q\&r)))$
31. $p \Rightarrow (q \Rightarrow (p\&r))$
32. $(p \Rightarrow r) \Rightarrow (q \Rightarrow r) \Rightarrow (p \vee q) \Rightarrow r)$
33. $(p\&\neg p) \equiv 0$
34. $(p \vee \neg p) \equiv 1$
35. $(p\&1) \equiv p$
36. $(p\&0) \equiv 0$
37. $(p \vee 0) \equiv p$
38. $(p \vee 1) \equiv 1$
39. $(p \Rightarrow 0) \equiv \neg p$
40. $(p \Rightarrow 1) \equiv 1$
41. $(1 \Rightarrow p) \equiv p$
42. $p \Rightarrow p) \equiv 1$
43. $p \Rightarrow \neg p) \equiv 1\neg p$
44. $(p \equiv q) \Rightarrow (\neg p \equiv \neg q)$
45. $(p \equiv q) \Rightarrow ((p\&r) \equiv (q\&r))$
46. $(p \equiv q) \Rightarrow ((p \vee r) \equiv (q \vee r))$
47. $(p \equiv q) \Rightarrow ((p \Rightarrow r) \equiv (q \Rightarrow r))$
48. $(p \equiv q) \Rightarrow ((r \Rightarrow p) \equiv (r \Rightarrow q))$
49. $(p \equiv q) \Rightarrow (p \Rightarrow q)$
50. $(p \equiv q) \Rightarrow (q \Rightarrow p)$

Úloha 1.1. *Dokážte pomocou pravdivostných tabuliek, že výroky 1-43 sú tautológie!*

Úloha 1.2. *Vprogramovacích jazykoch sa zvyčajne nevyskytuje operátor implikácie. Ako by ste vyjadrili implikáciu* $p \Rightarrow p)$ *pomocou výrokov* p, q *a logických operátorov AND, OR a NOT?*

Úloha 1.3. *Zistite, či pre implikáciu a negáciu platia asociatívne a komutatívne zákony!*

Úloha 1.4. *Preskúmajte vzťahy medzi implikáciou, akvivalenciou a ostatnými elementárnymi logickými operáciami!*

1.3 Výrokové formy a kvantifikované výroky

V matematike sa neraz stretávame s tvrdeniami, ktoré majú formu výroku, ale pritom nie sú výrokmi, pretože namiesto tvrdenia o nejakom objekte alebo množine objektov tvrdia niečo o nejakej neznámej veličine (napr. premennej x), a toto tvrdenie nie je možné bez znalosti hodnôt danej premennej overiť. Ak však za premennú x dosadíme vhodný objekt, alebo inak konkretizujeme množinu hodnôt, ktoré môže premenná x nadobúdať, dostávame výrok. Takéto formuly nazývame *výrokovými formami*, alebo *výrokovými funkciami*.

Príklad 1.1. *Nasledujúce výrazy sú výrokové formy*

- x *je prvočíslo*
- $x > 3$
- $5 \in x$
- x *nezískal olympijskú medailu*

Pre každú výrokovú formu existuje nejaká množina objektov, M, ktoré má zmysel do výrokovej formy dosadzovať. Označme výrazom $a(x)$ výrokovú formu definovanú na množine prirodzených čísel napríklad takto:

$$a(x) \quad \Longleftrightarrow x > 3.$$

Dosadzovaním prirodzených čísel do výrokovej formuly $a(x)$ dostávame výroky:

$$\begin{array}{lcl} a(1) & \Longleftrightarrow & 1{>}3 \\ a(2) & \Longleftrightarrow & 2{>}3 \\ a(3) & \Longleftrightarrow & 3{>}3 \\ a(4) & \Longleftrightarrow & 4{>}3 \\ a(5) & \Longleftrightarrow & 5{>}3 \\ & \dots & \end{array}$$

Dá sa ľahko vidieť, že prvé tri výroky z vyššie uvedeného zoznamu výrokov sú nepravdivé a všetky ostatné sú pravdivé. Z výrokovej formy môžeme dostať výrok nielen dosadením konkrétnych objektov za premenné, ale aj tým, že určíme (kvantifikujeme) pre aké množstvo (koľko)[8] prvkov množiny M predstavuje po dosadení výroková forma pravdivý výrok.

Príklad 1.2. *Využijeme výrokovú formu z predchádzajúceho príkladu a vytvoríme (zatiaľ menej formálnym spôsobom) dva výroky:*

1. *existuje* x $(x > 3)$,
2. *pre všetky* x $(x > 3)$.

[8] Ak výroková forma obsahuje viacero premenných, tak použitím rozličných kvantifikátorov na tieto premenné nebudeme špecifikovať len počty prvkov, ale aj vzťahy medzi nimi

Tieto tvrdenia chápeme nasledovne:

1. V množine prirodzených čísel $\mathbb{N}$ (na ktorej je výroková forma $a(x)$ definovaná), existuje (nájdeme) aspoň jeden prvok (napríklad $x = 13$) taký, že po dosadení daného prvku za premennú x vo výrokovej formule $a(x)$ je výsledný výrok $a(13)$pravdivý. Keďže skutočne $13 > 3$, existuje x $(x > 3)$ a výrok existuje x $(x > 3)$, je pravdivý.
2. V druhom prípade musí byť tvrdenie $(x > 3)$ splnené pre všetky prirodzené čísla. Keďže tvrdenie $(x > 3)$ nie je splnené pre hodnoty $0, 1, 2, 3$, výrok „pre všetky x $(x > 3)$“ má pravdivostnú hodnotu 0.

Výroky uvedeného typu nazývame *kvantifikovanými výrokmi*. Slovné spojenia „existuje“, „pre všetky“ budeme zapisovať pomocou symbolov, ktoré sa nazývajú *kvantifikátory*:

- „existuje“ $\ldots\exists\ldots$ existenčný (malý) kvantifikátor,
- „pre všetky“$\ldots\forall\ldots$ všeobecný (veľký) kvantifikátor.

Výroková forma môže obsahovať viac rozličných premenných, a preto zo zápisu kvantifikovaného výroku musí byť jasné, na akú premennú sa kvantifikátor vzťahuje. Preto sa za kvantifikátorom v kvantifikovanom výroku uvádza aj premenná. Formálne korektne zapísané kvantifikované výroky z príkladu 1.2 budú vyzerať takto:

1. existuje x $(x > 3)$ $\quad \exists x((x \in \mathbb{N})\&(x > 3))$,
2. pre všetky x $(x > 3)$ $\quad \forall x((x \in \mathbb{N}) \Rightarrow (x > 3))$.

Ak je zrejmé, pre ktoré hodnoty premennej x je daná výroková forma $b(x)$ definovaná, budeme namiesto podrobného zápisu kvantifikovaných výrokov používať len skrátenú formu zápisu: $\forall x\ b(x)$ a $\exists x\ b(x)$.

Poznámka. Predpokladajme, že nejaká výroková forma $a(x)$ je definovaná na množine $\mathbb{N}_n = \{0, 1, \ldots, n\}$. [9] Potom kvantifikované výroky $\forall x\ a(x)$ a $\exists x\ a(x)$ možno vyjadriť aj takto:

$$\forall x\ a(x) \quad \equiv \quad (a(0)\&a(1)\&\ldots\&a(n)\&1)\,, \tag{1.1}$$

$$\exists x\ a(x) \quad \equiv \quad (a(0) \vee a(1) \vee \cdots \vee a(n) \vee 0)\,. \tag{1.2}$$

Je potrebné uvedomiť si, že symboly $0, 1$ vo vyššie uvedených výrazoch majú dvojaký význam. Symbol 1 ako samostatný člen konjunkcie predstavuje ľubovoľnú tautológiu a podobne symbol 0 ako samostatný člen disjunkcie predstavuje ľubovoľnú kontradikciu. Vo výrokoch $(a(0), a(1)$ však symboly $0, 1$ predstavujú prirodzené čísla. Pomocou predchádzajúcich formúl môžeme ľahko určiť pravdivostné hodnoty kvantifikovaných výrokov $\forall x\ a(x), \exists x\ a(x)$ aj v prípade, keď je množina hodnôt premennej x prázdna.

[9] Výber množiny $\mathbb{N}_n$ nie je podstatný, rovnako dobre by sme mohli použiť ľubovoľnú množinu s konečným počtom prvkov.

Úloha 1.5. *Aký význam budú mať výroky* $\forall x\ a(x), \exists x\ a(x)$ *v prípade, keď premenná* x *nadobúda hodnoty z prázdnej, resp. jednoprvkovej množiny?*

Nad kvantifikovanými výrokmi možno robiť podobné operácie, ako nad „obyčajnými" výrokmi. Jedna z týchto operácií si zasluhuje zvláštnu pozornosť; negácia kvantifikovaných výrokov. Predpokladajme, že $a(x)$ je ľubovoľná výroková forma. Potom platí

- $\neg(\forall x\ a(x)) \equiv \exists x(\neg a(x))$, *pravidlo negácie všeobecného kvantifikátora*
- $\neg(\exists x\ a(x)) \equiv \forall x(\neg a(x))$ *pravidlo negácie existenčného kvantifikátora*

To znamená, že jeden kvantifikátor môžeme vyjadriť pomocou negácie a druhého kvantifikátora: $(\exists x a(x)) \equiv \neg(\forall x\ \neg a(x))$, a $(\forall x\ a(x)) \equiv \neg\exists x(\neg a(x))$. Ilustrujeme uvedené poznatky na príklade.

Príklad 1.3. *Prvočíslo je prirodzené číslo, ktoré je bezo zvyšku možné deliť len jednotkou a ním samým.*[10] *Nech* $P(x)$ *označuje výrokovú formu „*x *je prvočíslo" definovanú na množine prirodzených čísel. Budeme pracovať s kvantifikovaným výrokom* $\exists x\ P(x)$*, ktorý tvrdí, že existuje aspoň jedno prirodzené číslo, ktoré je prvočíslo. Zapíšeme výrok* $\exists x\ P(x)$ *formálne:*

$$\exists x\ P(x): \qquad \exists x[(x \in \mathbb{N})\&P(x)]$$

negujeme ho a budeme ho upravovať (nahrádzať postupne výroky ekvivalentnými výrokmi):

$$\neg\exists x[(x \in \mathbb{N})\&P(x)] \equiv \forall x\neg[(x \in \mathbb{N})\&P(x)].$$

Použili sme pravidlo negácie existenčného kvantifikátora. Teraz použijeme de Morganov zákon:

$$\forall x\neg[(x \in \mathbb{N})\&P(x)] \equiv \forall x[\neg(x \in \mathbb{N}) \vee \neg P(x)].$$

Výroková forma $P(x)$ *je definovaná len pre prirodzené čísla. Ak je preto pre nejakú hodnotu* x_0 *výrok* $\neg(x_0 \in \mathbb{N})$ *pravdivý, tak potom výroková forma* $P(x)$ *nie je pre hodnotu* x_0 *definovaná. To znamená, že ak má byť disjunkcia* $[\neg(x \in \mathbb{N}) \vee \neg P(x)]$ *pravdivá pre nejakú hodnotu* x_0*, musí byť výrok* $\neg(x_0 \in \mathbb{N})$ *nepravdivý; disjunkcia* $[\neg(x \in \mathbb{N}) \vee \neg P(x)]$ *je pre* $x_0 \in \mathbb{N}$*) ekvivalentá disjunkcii* $[0 \vee \neg P(x_0)]$ *resp.* $[\neg P(x_0)]$*. Ešte by sme mohli využiť ekvivalenciu* $p \equiv (1\&p)$*;* $\neg P(x_0) \equiv ((x \in \mathbb{N})\&\neg P(x_0))$*. Po tejto úprave dostávame konečnú podobu negovaného výroku:*

$$\neg\exists x[(x \in \mathbb{N})\&P(x)] \equiv \forall x((x \in \mathbb{N})\&\neg P(x_0))$$

Vyjadrené slovne - to, že nie je pravda, že existuje prirodzené číslo, ktoré je prvočíslom, je ekvivalentné tomu, že žiadne prirodzené číslo nie je prvočíslo.

Pozrime sa ešte na negáciu výroku obsahujúceho všeobecný kvantifikátor. Uvažujme kvantifikovaný výrok

$$\forall x P(x): \qquad \forall x[(x \in \mathbb{N}) \Rightarrow P(x)],$$

[10] najmenšie prvočísla sú $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

ktorý tvrdí zjavnú nepravdu, že každé prirodzené číslo je prvočíslo. Negujeme tento výrok a postupnými úpravami dostávame

$$\neg\forall x[(x \in \mathbb{N}) \Rightarrow P(x)] \equiv \exists x[(x \in \mathbb{N})\&\neg P(x)].$$

Vyjadrené slovne: „existuje prirodzené číslo, ktoré nie je prvočíslom". Toto tvrdenie je zjavne pravdivé.

Úloha 1.6. *Napíšte aspoň 5 rozličných výrokových foriem, vytvorte z nich kvantifikované výroky a negujte ich. Potom vyjadrite slovne obsah negovaných tvrdení.*

Úloha 1.7. *Pre ľubovoľné výrokové formy* $a(x), b(x)$ *sú nasledujúce kvantifikované výroky tautológiami*

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

$$\exists x[a(x) \Rightarrow b(x)] \Rightarrow [\forall x a(x) \Rightarrow \exists x b(x)]$$

Zistite, či sú tautológiami aj opačné implikácie

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

$$[\forall x a(x) \Rightarrow \exists x b(x)] \Rightarrow \exists x[a(x) \Rightarrow b(x)]$$

Návod: ak sa vám nepodarí dokázať, že opačné implikácie sú tautológie, skúste nájsť také výrokové formy $a(x), b(x)$*, pre ktoré uvedené kvantifikované výroky nie sú tautológie.*

Úloha 1.8. *Zistite, či sú nasledujúce kvantifikované výroky tautológiami:*

$$\begin{aligned}
\forall x a(x) &\Rightarrow \exists x a(x) \\
\exists x a(x) &\Rightarrow \forall x a(x) \\
\exists x[a(x) \Rightarrow b(x)] &\Rightarrow [\exists x a(x) \Rightarrow \exists x b(x)] \\
\forall x[a(x) \Rightarrow b(x)] &\Rightarrow [\forall x a(x) \Rightarrow \forall x b(x)]
\end{aligned}$$

Doteraz sme pracovali s výrokovými formami, ktoré obsahovali jednu premennú. Výrokové formy však môžu obsahovať aj viacero premenných. Napríklad $gt(x, y)$ označuje $(x > y)$, $fs(x, y)$ bude označovať výrokovú formu „x je otcom y", $sum(x, y, z)$ znamená $z = x + y$ a podobne. Ostaňme pri výrokových formách o dvoch premenných a pozrime sa na to, aké rozličné kvantifikované výroky z nich môžeme dostať pomocou rozličných kvantifikátorov. Nech $\phi(x, y)$ je ľubovoľná výroková forma, potom pomocou kvantifikátorov z nej môžeme vytvoriť týchto 8 kvantifikovaných výrokov:

1. $\forall x \forall y \phi(x, y)$ $\quad P_1$
2. $\forall x \exists y \phi(x, y)$ $\quad P_2$
3. $\exists x \forall y \phi(x, y)$ $\quad P_3$
4. $\exists x \exists y \phi(x, y)$ $\quad P_4$
5. $\forall y \forall x \phi(x, y)$ $\quad P_5$

6. $\forall y \exists x \phi(x, y)$ P_6
7. $\exists y \forall x \phi(x, y)$ P_7
8. $\exists y \exists x \phi(x, y)$ P_8

Úloha 1.9. *Zostrojte 5 rozličných príkladov výrokovej formy* $\phi(x, y)$. *Presvedčte sa, že kvantifikované výroky sú viazané nasledujúcimi vzťahmi*

$$\begin{array}{rccc} & P_3 \Rightarrow & P_6 & \\ & \Uparrow & \Downarrow & \\ P_1 \equiv & P_5 & P_4 & \equiv P_8 \\ & \Downarrow & \Uparrow & \\ & P_7 \Rightarrow & P_2 & \end{array}$$

a že žiadnu implikáciu v schéme nie je možné nahradiť ekvivalenciou.

Teraz, keď sme už získali isté predstavy o matematickej logike, môžeme sa pozrieť, ako sa dokazujú matematické tvrdenia; t.j. na problematiku matematických dôkazov.

1.4 Matematické dôkazy

Predpokladáme, že čitateľ má aspoň intuitívnu predstavu o tom, ako vyzerá matematický dôkaz. Ak nie, tak na začiatok stačí, ak si pod matematickým dôkazom tvrdenia B bude predstavovať postupnosť tvrdení $A_1, A_2, \ldots, A_n$, kde A_i, $i = 1, \ldots, n$ sú výroky alebo výrokové formy také, že implikácie $A_1 \Rightarrow A_2, A_2 \Rightarrow A_3 \Rightarrow, \ldots, A_{n-1} \Rightarrow A_n, A_n \Rightarrow B$ sú tautológie. Jedným z našich cieľov je upresniť túto intuitívnu predstavu a naučiť čitateľa niektorým štandardným postupom, ktoré sa používajú pri dôkazoch matematických tvrdení. V tejto kapitole uvedieme základné typy deduktívnych matematických dôkazov, a to

1. priame dôkazy,
2. nepriame dôkazy,
3. dôkazy matematickou indukciou.

Ďalšie kapitoly tejto knihy poskytnú čitateľovi dostatok príležitostí na precvičenie získaných teoretických poznatkov o matematických dôkazoch. Problematiku matematických dôkazov uzatvoríme v kapitolách 9, 10 kde sa okrem iného budeme zaoberať aj odvodzovaním (dokazovaním) tvrdení v axiomatických teóriách.

Vo všetkých typoch deduktívnych dôkazov potrebujeme mať k dispozícii odvodzovacie pravidlá, ktoré nám umožnia prejsť od pravdivých tvrdení k novým pravdivým tvrdeniam. Najdôležitejším odvodzovacím pravidlom, ktoré budeme často používať, je tzv. *pravidlo odlúčenia, modus ponens,* ktoré zapíšeme v nasledujúcom tvare

$$\frac{A \Rightarrow B, A}{B}.$$

Zmysel pravidla modus ponens je nasledujúci—ak platia výroky napísané nad čiarou (tzv. predpoklady), tak potom musí platiť aj záver, t.j. výrok B. Ľahko si to overíme pomocou pravdivostnej tabuľky implikácie

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

Vidíme, že oba predpoklady $A, A \Rightarrow B$ platia len v tom prípade, keď platí aj B. Pravidlo modus ponens možno zapísať aj v nasledujúcom tvare:

$$\frac{\neg B \Rightarrow \neg A, \neg B}{\neg A}.$$

Ak na implikáciu v predpoklade použijeme kontrapozíciu negácie, dostávame pravidlo nazývané *modus tolens*

$$\frac{A \Rightarrow B, \neg B}{\neg A}.$$

Ďalšie dôležité pravidlo odvodenia je *pravidlo sylogizmu,* ktoré umožňuje skracovať dlhé reťazce implikácií v dôkaze:

$$\frac{A \Rightarrow B, B \Rightarrow C}{A \Rightarrow C}.$$

Úloha 1.10. *Presvedčte sa o platnosti pravidiel modus ponens, modus tolens a pravidla sylogizmu pomocou pravdivostnej tabuľky.*

1.4.1 Priamy dôkaz

Pri priamom dôkaze matematického tvrdenia (vety) B postupujeme tak, že prijmeme nejaké predpoklady[11] napr. A (t.j. prehlásime tvrdenie A za pravdivé) a potom vytvoríme konečnú postupnosť tvrdení (výrokov) $A_1, \dots A_n$ takých, že

$$A \Rightarrow A_1, A_1 \Rightarrow A_2, \dots A_{n-1} \Rightarrow A_n, A_n \Rightarrow B.$$

Teraz použijeme n-krát pravidlo sylogizmu a dostávame:

$$\frac{A \Rightarrow A_1, A_1 \Rightarrow A_2}{A \Rightarrow A_2}, \frac{A \Rightarrow A_2, A_2 \Rightarrow A_3}{A \Rightarrow A_3}, \dots, \frac{A \Rightarrow A_n, A_n \Rightarrow B}{A \Rightarrow B}$$

Predpokladali sme však platnosť A, a preto z odvodeného tvrdenia (implikácie) $A \Rightarrow B$ pomocou pravidla modus ponens dostávame potrebný záver:

$$\frac{A, A \Rightarrow B}{B}.$$

[11] množina predpokladov môže byť aj prázdna

Poznámka. Pri dokazovaní matematických tvrdení je potrebné dávať pozor na predpoklady. Nie všetky predpoklady totiž bývajú formulované explicitne, niektoré vyplývajú z kontextu, iné sa považujú za zrejmé.

Ilustrujeme použitie priameho dôkazu na príklade. Dokážeme jednoduché tvrdenie o prirodzených číslach.

Príklad 1.4. *Ak je* x *párne prvočíslo, tak potom nie je deliteľné tromi.*

1. *Ak je* x *párne prvočíslo, tak je párne číslo a zároveň prvočíslo.*
2. *Ak je* x *párne číslo, tak je deliteľné číslom* 2*.*
3. *Ak je* x *prvočíslo, tak je deliteľné práve dvoma číslami* 1 *a* x*.*
4. *Číslo* x *má práve dvoch deliteľov, a preto* $1 = 2$ *alebo* $2 = x$*.*
5. *Keďže* $1 \neq 2$*,* $2 = x$*.*
6. *Číslo* x $(= 2)$ *má deliteľov* $1, 2$*.*
7. *Keďže* $3 \neq 2$ *ani* $3 \neq 1$*, číslo* x *nie je deliteľné číslom* 2*.*

1.4.2 Nepriamy dôkaz

Predpokladáme, že je pravdivý predpoklad A a že potrebujeme odvodiť tvrdenie B. Ak by sa nám podarilo odvodiť implikáciu $A \Rightarrow B$, tak môžeme použiť pravidlo *modus ponens* a z predpokladu A a odvodenej implikácie $A \Rightarrow B$ odvodíme platnosť tvrdenia B. Odvodenie implikácie $A \Rightarrow B$ však môže naraziť na ťažkosti. Skúsime preto dôkaz „otočiť“ namiesto implikácie $A \Rightarrow B$ odvodiť k nej ekvivalentné tvrdenie $\neg B \Rightarrow \neg A$. Medzi predpoklady zaradíme tvrdenie $\neg B$[12] a odvodíme, že je nepravdivý výrok A (*reductio ad absurdum*). Dokázali sme teda tvrdenie $\neg B \Rightarrow \neg A$, ktoré je kontrapozíciou negácie $A \Rightarrow B$. Z tvrdení A, $A \Rightarrow B$ potom pomocou pravidla *modus ponens* vyplýva platnosť tvrdenia B. Nepriamy dôkaz sa však prakticky končí odkazom na *spor*, kedy na základe negovaného tvrdenia $\neg B$ získavame očividne nepravdivé[13] tvrdenie $(\neg A)$. Posledné dva kroky; kontrapozícia negácie $\neg B \Rightarrow \neg A \equiv A \Rightarrow B$ a následne použitie pravidla modus ponens sa už nezvyknú robiť a priamo sa odvodzuje záver o platnosti tvrdenia B. Negácia tvrdenia, ktoré chceme dokázať (B) sa nazýva *antitéza*. Dôkazy, ktoré vedú k sporu sa nazývajú *dôkazy sporom*.

Efektívnosť nepriamych dôkazov je podstatne ovplyvnená tým, že sa k daným predpokladom pridal predpoklad o nepravdivosti toho tvrdenia, ktoré sa má dokázať; potom sa pri dôkaze vychádza z väčšieho počtu predpokladov. Vďaka tomu sú nepriame dôkazy mnohých matematických tvrdení ľahšie ako priame dôkazy. Ilustrujeme nepriamy dôkaz na jednoduchom príklade.

[12] predpoklady teda sú $A, \neg B$

[13] medzi predpokladmi je aj A!

Príklad 1.5. *Dokážeme tvrdenie z predchádzajúceho príkladu nepriamo (sporom). Aby sme uštrili priestor, uvedieme hlavnú myšlienku dôkazu a jej podrobné rozvedenie ponecháme čitateľovi. Predpokladáme, že platí:*

„x *je párne prvočíslo“ a zároveň negáciu pôvodného tvrdenia, t.j.„*x *je deliteľné číslom* 3*“ .*

podobne ako pri priamom dôkaze rozoberieme podrobne prvé tvrdenie:

1. x *je párne číslo, to znamená, že* x *je deliteľné číslom* 2*;*

2. x *je prvočíslo, to znamená, že* x *má práve dvoch deliteľov, a síce čísla* $1, x$*.*

3. *Podmienky (1) a (2) môžu platiť súčasne len v tom prípade, ak je jedno z čísel* $1, x$ *rovné* 2*. Keďže zrejme* $1 \neq 2$*, musí platiť* $x = 2$*.*

Číslo 2 *však nie je deliteľné číslom* 3*, a to je hľadaný spor s druhým predpokladom („x je deliteľné tromi“). To znamená, že aspoň jeden z predpokladov je nepravdivý; ak trváme na pravdivosti prvého predpokladu („*x *je párne prvočíslo“), musí byť nepravdivý druhý predpoklad, a teda musí platiť jeho negácia; „*x *nie je deliteľné tromi“.*

Uvedieme v krátkosti ďalšie schémy nepriameho dôkazu; už spomínané *Reductio ad absurdum* vyzerá nasledovne:

$$\frac{\neg A \Rightarrow A}{A}.$$

(Vyjadrené slovne: ak z negácie tvrdenia možno odvodiť dané tvrdenie, tak potom je dané tvrdenie pravdivé.)

1.4.3 Nepriame dôkazy implikácií

Mnohé matematické tvrdenia majú tvar implikácie $A \Rightarrow B$. Pravdivosť tejto implikácie môžeme nepriamo dokázať tak, že dokazujeme platnosť ekvivalentného tvrdenia $\neg B \Rightarrow \neg A$ a potom použijeme tautológiu (17). Iná možnosť dôkazu implikácie $A \Rightarrow B$ spočíva v tom, že predpokladáme platnosť negácie pôvodnej implikácie; t.j. $\neg(A \Rightarrow B)$ a snažíme sa odvodiť spor. Využijeme ekvivalencie (21) a (16) a namiesto negácie implikácie $\neg(A \Rightarrow B)$ budeme predpoklad $\neg(A \Rightarrow B)$ formulovať v tvare konjunkcie $A\&\neg B$. Úspešne zavŕšený dôkaz skončí jedným z troch nasledujúcich spôsobov:

1. odvodíme $\neg A$; t.j. dostaneme spor s predpokladom A (spor s antitézou)

2. odvodíme B; t.j. dostaneme spor s predpokladom $\neg B$ (spor s antitézou)

3. odvodíme nejaké dve navzájom si odporujúce tvrdenia $C, \neg C$.

Poznámka. Pri prvom čítaní možno nasledujúcu časť vynechať a pokračovať v čítaní rozlišovacou metódou.

Aby sme dokázali platnosť implikácie $A \Rightarrow B$ budeme v jednotlivých prípadoch postupovať nasledovne (predpokladáme, že predpoklad A implikácie $A \Rightarrow B$ je pravdivý. V opačnom prípade (A je nepravdivé tvrdenie) by sme skončili s dokazovaním veľmi rýchlo, pretože z nepravdivého predpokladu vyplynie ľubovoľný záver; resp. tvrdenie $A \Rightarrow B$ je pre nepravdivé A tautológiou).

1. V prvom prípade sme dokázali platnosť implikácie

   $$\neg(A \Rightarrow B) \Rightarrow \neg A.$$

   Použijeme kontrapozíciu negácie a odvodíme platnosť tvrdenia

   $$A \Rightarrow (A \Rightarrow B).$$

   Napokon využijeme predpoklad A a pomocou pravidla modus ponens odvodíme implikáciu $A \Rightarrow B$

2. V druhom prípade sme odvodili

   $$\neg(A \Rightarrow B) \Rightarrow B.$$

   Pomocou tautológiue (22) a pravidla sylogizmu odvodíme

   $$\frac{\neg(A \Rightarrow B) \Rightarrow B, B \Rightarrow (A \Rightarrow B)}{\neg(A \Rightarrow B) \Rightarrow (A \Rightarrow B)}.$$

   Napokon použijeme metódu *reductio ad absurdum* a dostávame

   $$\frac{\neg(A \Rightarrow B) \Rightarrow (A \Rightarrow B), \neg(A \Rightarrow B) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow B)}{(A \Rightarrow B)}.$$

3. V treťom prípade sme odvodili (pozri tautológiu (30)) tvrdenie

   $$\neg(A \Rightarrow B) \Rightarrow (C \& \neg C).$$

   Teraz použijeme kontrapozíciu negácie a „otočíme“ odvodenú formulu

   $$\neg(C \& \neg C) \Rightarrow (A \Rightarrow B).$$

   Predpoklad poslednej implikácie upravíme pomocou de Morganovho pravidla:

   $$\neg(C \& \neg C) \equiv (\neg C \vee C).$$

   Tvrdenie $(\neg C \vee C)$ je tautológia (13), a preto môžeme opäť použiť pravidlo modus ponens

   $$\frac{\neg(C \& \neg C) \Rightarrow (A \Rightarrow B), \neg(C \& \neg C)}{A \Rightarrow B}.$$

Úloha 1.11. *Doplňte a sformalizujte dôkazy uvedené v predchádzajúcom príklade !*

1.4.4 Rozlišovacia metóda

Ak je množina hodnôt, ktoré možno dosadzovať za premenné vo výrokových formulách, konečná, tak potom možno overiť pravdivosť kvantifikovaných výrokov postupným dosadením konečného počtu prvkov do výrokovej formuly (pozri vzťahy 1.1, 1.2). Takéto dôkazy sa nazývajú *verifikácie*. Keď sa všetky možnosti rozdelia do rozličných skupín a dôkaz sa spraví pre každú skupinu, hovoríme o *rozlišovaní prípadov*, alebo o *rozlišovacej metóde*. Pri použití rozlišovacej metódy je dôležité, aby sa pri rozdeľovaní prípadov do skupín nezabudlo na žiaden prípad.

To, že je množina možných hodnôt premennej výrokovej formuly konečná, nemusí ešte znamenať, že je možné použiť rozlišovaciu metódu. Použitie rozlišovacej metódy aj pri niektorých pomerne „jednoduchých“ problémoch naráža na ťažkosti spojené s príliš veľkým počtom prípadov, ktoré treba uvažovať. Príklady takýchto úloh sú šach, resp. úloha nájsť vyhrávajúcu postupnosť ťahov z danej pozície; zisťovanie toho, či je číslo $2^{2^{13}-1}-1$ prvočíslo, hľadanie kryptografického (šifrovacieho) kľúča úplným preberaním množiny všetkých možných kľúčov, zisťovanie, či je zložený výrok s n výrokovými premennými tautológia a pod.

Kým pravdivosť nejakého tvrdenia kvantifikovaného všeobecným kvantifikátorom sa (niekedy) dokazuje ťažko, pravdivosť takéhoto tvrdenia možno vyvrátiť nájdením jediného prípadu, v ktorom dané tvrdenie neplatí; t.j. nájdením tzv. *kontrapríkladu*: výrok $\forall x(x \in M \Rightarrow P(x)$, ktorý tvrdí, že každý prvok množiny M má vlastnosť P vyvrátime, ak v množine M nájdeme prvok x_0, ktorý vlastnosť P nemá.

Hľadanie kontrapríkladov patrí k základným metódam práce matematika. Matematik najprv preskúma neznáme skutočnosti pomocou príkladov, potom o nich formuluje všeobecnejšie tvrdenia, ktoré sa snaží vyvrátiť pomocou kontrapríkladov; ak sa mu to podarí, hľadá doplňujúce podmienky pre platnosť vyslovených tvrdení, resp. preformuluje dané tvrdenia tak, aby neboli logicky vyvrátiteľné. Toto je spôsob, akým sa často vytvárajú matematické tvrdenia.

Príklad 1.6. *Ukážeme niekoľko príkladov na použitie kontrapríkladov.*

1. *Tvrdenie „Každé nepárne číslo je prvočíslo“ je nepravdivé. Číslo 9 je nepárne, ale nie je prvočíslom, pretože má troch deliteľov; čísla $1, 3, 9$.*
2. *Tvrdenie „Každé prvočíslo je nepárne číslo“ je nepravdivé. Číslo 2 je prvočíslo, a je párne.*
3. *Druhé tvrdenie „padá“ na jedinom prípade, ak tento problematický prípad vylúčime, dostávame pravdivé tvrdenie: „Každé prvočíslo väčšie ako 2 je nepárne číslo“.*
4. *Jedinečné postavenie čísla 2 medzi prvočíslami môžeme vyjadriť aj takto: „existuje jediné párne prvočíslo“.*

1.4.5 Princíp matematickej indukcie

Dokazovanie vlastností prvkov nekonečných množín môže spôsobovať ťažkosti. Existujú však (našťastie) početné výnimky. Vo všetkých matematických disciplínach sa počítajú

nejaké objekty a vyslovujú sa výroky v ktorých vystupujú prirodzené čísla. Existuje dokazovacia metóda, nazývaná *metódou úplnej* alebo častejšie *matematickej indukcie*, umožňujúca dokázať platnosť výrokovej formy, ktorej premenné nadobúdajú hodnoty z množiny prirodzených čísel a sú viazané všeobecným kvantifikátorom. V tejto časti vysvetlíme podstatu matematickej indukcie a ilustrujeme ju na príkladoch.

Nech je daná výroková forma $A(n)$, ktoré je definovaná pre všetky prirodzené čísla $n \in \mathbb{N}$ a nech platí

1. $A(1)$ je pravdivý výrok *(báza indukcie)*,
2. pre každé prirodzené číslo n z platnosti výroku $A(n)$ vyplýva platnosť výroku $A(n+1)$ *(indukčný predpoklad)*
3. potom $A(n)$ platí pre všetky prirodzené čísla n *(záver)*.

Princíp matematickej indukcie je jednou z axióm matematickej teórie, ktorá sa nazýva formálna aritmetika. V práci [14] je axióma matematickej indukcie formulovaná nasledovne[14]:

$$A(0) \Rightarrow [\forall n(A(n) \Rightarrow A(n+1)) \Rightarrow \forall n A(n)]$$

Poznámka. Existuje iný variant metódy matematickej indukcie, v ktorom sa pri indukčnom kroku nepredpokladá platnosť tvrdenia $A(n)$ *len* pre predchádzajúcu hodnotu n, ale pre *všetky* menšie hodnoty argumentu. Matematická indukcia v tejto podobe vyzerá nasledovne:

Nech je daná výroková forma $A(n)$, ktoré je definovaná pre všetky prirodzené čísla $n \in \mathbb{N}$ a nech platí

1. $A(1)$ je pravdivý výrok *(báza indukcie)*,
2. pre každé prirodzené číslo n z platnosti výrokov $A(1), \ldots, A(n)$ vyplýva platnosť výroku $A(n+1)$ *(indukčný predpoklad)*
3. potom $A(n)$ platí pre všetky prirodzené čísla n *(záver)*.

Poznámka. V niektorých prípadoch má tvrdenie $A(n)$ zmysel až pre $n > 1$. Pri použití matematickej indukcie budeme preto v prvom kroku (báza indukcie) predpokladať platnosť formuly $A(n_0)$ namiesto $A(1)$, kde n_0 je najmenšie prirodzené číslo, pre ktoré má tvrdenie $A(n)$ zmysel. Je zrejmé, že princíp matematickej indukcie v pôvodnej podobe, je zvláštnym prípadom takto modifikovaného princípu matematickej indukcie; v ktorom položíme $n_0 = 1$.

Pomerne často budeme využívať matematickú indukciu v kombinatorike. Postup „uhádni výsledok a potom ho dokáž matematickou indukciou“ nevyzerá na prvý pohľad

[14] báza indukcie sa berie pre $n = 0$

dostatočne seriózne, ale je plne legitímny. Ilustrujeme tento postup na príklade. Označíme symbolom S_n súčet prvých n nenulových prirodzených čísel:

$$S_n = 1 + \cdots + n = \sum_{k=1}^{n} k.$$

Skúmaním malých prípadov sme došli k poznaniu (hypotéze), že

$$S_n = \frac{n \cdot (n+1)}{2}.$$

Dokážeme platnosť tejto hypotézy matematickou indukciou.

1. Báza indukcie. Pre $n = 1$ dostávame
$$S_1 = \frac{1 \cdot (1+1)}{2} = 1.$$

2. Indukčný krok. Predpokladáme, že
$$S_n = \frac{n(n+1)}{2}$$
a dokážeme platnosť hypotézy pre hodnotu $n+1$; t.j. dokážeme že
$$S_{n+1} = \frac{(n+1) \cdot (n+2)}{2};$$
$$\begin{aligned} S_{n+1} &= S_n + (n+1) = \frac{n \cdot (n+1)}{2} + (n+1) = \frac{n \cdot (n+1) + 2(n+1)}{2} = \\ &= \frac{(n+1) \cdot (n+2)}{2} \end{aligned}$$

3. Záver. V indukčnom kroku sme za predpokladu platnosti tvrdenia pre n dokázali platnosť tvrdenia pre $n+1$. Keďže tvrdenie platí aj pre $n = 1$, tým sme dokázali jeho platnosť pre všetky hodnoty n;
$$S_n = \frac{n \cdot (n+1)}{2}.$$

Nasledujúci príklad ukazuje, že pri dôkaze matematickou indukciou nie je možné vynechať žiaden z predpokladov.

Príklad 1.7. *Súčet geometrického radu* $1 + q + q^2 + \cdots + q^n$ *sa pre* $q \neq 1$ *rovná*[15]

$$q_n = \frac{q^{n+1} - q}{q - 1}.$$

[15] v skutočnosti $q_n = \frac{q^{n+1}-1}{q-1}$.

Preskočíme dôkaz bázy indukcie a prejdeme hneď k dôkazu indukčného kroku. Nech pre ľubovoľné prirodzené číslo n *platí*

$$q_n = 1 + q + q^2 + \cdots + q^n = \frac{q^{n+1} - q}{q - 1}, \quad q \neq 1,$$

potom

$$\begin{aligned} 1 + q + q^2 + \cdots + q^n + q^{n+1} &= \frac{q^{n+1} - q}{q - 1} + q^{n+1} = \frac{q^{n+1} - q}{q - 1} + \frac{q^{n+2} - q^{n+1}}{q - 1} = \\ &= \frac{q^{n+2} - q}{q - 1}; \end{aligned}$$

t.j. ak súčtový vzorec platí pre hodnotu n*, tak potom platí aj pre hodnotu* $n + 1$*. Napriek tomu geometrický rad nemá súčet* $(q^{n+2} - q)/(q - 1)$*. Kde nastala chyba? V dôkaze matematickou indukciou chýba dôkaz bázy indukcie, a preto indukčný krok vedie do prázdna. Pre* $n = 1$ *je súčet*

$$q_1 = 1 + q = \frac{q^2 - 1}{q - 1},$$

zatiaľ čo „odvodený“ vzorec dáva

$$q_2 = \frac{q^2 - q}{q - 1} = q.$$

Aj keď je matematická indukcia jednoduchá a pritom efektívna dôkazová metóda, nemožno ju používať mechanicky[16]. Nasledujúci príklad ukazuje, do akých problémov sa dostaneme, keď nevhodne zvolíme hodnotu pre bázu indukcie.

Príklad 1.8. *Tvrdenie „Každých* n *prirodzených čísel je zhodných“ je zjavne nesprávne, ale „dokážeme“ ho matematickou indukciou vzhľadom na počet čísel. Nech sú dané prirodzené čísla* $a_1, \ldots, a_n, \ldots$.

1. *(Báza indukcie.) Pre* $n = 1$ *nieto čo dokazovať, pretože číslo sa rovná sebe samému.*

2. *(Indukčný krok.) predpokladáme, že každých* n *čísel je zhodných. Vyberieme nejakých* $n + 1$ *čísel* $a_{i_1}, a_{i_2}, \ldots, a_{i_{n+1}}$*. Najprv z nich vynecháme číslo* a_{i_1}*. Ostalo nám* n *čísel, pre ktoré teda platí*

   $$a_{i_2} = \cdots = a_{i_{n+1}}$$

   Teraz z pôvodnej $n + 1$*-prvkovej množiny vynecháme číslo* $a_{i_{n+1}}$*. Keďže v nej zostalo* n *prvkov, opäť platí*

   $$a_{i_1} = a_{i_2}, \ldots, a_{i_n}.$$

   Spojením dvoch predchádzajúcich reťazcov rovností sa dostávame k (zjavne nepravdivému) tvrdeniu

   $$a_{i_1} = a_{i_2} = \cdots = a_{i_n} = a_{i_{n+1}}.$$

[16] v informatike sa na to používa výstižné úslovie „garbage in - garbage out“; v preklade: smetie dnu, smetie von.

3. *Záver. Každých* n *prirodzených čísel je zhodných.*

Kde je chyba? Chýba nám tu začiatok indukcie. Prípad $n = 1$ *bol len zdanlivý začiatok; zmysluplne porovnávať možno v prípade, keď máme aspoň dva prvky. Ak teda chceme naše tvrdenie dokazovať matematickou indukciou* vhľadom na počet prvkov *dokazujeme platnosť bázy indukcie pre* $n = 2$.

Poznámka. Je zrejmé, že predchádzajúce tvrdenie je nepravdivé pre $n > 1$, čo by sme ľahko dokázali výberom vhodného kontrapríkladu (množiny obsahujúcej aspoň dva rôzne prvky). Prípad $n = 1$ je zrejmý. Porozmýšľajte ešte o platnosti vyššie uvedeného tvrdenia v prípade $n = 0$.

V ďalších kapitolách nájde čitateľ dostatok príležitostí na to, aby získané poznatky uplatnil a zdokonalil. Čitateľovi, ktorý má záujem o hlbšie štúdium matematickej logiky, odporúčame knihy [14], [6]. Problematika matematických dôkazov je prístupnou formou vyložená v knihe [17].

Poznámka. Seržant Christopher Watson (v civile učiteľ matematiky) na svojej webovskej stránke `http://www.bluemoon.net/ watson/proof.htm` uvádza 36 ďalších užitočných a (nielen v matematike) často používaných metód dôkazov

Proof by obviousness The proof is so clear that it need not be mentioned.

Proof by general agreement All in favor?. . .

Proof by imagination Well, we' ll pretend it's true. . .

Proof by convenience It would be very nice if it were true, so . . .

Proof by necessity It had better be true, or the entire structure of mathematics would crumble to the ground.

Proof by plausibility It sounds good, so it must be true.

Proof by intimidation Don't be stupid; of course it's true.

Proof by lack of sufficient time Because of the time constraint, I' ll leave the proof to you.

Proof by postponement The proof for this is long and arduous, so it is given in the appendix.

Proof by accident Hey, what have we here?!

Proof by insignificance Who really cares, anyway?

Proof by mumbo-jumbo $\forall(B \subset \Pi), \exists(X \in \Omega)$

Proof by profanity (example omitted)

Proof by definition We define it to be true.

Proof by tautology It's true because it's true.

Proof by plagiarism As we see on page 289.....

Proof by lost reference I know I saw it somewhere.....

Proof by calculus This proof requires calculus, so we' ll skip it.

Proof by lack of interest Does anyone really want to see this?

Proof by illegibility (scribble, scribble) QED

Proof by terror When intimidation fails ...

Proof by logic If it is on the problem sheet, then it must be true!

Proof by majority rule Only to be used if general agreement is impossible

Proof by clever variable choice Let A be the number such that this proof works. .

Proof by tessellation This proof is the same as the last.

Proof by divine word And the Lord said, *Let it be true*, and it was true.

Proof by stubbornness I don't care what you say-it is true!

Proof by simplification This proof reduces to the statement 1 + 1 = 2.

Proof by hasty generalization Well, it works for 17, so it works for all reals.

Proof by deception Now everyone turn their backs...

Proof by supplication Oh please, let it be true.

Proof by poor analogy Well, it's just like ...

Proof by avoidance Limit of proof by postponement as it approaches infinity

Proof by design If it's not true in today's math, invent a new system in which it is.

Proof by authority Well, Don Knuth says it's true, so it must be!

Proof by intuition I just have this gut feeling...

Kapitola 2

Základy teórie množín

No one shall expel us from the Paradise that Cantor has created.
David Hilbert

Väčšinu objektov, s ktorými budeme v matematike a informatike pracovať, môžeme chápať buď ako nejaké množiny prípadne ako prvky nejakých množín. V tejto a nasledujúcich kapitolách sa preto zameriame na osvojenie si základných poznatkov o množinách, množinových operáciách, reláciách a zobrazeniach. Súčasne si precvičíme tie dôkazové metódy, o ktorých sme hovorili v predchádzajúcej kapitole.

Čitateľovi, ktorý sa zaujíma o históriu vzniku teórie množín, odporúčame do pozornosti knihy [4, 5]; záujemci o hlbšie štúdium teórie množín uspokoja napríklad práce [3, 2] a [4].

2.1 Základné pojmy

Teória množín je postavená na dvoch základných pojmoch: *množina* a *byť prvkom množiny*. Pod množinou si (zatiaľ) predstavujeme súbor prvkov, ktoré majú nejakú spoločnú vlastnosť. Množiny tvoria napríklad všetci študenti UK v akademickom roku 2004/5, všetci občania Slovenskej republiky, všetky body roviny, všetky prvočísla, veľké písmená anglickej abecedy a pod.

Množiny budeme označovať veľkými písmenami $A, B, C, \ldots$ a v prípade potreby indexovať $A_1, A_2, \ldots, A_n, \ldots$ Objekty, ktoré tvoria množinu, budeme nazývať prvkami[1] danej množiny. Prvky množiny označujeme malými písmenami $a, b, \ldots, x, y, z$ a v prípade potreby ich tiež indexujeme. Skutočnosť, že prvok x patrí do množiny A zapisujeme symbolicky takto: $x \in A$ a hovoríme tiež, že *prvok* x *je elementom množiny* A*, (množina)* A *obsahuje prvok* x*,* x *patrí do (množiny)* A. Skutočnosť, že x nie je prvkom množiny A zapisujeme symbolicky takto: $\neg(x \in A)$ alebo $x \notin A$.

Akým spôsobom môžeme určiť, aké prvky množina obsahuje?

[1] prvkami množiny môžu byť aj množiny

Opísať množinu možno v podstate dvoma spôsobami, a to buď vymenovaním jej prvkov, alebo charakterizáciou prvkov množiny pomocou nejakej vlastnosti, ktorú majú všetky prvky danej množiny.[2] V prvom prípade do zložených zátvoriek vypíšeme všetky prvky danej množiny[3], druhý prípad je trocha komplikovanejší.

Príklad 2.1. *Nasledujúce množiny je možné zadať vymenovaním všetkých ich prvkov*

- $A_1 = \{1, 2, 3, 4, 5\}$,
- $A_2 = \{a, b, c, d, e, f, \ldots, x, y, z\}$,
- $A_3 = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$.

Takto spôsob zadávania množiny možno použiť vtedy, ak množina obsahuje konečný a nie príliš veľký počet prvkov. V matematike sa však často stretávame s veľmi veľkými alebo nekonečnými množinami, ktoré z pochopiteľných dôvodov nie je možné zadať vymenovaním všetkých prvkov. Niektoré z nich sú všeobecne známe—napríklad číslené množiny:

N – množina prirodzených čísel,

Z – množina celých čísel,

Q – množina racionálnych čísel,

R – množina reálnych čísel,

C – množina komplexných čísel;

iné je potrebné definovať tak, že zadáme vlastnosti, ktoré musia spĺňať všetky prvky danej množiny. Bez toho, aby sme to explicitne povedali, využívame pri tom tzv. *axiómu špecifikácie*, ktorá hovorí, že každá rozumná vlastnosť definovaná na množine prvkov definuje novú množinu tých prvkov, ktoré majú danú vlastnosť.

Poznámka. Presnejšia formulácia schémy axióm špecifikácie znie [4]:

Ak je $\varphi(x)$ fomula, ktorá nemá voľné výskyty premennej B, tak potom formula

$$\forall A \exists B \forall x (x \in B \leftrightarrow x \in A \& \varphi(x)) \tag{2.1}$$

je axióma. Množina B je časťou množiny A, obsahujúcou všetky prvky x, ktoré majú vlastnoť φ. Prečo hovoríme o schéme axióm a nie o axióme špecifikácie? Pre každú formulu φ definuje formula 2.1 axiómu teórie množín.

[2] Podľa možnosti by to malo byť niečo iné ako to, že prvky patria do danej množiny.

[3] aby sme boli korektní, musíme dodať, že pri tomto spôsobe zápisu oddeľujeme jednotlivé prvky množiny v zložených zátvorkách čiarkami, prípadne ich nahradzujeme bodkami; čiarky a bodky sú v tomto prípade pomocnými symbolmi. Ak by sme uvažovali napríklad množinu ASCII znakov, pri zápise prvkov by sme museli rozlišovať medzi čiarkou ako pomocným symbolom a čiarkou ako prvkom množiny. Podobne by bolo potrebné rozlišovať aj ďalšie pomocné symboly (zložené zátvorky, bodky,ktoré sa pri zápise množiny znakov môžu vyskytovať v dvoch rozličných významoch.

Príklad 2.2. *Uvedieme niekoľko množín definovaných pomocou axiómy špecifikácie.*

- $A_4 = \{x|(x \in \mathbf{Z})\&(x > 3)\}$,
- $A_5 = \{x|(x \in \mathbf{N})\&(x$ *je deliteľné* $2\}$.

Množina A_5 predstavuje množinu všetkých párnych prirodzených čísel. Túto množinu by sme mohli zapísať takto

$$A_5 = \{2n|n \in \mathbf{N}\},$$

alebo aj takto

$$A_5 = \{0, 2, 4, 6, \ldots, 2n, \ldots\}.$$

Ak zovšeobecníme predchádzajúce príklady, vidíme, že množiny možno zadávať nasledujúcim spôsobom:

$$A = \{x|P(x)\},$$

ktorý vyjadruje skutočnosť, že množina A je množina všetkých tých prvkov, ktoré majú vlastnosť P a neobsahuje žiadne prvky, ktoré vlastnosť P nemajú. Pri takomto spôsobe zadávania množín si musíme dávať dobrý pozor na vlastnosť P. Axióma špecifikácie tento problém rieši tým, že sa prvky novej množiny vyberajú zo súboru, ktorý je množinou. Ak sa tento predpoklad zanedbá, môžeme zaviesť „množinu“, ktorá množinou nie je. Problémy vyplývajúce z príliš voľnej definície množiny pomocou ilustruje už spomínaný Russellov paradox.

Russellov paradox. Zatiaľ sme nekládli žiadne obmedzenia na to, aké objekty môžu byť prvkami množín. To znamená, že jedny množiny môžu byť prvkami iných množín. Napríklad $x \in \{x\}, \{x\} \in \{\{x\}\}$ alebo aj $x \in \{x, \{x\}\}, \{x\} \in \{x, \{x\}\}$. Na druhej strane, nech $\{1\}$ je jednoprvková množina obsahujúca prvok 1. Zrejme platí $1 \neq \{1\}$, a ani $\{1\} \notin \{1\}$. To znamená, že existuje množina X, ktorá má vlastnosť $P : X \notin X$, X nie je prvkom seba samej. Vlastnosť P je teda na prvý pohľad „rozumná“. Možno ju však použiť na definovanie množiny? Pokúsime sa vytvoriť „množinu“ všetkých množín, ktoré majú vlastnosť P; t.j. tých, ktoré nie sú prvkami seba samých:

$$M = \{X|X \notin X\}.$$

Je zrejmé, že do M patria všetky známe množiny $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, A_1, A_2, A_3, A_4, A_5$ a ďalšie. Čo však samotná „množina“ M ? Do úvahy prichádzajú na prvý pohľad len dve možnosti: buď $M \in M$, alebo $M \notin M$. Zistíme, ktorá z týchto možností nastane.

- Nech $M \in M$. „Množina“ M je však množinou všetkých množín X, pre ktoré platí $X \notin X$. Ak teda $M \in M$, tak pre M mus platiť $M \notin M$—spor.
- Nech teda $M \notin M$.„Množina“ M je však množinou všetkých množín X, pre ktoré platí $X \notin X$. To znamená, že $M \in M$. Spor.

V oboch prípadoch sme dospeli ku sporu. To znamená, že súbor množín s vlastnosťou P nemôže byť množinou.

Vyhnúť sa Russellovmu paradoxu a iným problémom a nejasnostiam vyplývajúcim z intuitívneho pojmu množiny možno pomocou axiomatickej výstavby teórie množín [3, 4]. V teórii množín sa rozlišujú množiny množín a súbory množín, ktoré nie sú množinami; takéto súbory sa nazývajú *triedami*. My sa axiomatizáciou teórie množín zaoberať nebudeme. Budeme pracovať s takými súbormi objektov, ktoré tvoria množiny a používať pri narábaní s nimi také postupy, ktoré nám z východiskových množín umožnia vytvárať nové množiny. Začneme tým, že zavedieme základné množinové operácie a vzťahy medzi množinami. K triedam množín sa vrátime neskôr v kapitole 8.

2.2 Základné množinové operácie a vzťahy medzi množinami

Definícia 2.1. *(Rovnosť množín) Nech sú* A, B *ľubovoľné množiny. Hovoríme, že množina* A *sa rovná množine* B *práve vtedy, ak je každý prvok množiny* A *prvkom množiny* B *a každý prvok množiny* B *je prvkom množiny* A*. Rovnosť množín* A, B *symbolicky zapisujeme takto* $A = B$.

Poznámka Formálne môžeme definíciu rovnosti množín zapísať nasledovne (A, B sú ľubovoľné množiny):

$$\begin{aligned} A = B &\equiv \forall x[[(x \in A) \Rightarrow (x \in B)]\&[(x \in B) \Rightarrow (x \in A)]] \equiv \\ &\equiv \forall x[[(x \in A) \equiv (x \in B)]. \end{aligned}$$

Definícia 2.2. *(Inklúzia množín) Nech sú* A, B *ľubovoľné množiny. Hovoríme, že množina* A *je* podmožinou množiny B *práve vtedy, ak je každý prvok množiny* A *prvkom množiny* B *Inklúziu množín* A, B *symbolicky zapisujeme takto* $A \subseteq B$.

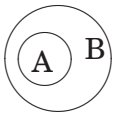
Ak $A \subseteq B$ *a zároveň existuje v množine* B *existuje prvok* x*, ktorý nepatrí do množiny* A*, hovoríme, že* A *je vlastnou podmnožinou množiny* B*, čo symbolicky zapisujeme nasledovne* $A \subset B$.

Poznámka Skutočnosť, že A je podmnožinou B sa dá formálne vyjadriť aj takto:

$$A \subseteq B \equiv \forall x[(x \in A) \Rightarrow (x \in B)].$$

Dokázať podľa definície, že sa dve množiny rovnajú, nemusí byť jednoduché. Keď však porovnáme definície rovnosti množín a inklúzie, vidíme, že rovnosť množín možno vyjadriť pomocou inklúzie:

$$A = B \equiv [(A \subseteq B)\&(B \subseteq A)].$$



Obrázok 2.1: Vennov diagram pre $A \subseteq B$

Tento posledný vzťah budeme často využívať pri dokazovaní rovnosti množín. V ďalšom budeme predpokladať, že všetky množiny s ktorými budeme pracovať, sú podmnožinami nejakej univerzálnej množiny U. Niektoré vzťahy medzi množinami a množinové operácie možno veľmi prehľadne reprezentovať pomocou tzv. Vennových diagramov. Každej množine vo Vennovom diagrame zodpovedá spojitá oblasť roviny (najčastejšie kruh, elipsa alebo podobný geometrický útvar). Na obrázku 2.1 sú znázornené dve množiny A, B také, že $A \subseteq B$. Zavedieme teraz operácie zjednotenia, prieniku, doplnku a rozdielu množín.

Definícia 2.3. *Nech sú A, B ľubovoľné množiny. Zjednotením množín A, B budeme nazývať množinu $A \cup B$ všetkých prvkov, ktoré patria aspoň do jednej z množín A, B:*

$$A \cup B = \{x | (x \in A) \vee (x \in B)\}.$$

Definícia 2.4. *Nech sú A, B ľubovoľné množiny. Prienikom množín A, B budeme nazývať množinu $A \cap B$ všetkých prvkov, ktoré patria súčasne do oboch množín A, B:*

$$A \cap B = \{x | (x \in A) \& (x \in B)\}.$$

Čo však v prípade, ak množiny A, B nemajú spoločný prvok? Je aj prienikom takýchto množín opäť množina? Odpoveď je kladná, áno a ide o veľmi dôležitú množinu, tzv. *prázdnu množinu*.

Definícia 2.5. *Prázdna množina je množina, ktorá neobsahuje žiaden prvok. Prázdnu množinu označujeme symbolom $\{\}$, alebo $\emptyset$.*

Prázdnu množinu možno definovať pomocou ľubovoľnej nesplniteľnej podmienky. Napríklad

- $\{x | x \in \mathbf{N} \& (x < 0)\} = \emptyset$,
- $\{x | x \neq x\} = \emptyset$,
- $\{x | (x \in R) \& \sin x > 1\} = \emptyset$.

Dve množiny, ktorých prienikom je prázdna množina, sa nazývajú *disjunktnými množinami*. V nasledujúcej vete vyslovíme a dokážeme dve dôležité vlastnosti prázdnej množiny.

Veta 2.1. *1. Prázdna množina je podmnožinou ľubovoľnej množiny.*

2. Existuje práve jedna prázdna množina.

Dôkaz. Prvé tvrdenie dokážeme sporom. Predpokladáme, že neplatí; to znamená, že platí jeho negácia:

$$\neg\forall X(\emptyset \subseteq X) \equiv \exists X\neg(\emptyset \subset X);$$

to znamená, že existuje taká množina X, že $\emptyset$ nie je podmnožinou X. Ale to by znamenalo, že $\emptyset$ musí obsahovať prvok, ktorý nepatrí do množiny X. To však nie je možné, pretože $\emptyset$ neobsahuje žiadne prvky. Dostali sme spor, a to znamená, že predpoklad ($\neg\forall X(\emptyset \subseteq X)$) neplatí, ale platí jeho negácia $\forall X(\emptyset \subseteq X)$, čo sme mali dokázať.

Pri dôkaze druhého tvrdenia budeme tiež postupovať sporom. Predpokladajme, že existujú dve rozličné prázdne množiny, ktoré označíme ako B_1, B_2. Využijeme práve dokázané tvrdenie. Keďže množina B_1 je prázdna, platí $B_1 \subseteq B_2$. Ale aj množina B_2 je prázdna, a teda platí $B_2 \subseteq B_1$. Z toho však vyplýva, že $B_1 = B_2$; t.j. ľubovoľné dve prázdne množiny sa rovnajú, čo je spor s predpokladom o existencii dvoch rozličných prázdnych množín. □

Úloha 2.1. *V programovacích jazykoch sa bežne používajú premenné typu CHAR, INTEGER, UNSIGNED INTEGER, REAL, DOUBLE. Vypíšte množinu CHAR a určte koľko prvkov obsahujú ostatné množiny napr. v jazyku C.*

Úloha 2.2. *Uveďte príklad množiny, ktorej prvkami sú množiny.*

Úloha 2.3. *Nech* $A = \{a, b, \emptyset, \{\emptyset\}\}$.

1. *Koľko prvkov má množina* A*?*
2. *Zistite, ktoré z nasledujúcich šiestich tvrdení sú pravdivé a ktoré nie:*
   - *(a)* $a \in A$
   - *(b)* $\emptyset \in A$
   - *(c)* $\{a, b\} \in A$
   - *(d)* $a \subseteq A$
   - *(e)* $\emptyset \subseteq A$
   - *(f)* $\{a, b\} \subseteq A$

Definícia 2.6. *Nech je* A *ľubovoľná množina,* $A \subseteq U$. *Doplnkom množiny* A *(vzhľadom na univerzálnu množinu* U *nazývame množinu všetkých tých prvkov množiny* U*, ktoré nepatria do* A*:*

$$A^c = \{x|(x \in U)\&(x \notin A)\}.$$

Keď uvažujeme doplnok nejakej množiny A vzhľadom na univerzálnu množinu U, často používame skrátený zápis:

$$A^c = \{x|x \notin A\}.$$

Doplnok množiny možno vyjadriť nielen vzhľadom na univerzálnu ale aj vzhľadom na ľubovoľnú inú množinu. Na to slúži ďalšia množinová operácia—rozdiel množín.

Definícia 2.7. *Nech sú* A, B *ľubovoľné množiny. Rozdielom množín* A, B *budeme nazývať množinu všetkých prvkov, ktoré patria do množiny* A *a zároveň nepatria do množiny* B*:*

$$A - B = \{x | (x \in A) \& (x \notin B)\}.$$

Rozdiel množín pripomína prienik množín. Skutočne, rozdiel množín A, B možno vyjadriť pomocou prieniku a doplnku množín nasledovným spôsobom:

$$A - B = A \cap B^c.$$

Všimnite si, že doplnok A^c množiny A vzhľadom na univerzálnu množinu U nie je nič iné ako

$$U - A = U \cap A^c = A^c.$$

Kým prienik a zjednotenie množín sú komutatívne množinové operácie, rozdiel množín komutatívny nie je; vo všeobecnosti $A - B \neq B - A$. Existuje však modifikácia rozdielu množín, ktorá je komutatívna—tzv. *symetrická diferencia množín*.

Definícia 2.8. *Nech sú* A, B *ľubovoľné množiny. Symetrickou diferenciou množín* A, B *budeme nazývať množinu množinu všetkých prvkov, ktoré patria práve do jednej z množín* A, B*:*

$$A \triangle B = \{x | [(x \in A) \& (x \notin B)] \vee [(x \in B) \& (x \notin A)]\}.$$

Ak využijeme definície prieniku a zjednotenia množín, môžeme vyjadriť symetrickú diferenciu stručnejšie takto:

$$A \triangle B = (A - B) \cup (B - A).$$

Vennove diagramy zjednotenia, prieniku, doplnku, rozdielu a symetrickej diferencie množín sú uvedené na obrázku **??**.

2.3 Abeceda, slová a jazyky

Skôr ako prikročíme ku skúmaniu vlastností množinových operácií, zavedieme niektoré špeciálne množiny, ktoré sa často používajú v informatike.

Ľubovoľnú konečnú neprázdnu množinu $\Sigma = \{a_1, \ldots, a_n\}$ budeme nazývať *abecedou*. Prvky abecedy Σ nazývame *symbolmi* alebo *znakmi abecedy* Σ. Postupnosť znakov abecedy Σ nazývame *slovom nad abecedou* Σ. Nech je ν slovo nad abecedou Σ, potom výrazom $\lambda(\nu)$ budeme označovať *dĺžku slova* ν; t.j. počet znakov (abecedy Σ) v slove ν. Ak slovo ν predstavuje nekonečnú postupnosť znakov, hovoríme, že slovo ν je nekonečné. V opačnom prípade je slovo ν konečné. Dôležitým špeciálnym prípadom je slovo, ktoré nemá jediný symbol; takéto slovo sa nazýva prázdnym slovom, označuje sa symbolom ε a má nulovú dĺžku; t.j. $\lambda(\varepsilon) = 0$.

Nech sú $u = a_1 a_2 \ldots a_k$; $\nu = b_1 b_2 \ldots b_m$ dve slová nad (nejakou) abecedou Σ. Potom slovo $u\nu = a_1 a_2 \ldots a_k b_1 b_2 \ldots b_m$, ktoré dostaneme tak, že za slovom u napíšeme sprava slovo ν je podľa definície slova tiež slovom nad abecedou Σ. Slovo $u\nu$ sa nazýva

zreťazením (konkatenáciou) slov u, v a vytváranie zreťazenia slov sa nazýva operáciou zreťazovania. Všimnite si, že ak sú slová u, v rôzne, $uv \neq vu$, t.j. operácia zreťazovania nie je vo všeobecnosti komutatívna. Nech $u = a_1 a_2 \dots a_k$. Ľubovoľná postupnosť znakov $a_i a_{i+1} \dots a_l$, kde $1 \leq i \leq l \leq k$ sa nazýva *podslovom* slova u. Slovo $a_1 a_2 \dots a_l$, $l \leq k$ sa nazýva *počiatočným podslovom*(prefixom) a slovo $a_i a_{i+1} \dots a_k$, $1 \leq i$ sa nazýva koncovým podslovom (sufixom) slova u. Znaky v slove možno aj preusporiadať. Dôležitým prípadom preusporiadania znakov je otočenie slova: *zrkadlovým obrazom* slova $u = a_1 \dots a_n$ nazveme slovo $u^R = a_n \dots a_1$

Slová môžu byť prvkami množín. Ľubovoľnú množinu slov nad abecedou Σ nazveme *jazykom nad abecedou* Σ. Okrem bežných množinových operácií nad množinami slov (jazykmi) zavedieme aj operácie s jazykmi odvodené od zreťazovania slov. Nech sú $\mathcal{L}_1, \mathcal{L}_2$ jazyky nad abecedou Σ, potom $\mathcal{L} = \mathcal{L}_1\mathcal{L}_2$ je jazyk nad abecedou Σ definovaný nasledovne: $\mathcal{L} = \{uv \mid u \in \mathcal{L}_1, v \in \mathcal{L}_2\}$. Jazyk $\mathcal{L}$ sa nazýva *zreťazenie (konkatenácia) jazykov* $\mathcal{L}_1, \mathcal{L}_2$. Jazyk možno zreťazovať so sebou samým; pre ľubovoľný jazyk $\mathcal{L}$ a ľubovoľné číslo $k \in \mathcal{N}$ definujeme:

1. $\mathcal{L}^0 = \{\varepsilon\}$,
2. $\mathcal{L}^{k+1} = \mathcal{L}^k\mathcal{L}$.

Na záver uvedieme ešte dve operácie nad jazykmi, ktoré nám umožnia popísať množinu všetkých možných slov, ktoré sa dajú vytvoriť pomocou operácie zreťazovania jazyka. Nech $\mathcal{L}$ je ľubovoľný jazyk, potom jazyky $\mathcal{L}^+ = \bigcup_{i>0}^{\infty} \mathcal{L}^i$ a $\mathcal{L}^* = \bigcup_{i\geq 0}^{\infty} \mathcal{L}^i$ sa nazývajú *kladná,* resp. *nezáporná iterácia jazyka* $\mathcal{L}^i$. Všimnite si, že abecedu Σ možno chápať aj ako jazyk pozostávajúci zo všetkých slov dĺžky 1 nad abecedou Σ a Σ^* predstavuje množinu všetkých slov nad abecedou Σ.

Ilustrujeme teraz zavedené pojmy na príkladoch.

Príklad 2.3. *1. Binárna abeceda* Σ_1 *je ľubovoľná dvojprvková množina. Znaky binárnej abecedy najčastejšie označujeme číslicami* $0, 1$*;* $\Sigma_1 = \{0, 1\}$.

2. Na zápis prirodzených čísel vystačíme s abecedou $\Sigma_2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

3. Racionálne čísla možno zapísať v podobe slov nad abecedou $\Sigma_3 = \Sigma_2 \bigcup \{"+", -", "."\}$.[4]

4. $\Sigma_4 = \{a, b, c, d, e, f, g, i, j, k, l, m, n, o, p, q, r, s, t, v, w, x, y, z\}$ *je abeceda pozostávajúca z malých písmen anglickej abecedy.*

5. Abecedu $\Sigma_5 = \{A, B, C, D, E, F, G, I, J, K, L, M, N, O, P, Q, R, S, T, V, W, X, Y, Z\}$ *tvoria veľké písmená anglickej abecedy.*

6. $\Sigma_6 = \Sigma_4 \bigcup \Sigma_5$.

7. Abecedu $\Sigma_7 = \{\alpha, \beta, \gamma, \delta, \epsilon, \varepsilon, \zeta, \eta, \theta, \vartheta, \iota, \kappa, \lambda, \mu, \nu, \xi, o, \pi, \varpi, \rho, \varrho, \sigma, \varsigma, \tau, \upsilon, \phi, \varphi, \chi, \psi, \omega\}$ *tvoria malé písmená gréckej abecedy.*

[4] Pripomíname, že čiarka a úvodzovky nie sú symbolmi abecedy Σ_3

8. *Ďalšími užitočnými abecedami by mohli byť rozličné znakové sady, napr. všetky znaky kódov ASCII. V teórii kódovania budeme často pracovať s abedcedami, ktorých symboly sú prvkami konečných polí. Tieto symboly budeme zapisovať pomocou prirodzených čísel;* $\Sigma_8 = Z_m = \{0, 1, \dots m-1\}$.

9. *Slovo* 2.78128 *je slovom nad* Σ_3*, ale nie je slovom nad abecedou* Σ_2.

10. *Ukážeme, ako možno využiť uvedené pojmy na formálnu definíciu niektorých pojmov v programovacích jazykoch:*

    (a) *Celé číslo možno definovať ako konečné slovo nad abecedou* Σ_3 *zapísané v tvare: [znamienko][číslica]* ^{i}*, kde [znamienko]*$\in \{+, -\}$*, [číslica]*$\in \Sigma_2$*,* $i \in \mathbf{N}$*,* $i > 0$*,*

    (b) *Identifikátor bude slovo nad abecedou* $\Sigma_6 \cup \Sigma_2$*, vyhovujúce nasledujúcej schéme: [písmeno]([písmeno] alebo [číslica])* ^{i}*, kde [písmeno]*$\in \Sigma_6$*, [číslica]*$\in \Sigma_2$*,* $i \in \mathbf{N}$.

11. *Zreťazením slov* $w_1 = \mathtt{pismeno}$ *a* $w_2 = \mathtt{male}$ *dostávame slová* $w_1w_2 = \mathtt{pismenomale}$ *a* $w_2w_1 = \mathtt{malepismeno}$ *(napr. nad abecedou* Σ_4*).*

12. *Nech je dané slovo* $w_1 = \mathtt{pismeno}$ *nad abecedou* Σ_4*, počiatočné a koncové podslová tohto slova sú uvedené v nasledujúcej tabuľke:*

prefix	sufix
ε	pismeno
p	ismeno
pi	smeno
pis	meno
pism	eno
pisme	no
pismen	o
pismeno	ε

13. *Nech je dané slovo* $w_1 = \mathtt{pismeno}$ *nad abecedou* Σ_4*, zrkadlový obraz slova* w_1 *je slovo* $w_1^R = \mathtt{onemsip}$ *nad abecedou* Σ_4.

14. *Nech sú* $\mathcal{L}_1 = \{\mathtt{ne}, \mathtt{pre}, \mathtt{po}, \mathtt{vy}\}$, $\mathcal{L}_2 = \{\mathtt{mysli}, \mathtt{hovor}, \mathtt{pis}, \mathtt{padni}\}$ *jazyky nad abecedou* Σ_4*. Jazyk* $\mathcal{L}_1\mathcal{L}_2$ *je uvedený v nasledujúcej tabuľke:*

$\mathcal{L}_1 / \mathcal{L}_2$	*ne*	*pre*	*po*	*vy*
mysli	*nemysli*	*premysli*	*pomysli*	*vymysli*
hovor	*nehovor*	*prehovor*	*pohovor*	*vyhovor*
pis	*nepis*	*prepis*	*popis*	*vypis*
padni	*napadni*	*prepadni*	*popadni*	*vypadni*

15. *Uvažujme binárnu abecedu* $\Sigma_1 = \{0, 1\}$*. Uvedieme množiny slov* Σ_1^k *pre niekoľko*

počiatočných hodnôt k.

k	Σ_1^k
0	$\{\varepsilon\}$
1	$\{0, 1\}$
2	$\{00, 01, 10, 11\}$
3	$\{000, 001, 010, 011, 100, 101, 110, 111\}$
4	$\{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$
5	$\{00000, 00001, 00010, 00011, 00100, 00101, 00110, 00111, 01000, 01001, 01010, 01011, 01100, 01101, 01110, 01111, 10000, 10001, 10010, 10011, 10100, 10101, 10110, 10111, 11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111\}$

Úloha 2.4. *Nech je* Σ *množina všetkých ASCII znakov. Definujte ako slová nad abecedou* Σ

1. *typ REAL,*
2. *typ INTEGER zapísaný desiatkovo aj hexadecimálne,*
3. *jednoduchý aritmetický výraz tvaru (operand*$_1 \pm$ *operand*$_2$*), kde operand*$_i$, $i = 1, 2$ *je buď číslo, alebo identifikátor.*

Úloha 2.5. *Nájdite všetky prefixy a sufixy slova* $\mathtt{abeceda}$.

Úloha 2.6. *Zvoľte jednoduchý jazyk* $\mathcal{L}$ *a skonštruujte* $\mathcal{L}^2, \mathcal{L}^3$.

Úloha 2.7. *Nech* $\Sigma = \{a, b\}, \mathcal{L}_1 = \{ab, aab\}, \mathcal{L}_2 = \{a, b, ab\}$. *Zostrojte jazyky*

1. $\mathcal{L}_1 \cup \mathcal{L}_2$,
2. $\mathcal{L}_1 \cap \mathcal{L}_2$,
3. $\mathcal{L}_1 \cap \mathcal{L}_2^2$,
4. $\mathcal{L}_1^* \cap \Sigma^5$
5. $(\mathcal{L}_1 \cup \mathcal{L}_2)^+ \cap \Sigma^6$,.

2.4 Základné množinové identity

Tú istú množinu možno zapísať rozličným spôsobom. Pre skúmanie vlastností množín je často výhodné zapisovať množiny ako výsledok množinových operácií nad inými, spravidla jednoduchšími množinami. Ale ani vyjadrenie množiny pomocou iných množín nie je jednoznačné. Preto sa budeme snažiť upraviť zápis množiny do čo možno najjednoduchšieho a najprehľadnejšieho tvaru, ktorý nám potom umožní dobre pracovať s danou množinou. Na tento účel budeme používať množinové identity. Množinová identita v

podstate predstavuje vyjadrenie tej istej množiny dvoma rozličnými (pritom ekvivalentnými) spôsobmi. Pri práci s množinami máme potom možnosť množinu zapisovať tým spôsobom, ktorý je pre spracovanie najvýhodnejší.

Ako budeme postupovať pri odvodzovaní množinových identít? Najprv vyslovíme niekoľko elementárnych tvrdení o vlastnostiach zjednotenia, prieniku a doplnku množín. Využijeme výrokový počet a tvrdenia o rovnosti množín budeme formulovať v podobe výrokov o príslušnosti prvkov do množín. Tieto zložené výroky o príslušnosti prvkov do množín upravíme a dokážeme pomocou známych tautológií výrokového počtu a tak dokážeme platnosť elementárnych množinových identít. Potom vyslovíme zložitejšie tvrdenia o vzťahoch množín a tieto budeme dokazovať už pomocou dokázaných množinových identít. V nasledujúcej vete vyslovíme a dokážeme popri množinových identitách aj niekoľko dôležitých množinových inklúzií.

Veta 2.2. *Nech sú* A, B, C *ľubovoľné množiny. Potom platia nasledujúce vzťahy*

1. $A \cup A = A$ *(idempotentnosť zjednotenia)*
2. $A \cap A = A$ *(idempotentnosť prieniku)*
3. $A \cup B = B \cup A$ *(komutatívnosť zjednotenia)*
4. $A \cap B = B \cap A$ *(komutatívnosť prieniku)*
5. $A \cup (B \cup C) = (A \cup B) \cup C$ *(asociatívnosť zjednotenia)*
6. $A \cap (B \cap C) = (A \cap B) \cap C$ *(asociatívnosť prieniku)*
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributívny zákon)*
8. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributívny zákon)*
9. $(A \cup B)^c = (A^c \cap B^c)$ *(de Morganov zákon)*
10. $(A \cap B)^c = (A^c \cup B^c)$ *(de Morganov zákon)*
11. $(A \cap B) \subseteq A$
12. $(A \cap B) \subseteq B$
13. $A \subseteq (A \cup B)$
14. $B \subseteq (A \cup B)$
15. $(A^c)^c = A$
16. $A \cap \emptyset = \emptyset$
17. $A \cup \emptyset = A$
18. $A \cap A^c = \emptyset$
19. $A \cup A^c = U$
20. $A \cap (A \cup B) = A$ *(absorbčný zákon)*
21. $A \cup (A \cap B) = A$ *(absorbčný zákon).*

Dôkaz. V jednotlivých prípadoch možno postupovať podľa nasledujúcej schémy:

$$(8) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{distributívny zákon}$$

1. Nech $x \in A \cup (B \cap C)$, kde x je ľubovoľný prvok;
2. $x \in A \cup (B \cap C) \equiv (x \in A) \vee (x \in (B \cap C))$ (definícia zjednotenia);
3. $(x \in A) \vee (x \in (B \cap C)) \equiv (x \in A) \vee ((x \in B)\&(x \in C))$ (definícia prieniku);
4. $(x \in A) \vee ((x \in B)\&(x \in C)) \equiv ((x \in A) \vee (x \in B))\&((x \in A) \vee (x \in C))$ (distributívny zákon pre konjunkciu a disjunkciu);
5. $((x \in A) \vee (x \in B))\&((x \in A) \vee (x \in C)) \equiv (x \in (A \cup B))\&(x \in (A \cup C))$ definícia zjednotenia
6. $(x \in (A \cup B))\&(x \in (A \cup C)) \equiv x \in (A \cup B) \cap (A \cup C)$ definícia prieniku

Na výber prvku x sme nekládli žiadne obmedzenia. Z toho vyplýva, že každý prvok x z množiny $A \cup (B \cap C)$ patrí aj do množiny $(A \cup B) \cap (A \cup C)$, a teda

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C).$$

Pri dôkaze sme používali len ekvivalentné úpravy výrokov, a teda celý postup možno otočiť a dokázať, že každý prvok x z množiny $(A \cup B) \cap (A \cup C)$ patrí aj do množiny $A \cup (B \cap C)$, a teda platí aj opačná inklúzia

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

Z dokázaných inklúzií potom priamo vyplýva požadovaná rovnosť (identita) množín:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Zovšeobecníme uvedený postup dokazovania množinových identít: vybrali sme ľubovoľný prvok x z množiny ležiacej na ľavej strane dokazovanej množinovej identity. Využili sme definície množinových operácií a výrok „x patrí do zloženej množiny“ sme upravili na zložený výrok, pozostávajúci z jednoduchých výrokov typu „x patrí do množiny (napr.) A“. Tento zložený výrok sme upravili využívajúc poznatky (tautológie, pravidlá odvodenia) výrokovej logiky. Pri úpravách je potrebné uvedomiť si, či sme použili ekvivalentné úpravy (napr. $(p\&q) \equiv (q\&p)$), alebo len „jednostranné“ úpravy (napr. $p\&q \Rightarrow q$). Zložený výrok sme potom spätne upravili do formy „x patrí do zloženej množiny z pravej strany identity“ pomocou definícií množinových operácií. Ak sme vo všetkých krokoch použili len ekvivalentné úpravy, dokázali sme rovnosť množín z pravej a ľavej strany identity. Ak sa však v niektorom kroku vyskytla „jednostranná“ úprava, tak sme dokázali len to, len to, že jedna z množín (na ľavej alebo pravej strane) z dokazovanej identity je podmnožinou druhej.

Úpravy, ktoré sme použili pri dôkaze identity (8) neboli príliš zložité. pri ďalších dôkazoch preto budeme stručnejší a budeme vynechávať komentáre jednotlivých krokov dôkazu. Dokážeme ešte jednu množinovú inklúziu. Dôkaz ostatných vzťahov z tejto vety ponechávame čitateľovi ako cvičenie.

Dôkaz inklúzie $(A \cap B) \subseteq A$**:**

1. $(x \in A \cap B)) \equiv (x \in A)\&(x \in B)$ (definícia prieniku)
2. $(x \in A)\&(x \in B) \Rightarrow (x \in A)$ (tautológia $p\&q \Rightarrow p$)
3. $x \in (A \cap B) \Rightarrow (x \in A)$ (pravidlo sylogizmu (1), (2)).

Keďže tvrdenie platí pre ľubovoľné x, dostávame požadovanú inklúziu $(A \cap B) \subseteq A$. Všimnite si, prečo nemôžeme dôkaz otočiť a dokázať rovnosť — v 2. kroku dôkazu sme namiesto ekvivalencie použili len (jednosmernú) implikáciu. □

Poznámka. Aby sme získali predstavu o množinových vzťahoch, ktoré máme dokazovať, je výhodné nakresliť pre príslušné množiny Vennov diagram.

Úloha 2.8. *Nájdite také množiny* A, B*, pre ktoré platí* $A \subset (A \cup B)$*, ale zároveň* $A \neq (A \cup B)$.

Úloha 2.9. *Dokážte podrobne ostávajúce tvrdenia vety 2.2*

Ostáva nám preskúmať ešte vlastnosti rozdielu a symetrickej diferencie množín. V nasledujúcej vete sa podrobnejšie pozrieme na rozdiel množín a v ďalšej potom na symetrickú diferenciu.

Veta 2.3. *Nech sú* A, B, C *ľubovoľné množiny. Potom platia nasledujúce vzťahy*

1. $(A \cap B) - C = A \cap (B - C)$,
2. $(A \cap B) - C = (A - B) \cap (B - C)$,
3. $(A \cup B) - C = (A - C) \cup (B - C)$,
4. $C - (A \cap B) = (C - A) \cup (C - B)$,
5. $C - (A \cup B) = (C - A) \cap (C - B)$,
6. $(A - B) = A - (A \cap B) = (A \cup B) - B$,
7. $A - (B - C) = (A - B) \cup (A \cap C)$,
8. $(A - B) - C = A - (B \cup C)$.

Dôkaz. Pri dôkaze budeme postupovať ináč, ako sme postupovali pri dôkaze vety 2.2. Nebudeme vychádzať z definícií množinových operácií, ale využijeme už dokázané množinové identity. Budeme sa pridržiavať nasledujúcej taktiky: zoberieme tú stranu rovnosti, ktorá vyzerá zložitejšie a ekvivalentnými úpravami sa ju budeme snažiť transformovať na výraz ležiaci na druhej strane identity. Pri množinových úpravách najprv vyjadríme rozdiel pomocou prieniku a doplnku, podľa potreby použijeme de Morganove pravidlá, aby sme nahradili doplnok zloženej množiny výrazom, obsahujúcim doplnky jednoduchších množín, potom použijeme distributívny, asociatívny, komutatívny zákon

alebo zákony absorbcie a idempotentnosti a upravíme výraz popisujúci množinu na potrebný tvar. Uvedený postup uplatníme pri dôkazoch identít (1) až (8).

$$
\begin{array}{lrcl}
(1) & (A\cap B)-C & = & A\cap B)\cap C^c = (A\cap (B\cap C^c) = A\cap (B-C)\\
(2) & (A\cap B)-C & = & (A\cap B)\cap C^c = (A\cap C^c)\cap (B\cap C^c) = (A-C)\cap (B-C)\\
(3) & (A\cup B)-C & = & (A\cup B)\cap C^c = (A\cap C^c)\cup (B\cap C^c) = (A-C)\cup (B-C)\\
(4) & C-(A\cap B) & = & C\cap (A\cap B)^c = C\cap (A^c\cup B^c) = (C\cap A^c)\cup (C\cap B^c) =\\
 & & = & (C-A)\cup (C-B)\\
(5) & C-(A\cup B) & = & C\cap (A\cup B)^c = C\cap (A^c\cap B^c) = (C\cap A^c)\cap (C\cap B^c) =\\
 & & = & (C-A)\cap (C-B)\\
(6) & A-(A\cap B) & = & A\cap (A\cap B)^c = A\cap (A^c\cup B^c) = (A\cap A^c)\cup (A\cap B^c) =\\
 & & = & \emptyset\cup (A\cap B^c) = (A\cap B^c) = (A-B)\\
(6') & (A\cup B)-B & = & (A\cup B)\cap B^c = (A\cap B^c)\cup (b\cap B^c) = (A\cap B^c)\cup \emptyset =\\
 & & = & (A\cap B^c) = (A-B)\\
(7) & A-(B-C) & = & A\cap (B\cap C^c)^c = A\cap (B^c\cup C) = (A\cap B^c)\cup (A\cap C) =\\
 & & = & (A-B)\cup (A\cap C)\\
(8) & (A-B)-C & = & (A\cap B^c)\cap C^c = A\cap (B^c\cap C^c) = A\cap (B\cup C)^c = A-(B\cup C).
\end{array}
$$

□

Všimnite si rozdiely medzi dôkazmi viet 2.2 a 2.3. Kým v dôkazoch tvrdení vety 2.2 sme robili (zväčša) ekvivalentné úpravy *výrokov*, v dôkazoch vety 2.3 sme robili ekvivalentné úpravy množín. Tento rozdiel si ľudia dosť často neuvedomujú a konštruujú nezmyselné tvrdenia typu $x\in A\vee x\in B = (A\cup B)$, kde sa do rovnosti dávajú neporovnateľné objekty; na jednej strane stojí výrok (výroková forma) a na druhej množina. Pozrieme sa teraz na najzložitejšiu z doteraz zavedených množinových operácií, na symetrickú diferenciu množín.

Veta 2.4. *Nech sú* A, B, C *ľubovoľné množiny. Potom platí*

1. $A\triangle B = B\triangle A$ *(komutatívnosť)*
2. $A\triangle B = (A\cup B)-(A\cap B)$,
3. $A\triangle(B\triangle C) = (A\triangle B)\triangle C$,
4. *rovnica* $X\triangle A = B$ *má jediné riešenie* $X = A\triangle B$.

Dôkaz.

1. Tvrdenie vyplýva priamo z definície symetrickej diferencie.

2. Upravíme pravú stranu identity

$$(A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)^c = (A \cup B) \cap (A^c \cup B^c) =$$
$$= ((A \cup B) \cap A^c) \cup ((A \cup B) \cap B^c) = ((A \cap A^c) \cup (B \cap A^c)) \cup ((A \cap B^c) \cup (B \cap B^c) =$$
$$= \emptyset \cup (B \cap A^c) \cup ((A \cap B^c) \cup \emptyset = (B \cap A^c) \cup ((A \cap B^c) = (B - A) \cup (A - B) = A \triangle B.$$

3. Dôkaz tohto tvrdenia je trocha zdĺhavý a vyžaduje si použitie niekoľkých umelých krokov. Aby sme sa im vyhli, nebudeme upravovať jednu stranu identity na druhú, ale upravíme obe strany identity (ekvivalentnými úpravami) na ten istý výraz:

$$A \triangle (B \triangle C) = [A - (B \triangle C)] \cup [(B \triangle C) - A] =$$
$$= [A - [(B - C) \cup (C - B)]] \cup [[(B - C) \cup (C - B)]] - A] =$$
$$= [A \cap [(B \cap C^c) \cup (C \cap B^c)]^c] \cup [[(B \cap C^c) \cup (C \cap B^c)]] \cap A^c] =$$
$$= [A \cap [(B \cap C^c)^c \cap (C \cap B^c)^c]] \cup [(B \cap C^c) \cup (C \cap B^c)] \cap A^c] =$$
$$= [A \cap [(B^c \cup C) \cap (C^c \cup B)]] \cup (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c) =$$
$$= [A \cap [[(B^c \cup C) \cap C^c)] \cup [(B^c \cup C) \cap B)]] \cup (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c) =$$
$$= [A \cap [[(B^c \cap C^c) \cup (C \cap C^c)] \cup [(B^c \cap B) \cup (C \cap B)]] \cup (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c) =$$
$$= (A \cap B^c \cap C^c) \cup (A \cap C \cap B) \cup (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c) =$$
$$= (A \cap B^c \cap C^c) \cup (A \cap B \cap C) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C)$$

Teraz upravíme pravú stranu identity (3). Mohli by sme postupovať presne tak, ako pri úpravách ľavej strany. Ukážeme si však postup, ktorý sa v matematike v rozličných obmenách často používa. Skúsime využiť už dokázané identity a previesť úlohu—úpravu výrazu $(A \triangle B) \triangle C$ —na úlohu, ktorú sme už vyriešili. Symetrická diferencia je komutatívna (identita (1) vety 2.3), a preto platí rovnosť:

$$(A \triangle B) \triangle C = C \triangle (A \triangle B).$$

Pred chvíľou sme však upravovali výraz $A \triangle (B \triangle C)$, ktorý sa na výraz $(A \triangle B) \triangle C$ veľmi podobá a dospeli sme k výrazu

$$A \triangle (B \triangle C) = (A \cap B^c \cap C^c) \cup (A \cap B \cap C) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C).$$

Teraz už stačí len dosadiť $A \leftarrow C$, $B \leftarrow A$, $C \leftarrow B$ do predchádzjúceho výrazu a dostávame

$$C \triangle (A \triangle B) = (C \cap A^c \cap B^c) \cup (C \cap A \cap B) \cup (C^c \cap A \cap B^c) \cup (C^c \cap A^c \cap B)$$

Dá sa ľahko vidieť, že výrazy pre $A \triangle (B \triangle C), (A \triangle B) \triangle C$ sa zhodujú.

4. Najprv dokážeme, že množina $A \triangle B$ je riešením rovnice $X \triangle A = B$:

$$(A \triangle B) \triangle A = A \triangle (A \triangle B) = (A \triangle A) \triangle B = \emptyset \triangle B = B.$$

Pri úpravách sme postupne využili komutatívnosť a asociatívnosť symetrickej diferencie. Teraz ukážeme, že riešenie $X = A \triangle B$ je jediné. Použijeme dôkaz sporom.

Budeme predpokladať, že existuje množina $Y \neq X$, pre ktorú platí $Y \triangle A = B$. Spočítame symetrickú diferenciu množín

$$(X \triangle A) \triangle (Y \triangle A) = X \triangle A \triangle Y \triangle A = X \triangle Y \triangle A \triangle A = X \triangle Y.$$

Na druhej strane,

$$X \triangle Y = B \triangle B = \emptyset.$$

To znamená, že $X = Y$ čo je hľadaný spor, ktorý dokazuje naše tvrdenie.

□

Vytvorili sme si dosť široký repertoár množinových identít a získali už isté skúsenosti s dokazovaním rovnosti množín. Aby sme dokázali, že nejaké dve množiny sú vo vzťahu inklúzie sme však museli namáhavo dokazovať, že každý prvok prvej množiny (podmnožiny) je aj prvkom druhej množiny (nadmnožiny). Nasledujúca veta ukazuje, ako možno dokazovanie množinovej inklúzie previesť na overovanie rovnosti množín.

Veta 2.5. *Nech sú* A, B *ľubovoľné množiny, podmnožiny univerzálnej množiny* U. *Potom sú nasledujúce výroky ekvivalentné*

1. $A \subseteq B$,
2. $A \cap B = A$,
3. $A \cup B = B$,
4. $A - B = \emptyset$,
5. $A^c \cup B = U$,
6. $A \triangle B = B - A$.

Dôkaz. Máme dokázať, že ľubovoľné dve z tvrdení 1 až 6 sú ekvivalentné. To znamená, že potrebujeme dokázať buď $\binom{6}{2} = 15$ ekvivalencií, alebo $6 \times 5 = 30$ implikácií. Ukážeme, ako sa dá dokazovanie veľkého počtu ekvivalencií optimalizovať. Budeme postupne dokazovať platnosť implikácií (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (1); platnosť ostatných implikácií odvodíme potom pomocou pravidla sylogizmu. Napríklad dôkaz ekvivalencie (2)$\equiv$ (6) prevedieme na dôkaz implikácií (2) $\Rightarrow$ (6) a (6) $\Rightarrow$ (2):

$$\frac{(2) \Rightarrow (3), (3) \Rightarrow (4), (4) \Rightarrow (5), (5) \Rightarrow (6)}{(2) \Rightarrow (6)}$$

$$\frac{(6) \Rightarrow (1), (1) \Rightarrow (2)}{(6) \Rightarrow (2)}.$$

V oboch prípadoch sme použili pravidlo sylogizmu. Pristúpime teraz k dôkazu vety 2.5.

1. (1) $\Rightarrow$ (2). Predpokladáme, že $A \subseteq B$ a za tohoto predpokladu potrebujeme dokázať dve inklúzie:

(a) $A \cap B \subset A$. Podľa vety 2.2 táto inklúzia platí pre ľubovoľné množiny A, B.

(b) $A \subseteq (A \cap B)$. Platnosť tejto inklúzie dokážeme sporom. Predpokladáme, že $A \subseteq B$ a súčasne neplatí $A \subseteq (A \cap B)$. Rozpíšeme druhý predpoklad:

$$\begin{aligned}
&\neg A \subseteq (A \cap B) \equiv \\
&\equiv \neg\forall x[(x \in A) \Rightarrow (x \in A \cap B)] \equiv \exists x \neg[(x \in A) \Rightarrow (x \in A)\&(x \in B)] \equiv \\
&\equiv \exists x[(x \in A)\&\neg[(x \in A)\&(x \in B)] \equiv \exists x[(x \in A)\&[(x \notin A) \vee (x \notin B)] \equiv \\
&\equiv \exists x[(x \in A)\&(x \notin A) \vee (x \in A)\&(x \notin B)] \equiv \exists x[(x \in A)\&(x \notin B)].
\end{aligned}$$

Predpokladali sme však, že $A \subseteq B$, t.j. že $\forall x[(x \in A) \Rightarrow (x \in B)]$. Predpoklad je v spore s odvodeným tvrdením $\exists x[(x \in A)\&(x \notin B)]$. To znamená, že musí platiť $A \subseteq (A \cap B)$.

2. (2) $\Rightarrow$ (3). Predpokladáme, že platí $A \cap B = A$. Potom však

$$A \cup B = (A \cap B) \cup B = B.$$

Využili sme predpoklad, vyjadrili množinu A v tvare prieniku $(A \cap B)$ a potom použili zákon absorbcie z vety 2.2.

3. (3) $\Rightarrow$ (4). Budeme postupovať podobne ako v predchádzajúcom prípade. Predpokladáme, že platí $A \cup B = B$. Potom

$$A - B = A - (A \cup B) = A \cap (A \cup B)^c = A \cap (A^c \cap B^c) = (A \cap A^c) \cap B^c = \emptyset.$$

4. (4) $\Rightarrow$ (5). Využijeme identity (16) a (17) z vety 2.2.

$$A^c \cup B \cup \emptyset = A^c \cup B \cup (A - B) = A^c \cup B \cup (A \cap B^c) = (A^c \cup B \cup A) \cap (A^c \cup B \cup B^c) = U \cap U = U.$$

5. (5) $\Rightarrow$ (6). Túto implikáciu dokážeme sporom. Predpokladáme, že platí $A^c \cup B = U$. Vo všeobecnom prípade $A \triangle B = (A - B) \cup (B - A)$. Ak má platiť $A \triangle B = (B - A)$, množina $A - B$ musí byť prázdna. Predpokladajme, že tomu tak nie je, t.j. že $A - B \neq \emptyset$. To však znamená, že existuje prvok, označme ho a, $a \in A - B$. Potom $a \in A \cap B^c$. Prvok a nepatrí do množiny B, ani do množiny A^c, a teda nemôže patriť ani do zjednotenia týchto dvoch množín: $a \notin (A^c \cup B)$. Ale podľa predpokladu $A^c \cup B = U$ a to znamená, že $a \notin U$. Spor.

6. (6) $\Rightarrow$ (1). Opäť použijeme dôkaz sporom. Nech $A \triangle B = (B - A)$ a súčasne $\neg(A \subseteq B)$. To znamená, že existuje prvok $a \in A$, ktorý nepatrí do B; t.j. $a \in A - B$. Potom $a \in (A \triangle B)$ ale $a \notin B - A$. To znamená, že $A \triangle B \neq (B - A)$, spor.

□

Poznámky.

1. V dôkazoch tvrdení predchádzajúcej vety sme niekoľkokrát využili nasledujúci myšlienkový postup: Vo všeobecnom prípade platilo nejaké tvrdenie—napríklad $A \triangle B = (A - B) \cup (B - A)$. Prijali sme nejaké ďalšie predpoklady ($A^c \cup B = U$) a dokázali sme špeciálny prípad všeobecného tvrdenia; $A \triangle B = (B - A)$. Musíme si uvedomiť, že vo všeobecnom prípade vzťah $A \triangle B = (B - A)$ neplatí; jeho platnosť je podmienená platnosťou ďalšieho tvrdenia ($A^c \cup B = U$). Na to si treba dávať pozor najmä pri dôkazoch zložitejších tvrdení, keď už nemusí byť zrejmé, aké predpoklady platia. V opačnom prípade sa stane, že sa budú používať tvrdenia, ktoré za daných predpokladov nie sú pravdivé.

2. Negácia tvrdenia $A \subseteq B$ je ekvivalentná tvrdeniu, že existuje nejaký prvok, označme ho tentoraz x, ktorý patrí do množiny A a nepatrí do množiny B; t.j. $x \in A - B$. Podobne možno negáciu tvrdenia $A = B$ formulovať aj tak, že $A \triangle B \neq \emptyset$, resp. že existuje prvok $x \in A \triangle B$.

3. Námaha, ktorú sme vynaložili pri dokazovaní vlastností symetrickej diferencie vo vete 2.3 sa nám vráti, keď máme upravovať zložité výrazy obsahujúce operátory symetrickej diferencie. Napríklad beznádejne vyzerajúci výraz

$$((A \triangle B) \triangle (C \triangle (D \triangle A) \triangle B) \triangle (C \triangle B)) \triangle ((A \triangle B) \triangle (C \triangle D \triangle (A \triangle C)))$$

upravíme za niekoľko sekúnd, ak si uvedomíme, že symetrická diferencia

- je asociatívna (môžeme zrušiť zátvorky),
- je komutatívna (môžeme zmeniť poradie operandov);
- a pre ľubovoľnú množinu X platí $X \triangle X = \emptyset$.

To znamená, že stačí spočítať, koľkokrát sa ktorý operand vo výraze vyskytuje a do výsledku uviesť len tie, ktoré sa vo výraze vyskytujú nepárny počet krát. Pozor! Platí to len v prípade, ak výraz neobsahuje iné operátory, ako operátory symetrickej diferencie. V našom príklade sa vo výraze množina A vyskytuje 4-krát, B—4-krát, C—4-krát,CD—2-krát; t.j. výsledkom je prázdna množina.

Úloha 2.10. *Zapíšte formálne negácie tvrdení* $A \subseteq B$, $A = B$ *a presvedčte sa o pravdivosti predchádzajúcej poznámky.*

Úloha 2.11. *Dokážte zostávajúcich 24 implikácií vety 2.5.*

Pomocou vety 2.5 ľahko dokážeme niekoľko užitočných tvrdení.

Veta 2.6. *(Nech sú* A, B, C *ľubovoľné množiny. Potom*

1. *inklúzia* $C \subseteq A \cap B$ *platí práve vtedy, ak* $C \subseteq A$ *a* $C \subseteq B$*;*

2. *inklúzia* $A \cup B \subseteq C$ *platí práve vtedy, ak* $CA \subseteq C$ *a* $B \subseteq C$.

Dôkaz. Vetu možno dokázať viacerými spôsobmi. Skôr, ako ju začneme dokazovať, všimnime si, aká je logická štruktúra jej tvrdení. Aby sa to dalo ľahšie rozlíšiť, označme výrokovými premennými elementárne výroky z ktorých zložené tvrdenia pozostávajú:

p výrok $C \subseteq A \cap B$,

q výrok $C \subseteq A$,

r výrok $C \subseteq B$,

s výrok A, B, C sú ľubovoľné množiny.

Analogicky by sme mohli popísať elementárne výroky, z ktorých pozostáva druhé tvrdenie. Prvé tvrdenie potom možno schematicky zapísať takto:

$$\frac{s}{p \equiv (q\&r)}$$

(v „čitateli“ je uvedený predpoklad a v „menovateli“ tvrdenie, ktoré treba dokázať.) Tvrdenie, ktoré máme dokázať, má tvar ekvivalencie. Dokázať ekvivalenciu znamená dokázať dve implikácie (a tým zároveň aj ich konjunkciu):

$$\frac{s}{p \Rightarrow (q\&r), (q\&r) \Rightarrow p}.$$

Prikročíme k samotnému dôkazu prvého tvrdenia. Implikáciu $p \Rightarrow (q\&r)$ dokážeme sporom. Budeme predpokladať platnosť predpokladov $s, \neg(p \Rightarrow (q\&r))$; t.j. $p\&\neg(q\&r)$. Nech teda $C \subseteq A \cap B$ a $\neg((C \subseteq A)\&(A \subseteq B))$. To znamená, že platí tvrdenie $\neg((C \subseteq A) \vee \neg(C \subseteq B))$, a teda existuje prvok $a \in C - A$ alebo $b \in C - B$[5] Keďže $C - A \subseteq C$, $C - B \subseteq C$ a $C \subseteq A \cap B$, potom musí byť aj množina $C - A$ podmnožinou $A \cap B$ a rovnako $C - B \subseteq A \cap B$. Kam však bude patriť prvok a (resp. b)? Prvok a nepatrí do množiny A, a teda nemôže patriť ani do množiny $A \cap B$ (analogicky prvok b). To však znamená, že množina C nemôže byť podmnožinou množiny $A \cap B$. Spor.

Druhú implikáciu, $(q\&r) \Rightarrow p$ dokážeme priamo. Nech platí $C \subseteq A$, $C \subseteq B$. Použijeme tvrdenie (2) vety 2.5 a dostávame $C \cap A = C$, $C \cap B = C$. Potom však platí

$$(A \cap B) \cap C = A \cap (B \cap C) = A \cap C = C.$$

Posledné tvrdenie je však podľa vety 2.5 ekvivalentné s tvrdením $C \subseteq A \cap B$.

Druhé tvrdenie sa dokazuje analogicky, a preto jeho dôkaz prenechávame čitateľovi. □

Ďalšie dôležité množinové vzťahy uvádzame v cvičeniach. Odporúčame preto čitateľovi, aby cvičenia vyriešil. Pripomíname, že symboly A, B, C, resp. $A_1, A_2, \ldots, A_n$; $B_1, \ldots, B_n$ označujú v nasledujúcich cvičeniach ľubovoľné množiny.

[5] tvrdenie má tvar disjunkcie, ktorá je pravdivá ak nastane ktorýkoľvek z nasledujúcich prípadov:

- existuje prvok $a \in C - A$ ale neexistuje prvok $b \in C - B$;
- existuje prvok $b \in C - B$ ale neexistuje prvok $a \in C - A$;
- existujú dva rôzne prvky $a \in C - A$ a $b \in C - B$;
- existuje prvok $a \in C - A$ a $b \in C - B$; $a = b$.

Úloha 2.12. *Dokážte druhé tvrdenie vety 2.6.*

Úloha 2.13. *Dokážte vetu 2.6 priamo a nepriamo.*

Úloha 2.14. *Ak* $A \subseteq B$*, tak pre ľubovoľnú množinu* C *platí*

1. $A \cup C \subseteq B \cup C$,
2. $A \cap C \subseteq B \cap C$,
3. $B^c \subseteq A^c$,
4. $A - C \subseteq B - C$,
5. $C - B \subseteq C - A$.

Úloha 2.15. *Určte, v akom sú vzťahu množiny* $A \triangle C$, $B \triangle C$*, ak* $A \subseteq B$.

Úloha 2.16. *Nájdite množiny, pre ktoré platia nasledujúce vzťahy:*

$$A \cup B = A \cup C, \quad B \neq C.$$

V akom vzťahu musia byť množiny A, B, C*, aby platila rovnosť* $A \cup B = A \cup C$*?*

Úloha 2.17. *Znázornite pomocou Vennových diagramov množiny, spĺňajúce nasledujúce podmienky*

1. $A \cup B \subseteq A \cup C, \quad B \not\subseteq C$,
2. $A \cap B \subseteq A \cap C, \quad B \not\subseteq C$,
3. $A \cup B = C \cup B, \quad A \neq C$,
4. $A \cap B = C \cap B, \quad A \neq C,$.

Úloha 2.18. *Dokážte,* $A \cup B = \emptyset$ *že práve vtedy, ak* $A = \emptyset, B = \emptyset$.

Úloha 2.19. *Ak* $A_1 \subseteq A_2,\ B_1 \subseteq B_2$ *tak*

$$A_1 \cup B_1 \subseteq A_2 \cup B_2, \quad A_1 \cap B_1 \subseteq A_2 \cap B_2.$$

Úloha 2.20. *Rovnosť* $A \cup (B \cap C) = (A \cup B) \cap C$ *platí práve vtedy, ak* $A \subseteq C$.

Úloha 2.21. *Rovnosť* $(A \cup B) = A \cap C$ *platí práve vtedy, ak* $B \subseteq A \subseteq C$.

Úloha 2.22. *Ak existuje taká množina* X*, že* $A \cap X = B \cap X$ *a* $A \cup X = B \cup X$*, tak* $A = B$.

Úloha 2.23. *Nech* $A_1 \cup A_2 = B_1 \cup B_2$*; zistite, či musí platiť* $A_1 = B_1,\ A_2 = B_2$.

Úloha 2.24. *Dokážte, že nasledujúce tvrdenia sú ekvivalentné*

1. $A \cup B = A \cup C = B \cup C$ *a*
2. $A \subseteq B \cup C,\ B \subseteq A \cup C,\ C \subseteq A \cup B$.

Úloha 2.25. *Dokážte, že nasledujúce tvrdenia sú ekvivalentné*

1. $A \cap B = A \cap C = B \cap C$,
2. $A \cap C \subseteq B,\ B \cap C \subseteq A,\ A \cap B \subseteq C$.

Úloha 2.26. *Dokážte ekvivalenciu nasledujúcich podmienok*

1. $A = B = C$,
2. $A \subseteq B \cap C,\ B \subseteq A \cap C,\ BC \subseteq A \cap B$,
3. $A \cup B \subseteq C,\ A \cup C \subseteq B,\ B \cup C \subseteq A$.

Úloha 2.27. *Nech* $A \subseteq U,\ B \subseteq U$. *Určte všetky množiny* $X \subseteq U$, *pre ktoré platí (nie súčasne):*

1. $A \cup X = B$,
2. $A \cap X = B$.

Úloha 2.28. $(A = B) \equiv (A^c = B^c)$.

Úloha 2.29. $(A - B) \cup B = A \cup B$.

Úloha 2.30. *Dokážte, že rovnosť* $A - B = A$ *platí práve vtedy, ak* $A \cap B = \emptyset$.

Úloha 2.31. *Ak* $A \subseteq B$ *tak rovnosť* $B - A = B$ *platí práve vtedy, ak* $A = \emptyset$.

Úloha 2.32. $(A - B) - C = (A - C) - B$.

Úloha 2.33. $(A \cap B) - (A \cap C) = A \cap (B - C)$.

Úloha 2.34. $(A - C) - (B - C) = A - (B \cup C)$.

Úloha 2.35. $A \cup (B - C) = (A \cup B) - (C - A)$.

Úloha 2.36. $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$

Úloha 2.37. *Rovnosť* $(A \cup B) - B = A$ *platí práve vtedy, ak* $(A \cap B) = \emptyset$.

Úloha 2.38. *Inklúzia* $A - B \subseteq C$ *platí práve vtedy, ak* $A - C \subseteq B$.

Úloha 2.39. *Rovnosť* $A - B = A \cup B$ *platí práve vtedy, ak* $B = \emptyset$.

Úloha 2.40. *Nasledujúce tvrdenia sú ekvivalentné*

1. $A - B \subseteq A - C$,
2. $A \cap C \subseteq A \cap B$.

Úloha 2.41. *Inklúzia* $A - C \subseteq B - C$ *platí práve vtedy, ak* $A \subseteq B \cup C$.

Úloha 2.42. *Rovnosť* $A \triangle B = A$ *platí práve vtedy, ak* $B = \emptyset$.

Úloha 2.43. *Rovnosť* $A \triangle B = \emptyset$ *platí práve vtedy, ak* $B = A$.

Úloha 2.44. *Rovnosť* $A \triangle B = A \cup B$ *platí práve vtedy, ak* $A \cap B = \emptyset$.

Úloha 2.45. *Rovnosť* $A \triangle B = A \cap B$ *platí práve vtedy, ak* $A = B = \emptyset$.

Úloha 2.46. *Rovnosť* $A \triangle B = A \triangle C$ *platí práve vtedy, ak* $B = C$.

Úloha 2.47. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

Úloha 2.48. $A \triangle B) \triangle (A \cap B) = A \cup B$.

Úloha 2.49. $(A \cup C) \triangle (B \cup C) = (A - C) \triangle (B - C)$.

Úloha 2.50. $(A - C) \subseteq (A - B) \cup (B - C)$.

Úloha 2.51. $(A \triangle C) \subseteq (A \triangle B) \cup (B \triangle C)$.

Úloha 2.52. *Dokážte (napríklad matematickou indukciou) nasledujúce identity (*$n > 1$*):*

1. $A_1 \cup \cdots \cup A_n = (A_1 - A_2) \cup \cdots \cup (A_{n-1} - A_n) \cup (A_n - A_1) \cup (A_1 \cap \cdots \cap A_n)$,
2. $A_1 \cup \cdots \cup A_n = A_1 \cup (A_2 - A_1) \cup [A_3 - (A_1 \cup A_2)] \cup \cdots \cup [A_n - (A_1 \cup \cdots \cup A_{n-1})]$.

Úloha 2.53. *Vyjadrite ostatné množinové operácie pomocou uvedených operácií, alebo ukážte, že sa to nedá:*

1. $\{\cup, ^c\}$,
2. $\{\cap, ^c\}$,
3. $\{\cap, \cup\}$,
4. $\{\cup, \triangle\}$.

2.5 Potenčná množina

Videli sme, že množiny môžu byť prvkami iných množín. To na prvý pohľad otvára nepreberné možnosti vytvárania nových množín (napr. množina, ktorej prvkami sú množiny množín a podobne). Na druhej strane, Russelov paradox („množina“ všetkých množín) nás nabáda k opatrnosti pri vytváraní príliš voľne definovaných veľkých „množín“. Asi najjednoduchšie by bolo obmedziť sa na množiny s jednoduchými, „neštruktúrovanými“ prvkami. V matematike sa však nezaobídeme bez množín, ktorých prvkami sú množiny (napríklad univerzálna množina). Aby sme sa pri tom vyhli podobným problémom ako je Russelov paradox, budeme pracovať s množinami, ktoré sa vytvárajú dobre definovaným spôsobom. „Veľkou“ množinou množín, ktorá môže poslúžiť ako univerzálna množina s prvkami ktorej sa dá bezpečne pracovať, je tzv. *potenčná množina*.

Definícia 2.9. *Nech je daná množina* M. *Potenčnou množinou množiny* M *nazývame množinu všetkých podmnožín množiny* M*:*

$$\mathcal{P}(M) = \{X | X \subseteq M\}.$$

Príklad 2.4. *Nech* $M = \{1, 2\}$*, potom* $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{1.2\}\}$.

Zdá sa, že potenčná množina má podstatne viac prvkov, ako pôvodná množina. Túto hypotézu podporuje poznanie, že pre každý prvok x pôvodnej množiny obsahuje potenčná množina jednoprvkovú množinu $\{x\}$, prvok x sa vyskytuje aj v dvojprvkových, trojprvkových množinách,... potenčnej množiny. V prípade konečných množín budú potenčné množiny omnoho „väčšie“, ale stále budú mať konečný počet prvkov. Štúdium potenčných množín nekonečných množín si vyžiada trochu silnejší aparát a povedie k zaujímavým, pre niekoho možno aj prekvapujúcim výsledkom. Ponechajme teraz bokom množiny s nekonečným počtom prvkov a uvažujme len potenčné množiny konečných množín. Predpokladajme, že skúmaná množina A je (napr.) n-prvková. Aj keď v množine nezáleží na poradí prvkov, predpokladajme, že tentoraz sú prvky množiny nejakým spôsobom usporiadané $A = \{a_1, \ldots, a_n\}$. Každá podmnožina množiny A sa dá jednoznačne zadať tým, že povieme, ktoré prvky z A do podmnožiny patria, a ktoré nie. (Neskôr zavedieme pojem charakteristickej funkcie množiny, teraz nám však pôjde len o určenie počtu všetkých podmnožín danej množiny, a preto sa uspokojíme s jednoduchšou charakterizáciou podmnožín.) Každej podmnožine B množiny A priradíme binárny vektor dĺžky n. Tento vektor bude mať na i-tom mieste 1, ak $a_i \in B$ a 0, ak $a_i \notin B$. Je zrejmé, že každej podmnožine prislúcha práve jeden takýto binárny vektor, a teda všetkých podmnožín n-prvkovej množiny je toľko, ako binárnych vektorov dĺžky n. A tých je 2^n. Ilustrujme si tento poznatok na príklade.

Príklad 2.5. *Nech* $M = \{1, 2, 3\}$*, potom potenčná množina* $\mathcal{P}(M)$ *má* $2^3 = 8$ *prvkov. Jednotlivé podmnožiny a im zodpovedajúce binárne vektory sú uvedené v nasledujúcej tabuľke.*

$\emptyset$	000
$\{a_1\}$	100
$\{a_2\}$	010
$\{a_3\}$	001
$\{a_1, a_2\}$	110
$\{a_1, a_3\}$	101
$\{a_2, a_3\}$	011
$\{a_1, a_2, a_3\}$	111

Práca s množinami množín bude spočiatku trocha náročnejšia, ako skúmanie množín s jednoduchými prvkami. Treba sa naučiť rozlišovať prvok (x), jednoprvkovú množinu obsahujúcu daný prvok ($\{x\}$), množinu, ktorej prvkom je množina obsahujúca daný prvok($\{\{x\}\}$). Keď naviac do jednej množiny dáme prvky, množiny prvkov, množiny množín prvkov, dokazovanie vlastností takejto množiny môže byť dosť náročné. Názorným príkladom sú množiny $\emptyset$ – prázdna množina, $\{\emptyset\}$, čo je jednoprvková množina, obsahujúca ako prvok prázdnu pmnožinu, $\{\emptyset, \{\emptyset\}\}$ čo je dvojprvková množina, ktorej prvkami sú prázdna množina a množina $\{\emptyset\}$, atď. Treba sa naučiť dobre počítať, koľko množinových zátvoriek je „okolo“ jednotlivých prvkov množiny a rozlišovať úrovne jednotlivých

prvkov. Veríme, že riešenie nasledujúcich úloh o potenčných množinách v tom čitateľovi pomôže.

Úloha 2.54. *Zostrojte potenčné množiny nasledujúcich množín:*

1. $\emptyset$,
2. $\{\emptyset\}$,
3. $\{\emptyset, \{\emptyset\}\}$,
4. $\{a\}$,
5. $\{a, b, \{a\}\}$.

Niektoré vzťahy medzi množinami sa prenášajú aj do vzťahov medzi ich potenčnými množinami.

Príklad 2.6. *Nech* $A \subset B$*, potom* $\mathcal{P}(A) \subset \mathcal{P}(B)$*. Dokážeme toto tvrdenie. Nech je* X *ľubovoľná množina, taká, že* $X \in \mathcal{P}(A)$*. Z definície potenčnej množiny vyplýva, že* $X \subseteq A$*. Keďže* $A \subset B$*, platí* $X \subset B$*. Opäť využijeme definíciu potenčnej množiny a z poslednej inklúzie odvodíme, že* $X \in \mathcal{P}(B)$*. To znamená, že* $\mathcal{P}(A) \subset \mathcal{P}(B)$*. Ukážeme, že ak* $A \subset B$ *a* $A \neq B$*, tak* $\mathcal{P}(A) \neq \mathcal{P}(B)$*. Z predpokladov* $A \subset B$ *a* $A \neq B$ *vyplýva, že existuje prvok* $y \in B - A$*. Potom* $\{y\} \in \mathcal{P}(B)$*, ale* $\{y\} \notin \mathcal{P}(A)$*. Tým sme dokázali, že ak je inklúzia medzi množinami* A, B *ostrá, bude zodpovedajúca ostrá inklúzia aj medzi ich potenčnými množinami.*

Dokážte nasledujúce tvrdenia

Úloha 2.55. $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$

Úloha 2.56. $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

Úloha 2.57. *Zistite, za akých podmienok sa inklúzia v predchádzajúcej úlohe mení na rovnosť.*

Úloha 2.58. *Ilustrujte vzťahy v úlohách 2.55 a 2.56 na konkrétnych množinách*

Úloha 2.59. *Čo sa dá povedať o potenčných množinách množín, ktoré majú tvar doplnku, rozdielu a symetrickej diferencie množín (*$\mathcal{P}(A^c)), \mathcal{P}(A - B)), \mathcal{P}(A \triangle B)$*) ?*

Poznámka. V tejto kapitole sme neformálne popísali základné množinové pojmy. Úroveň poznania, ktoré sme získali, by mala postačovať na to, aby čitateľ mohol úspešne využívať množinové pojmy pri riešení väčšiny matematických úloh. Existujú však aj problémy, na ktoré intuitívna (naivná) teória množín nestačí. Niektoré z nich rozoberáme podrobnejšie v kapitole 8, historickému pohľadu na vývoj teórie množín je venovaná časť 8.9.

Kapitola 3

Usporiadaná dvojica a karteziánsky súčin

V predchádzajúcej kapitole sme študovali vlastnosti množín a vzťahy medzi množinami bez toho, aby sme sa zamýšľali nad tým, či sú množiny „amorfné“, alebo majú nejakú vnútornú štruktúru. V matematike a najmä v informatike budeme často pracovať s množinami, ktorých prvky budeme potrebovať porovnávať, usporadúvať, rozdeľovať do disjunktných tried, zoskupovať podľa nejakých kritérií, popisovať vzťahy medzi prvkami i hľadať korešpondenciu medzi rozličnými množinami. Aby sme mohli študovať takéto „štruktúrované“ množiny, potrebujeme si vytvoriť vhodný matematický aparát. V tejto kapitole zavedieme dva kľúčové pojmy; *usporiadaná dvojica* a *karteziánsky súčin*, ktoré nám neskôr umožnia matematicky korektne definovať zložitejšie (a dúfajme, že aj zaujímavejšie) objekty, ako boli doteraz preberané „jednoduché“ množiny; relácie a zobrazenia.

3.1 Usporiadaná dvojica

Keď sme zadávali množinu vymenovaním prvkov, nezáležalo na tom, v akom poradí boli prvky v množine uvedené. Tú istú množinu[1] bolo vo všeobecnosti možné zadať rôznymi spôsobmi; napr. $\{a, b, c\} = \{b, c, a\} = \{c, a, b\}$.

V mnohých prípadoch však poradie prvkov v množine je podstatné. Tak napríklad zápis 5.8.2003 sa dá intepretovať ako 5. august 2003, ale aj 8. máj 2003 v závislosti na tom, ktoré číslo interpretujeme ako mesiac a ktoré ako deň.

Pevné poradie konečného[2] počtu prvkov možno stanoviť ich vyjadrením vo forme tzv. usporiadanej n-tice. Postupnosť prvkov

$$a_1, \ldots, a_n \qquad n \geq 2,$$

[1] aspoň dvpojprvkovú

[2] Usporiadať sa dá aj nekonečný počet prvkov. Tým sa však budeme zaoberať až v kapitole 8.

udeme nazývať usporiadanou n-*ticou (vektorom) prvkov* a označovať symbolicky výrazom $(a_1, \ldots, a_n)$. Prvok a_i, $i = 1, \ldots, n$ budeme nazývať i-tym prvkom usporiadanej n-tice. Pripomenieme ešte, že prvky usporiadanej n-tice nemusia byť navzájom rôzne. Intuitívne je jasné, že dve usporiadané n-tice sa rovnajú práve vtedy, ak sa rovnajú zodpovedajúce prvky týchto n-tíc:

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \equiv (a_1 = b_1) \& \ldots \& (a_n = b_n).$$

V predchádzajúcej kapitole (Russellov paradox) sme videli, že na intuitívnych predstavách sa nedajú spoľahlivo stavať matematické teórie. Naša „definícia“ usporiadanej n-tice sa opierala o zatiaľ nedefinovaný pojem postupnosti. Aby sme tento nedostatok odstránili, definujeme korektne pojem usporiadanej dvojice pomocou množín a potom pomocou usporiadanej dvojice zavedieme aj pojem usporiadanej n-tice.

Definícia 3.1. *Nech sú* a, b *prvky nejakej množiny* A. *Usporiadanou dvojicou prvkov* a, b *budeme nazývať množinu* $\{\{a\}, \{a, b\}\}$. *Usporiadanú dvojicu prvkov* a, b *budeme označovať výrazom* (a, b)*; pričom prvok* a *budeme nazývať prvým prvkom a prvok* b *druhým prvkom usporiadanej dvojice* (a, b).

Skôr ako použijeme usporiadanú dvojicu na zavedenie usporiadanej n-tice, musíme ukázať korektnosť definície.

Veta 3.1. *Usporiadaná dvojica* (a, b) *sa rovná usporiadanej dvojici* (c, d) *práve vtedy, ak* $a = c, b = d$.

Dôkaz. Je zrejmé, že ak $a = c$, $b = d$, tak $\{a\} = \{c\}$, $\{a, b\} = \{c, d\}$ a potom aj $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$; t.j. $(a, b) = (c, d)$.

Dokážeme opačnú implikáciu. Budeme rozlišovať dva prípady:

1. $a = b$; v tomto prípade $(a, b) = (a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$. Ak $(a, a) = (c, d)$, tak potom $\{\{c\}, \{c, d\}\} = \{\{a\}\}$; a to znamená, že $\{c\} = \{a\}$, resp. $c = a$ a $\{c, d\} = \{a\}$, t.j $d = a$. V tomto prípade teda $a = b = c = d$ a tvrdenie platí.

2. $a \neq b$. Máme dokázať rovnosť dvoch dvojprvkových množín. Teoreticky môžu nastať tieto možnosti.

   (a) $\{a\} = \{c\}, \{a, b\} = \{c\}$. Z druhej rovnosti však vyplýva, že $a = b = c$, čo je spor s predpokladom $a \neq b$.

   (b) $\{a\} = \{c, d\}$. Vtedy $a = c = d$, ale to znamená, že $\{a, b\} = \{c\}$, a teda aj $a = b = c$, čo je spor s predpokladom $a \neq b$. Zostáva nám posledná možnosť

   (c) $\{a\} = \{c\}, \{a, b\} = \{c, d\}$. Ak by sa $b \neq d$, potom $d = a = c$, a teda $b = d$, spor. To znamená, že $b = d$ a tvrdenie je dokázané.

□

Úloha 3.1. *Ak by sme usporiadanú dvojicu* (a, b) *definovali vzťahom* $(a, b) = \{a, b\}$*, veta 3.1 by neplatila. Dokážte!*

Úloha 3.2. *Ako vyzerá množinová reprezentácia usporiadanej dvojice* (a, a)*?*

Tak ako sme už naznačovali, pojem usporiadanej dvojice môžeme zovšeobecniť a zaviesť pomocou usporiadanej dvojice aj pojem usporiadanej n-tice.

Definícia 3.2. *Pre ľubovoľné prirodzené* $n > 1$ *nazveme usporiadanou* n*-ticou množinu*

1. $(a_1, a_2) = \{\{a_1\}, \{a_1, a_2\}\}$,
2. $(a_1, \ldots, a_n) = ((a_1, \ldots a_{n-1}), a_n) \quad n > 2$.

Úloha 3.3. *Vyjadrite usporiadanú trojicu* (a, b, c) *v podobe množiny podľa definície 3.2.*

Chvíľu sa ešte budeme zaoberať usporiadanou trojicou (a, b, c). Podľa definície 3.2 $(a, b, c) = ((a, b), c)$. Zaviesť usporiadanú trojicu pomocou usporiadanej dvojice možno však aj iným spôsobom, napríklad $(a, b, c) = (a, (b, c))$.

Úloha 3.4. *Zistite, či sa množinové reprezentácie usporiadaných trojíc, definovaných podľa definície 3.2 a ako* $(a, b, c) = (a, (b, c))$ *rovnajú!*

Podstatnú vlastnosť usporiadaných n-tíc vyjadruje nasledujúca veta, ktorá je zovšeobecnením vety 3.1.

Veta 3.2. *Usporiadaná* n*-tica* $(a_1, \ldots, a_n)$ *sa rovná usporiadanej* n*-tici* $(b_1, \ldots, b_n)$ *práve vtedy, ak* $a_1 = b_1, \ldots, a_n = b_n$.

Dôkaz. Vyplýva priamo z definície 3.2 a vety 3.1, a preto ho ponechávame čitateľovi. □

Poznámka. V ďalšom sa najčastejšie budeme zaoberať usporiadanými dvojicami.

3.2 Karteziánsky súčin

Mnohé dôležité vlastnosti rôznych objektov je možné popísať pomocou množín usporiadaných n-tíc. Napríklad pracovné zaradenie pracovníka v rámci organizácie je možné popísať pomocou usporiadanej trojice (meno, pracovisko, funkcia); podstatná informácia o daňovníkovi pre daňový úrad sa dá zapísať pomocou usporiadanej 7-ice (meno/názov daňovníka, typ dane, výška dane, dátum, k ktorému má splniť daňovú povinnosť, dátum podania daňového priznania, dátum zaplatenia príslušnej dane); register trestov vydáva informáciu v podobe usporiadanej trojice (meno, dátum, má/nemá k danému dátumu záznam v registri trestov). V podstate akýkoľvek dotazník s presne definovanými možnosťami odpovedí na jednotlivé otázky predstavuje usporiadanú n-ticu. Aj mnohé objekty v matematike a informatike môžeme definovať pomocou usporiadaných n-tíc (graf, ako usporiadanú dvojicu (množina vrcholov, množina hrán), konečný automat ako usporiadanú štvoricu (vstupná abeceda, množina stavov, prechodová funkcia, koncový

stav) a pod.) Vytvoríme aparát, ktorý nám umožní popísať množiny usporiadaných n-tíc a korektne s nimi pracovať. Zavedieme najprv pojem *karteziánskeho súčinu množín*, pomocou ktorého budeme z východiskových množín vytvárať akúsi základnú množinu usporiadaných n-tíc, potom preskúmame ako závisia vlastnosti karteziánskeho súčinu od množín, z ktorých sa vytvára. V ďalších kapitolách sa potom budeme zaoberať štúdiom podmožín karteziánskeho súčinu, reláciami a zobrazeniami (funkciami).

Definícia 3.3. *Nech sú* A, B *dve ľubovoľné množiny. Karteziánskym súčinom množín* A, B *nazveme množinu usporiadaných dvojíc*

$$A \times B = \{(a, b); a \in A \& b \in B\}.$$

Karteziánsky súčin množín A, B teda pozostáva zo všetkých usporiadaných dvojíc (a, b), kde prvý prvok usporiadanej dvojice je z množiny A a druhý z množiny B. Ak množiny A, B neobsahujú príliš veľký počet prvkov, ich karteziánsky súčin je možné zadať vypísaním všetkých usporiadaných dvojíc. Aby sme pri vypisovaní prvkov karteziánskehu súčinu na žiadny prvok nezabudli, je rozumné zapisovať prvky karteziánskeho súčinu systematicky. Na to sa dá výhodne použiť obdĺžniková tabuľka, ktorej riadky sú označené prvkami prvej množiny A a stĺce prvkami druhej množiny karteziánskeho súčinu, B. Predpokladajme, že $A = \{a_1, \ldots, a_n\}$; $B = \{b_1, \ldots, n_m\}$. Potom sa v políčku tabuľky ležiacom na priesečníku i-teho riadku a j-teho stĺpca nachádza usporiadaná dvojica (a_i, b_j); $1 \leq i \leq n$, $1 \leq i \leq m$. Obdĺžniková tabuľka s n riadkami a m stĺpcami sa nazýva *maticou typu* $n \times m$. Nech je M matica typu $n \times m$. Priesečník i-teho riadku a j-teho stĺpca matice M nazývame miestom (prvkom) matice, budeme ho označovať pomocou usporiadanej dvojice súradníc (i, j). Hodnotou prvku matice nemusí byť len usporiadaná dvojica. Do matice-tabuľky môžeme zapisovať hodnoty z nejakej množiny napr. C. Hodnotu prvku (i, j) matice M budeme označovať symbolom $m_{i,j}$. Maticu, ktorej prvky nadobúdajú hodnoty z množiny C budeme nazývať maticou nad množninou C; resp. ak je C množina celých (reálnych) čísel, tak M nazývame celočíselnou (reálnou) maticou. Vráťme sa k maticovej reprezentácii prvkov karteziánskeho súčinu množín $A = \{a_1, \ldots, a_n\}$; $B = \{b_1, \ldots, n_m\}$. Tabuľka 3.1 predstavuje karteziánsky súčin množín A, B v maticovom tvare[3]

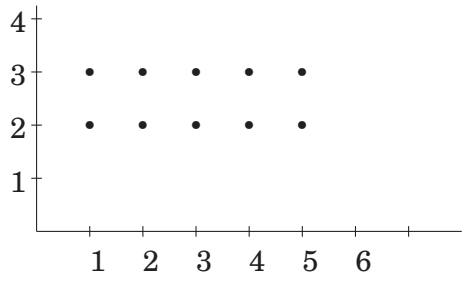
	b_1	b_2	$\ldots$	b_n
a_1	(a_1, b_1)	(a_1, b_2)	$\ldots$	(a_1, b_m)
a_2	(a_2, b_1)	(a_2, b_2)	$\ldots$	$(a_2, b_n m)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	(a_n, b_1)	(a_n, b_2)	$\ldots$	(a_n, b_m)

Tabuľka 3.1: $A \times B$

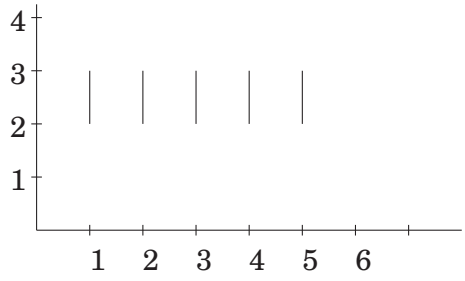
Uvedieme ešte niekoľko príkladov karteziánskych súčinov rôznych množín.

Príklad 3.1. *1. Nech* $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 3\}$. *Na obr. 3.1 je graficky znázornený karteziánsky súčin množín* A, B

[3]Ak to nepovedie k nedorozumeniu, označenia riadkov a stĺpcov matíc budeme v ďalšom texte vynechávať.



Obrázok 3.1: Karteziánsky súčin množín $\{1,2,3,4,5\} \times \{2,3\}$



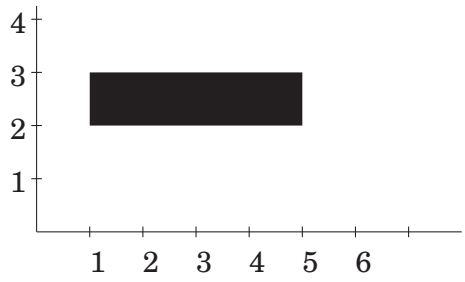
Obrázok 3.2: Karteziánsky súčin množín $\{1,2,3,4,5\} \times \{y \in \mathbf{R}; 2 \le y \le 3\}$

2. *Nech* $A = \{1,2,3,4,5\}$, $B = \{y \in \mathbf{R}; 2 \le y \le 3\}$. *Karteziánsky súčin množín* A, B *obsahuje nekonečný počet prvkov. Jeho graf je uvedený na obrázku 3.2.*

3. *Nech* $A = \{x \in \mathbf{R}; 1 \le x \le 5\}$, $B = \{y \in \mathbf{R}; 2 \le y \le 3\}$. *Karteziánsky súčin množín* A, B *je množina bodov obdĺžnika na obr. 3.3.*

Poznámka. Definíciu karteziánskeho súčinu dvoch množín môžeme zovšeobecniť na prípad karteziánskeho súčinu n množín podobným spôsobom, ako sme zovšeobecnili definíciu usporiadanej dvojice, definícia 3.2. Vystačíme však s jednoduchšou definíciou, ktorá bude vychádzať priamo z pojmu usporiadanej n-tice a využívať základnú vlastnosť usporiadaných n-tíc (veta 3.2).

Definícia 3.4. *Nech sú* $A_1, \ldots, A_n$, $n \ge 2$ *ľubovoľné množiny. Karteziánsky súčin množín*



Obrázok 3.3: Karteziánsky súčin množín $\{x \in \mathbf{R}; 1 \le x \le 5\} \times \{y \in \mathbf{R}; 2 \le y \le 3\}$

$A_1, \ldots, A_n$ *je množina usporiadaných* n*-tíc:*

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) | a_1 \in A_1 \& \ldots \& a_n \in A_n\}.$$

Úloha 3.5. *Zistite, či pre karteziánsky súčin množín platí komutatívny a asociatívny zákon; t.j. či*

- $A \times B = B \times A$,
- $A \times (B \times C) = (A \times B) \times C)$.

Úloha 3.6. *Dokážte alebo vyvráťte nasledujúce tvrdenia:*

1. *Ak* $A \times B \neq \emptyset$ *a* $A \times B = C \times D$*, tak potom* $A = C, B = D$.
2. *Ak* $C \neq \emptyset$ *a* $A \times C = B \times C$*, tak potom* $A = B$.

Východiskové množiny karteziánskeho súčinu môžu byť výsledkom množinových operácií nad inými „jednoduchými“ množinami. V nasledujúcej vete ukážeme súvislosti medzi kartézskymi súčinmi vytvorenými nad zloženými množinami a karteziánskymi súčinmi, v ktorých vystupujú dané „jednoduché“ množiny.

Veta 3.3. *Nech sú* A, B, C *ľubovoľné množiny, potom platia nasledujúce tvrdenia:*

1. *ak* $A \subseteq B$*, tak potom pre ľubovoľnú množinu* C *platí* $A \times C \subseteq B \times C$,
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
3. $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
4. $(A - B) \times C = (A \times C) - (B \times C)$,
5. *množiny* A, B *sú disjunktné práve vtedy, ak* $(A \times B) \cap (B \times A) = \emptyset$.

Dôkaz. Na ukážku dokážeme detailne prvé tvrdenie a jeho dôkaz zapíšeme formálne.

1. $A \subseteq B$ predpoklad,
2. $(x, y) \in (A \times C) \equiv (x \in A) \& (y \in C)$ definícia karteziánskeho súčinu,
3. $(x \in A) \& (y \in C) \Rightarrow (x \in A)$ tautológia $(p \& q) \Rightarrow p$
4. $(x \in A) \& (y \in C) \Rightarrow (y \in C)$ tautológia $(p \& q) \Rightarrow pq$
5. $(A \subseteq B) \equiv (x \in A) \Rightarrow (x \in B)$,
6. $(x \in A) \Rightarrow (x \in B)$ (1,5),
7. $((x \in A) \& (y \in C)) \Rightarrow (x \in B)$ (sylogizmus 3,5)
8. $((x \in A) \& (y \in C)) \Rightarrow (x \in B) \& (y \in C)$ $\frac{(p \& q) \Rightarrow r, (p \& q) \Rightarrow s,}{(p \& q) \Rightarrow (r \& s)}$

9. $(x \in B)\&(y \in C) \Rightarrow (x,y) \in (B \times C)$ definícia karteziánskeho súčinu,
10. $(x,y) \in (A \times C) \Rightarrow (x,y) \in (B \times C)$.

Dokázali sme, že ľubovoľná usporiadaná dvojica, ktorá patrí do karteziánskeho súčinu $A \times C$ patrí aj do $B \times C$. To znamená, že $A \times C \subseteq B \times C$. Dokážeme stručnejšie ešte jedno tvrdenie. Dôkaz ďalších ponecháme čitateľovi ako cvičenie.

$$\begin{aligned}
(x,y) \in (A \times C) - (B \times C) &\equiv \\
&\equiv [(x,y) \in (A \times C)]\&\neg[(x,y) \in (B \times C)] \equiv \\
&\equiv [(x \in A)\&(y \in C)]\&\neg[(x \in B)\&(y \in C)] \equiv \\
&\equiv [(x \in A)\&(y \in C)]\&[\neg(x \in B) \vee \neg(y \in C)] \equiv \\
&\equiv [(x \in A)\&(y \in C)\&\neg(x \in B)] \vee [(x \in A)\&(y \in C)\&\neg(y \in C)] \equiv \\
&\equiv (x,y) \in (A - B) \times C.
\end{aligned}$$

□

Úloha 3.7. *Dokážte alebo vyvráťte ostatné tvrdenia vety 3.3!*

Úloha 3.8. *Dokážte tvrdenie (1) vety 3.3 sporom!*

Úloha 3.9. *Zistite, pre aké množiny* A, B, C *platia / neplatia nasledujúce identity:*

1. $A \cup (B \times C) = (A \cup B) \times (A \cup C)$,
2. $A \cap (B \times C) = (A \cap B) \times (A \cap C)$,
3. $A - (B \times C) = (A - B) \times (A - C)$.

Uveďte príklady množín A, B, C *pre ktoré uvedené tvrdenia platia (neplatia).*

Úloha 3.10. *Aký vzťah platí pre karteziálnske súčiny*

$$(A \triangle B) \times C, \qquad (A \times C) \triangle (B \times C)?$$

Zdôvodnite!

Kapitola 4

Binárne relácie

Usporiadaná dvojica nám umožňuje dávať do vzťahov prvky rozličných množín. To, že sú dva prvky a, b v nejakom vzťahu môžeme vyjadriť pomocou usporiadanej dvojice (a, b). Usporiadaná dvojica však popisuje vzťah individuálnych prvkov. Ako potom definujeme samotný vzťah? Karteziánsky súčin (nejakých) množín A, B vytvára čosi ako univerzálnu množinu pre definovanie všetkých možných vzťahov medzi prvkami množín A, B, pretože obsahuje všetky možné usporiadané dvojice (a, b) kde $a \in A, b \in B$. Vzťah však znamená akúsi redukciu, nejaký výber z množiny všetkých možností. Uvažujme napríklad množinu prirodzených čísel menších ako 5; $N_5 = \{0, 1, 2, 3, 4\}$ a budeme skúmať vzťah medzi prvkami množiny N_5 definovaný nasledovne $x < y$. Karteziánsky súčin $N_5 \times N_5$ obsahuje 25 usporiadaných dvojíc, ale vzťahu $x < y$ z nich vyhovuje len 10: $(0,1), (0,2), (0,3), (0,4), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)$. Zmysluplný vzťah medzi prvkami množín A, B môžeme zostrojiť tak, že z kartézskeho súčinu $A \times B$ vyberieme nejakú podmnožinu usporiadaných dvojíc, ktorých prvky budú vyhovovať danému vzťahu.

V tejto kapitole upresníme intuitívnu predstavu vzťahu pomocou binárnej relácie, dokážeme základné vlastnosti binárnych relácií a ukážeme, ako sa dajú vytvárať binárne relácie z iných binárnych relácií.

4.1 Základné pojmy

Definícia 4.1. *Nech sú* A, B *ľubovoľné množiny.* Binárnou reláciou R *z množiny* A *do množiny* B *nazveme ľubovoľnú podmnožinu karteziánskeho súčinu* $A \times B$. *Skutočnosť* $(a, b) \in R$ *budeme zapisovať výrazom* aRb. *Množina* A *sa nazýva* oborom *a množina* B kooborom binárnej relácie R.

Prívlastok „binárna“ v definícii relácie znamená, že relácia je definovaná medzi dvoma množinami. Pojem binárnej relácie môžeme prirodzeným spôsobom zovšeobecniť:

Definícia 4.2. *Nech sú* $A_1, \ldots, A_n$ *ľubovoľné množiny, potom ľubovoľnú podmnožinu usporiadaných* n*-tíc karteziánskeho súčinu* $A_1 \times, \ldots, \times A_n$ *nazveme* n*-árnou reláciou na množinách* $A_1, \ldots, A_n$.

V tejto kapitole sa budeme zaoberať takmer výlučne binárnymi reláciami a ak nebude povedané iné, pojem relácia bude označovať binárnu reláciu. Binárne relácie môžeme zadávať viacerými spôsobmi. Nech je oborom binárnej relácie R n-prvková množina $A = \{a_1, \ldots, a_n\}$ a kooborom binárnej relácie R m-prvková množina B. Potom binárnu reláciu R môžeme jednoznačne zapísať pomocou matice $M_R = (m_{i,j})$ typu $n \times m$; takej, že pre $1 \leq i \leq n,\ 1 \leq j \leq m$

$$m_{i,j} = \begin{cases} 1 & (a_i, b_j) \in R, \\ 0 & (a_i, b_j) \notin R. \end{cases}$$

Poznámka. Maticu, ktorej prvky nadobúdajú hodnoty z množiny $\{0, 1\}$ budeme nazývať *binárnou*[1] alebo *Booleovskou maticou.*[2] Binárna matica M_R predstavuje v podstate kompaktnejšie zapísaný charakteristický vektor podmnožiny karteziánskeho súčinu $A \times B$. Pomocou maticovej reprezentácie binárnej relácie dokážeme odvodiť aj celkový počet binárnych relácií z množiny A do množiny B; tých je práve toľko, koľko je binárnych vektorov dĺžky $n \cdot m$; t.j. 2^{nm}.

Príklad 4.1. *Keď sme zavádzali maticovú reprezentáciu binárnej relácie, predpokladali sme, že obor a koobor binárnej relácie obsahujú indexované prvky* a_i, *resp.* b_j. *Binárne relácie možno reprezentovať pomocou matíc aj v prípade, keď ich obor a koobor neobsahujú indexované prvky. Nech* $A = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, $B = \{\alpha, \beta, \gamma, \delta\}$ *a* $R = \{(\clubsuit, \alpha), (\clubsuit\beta), (\clubsuit, \delta), (\diamondsuit, \beta), (\diamondsuit, \gamma), (\heartsuit, \alpha), (\spadesuit, \beta), (\spadesuit, \gamma)\}$. *Potom binárnu reláciu* R *popíšeme pomocou nasledujúcej tabuľky Ak sa dohodneme na nejakom usporiadaní*[3] *prvkov v množinách* A, B, *napr.*

	α	β	γ	δ
$\clubsuit$	1	1	0	1
$\diamondsuit$	0	0	1	1
$\heartsuit$	1	0	0	0
$\spadesuit$	0	0	1	1

Tabuľka 4.1: Tabuľka binárnej relácie R

$\clubsuit \prec \diamondsuit \prec \heartsuit \prec \spadesuit$ *a* $\alpha \prec \beta \prec \gamma \prec \delta$ *a na tom, že riadky a stĺpce tabuľky budú usporiadané v súlade s poradím prvkov v prvom riadku a prvom stĺpci, môžeme prvý riadok a prvý stĺpec tabuľky vynechať a binárnu reláciu* R *reprezentovať pomocou nasledujúcej binárnej matice* M_R*:*

$$M_R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Ďalšou reprezentáciou binárnej relácie, ktorú využijeme najmä pri skúmaní vlastností binárnych relácií a skladaní binárnych relácií, je jej grafová reprezentácia. Skôr,

[1] pretože jej prvky sú z binárnej množiny

[2] prvky matice nadobúdajú logické hodnoty.

[3] usporiadaniami množín sa budeme ešte špeciálne zaoberať v kapitole 6

ako ukážeme, ako možno danú reláciu reprezentovať pomocou grafu, zavedieme veľmi stručne nevyhnutné pojmy z teórie grafov.

Graf je objekt, ktorý pozostáva z množiny *vrcholov* a množiny *hrán*. Hrany sú určené dvojicami vrcholov. Hrany môžu byť orientované, vtedy ich reprezentujeme usporiadanými dvojicami vrcholov a neusporiadané, vtedy je hrana určená neusporiadanou dvojicou. (Vynecháme zatiaľ špeciálne prípady, kedy v grafe existuje viacero rovnakých hrán, resp., keď je hrana určená dvojicou rovnakých vrcholov.) Súvislosť hrany a vrcholov, ktoré ju určujú budeme vyjadrovať tak, že hrana (a, b) je *incidentná* s vrcholmi a, b. Graf možno zadať určením jeho množín vrcholov a hrán, a pracovať s ním ako s nejakou zvláštnou množinou. Graf sa však dá veľmi názorne reprezentovať graficky (nakresliť), a to tak, že jeho vrcholom priradíme body a hranám grafu úsečky s koncovými bodmi v príslušných vrcholoch. Orientované hrany budeme znázorňovať pomocou šípok; orientovanej hrane (a, b) priradíme šípku vychádzajúcu z bodu reprezentujúcemu vrchol a, ktorá vchádza do bodu reprezentujúceho vrchol b. Graf, ktorého hrany zadávajú neusporiadané dvojice vrcholov, sa nazýva *neorientovaný graf*, v opačnom prípade hovoríme o *orientovanom grafe*. (Orientovaný) graf G sa teda formálne dá zapísať ako usporiadaná dvojica $G = (V, U)$, kde V je množina vrcholov a $U \subseteq V \times V$ je množina (orientovaných) hrán. V mnohých aplikáciách potrebujeme zistiť, či existuje nejaká súvislosť medzi dvoma objektami, ktoré nie sú v bezprostrednom vzťahu (napríklad, či existuje dopravné spojenie medzi mestami A a B, ktoré nie sú spojené priamou linkou hromadnej dopravy). Takéto vlastnosti sa v grafovom modeli dajú popisovať pomocou pojmov ako je sled, ťah, cesta, súvislosť, ktoré teraz stručne zavedieme. Nech je $G = (V, U)$ neorientovaný graf, potom postupnosť

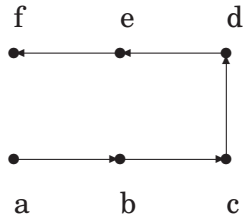
$$v_0, u_1, v_1, u_2, v_2, \ldots, v_{n-1}, u_n, v_n, \tag{4.1}$$

kde $v_i \in V$ $i = 0, \ldots, n$, $u_i \in U$ $i = 1, \ldots, n$ sú vrcholy, resp. hrany grafu G také, že hrana u_i je incidentná s vrcholmi v_{i-1}, v_i sa nazýva *sled*. Sled sa nazýva uzavretý, ak $v_0 = v_n$, v opačnom prípade je otvorený. Ak sa v postupnosti (4.1) neopakujú hrany, takýto sled nazývame *ťahom*[4]. Ak sa naviac v postupnosti (4.1) neopakuje žiaden vrchol (s výnimkou prvého a posledného), takýto sled nazývame *cestou*. Uzavretá cesta sa nazýva *cyklus*. Graf sa nazýva *súvislý*, ak medzi jeho ľubovoľnými dvoma vrcholmi existuje cesta, v opačnom prípade graf nie je súvislý. Podobne by sme definovali sled, ťah a cestu v orientovanom grafe; tam by sme však v postupnosti (4.1) museli vyžadovať aj dodržanie orientácie hrán; v grafe na obrázku 4.1 existuje cesta z vrcholu a do vrcholu f, ale už tam nie je cesta napr. z vrcholu e do vrcholu a.

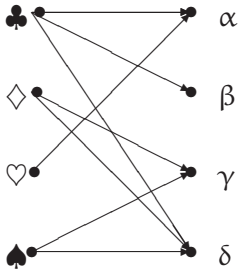
Príklad 4.2. *Uvažujme orientovaný graf* $G = (V, U)$*, kde* $V = \{a, b, c, d, e, f\}$*,* $V\{(a, b), (b, c), (c, d), (d, a), (e, f)\}$*. Graficky je graf* $G = (V, U)$ *znázornený na obr. 4.1*

Orientovanému grafu môžeme teda jednoznačne priradiť binárnu reláciu určenú množinou hrán $U \subseteq V \times V$. Dá sa to však spraviť aj opačne—binárnej relácii $R \subseteq A \times B$ môžeme priradiť orientovaný graf $G_R = (V_R, U_R)$, kde $V_R = A \cup B$ a $U = R$. Aby bol obrázok grafu prehľadný, rozdelíme množinu vrcholov grafu na dve disjunktné podmnožiny– prvá množina obsahuje vrcholy prislúchajúce prvkom oboru binárnej relácie; t.j. prvkom

[4]spomeňte si na úlohu nakresliť obrázok jedným ťahom, t.j. tak, že čiara musí byť súvislá, môže sa pretínať, ale po tej istej čiare nesmiete ísť viackrát



Obrázok 4.1: Graf $G = (V, U)$.



Obrázok 4.2: Graf binárnej relácie R

množiny A a druhá množina vrcholov obsahuje vrcholy prislúchajúce prvkom kooboru; t.j. množine B. Potom zakreslíme hrany zodpovedajúce jednotlivým usporiadaným dvojiciam binárnej relácie R. Orientovaný graf relácie R z príkladu 4.1 je uvedený na obr. 4.2

Úloha 4.1. *((Šachová) 4-árna relácia.) Nech* $A = \{a, b, c, d, e, f, g, h\}$, $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $C = \{$*biely, čierny* $\}$, $D = \{$*p,J,S,V,D,K, nič*$\}$

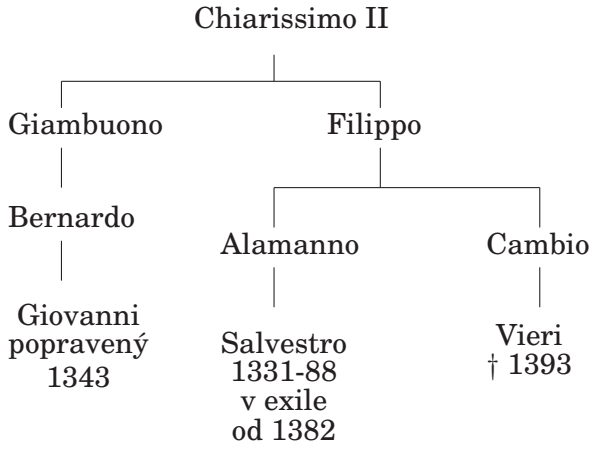
1. *Čo vyjadruje karteziánsky súčin* $A \times B \times C \times D$
2. *Zapíšte pomocou ternárnej (*$n = 4$*) relácie túto šachovú pozíciu:*
   biely: Kb1, Vd1, Jb4, pa3,pb2,pc2,pd4,
   čierny: Kh8, Vf8, Se7, ph7, pg6, pg5.
3. *Akú šachovú pozíciu predstavuje relácia* $\emptyset$*?*

4.2 Skladanie binárnych relácií

Na obrázku 4.3 je časť rodokmeňa rodiny Medici podľa [1]. Rodokmeň definuje reláciu $\Phi = \{(x, y) | x$ je synom $y\}$, pričom oborom a kooborom tejto relácie je množina obsahujúca Chiarissima II a jeho mužských potomkov [5]. Relácia Φ má 8 prvkov:

[5] dcéry sa v rodokmeni neuvádzali

{ (Chiarissimo II, Giambuono), (Chiarissimo II, Filippo), (Giambuono,Bernardo), (Filippo,Alamanno), (Filippo,Cambio), (Bernardo,Giovanni), (Alamanno,Salvestro), (Cambio, Vieri)}. Z relácie Φ môžeme vytvoriť niekoľko nových relácií. Napríklad, Bernardo bol synom Giambuona, Giambuono bol synom Chiarissima II, a to znamená, že Bernardo bol vnukom Chiarissima II. Spojením, alebo dvojnásobným použitím relácie Φ (x je synom y) sa dostávame k binárnej relácii x je vnukom z. Uvedený príklad je špeciálnym prípadom[6] operácie skladania binárnych relácií, ktorú formálne zavedieme v nasledujúcej definícii.



Obrázok 4.3: Rodokmeň rodiny Medici, slepá vetva Chiarissima II

Definícia 4.3. *Nech je* R *binárna relácia z množiny* A *do množiny* B*,* S *binárna relácia z množiny* B *do množiny* C*. Potom existuje binátna relácia* T *z množiny* A *do množiny* C*, ktorá sa nazýva kompozíciou relácií* R, S*, taká, že*

$$T = RS = \{(a, c) \mid \exists b(b \in B) \& (a, b) \in R \& (b, c) \in S.$$

Z definície 4.3 vyplýva, že kompozícia dvoch binárnych relácií nemusí vždy existovať. Postačujúcou podmienkou pre existenciu kompozície RS binárnych relácií R, S je, aby sa obor relácie S rovnal kooboru relácie R.

Poznámka Kompozícia RS sa nazýva zloženou reláciou (binárnych relácií R, S a niekedy sa označuje aj symbolom $R \circ S$. Všimnite si, že zápisy zloženej relácie RS a $R \circ S$ sa líšia poradím, v akom sú jednotlivé relácie R, S uvedené. Zakrátko si ukážeme, čo to vyjadruje.

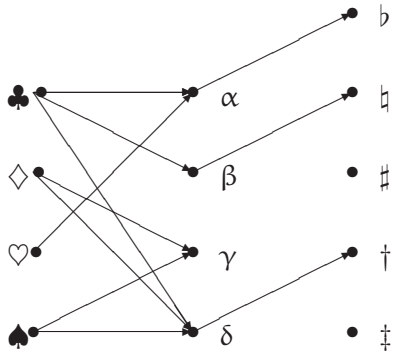
Teraz sa pozrieme, ako z relácií R, S dostaneme zloženú reláciu RS. Využijeme reláciu R z príkladu 4.1, reláciu S definujeme nasledovne: $S \subseteq \{\alpha, \beta, \gamma, \delta\} \times \{\flat, \natural, \sharp\dagger, \ddagger\}$;

Relácie R, S spĺňajú podmienky pre skladanie binárnych relácií, a preto bude existovať zložená relácia RS, ktorá je podmnožinou karteziánskeho súčinu $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\} \times$

[6] skladáme binárnu reláciu s ňou samotnou

	♭	♮	♯	†	‡
α	1	0	0	0	0
β	0	1	0	0	0
γ	0	0	0	0	0
δ	0	0	0	1	0

Tabuľka 4.2: Tabuľka binárnej relácie S



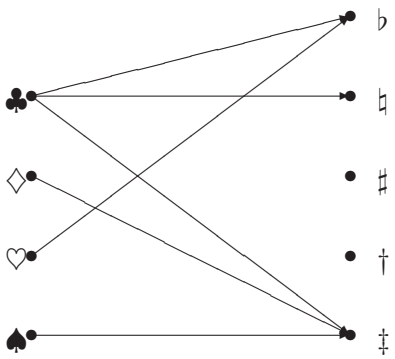
Obrázok 4.4: Zložená relácia RS

$\{\flat, \natural, \sharp\dagger, \ddagger\}$ Na obr. 4.5 sú nakreslené grafy oboch relácií R, S. Graf zloženej relácie RS zostrojíme tak, že vrchol priradený prvku z množiny $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ spojíme hranou s vrcholom-prvkom množiny $\{\flat, \natural, \sharp\dagger, \ddagger\}$, ak medzi týmito dvoma vrcholmi existuje aspoň jedna cesta. Naviac, prechádzať z vrcholu do vrcholu možno len v tom smere, ako je orientovaná hrana spájajúca tieto dva vrcholy. Tak dvojica $(\clubsuit, \flat)$ bude prvkom zloženej relácie RS, pretože, neformálne povedané, z vrcholu $\clubsuit$ vedie cesta do vrcholu α a z vrcholu α zasa vedie cesta do vrcholu $\flat$. Na druhej strane, v grafe neexistuje žiadna cesta spájajúca niektorý vrchol $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ s vrcholmi $\sharp, \ddagger$. To znamená, že sa v zloženej relácii nebudú vyskytovať usporiadané dvojice, ktorých druhým prvkom by bol jeden zo symbolov $\sharp, \ddagger$. Zložená relácia RS je popísaná v tabuľke 4.3, jej graf je uvedený na obr. 4.5.

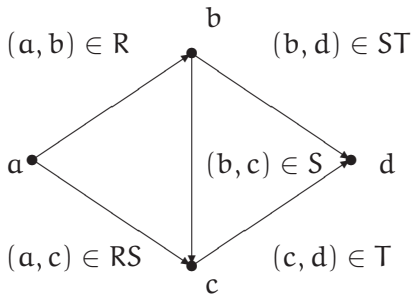
	♭	♮	♯	†	‡
♣	1	1	0	0	1
♢	0	0	0	0	1
♡	1	0	0	0	0
♠	0	0	0	0	1

Tabuľka 4.3: Tabuľka zloženej binárnej relácie RS

Hoci sme skladanie binárnych operácií definovali len pre dve binárne relácie, zložiť môžeme postupne aj viacero binárnych relácií. Nech sú A, B, C, D ľubovoľné množiny a tri binárne relácie $R \subseteq A \times B$, $S \subseteq B \times C$, $T \subseteq C \times D$. Potom môžeme zložiť relácie R a S a dostaneme zloženú binárnu reláciu $RS \subseteq A \times C$, ktorá sa dá zložiť s binárnou reláciou T. Rovnako dobre však môžeme najprv vytvoriť zloženú reláciu ST s tú zložiť s binárnou reláciou R. Pri väčšom počte relácií bude počet možností vytvárania zložených



Obrázok 4.5: Graf relácie RS



Obrázok 4.6: Skladanie relácií RST

relácií ešte väčší. Bude zložená relácia závisieť od spôsobu skladania, alebo, matematicky povedané, bude skladanie binárnych relácií asociatívne? Na túto dôležitú otázku dáva odpoveď nasledujúca veta.

Veta 4.1. *Nech sú dané* A, B, C, D *ľubovoľné množiny a binárne relácie* $R \subseteq A \times B$*,* $S \subseteq B \times C$*,* $T \subseteq C \times D$*. Potom*

$$R(ST) = (RS)T.$$

Dôkaz. Nech $(a, d) \in R(ST)$. To znamená, že existuje prvok $b \in B$ taký, že $(b, d) \in ST$. Ale ak $(b, d) \in ST$, potom musí existovať taký prvok $c \in C$, že $(b, c) \in S$ a $(c, d) \in T$. Ale ak existujú uporiadané dvojice $(a, b) \in R$ a $(b, c) \in S$, potom $(a, c) \in RS$. Teraz už stačí využiť existenciu $(c, d) \in T$ a dostávame, že $(a, d) \in (RS)T$. Pozri obr. 4.6. Opačná inklúzia sa dokazuje analogicky. □

Pozrime sa teraz skladanie binárnych relácií v maticovej reprezentácii. Nech sú ma-

tice M_R a M_S matice binárnej relácie $R \subseteq A \times B$, resp. $S \subseteq B \times C$; M_R je matica typu $n \times m$ a M_S je matica typu $m \times p$. Pripomenieme, že každý riadok matice M_R zodpovedá jednému prvku z množiny A a každý stĺpec matice M_R zodpovedá jednému prvku množiny B; analogicky pre maticu M_S. Ak usporiadaná dvojica $(a_i, b_j) \in R$, tak prvok ležiaci na priesečníku i-teho riadku a j-teho stĺpca matice nadobudne hodnotu 1, v opačnom prípade je jeho hodnota 0. Podobne pre reláciu S a maticu M_S. Kedy bude usporiadaná dvojica (a_i, c_k) patriť do relácie RS? Podľa definície kompozície relácií práve vtedy, ak existuje taký prvok $b_j \in B$, že $(a_i, b_j) \in R$ a $(b_j, c_k) \in S$; t.j. ak je súčasne jednotka na j-tom mieste v i-tom riadku matice M_R a na k-tom mieste v j-tom riadku matice M_S. Takýto postup nevyzerá na prvý pohľad ako efektívna metóda na výpočet kompozície binárnych relácií. Našťastie existuje efektívnejšie riešenie, ak sú binárne relácie zadané pomocou svojich matíc M_R a M_S, tak maticu kompozície relácií R, S vypočítame ako súčin matíc M_R a M_S. Definujeme najprv *súčin binárnych matíc* a potom sformulujeme naznačené tvrdenie.

Definícia 4.4. *(Násobenie Booleovských matíc.) Nech sú* $M_A = (\alpha_{i,j}$, $M_B = (\beta_{j,k}$, *binárne matice typu* $n \times m$, *resp.* $m \times p$. *Potom súčinom matíc* M_A, M_B *je binárna matica* $M_C = (\gamma_{i,k})$ *typu* $n \times p$, *ktorej hodnoty sú definované nasledovne:*

$$\gamma_{i,k} = \bigvee_{j=1}^{m} (\alpha_{i,j} \& \beta_{j,k})$$

pre $1 \leq i \leq n$, $1 \leq j \leq p$.

Ako máme rozumieť výrazu $\bigvee_{j=1}^{m} (\alpha_{i,j} \& \beta_{j,k})$ v definícii? Zoberieme i-ty riadok matice M_A a zapíšeme ho v podobe vektora $\alpha_{i,1}, \ldots, \alpha_{i,m}$, podobne zapíšeme v tvare vektora k-ty stĺpec matice M_B: $\beta_{1,k}, \ldots, \beta_{m,k}$. Potom vytvoríme konjunkcie zodpovedajúcich prvkov oboch vektorov a tieto konjunkcie spojíme disjunkciami a vypočítame hodnotu $\gamma_{i,k}$:

$$(\alpha_{i,1} \& \beta_{1,k}) \vee (\alpha_{i,2} \& \beta_{2,k}) \vee \cdots \vee (\alpha_{i,2m} \& \beta_{m,k}) = \gamma_{i,k}$$

Veta 4.2. *Nech sú matice* M_R *a* M_S *matice binárnej relácie* $R \subseteq A \times B$, *resp.* $S \subseteq B \times C$. *Potom pre maticu zloženej binárnej relácie* RS, M_{RS} *platí:*

$$M_{RS} = M_R \cdot M_S.$$

Dôkaz. Vyplýva priamo z definícií násobenia Booleovských matíc a zloženej relácie. □

Precvičte si získané poznatky o reláciách riešením nasledujúcich úloh.

Úloha 4.2. *Zvoľte si vhodné množiny* $A, B, C, D, \ldots$ *(4-5 prvkové) a definujte na nich aspoň 5 rozličných binárnych relácií. Zapíšte tieto relácie pomocou matíc aj grafov.*

Úloha 4.3. *Vytvorte aspoň 5 rozličných zložených relácií z relácií z predchádzajúceho príkladu. Použite grafovú aj maticovú reprezentáciu.*

Úloha 4.4. *Overte na konkrétnych príkladoch asociatívnosť skladania binárnych relácií.*

Úloha 4.5. *Vypočítajte aspoň 10 príkladov na násobenie Booleovských matíc.*

Úloha 4.6. *Je skladaníe relácií komutatívne? Za akých podmienok?*

Úloha 4.7. *Je násobenie Booleovských matíc asociatívne?*

Úloha 4.8. *Skúste definovať skladanie ternárnych ($n = 3$) relácií, nájdite jeho vhodnú reprezentáciu a preskúmajte vlastnosti skladania ternárnych relácií.*

Relácie sa často vyskytujú v databázach. Uvažujme nasledujúcu situáciu. Letecká spoločnosť zaisťuje dopravu na niekoľkých linkách, má k dispozícii lietadlá niekoľkých typov a pilotov, ktorí majú oprávnenia na niektoré typy lietadiel. Tieto informácie má zachytené v dvoch reláciách, uvedených v nasledujúcej tabuľke

číslo letu	typ lietadla	pilot	typ lietadla
83	727	Skinner	707
83	747	Skinner	727
84	727	Bart	727
84	747	Homer	727
109	707	Homer	747

Spoločnosť potrebuje vedieť, ktorých pilotov môže nasadiť na jednotlivé linky. Aby to zistila, potrebuje z binárnej relácie (pilot,typ lietadla) vytvoriť binárnu reláciu (typ lietadla, pilot). Takáto binárna relácia sa nazýva *opačnou reláciou*.

Definícia 4.5. *Nech je daná binárna relácia $R \subseteq A \times B$. Opačnou alebo inverznou reláciou k relácii R budeme nazývať binárnu reláciu R^{-}:*

$$R^{-} = \{(y, x) | (x, y) \in R\}$$

V našom prípade bude relácia (typ lietadla, pilot) vyzerať takto:

typ lietadla	pilot
707	Skinner
727	Skinner
727	Bart
727	Homer
747	Homer

Požadovanú informáciu (let, pilot) dostaneme zložením relácií (let, typ lietadla), (typ lietadla, pilot). V nasledujúcej tabuľke je okrem toho uvedený aj typ lietadla, ktorý sa na daný let dá použiť, pretože sú piloti, ktorí na tej istej linke môžu lietať s viacerými typmi lietadiel.

let	pilot	typ lietadla	let	pilot	typ lietadla
83	Skinner	(727)	84	Homer	(727)
83	Homer	(727)	84	Bart	(747)
83	Bart	(747)	84	Homer	(747)
83	Homer	(747)	109	Skinner	(707)
84	Skinner	(727)			

4.3 Množinové operácie nad binárnymi reláciami

Spomenuli sme už, že sa v databázach používajú údajové štruktúry, ktoré predstavujú relácie. Mnohé operácie nad údajmi v databázach sú v podstate množinové operácie. Ak abstrahujeme od toho, že prvkami relácií sú úsporiadané n-tice, množinové operácie s reláciami sa nijako nelíšia od množinových operácií nad „obyčajnými“ množinami. Nový aspekt však prináša operácia skladania binárnych relácií. Pozrieme sa preto bližšie na vzťahy medzi množinovými operáciami uplatňovanými nad binárnymi reláciami a novozavedenou operáciou skladania binárnych relácií.

Veta 4.3. *Nech sú* R, R_1, R_2 *binárne relácie z* A *do* B *a* S, S_1, S_2 *binárne relácie z* B *do* C. *Potom platia nasledujúce vzťahy*

1. $R(S_1 \cup S_2) = RS_1 \cup RS_2$
2. $(R_1 \cup R_2)S = R_1S \cup R_2S$
3. *ak* $S_1 \subseteq S_2$ *tak potom* $RS_1 \subseteq RS_2$,
4. *ak* $R_1 \subseteq R_2$ *tak potom* $R_1 \subseteq R_2S$,
5. $R(S_1 \cap R_2) \subseteq RS_1 \cap RS_2$
6. $(R_1 \cap R_2)S \subseteq R_1S \cap R_2S$
7. $R(S_1 - R_2) \supseteq RS_1 - RS_2$
8. $(R_1 - R_2)S \supseteq R_1S - R_2S$

Dôkaz.

1.

$$\begin{aligned}(a,c) \in R(S_1 \cup S_2) &\equiv \exists b[(b \in B)\&(a,b) \in R\&(b,c) \in (S_1 \cup S_2)] \equiv \\ &\equiv \exists b[(b \in B)\&(a,b) \in R\&[((b,c) \in S_1) \vee ((b,c) \in S_2)]] \equiv \\ &\equiv \exists b[[(b \in B)\&((a,b) \in R)\&((b,c) \in S_1)][(b \in B)\&((a,b) \in R)\&((b,c) \in S_2))]] \equiv \\ &\equiv [((a,c) \in RS_1) \vee ((a,c) \in RS_2)] \equiv (a,c) \in (RS_1 \cup RS_2)\end{aligned}$$

2. Identita $(R_1 \cup R_2)S = R_1S \cup R_2S$ sa dokazuje analogicky ako identita (1).
3. Využijeme tvrdenia vety 2.5. Keďže $S_1 \subseteq S_2$, potom $S_1 \cup S_2 = S_2$ Podľa identity (1) tejto vety $R(S_1 \cup S_2) = RS_1 \cup RS_2$. To znamená, že $R(S_1 \cup S_2) = RS_2$. Ale rovnosť $RS_1 \cup RS_2 = RS_2$ je podľa vety 2.5 ekvivalentná s tým, že $RS_1 \subseteq RS_2$.
4. Tvrdenie (4) sa dokazuje analogicky ako tvrdenie (3).
5. Opäť využijeme vetu 2.5. Keďže $S_1 \cap S_2 \subseteq S_1$ a $S_1 \cap S_2 \subseteq S_2$ podľa tvrdenia (2) tejto vety platia inklúzie $R(S_1 \cap S_2) \subseteq RS_1$ a $R(S_1 \cap S_2) \subseteq RS_2$. Z posledných dvoch inklúzií podľa vety 2.6 dostávame požadovanú inklúziu $R(S_1 \cap R_2) \subseteq RS_1 \cap RS_2$.

6. Tvrdenie $(R_1 \cap R_2)S \subseteq R_1S \cap R_2S$ sa dokazuje analogicky ako tvrdenie (5).

7. Dôkaz inklúzie $R(S_1 - R_2) \supseteq RS_1 - RS_2$ bude trocha zložitejší, pretože budeme musieť pracovať s negáciou existenčného kvantifikátora.

$$(a,c) \in RS_1 - RS_2 \quad \equiv \quad (a,c) \in RS_1 \& \neg[(a,c) \in RS_1] \tag{4.2}$$

Rozpíšeme obe tvrdenia z poslednej konjunkcie:

$$(a,c) \in RS_1 \equiv \exists y[(y \in B) \& (a,y) \in R \& (y,c) \in S_1].$$

Predpokladáme, že prvok spĺňajúci podmienky poslednej konjunkcie existuje a označíme ho symbolom b. To znamená, že platí

$$[(b \in B) \& (a,b) \in R \& (b,c) \in S_1].$$

Podobne upravíme druhý výrok z konjunkcie (4.2)

$$\begin{gathered}\neg[(a,c) \in RS_2] \equiv \neg\exists x[(x \in B) \& (a,x) \in R \& (x,c) \in S_2] \equiv \\ \equiv \forall x[(\neg(x \in B)) \vee (\neg(a,x) \in R) \vee (\neg(x,c) \in S_2)].\end{gathered}$$

Toto tvrdenie platí pre ľubovoľnú hodnotu $x \in B$, a preto musí platiť aj pre $x = b$; t.j.

$$[\neg(b \in B) \vee (\neg(a,b) \in R) \vee (\neg(b,c) \in S_2)].$$

Pri dôkaze sme doteraz použili tautológie $(p \& q) \Rightarrow p, (p \& q) \Rightarrow q$. Teraz využijeme tautológiu $(p \Rightarrow q) \Rightarrow ((p \Rightarrow r) \Rightarrow (p \Rightarrow (q \& r))$ a zapíšeme celý dôkaz formálne

$$\begin{aligned}
& (a,c) \in (RS_1 - RS_2) \Rightarrow \\
\Rightarrow\ & [(b \in B) \& (a,b) \in R \& (b,c) \in S_1] \& [\neg(b \in B) \vee \neg(a,b) \in R \vee \neg(b,c) \in S_2] \equiv \\
\equiv\ & [(b \in B) \& (a,b) \in R \& (b,c) \in S_1 \& \neg(b \in B] \vee \\
\vee\ & [(b \in B) \& (a,b) \in R \& (b,c) \in S_1 \& \neg(a,b) \in R] \vee \\
\vee\ & [(b \in B) \& (a,b) \in R \& (b,c) \in S_1 \& \neg(b,c) \in S_2] \equiv \\
\equiv\ & [(b \in B) \& (a,b) \in R \& (b,c) \in (S_1 - S_2)] \equiv (a,c) \in R(S_1 - S_2)
\end{aligned}$$

To však znamená, že

$$RS_1 - RS_2 \subseteq R(S_1 - RS_2).$$

8. Posledné tvrdenie sa dokazuje analogicky ako vzťah (7).

□

Úloha 4.9. *Dokážte tvrdenia (3),(5) takým spôsobom, ako sme dokázali tvrdenie (7) vety 4.3.*

Úloha 4.10. *Zostrojte binárne relácie* R, R_1, R_2, S, S_1, S_2 *a overte na nich platnosť vety 4.3.*

Úloha 4.11. *Dokážte, že inklúzie v tvrdeniach vety 4.3 nemožno nahradiť rovnosťami. (Návod: nájdite také relácie, pre ktoré rovnosti neplatia vo vzťahoch (5), (6), (7) a (8) neplatia).*

Úloha 4.12. *Dokážte, tie tvrdenia vety 4.3, ktoré sme explicitne nedokázali.*

V príklade o leteckej spoločnosti sme zaviedli opačnú (inverznú) reláciu k danej binárnej relácii. Keďže R^- obsahuje usporiadané dvojice ktoré vznikli z usporiadaných dvojíc binárnej relácie R zmenou poradia prvkov, dá sa očakávať, že vlastnosti R^- sa nebudú nejako mimoriadne líšiť od vlastností binárnej relácie R. Rekapituláciu vlastností inverznej relácie R^- poskytuje nasledujúca veta.

Veta 4.4. *Nech sú* R, R_1, R_2 *binárne relácie z* A *do* B *a* S *je binárna relácia z* B *do* C. *Potom platia nasledujúce vzťahy*

1. $(R^-)^- = R$.
2. *Ak* $R_1 \subseteq R_2$ *tak potom* $R_1^- \subseteq R_2^-$.
3. $(R_1 \cap R_2)^- = R_1^- \cap R_2^-$.
4. $(R_1 \cup R_2)^- = R_1^- \cup R_2^-$.
5. $(R_1 - R_2)^- = R_1^- - R_2^-$.
6. $(R^c)^- = R^-)^c$.
7. $(RS)^- = S^-R^-$.

Dôkaz. Dôkazy jednotlivých tvrdení sú jednoduché a väčšinou priamo vyplývajú z definície inverznej relácie.

1. $(a,b) \in (R^-)^- \equiv (b,a) \in R^- \equiv (a,b) \in R$.
2. Nech $R_1 \subseteq R_2$ a $(b,a) \in R_1^- \equiv (a,b) \in R_1 \Rightarrow (a,b) \in R_2 \equiv (b,a) \in R_2^-$.
3. $$\begin{aligned}(b,a) &\in (R_1 \cap R_2)^- \equiv (a,b) \in (R_1 \cap R_2) \equiv [(a,b) \in R_1 \& (a,b) \in R_2] \equiv \\ &\equiv [(b,a) \in R_1^- \& (b,a) \in R_2^-] \equiv (b,a) \in [R_1^- \cap R_2^-].\end{aligned}$$
4. Dôkaz je analogický ako dôkaz identity (3).
5. Dôkaz je analogický ako dôkaz identity (3).
6. $(b,a) \in (R^c)^- \equiv (a,b) \in R^c \equiv \neg(a,b) \in R \equiv \neg(b,a) \in R^- \equiv (b,a) \in (R^-)^c$.
7. $$\begin{aligned}(c,a) &\in (RS)^- \equiv (a,c) \in (RS) \equiv \exists x[(x \in B) \& (a,x) \in R \& (x,c) \in S] \equiv \\ &\equiv \exists x[(x \in B) \& (x,a) \in R^- \& (c,x) \in S^-] \equiv (c,a) \in S^-R^-.\end{aligned}$$

□

Úloha 4.13. *Nájdite vhodnú binárnu reláciu* R*, zostrojte k nej opačnú binárnu reláciu* R^- *a reprezentujte obe relácie* R, R^- *pomocou grafov a matíc. Čím sa odlišujú grafy (matice) relácií* R *a* R^-*? Ako možno na základe grafu (matice) binárnej relácie zostrojiť graf (maticu) k nej opačnej binárnej relácie?*

Ak ste správne vyriešili predchádzajúcu úlohu, zistili ste, že riadky matice M_{R^-} binárnej relácie R^- sú stĺpcami matice M_R a naopak. Matica M_{R^-} sa nazýva *transponovanou maticou* k matici M_R. Zavedieme pojem transponovanej matice formálne.

Definícia 4.6. *Nech je* $A = (a_{i,j})$ *matica typu* $n \times m$*, potom matica* $A^T = (a^{(T)}_{i,j})$*, typu* $m \times n$*, taká, že*

$$a^{(T)}_{i,j} = a_{j,i}$$

pre $1 \leq i \leq n, 1 \leq j \leq m$ *sa nazýva maticou transponovanou k matici* A.

Teraz vyslovíme a dokážeme tvrdenie o vzťahu medzi maticami relácie a opačnej relácie.

Veta 4.5. *Nech je* $R \subseteq A \times B$ *binárna relácia a* R^- *je opačná relácia k relácii* R*. Potom*

$$M_{R^-} = (M_R)^T.$$

Dôkaz. Bez ujmy na všeobecnosti môžeme predpokladať, že $A = \{a_1, \ldots a_n\}$, $B = \{b_1, \ldots, b_m\}$, potom $M_R = (m_{i,j})$ je matica typu $n \times m$. Nech je $(a_i, b_j) \in R$, ľubovoľná usporiadaná dvojica relácie R, potom $(b_j, a_i) \in R^-$. To však znamená, že $m_{i,j} = 1$ a $m_{j,i} = m^{(T)}_{i,j} = 1$. □

Úloha 4.14. *Zadajte 5 rozličných binárnych relácií pomocou matíc a vytvorte matice pre opačné relácie.*

Úloha 4.15. *Uveďte aspoň 5 príkladov binárnych relácií a k nim inverzných relácií z bežného života!*

Úloha 4.16. *Nech sú* A, B, C *ľubovoľné (konečné) množiny;* $R \subseteq A \times B, S \subseteq B \times C$*. Dokážte, že platí*

$$(M_{RS})^T = (M_S)^T (M_R)^T.$$

Reláciami, ktorých oborom a kooborom je tá istá množina sa síce budeme zaoberať až v 6. kapitole, ale jednu špeciálnu reláciu na množine definujeme už teraz.

Definícia 4.7. *Nech je* A *ľubovoľná množina, reláciu* $E_A = \{(a, a); a \in A\}$ *nazveme* identickou reláciou na množine A.

Pomocou identických relácií teraz popíšeme niektoré vzťahy medzi reláciami, ktoré sa vyskytnú pri skladaní binárnych relácií.

Veta 4.6. *Nech sú* A, B, C, D *ľubovoľné (konečné) množiny;* $R \subseteq A \times B, S \subseteq B \times C, T \subseteq C \times D$*. Potom sú nasledujúce výroky ekvivalentné*

1. $RS \cap T^{-} = \emptyset$,
2. $ST \cap R^{-} = \emptyset$,
3. $TR \cap S^{-} = \emptyset$,
4. $RST \cap E_A = \emptyset$,
5. $STR \cap E_B = \emptyset$,
6. $TSR \cap E_B C = \emptyset$.

Dôkaz. Ponechávame čitateľovi ako cvičenie. □

Uvažujme teraz množiny $A = \{a, b, c, d\}, B = \{1, 2, 3, 4\}$ a binárnu reláciu $R = \{(a, 1), (a, 2), (b, 1), (b, 2), (c_2)\}$. Na prvý pohľad je zrejmé, že nie každý prvok oboru (A) a kooboru (B) sa vyskytuje v niektorej z usporiadaných dvojíc relácie R. Aby sme nemuseli pracovať so zbytočne rozsiahlymi obormi a koobormi binárnych relácií, zavádzame pojem *projekcie relácie*.[7]

Definícia 4.8. *Nech je* $R \subseteq A \times B$ *ľubovoľná binárna relácia; nech* $X \subseteq A$. *Symbolom* $R[X]$ *označíme množinu všetkých takých* $y \in B$*, pre ktoré existuje* $x \in X$ *také, že binárna relácia* R *obsahuje usporiadanú dvojicu* (x, y). *Formálne*

$$R[X] = \{y \in B; (\exists x \in A) \& ((x, y) \in R\}.$$

Množina $R^{-}[B]$; $R^{-}[B] \subseteq A$ *sa nazýva prvou projekciou relácie* R *a označuje sa symbolom* $pr_1 R$*; množina* $R[A]$; $R[A] \subseteq B$ *sa nazýva druhou projekciou relácie* R *a označuje sa symbolom* $pr_2 R$*;*

Poznámka. V grafovej reprezentácii binárnej relácie $R \subseteq A \times B$ predstavuje prvá projekcia $pr_1 R$ množinu všetkých tých vrcholov, z ktorých vychádza aspoň jedna hrana a druhá projekcia $pr_2 R$ množinu tých vrcholov, do ktorých vchádza apoň jedna hrana. Prvkom množiny $A - pr_1 R \cup B - pr_2 R$ zodpovedajú vrcholy, z ktorých nevystupuje ani do nich nevstupuje žiadna hrana. [8]

Úloha 4.17. *Dokážte nasledujúce tvrdenie: nech je* $R \subseteq A \times B$ *ľubovoľná binárna relácia;* $X \subseteq A$ *a nech je* M *ľubovoľná množina. Potom platí*

$$(M \times X)R = M \times R[X].$$

Nech naviac $Y \subseteq B$*, potom*

$$R[Y \times M] = R^{-}[Y] \times M.$$

Úloha 4.18. *Možno priamo z matice* M_R *binárnej relácie* R *určiť obidve jej projekcie* $pr_1 R$ *a* $pr_2 R$*? Ak áno, ako?*

[7] Relácia R by mohla byť definovaná aj ako podmnožina karteziánskeho súčinu $\{a, b, c, d\} \times N$. V tomto prípade by sme však asi mali problémy tak s grafovou ako aj s maticovou reprezentáciou danej relácie.

[8] Vrchol grafu, do ktorého nevstupuje, ani z neho nevystupuje žiadna hrana, sa nazýva *izolovaný vrchol*.

Nasledujúce dve vety popisujú vlastnosti množiny $R[X]$. Na prvý pohľad pripomínajú tvrdenia vety 4.3. Aj dôkaz tejto vety nápadne pripomína dôkazy tvrdení vety 4.3. Rozdiel je v tom, že vo vete vystupujú relácie, t.j. množiny usporiadaných dvojíc, kým v nasledujúcich dvoch vetách budeme pracovať s (bližšie nešpecifikovanými) množinami prvkov.

Veta 4.7. *Nech je* R *binárna relácia,* $R \subseteq A \times B$ *a nech* $X_1, X_2 \subseteq A$. *Potom platia nasledujúce vzťahy*

1. $R[X_1 \cup X_2] = R[X_1] \cup R[X_2]$,
2. *ak* $X_1 \subseteq X_2$, *tak* $R[X_1] \subseteq R[X_2]$,
3. $R[X_1 \cap X_2] \subseteq R[X_1] \cap R[X_2]$,
4. $R[X_1 - X_2] \supseteq R[X_1] - R[X_2]$.

Dôkaz. Metódu dôkazu ilustrujeme na identite (1).

$$\begin{aligned} y \in R[X_1] \cup R[X_2] &\equiv y \in R[X_1] \vee y \in R[X_2] \equiv \\ &\equiv \exists a_1[(a_1 \in X_1)\&(a_1, y) \in R] \vee \exists a_2[(a_2 \in X_2)\&(a_2, y) \in R] \equiv \\ &\equiv \exists a[((a \in X_1) \vee (a \in X_2))\&(a, y) \in R] \equiv y \in R[X_1 \cup X_2]. \end{aligned}$$

Ukážeme ešte dôvod, pre ktorý sa inklúzia vo vzťahu (3) nedá nahradiť rovnosťou. Inklúziu jedným smerom dokážeme ľahko

$$\begin{aligned} y \in R[X_1 \cap X_2] &\equiv \exists x[(x \in X_1 \cap X_2)\&(x, y) \in R] \equiv \\ &\equiv \exists x[(x \in X_1)\&(x \in X_2)\&(x, y) \in R] \equiv \exists x[[(x \in X_1)(x, y) \in R]\&[(x \in X_2)\&(x, y) \in R]] \Rightarrow \\ &\Rightarrow [[(a \in X_1)(a, y) \in R]\&[(a \in X_2)\&(a, y) \in R]] \Rightarrow y \in R[X_1]\&y \in R[X_2] \equiv y \in R[X_1] \cap R[X_2]. \end{aligned}$$

(V treťom kroku sme použili *pravidlo C* (choice - výber), ktoré sa zapisuje v tvare

$$\frac{\exists x A(x)}{A(t)}$$

kde t je prvok s vlastnosťou A.) Pokúsme sa dokázať opačnú inklúziu:

$$\begin{aligned} y \in R[X_1] \cap R[X_2] &\equiv y \in R[X_1]\&y \in R[X_2] \equiv \\ &\equiv \exists x[(x \in X_1)\&(x, y) \in R]\&\exists z[(z \in X_2)\&(z, y) \in R]. \end{aligned}$$

A tu je podstata problému. V predchádzajúcom prípade sme mohli odvodiť, že ak existuje $a_1 \in X_1$ alebo $a_2 \in X_2$, tak potom existuje aj nejaké $a \in X_1 \cup X_2$ ($a = a_1$ alebo $a = a_2$). V našom prípade však môže nastať taká situácia, že a_1, a_2 sú jediné dva prvky množiny A také, že

$$\begin{aligned} &\exists x[(x \in X_1)\&(x, y) \in R] \Rightarrow [(a_1 \in X_1)\&(a_1, y) \in R] \\ &\exists z[(z \in X_2)\&(xz, y) \in R] \Rightarrow [(a_2 \in X_2)\&(a_2, y) \in R], \end{aligned}$$

a $a_1 \in X_1 - X_2, a_2 \in X_2 - X_1$. Potom však neexistuje prvok $a \in X_1 \cap X_2$, pre ktorý $(a, y) \in R$. Preto vo vzťahu (3) a z podobných dôvodov ani vo vzťahu (4) nemôžeme nahradiť inklúziu rovnosťou. □

Úloha 4.19. *Ilustrujte tvrdenia vety 4.7 na vhodných príkladoch!*

Úloha 4.20. *Dokážte zostávajúce tvrdenia vety 4.7!*

Veta 4.8. *Nech sú* R, R_1, R_2 *relácie z* A *do* B *a nech* $X \subseteq A, Y \subseteq B$. *Potom platia nasledujúce vťahy*

1. $(R_1 \cup R_2)[X] = R_1[X] \cup R_2[X]$,
2. *ak* $R_1 \subseteq R_2$, *tak potom* $R_1[X] \subseteq R_2[X]$,
3. $(R_1 \cap R_2)[X] \subseteq R_1[X] \cup R_2[X]$,
4. $(R_1 - R_2)[X] \supseteq R_1[X] - R_2[X]$.

Dôkaz. Ponechávame čitateľovi ako cvičenie. □

Aj dôkaz ďalšieho jednoduchého tvrdenia o skladaní binárnych relácií ponechávame čitateľovi.

Úloha 4.21. *Dokážte nasledujúce tvrdenie! Nech je* R *relácia z* A *do* B; S *relácia z* B *do* C *a nech* $X \subseteq A, Y \subseteq B$. *Potom platí*

1. $(RS)[X] = S[R[X]]$,
2. $X \subseteq pr_1 R$ *práve vtedy, ak* $X \subseteq (RR^{-})[X]$,
3. $Y \subseteq pr_2 R$ *práve vtedy, ak* $Y \subseteq (R^{-}R)[Y]$.

4.4 Jednoznačné relácie a všade definované relácie

Doteraz sme sa zaoberali binárnymi reláciami, o ktorých sme však (okrem toho, že sú podmnožinami nejakého karteziánskeho súčinu) nič nepredpokladali. Aby sme dostali zaujímavejšie a použiteľnejšie binárne relácie, musíme na takto všeobecne definované relácie položiť ďalšie podmienky. Ukázalo sa, že ak binárnu reláciu chápeme ako množinu usporiadaných dvojíc tak potom tú istú binárnu reláciu môžeme definovať ako podmnožinu karteziánskych súčinov rozličných množín.[9] Pri skúmaní projekcií binárnych relácií sme zistili, že obor a koobor binárnej relácie môže byť zbytočne veľký. Všade definovaná relácia je z hľadiska „veľkosti“ oboru binárnej relácie optimálna. (Koobor binárnej relácie môžeme zasa zbaviť zbytočných prvkov stanovením požiadavky, aby bola opačná relácia k danej binárnej relácii všade definovaná.) Zavedieme pojem všade definovanej relácie formálne a preskúmame základné vlastnosti všade definovaných relácií.

[9] binárnu reláciu $R \subseteq A \times B$ môžeme chápať aj ako usporiadanú trojicu $(A, B, R \subseteq A \times B)$. Potom sú však binárne relácie $(A, B, R \subseteq A \times B)$ a $(A', B', R \subseteq A' \times B')$ rôzne, pretože $A' \times B' \neq A \times B$.

Definícia 4.9. *Nech je* R *taká binárne relácia z* A *do* B*, že* $pr_1 R = A$*. Potom hovoríme, že relácia* R *je všade definovaná.*

Čím sa odlišuje všade definovaná relácia od „obyčajnej" binárnej relácie? Veľmi názorne sa vlastnosť „byť všade definovaná" prejavuje na grafe binárnej relácie. Z každého vrcholu prislúchajúcemu prvku oboru všade definovanej binárnej relácie vychádza aspoň jedna hrana. Pozrieme sa, ako súvisí vlastnosť binárnej relácie „byť všade definovaná" s jej inými vlastnosťami.

Veta 4.9. *Nech je* R *binárna relácia z* A *do* B*. Potom sú nasledujúce výroky ekvivalentné:*

1. *binárna relácia* R *je všade definovaná,*
2. *pre každé* $x \in A$ *platí* $R[\{x\}] \neq \emptyset$,
3. $E_A \subseteq RR^{-}$.

Dôkaz. Dokážeme tri implikácie: $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$:

(1) $\Rightarrow$ **(2)** Sporom. Nech je R všade definovaná, ale nech zároveň existuje $a \in A$ také, že $R[\{a\}] = \emptyset$. Potom však $a \notin pr_1 R$. Ale $pr_1 R = A$, lebo relácia R je všade definovaná. T.j. $a \in A$ a súčasne $a \notin A$. Spor.

(2) $\Rightarrow$ **(3)** Sporom. Nech $\forall[(x \in A) \Rightarrow (R[\{x\}] \neq \emptyset)]$ a zároveň $E_A \not\subseteq RR^{-}$. To znamená, že existuje nejaký prvok $a \in A$ taký, že $(a,a) \in E_A - RR^{-}$. Rozpíšeme podrobne tvrdenie $\neg[(a,a) \in RR^{-}]$:

$$\neg[(a,a) \in RR^{-}] \equiv \neg\exists x[(x \in B)\&((a,x) \in R)\&((x,a) \in R^{-})] \equiv$$
$$\equiv \forall x \neg[(x \in B)\&((a,x) \in R)\&((x,a) \in R^{-})] \equiv$$
$$\forall x[\neg(x \in B) \vee \neg((a,x) \in R) \vee \neg((x,a) \in R^{-})] \equiv$$
$$\equiv \forall x[\neg(x \in B) \vee \neg((a,x) \in R)] \equiv \forall x[(x \in B) \Rightarrow \neg((a,x) \in R)] \equiv R[\{a\}] = \emptyset.$$

Spor.

(3) $\Rightarrow$ **(1)** Sporom. Nech $E_A \subseteq RR^{-}$, ale binárna relácia R nie je všade definovaná. To znamená, že existuje prvok $a \in A$ taký, že $a \notin pr_1 R$. Potom však neexistuje také $y \in B$, že $(a,y) \in R$ (ani $(y,a) \in R^{-}$), a teda $(a,a) \notin RR^{-}$. Ale $(a,a) \in E_A \subseteq RR^{-}$, a to je hľadaný spor. □

Vlastnoť binárnej relácie „byť všade definovaná" zaručuje, že každý prvok oboru vystupuje (ako prvý prvok) aspoň v jednej usporiadanej dvojici danej relácie. To znamená, že pre ľubovoľný prvok oboru bude vo všade definovanej binárnej relácii určite existovať jedna a možno aj niekoľko usporiadaných dvojíc s daným prvkom oboru na prvom mieste. V reálnom živote ale aj matematike sa často stretávame s prirodzenou požiadavkou, aby prvku oboru binárnej relácie zodpovedal najviac jeden prvok kooboru (napríklad dvojice (pacient, výsledky vyšetrení), (tovar, cena), (študent, hodnotenie na konkrétnej skúške) a pod.) Relácia, ktorá spĺňa túto požiadavku, sa nazýva *jednoznačná relácia*.

Definícia 4.10. *Nech je* R *binárna relácia z* A *do* B. *Ak pre každý prvok* $(x \in A)$ *oboru relácie* R *platí, že množina* $R[\{x\}]$ *má najviac jeden prvok, tak potom hovoríme, že binárna relácia* R *je jednoznačná relácia.*

Poznámka. Kvôli zjednodušeniu označovania budeme namiesto $R[\{x\}]$ písať len $R(x)$.

Úloha 4.22. *Zaviedli sme dve nové vlastnosti binárnych relácií - jednoznačnosť a „byť všade definovaná". Binárna relácia nemusí mať žiadnu z týchto vlastností, jednu z nich, alebo obidve súčasne. Preskúmajte všetky 4 možnosti a charakterizujte, čím sa vyznačuje grafová (maticová) reprezentácia binárnej relácie s danými vlastnosťami!*

Úloha 4.23. *Nech je* R *binárna relácia z* A *do* B. *Aké vzťahy platia medzi reláciami* RR^-, R^-R, E_A, E_B*?*

Teraz preskúmame, aký vplyv má jednoznačnosť binárnej relácie na jej ostatné vlastnosti.

Veta 4.10. *Nech je* R *binárna relácia z* A *do* B, C *je ľubovoľná množina, potom nasledujúce tvrdenia sú ekvivalentné:*

1. R *je jednoznačná relácia,*
2. $RR^- \subseteq E_B$,
3. *ak* S_1, S_2 *sú ľubovoľné relácie z* B *do* C, *tak* $R(S_1 \cap S_2) = RS_1 \cap RS_2$,
4. *ak* S_1, S_2 *sú ľubovoľné relácie z* B *do* C, *tak* $R(S_1 - S_2) = RS_1 - RS_2$,
5. *ak* $Y_1, Y_2 \subseteq B$, *tak* $R^-[Y_1 - Y_2] = R^-[Y_1] - R^-[Y_2]$,
6. *ak* $Y_1, Y_2 \subseteq B$, *tak* $R^-[Y_1 \cap Y_2] = R^-[Y_1] \cap R^-[Y_2]$,
7. *ak* $Y_1, Y_2 \subseteq B$ *a* $Y_1 \cap Y_2 = \emptyset$, *tak* $R^-[Y_1 \cap Y_2] = \emptyset$.

Dôkaz. Budeme postupovať podľa schémy $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 5 \Rightarrow 6 \Rightarrow 7 \Rightarrow 1$.

(1) $\Rightarrow$ (2) Nech je R jednoznačná relácia a nech neplatí $RR^- \subseteq E_B$. To znamená, že existuje usporiadaná dvojica $(y_1, y_2) \in R^-R$ a $y_1 \neq y_2$; t.j. $(y_1, y_2) \notin E_B$. Potom však existuje $x \in A$ také, že $(y_1, x) \in R^-$ a $(x, y_2) \in R$. Podľa definície inverznej relácie tvrdenie $(y_1, x) \in R^-$ je ekvivalentné tvrdeniu $(x, y_1) \in R$. Ale aj $(x, y_2) \in R$ a $y_1 \neq y_2$ a to je spor s jednoznačnosťou relácie R.

(2) $\Rightarrow$ (3) Sporom. Nech $RR^- \subseteq E_B$, ale $R(S_1 \cap S_2) \neq RS_1 \cap RS_2$. Vo vete 4.3 sme už dokázali platnosť inklúzie $R(S_1 \cap S_2) \subseteq RS_1 \cap RS_2$. Tvrdenie $R(S_1 \cap S_2) \neq RS_1 \cap RS_2$ je teda ekvivalentné tomu, že $R(S_1 \cap S_2) \not\supseteq RS_1 \cap RS_2$; resp. že existuje usporiadaná dvojica $(x, y) \in RS_1 \cap RS_2 - R(S_1 \cap S_2)$. Ak $(x, y) \in RS_1 \cap RS_2$, tak potom existujú také $z_1, z_2 \in B$, že $(x, z_1) \in R$ a $(z_1, y) \in S_1$ a $(x, z_2) \in R$ a $(z_2, y) \in S_2$. Súčasne musí platiť $z_1 \neq z_2$,

$(z_1, y) \notin S_2$, $(z_2, y) \notin S_1$ a neexistuje $z \in B$ také, že $(x, z) \in R$ a $(z, y) \in S_1 \cap S_2$, pretože ináč by $(x, y) \in R(S_1 \cap S_2)$. Ale potom z toho, že $(x, z_1) \in R$ a $(x, z_2) \in R$, vyplýva, že $(z_1, x) \in R^-$ a $(x, z_2) \in R$, a napokon $(z_1, z_2) \in R^-R$. Keďže $z_1 \neq z_2$, $(z_1, z_2) \notin E_B$, a to je potrebný spor.

(3) ⇒ (4) Predpokladajme, že $R(S_1 \cap S_2) = RS_1 \cap RS_2$, ale $R(S_1 - S_2) \neq RS_1 - RS_2$. Podľa vety 4.3 je posledné tvrdenie ekvivalentné s tým, že $R(S_1 - S_2) \supset RS_1 - RS_2$. To znamená, že existuje usporiadaná dvojica (napríklad) $(x, y) \in R(S_1 - S_2)$, ktorá nepatrí do $RS_1 - RS_2$. Ak $(x, y) \in R(S_1 - S_2)$, tak existuje $z_1 \in B$; také, že $(x, z_1) \in R \& (z_1, y) \in (S_1 - S_2)$. Z toho však vyplýva, že $(x, z_1) \in R \& (z_1, y) \in S_1$; t.j., že $(x, y) \in RS_1$. Aby bol splnený predpoklad, že $(x, y) \notin (RS_1 - RS_2)$, musí platiť $(x, y) \in RS_2$. Keďže $(z_1, y) \notin S_2$, musí existovať iný prvok $z_2 \in B; z_2 \neq z_1$ pre ktorý platí $(x, z_2) \in R \& (z_2, y) \in S_2 - S_1$. Potom platí $(x, y) \in RS_2$. Na druhej strane, $(x, y) \in RS_1 \cap RS_2$ ale keďže nemôže existovať prvok $z \in B; (x, z) \in R \& (z, x) \in S_1 \cap S_2$, potom $(x, y) \notin R(S_1 \cap S_2)$. Spor.

(4) ⇒ (5) Nech $R(S_1 - S_2) = RS_1 - RS_2$ a nech $R^-[Y_1 - Y_2] \neq R^-[Y_1] - R^-[Y_2]$. Na opačnú reláciu R^- sa dívame ako na reláciu z B do A a budeme používať vetu 4.7. Z druhého predpokladu vyplýva, že $R^-[Y_1 - Y_2]$ je vlastnou nadmnožinou $R^-[Y_1] - R^-[Y_2]$. To znamená, že $R^-[Y_1 - Y_2]$ obsahuje prvok x, ktorý nepatrí do množiny $R^-[Y_1] - R^-[Y_2]$. Ale $x \in R^-[Y_1 - Y_2]$ práve vtedy, ak existuje $y_1 \in Y_1 - Y_2$ také, že $(y_1, x) \in R^-$. To znamená, že $y_1 \in Y_1, x \in R^-[Y_1]$. Ak $x \notin R^-[Y_1] - R^-[Y_2]$, tak potom $x \in R^-[Y_2]$. Ale $y_1 \notin Y_2$. To znamená, že musí existovať ešte jeden prvok, $y_2 \in Y_2 - Y_1, y_2 \neq y_1$ a $(y_2, x) \in R^-$. Ak však $(y_1, x) \in R^-$ a $(y_2, x) \in R^-$, potom $(x, y_1) \in R$ a $(x, y_2) \in R$. Zvolíme si relácie $S_1 = \{(y_1, z)\}, S_2 = \{(y_2, z)\}$. Potom $R(S_1 - S_2) = \{(x, z)\}$, ale $RS_1 - RS_2 = \emptyset$. Spor.

(5) ⇒ (6) Nech $R^-[Y_1 - Y_2] = R^-[Y_1] - R^-[Y_2]$ a $R^-[Y_1 \cap Y_2] \neq R^-[Y_1] \cap R^-[Y_2]$. Potom zrejme $R^-[Y_1 - \cap Y_2]$ je vlastnou podmnožinou $R^-[Y_1] \cap R^-[Y_2]$. Podobne ako v predchádzajúcom prípade nech $x \in R^-[Y_1] \cap R^-[Y_2]$ a nech $x \notin R^-[Y_1 \cap Y_2]$. To znamená, že v B existujú prvky $y_1 \in Y_1 - Y_2$ a $y_2 \in Y_2 - Y_1$ také, že $(y_1, x) \in R^-$ a $(y_2, x) \in R^-$. Potom $x \notin R^-[Y_1 \cap Y_2]$, ale $x \in R^-[Y_1] \cap R^-[Y_2]$. Na druhej strane $x \in R^-[Y_1 - Y_2]$, lebo $y_1 \in Y_1 - Y_2$, ale $x \notin R^-[Y_1] - R^-[Y_2]$. Spor.

(6) ⇒ (7) Nech $R^-[Y_1 \cap Y_2] = R^-[Y_1] \cap R^-[Y_2]$, a $Y_1 \cap Y_2 = \emptyset$, ale $R^-[Y_1 \cap Y_2] \neq \emptyset$. Ak $Y_1 \cap Y_2 = \emptyset$, tak potom $Y_1 - Y_2 = Y_1$ a $R^-[y_1 - Y_2] = R^-[Y_1] = R^-[Y_1] - R^-[Y_2]$. Ak by $R^-[Y_1 \cap Y_2] \neq \emptyset$, tak potom by $R^-[Y_1] - R^-[Y_2] \neq R^-[Y_1]$. Spor.

(7) ⇒ (1) Nech pre ľubovoľné $Y_1, Y_2 \subseteq B$ platí ak $Y_1 \cap Y_2 = \emptyset$, tak $R^-[Y_1 \cap Y_2] = \emptyset$, a R nie je jednoznačná relácia. Potom obsahuje usporiadané dvojice $(x, y_1), (x, y_2); y_1 \neq y_2$. Zvolíme $Y_1 = \{y_1\}, Y_2 = \{y_2\}$. Zrejme $Y_1 \cap Y_2 = \emptyset$, ale $R^-[Y_1] \cap R^-[Y_2] \neq \emptyset$. Spor. □

Dôkaz ďalšieho tvrdenia ponechávame na čitateľa.

Veta 4.11. *Nech sú* A, B *ľubovoľné množiny, nech* $X \subseteq A$ *a* R_1, R_2 *sú ľubovoľné relácie z* A *do* B. *Potom sú nasledujúce výroky ekvivalentné*

1. $(R_1 \cap R_2)[X] = R_1[X] \cap R_2)[X]$,
2. $(R_1 - R_2)[X] = R_1[X] - R_2)[X]$,
3. X *obsahuje najviac jeden prvok.*

Zostáva pri skladaní relácií zachovaná jednoznačnosť a vlastnosť „byť všade definovaná“? Na túto otázku dáva odpoveď nasledujúca veta.

Veta 4.12. *Nech je* R *relácia z* A *do* B*,* S *relácia z* B *do* C*. Potom platí*

1. *Ak sú* R, S *všade definované relácie, tak potom je aj relácia* RS *všade definovaná,*
2. *Ak sú* R, S *jednoznačné relácie, tak potom je aj relácia* RS *jednoznačná.*

Dôkaz. (1) Nech sú R, S všade definované relácie, potom $R^-[B] = A, S^-[C] = B$. Ale potom $(RS)^-[C] = (S^-R^-)[C] = S^-[R^-[C]] = S^-[B] = A$.

(2) Nech sú R, S jednoznačné relácie, potom $R^-R \subseteq E_B$, $S^-S \subseteq E_C$. Z toho a z vety 4.10 pre zloženú reláciu RS vyplýva

$$(RS)^-(RS) = (S^-R^-)(RS) = S^-(R^-R)S \subseteq S^-E_BS = S^-S \subseteq E_C.$$

□

Predpokladajme, že je daná nejaká relácia R z A do B. Niekedy nás nemusí zaujímať celá relácia R, ale len tie usporiadané dvojice z R, ktorých prvý, resp. druhý prvok je z nejakej podmnožiny $A_1 \subset A$, resp. $B_1 \subset B$. Keďže aj množina takýchto usporiadaných dvojíc je podmnožinou karteziánskeho súčinu, ide o špeciálny prípad binárnej relácie $R_1 \subset R \subseteq A \times B$, ktorú budeme nazývať *zúžením relácie* R.

Definícia 4.11. *Nech je* R *relácia z* A *do* B *a nech* $A_1 \subseteq A$*,* $B_1 \subseteq B$*. Relácia* R_1 *z* A_1 *do* B_1*;* $R_1 = R \cap A_1 \times B_1$ *sa nazýva zúžením relácie* R *na* (A, B)*. Relácia* R *sa nazýva rozšírením relácie* R_1 *na* (A, B)*.*

Úloha 4.24. *Dokážte alebo vyvráťte nasledujúce tvrdenia. Zúženie jednoznačnej relácie je jednoznačná relácia. Zúženie všade definovanej relácie je všade definovaná relácia.*

K najdôležitejšíjm binárnym reláciám patria relácie usporiadania, ekvivalencie a zobrazenia. Túmto reláciám venujeme samostatné kapitoly.

Kapitola 5

Zobrazenia/funkcie

Zobrazenia (alebo funkcie) sú z formálneho hľadiska „len“ zvláštnym prípadom relácií. V matematike a jej aplikáciách však zohrávajú veľmi významnú úlohu, a (aj) preto ich štúdiu budeme venovať samostatnú kapitolu. Najprv zavedieme pojem zobrazenia (funkcie) a budeme študovať základné vlastnosti zobrazení, potom položíme na zobrazenia dodatočné požiadavky (injektívnosť, surjektívnosť a bijektívnosť) a pozrieme sa na to, ako sa zmenia množinové vzťahy platiace pre „obyčajné“ zobrazenia. Zavedené pojmy ilustrujeme na niekoľkých zaujímavých funkciách, ktoré sa v informatike často používajú. Začneme základnými pojmami.

Definícia 5.1. *Všade definovaná jednoznačná relácia* f *z* A *do* B *sa nazýva zobrazením (funkciou) z* A *do* B*; množina* A *sa nazýva definičným oborom (alebo len oborom) zobrazenia* f *a množina* B *oborom funkčných hodnôt (alebo len kooborom) zobrazenia* f*. Ak* $x \in A$*, tak prvok* $f(x)$ *sa nazýva obrazom prvku* x *v zobrazení* f *(alebo hodnotou funkcie* f *v prvku* x*). To, že je* f *zobrazenie z* A *do* B *budeme symbolicky zapisovať takto* $f : A \to B$.

Poznámka. Pripomíname, že aj pre zobrazenia zostávajú v platnosti pojmy a označenia, ktoré sme zaviedli pre binárne relácie. Len podmnožinu $f[X]$ kooboru zobrazenia f budeme označovať symbolom $f(X)$ tak ako to je bežné v matematickej literatúre. Pod pojmom funkcia sa niekedy rozumie zobrazenie definované na číselných množinách. My budeme pojmy zobrazenie a funkcia chápať a používať ako synonymá.

Príklad 5.1. *Uvedieme niekoko príkladov zobrazení.*

1. *Konštantná funkcia* $f : R \to R$*, napr. pre* $\forall x \in R f(x) = 5$*,*
2. *Identické zobrazenie* $E_A : A \to A; \forall x \in A E_A(x) = x$*,*
3. *Usporiadanú* n*-ticu prvkov* $(a_1, \ldots, a_n)$ *možno chápať ako zobrazenie* $f : \{1, \ldots, n\} \to A; f(i) = a_i$.
4. *Od usporiadanej* n*-tice môžeme prejsť k nekonečnej postupnosti prvkov množiny* A*:* $\{a_n\}_{n \geq 0} = a_0, a_1, \ldots$*, ktorú môžeme definovať ako zobrazenie* $f : N \to A; f(i) = A_i$.

5. *Na základe usporiadania*[1] *množiny prirodzených čísel definujeme funkciu bezprostredného nasledovníka:* $s : \mathbb{N} \to \mathbb{N}; s(n) = n + 1$.

6. *Obor zobrazenia môže byť množina s nejakou štruktúrou. Nech napríklad* $A = A_1 \times A_2 \times \cdots \times A_n$. *Užitočným zobrazením je projekcia*[2] $l_n^m : A \to A_m; l_n^m(x_1, \ldots, x_n) = x_m$, *ktorá z* n*-tice prvkov vyberie* m*-tý.*

7. *Pomocou funkcie môžeme popísať aj množiny. Predpokladajme, že potrebujeme popísať podmnožiny množiny* M. *Charakteristická funkcia množiny* $A \subseteq M$ *je funkcia* $\chi_A : M \to \{0, 1\}$, *definovaná nasledovne:*

$$\chi_A(x) = \begin{cases} 1 & x \in A; \\ 0 & x \notin A \end{cases}$$

8. *Nech je* A *ľubovoľná množina. Zobrazenie* $f : A \times A \to A$ *sa nazýva binárnou operáciou. Príkladmi binárnych operácií na množine reálnych čísel sú aritmetické operácie sčítania, odčítania, násobenia a delenia.*

9. *Nech je daný zložený výrok* A *obsahujúci (elementárne) výroky* $p_1, p_2, \ldots, p_n$. *Každému elementárnemu výroku* p_i *priradíme premennú* x_i *takú, že*

$$x_i = \begin{cases} 1 & \textit{ak je výrok } p_i \textit{ pravdivý} \\ 0 & \textit{ak je výrok } p_i \textit{ nepravdivý.} \end{cases}$$

   Výroku A *priradíme funkciu* $f : \{0, 1\}^n \to \{0, 1\}$ *definovanú takto*

$$f(x_1, \ldots, x_n) = \begin{cases} 1 & \textit{ak je výrok } A \textit{ pravdivý pre daný súbor hodnôt} \\ & \textit{elementárnych výrokov;} \\ 0 & \textit{ináč.} \end{cases}$$

   takto definovaná funkcia f *sa nazýva Booleovskou funkciou a predstavuje pravdivostnú funkciu výroku* A.

10. *Pomocou zobrazení v matematike často popisujeme rozličné objekty a ich vlastnosti. Napríklad graf je definovaný ako usporiadaná dvojica* $G = (V, U)$ *, kde je množina vrcholov,* $V = \{v_0, \ldots, v_n\}$ *a* $U \subseteq V \times V$ *je množina hrán. Zobrazenie* $\deg : V \to \mathbb{N}$, *definované tak, že* $\deg(v_i) =$ *počet hrán incidentných*[3] *s vrcholom* v_i *určuje tzv. stupeň vrchola* v_i.

Pre lepšie pochopenie zavedených pojmov vyriešte nasledujúce úlohy.

Úloha 5.1. *Zistite, či sa usporiadaná dvojica* (a_1, a_2) *definovaná spôsobom uvedeným v predchádzajúcom príklade, zhoduje s usporiadanou dvojicou* $(a_1, a_2) = \{\{a_1\}, \{a_1, a_2\}\}$*!*

Úloha 5.2. *Ako vyzerá funkcia nasledovníka pre nasledujúce množiny:*

[1] zatiaľ sa uspokojíme s intuitívnycm chápaním usporiadania, korektnú definíciu zavedieme v kapitole 6

[2] presnejšie, projekciu možno definovať pre ľubovoľné $1 \leq m \leq n$. Projekciu l_n^m by sme mohli nzvať m-tou n-árnou projekciou

[3] to znamená vchádzajúcich do vrchola alebo vychádzajúcich z daného vrchola

(a) *párnych prirodzených čísel,*

(b) *prirodzených čísel deliteľných siedmimi,*

(c) *celých čísel?*

Úloha 5.3. *Zapíšte charakteristické funkcie nasledujúcich podmnožín množiny prirodzených čísel:*

(a) *párnych prirodzených čísel,*

(b) $\emptyset$*,*

(c) $\{1, 2, 3\}$

(d) $\mathbb{N}$.

Úloha 5.4. *Uveďte aspoň 5 príkladov binárnych operácií na množine celých čísel ktoré spĺňajú podmienky definície 5.1!*

Úloha 5.5. *Čím sa odlišuje grafová (maticová) reprezentácia relácie, ktorá nie je zobrazením od grafovej (maticovej) reprezentácie zobrazenia?*

Prikročíme ku skúmaniu základných vlastností zobrazení. Mnohé z týchto vlastností vyplývajú z toho, že každé zobrazenie je reláciou, na ktoré sú kladené dve doplňujúce podmienky ($f : A \to B$):

1. Každý prvok definičného oboru A je v relácii f s najviac jedným prvkom kooboru B (jednoznanosť),
2. Každý prvok definičného oboru A je v relácii f s aspoň jedným prvkom kooboru B (f je všade definovaná relácia).

Ak oslabíme definíciu zobrazenia tým, že upustíme od 2. podmienky (všade definovaná relácia), dostávame reláciu, ktorá nemusí byť pre niektoré prvky oboru definovaná. Takáto relácia f je potom zobrazením $f : \mathrm{pr}_1(f) \to B$ a nazýva sa *parciálnym (čiastočným) zobrazením* z A do B. Na označenie všade definovanej funkcie sa zvykne (v teórii vypočítateľnosti) používať aj pojem *totálna funkcia*.

Veta 5.1. *Nech je* R *relácia z* A *do* B. *Potom relácia* R *je zobrazením práve vtedy, ak* $E_A \subseteq RR^-$ *a* $E_B \supseteq R^-R$.

Dôkaz. Vyplýva z viet 4.10 a 4.9. Podľa vety 4.10 je relácia R jednoznačná práve vtedy, ak $R^-R \subseteq E_B$. Podľa vety 4.9 je relácia R všade definovaná práve vtedy, ak $E_A \subseteq RR^-$. □

Nech je $f : A \to B, X \subseteq A$. Pripomíname, že symbol $f(X)$ (obraz množiny X v zobrazení f) označuje množinu obrazov prvkov z množiny X v zobrazení f:

$$f(X) = \{y; y = f(x), x \in X\}.$$

Pozrieme sa, ako budú vyzerať obrazy zjednotenia, prieniku a rozdielu podmnožín z oboru (kooboru) zobrazenia.

Veta 5.2. *Nech je* $f : A \to B,\ X_1, X_2 \subseteq A,\ Y_1, Y_2 \subseteq B$. *Potom platia nasledujúce vzťahy*

(a) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$,

(b) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$,

(c) $f(X_1 - X_2) \supseteq f(X_1) - f(X_2)$,

(d) $f^-(Y_1 \cup Y_2) = f^-(Y_1) \cup f^-(Y_2)$,

(e) $f^-(Y_1 \cap Y_2) = f^-(Y_1) \cap f^-(Y_2)$,

(e) $f^-(Y_1 - Y_2) = f^-(Y_1) - f^-(Y_2)$.

Dôkaz. Veta je dôsledkom viet 4.10 a 4.8. □

Úloha 5.6. *Dokážte tvrdenie vety 5.2 priamo, bez odvolania sa na vety 4.10 a 4.8!*

Vieme, (a veríme, že ak čitateľ vyriešil úlohy, tak to vie aj on) že grafová reprezentácia zobrazenia sa vyznačuje tým, že z každého vrchola prislúchajúceho nejakému prvku z oboru zobrazenia vychádza práve jedna orientovaná hrana. Zdôrazňujeme ešte raz, že práve jedna a teda nie žiadna hrana, alebo naopak $2, 3$ alebo viac hrán. V maticovej reprezentácii zobrazenia ($f : A \to B$) sa zasa v každom riadku nachádza práve jedna jednotka. Preto možno maticu zobrazenia zjednodušiť (v prípade, ak má obor zobrazenia n prvkov)na maticu typu $n \times 1$. Táto matica bude mať na mieste, ktoré prislúcha prvku $a_i \in A$ hodnotu $f(a_i)$.

Príklad 5.2. *Štandardná a zjednodušená maticová reprezentácia zobrazenia je uvedená v nasledujúcich tabuľkách:*

	α	β	γ
a	*1*	*0*	*0*
b	*0*	*1*	*0*
c	*0*	*0*	*1*

x	$f(x)$
a	α
b	β
c	γ

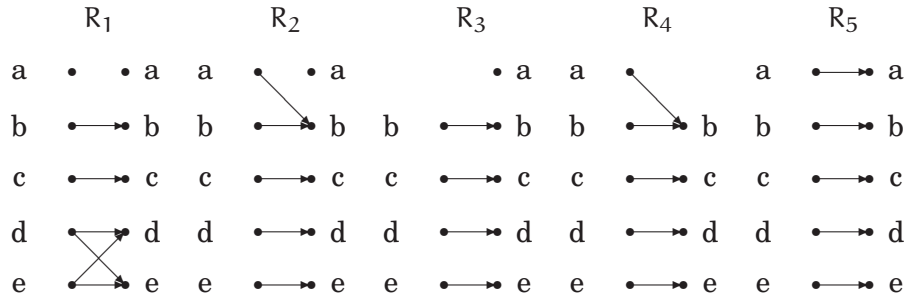
5.1 Injektívne, surjektívne a bijektívne zobrazenia

V definícii zobrazenia sa nič nehovorilo o tom, koľko prvkov oboru sa môže zobraziť na nejaký prvok kooboru, resp. či sa na každý prvok kooboru musí zobraziť nejaký prvok oboru. Doplnením dodatočných podmienok na zobrazenie upravujúcich—vyjadrené v grafovej terminológii—obmedzenia na stupne vrcholov zodpovedajúcich prvkom kooboru, dostávame tri dôležité triedy zobrazení.

Definícia 5.2. *Zobrazenie* $f : A \to B$ *sa nazýva*

(a) *injektívne, ak je relácia* f^- *jednoznačná,*

(b) *surjektívne, ak je relácia* f^- *všade definovaná*



Obrázok 5.1: Grafy relácií R_1, R_2, R_3, R_4, R_5.

(c) *bijektívne, ak je zobrazenie* f *injektívne a zároveň surjektívne.*

Injektívne zobrazenie f sa nazýva aj *injekcia* (alebo *prosté zobrazenie*), surjektívne zobrazenie budeme nazývať aj *surjekciou* (alebo *zobrazením z množiny* A *na množinu* B) a napokon bijektívne zobrazenie sa nazýva *bijekciou*, alebo *jedno-jednoznačným zobrazením*. Bijekciu $f : A \to A$ budeme nazvať aj *permutáciou množiny* A.

Na obrázku 5.1 sú uvedené grafy relácií R_1, R_2, R_3, R_4, R_5. Z nich

- R_1 nie je zobrazenie,
- R_2 je zobrazenie, ktoré však nie je ani injektívne, ani surjektívne,
- R_3 je len injekcia,
- R_4 je len surjekcia,
- R_4 je bijekcia.

Graf názorne ilustruje rozdiely medzi zobrazeniami, injekciami, surjekciami a bijekciami. Vidíme, že na to, aby zobrazenie $f : A \to B$ bolo injekciou, musí do každého vrcholu $b \in B$ vchádzať *najviac jedna* orientovaná hrana, pre surjekciu $f : A \to B$ platí, že do každého vrcholu $b \in B$ musí vchádzať *aspoň jedna* orientovaná hrana, a napokon bijekciu charakterizuje to, že do každého vrcholu $b \in B$ vchádza *práve jedna* orientovaná hrana. Využite grafovú reprezentáciu zobrazení a skúste spočítať, koľko existuje rozličných zobrazení medzi konečnými množinami!

Úloha 5.7. *Nech je* A n*-prvková a* B m*-prvková množina.*

(a) *Zistite, koľko existuje rozličných zobrazení z* A *do* B.

(b) *Zistite, koľko existuje rozličných injektívnych, surjektívnych a bijektívnych zobrazení z* A *do* B.

(c) *Spravte diskusiu vzhľadom na* n, m*!*

Preskúmame teraz vlastnosti injektívnych, surjektívnych a bijektívnych zobrazení trocha podrobnejšie.

Veta 5.3. *Nech je* f *ľubovoľné zobrazenie z* A *do* B. *Potom platí*

(a) f *je bijekcia práve vtedy, ak je opačná relácia* f^- *zobrazením,*

(b) *ak je zobrazenie* f *bijekcia, tak potom aj opačná relácia* f^- *je bijekciou z* B *do* A.

Dôkaz. (a) Ak je zobrazenie f bijekcia, tak je súčasne injektívne a surjektívne zobrazenie:

- f je injekcia práve vtedy, ak je opačná relácia f^- jednoznačná,
- f je surjekcia práve vtedy, ak je opačná relácia f^- všade definovaná relácia.

To znamená, že ak je zobrazenie f bijekcia, tak opačná relácia f^- je jednoznačná a všade definovaná relácia; t.j. opačná relácia f^- je zobrazením (z B do A).

(b) Podľa tvrdenia (a) ak je zobrazenie f bijekcia, tak opačná relácia f^- je zobrazením. Ale opačná relácia k relácii (zobrazeniu) f^- je f. Keďže f je zobrazenie, potom podľa (a) musí f^- byť bijekcia. □

Injektívnosť funkcie zjednodušuje aj vzťahy medzi obrazmi množín.

Veta 5.4. *Nech je* f *ľubovoľné zobrazenie z* A *do* B. *Potom sú nasledujúce výroky ekvivalentné*

(a) f *je injekcia,*

(b) *ak* $x_1, x_2 \in A,\ x_1 \neq x_2$, *tak* $f(x_1) \neq f(x_2)$,

(c) $f \circ f^- = E_A$,

(d) *ak* $X_1, X_2 \subseteq A$, *tak* $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$,

(e) *ak* $X_1, X_2 \subseteq A$, *tak* $f(X_1 - X_2) = f(X_1) - f(X_2)$,

(f) *ak* $X_1, X_2 \subseteq A$ *a* $X_1 \cap X_2 = \emptyset$ *tak* $f(X_1 \cap X_2) = \emptyset$.

Dôkaz. Dokážeme ekvivalenciu tvrdení (a) a (b). Ostatné tvrdenia vyplývajú z injektívnosti funkcie f a vety 4.10.

(a)$\Rightarrow$ **(b).** Sporom. Nech je f injekcia a súčasne existujú také $x_1, x_2 \in A,\ x_1 \neq x_2$, pre ktoré platí $f(x_1) = f(x_2) = y$. Potom však usporiadané dvojice $(x_1, y), (x_2, y)$ patria do f, a teda $(y, x_1) \in f^-,\ (y, x_2) \in f^-$, čo je v spore s jednoznačnosťou relácie f^-.

(b)⇒ (a). Sporom. Nech platí tvrdenie (b) a neplatí tvrdenie (a); t.j. pre ľubovoľné $x_1, x_2 \in A$, $x_1 \neq x_2$, tak $f(x_1) \neq f(x_2)$, ale f nie je injekcia. To znamená, že relácia f^- nie je jednoznačná, a teda existuje prvok $y \in B$, taký, že $(y, a) \in f^-$, $(y, b) \in f^-$ a $a \neq b$. Potom stačí položiť $x_1 = a, x_2 = b$ a dostávame $f(x_1) = f(x_2)$ pre $x_1 \neq x_2$, spor. □

Úloha 5.8. *Dokážte ekvivalenciu tvrdení predchádzajúcej vety 5.4 bez odvolania sa na vetu 4.10!*

Úloha 5.9. *Aby ste lepšie pochopili význam injektívnosti zobrazení, zostrojte jednoduché injektívne zobrazenie a demonštrujte na ňom tvrdenia vety 5.4!*

Úloha 5.10. *Porovnajte vlastnosti injektívneho zobrazenia a zobrazenia, ktoré nie je injektívne!*

Tvrdenie (b) z vety 5.4 sa veľmi často používa pri dokazovaní injektívnosti zobrazení. Aj surjektívne zobrazenie možno charakterizovať pomocou podobných tvrdení:

Veta 5.5. *Nech je f ľubovoľné zobrazenie z A do B. Potom sú nasledujúce výroky ekvivalentné*

(a) f *je surjekcia,*

(b) *pre každé* $y \in B$ *platí* $f^-(y) \neq \emptyset$,

(c) $f^- \circ f = E_B$.

Dôkaz. Vyplýva z viet 4.10, 4.9 a z toho, že relácia f^-. je všade definovaná relácia a zobrazenie f je jednoznačná relácia. □

Úloha 5.11. *Dokážte tvrdenie vety 5.5 bez odvolania sa na vety 4.10, 4.9!*

Pri spracovaní informácie je často výhodnejšie údaje transformovať z formy, v ktorej sme ich získali, do podoby, ktorá je vhodnejšia na spracovanie (napríklad prepísanie obsahu papierového dotazníka do elektronickej podoby). Takáto transformácia je zvláštnym prípadom kódovanie informácie. Kvôli jednoduchosti budeme predpokladať, že kódujeme texty zapísané nad nejakou *(zdrojovou) abecedou* pomocou textov nad tzv. *kódovou abecedou* Σ_2. *Kódovanie informácie* možno potom zadať pomocou zobrazenia (kódovacej funkcie) $\mathrm{Enc} : \Sigma_1^+ \to \Sigma_2^+$. Aby nebola kódovacia funkcia príliš zložitá, v kódovaní sa veľmi často definuje ako zobrazenie $\mathrm{Enc} : \Sigma_1 \to \Sigma_2^+$; t.j. popisuje, ako sa zapisujú znaky zdrojovej abecedy pomocou slov nad kódovou abecedou. Veľmi často, najmä ak sa informácia kóduje kvôli prenosu, alebo automatizovanému spracovaniu ale výsledok je určený človeku, je potrebné kódovanú informáciu spätne previesť do pôvodnej podoby. Túto transformáciu ralizuje *dekódovacia funkcia* $\mathrm{Dec} : \Sigma_2^+ \to \Sigma_1$.[4] Kódovanie je teda zadané usporiadanou dvojicou funkcií $(\mathrm{Enc}, \mathrm{Dec})$.[5] Nie každá dvojica funkcií $(\mathrm{Enc}, \mathrm{Dec})$ môže slúžiť na kódovanie a dekódovanie údajov. Nutnou požiadavkou, ktorá sa kladie

[4] Enc je skratka zo slova encoding a Dec označuje decoding (function).

[5] v dvojici kódovacia/dekódovacia funkcia je implicitne uchovaná aj informácia o zdrojovej a kódovej abecede a o slovách kódu.

na kódovaciu a dekódovaciu funkciu je jednoznačnosť dekódovania. Táto požiadavka sa dá definovať nasledovne: nech je M ľubovoľná množina správ nad zdrojovou abecedou. Potom dvojica funkcií (Enc, Dec) spĺňa požiadavku jednoznačnosti dekódovania, ak

$$\forall m \in M \quad Dec(Enc(m)) = m,$$

t.j. ľubovoľnú správu zakódovanú pomocou kódovacej funkcie Enc jednoznačne dekódujeme pomocou dekódovacej funkcie Dec.

Úloha 5.12. *Vypíšte tabuľku ASCII kódu znakov abecedy. Definujte zdrojovú abecedu, kódovú abecedu a kódovaciu a dekódovaciu funkciu. Ako sú tieto funkcie realizované napríklad v jazyku C?*

Injektívne zobrazenia sa od bijekcií odlišujú tým, že „nevyužívajú“ celý koobor, ktorý „majú k dispozícii“. Ak však vhodne zúžime koobor injektívneho zobrazenia, dostaneme bijekciu.

Veta 5.6. *Nech je* f *injekcia z* A *do* B *a nech* f_1 *je zúžením zobrazenia* f *na* $(A, pr_2 f)$. *Potom platí*

(a) *zobrazenie* f_1 *je bijekcia,*

(b) *ak* $g : B \to A$, *tak* $fg = E_A$ *práve vtedy, ak* g *je rozšírením zobrazenia* f_1^-.

Dôkaz. **(a)** Relácia f_1^- je jednoznačná a všade definovaná. To znamená, že f_1^- je zobrazenie, a teda opačné zobrazenie k f_1^-, $f_1 = (f_1^-)^-$ je bijekciou.

(b) Keďže tvrdenie má tvar ekvivalencie, potrebujeme dokázať dve implikácie. Prvú dokážeme sporom. Nech $g : B \to A$ a $fg = E_A$, ale g nie je rozšírením zobrazenia f_1^-. Potom existuje taká usporiadaná dvojica $(y, x) \in f_1^-$, ktorá nepatrí do g. Zobrazenie f je však injektívne, a to znamená, že množina $f^-(y)$ obsahuje najviac jeden prvok. Nech napr. $(x, y) \in f_1$, potom $(x, y) \in f$ a $f^-(y) = \{x\}$. Ale potom usporiadaná dvojica (x, x) nepatrí do zloženého zobrazenia fg, pretože $f(x) = y$ a zobrazenie g buď na prvku y nie je definované, alebo $g(y) \neq x$. Spor.

Dokážeme opačnú implikáciu. Nech $g : B \to A$, g je rozšírením zobrazenia f_1^- a $fg \neq E_A$ Keďže f je injekcia, platí $ff^- = E_A$ a zároveň $f_1 f_1^- = E_A$. Keďže zobrazenie g je rozšírením zobrazenia f_1^-, potom platí $E_A = f_1 f_1^- \subseteq f_1 g \subseteq fg$. Podľa predpokladu však $fg \neq E_A$; to znamená, že $E_A \subsetneq fg$. Z posledného tvrdenia výplýva, že musí existovať usporiadaná dvojica $(x_1, x_2) \in fg$; $x_1 \neq x_2$. Ak však $(x_1, x_2) \in fg$, tak potom existuje $y \in B$ také, že $(x_1, y) \in f$ a $(y, x_2) \in g$. Ale f_1 je zúžením zobrazenia f na $(A, pr_2 f)$, a teda platí $(x_1, y) \in f_1$, resp. $(y, x_1) \in f_1^-$. Zobrazenie g je rozšírením zobrazenia f_1^-, a teda $(y, x_1) \in g$. Potom však zobrazenie g obsahuje dve usporiadané dvojice $(y, x_1), (y, x_2)$; čo je v spore s jednoznačnosťou g. To znamená, že $fg = E_A$. □

Veta 5.7. *Nech je* f *surjekcia z* A *do* B *a nech* $h : B \to A$. *ptom* $hf = E_B$ *práve vtedy, ak* $h \subseteq f^-$.

Dôkaz. ($\Leftarrow$) Nech $h \subseteq f^-$. Pripomenieme, že podľa vety 5.1 pre zobrazenie platí $E_B \subseteq hh^-$. Využijeme teraz vetu 4.9. Keďže $h \subseteq f^-$ platí $h^- \subseteq f$ a

$$E_B \subseteq hh^- \subseteq hf \subseteq f^-f = E_B,$$

pretože f surjekcia.

($\Rightarrow$) Dokážeme opačnú implikáciu. Nech $hf = E_B$, potom $h^- = h^-E_B = h^-(hf) = (hh^-)f \subseteq E_Af = f$. To znamená, že $h \subseteq f^-$. □

Úloha 5.13. *Dokážte vetu 5.7 bez odvolania sa na vety 5.1 a 4.9!*

Poznámka. V definícii zobrazenia sme nekládli žiadne obmedzenia na množiny A, B (na obor a koobor zobrazenia). Čo by sa stalo, keby bola niektorá z týchto množín prázdna? Nech $A = \emptyset$. Potom $A \times B = \emptyset$ a keďže $f \subseteq A \times B$, potom aj $f = \emptyset$. Relácia f je jednoznačná a všade definovaná, a teda je zobrazením. Ak by však $A \neq \emptyset, B = \emptyset$ $f \subseteq A \times B = \emptyset$ je opäť prázdna relácia. Ale v tomto prípade f nie je všade definovaná, lebo jej obor $A \neq \emptyset$, a teda f nie je zobrazením. To znamená, že z podmienok $A \neq \emptyset, f : A \to B$ vyplýva, že $B \neq \emptyset$. V ďalšom sa budeme zaoberať zobrazeniami, ktoré majú neprázdny (definičný) obor. Nasledujúca veta umožňuje inú charakterizáciu injektívnosti a surjektívnosti zobrazení.

Veta 5.8. *Nech* $A \neq \emptyset, f : A \to B$. *Potom platí*

(a) *zobrazenie* f *je injekcia práve vtedy, ak existuje také zobrazenie* $g : B \to A$, *že* $fg = E_A$,

(b) *zobrazenie* f *je surjekcia práve vtedy, ak existuje také zobrazenie* $g : B \to A$, *že* $gf = E_B$.

Dôkaz. (a) Využijeme vetu 5.6. Ak je f injekcia, tak potom jej zúženie $f_1 : A \to pr_2 f$ je bijekcia a platí $f_1 f_1^- = ff^- = E_A$. Zobrazenie f_1^- nie je definované na množine $B - pr_2 f$, a preto nemôže byť hľadaným zobrazením g. Rozšírime vhodným spôsobom f_1^- na g. Vyberieme ľubovoľný prvok $a \in A$ a definujeme zobrazenie $g : B \to A$ nasledujúcim spôsobom:

$$g(y) = \begin{cases} f_1^-(y) & \text{ak} \quad y \in pr_2 f, \\ a & \text{ak} \quad y \in B - pr_2 f. \end{cases}$$

Relácia $g \subseteq B \times A$ je jednoznačná a všade definovaná, a teda je zobrazením. Presvedčíme sa ešte, že platí $fg = E_A$. Nech $x \in A$. Potom

$$(fg)(x) = g(f(x)) = g(f_1(x)) = f_1^-(f_1(x)) = x.$$

Dokážeme opačnú implikáciu. Nech existuje zobrazenie $g : B \to A$ také, že $fg = E_A$ a nech f nie je injekcia. To znamená, že existujú dva prvky $x_1, x_2 \in A$ a prvok $y \in B$ také, že $x_1 \neq x_2$ a $f(x_1) = f(x_2) = y$. Zobrazenie g je však jednoznačné a na prvku y nadobúda

hodnotu (napr.) $g(y) = a'$. Je zrejmé, že najviac jeden z prvkov $x_1, x_2 \in A$ sa môže rovnať a'. Nech napríklad $x_1 \neq a'$, potom

$$(fg)(x_1) = g(f(x_1)) = g(y) = a',$$

a teda $(x_1, a') \in fg$ a súčasne $(x_1, a') \notin E_A$. Spor.

(b) Nech $f : A \to B$ surjekcia. Uvažujeme reláciu $f^- \subseteq B \times A$. Táto relácia je všade definovaná, ale nemusí byť jednoznačná. Definujeme zobrazenie $g : B \to A$ nasledujúcim spôsobom:

- ak $f^-(y) = \{x\}$, položíme $g(y) = x$,
- ak $f^-(y)$ obsahuje viacero prvkov, napr. $f^-(y) = \{x_1, x_2, \dots\}$, vyberieme jeden z nich a položíme (napr.) $g(y) = x_2$.

Dostávame jednoznačnú a všade definovanú reláciu (zobrazenie) $g \subseteq f^-$, pre ktorú podľa vety 5.7 platí $gf = E_B$.

Opačné tvrdenie dokážeme opäť sporom. Nech existuje zobrazenie $g : B \to A$ také, že $gf = E_b$ ale f nie je surjekcia. Potom existuje $y \in B$ také, že $f^-(y) = \emptyset$. Zobrazenie g je všade definované, a preto zobrazuje aj prvok y na nejaký prvok $a' \in A$; $g(y) = a'$. Zobrazenie f je však tiež všade definované, a teda zobrazuje aj prvok $a' \in A$ na nejaký prvok z množiny B: $f(a') = z$. Keďže $y \notin pr_2 f$, $z \neq y$ a platí

$$(gf)(y) = f(g(y)) = f(a') = z.$$

To znamená, že $(y, z) \in gf$. Keďže $y \neq z$, $(y, z) \notin E_B$, a nakoniec $gf \neq E_B$. Spor. □

Úloha 5.14. *Zistite, či by veta 5.8 platila aj bez predpokladu $A \neq \emptyset$!*

Úloha 5.15. *Dokážte nasledujúce tvrdenie. Nech $f : A \to B, g : B \to A$. Ak $fg = E_A$ tak potom f je injekcia a g surjekcia.*

Úloha 5.16. *Pokračovanie. Dokážte, že f nemusí byť surjekcia a g injekcia!*

Na záver tejto časti uvedieme ešte niekoľko tvrdení charakterizujúcich bijektívne zobrazenia.

Veta 5.9. *Nech $f : A \to B$ a obor A obsahuje aspoň dva prvky. Potom sú nasledujúce výroky ekvivalentné*

(a) *zobrazenie f je bijekcia,*

(b) *existujú také zobrazenia $g, h : B \to A$; $fg = E_A$ a $hf = E_B$.*

(c) *existuje jediné zobrazenie $f^{-1} : B \to A$, také, že $ff^{-1} = E_A, \quad f^{-1}f = E_B$,*

(d) *existuje jediné zobrazenie $g : B \to A$ také, že $fg = E_A$,*

(d) *existuje jediné zobrazenie $h : B \to A$ také, že $hf = E_B$.*

Dôkaz. (a)⇒(b) Ak je zobrazenie f bijektívne, tak je injektívne a zároveň surjektívne a existencia zobrazení $g, h : B \to A$ takých, že $fg = E_A$ a $hf = E_B$ vyplýva z vety 5.8.

(b)⇒(c) Nech existujú také zobrazenia $g, h : B \to A$; $fg = E_A$ a $hf = E_B$. Potom $g = E_b g = (hf)g = h(fg) = hE_A = h$, čiže zobrazenie f^{-1} existuje; $f^{-1} = g$. Dokážeme, že je jediné. Nech sú $f_1^{-1} \neq f_2^{-1}$ dve zobrazenia s vlastnosťami popísanými v (c). Potom platí

$$f_1^{-1} = E_B f_1^{-1} = hf_1 f_1^{-1} = h = hf_2 f_2^{-1} = E_b f_2^{-1} = f_2^{-1}.$$

(c)⇒(d) Zobrazenie $g : B \to A$ také, že $fg = E_A$ existuje, stačí položiť $g = f^{-1}$. Podľa tvrdenia (c) je takéto zobrazenie definované jednoznačne.

(d)⇒(e) Ak existuje zobrazenie $g : B \to A$ také, že $fg = E_A$, tak potom f je injektívne a g surjektívne zobrazenie (úloha 5.15).

(e)⇒(a) Ak existuje zobrazenie $h : B \to A$ také, že $hf = E_B$, tak f musí podľa vety 5.7. Predpokladajme, že f nie je injekcia. To znamená, že existujú aspoň dva prvky množiny A (tu sa uplatňuje predpoklad že množina A má aspoň dva prvky), $x_1, x_2 \in A$ a prvok $y \in B$ také, že $x_1 \neq x_2$ a $f(x_1) = f(x_2) = y$. Ale potom existujú dve rozličné zobrazenia $h_1, h_2 : B \to A$ také, že

- $h_1(z) = h_2(z)$, ak $z \neq y$,
- $h_1(y) = x_1$ a $h_2(y) = x_2$.

Pre zobrazenia h_1, h_2 zároveň platí $h_1 f = E_B = h_2 f$. Dostávame spor s tým, že zobrazenie $h : B \to A$ s vlastnoťou $hf = E_B$ je jediné. To znamená, že f musí byť injekcia. □

Poznámka. Trocha nezvyčajný je predpoklad o tom, že obor zobrazenia f je aspoň dvojprvkový. Predpokladajme, že $A = \{x\}$ a $B = \{y_1, y_2\}$. Nech $f(x) = y_1$. Potom existuje jediné zobrazenie $g : B \to A, g(y_1) = g(y_2) = x$ také, že $fg = E_A$ (tvrdenie (d)), ale f nie je surjekcia, a teda ani bijekcia, ako sa tvrdí v (a).

Úloha 5.17. *Zistite, ktoré z tvrdení vety 5.9 zostávajú v platnosti, ak sa vypustí predpoklad o tom, že množina A je aspoň dvojprvková.*

Kapitola 6

Relácie na množine

Doteraz sme sa zaoberali (najmä binárnymi) reláciami, ktoré popisovali vzťahy medzi prvkami rozličných typov. Zaujímavé a užitočné vzťahy však môžu existovať aj medzi prvkami toho istého typu. Tieto budeme popisovať pomocou relácií na množine. Skôr ako ich formálne definujeme, uvedieme niekoľko príkladov.

Príklad 6.1. *Nech* A *označuje množinu ľudí,* $x, y, z \in A$. *Definujeme nasledujúce vzťahy*

(a) $(x, y) \in R_1$ *práve vtedy, ak* x *je priateľ* y,

(b) $(x, y) \in R_2$ *práve vtedy, ak* x *je otec* y,

(c) $(x, y) \in R_3$ *práve vtedy, ak* x *je potomok* y,

(d) $(x, y) \in R_4$ *práve vtedy, ak* x *je brat* y,

(e) $(x, y, z) \in R_5$ *práve vtedy, ak* x *a* y *sú rodičia* z.

Príklad 6.2. *Nech* Z *označuje množinu celých čísel, pre* $x, y, z \in Z$ *definujeme*

(a) $(x, y) \in S_1$ *práve vtedy, ak* $x < y$,

(b) $(x, y) \in S_2$ *práve vtedy, ak* $x = y$,

(c) $(x, y) \in S_3$ *práve vtedy, ak* $x|y$ *(*x *delí* y*),*

(d) $(x, y) \in S_4$ *práve vtedy, ak* $x \leq y$.

(e) $(x, y, z) \in S_5$ *práve vtedy, ak* $x + y = z$.

Príklad 6.3. *Nech* C *označuje množinu priamok v rovine,* $p, q \in C$.

(a) $(p, q) \in T_1$ *práve vtedy, ak* $x||y$,

(b) $(p, q) \in T_2$ *práve vtedy, ak* $p \perp q$,

(c) $(p, q) \in T_3$ *práve vtedy, ak* p, q *majú spoločný bod.*

„Obyčajné“ n-árne[1] relácie, ktoré sme študovali predtým, boli definované ako podmnožiny karteziánskeho súčinu $A_1 \times A_2 \times \cdots \times A_n$ (vo všeobecnom prípade sú množiny A_i rôzne), relácie z predchádzajúcich príkladov boli definované ako podmnožiny karteziánskeho súčinu rovnakých množín.

Definícia 6.1. *Nech je A ľubovoľná množina, A^n označuje karteziánsky súčin $\underbrace{A \times \cdots \times A}_{n}$. Ľubovoľnú podmnožinu karteziánskeho súčinu A^n nazveme n-árnou reláciou na množine A.*

V ďalšom výklade sa sústredíme na skúmanie binárnych relácií na množine, pretože medzi nimi je viacero v matematike často používaných užitočných relácií, ako je usporiadanie, rovnosť, ekvivalencia. Tam, kde to nepovedie k nedorozumeniu, budeme namiesto pojmu binárna relácia používať len pojem relácia.

Poznámka. Medzi reláciami a reláciami na množine nie je zasa až taký veľký rozdiel. Uvažujme binárnu reláciu $R \subseteq A \times B$. Ak položíme $C = A \cup B$, môžeme definovať binárnu reláciu na množine $R' \subseteq C \times C$, takú, že $(x, y) \in R'$ práve vtedy, ak $(x, y) \in R$. Relácie R', R sú (ako množiny usporiadaných dvojíc) rovné; relácia R' je rozšírením relácie R.

Ak je binárna relácia R definovaná na n-prvkovej množine $A = \{a_1, \ldots, a_n\}$, možno ju jednoznačne popísať pomocou štvorcovej matice M_R typu $n \times n$. Ako uvidíme neskôr, v štvorcovej matici majú zvláštny význam prvky ležiace na miestach $(i, i); i = 1, \ldots, n$. Tieto prvky tvoria tzv. *hlavnú diagonálu matice*. (V štvorcovej matici existuje okrem hlavnej ešte jedna diagonála, tvoria ju prvky ležiace na miestach $(n-i+1, i); i = 1, \ldots, n$.) Reláciu R možno popísať aj pomocou grafu G_R. Graf G_R má n vrcholov, označených prvkami množiny A. Ak relácia R obsahuje usporiadanú dvojicu (a_i, a_j) v grafe G_R existuje orientovaná hrana vychádzajúca z vrcholu a_i a vchádzajúca do vrcholu a_j.

Úloha 6.1. *Využite grafovú reprezentáciu relácií na množine a vypočítajte, koľko je rozličných binárnych relácií na n-prvkovej množine A!*

Úloha 6.2. *Zvoľte vhodné podmnožiny množín A, B, C z príkladov 6.1,6.2 a 6.3 a vyjadrite príslušné binárne relácie pomocou maticovej i grafovej reprezentácie!*

S niektorými reláciami na množine sme sa už stretli v predchádzajúcich kapitolách:

- *identická relácia* na množine A, E_A je definovaná nasledovne
$$E_A = \{(x, x); x \in A\}$$
- *prázdna relácia* $\emptyset$ neobsahuje žiadne usporiadané dvojice a predstavuje teda prázdnu podmnožinu karteziánskeho súčinu $A \times A$.
- Špeciálnym prípadom binárnej relácie na množine A je samotný karteziánsky súčin $A \times A$. Ten predstavuje univerzálnu množinu pre všetky binárne relácie na množine A (napr. $R^c = A \times A - R$.)

[1] najčastejšie $n = 2$

Úloha 6.3. *Zostrojte maticovú reprezentáciu identickej relácie množiny* $\{0,1,2,3,4,5\}$*!*

Úloha 6.4. *Nech je* R *ľubovoľná relácia na množine* A*. Dokážte platnosť nasledujúcich vzťahov*

(a) $(x,y) \in E_A \equiv (x = y)$,

(b) $E_A R = R E_A = R$,

(c) $\emptyset R = R\emptyset = \emptyset$*!*

6.1 Vlastnosti binárnych relácií na množine

Binárne relácie na množine majú mnoho zaujímavých vlastností. My sa teraz sústredíme na skúmanie základných vlastností, ktoré sa v matematike používajú najčastejšie.

Definícia 6.2. *Nech* $R \subseteq A \times A$*. Binárnu reláciu* R *nazývame*

(a) *reflexívnou, ak* $\forall a[(a \in A) \rightarrow (a,a) \in R]$,

(b) *symetrickou, ak* $[(a,b) \in R] \rightarrow [(b,a) \in R]$,

(c) *tranzitívnou, ak* $[(a,b) \in R \& (b,c) \in R] \rightarrow [(a,c) \in R]$,

(d) *ekvivalenciou, ak je súčasne reflexívna, symetrická a tranzitívna,*

(e) *antisymetrickou, ak* $[(a,b) \in R \& (b,a) \in R] \rightarrow (a = b)$.

Uvažujme 6-prvkovú množinu $B = \{1,2,3,4,5,6\}$ a binárne relácie S_1, S_2, S_3, S_4 z príkladu 6.2. Vidíme, že S_1 je tranzitívna a ostatné vlastnosti z definície 6.2 nemá; S_2 je ekvivalencia; S_3 je reflexívna a antisymetrická; a napokon S_4 je reflexívna a antisymetrická a tranzitívna relácia.

Úloha 6.5. *Zostrojte maticové reprezentácie binárnych relácií* S_1, S_2, S_3, S_4 *z príkladu 6.2.*

Vlastnosti binárnych relácií, ktoré sme zaviedli v definícii 6.2 možno charakterizovať aj pomocou množinových vzťahov.

Veta 6.1. *Nech je* R *binárna relácia na množine* A*. Potom pre* R *platia nasledujúce vzťahy*

(a) *relácia* R *je reflexívna práve vtedy, ak* $E_A \subseteq R$,

(b) *relácia* R *je symetrická práve vtedy, ak* $R^- \subseteq R$,

(c) *relácia* R *je tranzitívna práve vtedy, ak* $R^2 \subseteq R$,

(d) *relácia* R *je antisymetrická práve vtedy, ak* $R \cap R^- \subseteq E_A$.

Dôkaz. Ponechávame čitateľovi ako cvičenie. □

Poznámka. Je zrejmé, že tvrdenie v bode (b) predchádzajúcej vety môžeme formulovať aj nasledovne: relácia R je symetrická práve vtedy, ak $R^{-} = R$.

Poznámka. V matematickej literatúre sa občas spomínajú aj iné binárne relácie na množine. Uvedieme niektoré z nich. Predpokladáme, že R je binárna relácia na množine A. Potom hovoríme, že relácia R je

(a) ireflexívna, ak $\forall a[(a \in A) \rightarrow [(a, a) \notin R]$

(b) asymetrická, ak $\forall a \forall b[(a, b) \in R \rightarrow (b, a) \notin R]$

(c) atranzitívna, ak $[(a, b) \in R \& (b, c) \in R] \rightarrow [(a, c) \notin R$

(d) trichotomická, ak

$$\forall a \forall b[(a \in A) \& (b \in A) \& (a \neq b)] \rightarrow [(a, b) \in R \vee (b, a) \in R],$$

(e) tolerancia, ak je reflexívna a symetrická.

Úloha 6.6. *Ktoré z binárnych relácií na množine, ktoré sme doposiaľ skúmali, majú niektoré z vlastností (a) - (e) uvedených v predchádzajúcej poznámke?*

Úloha 6.7. *Uveďte aspoň po 3 príklady na relácie s vlastnosťami zavedenými v definícii 6.2 a v predchádzajúcej poznámke!*

Úloha 6.8. *Dokážte, že ak má relácia R a množine A niektorú z nasledujúcich vlastnostní: reflexívnosť, symetrickosť, tranzitívnosť, antisymetrickosť, asymetrickosť, ireflexívnosť, ekvivalencia; tak totom má túto vlastnosť aj opačná relácia R^{-}!*

Binárne relácie na množine môžeme skladať, zostrojovať k nim opačné relácie, resp. aplikovať na ne rozličné množinové operácie. Nie je ťažké zistiť, za akých podmienok sa zachovávajú vlastnosti binárnych relácií, ktoré sme definovali. Niekoľko úloh tohto typu vyriešime, ďalšie uvádzame ako cvičenia pre čitateľa.

Veta 6.2. *Nech je R reflexívna relácia na množine A a S ľubovoľná relácia na množine A. Potom platí $S \subseteq RS \cap SR$. Ak je aj S reflexívna relácia, tak potom je aj zložená relácia RS reflexívna a $R \cup S \subseteq RS \cap SR$.*

Dôkaz. Keďže R je reflexívna relácia na množine A, $E_A \subseteq R$ (6.2). Potom platí $S = E_A S \subseteq RS$ a $S = SE_A \subseteq SR$. To znamená, že $S \subseteq RS \cap SR$. Ak je S reflexívna relácia, tak potom $E_A \subseteq S$ a $RE_A \subseteq RS$, $E_A R \subseteq SR$. To znamená, že $R \subseteq RS \cap SR$. Keďže zároveň $S \subseteq RS \cap SR$, tak potom aj $R \cup S \subseteq RS \cap SR$. □

Úloha 6.9. *Dokážte nasledujúce tvrdenie: Nech sú R a R_i pre $i = 1, \ldots, n$ reflexívne relácie na množine A. Potom platí*

(a) $\bigcap R_i$ *je reflexívna relácia na množine A,*

(b) *pre ľubovoľnú reláciu* S *na množine* A *je relácia* $R \cup S$ *reflexívna (relácia na množine* A*).*

Keďže pracujeme výlučne s binárnymi reláciami na tej istej množine (napríklad množine A), operácia skladania relácií je definovaná pre ľubovoľnú množinu binárnych relácií (na množine A). Pomocou skladania binárnych relácií môžeme zaviesť operáciu umocňovania binárnej relácie na celočíselný exponent takto:

$$\begin{aligned} R^0 &= E_A, \\ R^i &= RR^{i-1}, \quad \text{pre} \quad i > 0, \\ R^i &= (R^{-i})^-, \quad \text{pre} \quad i < 0. \end{aligned}$$

Ak $(x, y) \in R^k$ pre nejaké $k > 0$, tak potom musí existovať postupnosť prvkov $x = x_0, x_1 \ldots, x_k = y$ množiny A taká, že

$$(x_0, x_1) \in R, (x_1, x_2) \in R, \ldots, (x_{k-1}, x_k) \in R.$$

Veta 6.3. *Nech sú* R, S *a* R_i, $i = 1, \ldots, n$ *symetrické relácie na množine* A*. Potom platia nasledujúce tvrdenia:*

(a) *relácie* $\bigcup R_i$ *a* $\bigcap R_i$ *sú symetrické*

(b) *relácia* RS *je symetrická práve vtedy, ak* $RS = SR$*,*

(c) *relácia* R^n *je symetrická pre každé* $n \in Z$*.*

Dôkaz. Dokážeme napríklad tvrdenie (b). Ak sú R, S symetrické relácie (na množine A), tak $R = R^-$ a $S = S^-$. Relácia RS je symetrická práve vtedy, ak $RS = (RS)^-$. Ale $(RS)^- = S^-R^- = SR$. To znamená, že $RS = SR$. Opačne, nech $RS = SR$, dokážeme, že relácia RS je symetrická:

$$(RS)^- = (SR)^- = R^-S^- = RS.$$

□

Úloha 6.10. **(a)** *Dokážte zostávajúce tvrdenia predchádzajúcej vety!*

(b) *Nájdite také symetrické relácie* R, S *na množine* A*, že zložená relácie* RS *nie je symetrická relácia!*

Úloha 6.11. *Nech sú* R, S *antisymetrické relácie na množine* A*. Dokážte, že aj*

(a) $R \cap S$ *je antisymetrická relácia na množine* A*,*

(b) $R \cup S$ *je antisymetrická relácia práve vtedy, ak* $R \cap S^- \subseteq E_A$*.*

(c) *Nájdite také antisymetrické relácie* R, S*, ktorých zjednotenie nie je antisymetrická relácia!*

Uvedieme ešte niektoré vlastnosti tranzitívnych relácií:

Veta 6.4. *Nech sú* R, S *tranzitívne relácie na množine* A*. Potom platia nasledujúce tvrdenia*

(a) $R \cap S$ *je tranzitívna relácia na množine* A*,*

(b) $R \cup S$ *je tranzitívna relácia na množine* A *práve vtedy, ak* $(RS \cup SR) \subseteq (R \cup S)$*,*

(c) *ak* $RS = SR$*, tak* RS *je tranzitívna relácia,*

(d) $R^n \subseteq R$ *pre každé prirodzené* n*.*

Dôkaz. (b) Nech je $R \cup S$ tranzitívna relácia, potom $(R \cup S)^2 \subseteq (R \cup S)$. Upravíme zloženú reláciu

$$(R \cup S)^2 = (R \cup S)(R \cup S) = R^2 \cup RS \cup SR \cup S^2.$$

Potom

$$(RS \cup SR) \subseteq (RS \cup SR) \cup (R^2 \cup S^2) = (R \cup S)^2 \subseteq (R \cup S).$$

Opačne, nech $(RS \cup SR) \subseteq (R \cup S)$, ukážeme, že $(R \cup S)^2 \subseteq (R \cup S)$, t.j. že $(R \cup S)$ je tranzitívna relácia. Platí

$$(R \cup S)^2 = R^2 \cup RS \cup SR \cup S^2.$$

Keďže obe relácie R, S sú tranzitívne, platí $R^2 \subseteq R$, $S^2 \subseteq S$, a teda $R^2 \cup S^2 \subseteq R \cup S$. Podľa predpokladu $RS \cup SR \subseteq R \cup S$, a teda

$$(R \cup S)^2 = (R^2 \cup S^2) \cup (RS \cup SR) \subseteq (R \cup S).$$

(c) Nech $RS = SR$, dokážeme, že $(RS)^2 \subseteq RS$.

$$(RS)^2 = (RS)(RS) = R(SR)S = R(RS)S = (RR)(SS) = R^2S^2 \subseteq RS^2 \subseteq RS.$$

□

Úloha 6.12. (a) *Dokážte ostávajúce tvrdenia vety 6.4.*

(b) *Nájdite také tranzitívne relácie* R, S*, ktorých zjednotenie, resp. zloženie nie je tranzitívna relácia.*

Definícia 6.3. *Nech je* R *tranzitívna relácia na množine* A*. Tranzitívnym, resp. reflexívno-tranzitívnym uzáverom relácie* R *nazývame reláciu* R^+*, resp.* R^**, definovanú nasledujúcimi vzťahmi:*

$$R^+ = R^1 \cup R^2 \cup \cdots = \bigcup_{k \geq 1} R^k; \qquad R^* = E_A \cup R^1 \cup R^2 \cup \cdots = \bigcup_{k \geq 0} R^k.$$

Je zrejmé, že $R \subseteq R^+ \subseteq R^*$. Ak je R tranzitívna relácia, tak potom $R = R^+$, ak je R zároveň aj reflexívna relácia, tak potom $R = R^*$.

Ďalšie vlastnosti tranzitívneho a reflexívno-tranzitívneho uzáveru uvádza nasledujúca veta.

Veta 6.5. *Nech* R^+, R^* *tranzitívny, resp. reflexívno-tranzitívny uzáver relácie* R *na množine* A. *Potom platia nasledujúce tvrdenia*

(a) *Relácia* R^+ *je tranzitívna relácia.*

(b) *Ak* S *je tranzitívna relácia na množine* A, *že* $R \subseteq S$, *tak potom aj* $R^+ \subseteq S$.

(c) *Relácia* R^* *je reflexívna a tranzitívna relácia.*

(d) *Ak* S *je reflexívna a tranzitívna relácia na množine* A, *taká že* $R \subseteq S$, *tak potom aj* $R^* \subseteq S$.

Dôkaz. (a) Ukážeme, že $(R^+)^2 \subseteq R^+$.

$$(R^+)^2 = (R^1 \cup R^2 \cup R^3 \cup \dots)(R^1 \cup R^2 \cup R^3 \cup \dots) = R^2 \cup R^3 \cup R^4 \cup \dots \subseteq R^+.$$

(b) Keďže R je tranzitívna relácia, podľa vety 6.4 $R^n \subseteq R$ pre $n = 1, 2, \dots$. To znamená, že $R^+ \subseteq R$. Z poslednej inklúzie, predpokladu vety a tranzitívnosti inklúzie vyplýva tvrdenie vety: $R^+ \subseteq R \subseteq S$, t.j. $R^+ \subseteq S$. Tvrdenia (c) a (d) sa dokazujú analogicky. □

Úloha 6.13. **(a)** *Dokážte tvrdenia (c) a (d) vety 6.5.*

(b) *Dokážte, že ak* $R \subseteq S$, *tak* $R^+ \subseteq S^+$ *a* $R^* \subseteq S^*$.

(c) *Preskúmajte postupnosť relácií* $\{R^n\}_{n\geq 0}$*! Môžu byť mocniny* R^n *rôzne?*

(d) *Vyberte si vhodnú binárnu reláciu* R *a zostrojte jej tranzitívny a reflexívno-tranzitívny uzáver!*

Z vety 6.5 vyplýva, že uzáver binárnej relácie je najmenšia tranzitívna (reflexívna a tranzitívna) relácia, ktorá obsahuje danú reláciu. S reflexívno-tranzitívnym a tranzitívnym uzáverom relácie sa budeme stretávať v teórii formálnych jazykov a automatov, matematickej logike a iných oblastiach matematiky a informatiky.

Úloha 6.14. *Zistite, či sú nasledujúce relácie na množine prirodzených čísel*[2] *reflexívne, symetrické, alebo tranzitívne:*

(a) $(x, y) \in R \equiv x + y$ *je párne číslo,*

(b) $(x, y) \in R \equiv x - y$ *je párne číslo,*

(c) $(x, y) \in R \equiv x + y$ *je nepárne číslo,*

(d) $(x, y) \in R \equiv x + y \leq 100$,

(e) $(x, y) \in R \equiv |x - y| \leq 1$,

(f) $(x, y) \in R \equiv x = l \cdot y; k \in N$

(g) $(x, y) \in R \equiv x = 2^y$,

[2] nenechajte sa pomýliť označením, symbol R označuje reláciu a nie množinu reálnych čísel.

(h) $(x, y) \in R \equiv 3|(x^2 + y^2)$.

Aj relácie, ktoré nie sú symetrické, možno doplniť tak, aby výsledná relácia bola symetrická.

Definícia 6.4. *Nech je* R *binárna relácia na množine* A. *Relácia* $\tilde{R} = R \cup R^{-}$ *sa nazýva* symetrizáciou relácie R.

Veta 6.6. *Nech je* R *binárna relácia na množine* A. *Potom*

(a) *symetrizácia* $\tilde{R}$ *je najmenšia symetrická relácia na množine* A, *ktorá obsahuje* R.

(b) *Binárna relácia* R *je symetrická práve vtedy, ak* $R = \tilde{R}$.

Dôkaz. Prenechávame čitateľovi ako cvičenie. □

6.2 Relácia ekvivalencie a rozklad množiny

V matematike často potrebujeme skúmať nekonečné množiny rozličných objektov. Popísať prvky čo i len veľkej množiny jednotlivo môže byť nezvládnuteľné; pre nekonečné množiny sa to jednoducho nedá spraviť. Napriek tomu, že prvky (veľkej/nekonečnej) množiny sú rôzne, môžu mať nejakú spoločnú vlastnosť, ktorá nám umožňuje rozdeliť prvky množiny do skupín podľa tejto vlastnosti a namiesto skúmania jednotlivých prvkov, skúmať potom vlastnosti reprezentanov jednotlivých skupín. Pri rozdeľovaní objektov do skupín využívame reláciu ekvivalencie; do jednej skupiny zaraďujeme objekty, ktoré sú z hľadiska nejakej vlastnosti ekvivalentné (rovnocenné, nerozlíšiteľné). Pripomíname, že ekvivalencia je relácia, ktorá je reflexívna, symetrická a tranzitívna. Upresníme to, čo sme zatiaľ vyjadrili neformálne.

Definícia 6.5. *Nech je* A *ľubovoľná neprázdna množina. Rozkladom množiny* A *sa nazýva systém* $\mathcal{S} \subseteq \mathcal{P}(A)$ *podmnožín, ktorý spĺňa nasledujúce podmienky*

1. $\forall i[(B_i \in \mathcal{S}) \rightarrow (B_i \neq \emptyset)]$,
2. $\forall i \forall j[(B_i \in \mathcal{S}) \& (B_j \in \mathcal{S}) \& (i \neq j)] \rightarrow [B_i \cap B_j = \emptyset]$,
3. $\bigcup_{B_i \in \mathcal{S}} B_i = A$.

Rozklad množiny A je teda taký systém neprázdnych podmnožín, že každý prvok $x \in A$ patrí práve do jednej množiny tohto systému. Podmnožiny tvoriace rozklad množiny sa nazývajú *triedy rozkladu.*

Príklad 6.4. $A = \{0, 1, 2, 3\}$. *Nasledujúce tri systémy podmnožín tvoria rozklad množiny* A*:*

(a) $\mathcal{S}_1 = \{0, 1, 2, 3\}$,

(b) $\mathcal{S}_2 = \{\{0\}, \{1,2\}, \{3\}\}$,

(c) $\mathcal{S}_3 = \{\{0\}, \{1\}, \{2\}, \{3\}\}$.

Súvislosť medzi reláciou ekvivalencie a rozkladom príslušnej množiny popisuje nasledujúca veta.

Veta 6.7. *Nech je* R *relácia ekvivalencia na množine* $A \neq \emptyset$. *Nech pre ľubovoľné* $x \in A$, $R[x] = \{y; (x,y) \in R\}$. *Potom systém množín* $\mathcal{S} = \{R[x] \in \mathcal{P}(A); x \in A\}$ *je rozkladom množiny* A.

Dôkaz. Ukážeme, že $\mathcal{S}$ má všetky tri vlastnosti rozkladu.

1. Keďže $x \in R[x]$, $R[x] \neq \emptyset$ pre ľubovoľné $x \in A$.
2. Nech sú $R[x], R[y]$ ľubovoľné množiny zo systému $\mathcal{S}$, $x \neq y$. Ukážeme, že buď $R[x] = R[y]$ alebo $R[x] \cap R[y] = \emptyset$. Nech $z \in R[x] \cap R[y]$. Potom podľa definície triedy $R[x]$ platí $(x,z) \in R$ a $(y,z) \in R$. Zo symetrickosti a tranzitívnosti R vyplýva, že aj $(x,y) \in R$; to znamená, že $y \in R[x]$. Nech $v \in R[y]$, potom $(y,v) \in R$ a zo symetrickosti a tranzitívnosti R vyplýva, že $(x,v) \in R$; t.j. $v \in R[x]$. To znamená, že $R[y] \subseteq R[x]$. Podobným spôsobom možno dokázať opačnú inklúziu, a teda aj rovnosť $R[y] = R[x]$. Množiny $R[x], R[y]$, $x, y \in A$ sú teda buď disjunktné, alebo sa rovnajú.
3. Keďže každý prvok $x \in A$ patrí do množiny $R[x]$, $\bigcup_{x \in A} R[x] = A$.

□

Poznámka. Rozklad definovaný vo vete 6.7 sa nazýva *rozklad indukovaný ekvivalenciou*, alebo *prislúchajúci k ekvivalencii* R.

Úloha 6.15. *Popíšte triedy rozkladov indukovaných nasledujúcimi reláciami ekvivalencie*

(a) $R_1 \subseteq Z \times Z$; $(x,y) \in R_1 \equiv 2|(x-y)$,

(b) R_2 *je relácia definovaná na množine ľudí;* $(x,y) \in R_2 \equiv x, y$ *sa narodili v tom istom roku.*

Ukázali sme, že relácia ekvivalencie indukuje na príslušnej množine rozklad. Platí aj opačný vzťah—rozklad množiny definuje ekvivalenciu.

Veta 6.8. *Nech je* A *neprázdna množina a* $\mathcal{S} = \{B_1, \dots\}$ *je jej rozklad. Potom je binárna relácia na množine* A *definovaná vzťahom*

$$R = \{(x,y) \in A \times A; \exists B_i[(B_i \in \mathcal{S}) \& (x \in B_i) \& (y \in B_i)]\}$$

je reláciou ekvivalencie na množine A *a* $\mathcal{S}$ *je ňou indukovaný rozklad.*

Dôkaz. Vzťah vo vete 6.8 definuje množinu usporiadaných dvojíc (v krajnom prípade prázdnu), teda R je binárna relácia na množine A. Ukážeme, že R je ekvivalencia.

Reflexívnosť. Ak $x \in A$, potom musí existovať trieda rozkladu $B_i \in \mathcal{S}$ tak, že $x \in B_i$; v opačnom prípade by totiž $x \notin \bigcup_i B_i = A$. Ak však $x \in B_i$, tak potom podľa definície relácie R $\forall x[(x \in A) \rightarrow (x, x) \in R]$.

Symetrickosť. Z toho, že $(x, y) \in R$ vyplýva, že existuje také $B_i \in \mathcal{S}$, že $x, y \in B_i$. To znamená, že aj $(y, x) \in R$.

Tranzitívnosť. Ak $(x, y) \in R$, $(y, z) \in R$, tak potom podľa definície relácie R existujú triedy rozkladu B_i, B_j také, že $x, y, \in B_i, y, z \in B_j$. To znamená, že $y \in B_i \cap B_j$. Keďže $\mathcal{S}$ je rozklad, $B_i = B_j$ a teda $x, z \in B_i$, resp. $(x, z) \in R$.

Dokážeme druhú časť tvrdenia. Nech $\mathcal{S}_0$ označuje rozklad množiny A indukovaný ekvivalenciou R. Dokážeme, že $\mathcal{S}_0 = \mathcal{S}$. Najprv ukážeme, že $\mathcal{S}_0 \subseteq \mathcal{S}$. Nech $R[x] \in \mathcal{S}_0$. Keďže $\mathcal{S}$ je rozklad množiny A, existuje trieda rozkladu $B_i \in \mathcal{S}$ taká, že $x \in B_i$. Nech $y \in B_i$ (ak je trieda B_i jednoprvková, tak $y = x$), potom $(x, y) \in R$ a súčasne $y \in R[x]$. To znamená, že $B_i \subseteq R[x]$. Nech $z \in R[x]$ Potom prvky x, z musia patriť do jednej triedy rozkladu systému $\mathcal{S}$. Keďže $\mathcal{S}$ je rozklad a prvok x patrí do triedy B_i, potom aj prvok z patrí do triedy B_i. Ale potom $R[x] \subseteq B_i$, a teda $B_i = R[x]$.

Dokázali sme, že rozklad $\mathcal{S}_0$ je podmnožinou rozkladu $\mathcal{S}$. Ukážeme, že platí aj opačná inklúzia; $\mathcal{S} \subseteq \mathcal{S}_0$. Predpokladajme opak, t.j. že $\mathcal{S}$ obsahuje triedu rozkladu B, ktorá nepatrí do $\mathcal{S}_0$. Trieda B je podľa definície rozkladu neprázdna, a teda musí obsahovať aspoň jeden prvok, označme ho w. Potom však existuje $x \in A$ také, že $w \in R[x]$, pretože v opačnom prípade $w \notin \bigcup_{x \in A} R[x] = A$). Ale potom $B = R[x]$ a $B \in \mathcal{S}$. Spor. □

Úloha 6.16. *1. Nech $A = \{0, 1, 2\}$. Zostrojte všetky rozklady množiny A a nájdite k nim prislúchajúce relácie ekvivalencie!*
2. Pripusťme, že $A = \emptyset$. Ako by vyzeral rozklad množiny A a k nemu prislúchajúca relácia ekvivalencie?

Úloha 6.17. *Nech $A \neq \emptyset$. Je niektorá z relácií $\emptyset, A \times A$ reláciou ekvivalencie na množine A?*

Úloha 6.18. *Nech $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ označujú množiny celých, racionálnych a reálnych čísel. Relácie T a U definujeme nasledujúcim spôsobom:*

$$T = \{(x, y) \in \mathbb{R} \times \mathbb{R}; x - y \in \mathbb{Z}\}, \quad U = \{(x, y) \in \mathbb{R} \times \mathbb{R}; x - y \in \mathbb{Q}\}.$$

Dokážte, že relácie T a U sú ekvivalencie na množine $\mathbb{R}$. Opíšte rozklady množiny reálnych čísel indukované reláciami ekvivalencie T a U!

Úloha 6.19. *Nech je R relácia ekvivalencie na množine A. Je aj opačná relácia R^- reláciou ekvivalencie na množine A?*

Úloha 6.20. *Koľko je rozličných relácií ekvivalencie na štvorprvkovej množine?*

Veta 6.9. *Nech sú R a S relácie ekvivalencie na množine A, potom platia nasledujúce tvrdenia*

(a) *relácia* $R \cap S$ *je ekvivalencia,*

(b) *zložená relácia* RS *je ekvivalenciou práve vtedy, ak* $RS = SR$*,*

(c) *reácia* $R \cup S$ *je ekvivalenciou práve vtedy, ak* $R \cup S = RS$.

Dôkaz. Ponechávame čitateľovi ako cvičenie. □

Úloha 6.21. *Nájdite príklady relácií ekvivalencie* R, S *na množine* A *takých, že relácie* RS*, resp.* $R \cup S$ *nie sú ekvivalencie na množine* A*!*

6.3 Usporiadania

Ďalšou veľmi často používanou reláciou na množine je *relácia usporiadania*. Relácia usporiadania umožňuje prvky množiny nejakým spôsobom porovnávať, alebo usporadúvať. Pre číselné množiny $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sú usporiadania založené na veľkosti čísel dobre známe. Často však potrebujeme zaviesť usporiadanie aj v množinách, ktorých prvkom nevieme priradiť veľkosť. Aby sme mohli zaviesť usporiadanie aj v množinách, kde neexistuje prirodzené usporiadanie založené na veľkosti prvkov, preskúmame základné vlastnosti relácie usporiadania a uvedieme niekoľko užitočných relácií usporiadania.

Definícia 6.6. *Usporiadaním na množine* A *nazveme ľubovoľnú reflexívnu, antisymetrickú a tranzitívnu reláciu na množine* A.

Na označenie usporiadania sa často používa symbol $\leq$. Množina A spolu s usporiadaním $\leq$ tvorí tzv. *usporiadanú množinu*, ktorú označujeme $(A, \leq)$. Množina A sa nazýva nosičom usporiadanej množiny $(A, \leq)$. Opačnú reláciu k usporiadaniu $\leq$ označujeme symbolom $\geq$.

Úloha 6.22. *Nech je* $\leq$ *usporiadanie na množine* A*. Dokážte (alebo vyvráťte), že aj relácie* $(\leq)^{-}, =, \geq$ *sú usporiada na množine* A.

Ak platí $a \leq b$ alebo $b \leq a$, tak prvky a, b nazývame *porovnateľnými prvkami* v množine $(A, \leq)$. Ak sú ľubovoľné dva prvky usporiadanej množiny porovnateľné, nazývame ju *úplne usporiadanou množinou* (takéto usporiadanie sa nazýva aj *totálne* alebo *lineárne usporiadanie množiny*).

Príklad 6.5. *Zistite, či sú nasledujúce množiny usporiadané; t.j. či dané relácie sú reláciami usporiadania:*

(a) *Množina prirodzených čísel s reláciou* $\leq$*,*

(b) $\mathcal{P}(A)$ *s reláciou* $\subseteq$.

Príklad 6.6. *Zistite, či sú množiny* $(\mathbb{N}, \leq)$ *a* $(\mathcal{P}(A), \subseteq)$ *z predchádzajúceho príkladu úplne usporiadané.*

Príklad 6.7. *Nech sú* R, S *usporiadania na množine* A*. Zistite, či sú nasledujúce relácie usporiadaniami na množine* A*:*

(a) $R \cup S$,

(b) $R \cap S$,

(c) RS.

Vzťah $a \leq b, a \neq b$, zapisujeme stručne $a < b$ a reláciu $<$ nazývame *ostrým usporiadaním zodpovedajúcim usporiadaniu* $\leq$. (Relácia $a < b$ sa zvykne nazývať ostrým usporiadaním, aj keď nie je usporiadaním v zmysle definíce.) Ostré usporiadanie je tranzitívna a ireflexívna relácia. Úplné ostré usporiadanie na množine A spĺňa naviac podmienku

$$(x = y) \vee (x < y) \vee (y < x),$$

pre všetky prvky $x, y \in A$. Ľubovoľné ostré usporiadanie $<$ možno rozšíriť na príslušné („neostré“) usporiadanie tak, že sa relácia $<$ zjednotí s identickou reláciou E_A na množine A.

Príklad 6.8. *1. Nech* $A \neq \emptyset$*, potenčná množina* $\mathcal{P}(A)$ *s reláciou množinovej inklúzie* $\subseteq$ *tvorí usporiadanú množinu (ktorá však nie je úplne usporiadaná). Ostrá množinová inklúzia* $\subset$ *zodpovedá neúplnému ostrému usporiadaniu na množine* $\mathcal{P}(A)$*.*
2. Nech je usporiadanie $|$ *množiny* $\mathbb{N}$ *definované takto* $(a, b) \in |$ *práve vtedy, ak* a *delí* b*; t.j. ak existuje prirodzené číslo* k *také, že* $a \cdot k = b$*. Je zrejmé, že* $(\mathbb{N}, |)$ *nie je úplne usporiadaná množina.*

Aby sme uľahčili štúdium vlastností usporiadaní a usporiadaných množín, zobrazíme vzťahy medzi jednotlivými prvkami graficky tak, ako sme zobrazovali relácie a funkcie; usporiadanej množine (A, R) priradíme graf, v ktorom prvkom z A zodpovedajú vrcholy grafu a usporiadaným dvojiciam $(a, b) \in R$ zodpovedajú orientované hrany spájajúce príslušné vrcholy grafu.

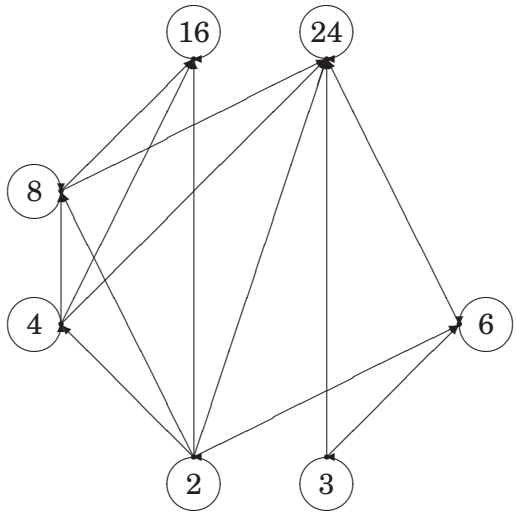
Príklad 6.9. *Uvažujme množinu prirodzených čísel* $M = \{2, 3, 4, 6, 8, 16, 24\}$ *s reláciou* $| = \{(x, y) \in M^2; x|y\}$*. Graf usporiadanej množiny* $(M, |)$ *je uvedný na obrázku 6.1.*

Graf na obrázku 6.1 je však značne (a pritom zbytočne) neprehľadný. Možno ho zjednodušiť bez toho, aby sa stratila informácia o usporiadaní množiny M.

Definícia 6.7. *Nech je* R *binárna relácia na množine* A. Redukciou relácie R *nazveme binárnu reláciu* R_r *definovanú vzťahom*

$$R_r = R - R^2.$$

Ak je R *ostrým usporiadaním na množine* A*, tak potom redukciu* R_r *nazývame tiež* reláciou pokrytia*, alebo* reláciou bezprostredného predchádzania príslušného usporiadania R.



Obrázok 6.1: Graf relácie |

Redukciou sa z relácie R vylúčia všetky také usporiadané dvojice (x, y), pre ktoré v množine A existuje „prechodový“ prvok z taký, že platí $(x, z) \in R$ a $((z, y) \in R$. Zdalo by sa, že pomocou reflexívno-tranzitívneho uzáveru relácie R_r sa nám podarí zrekonštruovať pôvodnú reláciu R. Nie je tomu vždy tak. Pozri [12].

Úloha 6.23. *Nech je R reflexívna relácia na množine A. Ukážte, že $R_r^+ = \emptyset$ a $R_r^* = E_A$.*

Úloha 6.24. *Uvažujme množinu racionálnych čísel $\mathbb{Q}$ s reláciou $<$. Ukážte, že redukcia relácie $<$ je prázdna.*

Pre konečné množiny však platí nasledujúca veta.

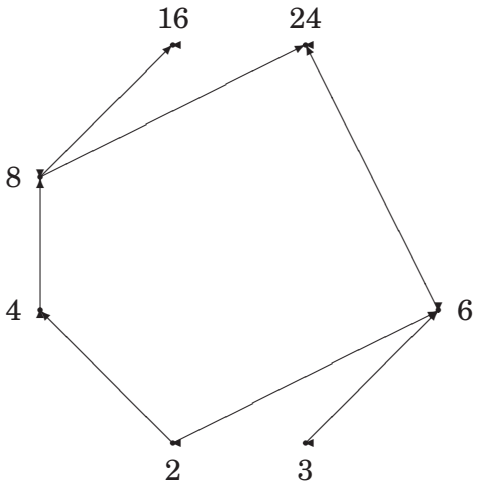
Veta 6.10. *Nech je (A, R) konečná usporiadaná množina a relácia $S = R - E_A$ je ostré usporiadanie zodpovedajúce usporiadaniu R. Nech je $S_r = S - S^2$ redukcia relácie S. Potom platia nasledujúce tvrdenia*

(a) $S_r^+ = S$ *(tranzitívny uzáver relácie S_r sa rovná S),*

(b) $S_r^* = R$ *(reflexívno-tranzitívny uzáver relácie S_r sa rovná pôvodnej relácii usporiadania R.)*

Dôkaz Vetu nebudeme dokazovať, čitateľ sa o to môže pokúsiť sám, alebo si pozrieť dôkaz v [12]. □

Upravíme teraz na základe vety 6.10 reláciu | z predchádzajúceho príkladu a zostrojíme pre ňu nový graf (pozri obrázok 6.2). Takto zostrojený graf pokrytia nazývame *Hasseho diagramom* (alebo *diagramom pokrytia*) danej množiny. Na základe Hasseho diagramu usporiadanej množiny (A, R) možno ľahko zistiť, čo platí pre ľubovoľné prvky $a, b \in A$: ak v Hasseho diagrame existuje orientovaná cesta (postupnosť na seba naväzujúcich orientovaných hrán) začínajúca vo vrchole a a končiaca vo vrchole b, tak potom



Obrázok 6.2: Hasseho diagram množiny M

$(a, b) \in R$; analogicky by sme riešili prípad $(b, a) \in R$. Ak vrcholy a, b nie sú v Hasseho diagrame spojené orientovanou cestou, tak potom sú prvky a, b v množine (A, R) neporovnateľné.

Príklad 6.10. *Uvažujme potenčnú množinu množiny $A = \{1, 2, 3\}$ s reláciou usporiadania definovanou množinovou inklúziou $\subseteq$. Hasseho diagram pre množinu $\mathcal{P}(A)$ je uvedený na obrázku 6.3.*

Hasseho diagram možno ešte zjednodušiť tým, že sa vrcholy grafu rozmiestnia tak, aby boli hrany orientované zdola nahor. Potom možno v grafe namiesto orientovaných hrán (šípiek) kresliť len neorientované hrany (úsečky).

Na Hasseho diagrame na obrázku 6.3 je možné vidieť, že množiny $\{1, 2\}$ a $\{3\}$ nie sú porovnateľné. (Aby sme sa dostali z vrcholu $\{1, 2\}$ do vrcholu $\{3\}$, musíme ísť najprv v smere orientovanej hrany do vrcholu $\{1, 2, 3\}$, ale potom by sme museli pokračovať proti smeru orientácie hrán postupne do vrcholu $\{1, 3\}$ alebo $\{2, 3\}$ a odtiaľ opäť v „protismere“ do vrcholu $\{3\}$.) Neporovnateľných množín je viac, podobne by sme mohli ukázať, že sú neporovnateľné napríklad množiny $\{1\}$ a $\{2\}$. Teraz keď vieme graficky zobraziť usporiadanú množinu (A, R), nebude problém pochopiť podstatu ďalších dôležitých pojmov, ktoré súvisia s usporiadaním.

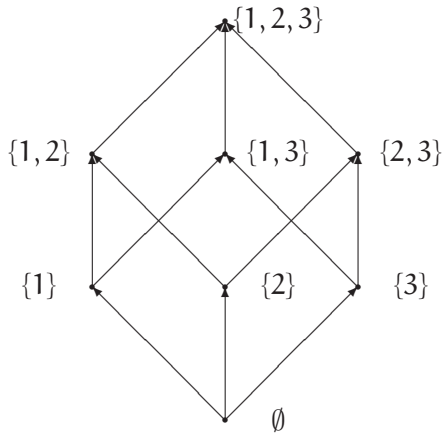
Definícia 6.8. *Nech je $(A, \leq)$ usporiadaná množina a nech je relácia $<$ ostré usporiadanie zodpovedajúce usporiadaniu $\leq$. Potom prvok $a \in A$ nazývame*

(a) *minimálnym prvkom množiny A, ak*

$$\neg\exists x[(x \in A)\&(x < a)]$$

(b) *najmenším prvkom množiny A, ak*

$$\forall x[(x \in A) \rightarrow (x > a)]$$



Obrázok 6.3: Hasseho diagram množiny M

(c) *maximálnym prvkom množiny* A*, ak*

$$\neg\exists x[(x \in A)\&(x > a)]$$

(d) *najväčším prvkom množiny* A*, ak*

$$\forall x[(x \in A) \rightarrow (x < a)].$$

Jednoducho povedané, v množine A neexistuje menší prvok, ako je minimálny prvok, väčší prvok, ako je maximálny prvok a všetky prvky množiny A (okrem najmenšieho) sú väčšie ako najmenší prvok; všetky prvky množiny A (okrem najväčšieho) sú menšie ako najväčší prvok. To okrem iného znamená, že množina $(A, \leq)$ môže mať niekoľko maximálnych, niekoľko minimálnych, ale len jeden najväčší a jeden najmenší prvok.

Úloha 6.25. *(a) Nájdite maximálne, minimálne, najväčšie a najmenšie prvky v nasledujúcich Hasseho diagramoch.*

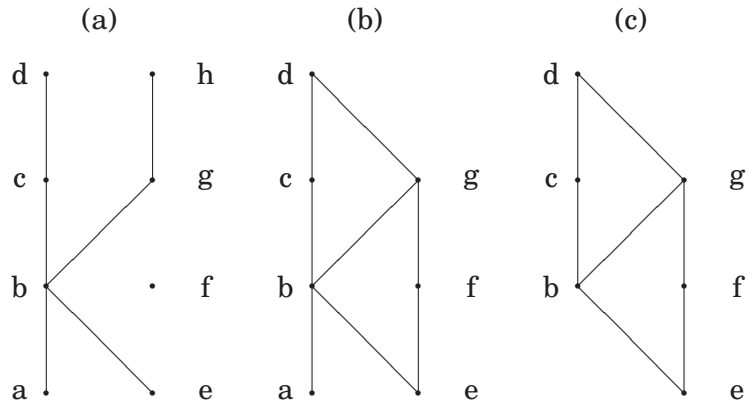
(b) Nájdite usporiadanú množinu, ktorá bude mať n *maximálnych a* m *minimálnych prvkov!*

Príklad 6.11. *Uvedieme niekoľko príkladov usporiadaných (čiastočne usporiadaných) množín.*

1. *Množina reálnych čísel* $\langle 0, 1\rangle$ *má najväčší (zároveň maximálny) prvok* 1 *a najmenší prvok* 0*, ktorý je zároveň minimálnym prvkom tejto množiny.*

2. *Množina reálnych čísel* $(0, 1)$ *nemá ani minimálny, ani maximálny prvok.*

3. *Množina racionálnych čísel z intervalu* $\langle 0, \sqrt{2}\rangle$*má najmenší (minimálny) prvok* 0 *a nemá maximálny prvok, lebo* $\sqrt{2}$ *nie je racionálne číslo.*



Obrázok 6.4: Hasseho diagram množiny M

4. *Nech je daná množina* E^n *všetkých binárnych* n*-tíc a nech* $\alpha = (a_1, \ldots, a_n); \beta = (b_1, \ldots, b_n)$ *sú ľubovoľné dve* n*-tice z množiny* E^n*. Potom usporiadanie na množine* E^n *definujeme nasledovne:*

$$\alpha \preceq \beta \equiv a_i \leq b_i;\ i = 1, \ldots, n.$$

   (a) *Množina* E^n *má najväčší prvok (jednotkový vektor) a najmenší prvok (nulový vektor).*

   (b) *Množina* $E^n - \{(0, \ldots, 0)\}$ *má najväčší prvok (jednotkový vektor), nemá najmenší prvok, ale má* n *minimálnych prvkov (všetky vektory, ktoré majú práve jednu zložku jednotkovú a všetky ostatné nulové.)*

5. *Množina* $\mathbb{N}$ *prirodzených čísel má najmenší prvok* 0 *ale nemá maximálny prvok.*

6. *Množina* $\mathbb{Z}^-$ *záporných celých čísel má najväčší prvok* -1*, ale nemá minimálny prvok.*

7. *Množina* $\mathbb{Z} \cup \{+\infty, -\infty\}$ *s prirodzeným usporiadaním čísel má najväčší aj najmenší prvok.*

Pri dôkazoch niekedy potrebujeme v množine nájsť najmenší prvok s danou vlastnosťou. Je výhodné, ak je daná množina *dobre usporiadaná*; t.j. ak každá jej podmnožina má najmenší prvok.[3]

Úloha 6.26. *(a) Zistite, ktoré z množín* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *sú dobre usporiadané pomocou „prirodzeného“ usporiadania* $\leq$*!*

(b) Charakterizujte prirodzené usporiadanie $\leq$ *množín* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *(úplnosť, existencia minimálnych a maximálnych prvkov a pod.)*

[3] dobrým usporiadaním sa ešte budeme zaoberať v kapitole 8

Úloha 6.27. *Nájdite všetky relácie usporiadania a dobrého usporiadania* 4*-prvkovej množiny!*

Úloha 6.28. *Nech je* R *ireflexívna relácia na množine* A*. Potom na množine* A *existuje usporiadanie* S*, ktoré obsahuje reláciu* R *práve vtedy, ak je relácia* R^+ *ireflexívna. Dokážte alebo vyvráťte!*

Úloha 6.29. *Nech je daná relácia* R *na množine* A*. Reflexívno-tranzitívny uzáver* R^* *relácie* R *je usporiadaním na množine* A *práve vtedy, ak je* $(R - E_A)^+$ *ireflexvna relácia. Dokážte!*

Úloha 6.30. *(Pokračovanie.) Dokážte, že relácia* R^* *je potom zároveň najmenšie usporiadanie na množine* A*, ktoré obsahuje reláciu* R*!*

Úloha 6.31. *Dokážte alebo vyvráťte nasledujúce tvrdenie: každá reflexívna a tranzitívna relácia je asymetrická.*

Kapitola 7

Zovšeobecnené množinové operácie

Definícia prieniku a zjednotenia dvoch množín a asociatívnosť týchto operácií nám umožňujú definovať zjednotenie a prienik ľubovoľného *konečného* počtu množín. Už v predchádzajúcich kapitolách sme sa však neraz stretli s potrebou utvoriť prienik alebo zjednotenie aj nekonečného počtu množín, alebo takého počtu, ktorý sme v danej chvíli nepoznali. Z toho vyplýva nevyhnutnosť vhodným spôsobom rozšíriť definíciu prieniku a zjednotenia tak, aby sme dokázali zjednocovať, či prenikať ľubovoľné systémy množín. Predtým, než pristúpime k všeobecnej definícii, necháme sa inšpirovať fungujúcim prípadom prieniku a zjednotenia konečného počtu množín.

Ak máme prienik

$$A = A_1 \cap A_2 \cap \dots A_n,$$

tak množinu A môžeme vyjadriť aj takto:

$$A = \{a; \forall i[i \in \{1, \dots, n\} \rightarrow (a \in A_i)\}. \tag{7.1}$$

Podobne aj zjednotenie

$$B = B_1 \cup B_2 \cup \dots B_n,$$

môžeme opísať takto

$$B = \{b; \exists i[i \in \{1, \dots, n\} \& (b \in B_i)\}. \tag{7.2}$$

Aj keď to zo zápisu (7.2) na prvý pohľad nevidno, množina na pravej strane rovnosti (7.2) je tá istá ako tá, ktorú získame postupne „prizjednocovaním“ B_3 k $B_1 \cup B_2$, B_4 k $B_1 \cup B_2 \cup B_3$ atď. Podobnú vlastnosť má aj zápis (7.1) pre prienik.

Rovnosti (7.1) a (7.2) zoberieme za východisko definície zovšeobecneného prieniku a zjednotenia. Naprv však potrebujeme pojem *indexovaný systém*.

Definícia 7.1. *Nech S a I sú množiny. Zobrazenie $x : I \rightarrow S$ budeme nazývať indexovaným systémom prvkov z S a množinu I množinou indexov. Namiesto zvyčajného označenia $x(i)$ pre obraz prvku $i \in I$ v zobrazení x budeme písať x_i. zobrazenie $x : I \rightarrow S$ budeme zapisovať ako $x = (x_i)_{i \in I}$, alebo $x = (x_i; i \in I)$; ak je množina I známa, tak budeme*

písať aj $x = (x_i)$. *Pritom prvok* x_i *budeme niekedy nazývať aj* i*-tym členom indexovaného systému* x.

Poznamenávame, že množina indexov I nemusí byť vôbec podmnožinou množiny prirodzených čísel, ba ani číselnou množinou.

Pojem indexovaný systém a pojem zobrazenia sú synonymá, a teda niet medzi nimi žiadneho obsahového rozdielu. jediný rozdiel je formálny, čiže v spôsobe zápisu a vo výbere terminológie podľa toho, čo je pre nás v danom kontexte výhodnejšie.

Ak v definícii 7.1 S je množina všetkých podmnožín nejakej množiny M, teda $S = \mathcal{P}(M)$, tak indexovaný systém x nazývame *indexovaným systémom množín*. Namiesto malého písmena x v takom prípade uprednostníme na označenie indexovaného systému množín veľké písmená.

Definícia 7.2. *Nech* M *a* I *sú ľubovoľné množiny a nech* $A = (A_i)_{i\in I}$ *je indexovamý systém podmnožín množiny* M*; t.j. zobrazenie z* I *do* $\mathcal{P}(M)$. *Položme*

$$\bigcap_{i\in I} A_i = \{a; \forall i[i \in \{1,\dots,n\} \to (a \in A_i)\};$$

a

$$\bigcup_{i\in I} A_i = \{a; \exists i[i \in \{1,\dots,n\} \& (a \in A_i)\}.$$

Potom množinu $\bigcap_{i\in I} A_i$ *nazývame prienikom systému* $A = (A_i)_{i\in I}$ *a množinu* $\bigcup_{i\in I} A_i$ *nazývame zjednotením systému* $A = (A_i)_{i\in I}$. *Ak je zo súvislosti jasné, o ktorú množinu indexov ide, používame tiež jednoduchšie označenie* $\bigcap A$ *a* $\bigcup A$.

Poznámka. Z definície 7.2 vidno, že ak $I = \emptyset$, tak

$$\bigcap_{i\in\emptyset} A_i = M, \ \bigcup_{i\in\emptyset} A_i = \emptyset.$$

Vo zvyšných prípadoch $\bigcap A$ a $\bigcup A$ závisí len od množín A_i systému A a nie od ich spoločnej nadmnožiny M.

Príklad 7.1. *(1) Ak* $I = \{1, 2, \dots, n\}$*, tak*

$$\bigcap_{i\in I} A_i = A_1 \cap A_2 \cap \dots \cap A_n, \quad \bigcup_{i\in I} A_i = A_1 \cup A_2 \cup \dots \cup A_n.$$

(2) Ak $I = \{0, 1, 2, \dots\} = \mathbb{N}$, $C_i = \{i\}$ *a* $D_i = \langle 0, \frac{1}{i+1}\rangle$*, tak*

$$\bigcup_{i\in I} C_i = \mathbb{N}, \quad \bigcap_{i\in I} D_i = \{0\}.$$

O všeobecnosti ak $I = N$, tak namiesto označení $(A_i)_{i\in N}, \bigcap_{i\in N} A_i, \bigcup_{i\in N} A_i$ sa bežne používajú aj označenia $(A_i)_{i=0}^{\infty}, \bigcap_{i=0}^{\infty} A_i, \bigcup_{i=0}^{\infty} A_i$. Napr. $\bigcap_{i=0}^{\infty}(0, \frac{1}{i+1}) = \emptyset$.

Veta 7.1. *Nech* $(A_i)_{i\in I}$ *a* $(B_i)_{i\in I}$ *sú indexované systémy podmnožín množiny* M *a nech* $C, D \subseteq M$. *Potom platí:*

(a) *Ak* $A_i \subseteq B_i$ *pre všetky* $i \in I$*, tak*

$$\bigcup_{i\in I} A_i \subseteq \bigcup_{i\in I} B_i, \quad \bigcap_{i\in I} A_i \subseteq \bigcap_{i\in I} B_i.$$

(b) *Ak pre každé* $i \in I$ *je* $C \subseteq A_i \subseteq D$*, tak*

$$C \subseteq \bigcap_{i} A_i; \quad \bigcup_{i} A_i \subseteq D.$$

(c) *Ak* $J \subseteq I$*, tak*

$$\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in J} A_i, \quad \bigcup_{i\in J} A_i \subseteq \bigcup_{i\in I} A_i.$$

(d) *Pre každé* $j \in I$ *platí*

$$\bigcap_{i\in I} A_i \subseteq A_j \subseteq \bigcup_{i\in I} A_i.$$

Dôkaz. (a) Nech $x \in \bigcup_{i\in I} A_i$. Potom existuje $i \in I$ také, že $x \in A_i$. Keďže $A_i \subseteq B_i$, $x \in B_i$, a teda aj $x \in \bigcup_{i\in I} B_i$. To znamená, že $\bigcup_{i\in I} A_i \subseteq \bigcup_{i\in I} B_i$.

Nech $x \in \bigcap_{i\in I} A_i$. Potom $x \in A_i$ pre každé $i \in I$. Keďže $A_i \subseteq B_i$ pre všetky $i \in I$, máme aj $x \in B_i$ pre všetky $i \in I$. Preto aj $x \in \bigcap_{i\in I} B_i$. To znamená, že $\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in I} B_i$.

Tvrdenie (b) je dôsledkom (a), ak položíme $A_i = C$ alebo $B_i = D$ pre každé $i \in I$.

(c) Dokážeme najprv prvú inklúziu. Nech $x \in \bigcap_{i\in I} A_i$. Potom $x \in A_i$ pre všetky $i \in I$, a keďže $J \subseteq I$, tým aj pre všetky $i \in J$. Ale potom $x \in \bigcap_{i\in J} A_i$, čiže $\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in J} A_i$.

Nech $x \in \bigcup_{i\in J} A_i$, potom existuje také $i \in J$, že $x \in A_i$. Keďže $J \subseteq I$, $x \in \bigcup_{i\in I} A_i$ a $\bigcup_{i\in J} A_i \subseteq \bigcup_{i\in I} A_i$.

Tvrdenie (d) vyplýva z (c); položíme $J = \{j\}$ a $\bigcup_{i\in\{j\}} A_i = A_j = \bigcap_{i\in\{j\}} A_i$. □

Veta 7.2. *(Zovšeobecnené de Morganove pravidlá) Nech* $(A_i)_{i\in I}$ *je indexovaný systém podmnožín množiny* M. *Potom platí:*

$$M - \bigcap_{i} A_i = \bigcup_{i} (M - A_i),$$

a

$$M - \bigcup_{i} A_i = \bigcap_{i} (M - A_i),$$

Dôkaz. Pre každé $x \in M$ platí $x \in M - \bigcap_i A_i$ práve vtedy, keď $x \in M$ a existuje $j \in I$ také, že $x \notin A_j$, t.j. práve vtedy, keď existuje $j \in I$, pre ktoré $x \in M - A_j$; inými slovami, keď $x \in \bigcup_i (M - A_i)$. Tým sme dokázali prvú rovnosť. Ak v prvej rovnosti namiesto systému $(A_i)_{i\in I}$ použijeme indexovaný systém $(M - A_i)_{i\in I}$, tak dostávame rovnosť

$$M - \bigcap (M - A_i) = \bigcup A_i,$$

z ktorej vyplýva druhá rovnosť. Možno ju však dokázať aj priamo, a to podobným spôsobom ako prvú rovnosť. □

Veta 7.3. *(Zovšeobecnený komutatívny zákon) Nech* $(A_i)_{i\in I}$ *je indexovaný systém podmnožín množiny* M *a nech* $f : I \to I$ *je ľubovoľná bijekcia (permutácia množiny* I*). Potom*

$$\bigcap_{i\in I} A_i = \bigcap_{i\in I} A_{f(i)}, \quad a \quad \bigcup_{i\in I} A_i = \bigcup_{i\in I} A_{f(i)}$$

Dôkaz. Tvrdenia vyplývajú z faktu, že $f(I) = I$ a z poznámky uvedenej za definíciou 7.2. □

Veta 7.4. *(Zovšeobecnený asociatívny zákon) Nech* $(A_i)_{i\in I}$ *je indexovaný systém podmnožín množiny* M*. Ak je* $(I_j)_{j\in J}$ *je indexovaný systém podmnožín množiny* I *taký, že* $\bigcup_{j\in J} I_j = I$*, tak*

$$\bigcap_{j\in J}\bigcap_{i\in I_j} A_i = \bigcap_{i\in I} A_i \quad a \quad \bigcup_{j\in J}\bigcup_{i\in I_j} A_i = \bigcup_{i\in I} A_i.$$

Dôkaz. Položme $D = \bigcap_{i\in I} A_i$ a $D_j = \bigcap_{i\in I_j} A_i$. Podľa tvrdenia (c) vety 7.1 máme $D \subseteq D_j$ pre každé $j \in J$, a teda $D \subseteq \bigcap_{j\in J} D_j$. Z druhej strany ku každému $i \in I$ existuje $j \in J$ tak, že $i \in I$. Preto podľa časti (d) vety 7.1 platí $A_i \supseteq D_j \supseteq \bigcap_{j\in j} D_j$. Napokon odtiaľ pomocou vety 7.1 (d) $D = \bigcap_{i\in I} A_i \supseteq \bigcap_{j\in J} D_j$, čím sme dokázali prvú rovnosť. Druhú môžeme dokázať podobne alebo získať z prvej a z vety 7.2. □

Príklad 7.2. *Nech* $I = \{1, 2, 3\}$*. Ak* $f : I \to I$ *je permutácia* $\begin{pmatrix} 123 \\ 132 \end{pmatrix}$*, tak veta 7.3 hovorí, že* $A_1 \cup A_2 \cup A_3 = A_1 \cup A_3 \cup A_2$*. Ak* $J = \{1, 2\}, I_1 = \{1, 2\}$ *a* $I_2 = \{3\}$*, tak veta 7.4 hovorí, že* $(A_1 \cup A_2) \cup A_3 = A_1 \cup A_2 \cup A_3$*, a teda* $(A_1 \cup A_2) \cup A_3 = A_1 \cup (A_2 \cup A_3)$*. Toto je klasický asociatívny zákon pre zjednotenie. Tým sa vysvetľujú názvy viet 7.3 a 7.4.*

Veta 7.5. *(Zovšeobecnené distributívne zákony) Nech* $(A_i)_{i\in I}$ *a* $(B_k)_{k\in IK}$ *sú indexované systémy podmnožín množiny* M*. Potom platia nasledujúce vzťahy*

(a)

$$\left(\bigcup_{i\in I} A_i\right) \bigcap \left(\bigcup_{k\in K} B_k\right) = \bigcup_{(i,k)\in I\times K} (A_i \cap B_k),$$

(b)

$$\left(\bigcap_{i\in I} A_i\right) \bigcup \left(\bigcap_{k\in K} B_k\right) = \bigcap_{(i,k)\in I\times K} (A_i \cup B_k).$$

Dôkaz. (a) Pre každé $(i,k) \in I \times K$ je $A_i \cap B_k \subseteq (\bigcup A_i) \cap \left(\bigcap_{k\in K} B_k\right)$, a teda $\bigcup_{(i,k)\in I\times K}(A_i \cap B_k) \subseteq (\bigcup A_i) \cap \left(\bigcap_{k\in K} B_k\right)$. Obrátene, ak $x \in (\bigcup A_i) \cap \left(\bigcap_{k\in K} B_k\right)$ tak existujú indexy $j \in J$ a $l \in K$ také, že $x \in A_j \cap B_l$, a teda $x \in \bigcup_{(i,k)}(A_i \cap B_k)$.

(b) Dôkaz tejto rovnosti je podobný predchádzajúcemu dôkazu. Môžeme ju však dokázať aj pomocou vety 7.2:

$$\left(\bigcap A_i\right) \cup \left(\bigcap B_k\right) = (M - \cup(M - A_i)) \cup (M - \cup(M - B_k)) =$$

$$= M - \left(\bigcup(M - A_i) \cap \bigcup(M - B_k)\right) = M - \bigcup (M - (A_i \cup B_k)) = \bigcap(A_i \cup B_k).$$

□

Vo zvyšnej časti kapitoly zovšeobecníme pojem karteziánskeho súčinu dvoch množín na súčin ľubovoľného indexovaného systému množín. Prv než tak učiníme, pripomenieme, že karteziánsky súčin množín nie je asociatívny. Preto na rozdiel od prieniku a zjednotenia konečného počtu množín neexistuje prirodzená, t.j. „jediná správna“ definícia karteziánskeho súčinu n množín pre $n > 3$. Tak napríklad za karteziánsky súčin $n = 3$ množín môžeme rovnocenne zobrať $A_1 \times (A_2 \times A_3)$ aj $(A_1 \times A_2) \times A_3$ (pritom $A_1 \times (A_2 \times A_3) \neq (A_1 \times A_2) \times A_3$) a pri väčších n je možností stále viac. Kvôli určitosti sa preto za usporiadanú n-ticu $(x_1, x_2, \ldots, x_n)$ volí prvok $(\ldots((x_1, x_2), x_3)\ldots), x_{n-1}), x_n)$, pričom $(a,b) = \{\{a\},\{a,b\}\}$ e usporiadaná dvojica, ako sme ju definovali vo štvrtej kapitole. Podľa tejto dohody teda za karteziálnsky súčin $A_1 \times A_2 \times \cdots \times A_n$ n množín $A_1, \ldots, A_n$ berieme karteziálnsky súčin $(\ldots((A_1 \times A_2) \times A_3)\ldots) \times A_{n-1}) \times A_n)$, získaný postupným „prinásobovaním sprava“ A_3 k $A_1 \times A_2$, A_4 k $(A_1 \times A_2) \times A_3$, atď.

Všimnime si však, že v ľubovoľnej usporiadanej n-tici $(x_1, x_2, \ldots, x_n) \in A_1 \times A_2 \times \cdots \times A_n$ môžeme jednoznačne priradiť zobrazenie x z množiny indexov $\{1, 2, \ldots, n\}$ do množiny $A_1 \cup A_2 \cup \cdots \cup A_n$, ktoré indexu $i \in \{1, 2, \ldots, n\}$ priradí prvok $x_i \in A_i$. Obrátene, k ľubovoľnému zobrazeniu $f : \{1, 2, \ldots, n\} \to A_1 \cup A_2 \cup \cdots \cup A_n$ takému, že pre každý index $i \in \{1, 2, \ldots, n\}$ platí $f(i) \in A_i$ môžeme jednoznačne priradiť usporiadanú n-ticu $(f(1), f(2), \ldots, f(n)) \in A_1 \times A_2 \times \cdots \times A_n$. Existuje teda jedno-jednoznačná korešpondencia (bijekcia), ktorá nám dvoľuje stotožniť $A_1 \times A_2 \times \cdots \times A_n$ s množinou zobrazení $x : \{1, 2, \ldots, n\} \to A_1 \cup A_2 \cup \cdots \cup A_n$ takých, že $x(i) \in A_i$ pre každé $i \in \{1, 2, \ldots, n\}$. Tieto zobrazenia nie sú nič iné, ako indexované systémy, a preto môžeme vysloviť nasledujúcu všeobecnú definíciu.

Definícia 7.3. *Nech $(A_i)_{i\in I}$ je indexovaný systém množín. Potom súčinom indexovaného systému množín $(A_i)_{i\in I}$ budeme rozumieť množinu všetkých takých indexovaných systémov $x \in (x_i)_{i\in I}$ prvkov zo $\bigcup_{i\in I} A_i$, že pre každý index $i \in I$ platí $x_i \in A_i$. Súčin indexovaného systému $(A_i)_{i\in I}$ označujeme symbolom $\prod_{i\in I} A_i$ a ak množina indexov I je známa, tak aj symbolom $\prod_i A_i$ alebo $\prod A_i$.*

Príklad 7.3. *Ak $I = \{1, 2\}$, tak zobrazenie $f : A_1 \times A_2 \to \prod_{i\in\{1,2\}} A_i$ dané predpisom $(a_1, a_2) \to \{(1, a_1), (2, a_2)\}$ je bijekcia umožňujúca stotožniť $\prod_{i\in\{1,2\}} A_i$ s $A_1 \times A_2$.*

Nie všetky vlastnosti karteziánskeho súčinu možno „beztrestne“ preniesť na súčiny ľubovoľných indexovaných systémov. Napríklad vieme, že $A_1 \times A_2 \neq \emptyset$ práve vtedy, keď $A_1 \neq \emptyset$ a súčasne $A_2 \neq \emptyset$. Všeobecnejšie, $A_1 \times A_2 \times \cdots \times A_n \neq \emptyset$ práve vtedy, keď $A_i \neq \emptyset$ pre každé $i = 1, 2, \ldots, n$. Naproti tomu dôsledky výroku

„Ak $A_i \neq \emptyset$ pre všetky $i \in I$, tak $\prod_{i\in I} A_i \neq \emptyset$“ (AC)

ktorý vyzerá veľmi prirodzene, sú niekedy veľmi paradoxné. Výrok (AC) je známy ako *axióma výberu (Axiom of Choice)* a svojho času patril k najdiskutovanejším otázkam teórie množín. Má vážny význam pre axiomatickú výstavbu teórie množín, ktorou sa však v tomto texte nezaoberáme.

V prípade, že množiny A_i sú navzájom disjunktne, dá sa existencia zobrazenia (indexového systému) patriaceho do $\prod A_i$ chápať ako možnosť zostrojiť množinu tak, že z každej množiny A_i vyberieme po jednom prvku. Odtiaľ pochádza názov axióma výberu.

Úloha 7.1. *Dokážte časti viet 7.1- 7.5, ktoré sme uviedli bez dôkazov.*

Úloha 7.2. *Nech* $(A_i)_{i\in I}$ *a* $(B_i)_{i\in I}$ *sú ľubovoľné indexované systémy množín. Potom platí:*

(a) $A \times (\bigcup_i B_i) = \bigcup_i (A \times B_i)$,

(b) $(\bigcup_i A_i)_{i\in I} \times B = \bigcup_i (A_i \times B)$,

(c) $A \times (\bigcap_i B_i) = \bigcap_i (A \times B_i)$,

(d) $(\bigcap_i A_i)_{i\in I} \times B = \bigcap_i (A_i \times B)$,

Úloha 7.3. *Nech pre* $i \in I$ *sú* R *a* R_i *relácie z* A *do* B *a* S, S_i *relácie z* B *do* C. *Potom platí:*

(a) $(\bigcup_i R_i)^- = \left(\bigcup_i R_i^-\right)$, $\quad (\bigcap_i R_i)^- = \left(\bigcap_i R_i^-\right)$

(b) $R\,(\bigcup_i S_i) = \bigcup_i (RS_i)$, $\quad (\bigcup_i R_i)\,S = \bigcup_i (R_iS)$

(c) $R\,(\bigcap_i S_i) \subseteq \bigcap_i (RS_i)$, *pričom rovnosť platí práve vtedy, keď* R *je jednoznačná relácia.*

(d) $(\bigcup_i R_i)\,S \subseteq \bigcup_i (R_iS)$ *pričom rovnosť platí práve vtedy, keď* S^- *je jednoznačná relácia.*

Úloha 7.4. *Nech pre* $i \in I$ *sú* R *a* R_i *relácie z* A *do* B *a nech* $X, X_i \subseteq A$. *Potom platí:*

(a) $R\,[\bigcup_i X_i] = \bigcup_i R[X_i]$,

(b) $R\,[\bigcap_i X_i] \subseteq \bigcap_i R[X_i]$,*pričom rovnosť platí práve vtedy, keď* R *je jednoznačná relácia.*

(c) $(\bigcup_i R_i)\,[X] = \bigcup_i R_i[X]$,

(d) $(\bigcap_i R_i)\,[X] \subseteq \bigcap_i R_i[X]$, *pričom rovnosť platí práve vtedy, keď* X *má najviac jeden prvok.*

Úloha 7.5. *Nech* $(A_i)_{i\in I}, (B_i)_{i\in I}$ *sú indexované systémy množín. Potom platí:*

(a) $\bigcup_{i\in I}(A_i \cap B_i) \subseteq \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{i\in I} B_i\right)$

(b) $\bigcap_{i\in I}(A_i \cup B_i) \supseteq \left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{i\in I} B_i\right)$

Úloha 7.6. *Nech* $(A_i)_{i\in I}, (B_i)_{i\in I}$ *sú indexované systémy podmnožín množiny* M. *Potom platí:*

$$\left(M - \bigcup_{i\in I} A_i\right) \cup \left(\bigcap_{i\in i} B_i\right) \subseteq \bigcap_{i\in I}((M - A_i) \cup B_i).$$

Možno inklúziu nahradiť rovnosťou?

Úloha 7.7. *Nech* $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots A_n \supseteq \ldots$ *a* $B_0 \supseteq B_1 \supseteq B_2 \supseteq \ldots B_n \supseteq \ldots$. *Potom platí:*

(a) $\bigcap_{n=0}^{\infty}(A_n \cup B_n) = (\bigcap_{n=0}^{\infty} A_n) \cup (\bigcap_{n=0}^{\infty} B_n)$.

(b) $(A_1 - A_2) \cup (A_3 - A_4) \cup \cdots \cup (\bigcap_{n=0}^{\infty} A_n = A_0 - \bigcup_{n=0}^{\infty}(A_{2n} - A_{2n-1}).)$

Úloha 7.8. *Nech* $(A_i)_{i\in I}$ *je indexovaný systém množína nech* $f : I \to I$ *je surjekcia. Zistite, či platia rovnosti:*

(a) $\bigcup_{i\in I} A_i = \bigcup_{i\in I} A_{f(i)}$,

(b) $\bigcap_{i\in I} A_i = \bigcap_{i\in I} A_{f(i)}$.

(c) *Čo možno povedať o (a), (b) ak je* f *injekcia?*

Úloha 7.9. *Dokážte, že platí:*

(a) $\left(\bigcup_{i\in I} A_i\right) \times \left(\bigcup_{j\in J} B_j\right) = \bigcup_{i\in I}(\bigcup_{j\in J}(A_i \times B_j))$,

(b) $\left(\bigcap_{i\in I} A_i\right) \times \left(\bigcap_{j\in J} B_j\right) = \bigcap_{i\in I}(\bigcap_{j\in J}(A_i \times B_j))$.

Úloha 7.10. *Dokážte, že platí:*

$$\left(\prod_{i\in I} A_i\right) \cap \left(\prod_{i\in I} B_i\right) = \prod_{i\in I}(A_i \cap B_i).$$

Platí podobné tvrdenie aj pre zjednotenie namiesto prieniku?

Kapitola 8

Mohutnosti a usporiadania množín

Aktuálne nekonečno neexistuje!
Henri Poincaré

Jednou zo základných vlastností množín, je ich „veľkosť“. V prípade konečných množín sa dá veľkosť množiny vyjadriť pomocou počtu jej prvkov. K takýmto množinám patrí prázdna množina (ktorá neobsahuje žiaden prvok), množina všetkých ľudí, množina všetkých atómov v slnečnej sústave a pod. Ak by sme (aspoň teoreticky) odoberali z konečnej množiny prvok po prvku, po istom počte krokov by sme celú konečnú množinu vyčerpali. Naproti tomu existujú nekonečné množiny ako sú napríklad množina všetkých prirodzených čísel, celých čísel, racionálnych, reálnych a komplexných čísel a pod. Ak by sme postupne odoberali prvky z takejto (nekonečnej) množiny, po ľubovoľnom počte krokov by ešte stále obsahovala nakonečne veľa prvkov. Ak potrebujeme porovnať veľkosti dvoch konečných množín, stačí spočítať počty prvkov v jednotlivých množinách a potom porovnávať tieto čísla. Tento postup však nie je použiteľný v prípade nekonečných množín. Napríklad taká množina celých čísel, $\mathbb{Z}$. Keďže platí $\mathbb{N} \subset \mathbb{Z}$, dalo by sa očakávať, že veľkosť množiny $\mathbb{Z}$ bude väčšia ako veľkosť množiny $\mathbb{N}$[1]. Alebo počet bodov priamky a roviny. Keďže priamka je podmnožinou roviny, opäť by sa dalo očakávať, že bude obsahovať menší počet bodov, ako rovina. Ukazuje sa však, že tieto intuitívne predstavy, založené na skúsenostiach s konečnými množinami sa nedajú pre nekonečné množiny použiť. V tejto kapitole preto vytvoríme aparát, ktorý nám umožní porovnávať veľkosti množín aj v prípade, keď sú nekonečné. Využijeme pri tom jednoduchý princíp, ktorý sa dá uplatniť tak v prípade konečných, ako aj nekonečných množín. Na to, aby sme ukázali, že dve konečné množiny napríklad A, B majú rovnakú veľkosť (v prípade konečných množín vyjadrenú počtom prvkov), stačí, aby sme zostrojili nejakú bijekciu $f : A \to B$. Keďže bijekcia je injektívne a surjektívne zobrazenie, každému prvku množiny A musí byť priradený práve jeden prvok množiny B a opačne. Tento spôsob porovnávania veľkosti množín sa dá použiť aj pre nekonečné množiny. V

[1] ak by sme sa držali analógie z konečných množín, veľkosť $\mathbb{Z}$ by sme odhadli zhruba na dvojnásobok veľkosti $\mathbb{N}$

tejto kapitole sa budeme zaoberať najmä skúmaním nekonečných množín.

8.1 Spočítateľné množiny

Najjednoduchšou nekonečnou množinou je množina prirodzených čísel, $\mathbb{N}$. Táto bude slúžiť ako nejaký etalón (mierka) na určovanie veľkostí (v matematike sa na označenie veľkosti množiny používa pojem *mohutnosť množiny*) množín. Množinu budeme nazývať spočítateľnou množinou, ak existuje bijekcia z množiny A do množiny prirodzených čísel, $\mathbb{N}$. Ináč povedané, množina A je spočítateľná práve vtedy, ak jej prvky možno očíslovať pomocou prirodzených čísel; t.j. vytvoriť postupnosť (navzájom rôznych) prvkov množiny A:

$$a_0, a_1, a_2, \ldots$$

Nekonečná množina, ktorá nie je spočítateľná, sa nazýva *nespočítateľná*. Aj prvky konečnej množiny je možné zoradiť do postupnosti, (akurát po konečnom počte krokov sa nám prvky množiny „minú“ a postupnosť sa skončí), a preto budeme konečné a spočítateľné množiny označovať spoločným pojmom *nanajvýš spočítateľné množiny*. Uvedieme teraz niekoľko príkladov spočítateľných množín.

Príklad 8.1. **(1)** *Začneme celými číslami a nájdeme odpoveď na otázku formulovanú v úvode kapitoly. Množina celých čísel $\mathbb{Z}$ je spočítateľná. Usporiadame celé čísla do postupnosti (aby sme došiel rad na každé celé číslo, musíme nejako striedať kladné a záporné čísla), napríklad takto:*

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

Hľadaná bijekcia $f : \mathbb{Z} \to \mathbb{N}$ bude definovaná nasledujúcim vzťahom:

$$f(x) = \begin{cases} 2x - 1 & \text{ak } x > 0 \\ -2x & \text{ak } x \leq 0 \end{cases}$$

(2) *Množina všetkých párnych nezáporných čísel, $Z_2^+ = \{0, 2, 4, \ldots\}$ je spočítateľná. Hľadaná bijekcia je daná napríklad predpisom $f(2x) = x$.*

Poznámka. V niektorých prípadoch bude výhodnejšie začať číslovať prvky spočítateľnej množiny A od čísla 1 ako od čísla 0. Na dôkaz spočítateľnosti množiny A takéto číslovanie postačuje, lebo postupnosť $a_1, a_2, \ldots, a_n, \ldots$ možno ľahko transformovať na postupnosť v štandardnom tvare $a_0, a_1, a_2, \ldots, a_n, \ldots$ napríklad pomocou bijekcie $f : \mathbb{N} - \{0\} \to \mathbb{N}$; $f(n + 1) = n$ pre každé $n \in \mathbb{N}$.

Prikročíme ku skúmaniu základných vlastností spočítateľných množín. Nasledujúca veta v postate hovorí, že spočítateľné množiny sú „najmenšie“ nekonečné množiny.

Veta 8.1. *Ľubovoľná nekonečná množina M obsahuje spočítateľnú podmnožinu.*

Dôkaz. Keďže M je nekonečná množina, $M \neq \emptyset$, a teda z nej možno vybrať nejaký prvok. Označíme tento prvok symbolom a_1. Z toho, že M je nekonečná množina vyplýva, že množina $M - \{a_1\}$ je tiež nekonečná a neprázdna množina, a teda z nej možno vybrať nejaký prvok, a_2. Takto môžeme postupovať ďalej, a postupne vytvoríme množinu $A = \{a_1, a_2, \ldots, a_n, \ldots\}$; $A \subseteq M$ ktorá je spočítateľná. □

Veta 8.2. *Ľubovoľná podmnožina nanajvýš spočítateľnej množiny je nanajvýš spočítateľná množina.*

Dôkaz. Nech A je nanajvýš spočítateľná množina. To znamená, že všetky jej prvky možno očíslovať pomocou prirodzených čísel a usporiadať do postupnosti

$$a_1, a_2 \ldots, a_n, \ldots \tag{8.1}$$

Nech B je ľubovoľná podmnožina množiny A. To znamená, že prvky množiny B sa nachádzajú v postupnosti (8.1). Vytvoríme teraz postupnosť prvkov množiny B. Na prvé miesto dáme ten prvok množiny B, ktorý má spomedzi všetkých prvkov množiny B v postupnosti (8.1) najmenšie číslo; prvok a_{i_1}, na druhé miesto postupnosti umiestnime druhý z prvkov B v postupnosti (8.1), prvok a_{i_2}, atď. Môžu nastať dve možnosti: buď po konečnom počte krokov vyčerpáme celú množinu B, čo znamená, že množina B je konečná, alebo vytvoríme nekonečnú postupnosť

$$a_{i_1}, a_{i_2}, \ldots, a_{i_n}, \ldots$$

pozostávajúcu zo všetkých prvkov množiny B. Zobrazenie $f : B \to \mathbb{N} - \{0\}$ definované predpisom $f(a_{i_n}) = n$ je zrejme bijekcia, a teda B je spočítateľná množina. □

Úloha 8.1. *Dokážte, že množina prvočísel je spočítateľná!*

Na celých číslach sa ukázalo, že s nekonečnami sa bude počítať ináč ako s konečnými číslami. Celé čísla možno vyjadriť ako zjednotenie množiny kladných celých čísel a záporných celých čísel: $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^-$. Všetky tri množiny majú pritom mohutnosť množiny $\mathbb{N}$. Ponúkajú sa minimálne dve prirodzené otázky: existuje len jedno nekonečno, a to nekonečno množiny prirodzených čísel? Akým spôsobom môžeme vytvoriť nekonečnú množinu, ktorá nie je spočítateľná? Neskôr ukážeme, že existuje „nekonečne veľa“ nekonečien. Najprv preskúmame, ktoré operácie nad spočítateľnými množinami vedú k vytvoreniu spočítateľných množín. Spôsob konštrukcie nespočítateľných množín odložíme až do podkapitoly 8.2.

Veta 8.3. *Zjednotenie nanajvýš spočítateľného systému nanajvýš spočítateľných množín je nanajvýš spočítateľná množina.*

Dôkaz. Predpokladáme najprv, že množín tvoriacich systém je spočítateľne veľa, že každá z nich je spočítateľná a že sú po dvoch disjunktné. Vzhľadom na tieto predpoklady

môžeme množiny systému zapísať v podobe postupností ich prvkov:

$$\begin{aligned} A_1 &= \{a_{1,1}, a_{1,2}, a_{1,3} \ldots, a_{1,n}, \ldots\} \\ A_2 &= \{a_{2,1}, a_{2,2}, a_{2,3} \ldots, a_{2,n}, \ldots\} \\ &\vdots \\ A_m &= \{a_{m,1}, a_{m,2}, a_{m,3} \ldots, a_{m,n}, \ldots\} \\ &\vdots \end{aligned}$$

Prvky množiny $A = \bigcup_m A_m$ usporiadame do postupnosti nasledujúcim spôsobom:

$$a_{1,1}, a_{1,2}, a_{2,1}, a_{1,3}, a_{2,2}, a_{3,1}, a_{1,4}, a_{2,3}, a_{3,2}, s_{4,1}, a_{1,5} \ldots \tag{8.2}$$

Ak by systém obsahoval len konečne veľa množín, napríklad m, z postupnosti (8.2) by vypadli všetky prvky $a_{j,i}, j > m, i \in \mathbb{N}$. Ak množina A_k obsahuje len konečný počet prvkov (napríklad r), tak z postupnosti (8.2) vypadnú všetky prvky $a_{k,i}, i > r, i \in \mathbb{N}$. A napokon, ak by množiny A_i neboli disjunktné, v postupnosti (8.2) ponecháme z viacerých výskytov toho istého prvku len jeden (napríklad prvý). Vo všetkých troch uvedených prípadoch dostávame podpodstupnosť postupnosti (8.2), ktorá je podľa vety 8.2 buď konečná alebo spočítateľná. □

Úloha 8.2. *Nech je* $(A_i)_{i\in I}$ *systém nanajvýš spočítateľných množín,* $A_i \cap A_j \neq \emptyset$ *pre* $i \neq j$. *Zostrojte systém po dvoch disjunktných množín* $(B_i)_{i\in I}$ *taký, že* $\bigcup A_i = \bigcup B_i$*!*

Úloha 8.3. *Nájdite*

(a) *Konečný systém nanajvýš spočítateľných množín, ktorých zjednotenie je spočítateľná množina!*

(b) *Nanajvýš spočítateľný systém konečných množín, ktorých zjednotenie je spočítateľná množina!*

Veta 8.4. *Množina* $P = \mathbb{N} \times \mathbb{N}$ *všetkých usporiadaných dvojíc prirodzených čísel je spočítateľná.*

Dôkaz. Výškou usporiadanej dvojice prirodzených čísel (p, q) je prirodzené číslo $p + q$. Je zrejmé, že dvojice prirodzených čísel môžu mať výšku $0, 1, 2, 3, \ldots$ a že pre $n \geq 0$ existuje $n+1$ usporiadaných dvojíc s výškou n : $(0, n), (1, n-1), (2, n-2), \ldots (n-1, 1), (n, 0)$. Ak označíme symbolom P_n množinu usporiadaných dvojíc prirodzených čísel s výškou n, tak množinu P môžeme vyjadriť ako zjednotenie spočítateľného počtu konečných množín. Podľa vety 8.3 je teda P nanajvýš spočítateľná množina. Keďže však P obsahuje všetky usporiadané dvojice tvaru $(1, n)$ kde $n \in \mathbb{N}$, P nemôže byť konečná množina. Z toho vyplýva, že P je spočítateľná množina. □

Všimnite si, že každé nezáporné racionálne číslo možno vyjadriť ako zlomok $\frac{p}{q}$ vzájomne nesúdeliteľných prirodzených čísel, $q \neq 0$. Usporiadané dvojice prirodzených čísel (p, q), kde p, q sú navzájom nesúdeliteľné a naviac $q \neq 0$, tvoria podmnožinu množiny

P. Z viet 8.2 a 8.4 vyplýva, že kladné racionálne čísla $\mathbb{Q}^+$ tvoria spočítateľnú množinu. Keďže záporné racionálne čísla $\mathbb{Q}^-$ tvoria spočítateľnú množinu a $\mathbb{Q} = \mathbb{Q}^- \cup \mathbb{Q}^+ \cup \{0\}$ je zjednotenie dvoch spočítateľných a jednej konečnej (jednoprvkovej) množiny, množina racionálnych čísel je spočítateľná. Tým sme dokázali nasledujúcu vetu.

Veta 8.5. *Množina všetkých racionálnych čísel je spočítateľná.*

K pojmu spočítateľnosti sme dospeli porovnávaním nekonečných množín s množinou prirodzených čísel. Porovnávať medzi sebou však môžeme aj ľubovoľné dve množiny.

Definícia 8.1. *Množiny* A, B *sa nazývajú ekvivalentné, ak existuje bijekcia* $f : A \to B$. *Ekvivalentnosť množín* A, B *zapisujeme* $A \sim B$.

Úloha 8.4. *Presvedčte sa, či binárny vzťah "$\sim$"je reflexívny, symetrický a tranzitívny. Prečítajte si definíciu relácie a zistite, či možno "$\sim$"považovať za reláciu ekvivalencie!*

Bijekciu možno zostrojiť tak medzi konečnými ako aj nekonečnými množinami. Dve konečné množiny sú ekvivalentné, ak majú rovnaký počet prvkov. Množina je spočítateľná, ak je ekvivalená s množinou prirodzených čísel. Z tranzitívnosti vzťahu "$\sim$"vyplýva, že ak sú dve množiny ekvivalentné medzi sebou, tak sú ekvivalentné aj navzájom. To znamená, že všetky spočítateľné množiny sú ekvivalentné. Uvedieme niekoľko príkladov ekvivalentných množín.

Príklad 8.2. *(1) Interval* $\langle a, b\rangle, a \neq b$ *je ekvivalentný s ľubovoľným uzavretým intervalom* $\langle c, d\rangle, c \neq d$ *na reálnej osi. Hľadanou bijekciou je (napríklad) lineárna funkcia*

$$f(x) = \frac{c-d}{a-b}x + \frac{ad-bc}{a-b}.$$

(2) Množina všetkých reálnych čísel $0 < x < 1$ *je ekvivalentná s množinou všetkých bodov* y *reálnej osi. Bijekciu možno definovať napríklad pomocou funkcie*

$$y = \frac{1}{\pi}\arctan x + \frac{1}{2}.$$

V predchádzajúcich príkladoch sme mohli pozorovať zaujímavú vlastnosť nekonečných množín: množina je ekvivalentná so svojou vlastnou podmnožinou (napríklad $\langle 0, 1\rangle \sim \langle 0, 2\rangle$, $(0, 1) \sim \mathbb{R}$, $\mathbb{Z} \sim \mathbb{N}, \mathbb{Q} \sim \mathbb{N}$ a podobne). Táto vlastnosť je charakteristická pre nekonečné množiny, ale neplatí pre konečné množiny.

Veta 8.6. *Každá nekonečná množina* M *je ekvivalentná s niektorou svojou vlastnou podmnožinou.*

Dôkaz. Nech je nekonečná množina, potom podľa vety 8.1 možno z M vybrať spočítateľnú podmnožinu. Označme túto podmnožinu $A; A = \{a_1, a_2, \ldots, a_n \ldots\}$. Množinu A rozložíme na dve spočítateľné podmnožiny $A_1 = \{a_1, a_3, \ldots\}, A_2 = \{a_2, a_4, \ldots\}$. Zostrojíme bijekciu medzi množinami A, A_1. Nech napríklad $f : A \to A_1; f(a_i) = a_{2i-1}$. Zobrazenie f rozšírime na bijekciu medzi množinami $(M - A) \cup A$ a $(M - A) \cup A_1$:

$$\begin{aligned} f(x) &= x; \quad x \in M - A, \\ f(a_i) &= a_{2i-1}; \quad a_i \in A, \end{aligned}$$

kde $(M - A) \cup A_1 = M - A_2$. Zostrojili sme teda bijekciu medzi M a je jej vlastnou podmnožinou $M - A_2$. □

Nekonečnú množinu môžeme teraz charakterizovať aj takto: množina je nekonečná práve vtedy, ak je ekvivalentná s niektorou svojou vlastnou podmnožinou.

Úloha 8.5. *Nech je M nekonečná a A spočítateľná množina. Potom $(M \cup A) \sim M$. Dokážte!*

8.2 Nespočítateľné množiny

Doteraz sme sa zaoberali len spočítateľnými nekonečnými množinami. Ukázalo sa, že vytváranie „väčších" množín pomocou operácie zjednotenia množín nestačilo na vytvorenie množiny väčšej mohutnosti ako spočítateľnej. Ani karteziálnsky súčin spočítateľných množín neviedol k vytvoreniu nespočítateľnej množiny. Ukážeme, že napriek doterajším neúspechom pri hľadaní nespočítateľných množín, nespočítateľné množiny nie sú žiadnou fikciou, ale skutočne existujú.

Veta 8.7. *Množina všetkých reálnych čísel ležiacich v intervale $\langle 0, 1\rangle$ je nespočítateľná.*

Dôkaz. Každé reálne číslo z intervalu $\langle 0, 1\rangle$ možno zapísať v tvare postupnosti desiatkových číslic: $0, a_1a_2a_3\ldots$ (ak má reálne číslo $a \in \langle 0, 1\rangle$ konečný desatinný rozvoj, budú sa v postupnosti číslic, ktorá ho reprezentuje od istého miesta vyskytovať len samé nuly.) Predpokladajme, že je množina reálnych čísel z intervalu $\langle 0, 1\rangle$ spočítateľná. Potom tieto čísla môžeme tiež usporiadať do postupnosti

$$\begin{aligned} \alpha_1 &= 0a_{1,1}a_{1,2}a_{1,3}\ldots \\ \alpha_2 &= 0a_{2,1}a_{2,2}a_{2,3}\ldots \\ \alpha_3 &= 0a_{3,1}a_{3,2}a_{3,3}\ldots \\ &\ldots \\ \alpha_n &= 0a_{n,1}a_{n,2}a_{n,3}\ldots \\ &\ldots \end{aligned} \tag{8.3}$$

kde $a_{i,k}$ je k-ta cifra desatinného rozvoja čísla α_i. Ukážeme, že existuje číslo $\beta = 0, b_1b_2\ldots$, ktoré zrejme patrí do intervalu $\langle 0, 1\rangle$, ale nie je uvedené v postupnosti $\alpha_1, \alpha_2, \ldots$. Stačí vziať $b_1 \neq a_{1,1}, b_2 \neq a_{2,2}, \ldots, b_i \neq a_{i,i}, \ldots$. Keďže β sa v i-tej cifre líši od i-teho čísla v postupnosti (8.3), nemôže sa rovnať žiadnemu číslu uvedenému (8.3). Dostávame spor s tým, že postupnosť (8.3) obsahuje všetky reálne čísla z intervalu $\langle 0, 1\rangle$. To znamená, že žiadna spočítateľná množina reálnych čísel z intervalu $\langle 0, 1\rangle$ nemôže obsahovať všetky reálne čísla z intervalu $\langle 0, 1\rangle$, resp. množina reálnych čísel nie je spočítateľná. □

Poznámka. (1) Zapamätajte si postup, akým sme zostrojili číslo β. Nazýva sa *Cantorova diagonalizačná metóda* a určite sa s ňou ešte v matematike alebo teoretickej informatike stretnete.

(2) Pozornému čitateľovi určite neuniklo, že existujú reálne čísla, ktoré nemajú jednoznačný zápis. Presnejšie, ak má nejaké číslo konečný desatinný rozvoj, možno ho

zapísať dvoma rozličnými spôsobmi, a to tak, že od určitého miesta bude postupnosť číslic v jeho zápise pozostávať zo samých núl, alebo samých deviatok. Napríklad, $0.2 = 0.200000\cdots = 0.199999\ldots$. Ak postupnosť (8.3) obsahuje oba zápisy čísla x s konečným desatinným rozvojom, zostrojené číslo β sa bude líšiť od obidvoch. Ak však postupnosť (8.3) obsahuje z dvoch možných zápisov čísla x len jeden, teoreticky by sme mohli skonštruovať číslo β, ktoré by sa rovnalo druhému zápisu čísla x. Aby sme sa tomuto problému vyhli, nebudeme pri konštrukcii čísla β používať číslice $0, 9$.

Úloha 8.6. *Koľko je vlastne čísel z intervalu $\langle 0, 1\rangle$, ktoré možno zapísať dvoma rozličnými spôsobmi?*

Úloha 8.7. *Dokážte, že nasledujúce množiny sú nespočítateľné:*

(a) *množiny reálnych čísel z intervalov $\langle a, b\rangle, \langle a, b), (a, b\rangle, (a, b)$ $\quad a \neq b$,*

(b) *množina bodov reálnej osi,*

(c) *množiny bodov (reálnej) roviny, trojrozmerného priestoru; plochy štvorca, povrchu gule, gule (s nenulovým polomerom),*

(d) *množina všetkých priamok v rovine,*

(e) *množina všetkých spojitých reálnych funkcií jednej premennej (konečného počtu premenných).*

8.3 Cantor-Bernsteinova veta

Zatiaľ vieme dokazovať ekvivalenciu dvoch množín A, B len tak, že skonštruujeme nejakú bijekciu napríklad z A do B.[2] To nemusí byť práve jednoduchá úloha (skúste zostrojiť bijekciu medzi množinami reálnych čísel $\langle 0, 1\rangle$ a $\langle 0, 1)$). Jednoduchšie riešenie ponúka nasledujúca veta.

Veta 8.8. *Nech sú A, B ľubovoľné množiny a nech existujú injektívne zobrazenia $f : A \to B$ a $g : B \to A$. Potom sú množiny A, B ekvivalentné.*

Dôkaz. Je známych viacero dôkazov tejto dôležitej vety. Vyberieme spomedzi nich dva.

Injekcia f zobrazuje množinu A na podmnožinu B_1 množiny B a injekcia g zobrazuje množinu B na podmnožinu A_1 množiny A:

$$f(A) = B_1 \subseteq B, \quad g(B) = A_1 \subseteq A.$$

Ak zúžime injekciu g na (B, A_1), dostávame bijekciu (veta 5.6). To znamená, že $B \sim A_1$. Ukážeme, že $A_1 \sim A$ a tým aj ekvivalenciu $A \sim B$. Označme

$$g(f(A)) = g(B_1) = A_2 \subseteq A_1,$$

[2] pripomíname, že je jedno, či skonštruujeme bijekciu $f : A \to B$ alebo $g : B \to A$, pretože aj inverzná funkcia k bijekcii je bijekcia.

podobne

$$f(g(B)) = f(A_1) = B_2 \subseteq B_1.$$

Budeme pokračovať ďalej a zostrojíme postupnosť množín $A_1, A_2, A_3 \ldots$:

$$\begin{aligned} A_3 &= g(f(A_1)) \subseteq g(f(A)) = A_2 \\ A_4 &= g(f(A_2)) \subseteq g(f(A_1)) = A_3 \\ &\ldots \\ A_{k+2} &= g(f(A_k)) \subseteq g(f(A_{k-1})) = A_{k+1}. \end{aligned}$$

Zrejme platí

$$A \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \supseteq A_k \supseteq A_{k+1} \supseteq \ldots$$

Položíme

$$D = \bigcap_{k=1}^{\infty} A_k$$

a vyjadríme množiny A, A_1 ako zjednotenie po dvoch disjuntných množín:

$$A = D \cup (A - A_1) \cup (A_1 - A_2) \cup \cdots \cup (A_k - A_{k+1}) \cup \ldots \tag{8.4}$$

$$A_1 = D \cup (A_1 - A_2) \cup (A_2 - A_23) \cup \cdots \cup (A_k - A_{k+1}) \cup \ldots \tag{8.5}$$

Upravíme rozklady množín A, A_1 (8.4) a (8.5):

$$A = D \cup [(A_1 - A_2) \cup (A_3 - A_4) \cup \ldots] \cup [(A - A_1) \cup (A_2 - A_3) \cup \ldots] \tag{8.6}$$

$$A_1 = D \cup [(A_1 - A_2) \cup (A_3 - A_4) \cup \ldots] \cup [(A_2 - A_3) \cup (A_4 - A_5) \cup \ldots]. \tag{8.7}$$

Teraz zostrojíme bijekciu $\varphi : A \to A_1$.

$$\varphi(x) = \begin{cases} x & \text{pre } x \in D \cup [(A_1 - A_2) \cup (A_3 - A_4) \cup \ldots] \\ (g \circ f)(x) & \text{pre } x \in [(A - A_1) \cup (A_2 - A_3) \cup \ldots]. \end{cases}$$

Je zrejmé, že zobrazenie $\varphi : A \to A_1$ je injekcia (identické zobrazenie na množine $D \cup [(A_1 - A_2) \cup (A_3 - A_4) \cup \ldots]$ je injekcia a obe zobrazenia f, g sú injekcie.) Ukážeme ešte, že φ je surjekcia, t.j., že $\varphi(A) = A_1$. Zrejme stačí ukázať, že

$$\varphi([(A - A_1) \cup (A_2 - A_3) \cup \ldots]) = [(A_2 - A_3) \cup (A_4 - A_5) \cup \ldots].$$

Postupne dostávame

$$\begin{gathered} \varphi((A - A_1) \cup (A_2 - A_3) \cup \cdots \cup (A_k - A_{k+1}) \cup \ldots) = \\ = (g \circ f)((A - A_1) \cup (A_2 - A_3) \cup \cdots \cup (A_k - A_{k+1}) \cup \ldots) = \\ = (g \circ f)(A - A_1) \cup (g \circ f)(A_2 - A_3) \cup \ldots (g \circ f)(A_k - A_{k+1}) \cup \cdots = \\ = [(g \circ f)(A) - (g \circ f)(A_1)] \cup [(g \circ f)(A_2) - (g \circ f)(A_3)] \cup \cdots \cup [(g \circ f)(A_k) - \\ -(g \circ f)(A_{k+1})] \cup \cdots = (A_2 - A_3) \cup (A_4 - A_5) \cup \cdots \cup (A_{k+2} - A_{k+3} \cup \ldots \end{gathered}$$

V odvodení sme využili to, že zobrazenie $(g \circ f)$ je injektívne, a teda platí

$$(g \circ f)(A_i - A_{i+1}) = (g \circ f)(A_i) - (g \circ f)(A_{i+1}).$$

Iný dôkaz. Keďže $f : A \to B, g : B \to A$ sú injekcie, každý prvok $a \in A$ je obrazom nanajvýš jedného prvku $b = g^{-1}(a)$ z B. Tento prvok, ak existuje, má opäť najviac jedného *rodiča* $a' = f^{-1}(b) = f^{-1}(g^{-1}(a))$ v A, atď. Ak takýmto spôsobom sledujeme všetkých *predkov* daného prvku množiny A (ako aj množiny B) tak dlho ako to je len možné, vidíme, že pre daný prvok môžu nastať tri navzájom sa vylučujúce prípady:

(1) každý predok daného prvku má rodiča; t.j. existuje nekonečná reťaz predkov;

(2) daný prvok má takého predka v množine A, ktorý už nemá rodiča (t.j. reťaz predkov daného prvku sa končí v A)

(3) daný prvok má takého predka v množine B, ktorý už nemá rodiča (t.j. reťaz predkov daného prvku sa končí v B).

Vzhľadom na uvedené tri prípady rozdelíme A na tri podmnožiny A_1, A_2, A_3 a podobne rozdelíme B na tri podmnožiny B_1, B_2, B_3.

Ak $a \in A_1$, tak zrejme $f(a) \in B_1$. Podľa definície B_1 ku každému prvku $b \in B$ existuje prvok $A \in A$, nutne patriaci do A_1, taký, že $f(a) = b$. Preto zúženie zobrazenia f na množinu A_1, $f|A_1$ je bijekcia $f|A_1 : A_1 \to B_1$. (Podobne zúženie $g|B_1$ je bijekcia $g|B_1 : B_1 \to A_1$.)

Ak $b \in B_2$, tak očividne $g(b) \in A_2$. Z definície množiny A_2 vyplýva, že každý jej prvok má predka, a ten nutne patrí do B_2. Preto $g|B_2$ je bijekcia, $g|B_2 : B_2 \to A_2$. Nemožno však tvrdiť, že $f|A_2$ je bijekcia z A_2 do B_2!)

Napokon, podobne ako v predchádzajúcom prípade, $f|A_3$ je bijekcia z A_3 do B_3 (no pritom nemožno tvrdiť, že $f|A_3$ je bijekcia z B_3 do A_3.)

Teraz už ľahko z týchto zobrazení skombinujeme bijekciu $h : A \to B$. Stačí totiž pre ľubovoľné $x \in A$ položiť:

$$h(x) = \begin{cases} f(x), & \text{ak } x \in A_1 \cup A_3, \\ g^{-1}(x), & \text{ak } x \in A_2. \end{cases}$$

Z vyššie uvedeného je zrejmé, že $h : A \to B$ je bijekcia, □

Úloha 8.8. *Napíšte explicitné vyjadrenie bijekcie* $F : A \to B$ *pomocou injekcií* f, g.

8.4 Kardinálne čísla

Čo majú spoločné ekvivalentné množiny? V prípade konečných množín to je počet prvkov. V prípade nekonečných množín sa nedá hovoriť o počte prvkov, a preto zavádzame všeobecnejší pojem na určenie „veľkosti“ množín. Budeme hovoriť, že dve množiny majú rovnakú mohutnosť, ak sú ekvivalentné. Je zrejmé, že v prípade konečných množín sa mohutnosť množiny zhoduje s počtom prvkov. Zakrátko zavedieme podobný pojem aj pre počty prvkov nekonečných množín. Začneme množinou prirodzených čísel, $\mathbb{N}$.

Mohutnosť množiny prirodzených čísel $\mathbb{N}$ označíme symbolom $\aleph_0$ ($\aleph$ je hebrejské písmeno *alef*, symbol $\aleph_0$ čítame *alef nula*). Ak teda množina $\mathbb{N}$ má mohutnosť $\aleph_0$, tak potom majú aj všetky spočítateľné množiny mohutnosť $\aleph_0$.

Ďalšia základná nekonečná množina je množina reálnych čísel, $\mathbb{R}$. Množina $\mathbb{R}$ má mohutnosť nazývanú *mohutnosťou kontinua*.[3] Mohutnosť kontinua sa označuje symbolom $\mathcal{C}$. Tak ako sú všetky množiny ekvivalentné s množinou prirodzených čísel $\mathbb{N}$ spočítateľné, majú všetky množiny ekvivalentné množine $\mathbb{R}$ mohutnosť kontinua.

Mohutnosti množín sa nazývajú *kardinálnymi číslami*. Zatiaľ poznáme kardinálne čísla konečných množín $0, 1, 2, 3, \ldots$, a dve kardinálne čísla nekonečných množín $\aleph_0, \mathcal{C}$. Zakrátko ukážeme, že existujú aj ďalšie kardinálne čísla. Pre tieto kardinálne čísla však už ťažšie budeme nachádzať „prirodzené“ množiny objektov s danou mohutnosťou. Aby sme si udržali prehľad a dokázali porovnávať mohutnosti abstraktných množín, vytvoríme aparát, ktorý nám umožní porovnávať ľubovoľné kardinálne čísla. Označme mohutnosť množiny A symbolom $|A|$. Pozrieme sa najprv na kardinálne čísla konečných množín. Keďže kardinálne čísla konečných množín vyjadrujú počty ich prvkov (čo sú prirodzené čísla) a množina $\mathbb{N}$ je usporiadaná, pre ľubovoľné dve konečné množiny A, B môže nastať len jedna z nasledujúcich troch možností:

$$|A| = |B|, \quad |A| < |B|, \quad |A| > |B|.$$

Podobný vzťah platí aj pre nekonečné množiny. Keďže pre kardinálne čísla nekonečných množín nemôžeme využiť usporiadanie množiny prirodzených čísel, využijeme na porovnávanie mohutností nekonečných množín injektívne zobrazenia[4]

Nech sú A, B ľubovoľné dve množiny[5] a nech $|A| = \alpha, |B| = \beta$ sú kardinálne čísla (mohutnosti) množín A, B. Budeme hovoriť, že

(1) $\alpha = \beta$, ak existujú injekcie $f : A \to B$ a $g : B \to A$. Potom zrejme existuje bijekcia z A do B a platí $A \sim B$.

(2) $\alpha < \beta$, ak existuje injekcia $f : A \to B$ ale neexistuje injekcia $g : B \to A$.

(3) $\alpha > \beta$, ak existuje injekcia $g : B \to A$ ale neexistuje injekcia $f : A \to B$.

(4) Teoreticky musíme pripustiť aj možnosť, že α,β sú neporovnateľné, ktorá by nastala, ak by neexistovali injekcie $f : A \to B$, $g : B \to A$. Z Zermelovej vety (pozri napríklad [13]) však vyplýva, že táto možnosť nemôže nastať.

To znamená, že pre ľubovoľné kardinálne čísla α, β platí jeden z nasledujúcich vzťahov

$$\alpha < \beta, \quad \alpha = \beta, \quad \alpha > \beta.$$

Vieme, že spočítateľné množiny sú „najmenšie“ nekonečné množiny a že okrem nich existujú ešte množiny mohutnosti kontinua. Naskytá sa niekoľko prirodzených otázok.

[3] kontinuum je kompaktná súvislá podmnožina topologického priestoru obsahujúca aspoň jeden bod [7]

[4] daná metóda je použiteľná aj na porovnanie mohutností konečných množín

[5] pozri predchádzajúcu poznámku

Aký je vzťah medzi spočítateľnými množinami a množinami mohutnosti kontinua? Existujú nekonečné množiny väčšej mohutnosti, ako je mohutnosť kontinua? Ak áno, ako sa dajú zostrojiť? Existuje „najväčšie“ kardinálne číslo? Na tieto otázky dáme (dúfajme, že uspokojivé) odpovede vo zvyšku tejto kapitoly. Začneme operáciou, ktorá nám umožní vytvárať nové (väčšie) kardinálne čísla.

Veta 8.9. *Nech je ľubovoľná množina a $\mathcal{P}(M)$ je jej potenčná množina. Potom platí*

$$|M| < |\mathcal{P}(M)|.$$

Dôkaz. Injekciu $f : M \to \mathcal{P}(M)$ zostrojíme ľahko: každému prvku $x \in M$ priradíme jednoprvkovú množinu $\{x\} \in \mathcal{P}(M)$. Zložitejšie bude dokázať, že neexistuje injekcia $g : \mathcal{P}(M) \to M$. Dokážeme to tak, že ukážeme existenciu aspoň jednej množiny X, ktorá sa „nemá na čo zobraziť.“ Predpokladajme, že potrebná injekcia $g : \mathcal{P}(M) \to M$ existuje. Nech

$$X = \{a \in M; a \notin g^{-}(a)\},$$

t.j. X je množina všetkých tých prvkov množiny M, ktoré nepatria do svojho vzoru. Na čo sa potom zobrazí samotná množina X?

Nech $g(X) = x$, t.j. $X = g^{-}(x)$. Patrí prvok x do množiny X? Ak platí $x \notin X$, potom podľa definície množiny X by malo platiť $x \in X$. Ak však $x \in X$, tak potom $x \in g^{-}(x)$, a to je spor s definíciou množiny X. To znamená, že taký prvok $x \in M$, pre ktorý $g(X) = x$ neexistuje. Tým je veta dokázaná. □

Z tvrdenia vety 8.9 vyplýva, že k množine ľubovoľnej mohutnosti možno zostrojiť množinu väčšej mohutnosti. To znamená, že možno zostrojiť zhora neohraničenú postupnosť kardinálnych čísel.

V matematickej analýze sa budeme najčastejšie stretávať s množinami mohutnosti $\aleph_0$ a $\mathcal{C}$. Ukážeme, aký je vzťah medzi týmito dvomi kardinálnymi číslami. Nech je M konečná množina a nech $|M| = m$. Potom potenčná množina $\mathcal{P}(M)$ bude mať $2^{|M|} = 2^m$ prvkov. Zovšeobecníme toto označenie aj pre nekonečné množiny a položíme $|\mathcal{P}(A)| = 2^{|A|}$.

Veta 8.10. $2^{\aleph_0} = \mathcal{C}$.

Dôkaz. Každú podmnožinu A množiny prirodzených čísel je možné zadať jednoznačne pomocou charakteristickej funkcie $\chi_A : \mathbb{N} \to \{0, 1\}$ definovanej takto:

$$\chi_A(x) = \begin{cases} 1 & \text{pre } x \in A \\ 0 & \text{pre } x \notin A. \end{cases}$$

Charakteristickú funkciu χ_A môžeme popísať pomocou postupnosti hodnôt, ktoré nadobúda na prvkoch množiny $\mathbb{N}$. Napríklad

0	1	2	3	4	5	...	k	...	
0	0	0	0	0	0	...	0	...	$A = \emptyset$
1	0	0	0	0	0	...	0	...	$A = \{0\}$
						...		...	
1	1	1	1	1	1	...	1	...	$A = \mathbb{N}$

Postupnosť hodnôt charakteristickej funkcie množiny $A \subseteq \mathbb{N}$; $e_0, e_1, e_2, \dots e_n, \dots$ interpretujeme ako binárne zapísané číslo

$$0.e_0e_1e_2\cdots = e_0 \cdot 2^{-1} + e_1 \cdot 2^{-2} + e_2 \cdot 2^{-3} + \dots$$

Je zrejmé, že každej množine $A \subseteq \mathbb{N}$ možno jednoznačne priradiť reálne číslo z intervalu $\langle 0, 1\rangle$. Napríklad $\{1\} \to 1/2, \emptyset \to 0, \mathbb{N} \to 1$, atď. Podobne ako pri dôkaze nespočítateľnosti množiny $\langle 0, 1\rangle$ vznikajú aj tu problémy s nejednoznačnosťou vyjadrenia reálneho čísla pomocou binárneho zlomku. Existujú čísla, ktoré majú dvojaké vyjadrenie (napríklad $1/2 = 0.1000\cdots = 0.011\dots$) a teda dve rôzne podmnožiny sa zobrazia na to isté číslo. Tento problém však ľahko vyriešime. Čísla, ktoré majú dvojaké vyjadrenie sú charakteristické tým, že sa v im prislúchajúcej binárnej postupnosti od istého miesta vyskytujú samé jednotky. Takýmto číslam v $\mathcal{P}(\mathbb{N})$ zodpovedajú podmnožiny, ktorých doplnkami sú konečné množiny. Množinu týchto podmnožín označíme symbolom $\mathcal{S}$ a symbolom $\mathcal{R}$ označíme množinu $\mathcal{P}(\mathbb{N}) - \mathcal{S}$. Je zrejmé, že zobrazenie z množiny $\mathcal{R}$ do množiny $\langle 0, 1\rangle$ je bijektívne.to znamená, že $|\mathcal{R}| = \mathcal{C}$. Na druhej strane $\mathcal{P}(\mathbb{N}) = \mathcal{R} \cup \mathcal{S}$. Keďže $\mathcal{R}$ je nespočítateľná a $\mathcal{S}$ je spočítateľná množina, $|\mathcal{R} \cup \mathcal{S}| = |\mathcal{R}|$ (úloha 8.5), a teda $|\mathcal{P}(\mathbb{N})| = \mathcal{C}$. □

Úloha 8.9. *Pomocou Cantor-Bernsteinovej vety dokážte, že množiny z úlohy 8.7 majú mohutnosť $\mathcal{C}$!*

Úloha 8.10. *Dokážte ekvivalenciu nasledujúcich množín:*

(a) $S_1 = \langle 0, 1\rangle$;

(b) $S_2 = \langle 0, 1\rangle \times \langle 0, 1\rangle$;

(c) $S_2 = \langle 0, 1\rangle \times \langle 0, 1\rangle \times \langle 0, 1\rangle$.

Úloha 8.11. *Dokážte, že množina bodov kruhu a štvorca v reálnej rovine sú ekvivalentné!*

Úloha 8.12. *Určte mohutnosti nasledujúcich množín:*

(a) *množina všetkých intervalov* (a, b) *na reálnej osi,* $a, b \in \mathbb{Q}$,

(b) *množina všetkých disjunktných neprázdnych intervalov na reálnej osi,*

(c) *množina všetkých reálnych spojitých funkcií jednej premennej;*

(d) *množina polynómov s racionálnymi koeficientami,*

(e) *množina všetkých nekonečných postupností znakov nad abecedou* $\{a, b, c\}$,

(f) $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Z}$;

(g) $\mathbb{Q} \times \mathbb{R}$;

(h) $\mathbb{Q}^{\mathbb{N}}, \mathbb{N}^{\mathbb{Q}}, \mathbb{Q}^{\mathbb{Q}}, \mathbb{R}^2, \{0, 1\}^{\mathbb{R}}, \mathbb{R}^{\mathbb{R}}$,

(i) *množina hodnôt funkcie* $f : R \to \mathbb{N}$.

8.5 Aritmetika kardinálnych čísel

Kardinálne čísla sú v istom zmysle zovšeobecnením prirodzených čísel. Dá sa preto prirodzene očakávať, že aspoň niektoré základné vlastnosti prirodzených čísel možno zovšeobecniť tak, aby platili aj pre kardinálne čísla. V tejto časti sa budeme zaoberať aritmetickými operáciami s kardinálnymi číslami (kardinálnou aritmetikou). Ukážeme, že pre kardinálne čísla sa dajú zaviesť podobné aritmetické operácie ako pre prirodzené čísla. (Naviac, tieto operácie sa v prípade konečných kardinálnych čísel budú zhodovať s operáciami na prirodzených číslach.[6]) Toto zovšeobecnenie však nebude priamočiare; viaceré z vlastností kardinálnych operácií budú platiť len za istých predpokladov (platnosť axiómy výberu).

Operácia nasledovníka Jednou zo základných vlastností prirodzených čísel (ktorú sme využívali napríklad pri dôkazoch matematickou indukciou) je, že pre každé prirodzené číslo k existuje prirodzené číslo, ktoré za ním bezprostredne nasleduje[7], Toto číslo sa dá určiť pomocou operácie nasledovníka $\sigma(k) = k+1$. Pre konečné kardinálne čísla, ktoré sú prirodzenými číslami nasledovníci samozrejme existujú. V prípade nekonečných kardinálnych čísel je existencia nasledovníkov podmienená platnosťou axiómy výberu:

Ak platí axióma výberu, pre každé kardinálne číslo κ existuje kardinálne číslo $\sigma(\alpha)$ také, že

1. $\sigma(\alpha) > \alpha$
2. neexistuje kardinálne číslo β; $\sigma(\alpha) > \beta > \alpha$.

Súčet kardinálnych čísel Nech sú A, B množiny s mohutnosťami $|A| = \alpha, |B| = \beta$. Predpokladajme kvôli jednoduchosti, že množiny A, B sú disjunktné; $A \cap B = \emptyset$. (Ak nie, vezmeme namiesto množín A, B množiny $A_1 = A \times \{0\}$ resp. $B_1 = B \times \{1\}$. Je zrejmé, že $|A| = |A_1|, |B| = |B_1|$ a $A_1 \times B_1 = \emptyset$.) *Súčtom mohutností* (kardinálnych čísel) α, β nazveme kardinálne číslo množiny $A \cup B$. Ak $|A \cup B| = \gamma$, tak túto skutočnosť zapisujeme $\alpha + \beta = \gamma$. Súčet kardinálnych čísel má nasledujúce vlastnosti:

1. neutrálnym prvkom vzhľadom na sčítanie kardinálnych čísel je podobne ako v prípade prirodzených čísle 0; ak totiž $|A| = \alpha$, tak
$$\alpha + 0 = 0 + \alpha = |A \cup \emptyset| = |A| = \alpha.$$
2. Operácie sčítania kardinálnych čísel je komutatívna operácia;
$$\alpha + \beta = \beta + \alpha$$

[6] Po zavedení ordinálnych čísel by sme mohli ďalej pokračovať v zovšeobecňovaní aritmetických operácií a ukázať, že aritmetika ordinálnych čísel (ordinálna aritmetika) má mnoho spoločného s kardinálnou aritmetikou. Táto problematika však prekračuje rámec základnej učebnice, a preto sa ňou nebudeme zaoberať.

[7] to znamená, že medzi prirodzeným číslom a jeho nasledovníkom už neexistuje žiadne iné prirodzené číslo.

3. Operácie sčítania kardinálnych čísel je asociatívna operácia;
$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$
4. Operácia sčítania (dvoch) kardinálnych čísel je neklesajúca vzhľadom na oba argumenty; t.j. súčet dvoch kardinálnych čísel nemôže byť menší ako ľubovoľný z jeho argumentov:
$$(\alpha \leq \beta) \Rightarrow (\alpha + \gamma \leq \beta + \gamma) \& (\gamma + \alpha \leq \gamma + \beta).$$
5. Súčet dvoch konečných kardinálnych čísel je v skutočnosti súčtom dvoch prirodzených čísel. V prípade, ak je aspoň jedno z kardinálnych čísle v súčte $\alpha+\beta$ nekonečné a **platí axióma výberu**, tak
$$\alpha + \beta = \max(\alpha, \beta).$$

Na prirodzených číslach je možné (s istými obmedzeniami) definovať aj operáciu odčítania. Pre nekonečné kardinálne čísla sa operácia odčítania nedá definovať.

Súčin kardinálnych čísel *Súčinom mohutností* (kardinálnych čísel) α, β nazveme kardinálne číslo množiny $A \times B$. Ak $|A \times B| = \gamma$, tak túto skutočnosť zapisujeme $\alpha \cdot \beta = \gamma$. Pre násobenie kardinálnych čísel platí

1. Pre ľubovoľné kardinálne číslo α je súčin $\alpha \cdot 0 = 0$.
2. Číslo 1 je neutrálnym prvkom vzhľadom na násobenie kardinálnych čísel;
$$\alpha \cdot 1 = 1 \cdot \alpha = \alpha.$$
3. Súčin dvoch kardinálnych čísel α, β je nulový práve vtedy, ak je jeden z „činiteľov“ nulový;
$$\alpha \cdot \beta = 0 \equiv (\alpha = 0) \vee (\beta = 0)$$
4. Násobenie kardinálnych čísel je komutatívne;
$$\alpha \cdot \beta = \beta \cdot \alpha.$$
5. Násobenie kardinálnych čísel je asociatívne;
$$\alpha \cdot (\beta \cdot \delta) = (\alpha \cdot \beta) \cdot \delta.$$
6. Násobenie kardinálnych čísel je distributívne vzhľadom na sčítanie kardinálnych čísel
$$\alpha \cdot (\beta + \delta) = (\alpha \cdot \beta) + (\alpha \cdot \delta)$$
7. Operácia súčinu (dvoch) kardinálnych čísel je neklesajúca vzhľadom na oba argumenty; t.j. súčin dvoch kardinálnych čísel nemôže byť menší ako ľubovoľný z jeho argumentov:
$$(\alpha \leq \beta) \Rightarrow (\alpha \cdot \gamma \leq \beta \cdot \gamma) \& (\gamma \cdot \alpha \leq \gamma \cdot \beta).$$
8. Ak platí axióma výberu, tak
$$\alpha \cdot \beta = \max(\alpha, \beta).$$

Umocňovanie kardinálnych čísel Kardinálnym číslom α umocneným na kardinálne číslo β nazveme mohutnosť (kardinálne číslo) množiny A^B, množiny všetkých zobrazení z množiny B do množiny A. Nech $|A|^{|B|} = |A^B| = \gamma$, potom $\alpha^\beta = \gamma$. Uvedieme základné vlastnosti umocňovania kardinálnych čísel. Podobne ako v predchádzajúcich prípadoch budeme predpokladať, že α, β, γ sú kardinálne čísla nejakých množín A, B, C.

1. Najprv rozoberieme špeciálne prípady. Pripomíname, že prázdna množina má mohutnosť $|\emptyset| = 0$. Pre ľubovoľné kardinálne číslo α platí

   $$\alpha^0 = 1,$$

   kde 1 je mohutnosť jednoprvkovej množiny. Tento vzťah platí aj v špeciálnom prípade, keď $\alpha = 0$:

   $$0^0 = 1.$$

2. Ak je však $\alpha = 0$ a β nenulové kardinálne číslo, tak

   $$\alpha^\beta = 0^\beta = 0.$$

3. Ďalšie špeciálne prípady nastávajú, keď je jedno z kardinálnych čísel α, β jednotkové:

   $$1^\beta = 1$$

   resp.

   $$\alpha^1 = \alpha.$$

4. Umocňovanie na súčet kardinálnych čísel

   $$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma.$$

5. Umocňovanie na súčin kardinálnych čísel

   $$\alpha^{\beta\cdot\gamma} = \left(\alpha^\beta\right)^\gamma.$$

6. Umocňovanie súčinu kardinálnych čísel

   $$(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma.$$

7. Doteraz uvedené vlastnosti umocňovania boli priamočiarym zovšeobecnením vlastností umocňovania prirodzených čísel. Zaujímavé prípady nastanú, keď sa pri umocňovaní kardinálnych čísel použijú aj konečné aj nekonečné kardinálne čísla. Ak sú α, β konečné kardinálne čísla väčšie ako 1 a γ je nekonečné kardinálne číslo, tak potom

   $$\alpha^\gamma = \beta^\gamma$$

   a ak je α nekonečné a β konečné nenulové kardinálne číslo, tak potom

   $$\alpha^\beta = \alpha.$$

8. Podobne ako pre súčet a súčin kardinálnych čísel je aj umocňovanie kardinálnych čísel neklesajúce vzhľadom na oba svoje argumenty:

$$(1 \leq \alpha)\&(\beta \leq \gamma) \Rightarrow (\alpha^{\beta} \leq \alpha^{\gamma})$$

a

$$(\alpha \leq \beta) \Rightarrow (\alpha^{\gamma} \leq \beta^{\gamma}).$$

9. Výpočet hodnoty mocniny kardinálnych čísel je trocha komplikovanejší. Pripomíname, že špeciálnym prípadom umocňovania kardinálnych čísel je $2^{|A|}$, mohutnosť potenčnej množiny $P(A)$ množiny A. Ak platí axióma výberu a $2 \leq \alpha$ a $1 \leq \beta$ a aspoň jedno z kardinálnych čísel α, β je nekonečné, tak potom

$$\max\left(\alpha, 2^{\beta}\right) \leq \alpha^{\beta} \leq \max\left(2^{\alpha}, 2^{\beta}\right).$$

Vlastnosti aritmetických operácií nad kardinálnymi číslami sú prístupnou formou popísané v [5].

Väčšina uvedených vlastností kardinálnej aritmetiky sa dokazuje ľahko. Ťažšie sú len dôkazy, ktoré si vyžadujú platnosť axiómy výberu. Na ilustráciu ukážeme niektoré z „ľahších“ tvrdení, ďalšie ponecháme čitateľovi ako cvičenia. Dôkazy využívajúce axiómu výberu prekračujú rámec tejto knihy a čitateľ ich nájde napríklad v [**?**]. Budeme predpokladať, že A, B, C sú množiny mohutností $|A| = \alpha, |B| = \beta, |C| = \gamma$ a $A \cap B = \emptyset$.

1. Komutatívnosť súčtu kardinálnych čísel vyplýva z definície súčtu kardinálnych čísel a z komutatívnosti zjednotenie množín. Keďže $A \cup B = B \cup A$ a $A \cap B = \emptyset$,

$$\alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha.$$

2. Pre ľubovoľné kardinálne číslo α je $\alpha \cdot 0 = 0$ a $\alpha \cdot 1 = 0\alpha$. Pripomíname, že 0 je mohutnosť prázdnej množiny $\emptyset$ a 1 je mohutnosť ľubovoľnej jednoprvkovej množiny, napríklad $\{\spadesuit\}$. Z definíce násobenia kardinálnych čísel vyplýva, že

$$\alpha \cdot 0 = |A \times \emptyset|.$$

Karteziánsky súčin $|A \times \emptyset|$ je prázdna množina (nemáme z čoho vyberať druhý prvok usporiadanej dvojice, ktorá by patrila do $|A \times \emptyset|$). To znamená

$$\alpha \cdot 0 = |A \times \emptyset| = |\emptyset| = 0.$$

Na druhej strane dá sa ľahko nahliadnuť, že karteziánsky súčin

$$A \times \{\spadesuit\} = \{(a, \spadesuit); a \in A\}$$

má rovnakú mohutnosť ako množina A; hľadaná bijekcia $\varphi : A \to A \times \{\spadesuit\}$ je definovaná napríklad takto

$$\forall x \in A \varphi(x) = (x, \spadesuit).$$

3. Distributívny zákon pre súčin a súčet kardinálnych čísel vyplýva z nasledujúceho vzťahu platného pre karteziánsky súčin (Veta 3.3)

$$(A \cup B) \times C = (A \times C) \cup (B \times C).$$

4. Podobne „monotónnosť“ súčinu kardinálnych čísel vyplýva zo vzťahu (Veta 3.3)

$$(A \subseteq B) \Rightarrow (A \times C) \subseteq (B \times C).$$

5. Dokážeme rovnosť $\alpha^0 = 1$. Mohutnosť α^0 má podľa definície umocňovania kardinálnych čísel množina všetkých zobrazení z prázdnej množiny do množiny A, $A^\emptyset$. Podľa definície zobrazenia je zobrazenie z množiny $A^\emptyset$ množinou usporiadaných dvojíc karteziálnskeho súčinu $\emptyset \times A$ takou, že pre každý prvok x množiny $\emptyset$ v ňom existovať práve jedna dvojica, ktorej prvým prvkom je prvok x. Túto požiadavku paradoxne spĺňa práve prázdna množina (usporiadaných dvojíc), a teda existuje práve jedno takého zobrazenie:

$$|A^\emptyset| = |\{\emptyset\}| = 1.$$

6. Dokážeme, že $\forall \beta \neq 0, 0^\beta = 0$. Z definície umocňovania kardinálnych čísel vyplýva, že 0^β je mohutnosťou množiny $\emptyset^B$ všetkých zobrazení z neprázdnej množiny B do prázdnej množiny. Predpokladajme, že také zobrazenie existuje, označme ho $\varphi : B \to \emptyset$. Potom však pre každý prvok x neprázdnej množiny B musí usporiadaná dvojica $(x, \varphi(x)) \in \varphi$, pričom $\varphi(x) \in \emptyset$. To vedie k sporu, pretože $\emptyset$ neobsahuje žiadne prvky a teda prvky množiny B sa „nemajú na čo zobraziť.“ To znamená, že

$$0^\beta = |\emptyset^B| = |\emptyset| = 0.$$

7. Rovnosť $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$, dokážeme pomocou Cantor Bernsteinovej vety. Položíme

$$\alpha^\beta = |A^B|,\ \alpha^\gamma = |A^C|$$

a prijmememe ešte predpoklad $B \cap C = \emptyset$. Skonštruujeme dve injektívne zobrazenia $\Phi : A^{B\cup C} \to A^B \times A^C$ a $\Psi : A^B \times A^C \to A^{B\cup C}$. Nech je f ľubovoľné zobrazenie také, že $f : B \cup C \to A$. Zúžením zobrazenia f na množinu B, resp. C skonštruujeme dve zobrazenia

$$f_1 : B \to A; \forall x \in B : f_1(x) = f(x);$$
$$f_2 : C \to A; \forall x \in C : f_2(x) = f(x),$$

ktoré tvoria usporiadanú dvojicu $(f_1, f_2) \in A^B \times A^C$. Dá sa ľahko ukázať, že zobrazenie $\Phi; \forall f \in A^{B\cup C}; \Phi(f) = (f_1, f_2)$ je injektívne. Zobrazenie Ψ skonštruujeme podobným spôsobom. Nech $(g, h) \in A^B \times A^C$; t.j. g, h sú ľubovoľné zobrazenia; $g : B \to A$ a $h : C \to A$. Zobrazenie Ψ priradí dvojici zobrazení (g, h) zobrazenie f, $f : B \cup C \to A$ kde f je definované nasledovne

$$f(x) = \begin{cases} g(x) & \forall x \in B; \\ h(x) & \forall x \in C. \end{cases}$$

Zobrazenie Ψ je zrejme injektívne a teda množiny $A^{B\cup C}$ a $A^B \times A^C$ majú rovnakú mohutnosť.

Úloha 8.13. *Dokážte ostatné vlastnosti operácií kardinálnej aritmetiky, ktoré si nevyžadujú platnosť axiómy výberu.*

Príklad 8.3. *Pomocou vyššie uvedených pravidiel vypočítame niekoľko kardinálnych čísel. Budeme pracovať s konkrétnymi prirodzenými číslami, konečnými kardinálnymi číslami* $a_0, \ldots, a_n$, *nekonečnými kardinálnymi číslami* $\aleph_0, \mathcal{C}, \alpha, \beta, \gamma$ *a budeme predpokladať platnosť axiómy výberu.*

1. *Určíme* $\aleph_0^{\aleph_0}$. *Zostrojíme dolný a horný odhad kardinálneho čísla.*

$$\aleph_0^{\aleph_0} \leq \mathcal{C}^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0} = \mathcal{C}$$

Dolný odhad

$$\aleph_0^{\aleph_0} \geq 2^{\aleph_0} = \mathcal{C},$$

preto

$$\aleph_0^{\aleph_0} = \mathcal{C}.$$

2. $$2^{\aleph_0 \cdot 3^{\aleph_0}} = 2^{3^{\aleph_0}} = 2^{2^{\aleph_0}} = 2^{\mathcal{C}}.$$

3. $$2^{\aleph_0} + {\aleph_0}^2 = 2^{\aleph_0} + \aleph_0 = 2^{\aleph_0} = \mathcal{C}.$$

4. $$\left(\aleph_0^5 + \mathcal{C}\right)^{\aleph_0^8} = \left(\aleph_0^5 + \mathcal{C}\right)^{\aleph_0} = (\aleph_0 + \mathcal{C})^{\aleph_0} = \mathcal{C}^{\aleph_0} = \mathcal{C}.$$

5. $$\mathcal{C}^{\mathcal{C}} = 2^{\aleph_0 \cdot \mathcal{C}} = 2^{\mathcal{C}}.$$

6. $$a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \cdots + a_2 n \cdot \alpha^n = a_0 + \alpha + \alpha^2 + \cdots + \alpha^n = \alpha^n.$$

7. *Nech* $\alpha < \beta < \gamma$, *potom*
$$(\alpha + \beta)^\gamma = \beta^\gamma = 2^\gamma.$$

8. *Nech* $\alpha < \gamma < \beta$, *potom*
$$(\alpha + \beta)^\gamma = \beta^\gamma = \beta.$$

9. *Nech* $\alpha < \beta < \gamma$, *potom*
$$(\alpha \cdot \beta)^\gamma = \beta^\gamma = 2^\gamma.$$

10. *Nech* $\alpha < \gamma < \beta$, *potom*
$$(\alpha \cdot \beta)^\gamma = \beta^\gamma = \beta.$$

8.6 Usporiadania nekonečných množín

Pomocou prirodzených čísel možno (okrem iného) vyjadriť veľkosti (konečných) množín a určiť miesto, na ktorom sa nejaký prvok vyskytuje v postupnosti. V prípade konečných množín sú, ako zakrátko ukážeme, pojmy „veľkosť“ a „poradie“, resp. „usporiadanie“ veľmi blízke; v prípade nekonečných množín ich treba odlišovať. Keď sme sa zaoberali veľkosťami (mohutnosťami) nekonečných množín, zovšeobecnením prirodzených čísel sme sa dostali ku kardinálnym číslam. Kardinálne čísla sa spájali s množinami, u ktorých sme abstrahovali od akejkoľvek vnútornej štruktúry; jediné, čo bolo pre kardinálne čísla podstatné, bola mohutnosť množín. Také zovšeobecnenie prirodzených čísel, ktoré umožňuje určovať poradie/usporiadanie v konštrukciách, v ktorých vystupujú nekonečné množiny, si vyžaduje vhodným spôsobom zovšeobecniť usporiadanie prirodzených čísel. Takýmto zovšeobecnením prirodzených čísel sú tzv. *ordinálne čísla*. V tejto časti definujeme ordinálne čísla a ordinálne typy, budeme sa zaoberať ich vzťahom ku kardinálnym číslam a zavedieme ordinálnu aritmetiku, umožňujúcu vykonávať operácie s ordinálnymi číslami.[8]

8.6.1 Zobrazenia zachovávajúce usporiadanie

Existencia bijekcie medzi dvoma množinami (napr. A, B) nám umožnila vysloviť tvrdenie, že tieto množiny majú rovnaký počet prvkov v prípade konečných množín a rovnakú mohutnosť v prípade nekonečných množín. Ak aj tieto množiny mali nejakú vnútornú štruktúru, pri porovnávaní mohutnosti množin sme ju nezohľadňovali. Rozšírime teraz predpoklady o množinách A, B o (čiastočné) usporiadanie a od konštruovaných zobrazení budeme vyžadovať, aby ho zohľadňovali, t.j. aby napríklad menší prvok množiny A zobrazovali na menší prvok množiny B. Sformulujeme túto požiadavku presnejšie.

Definícia 8.2. *Nech sú* A, B *dve čiastočne usporiadané množiny a*

1. *nech* $f : A \to B$ *je injekcia. Budeme hovoriť, že* zobrazenie f *zachováva usporiadanie, ak*
$$\forall a \forall b[(a, b \in A) \& (a \leq b) \Rightarrow (f(a) \leq f(b))];$$
2. *Nech* $f : A \to B$ *je bijekcia. Budeme hovoriť, že* f *je* izomorfizmus *(alebo* podobnosť*) čiastočne usporiadaných množín* A, B*, ak*
$$\forall a \forall b[(a, b \in A) \& (a \leq b) \Leftrightarrow (f(a) \leq f(b))].$$
Čiastočne usporiadané množiny A, B*, pre ktoré existuje izomorfizmus nazývame* izomorfnými *alebo* podobnými *množinami.*

V teórii množín zohráva kľúčovú úlohu špeciálne usporiadanie, nazývané dobrým usporiadaním, ktoré sme už spomenuli v kapitole 6 .

[8] pri písaní tejto časti sme popri klasickej monografii [4] a učebniciach [13] a [3] vychádzali zo zdrojov uverejnených na internete, najmä článkov wikipedie

Definícia 8.3. *Nech je daná množina* A *s čiastočným usporiadaním* R. *Budeme hovoriť, že čiastočné usporiadanie* R *je dobré usporiadanie, ak každá podmnožina množinay* A *má najmenší prvok. Množinu* A *budeme nazývať* dobre usporiadanou množinou *práve vtedy, ak existuje nejaké dobré usporiadanie na množine* A

Ukážkovým príkladom dobre usporiadanej množiny je množina prirodzených čísel $\mathbb{N}$ s „prirodzeným“ usporiadaním. Na druhej strane, už množina celých čísel $\mathbb{Z}$ nie je dobre usporiadaná pomocou prirodzeného usporiadania $\leq$, lebo množina všetkých záporných čísel nemá najmenší prvok. Keďže $\mathbb{Z}$ je podmnožinou racionálnych, reálnych a komplexných čísel, ani jedna z množín $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ nemôže byť dobre usporiadaná prirodzeným usporiadaním. Ak by sme zobrali namiesto $\mathbb{Z}$ jej podmnožinu $\{j; j \in \mathbb{Z} \& j > m\}$ s prirodzeným usporiadaním a ľubovoľným celým (alebo reálnym) číslom m, táto množina už bude dobre usporiadanou. Dobrému usporiadaniu množiny $\mathbb{Z}$ prirodzeným usporiadaním prekážalo to, že postupnosť $-1, -2, -3 \ldots$ nebola zdola ohraničená. Problémy nemusia spôsobovať len množiny prvkov postupností, ktorých limita je $-\infty$. S dobrým usporiadaním môžu mať problém aj na prvý pohľad bezproblémové ohraničené množiny. Ako príklad uvedieme množinu racionálnych čísel $\mathbb{Q}_1$ z intervalu $\langle 0, 1\rangle$ s prirodzeným usporiadaním $\leq$. Predpokladajme, že $\mathbb{Q}_1$ je dobre usporiadaná, t.j. že každá jej podmnožina má najmenší prvok. Uvažujme teraz množinu $\mathbb{Q}_2$ racionálnych čísel z otvoreného intervalu $(0, 1)$ a predpokladajme, že r je najmenším prvkom tejto množiny. Je zrejmé, že $r \neq 0$, ale potom $r/2 \neq 0$ je tiež nenulové racionálne číslo patriace do množiny $\mathbb{Q}_2$ a menšie ako jej najmenší prvok r. Spor. Usporiadanie $\leq$ nie je dobrým usporiadaním na množine $\mathbb{Q}_1$, resp. množina $\mathbb{Q}_1$ nie je dobre usporiadaná usporiadaním $\leq$. Pozorní čitatelia si iste všimli, že vlastnosť usporiadania „byť dobrým usporiadaním“ nie je absolútna. Rovnako definované usporiadanie môže byť dobrým usporiadaním pre jednu množinu, zatiaľ čo pre inú množinu túto vlastnosť nemá.[9] Podobne to je s množinami, to že jedno usporiadanie prvkov množiny nie je dobré ešte neznamená, že množina nie je dobre usporiadateľná pomocou iného usporiadania. Jeden z trochu prekvapujúcich výsledkov teórie množín hovorí o tom, že každú množinu možno dobre usporiadať.

Ilustrujeme ešte pojem zobrazenia zachovávajúceho usporiadanie [13]. Ako množinu B uvažujeme množinu prirodzených čísel $\mathbb{N}$ s prirodzeným usporiadaním ($a \geq b$ práve vtedy, ak $a - b \geq 0$.) Množinou A bude množina prirodzených čísel $\mathbb{N}$ s čiastočným usporiadaním definovaným takto $(a \preceq b) \Leftrightarrow (a$ je deliteľom $b)$. Identické zobrazenie $f : A \to B$ zachováva usporiadanie, ale nie je bijekciou, pretože napríklad $3 \leq 5$, ale $3 \not\preceq 5$, nakoľko číslo 3 nie je deliteľom čísla 5.

8.6.2 Ordinálne typy

Uvažujme teraz všetky čiastočne usporiadané množiny. Keďže ich príliš veľa na to, aby mohli tvoriť množinu, pomožeme si tým, že súbor všetkých čiastočne usporiadaných množín budeme považovať za triedu.[10] Triedu všetkých čiastočne usporiadaných množín

[9] keď sa však na usporiadanie dívame ako na reláciu na množine, tento problém nenastáva. Napríklad prirodzené usporiadania $\leq$ množín reálnych, racionálnych, celých a prirodzených čísel sú rôzne, pretože predstavujú rôzne množiny usporiadaných dvojíc. Na druhej strane, $\leq$ napr. na celých číslach je zúžením relácie usporiadania $\leq$ definovaného na racionálnych, či reálnych číslach.

[10] to bude chcieť nejakú poznámku o triedach a ich vzťahu k množinám

môžeme rozložiť na časti (stále ešte príliš veľké na to, aby mohli byť množinami) tak, že v jednej „podtriede“ sa budú nachádzať všetky čiastočne usporiadané množiny, ktoré sú izomorfné. Dá sa ľahko ukázať, že takéto rozdelenie triedy všetkých čiastočne usporiadaných množín má všetky vlastnosti rozkladu; jediným problémom je, že rozklad sme definovali na množine a trieda všetkých čiastočne usporiadaných množín nie je množina. Pre naše potreby však nepotrebujeme rozlišovať rozdiely medzi rozkladom množiny a rozkladom triedy. Množiny každej triedy (podtriedy) rozkladu triedy všetkých čiastočne usporiadaných množín majú ten istý typ usporiadania. Každej triede rozkladu priradíme *ordinálny typ*. Skutočnosť, že dve množiny sú z hľadiska svojho usporiadania izomorfné znamená, že majú rovnaký ordinálny typ. Zvláštnym druhom ordinálneho typu je *ordinálne číslo*; to je definované ako ordinálny typ dobre usporiadanej množiny.

8.6.3 Ordinálne čísla

S predstavou ordinálneho čísla ako triedy ekvivalencie dobre usporiadaných množín sa trocha ťažšie pracuje. Preto sa pokúsime zaviesť ordinálne číslo ako nejakú dobre usporiadanú množinu, ktorá bude reprezentovať celú triedu ekvivalentných dobre usporiadaných množín. Od tejto konštrukcie budeme požadovať, aby každá dobre usporiadaná množina bola izomorfná (vzhľadom na usporiadanie) jedinému ordinálnemu číslu. John von Neumann definoval ordinálne číslo ako špeciálnu množinu obsahujúcu všetky ordinálne čísla menšie ako dané ordinálne číslo. Formálne

Definícia 8.4. *Množina S je ordinálnym číslom práve vtedy, ak S je úplne usporiadaná a každý prvok množiny S je zároveň podmnožinou množiny S.*

Všimneme si, že samotná množina S je dobre usporiadaná vzhľadom na reláciu množinovej príslušnosti ($\in$). Dôkaz sa opiera o tzv. axiómu fundovanosti (alebo axiómu regularity), ktorá tvrdí, že žiadna množina nemôže byť prvkom seba samej. (Pozri prílohu 14.1.) Pozrieme sa teraz na to ako budú podľa tejto definície vyzerať najjednoduchšie ordinálne čísla, prirodzené čísla. Položíme

$$\begin{array}{lcll}
0 & = & \emptyset & = \{\} \\
1 & = & \{0\} & = \{\emptyset\} \\
2 & = & \{0,1\} & = \{\emptyset,\{\emptyset\}\}, \\
3 & = & \{0,1,2\} & = \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}, \\
4 & = & \{0,1,2,3\} & = \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\},\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}\}, \\
\vdots & & & \\
n & = & \{0,1,2\ldots,n-1\} & = \ldots
\end{array}$$

Na to, aby sme dokázali, že takto definované ordinálne čísla spĺňajú aj druhú požiadavku (každá dobre usporiadaná množina je izomorfná (vzhľadom na usporiadanie) jedinému ordinálnemu číslu) potrebujeme tzv. *transfinitnú indukciu*.. Prvkami ordinálneho čísla (množiny predstavujúcej ordinálne číslo), sú opäť ordinálne čísla. Uvažujme dve ordinálne čísla α, β; potom $\alpha \in \beta$ práve vtedy, ak $\alpha \subsetneq \beta$ a pre α, β platí práve jeden zo vzťahov $\alpha \in \beta$, alebo $\beta \in \alpha$ alebo $\alpha = \beta$. To znamená, že každá množina ordinálnych čísel je úplne usporiadaná. V skutočnosti platí ešte silnejšie tvrdenie, každá množina ordinálnych čísel je dobre usporiadaná. Tento dôležitý výsledok zovšeobecňuje skutočnosť,

že každá množina prirodzených čísel je dobre usporiadaná a umožňuje nám používať transfinitnú indukciu na ordinálnych číslach. Ďalšou dôležitou vlastnosťou ordinálneho čísla je, že obsahuje všetky ordinálne čísla menšie ako dané ordinálne číslo. Táto vlastnosť sa dá využiť pri dokazovaní mnohých užitočných vlastností ordinálnych čísel. Na ilustráciu uvedieme dve

1. Každá množina A ordinálnych čísle má supremum, ordinálne číslo, ktoré dostaneme zjednotením všetkých ordinálnych čísel množiny A.
2. Druhý príklad naznačuje, že je potrebné zvažovať, ktoré súbory ordinálnych čísel tvoria množiny. Predpokladajme, že súbor všetkých ordinálnych čísel tvorí množinu. Táto množina obsahuje ordinálne čísla, podľa definície ordinálnych čísel by sama mala byť ordinálnym číslom. Ale keďže je zároveň množinou všetkých ordinálnych čísel, potom by ako ordinálne číslo mala byťprvkom seba samej, čo je rozpore s axiómou regularity. (Pozri aj Burali-Fortiho paradox)

Súbor všetkých ordinálnych čísel je teda trieda, ktorá sa zvykne označovať Ord alebo ON (ordinals, resp. ordinal numbers).

Zatiaľ sme uvádzali konkrétne príklady len konečných ordinálnych čísel (prirodzených čísel). Definujeme teraz konečné ordinálne čísla všeobecnejšie, aby sme mohli vymedziť nekonečné (transfinitné) ordinálne čísla. Pripománame, že ordinálne číslo je definované ako množina (ordinálnych čísel).

Definícia 8.5. *Ordinálne číslo je konečné práve vtedy, ak každá z jeho podmnožín má najväčší prvok.*

Nekonečné (transfinitné) ordinálne čísla budú potom tie ordinálne čísla, ktoré nie sú konečné.

V predchádzajúcich riadkoch sme niekoľkokrát spomenuli transfinitnú indukciu ako prostriedok na dokazovanie základných vlastností ordinálnych čísel. V nasledujúcej časti ju zavedieme formálne.

8.6.4 Transfinitná indukcia

Transfinitná indukcia je zovšeobecnením matematickej indukcie definovanej na množine prirodzených čísel.

Definícia 8.6. *Nech je* P *nejaká vlastnosť definovaná pre ordinálne čísla. Ak pre každé ordinálne číslo* $\beta < \alpha$ *platí* $P(\beta)$*, tak potom platí aj* $P(\alpha)$.

Matematickú indukciu často používame v obrátenom garde - namiesto toho, aby sme dokazovali platnosť bázy indukcie a na základe nej a indukčného predpokladu dokázali platnosť nejakého tvrdenia pre všetky prirodzené čísla, definujeme rekurentný vzťah, ktorý nám umožní vyjadriť riešenie väčšieho problému pomocou menších problémov toho istého typu a nájdeme riešenie pre najmenší možný prípad problému. Podobný postup, tzv. *transfinitnú rekurziu* budeme používať napríklad na definovanie operácií nad ordinálnymi číslami.

8.6.5 Nasledovníci a limitné ordinálne čísla

Každé nenulové ordinálne číslo má najmenší prvok a môže a nemusí mať najväčší prvok. Napríklad, ordinálne číslo 30 má najväčší prvok 29 a ordinálne číslo $\omega + 7$ má najväčší prvok $\omega + 6$. Na druhej strane ω nemá najväčší prvok, lebo najväčšie prirodzené číslo neexistuje. Ak má ordinálne číslo najväčší prvok α, tak potom existuje ordinálne číslo nasledujúce za α, ktoré sa nazýva *nasledovníkom ordinálneho čísla* α a označuje sa $\alpha+1$. Ak využijeme von Neumannovu definíciu ordinálneho čísla, tak nasledovníkom ordinálneho čísla α je ordinálne číslo $\alpha \cup \{\alpha\}$. Na druhej strane, ordinálne číslo α sa nazýva predchodcom ordinálneho čísla $\alpha + 1$. V závislosti na tom, či ordinálne číslo má alebo nemá predchodcu možno triedu ON rozdeliť na dve disjunktné časti.

Definícia 8.7. *Ordinálne číslo α sa nazýva*

1. izolované*, ak $\alpha = 0$ alebo existuje ordinálne číslo β také, že $\alpha = \beta \cup \{\beta\}$, t.j. predchodca ordinálneho čísla α;*
2. limitné*, ak je nenulové a nemá predchodcu.*

Každé prirodzené číslo je izolované a ω je limitné ordinálne číslo. Ordinálne číslo $\omega + 1$ je izolované ordinálne číslo, ale nie je to prirodzené číslo.

8.7 Ordinálna aritmetika

Pojem *ordinálna aritmetika* označuje operácie s ordinálnymi číslami. V teórii množín sa bežne používajú tri základné operácie na ordinálnych číslach - sčítanie, násobenie a umocňovanie ordinálnych čísel. Tieto operácie sa dajú zaviesť buď pomocou explicitnej konštrukcie dobre usporiadanej množiny, alebo pomocou tzv. transfinitnej indukcie. Využijeme obe možnosti.

Súčet ordinálnych čísel Zjednotenie dvoch disjunktných dobre usporiadaných množín A, B možno dobre usporiadať; t.j. ordinálnym typom množiny $A \cup B$ je ordinálne číslo. Nech α je ordinálne číslo množiny A, β—ordinálne číslo množiny B a γ je ordinálne číslo množiny $A \cup B$, potom súčet ordinálnych čísel definujeme nasledovne

$$\alpha + \beta = \gamma.$$

Prípad dobre usporiadaných množín A, B, ktoré nie sú disjunktné ($A \cap B \neq \emptyset$) vyriešime podobne ako v kardinálnej aritmetike; namiesto množín A, B použijeme napríklad množiny $A \times \{0\}, B \times \{1\}$. Je zrejmé, že $A \times \{0\}$ má ordinálny typ (ordinálne číslo) α a $B \times \{1\}$ má ordinálny typ (ordinálne číslo) β a že $A \times \{0\} \cap B \times \{1\} = \emptyset$.

Usporiadanie množiny $A \cup B$ bude vyzerať tak, že najprv budú uvedené všetky prvky množiny A v poradí danom dobrým usporiadaním množiny A a za nimi budú nasledovať všetky prvky množiny B v poradí danom dobrým usporiadaním množiny B. To znamená,

že každý prvok množiny B je väčší ako ľubovoľný prvok množiny A. Súčet ordinálnych čísel bude zrejme asociatívny, ale ako to bude vyzerať s komutatívnosťou? V prípade konečných množín bude súčet ordinálnych čísel komutatívny. Skutočne, ak $|A| = n, |B| = m$ a

$$A = \{a_1, \dots, a_n; a_1 < a_2 < \cdots < a_n\}, \quad B = \{b_1, \dots, b_m; b_1 < b_2 < \cdots < b_m\}$$

tak bijekcia $f : A \cup B \to B \cup A$ zachovávajúca usporiadanie je definovaná nasledovne (bez ujmy na všeobecnosti môžeme predpokladať, že $m \leq n$)

$$\begin{array}{lccccccccc} A \cup B & a_1 & a_2 & \dots & a_m & a_{m+1} & \dots & a_n & b_1 & \dots & b_m \\ & \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow \\ B \cup A & b_1 & b_2 & \dots & b_m & a_1 & \dots & a_{n-m} & a_{n-m+1} & \dots & a_n \end{array}$$

Uvažujme teraz prvé transfinitné ordinálne číslo, ω, ordinálne číslo množiny prirodzených čísel $\mathbb{N}$ a preskúmajme súčty ordinálnych čísel $1 + \omega$ a $\omega + 1$. Vychádzajúc z definície súčtu ordinálnych čísel $1 + \omega$ predstavuje ordinálne číslo zjednotenia jednoprvkovej množiny (napríklad $\{a\}$) a množiny s ordinálnym číslom ω, napríklad množiny $\mathbb{N}$. Prvky množiny $\{a\} \cup \mathbb{N}$ budú potom usporiadané nasledovne $a < 0 < 1 < 2 < \dots$. Dá sa ľahko nahliadnuť, že táto množina je izomorfná s množinou $\mathbb{N}$. Potrebná bijekcia je jednoduchá:

$$f : \{a\} \cup \mathbb{N} \to \mathbb{N}; \qquad \begin{cases} f(a) = 0; \\ f(k) = k + 1; \quad \forall k \in \mathbb{N}. \end{cases}$$

To znamená, že $1 + \omega = \omega$. Na druhej strane,$\omega + 1$ predstavuje ordinálne číslo množiny $\mathbb{N} \cup \{a\}$, ktorej prvky sú usporiadané takto:

$$0 < 1 < 2 < \cdots < n \cdots < a.$$

Táto množina obsahuje prvok a, ktorý je väčší ako ľubovoľné prirodzené číslo. To znamená, že $1 + \omega \neq \omega + 1$ a súčet ordinálnych čísel nie je komutatívny (!). Vo všeobecnosti pre ľubovoľné ordinálne číslo $\alpha + 1 \neq \alpha$. Ordinálne číslo $\alpha + 1$ budeme v ordinálnej aritmetike často používať a preto preň zavedieme zvláštne označenie. Nech α je ľubovoľné ordinálne číslo potom ordinálne číslo $\alpha + 1$ budeme nazývať *nasledovníkom ordinálneho čísla* α.

Trocha zovšeobecníme predchádzajúci príklad. Ak namiesto jednoprvkovej množiny A zoberieme ľubovoľnú dobre usporiadanú konečnú množinu $|A| = n$, tak podobne ako pre jednoprvkovú množinu dokážeme, že $n+\omega = \omega$. Ordinálne číslo $\omega+n$ bude reprezentovať ordinálny typ množiny $\mathbb{N} \cup A$, ktorej prvky sú usporiadané nasledovne:

$$0 < 1 < 2 < \cdots < n \cdots < a_1 < a_2 < \cdots < a_n.$$

Aj v tomto prípade bude existovať najväčší prvok (a_n) a ľubovoľný prvok množiny A bude väčší ako ľubovoľné priridzené číslo; samotné prvky množiny A budú v množine $\mathbb{N} \cup A$ usporiadané podľa usporiadania v množine A. Pre ľubovoľné prirodzené číslo n teda platí $n + \omega = \omega$. Čo sa však stane, ak namiesto konečného ordinálneho čísla n zoberieme transfinitiné? Zatiaľ poznáme jediné transfinitné ordinálne číslo, a to je ω. Súčet $\omega + \omega$ bude reprezentovať ordinálne číslo dvoch množín, izomorfných množine $\mathbb{N}$. Aby sme nekomplikovali označenie a zároveň zachovali požiadavku disjunktnosti

oboch množín, budeme prvky oboch množín označovať pomocou prirodzených čísel a prvky druhej množiny odlišovať čiarkami. Ordinálne číslo $\omega + \omega$ predstavuje množinu usporiadanú nasledovne

$$0 < 1 < 2 < \cdots < 0' < 1' < \ldots$$

Zaujímavosťou tohto usporiadania je, že existujú dva prvky, ktoré nemajú priameho predchodcu[11], a to prvky $0, 0'$.

Ako sme už spomenuli na začiatku tejto časti, aritmetické operácie na ordinálnych číslach možno zaviesť aj pomocou transfinitnej indukcie. Pri prvom čítaní čitateľ môže nasledujúcu časť vynechať a pokračovať na označenom mieste.

Pripomenieme, že limitným ordinálnym číslom je transfinitné ordinálne číslo, ktoré nemá priameho predchodcu. Nech sú α, β ľubovoľné ordinálne čísla, potom

1. $\alpha + 0 = \alpha$,
2. $\alpha + (\beta + 1) = (\alpha + \beta + 1)$
3. ak je δ limitné transfinitné ordinálne číslo, tak potom $\alpha + \delta$ je limitným ordinálnym číslom ordinálne čísla $\alpha + \beta$ pre všetky ordinálne čísla $\beta < \delta$.

Koniec preskakovania.

Zhrnieme základné vlastnosti sčítania ordinálnych čísel. Symboly α, β, γ označujú ľubovoľné ordinálne čísla.

1. Obojstranným neutrálnym prvkom pre sčítanie ordinálnych čísel je 0:
$$\alpha + 0 = 0 + \alpha = \alpha.$$
2. Sčítanie ordinálnych čísel je asociatívne:
$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$
3. Sčítanie ordinálnych čísel vo vvšeobecnosti nie je komutatívne
$$\exists \alpha, \beta [(\alpha + \beta) \neq (\beta + \alpha)]$$
4. Sčítanie ordinálnych čísel je ostro rastúce vzhľadom na pravý argument

Úloha 8.14. *Zistite, prečo nie je sčítanie ordinálnych čísel ostro rastúce aj pre ľavý argument; t.j. prečo neplatí*

$$\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma.$$

Pre ordinálne čísla vo všeobecnosti nemožno definovať odčítanie. Ale pre sčítanie platí

$$\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma.$$

Úloha 8.15. *Dokážte uvedené tvrdenie a zistite, prečo neplatí podobné tvrdenie*

$$\beta + \alpha = \gamma + \alpha \Rightarrow \beta = \gamma.$$

Napokon, ak $\alpha \leq \beta$ tak potom existuje jediné ordinálne číslo γ také, že $\beta = \alpha + \gamma$.

[11] priamym predchodcom prvku a je prvok b taký, že $b + 1 = a$.

Súčin ordinálnych čísel Uvažujme dve dobre usporiadané množiny A, B s ordinálnymi číslami α, resp. β. Karteziánsky súčin $A \times B$ je tiež dobre usporiadaná množina. Na jej usporiadanie využijeme modifikovaný variant[12] *lexikografického usporiadania* , definovaného pomocou usporiadaní množín A, B; $<_A$, resp. $<_B$ nasledovne

$$(a_1, b_1) < (a_2, b_2) \Leftrightarrow \begin{cases} b_1 <_B b_2; & \text{alebo} \\ (b_1 = b_2) \& (a_1 <_A a_2). \end{cases}$$

Súčin ordinálnych čísel $\alpha \cdot \beta$ definujeme ako ordinálny typ (ordinálne číslo) karteziánskeho súčinu $A \times B$ dobre usporiadaných množín A, B. Pozrieme sa teraz na niektoré zaujímavé prípady súčinov ordinálnych čísel, potom zavedieme násobenie ordinálnych čísel pomocou transfinitnej indukcie a nakoniec zhrnieme najdôležitejšie vlastnosti násobenia ordinálnych čísel.

V prípade konečných ordinálnych čísel α, β ich násobenie zodpovedá násobeniu prirodzených čísel. Preskúmanie tohto prípadu ponecháme čitateľovi ako cvičenie. Predpokladajme, že jedno z ordinálnych čísel α, β je transfinitné a druhé je konečné. Vzhľadom na definíciu násobenia ordinálnych čísel a vlastnosti karteziálnskeho súčinu nemá zmysel zaoberať sa prípadom, keď je jedno z ordinálnych čísel nulové. Prípad, keď je jedno z ordinálnych čísel vystupujúcich v súčine rovné 1 takisto ponechávame na čitateľa a budeme predpokladať, že $\beta = 2$. Kvôli jednoduchosti položíme $\alpha = \omega$. Čo zodpovedá súčinu $\omega \cdot 2$? Predpokladajme, že množina $B = \{0, 1\}$, potom prvky karteziánskeho súčinu $A \times B$ usporiadame takto

$$(0,0) < (1,0) < (2,0) < \cdots < (0,1) < (1,1) < (2,1) < \ldots$$

a vidme, že $\omega \cdot 2 = \omega + \omega$. Bude násobenie ordinálnych čísel komutatívne? Súčinu $2 \cdot \omega$ zodpovedá karteziánsky súčin $B \times A$, ktorého prvky možno usporiadať takto:

$$(0,0) < (1,0) < (0,1) < (1,1) < (0,2) < (1,2) < \ldots$$

Z uvedeného vyplýva, že karteziánsky súčin $B \times A$ má ordinálne číslo ω, a teda súčin ordinálnych čísel nie je komutatívny. Keďže pre ordinálne čísla je definované násobenie aj sčítanie, prirodzenou otázkou bude, či platí distributívny zákon. Odpoveď znie, čiastočne. Pre ľubovoľné ordinálne čísla α, β, γ platí

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma,$$

ale rovnosť

$$(\beta + \gamma) \cdot \alpha = \beta \cdot \alpha + \gamma \cdot \alpha$$

vo všeobecnosti neplatí. Stačí uvážiť prípady, ktorými sme sa už zaoberali:

$$(1+1) \cdot \omega = 2 \cdot \omega = \omega \quad \text{a} \quad 1 \cdot \omega + 1 \cdot \omega = \omega + \omega \neq \omega.$$

Pri prvom čítaní preskoč!

Definícia násobenia ordinálnych čísel pomocou transfinitnej indukcie.

[12] lexikografické alebo slovníkové usporiadanie je definované pre reťazce znakov nerovnakej dĺžky. Pri stanovovaní ich poradia dáva najväčšiu váhu prvému prvku z ľava, potom porovnáva reťazce s rovnakým prvým prvkom podľa druhého prvku, atď. Retazce nerovnakej dĺžky sú doplnené medzerami, ktoré sa považujú za najmenšie prvky množiny znakov. V našom prípade majú všetky reťazce dĺžku 2 a najvýznamnejší prvok je prvý prvok z prava. Lexikografickým usporiadaním sa ešte budeme zaoberať v kapitole 13

1. $\alpha \cdot 0 = 0$,
2. $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \beta$,
3. ak je δ limitné ordinálne číslo, súčin $\alpha \cdot \delta$ je limitným ordinálnym číslom čísel $\alpha \cdot \gamma$, kde $\gamma < \delta$.

Zhrnieme v prehľadnej forme vlastnosti násobenia ordinálnych čísel. Ak nebude uvedené iné, predpokladáme, že α, β, γ sú ľubovoľné ordinálne čísla.

Odtiaľto pokračuj v čítaní.

1. $\alpha \cdot 0 = 0 \cdot \alpha = 0$,
2. ordinálne číslo 1 je obojstranným neutrálnym prvkom vzhľadom na násobenie ordinálnych čísel $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$,
3. Násobenie ordinálnych čísel je asociatívne $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$,
4. Násobenie ordinálnych čísel nie je komutatívne
5. Násobenie ordinálnych čísel je ostro rastúce vzhľadom na pravý argument

$$(\alpha < \beta) \& (\gamma \neq 0) \Rightarrow (\gamma \cdot \alpha < \gamma \cdot \beta),$$

6. Násobenie ordinálnych čísel je rastúce (ale nie ostro rastúce !) vzhľadom na ľavý argument

$$(\alpha < \beta) \Rightarrow (\gamma \cdot \alpha \leq \gamma \cdot \beta)$$

7. Krátenie **ľavého** činiteľa súčinu

$$(\alpha > 0) \& (\alpha \cdot \beta = \alpha \cdot \gamma) \Rightarrow \beta = \gamma,$$

ale

8. nemožno krátiť **pravého** činiteľa súčinu.
9. Pre násobenie ordinálnych čísel platí distributívny zákon zľava ale nie sprava;

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

napríklad

$$(\omega + 1) \cdot 2 = (\omega + 1) + (\omega + 1) = \omega + \omega + 1 = \omega \cdot 2 + 1 \neq \omega \cdot 2 + 2.$$

10. Uvedieme ešte jednu zaujímavú vlastnosť ordinálnych čísel, pripomínajúcu delenie so zvyškom prirodzených čísel. Pre ľubovoľné dve ordinálne čísla $\alpha, \beta; \beta > 0$ existujú jediné dve ordinálne čísla γ, δ také, že

$$\alpha = \beta \cdot \gamma + \delta, \quad \delta < \beta.$$

Umocňovanie ordinálnych čísel Umocňovanie ordinálnych čísel je najzložitejšia z operácií ordinálnej aritmetiky, ktorými sa zaoberáme. Nech sú A, B dobre usporiadané množiny s ordinálnymi číslami α, resp. β. Ordinálne číslo α^β definujeme ako ordinálny typ (ordinálne číslo) dobre usporiadanej množiny A^B; množiny všetkých zobrazení z množiny B do množiny A. Aby sme si utvorili predstavu o tom, ako budú usporiadané prvky množiny A^B pozrieme sa najprv na konkrétne jednoduchšie prípady. Ak je ordinálne číslo v exponente konečné, môžeme umocňovanie ordinálnych čísel definovať priamo pomocou násobenia ordinálnych čísel: napríklad $\omega^2 = \omega \cdot \omega$. To je prípad, ktorý sme už rozoberali. Teraz sa na ordinálne číslo ω^2 pozrieme v súlade s tým, ako sme zaviedli umocňovanie ordinálnych čísel; t.j. ako na ordinálny typ množiny všetkých zobrazení z dvojprvkovej množiny do množiny s ordinálnym číslom ω, napríklad do množiny $\mathbb{N}$. Uvažujeme dvojprvkovú množinu $B = \{0, 1\}$. Ľubovoľné zobrazenie $f : B \to \mathbb{N}$ možno jednoznačne zadať vymenovaním dvoch dvojíc $(0, f(0))$, $(1, f(1))$. Ak využijeme dobré usporiadanie množiny B, tak tú istú funkciu môžeme zadať dvojicou funkčných hodnôt $f(0), f(1)$, t.j. dvojíc prirodzených čísel. Množinu usporiadaných dvojíc sme už raz dobre usporiadali pomocou mierne modifikovaného lexikografického usporiadania, ktoré usporadúvalo dvojice najprv podľa druhého a až potom podľa prvého prvku. Uvedieme dobré usporiadanie zobrazení $f : B \to \mathbb{N}$ najprv v skrátenom zápise a potom pomocou tabuľky:

$$(0,0) < (1,0) < (2,0) < (3,0) < \cdots < (0,1) < (1,1) < (2,1) < \ldots (0,2) < (1 < 2) < \ldots$$

x	$f_{0,0}$	$f_{1,0}$	$f_{2,0}$	$f_{3,0}$	$\ldots$	$f_{0,1}$	$f_{1,1}$	$f_{2,1}$	$f_{3,1}$	$\ldots$	$f_{0,2}$	$f_{1,2}$	$f_{2,2}$	$f_{3,2}$	
0	0	1	2	3	$\ldots$	0	1	2	3	$\ldots$	0	1	2	3	$\ldots$
1	0	0	0	0	$\ldots$	1	1	1	1	$\ldots$	2	2	2	2	$\ldots$

Podobne by sme postupovali, ak by exponent ordinálneho čísla bolo prirodzené číslo (konečné ordinálne číslo) n. Napríklad ω^n bude predstavovať ordinálne číslo množiny všetkých zobrazení z n-prvkovej množiny (napríklad) do množiny $\mathbb{N}$. Každé také zobrazenie sa dá zapísať pomocou tabuľky, ktorá bude mať 2 riadky a $n + 1$ stĺpcov (vrátane záhlavia). Bez ujmy na všeobecnosti môžeme n-prvkovú dobre usporiadanú množinu reprezentovať množinou prirodzených čísel $\{0, 1, \ldots, n-1\}$. Tabuľka zadávajúca funkciu $f : \{0, 1, \ldots, n-1\} \to \mathbb{N}$ bude vyzerať nasledovne

x	0	1	2	3	$\ldots$	$n-1$
f(x)	f(0)	f(1)	f(2)	f(3)	$\ldots$	$f(n-1)$

Takáto funkcia je jednoznačne zadaná n-ticou svojich hodnôt (pravda za predpokladu, že budeme dodržiavať konvenciu, že 1. prvok usporiadanej n-tice je funkčná hodnota $f(0)$, druhý predstavuje $f(1)$, atď., až napokon posledný prvok n-tice predstavuje funkčnú hodnotu $f(n-1)$.) Usporiadané n-tice prirodzených čísel dokážeme dobre usporiadať pomocou modifikovaného lexikografického usporiadania.

Čo však spravíme v prípade, keď aj základ aj exponent mocniny ordinálnych čísel budú transfinitné ordinálne čísla? Naša intuícia pravdepodobne zlyhá, ak sa pokúsime takýmto spôsobom reprezentovať napríklad už ordinálne číslo ω^ω. Zobrazenia z množiny $\mathbb{N}^\mathbb{N}$ môžeme síce reprezentovať pomocou postupností prirodzených čísel, ale ak sa ich

pokúsime usporiadť pomocou lexikografického usporiadania, zistíme, že usporiadanie nemá vlastnosti dobrého usporiadania. Musíme prijať predpoklad, že konečný počet prvkov v postupnosti (hodnôt funkcie) je nenulových. Takéto postupnosti budú reprezentovať prirodzené čísla.

Pri prvom čítaní preskoč!

Aj umocňovanie ordinálnych čísel je možné definovať induktívne (vzhľadom na exponent β). Nech sú α, β ľubovoľné ordinálne čísla, potom

1. $\alpha^0 = 1$,
2. $\alpha^{\beta+1} = (\alpha^\beta) \cdot \alpha$,
3. a ak δ je limitné ordinálne číslo, tak potom α^δ je limitné ordinálne číslo α^β, kde $\beta < \delta$.

Pokračuj.

Zhrnieme základné vlastnosti umocňovania ordinálnych čísel. Ak nebude uvedené iné, predpokladáme, že α, β, γ sú ľubovoľné ordinálne čísla.

1. $\alpha^0 = 1$.
2. Ak $0 < \alpha$, tak potom $0^\alpha = 0$.
3. $1^\alpha = 1$
4. $\alpha^1 = \alpha$
5. Umocňovanie ordinálnych čísel je ostro rastúce a spojité vzhľadom na pravý argument
$$(\gamma > 1)\&(\alpha < \beta) \Rightarrow \gamma^\alpha < \gamma^\beta.$$
6. $(\alpha \leq \beta) \Rightarrow (\alpha^\gamma \leq \beta^\gamma)$
7. $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$
8. $\left(\alpha^\beta\right)^\gamma = \alpha^{\beta\cdot\gamma}$
9. Ak $\alpha > 1$ a $\alpha^\beta = \alpha^\gamma$, tak potom $\beta = \gamma$
10. Pre ľubovoľné ordinálne čísla α, β platí: ak $1 < \beta \leq \alpha$, tak potom existujú jediné ordinálne čísla γ, δ, ρ také, že
$$\alpha = \beta^\gamma \cdot \delta + \rho$$
a $0 < \delta < \beta$ a $\rho < \beta^\gamma$.

8.8 Vzťah ordinálnych a kardinálnych čísel

Každému ordinálnemu číslu možno jednoznačne priradiť kardinálne číslo, ktoré vyjadruje jeho mohutnosť (pripomíname, že ordinálne číslo sme definovali ako špecifickú množinu). Všetky dobre usporiadané množiny, ktoré majú ten istý ordinálny typ (to isté ordinálne číslo), majú aj rovnakú mohutnosť. (Opačné tvrdenie zrejme neplatí, stačí zobrať $\omega, \omega + 1$.) Najmenšie ordinálne číslo s danou kardinalitou sa nazýva *počiatočným ordinálnym číslom daného kardinálneho čísla*. Každé konečné ordinálne číslo je zároveň počiatočným ordinálnym číslom, ale väčšina nekonečných ordinálnych čísel nie. Jedno z tvrdení, akvivalentných axióme výberu hovorí, že každú množinu možno dobre usporiadať. To znamená, že každému kardinálnemu číslu prislúcha práve jedno počiatočné ordinálne číslo. Kardinálne čísla teda môžeme považovať (za predpokladu, že prijímame axiómu výberu) za počiatočné ordinálne čísla. Na druhej strane pri operáciách s kardinálnymi a ordinálnymi číslami je potrebné striktne rozlišovať, ktorú aritmetiku používame. Napríklad ordinálne umocňovanie sa podstatne odlišuje od kardinálneho; $2^{\omega} = \omega$, ale $2^{\aleph_0} = \mathcal{C}$ čo je kardinálne číslo väčšie ako $\aleph_0$.

8.9 *Historické poznámky

Teória množín výrazne prispela k rozvoju modernej matematiky. Po jej vytvorení koncom 19. a začiatkom 20. storočia sa nejaký čas zdalo, že to je tá dlho hľadaná teória, na ktorej bude možné vybudovať matematiku zbavenú nepresností a paradoxov. Hoci sa tento predpoklad nenaplnil, teória množín poskytla matematike pomerne univerzálny jazyk, v ktorom je možné nielen vytvárať matematické teórie, ale aj formulovať matematické problémy a hľadať ich riešenia. Nespochybniteľnou zásluhou teórie množín je prehĺbenie chápania pojmu nekonečna v matematike.[13]

Už samotná história vzniku teórie množín je výnimočná. Kým iné matematické teórie sa vyvíjali dlhodobo a na ich budovaní sa podieľalo viacero ľudí, teóriu množín vytvoril v relatívne krátkom čase jeden človek, Georg Cantor. Skôr ako sa pozrieme na Cantorovu prácu na budovaní základov teórie množín, pripomenieme niektoré dávnejšie výsledky súvisiace s nekonečnom a množinami.

Idea nekonečna priťahovala ľudí už od antických čias. Zenon z Elea (okolo 450 p.n.l.) formuloval niekoľko paradoxov založených na pojme nekonečna[14]. Už v stredoveku viedli diskusie o nekonečne k porovnávaniu (vyjadrené v súčasnej terminológii) nekonečných množín. Albert Saský[15] dokonca dokázal, že priamka má rovnakú mohutnosť ako trojrozmerný priestor (!) Vo vývoji matematiky dlhý čas zohrávala veľmi dôležitú úlohu matematická analýza. Ale až do polovice 19. storočia sa dôkazy základných viet analýzy odvolávali na geometrickú názornosť. Neexistovala korektná teória reálnych čísel a hoci sa nekonečne veľké a nekonečne malé veličiny používali v difer-

[13] Teória množín rieši problémy presahujúce rámec tejto knižky. Väčšinou z náročnejších problémov sa nebudeme zaoberať, na elementárnej úrovni sme sa dotkli dôležitých pojmov mohutnosti a usporiadania množín (kapitola 8).

[14] najznámejší je pravdepodobne paradox Achilles a korytnačka

[15] v práci Questiones subtilissime in libros de celo et mundi

enciálnom a integrálnom počte, nekonečno sa objavovalo len v podobe potenciálneho nekonečna. Prvý významnejší pokus o zmenu podnikol veľký filozof a matematik 19. storočia, Bernard Bolzano. Ten zaviedol pojem „množiny“ už v roku 1847 ako

> an embodiment of the idea or concept which we conceive when we regard the arrangement of its parts as a matter of indifference.

Bolzano obhajoval aj pojem nekonečnej množiny v čase, keď si mnohí matematici mysleli, že nekonečné „množiny“ nemôžu existovať. Sám veľký K.F.Gauss napísal

> Nekonečno nemožno v matematike použiť ako niečo definitívne, je to len spôsob vyjadrenia, ktorý označuje istú hranicu, ku ktorej sa môžu niektoré veličiny neobmedzene blížiť, kým iné veličiny rastú neobmedzene.

Nekonečné množiny predstavujú inú „aktuálnu“ podobu nekonečna. Bolzano uvádzal príklady množín, pre ktoré na rozdiel od konečných množín bolo možné zostrojiť bijektívne zobrazenie medzi danou množinou a niektorou z jej vlastných podmnožín. Táto myšlienka sa využíva pri definícii konečných množín.

Na Bolzanove výsledky nenadviazal žiaden z jeho žiakov. Až s odstupom 20 rokov sa podobnými problémami začal zaoberať Georg Cantor, ktorý teóriu množín postavil na matematickom základe. Cantor sa pôvodne zaoberal teóriou čísel a pre jeho ďalšiu prácu malo rozhodujúúci význam stretnutie a priateľstvo s Richardom Dedekindom. Dedekindovo abstraktné logické myslenie výrazne ovplyvnilo Cantora a jeho spôsob myslenia. Cantor prešiel od teórie čísel ku skúmaniu trigonometrických radov. Jeho práce z toho obdobia obsahujú prvé idey o teórii množín a prvé dôležité výsledky o iracionálnych číslach.[16] V roku 1874 Cantor publikoval článok, v ktorom prišiel s myšlienou existencie aspoň dvoch druhov nekonečna. To bola skutočne revolučná myšlienka, pretože v tých časoch sa buď predpokladalo, že nekonečno neexistuje, alebo že všetky nekonečné súbory majú tú istú veľkosť. Cantor dokázal, že neexistuje bijekcia medzi reálnymi a prirodzenými číslami. V ďalších prácach Cantor zaviedol pojem ekvivalencie množín (prostredníctvom bijekcie medzi množinami) a ukázal ekvivalenciu množín $\mathbb{R}^n$ a $\mathbb{R}$. Prácu na základoch teórie množín zavŕšil pojednaniami, v ktorých zaviedol dobre usporiadané množiny, ordinálne typy a ordinálne čísla a ordinálnu aritmetiku. Koncom 90-tych rokov 19. storočia publikoval Cantor dve práce v ktorých podáva ucelený výklad teórie množín. V týchtop prácach sa nachádza aj veta, v súčasnosti známa ako Cantor Bernsteinova veta, ktorú nezávisle na Cantorovi dokázal aj Felix Bernstein a E. Schröder.

Cantorove neformálne „definície“ množinových pojmov spočiatku postačovali na konštrukciu dôkazov v novej teórii (množín) a všeobecne sa predpokladalo, že neformálne pojmy bude v prípade potreby možné ľahko formalizovať pomocou nejakého systému axióm. Začiatkom 20. storočia sa potreba axiomatizácie teórie množín stala akútnou. Viedli k tomu najmä dva dôvody. Prvým bolo objavenie paradoxov (Ceasare Burali-Fortiho a známejší Russellov paradox), ktoré naznačili, že prílišná voľnosť pri konštrukcii

[16] Cantor prišiel s myšlienkou definovať iracionálne čísla pomocou limít postupností racionálnych čísel. Nezávisle na ňom prišiel Dedekind s definíciou iracionálnych čísel pomocou tzv. „Dedekindových rezov“

„množín“ môže spôsobovať problémy. V tom období však už teória množín výrazne ovplyvňovala matematiku. Lebesgue zaviedol pomocou množinových pojmov v roku 1901 pojem miery a v roku 1902 definoval Lebesgueov integrál. Ani matematická analýza nevystačila s intuicistickou matematikou[17] a potrebovala Cantorovu teóriu množín. Preto bolo rozumnejšie hľadať spôsob, ako uchovať hlavné črty teórie množín a eliminovať paradoxy, ako zavrhnúť kvôli paradoxom celú teóriu. Ukázalo sa, že Russellovmu a podobným paradoxom sa dá vyhnúť starostlivým výberom princípov konštrukcie množín, ktoré umožnili zachovať vyjadrovaciu silu teórie množín potrebnú na riešenie matematických problémov, ale vylúčili existenciu problematických množín.

Druhý dôvod axiomatizácie teórie množín bol zložitejší. Keď Cantor pracoval na teórii kardinálnych a ordinálnych čísel narazil na problém, či každú množinu možno vybaviť istou vnútornou štruktúrou, nazvanou dobrým usporiadaním. Pritom dobré usporiadanie, či vlastosti ekvivalentné dobrému usporiadaniu potreboval na dôkaz aj pomerne jednoduchých tvrdení. Ernest Zermelo začiatkom 20. storočia vytvoril systém axióm teórie množín a ukázal, že každú množinu možno dobre usporiadať za predpokladu, že platí axióma (AC) výberu[18] . Táto axióma vzbudila mnohé diskusie tak matematikov ako aj filozofov, ale neskôr sa stala štandardným nástrojom modernej matematiky.[19] Postoj matematikov k axióme výberu ilustruje nasledovný žartom myslený výrok Jerryho Bona

> The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?

ktorý vyjadruje to, že hoci sú AC, princíp dobrého usporiadania a tzv. Zornova lema matematicky ekvivalentné, väčšina matematikov považuje axiómu výberu za intuitívne zrejmú, princíp dobrého usporiadania za kontraintuitívny a Zornovu lemu za príliš komplikovanú na to, aby si o nej bolo možné vytvoriť akúkoľvek intuitívnu predstavu.

Zermelov systém axióm dopracoval v prvej polovici 20. storočia Fraenkel do podoby v ktorej sa používa dodnes. Zermelo-Fraenkelov systém axióm, označovaný ZFC je uvedený v prílohe.

[17] intuicizmus neprijíma aktuálne nekonečno a vyžaduje konečné a konštruktívne dôkazy.

[18] Predtým, ako Zermelo sformuloval AC explicitne, sa často v matematike používala implicitne.

[19] Históriu AC, nazávislosť AC od ostatných axióm ZFC systému a zoznam tvrdení ekvivalentných AC možno nájsť na adrese xxx

Kapitola 9

Výrokový počet

Teraz, keď už máme isté skúsenosti s dokazovaním matematických tvrdení a vieme formálne zapisovať tvrdenia a ich dôkazy, vrátime sa k výrokom z časti 1.2 a postavíme na pevný základ výrokovú logiku, ktorú sme zatiaľ používali len intuitívne, opierajúc sa o pravdivostné tabuľky. Začneme axiomatickou výstavbou výrokovej logiky a vytvoríme axiomatickú teóriu a ukážeme, že všetky „pravdy“ výrokovej logiky možno odvodiť z malého počtu východiskových tvrdení (axióm) výrokového počtu. Upresníme predstavy, ktoré sme dosiaľ mali o matematických dôkazoch a naučíme sa konštruovať deduktívne dôkazy pomocou axióm a odvodzovacích pravidiel. Výrokový počet bude pre nás slúžiť (okrem iného) ako ukážková „cvičná“ teória, na ktorej ukážeme, ako sa vytvára formálna axiomatická teória, ako sa zavádzajú základné pojmy, ako vyzerá formálne odvodenie z axióm. Okrem toho na príklade výrokového počtu vysvetlíme také závažné pojmy, ako je *úplnosť, neprotirečivosť teórie* a *nezávislosť systému jej axióm a odvodzovacích pravidiel*. Na záver ukážeme, že axiomatizácia výrokového počtu, ktorú sme uviedli, nie je jediná; že existujú aj iné systémy axióm a odvodzovacích pravidiel, pomocou ktorých možno vytvoriť buď iné axiomatické teórie výrokového počtu ekvivalentné axiomatickej teórii, ktorú sme vytvorili, alebo alternatívne axiomatické teórie výrokového počtu.

Výrokový počet však nie je dostatočne silný na to, aby mohol tvoriť logický základ pre väčšinu matematických teórií. Preto sa v ďalšej kapitole oboznámime so základmi silnejšej matematickej teórie—predikátového počtu. Predikátový počet je rozšírením výrokového počtu a už postačuje napríklad aj na vyjadrenie teórie množín, aritmetiky prirodzených čísel, či iných matematických teórií.

9.1 Axiomatická výstavba výrokového počtu

Zavedieme formálnu axiomatickú teóriu $\mathcal{L}$ pre výrokový počet:

(1) je daná abeceda teórie $\mathcal{L}$ pozostávajúca z

(a) množiny pomocných symbolov a logických spojok: $(,), \Rightarrow, \neg, \vdash$;

(b) množiny symbolov $A_1, A_2, A_3, \ldots, A_i$, kde $i \in \mathbb{N}$, ktoré nazývame výrokovými premennými (výrokovými symbolmi);

(2) Ľubovoľná konečná postupnosť symbolov teórie $\mathcal{L}$ sa nazýva *výrazom teórie* $\mathcal{L}$;

(3) *Formuly teórie* $\mathcal{L}$

(a) Všetky výrokové premenné sú formuly teórie $\mathcal{L}$.

(b) Ak sú $\mathcal{A}, \mathcal{B}$ formuly teórie $\mathcal{L}$, tak potom sú aj $\neg\mathcal{A}$ a $\mathcal{A} \Rightarrow \mathcal{B}$ formuly teórie $\mathcal{L}$.

(c) Formulami teórie $\mathcal{L}$ sú len výrazy teórie $\mathcal{L}$, ktoré spĺňajú podmienky (a) alebo (b). Iných formúl teórie $\mathcal{L}$ niet.

(4) Nech sú $\mathcal{A}, \mathcal{B}, \mathcal{C}$ ľubovoľné formuly teórie $\mathcal{L}$. Potom nasledujúce formuly sú *axiómy teórie* $\mathcal{L}$:

(A1) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$

(A2) $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$

(A3) $(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$

(5) Jediným *pravidlom odvodenia* formálnej teórie $\mathcal{L}$ je pravidlo *modus ponens,* ktoré hovorí: ak sú odvodené formuly $\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{A}$ tak potom je odvodená aj formula $\mathcal{B}$. Formálne zapisujem pravidlo modus ponens nasledovne:

$$\frac{\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}}{\mathcal{B}}.$$

Pravidlo modus ponens budem označovať skratkou MP. Budeme tiež hovoriť, že formula $\mathcal{B}$ je bezprostredným dôsledkom formúl $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$ alebo tiež že formula $\mathcal{B}$ priamo vyplýva z formúl $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$.

Zmyslom formálnej teórie je popísať nejakú potenciálne nekonečnú množinu „právd“, ktoré majú rovnaký charakter ako axiómy. Axiómy (A1), (A2), (A3) sú *de facto* schémy axióm a axiómami sa stávajú až po dosadení konkrétnych formúl teórie $\mathcal{L}$. Keďže formúl teórie $\mathcal{L}$ je nekonečne veľa, pomocou troch axióm (A1), (A2), (A3) je zadaná nekonečná množina axióm teórie $\mathcal{L}$. Nakoľko existuje presný postup, podľa ktorého sa dá pre ľubovoľnú formulu $\mathcal{A}$ teórie $\mathcal{L}$ jednoznačne určiť, či je daná formula axiómou teórie $\mathcal{L}$, hovoríme, že $\mathcal{L}$ je *efektívne axiomatizovateľná teória.* Aj keď je axióm teórie $\mathcal{L}$ nekonečne veľa, nie všetky pravdivé tvrdenia (pravdivé formuly) teórie $\mathcal{L}$ možno zostrojiť dosadením vhodných formúl do niektorej z axióm (A1), (A2),(A3). Prikročíme preto teraz k ďalšiemu veľmi dôležitému pojmu—k pojmu *odvodenia* alebo *dôkazu v teórii* $\mathcal{L}$, ktoré nám omožňuje vytvárať z axióm pomocou pravidla odvodenia nové pravdivé formuly teórie $\mathcal{L}$. *Odvodením v teórii* $\mathcal{L}$ sa nazýva ľubovoľná postupnosť formúl teórie $\mathcal{L}$, $\mathcal{A}_1, \ldots, \mathcal{A}_n$ taká, že pre ľubovoľné $i \in \{1, \ldots, n\}$ je formula $\mathcal{A}_i$

(a) axióma teórie $\mathcal{L}$;

(b) bezprostredný dôsledok formúl $\mathcal{A}_j, \ldots, \mathcal{A}_k$, $\quad j, k < i$ podľa pravidla modus ponens.

(Číslo n, počet formúl v odvodení sa nazýva *dĺžkou odvodenia*.) Formula $\mathcal{A}$ teórie $\mathcal{L}$ sa nazýva teorémou teórie $\mathcal{L}$, ak existuje také odvodenie $\mathcal{A}_1, \ldots, \mathcal{A}_n$ v $\mathcal{L}$, že $\mathcal{A}_n = \mathcal{A}$. Takéto odvodenie sa nazýva *odvodením formuly* $\mathcal{A}$.

Okrem absolútnych právd, ktorých platnosť je odvodená priamo z axióm, existujú aj užitočné tvrdenia (formuly), ktoré platia len za istých predpokladov. Formalizujeme tento pojem. Formula $\mathcal{A}$ sa nazýva dôsledkom množiny formúl Γ v teórii $\mathcal{L}$ práve vtedy, ak v $\mathcal{L}$ existuje postupnosť formúl $\mathcal{A}_1, \ldots, \mathcal{A}_n$ taká, že $\mathcal{A}_n = \mathcal{A}$ a pre každé $i, i = 1, \ldots, n$ platí jedna z nasledujúcich podmienok:

(a) $\mathcal{A}_i$ je axióma teórie $\mathcal{L}$;

(b) $\mathcal{A}_i \in \Gamma$,

(c) $\mathcal{A}_i$ je bezprostredný dôsledok formúl $\mathcal{A}_j, \ldots, \mathcal{A}_k$, $j, k < i$ tejto postupnosti podľa pravidla modus ponens.

Postupnosť $\mathcal{A}_1, \ldots, \mathcal{A}_n$ spĺňajúca vyššie uvedené podmienky sa nazýva *odvodením formuly $\mathcal{A}$ z Γ*. Formuly z množiny Γ sa nazývajú *hypotézy* a samotná množina Γ sa nazýva *množina hypotéz*. Skutočnosť, že „formula $\mathcal{A}$ je dôsledkom Γ“ budeme zapisovať symbolicky $\Gamma \vdash \mathcal{A}$ a slovne vyjadrovať aj tak, že formula $\mathcal{A}$ je odvodená z množiny hypotéz Γ. V prípade, keď $\Gamma = \emptyset$ a $\Gamma \vdash \mathcal{A}$, zapisujeme skutočnosť, že formula $\mathcal{A}$ je odvodená z prázdnej množiny hypotéz symbolicky takto $\vdash \mathcal{A}$. Posledný zápis znamená, že $\mathcal{A}$ je *teorémou teórie $\mathcal{L}$*.

Aj keď pri odvodeniach formúl v teórii $\mathcal{L}$ by sme vystačili s negáciou a implikáciou, zavedieme kvôli zjednodušeniu niektorých odvodení aj ďalšie logické spojky (operátory). Nech sú $\mathcal{A}, \mathcal{B}$ ľubovoľné formuly teórie $\mathcal{L}$. Potom

(D1) $\mathcal{A}\&\mathcal{B}$ označuje formulu $\neg(\mathcal{A} \Rightarrow \neg\mathcal{B})$

(D2) $\mathcal{A} \vee \mathcal{B}$ označuje formulu $\neg(\mathcal{A}) \Rightarrow \mathcal{B}$

(D3) $\mathcal{A} \equiv \mathcal{B}$ označuje formulu $(\mathcal{A} \Rightarrow \mathcal{B})\&(\mathcal{B} \Rightarrow \mathcal{A})$.

Aby sme v zápise formúl teórie $\mathcal{L}$ nemuseli používať príliš veľa zátvoriek, dohodneme sa na nasledujúcej konvencii:

1. Priorita logických operátorov (od najvyššej po najnižšiu) je: $\neg, \&, \vee, \Rightarrow, \equiv$.
2. Keď je vo formule možné použiť dva alebo viac logických operátorov s rozličnou prioritou, najprv uplatníme operátor s najvyššou prioritou. Napríklad vo formule $\neg\mathcal{A}\&\neg\mathcal{B} \Rightarrow \mathcal{C}$ budeme používať logické operátory v nasledujúcom poradí
$$((\neg\mathcal{A})\&(\neg\mathcal{B})) \Rightarrow \mathcal{C}.$$
3. Ak máme vo fomule možnosť uplatniť viacero operátorov s rovnakou prioritou, tak formulu vyhodnocujeme sprava doľava[1] Napríklad formula $\mathcal{A} \Rightarrow \mathcal{B} \Rightarrow \mathcal{C}$ sa vyhodnocuje v nasledujúcom poradí $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})$.

[1]toto pravidlo má zmysel len pre logické operátory, ktoré nie sú asociatívne. V našom prípade ide o operátor implikácie.

4. Ak vo formule chceme stanoviť iné poradie uplatňovania logických operátorov ako vyplýva z tejto konvencie, určíme toto poradie zátvorkami. Príklad: formula $\neg\mathcal{A} \Rightarrow \mathcal{B}$ by sa podľa tejto konvencie vyhodnocovala ako $(\neg\mathcal{A}) \Rightarrow \mathcal{B}$. Ak však chceme negovať implikáciu, umiestnime zátvorky takto $\neg(\mathcal{A} \Rightarrow \mathcal{B})$.

Príklad 9.1. *Uvedieme ešte niekoľko príkladov na zjednodušený zápis formúl použitím práve zavedenej konvencie:*

- $\mathcal{A}\&\mathcal{B} \Rightarrow \neg\mathcal{C} \vee \mathcal{D}$ *je iný zápis formuly* $(\mathcal{A}\&\mathcal{B}) \Rightarrow ((\neg\mathcal{C}) \vee \mathcal{D})$,
- $\neg\neg\mathcal{A}$ *je iný zápis formuly* $(\neg(\neg\mathcal{A}))$,
- $\mathcal{A}\&\mathcal{B}\&\mathcal{C}\&\mathcal{D}$ *je iný zápis formuly* $\mathcal{A}\&(\mathcal{B}\&(\mathcal{C}\&(\mathcal{D})))$.

9.2 Teorémy výrokového počtu

Začneme odvodením na prvý pohľad triviálnej, ale (ako sa ukáže neskôr) veľmi užitočnej teorémy.

Veta 9.1. $\vdash \mathcal{A} \Rightarrow \mathcal{A}$.

Dôkaz.

1.	$\vdash (\mathcal{A} \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{A}) \Rightarrow ((\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{A})) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{A}))$	A2
2.	$\vdash \mathcal{A} \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{A})$	A1
3.	$\vdash (\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{A})) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{A})$	MP 1,2
4.	$\vdash (\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{A}))$	A1
5.	$\vdash \mathcal{A} \Rightarrow \mathcal{A}$	MP 1,4

□

Poznámka. Aby boli odvodenia teorém prehľadné, budeme ich zapisovať takto: na ľavej strane riadka napíšeme formulu a na pravej strane komentár, ktorý objasňuje, akým spôsobom sme danú formulu odvodili. Aby sme sa mohli jednoznačne odvolávať na formuly v odvodení, skôr odvodené teorémy a axiómy, budeme číslovať jednotlivé formuly odvodenia, axiómy označujeme symbolmi (A1), (A2), (A3) a teorémy označujeme symbolom Tn, kde n je poradové číslo teorémy. Potom napríklad zápis MP 1,4 v 5. riadku predchádzajúceho odvodenia znamená, že formulu $\mathcal{A} \Rightarrow \mathcal{A}$ sme odvodili pomocou pravidla modus ponens a formúl z 1. a 4. riadku odvodenia. Podobne komentár vo štvrtom riadku hovorí, že formulu $(\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{A}))$ sme dostali z 1. axiómy (dosadili sme formulu $\mathcal{A}$ za formuly $\mathcal{A}$ a $\mathcal{B}$.

Príklad 9.2. *Zostrojte odvodenia nasledujúcich formúl:*

1.		$\vdash (\neg\mathcal{A} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{A}$,	
2.	$\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{B} \Rightarrow \mathcal{C}$	$\vdash \mathcal{A} \Rightarrow \mathcal{C}$,	*pravidlo sylogizmu*
3.	$\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})$	$\vdash \mathcal{B} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C})$.	*zámena predpokladov*

Ak matematik potrebuje dokázať tvrdenie „ak $\mathcal{A}$, tak potom $\mathcal{B}$“ priamo, tak spravidla predpokladá, že platí $\mathcal{A}$ a potom dokazuje platnosť $\mathcal{B}$. Takýto postup sa používa aj vo formálnych logických teóriách. Jeho oprávnenosť vo výrokovom počte zaručuje nasledujúca veta.

Veta 9.2. *(o dedukciii) Nech Γ je množina formúl, $\mathcal{A}, \mathcal{B}$ sú formuly teórie $\mathcal{L}$ a nech platí*

$$\Gamma, \mathcal{A} \vdash \mathcal{B},$$

potom

$$\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}.$$

Dôkaz. Nech $\mathcal{B}_1, \ldots, \mathcal{B}_n$ je odvodenie formuly $\mathcal{B}$ z množiny hypotéz $\Gamma \cup \{\mathcal{A}\}$. Matematickou indukciou vzhľadom na dĺžku odvodenia dokážeme, že $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$.

1. Nech $n = 1$. Potom odvodenie pozostáva z jedinej formuly $\mathcal{B}_1$ ($\mathcal{B}_1 = \mathcal{B}$). Z definície odvodenia vyplývajú pre $\mathcal{B}$ tri možnosti:

   (a) $\mathcal{B}$ je axióma. V tom prípade platí:

1.	$\vdash \mathcal{B}$	$\mathcal{B}$ je axióma
2.	$\vdash \mathcal{B} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	A1
3.	$\vdash \mathcal{A} \Rightarrow \mathcal{B}$	MP 1,2

   Ale ak formulu $\mathcal{A} \Rightarrow \mathcal{B}$ možno odvodiť z prázdnej množiny hypotéz, tak potom túto formulu možno odvodiť aj z ľubovoľnej neprázdnej množiny hypotéz, a teda platí

   $$\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}.$$

   (b) $\mathcal{B} \in \Gamma$. Potom

1.	$\Gamma \vdash \mathcal{B}$	
2.	$\vdash \mathcal{B} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	A1
3.	$\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$	MP 1,2

   (c) $\mathcal{B} = \mathcal{A}$. Potom podľa vety 9.1

1.	$\vdash \mathcal{A} \Rightarrow \mathcal{A}$	a teda aj
2.	$\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{A}$.	

   Prípad „$\mathcal{B}_i$ je bezprostredným dôsledkom niektorých predchádzajúcich formúl“ nemôže nastať, pretože formula $\mathcal{B}_i$ (=$\mathcal{B}_1 = \mathcal{B}$) je jediná formula v tomto odvodení.

2. Nech tvrdenie vety platí pre formuly s odvodením kratším ako n. Dokážeme, že platí aj pre formuly s odvodením dĺžky n. Pre formulu $\mathcal{B}_n (= \mathcal{B})$ môžu nastať 4 rozličné prípady:

   (a) $\mathcal{B}_n$ je axióma,

   (b) $\mathcal{B}_n \in \Gamma$,

   (c) $\mathcal{B}_n = \mathcal{A}$,

(d) $\mathcal{B}_n$ vyplýva z niektorých predchádzajúcich formúl $\mathcal{B}_i, \mathcal{B}_j$ pomocou pravidla modus ponens; $\mathcal{B}_i = (\mathcal{B}_j \Rightarrow \mathcal{B}_n)$ a

$$\frac{(\mathcal{B}_j \Rightarrow \mathcal{B}_n), \mathcal{B}_j}{\mathcal{B}_n}.$$

Prvé tri prípady sa riešia rovnako ako pre $n = 1$. V poslednom prípade budeme postupovať nasledovne: keďže $\mathcal{B}_i, \mathcal{B}_j$ predchádzajú v odvodení formulu $\mathcal{B}_n$, majú odvodenie dĺžky kratšej ako n, a preto pre ne platí indukčný predpoklad. To znamená, že

1. $\Gamma, \mathcal{A} \vdash \mathcal{B}_i$
2. $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$ indukčný predpoklad
3. $\Gamma, \mathcal{A} \vdash \mathcal{B}_j$
4. $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_j$ indukčný predpoklad.

Formulu $\mathcal{B}_n$ sme odvodili pomocou pravidla modus ponens z formúl $\mathcal{B}_i, \mathcal{B}_j$, kde $\mathcal{B}_i = (\mathcal{B}_j \Rightarrow \mathcal{B}_n)$:

5.	$\Gamma, \mathcal{A} \vdash \mathcal{B}_n$	MP 1,3
6.	$\Gamma \vdash \mathcal{A} \Rightarrow (\mathcal{B}_j \Rightarrow \mathcal{B}_n)$	krok 2
7.	$\vdash (\mathcal{A} \Rightarrow (\mathcal{B}_j \Rightarrow \mathcal{B}_n)) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_n))$	A2
8.	$\Gamma \vdash ((\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_n))$	MP 6,7
9.	$\Gamma \vdash (\mathcal{A} \Rightarrow \mathcal{B}_n))$	MP 8,4

□

Úloha 9.1. *Prečítajte si znova definíciu odvodenia a potom dokážte nasledujúce tvrdenia o vlastnostiach odvodenia!*

(a) *Ak* $\Gamma_1 \subseteq \Gamma_2$ *a* $\Gamma_1 \vdash \mathcal{A}$*, tak potom aj* $\Gamma_2 \vdash \mathcal{A}$.

(b) *Tvrdenie* $\Gamma \vdash \mathcal{A}$ *platí práve vtedy, ak existuje konečná podmnožina formúl* $\Delta \subseteq \Gamma$ *taká, že* $\Delta \vdash \mathcal{A}$.

(c) *Ak* $\Delta \vdash \mathcal{A}$ *a pre ľubovoľnú formulu* $\mathcal{B} \in \Delta$ *platí* $\Gamma \vdash \mathcal{B}$*, tak potom* $\Gamma \vdash \mathcal{A}$.

Úloha 9.2. *Dokážte (pomocou vety o dedukcii)*

$$\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{B} \Rightarrow \mathcal{C} \vdash \mathcal{A} \Rightarrow \mathcal{C}.$$

Úloha 9.3. *Dokážte:*

$$\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C}), \mathcal{B} \vdash \mathcal{A} \Rightarrow \mathcal{C}.$$

Poznámka. Tvrdenie vety 9.2 platí aj v prípade, keď je množina hypotéz Γ prázdna.

Príklad 9.3. *Ak platí* $\mathcal{A} \vdash \mathcal{B}$*, tak potom podľa vety o dedukcii platí aj* $\vdash \mathcal{A} \Rightarrow \mathcal{B}$*, t.j. formula* $\mathcal{A} \Rightarrow \mathcal{B}$ *je teorémou teórie* $\mathcal{L}$.

Aby sme získali potrebnú prax pri odvodzovaní formúl, dokážeme teraz o niekoľkých formulách, že sú to teorémy teórie $\mathcal{L}$.

Veta 9.3. *Nech sú $\mathcal{A}, \mathcal{B}$ ľubovoľné formuly teórie $\mathcal{L}$, potom nasledujúce formuly sú teorémami teórie $\mathcal{L}$:*

(a)	$\neg\neg\mathcal{B} \Rightarrow \mathcal{B}$	(T2)
(b)	$\mathcal{B} \Rightarrow \neg\neg\mathcal{B}$	(T3)
(c)	$\neg\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	(T4)
(d)	$(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	(T5)
(e)	$(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$	(T6)
(f)	$\mathcal{A} \Rightarrow (\neg\mathcal{B} \Rightarrow \neg(\mathcal{A} \Rightarrow \mathcal{B}))$	(T7)

Dôkaz. Zostrojíme odvodenia formúl (a)—(f):

(a) Pozrieme sa, ktorá z axióm, resp. ktorá z doteraz odvodených teorém obsahuje negácie. Je to axióma A3. Vieme, že nie je potrebné odvodzovať implikáciu $\neg\neg\mathcal{B} \Rightarrow \mathcal{B}$, ale stačí ukázať, že platí $\neg\neg\mathcal{B} \vdash \mathcal{B}$ a potom použiť vetu o dedukcii. Preto budeme pri dôkaze postupovať nasledovne:

1.		$\neg\neg\mathcal{B}$	H1 (hypotéza 1)
2.		$\vdash (\neg\mathcal{B} \Rightarrow \neg\neg\mathcal{B}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \neg\mathcal{B}) \Rightarrow \mathcal{B})$	(A3)
3.		$\vdash \neg\neg\mathcal{B} \Rightarrow (\neg\mathcal{B} \Rightarrow \neg\neg\mathcal{B})$	(A1)
4.	H1	$\vdash (\neg\mathcal{B} \Rightarrow \neg\neg\mathcal{B})$	MP 1,3
5.	H1	$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{B}) \Rightarrow \mathcal{B}$	MP 2,4
6.		$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{B})$	T1 (teoréma 1)
7.	H1	$\vdash \mathcal{B}$	MP 5,6
8.		$\vdash \neg\neg\mathcal{B} \Rightarrow \mathcal{B}$	VD 1,7 (veta o dedukcii)

(b) Pri dôkaze využijeme práve dokázanú teorému T2:

1.		$\mathcal{B}$	H1 (hypotéza 1)
2.		$\vdash (\neg\neg\neg\mathcal{B} \Rightarrow \neg\mathcal{B}) \Rightarrow ((\neg\neg\neg\mathcal{B} \Rightarrow \mathcal{B}) \Rightarrow \neg\neg\mathcal{B})$	(A3)
3.		$\vdash (\neg\neg\neg\mathcal{B} \Rightarrow \neg\mathcal{B})$	T2
4.		$\vdash ((\neg\neg\neg\mathcal{B} \Rightarrow \mathcal{B}) \Rightarrow \neg\neg\mathcal{B})$	MP 2,3
5.		$\vdash \mathcal{B} \Rightarrow (\neg\neg\neg\mathcal{B} \Rightarrow \mathcal{B})$	A1
6.	H1	$\vdash (\neg\neg\neg\mathcal{B} \Rightarrow \mathcal{B})$	MP 1,5
7.	H1	$\vdash \neg\neg\mathcal{B}$	MP 6,4
8.		$\vdash \mathcal{B} \Rightarrow \neg\neg\mathcal{B}$	VD 7,1

(c) V tomto prípade prijmeme zdanlivo nelogické hypotézy; budeme predpokladať, že súčasne platí $\mathcal{A}$ aj $\neg\mathcal{A}$. Keď sa však lepšie pozrieme na teorému T3, vidíme, že formula $\mathcal{B}$ nijako nesúvisí s formulami $\mathcal{A}$ aj $\neg\mathcal{A}$. Teoréma T3 vlastne hovorí, že

z protirečivých predpokladov možno odvodiť akúkoľvek formulu.

1.		$\neg\mathcal{A}$	H1 (hypotéza 1)
2.		$\mathcal{A}$	H2 (hypotéza 2)
3.		$\vdash \mathcal{A} \Rightarrow (\neg\mathcal{B} \Rightarrow \mathcal{A})$	(A1)
4.		$\neg\mathcal{A} \Rightarrow (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$	(A1)
5.		$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$	(A3)
6.	H2	$\vdash (\neg\mathcal{B} \Rightarrow \mathcal{A})$	MP 2,3
7.	H1	$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$	MP 1,4
8.	H1	$\vdash ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$	MP 7,5
9.	H1, H2	$\vdash \mathcal{B}$	MP 8,6
10.		$\vdash \neg\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	2×VD 1,2,9

(d) Táto teoréma—nazýva sa kontrapozícia negácie—je veľmi dôležitá; v niektorých axiomatických systémoch býva axiómou namiesto A3.

1.		$(\neg\mathrm{B} \Rightarrow \neg\mathcal{A})$	H1
2.		$\mathcal{A}$	H2
3.		$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$	(A3)
4.	H1	$\vdash ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$	MP 1,3
5.		$\vdash \mathcal{A} \Rightarrow (\neg\mathrm{B} \Rightarrow \mathcal{A})$	(A1)
6.	H2	$\vdash (\neg\mathrm{B} \Rightarrow \mathcal{A})$	MP 5,2
7.	H1, H2	$\vdash \mathrm{B}$	MP 6,4
8.		$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	2×VD 1,2,7

(e)

1.		$\mathcal{A} \Rightarrow \mathrm{B}$	H1
2.		$\vdash \neg\neg\mathcal{A} \Rightarrow \mathcal{A}$	T2
3.	H1	$\vdash \neg\neg\mathcal{A} \Rightarrow \mathrm{B}$	pravidlo sylogizmu 1,2
4.		$\vdash \mathrm{B} \Rightarrow \neg\neg\mathrm{B}$	T3
5.	H1	$\vdash \neg\neg\mathcal{A} \Rightarrow \neg\neg\mathrm{B}$	pravidlo sylogizmu 3,4
6.		$\vdash (\neg\neg\mathcal{A} \Rightarrow \neg\neg\mathrm{B}) \Rightarrow (\neg\mathrm{B} \Rightarrow \neg\mathcal{A})$	T5
7.	H1	$\vdash (\neg\mathrm{B} \Rightarrow \neg\mathcal{A})$	MP 5,6
8.		$\vdash (\mathcal{A} \Rightarrow \mathrm{B}) \Rightarrow (\neg\mathrm{B} \Rightarrow \neg\mathcal{A})$	VD 1,7

(f) V predchádzajúcich odvodeniach sme vetu o dedukcii používali až na konci odvodenia. V odvodení teorémy 7 je kľúčovým krokom práve použitie vety o dedukcii uprostred odvodenia—v kroku 4. Všimnite si, že teoréma 7 predstavuje vlastne formulu $\mathcal{A} \Rightarrow (\neg\mathrm{B} \Rightarrow (\mathcal{A}\&(\neg\mathrm{B})))$ ktorú poznáme ako pravidlo spojenia predpokladov.

1.		$\mathcal{A}$	H1
2.		$\mathcal{A} \Rightarrow \mathrm{B}$	H2
3.	H1, H2	$\vdash \mathrm{B}$	MP 1,2
4.	H1	$\vdash (\mathcal{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B}$	VD 2,3
5.		$\vdash ((\mathcal{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B}) \Rightarrow (\neg\mathrm{B} \Rightarrow \neg(\mathcal{A} \Rightarrow \mathrm{B}))$	T6
6.	H1	$\vdash (\neg\mathrm{B} \Rightarrow \neg(\mathcal{A} \Rightarrow \mathrm{B}))$	MP 4,5
7.		$\vdash \mathcal{A} \Rightarrow (\neg\mathrm{B} \Rightarrow \neg(\mathcal{A} \Rightarrow \mathrm{B}))$	VD 1,6

□

Naše doterajšie skúsenosti s dokazovaním teorém výrokového počtu by sme mohli sformulovať do nasledujúceho návodu: ak má formula, ktorú máme odvodiť tvar implikácie $\mathcal{A} \Rightarrow \mathcal{B}$, presunieme formulu $\mathcal{A}$ do predpokladov. Potom analyzujeme formulu $\mathcal{B}$. Keď sme už popresúvali do predpokladov všetko, čo sa dalo, zostáva nám dokázať nejakú formulu $\mathcal{C}$. Pozrieme sa teraz na axiómy a teorémy, ktoré sme už dokázali a vyberieme tú, ktorá má „na konci" formulu zhodnú alebo podobnú formule $\mathcal{C}$. Ak má formula $\mathcal{C}$ napríklad tvar $\neg(B_1 \Rightarrow B_2)$, použijeme teorému 7. Ak štruktúru formuly $\mathcal{C}$ nepoznáme a v množine predpokladov (hypotéz) sa vyskytuje napríklad formula $\neg\mathcal{A} \Rightarrow \neg\mathcal{C}$, tak použijeme axiómu 3, atď. Potom dosadíme vhodné formuly do zvolenej teorémy alebo axiómy a použitím množiny hypotéz a pravidla modus ponens sa snažíme „odbúrať" predpoklady z danej teorémy a odvodiť formulu $\mathcal{C}$.

Všimnite si, že pri odvodení teorém T2—T7 sa niekoľkokrát vyskytla nasledujúca postupnosť formúl:

1.		$\mathcal{A}$	H1
2.		$\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$	(A1)
3.	H1	$\vdash (\mathcal{B} \Rightarrow \mathcal{A})$	MP 1,2

Kvôli skráteniu odvodení môžeme zaviesť nové pravidlo odvodenia:

$$\frac{\mathcal{A}}{\mathcal{B} \Rightarrow \mathcal{A}},$$

ktoré budeme označovať symbolom P1 (aby sme vyjadrili, že pravidlo vznikli z axiómy 1). Podobne môžeme zaviesť pravidlo sylogizmu (syl.)

$$\frac{\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{B} \Rightarrow \mathcal{C}}{\mathcal{A} \Rightarrow \mathcal{C}},$$

resp. pravidlo kontrapozície negácie

$$\frac{\mathcal{A} \Rightarrow \mathcal{B}}{\neg\mathcal{B} \Rightarrow \neg\mathcal{A}} \text{ alebo } \frac{\neg\mathcal{B} \Rightarrow \neg\mathcal{A}}{\mathcal{A} \Rightarrow \mathcal{B}}.$$

Zavedenie týchto pravidiel možno zdôvodniť nasledovne

pravidlo sylogizmu

1.		$\mathcal{A} \Rightarrow \mathcal{B}$	H1
2.		$\mathcal{B} \Rightarrow \mathcal{C}$	H2
3.		$\mathcal{A}$	H3
4.	H1, H3	$\vdash \mathcal{B}$	MP 1,3
5.	H1, H2, H3	$\vdash \mathcal{C}$	MP 2,4
6.	H1, H2	$\vdash \mathcal{A} \Rightarrow \mathcal{C}$	VD 3,5

kontrapozícia negácie (1)

1.		$\mathcal{A} \Rightarrow \mathcal{B}$	H1
2.		$(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$	T6
3.	H1	$\vdash (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$	MP 1,2

kontrapozícia negácie (2)

1.		$\neg B \Rightarrow \neg \mathcal{A}$	H1
2.		$\vdash (\neg \mathcal{B} \Rightarrow \neg \mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	T5
3.	H1	$\vdash (\mathcal{A} \Rightarrow \mathcal{B})$	MP 1,2

Úloha 9.4. *Dokážte nasledujúce teorémy:*

1.	$\vdash (\neg \mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow (\neg \mathcal{A} \Rightarrow \mathcal{B})$	*T8*
2.	$\vdash (\mathcal{B} \Rightarrow \neg \mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \neg \mathcal{B})$	*T9*
3.	$\vdash (\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow ((\neg \mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow \mathcal{B})$	*T10*

Úloha 9.5. *Skúste dokázať teorémy T2–T11 bez použitia vety o dedukcii!*

9.3 Úplnosť výrokového počtu

Cieľom nášho snaženia okrem iného bolo poskytnúť alternatívu k zisťovaniu pravdivosti tvrdení algebry logiky pomocou pravdivostných tabuliek; vybudovať takú teóriu $\mathcal{L}$, v ktorej by každá teoréma bola tautológiou algebry logiky a naopak, každá tautológia bola teorémou teórie $\mathcal{L}$.[2] Ukážeme, že sa nám to skutočne podarilo. Z jednej strany to je celkom jednoduché.

Veta 9.4. *Každá teoréma teórie $\mathcal{L}$ je tautológia.*

Dôkaz. Pomocou pravdivostných tabuliek sa dá ľahko overiť, že každá axióma teórie $\mathcal{L}$ je tautológia. Pozrieme sa na pravidlo odvodenia modus ponens. Nech sú $\mathcal{A}, \mathcal{B}$ ľubovoľné formuly teórie $\mathcal{L}$. Z nasledujúcej pravdivostnej tabuľky je vidieť, že formuly $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$ sú súčasne pravdivé len v tom prípade, ak je pravdivá aj formula $\mathcal{B}$.

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	
0	0	1	
0	1	1	
1	0	0	
1	1	1	✓

Keďže teoréma je odvodená z axióm (ktoré sú tautológie) pomocou pravidla modus ponens (ktoré z tautológií odvodzuje opäť tautológie) každá teoréma teórie $\mathcal{L}$ je tautológia. □

Zavedieme teraz pojem *hĺbky formuly*, ktorý budeme potrebovať v tvrdení nasledujúcej vety.

[2] Nejde tak ani o axiomatizáciu samotného výrokového počtu, ako skôr o to, aby sme ukázali, ako sa buduje axiomatická teória, ako vyzerajú dôkazy a aké vlastnosti má zmysel v takejto teórii skúmať. V prípade takej jednoduchej axiomatickej (logickej) teórie, ako je výrokový počet budú možno odpovede na uvedené otázky vyzerať jednoducho. V nasledujúcej kapitole sa však budeme zaoberať základami predikátového počtu, ktorý je síce rozšírením výrokového počtu, ale uvedené otázky pre predikátový počet sú podstatne náročnejšie.

1. Ak je formula $\mathcal{A}$ rovná logickej premennej, tak $\mathbf{hl}(\mathcal{A}) = 0$.
2. Predpokladáme, že dokážeme určiť hĺbku formúl $\mathcal{B}, \mathcal{B}_1, \mathcal{B}_2$, a formuly $\mathcal{A}_1, \mathcal{A}_2$ sú vyjadrené pomocou formúl $\mathcal{B}, \mathcal{B}_1, \mathcal{B}_2$ takto $\mathcal{A}_1 = \neg\mathcal{B}, \quad \mathcal{A}_2 = \mathcal{B}_1 \Rightarrow \mathcal{B}_2$. Potom hĺbka formúl $\mathcal{A}_1, \mathcal{A}_2$ je definovaná nasledovne:
   (a) $\mathbf{hl}(\mathcal{A}_1) = \mathbf{hl}(\mathcal{B}) + 1$;
   (b) $\mathbf{hl}(\mathcal{A}_2) = \max\{\mathbf{hl}(\mathcal{B}_1), \mathbf{hl}(\mathcal{B}_1)\} + 1$.

Úloha 9.6. *Zapíšte 10 formúl teórie $\mathcal{L}$ a určte ich hĺbku!*

Úloha 9.7. *Aká je hĺbka formúl* $(A \vee \mathcal{B}), (A\&\mathcal{B}), (A \equiv \mathcal{B})$

(a) *v teórii* $\mathcal{L}$[3]

(b) *vo výrokovom počte, ktorý obsahuje* $\vee, \&, \equiv$ *ako základné logické operátory?*

Nech je $\mathcal{A}$ ľubovoľná formula (teóriie $\mathcal{L}$) a nech sú $B_1, \ldots, B_k$ (všetky) logické premenné, ktoré formula $\mathcal{A}$ obsahuje. Označíme symbolom σ_i pravdivostnú hodnotu, ktorú nadobúda logická premenná B_i formuly $\mathcal{A}$, $\sigma_i \in \{0, 1\}$, pre $i = 1, \ldots, k$. Vektor pravdivostných hodnôt $(\sigma_1, \ldots, \sigma_k)$ logických premenných $B_1, \ldots, B_k$ formuly $\mathcal{A}$ označíme symbolom $\tilde{\sigma}$. Zavedieme nasledujúce označenie: formula

$$\mathcal{A}^{\tilde{\sigma}} = \begin{cases} \mathcal{A} & \text{ak pre daný vektor pravdivostných hodnôt } \tilde{\sigma} \text{ formula } \mathcal{A} \text{ má pravdivostnú} \\ & \text{hodnotu 1, a} \\ \neg\mathcal{A} & \text{ináč.} \end{cases}$$

Veta 9.5. *Nech je $\mathcal{A}$ formula a $B_1, \ldots, B_k$ sú logické premenné formuly $\mathcal{A}$. Nech je daný vektor $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_k)$ pravdivostných hodnôt premenných $B_1, \ldots, B_k$ a nech*

$$B_i^{\sigma_i} = \begin{cases} B_i, & \textit{ak } \sigma_i = 1, \\ \neg B_i, & \textit{ak } \sigma_i = 0; \end{cases}$$

potom

$$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{A}^{\tilde{\sigma}}.$$

Poznámka. Výraz B^σ sa dá vyjadriť pomocou formuly $B^\sigma = (B\sigma) \vee (\neg B \neg\sigma)$. Vimnite si, že $B^\sigma = 1$ práve vtedy, ak $B = \sigma$.

Dôkaz. Tvrdenie vety budeme dokazovať indukciou vzhľadom na hĺbku formuly $\mathcal{A}$.

1. Nech je hĺbka formuly $\mathbf{hl}(\mathcal{A}) = 0$, potom $\mathcal{A} = B_1$. Ak B_1 nadobúda pravdivostnú hodnotu 1, potom platí:
$$B_1 \vdash B_1,$$
lebo $B_1^{\sigma_1} = B_1^1 = B_1$, a $\mathcal{A}^{\tilde{\sigma}} = \mathcal{A} = B_1 = B_1^{\sigma_1}$. V opačnom prípade; t.j. keď $\sigma_1 = 0$ platí
$$\neg B_1 \vdash \neg B_1,$$
lebo $B_1^{\sigma_1} = B_1^0 = \neg B_1$, a $\mathcal{A}^{\tilde{\sigma}} = \neg\mathcal{A} = \neg B_1 = B_1^{\sigma_1}$.

[3] pripomíname, že v teórii $\mathcal{L}$ sú logické operátory $\vee, \&, \equiv$ definované pomocou operátorov $\Rightarrow, \neg$.

2. Predpokladajme, že tvrdenie platí pre všetky formuly hĺbky menšej než n. Dokážeme, že tvrdenie vety platí aj pre formuly hĺbky n; $(n > 0)$. Formula $\mathcal{A}$ môže mať jeden z nasledujúcich dvoch tvarov:

   (a) $\mathcal{A} = \neg\mathcal{C}$,

   (b) $\mathcal{A} = \mathcal{C}_1 \Rightarrow \mathcal{C}_2$,

   kde $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2$ sú formuly hĺbky menšej ako n. Rozoberieme obidva prípady.

   (a) Nech $A = \neg\mathcal{C}$. Formula $\mathcal{C}$ má hĺbku menšiu ako n, a preto podľa indukčného predpokladu pre ľubovoľný vektor $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_k)$ pravdivostných hodnôt jej premenných platí
   $$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{C}^{\tilde{\sigma}}.$$

      i. Nech je pre daný vektor pravdivostných hodnôt $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_k)$ formula $\mathcal{C}$ nepravdivá. To znamená, že je pravdivá formula $\mathcal{A} = \neg\mathcal{C}$. Dostávame
      $$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{C}^{\tilde{\sigma}},$$
      kde $\mathcal{C}^{\tilde{\sigma}} = \neg\mathcal{C}$. Ale $\neg\mathcal{C} = \mathcal{A} = \mathcal{A}^{\tilde{\sigma}}$, čiže
      $$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{A}^{\tilde{\sigma}}.$$

      ii. Nech je pre daný vektor pravdivostných hodnôt $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_k)$ formula $\mathcal{C}$ pravdivá. To znamená, že $\mathcal{C}^{\tilde{\sigma}} = \mathcal{C}$ a $\mathcal{A}^{\tilde{\sigma}} = \neg\mathcal{A}$. Potom postupne dostávame

1.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \mathcal{C} \quad (= \mathcal{C}^{\tilde{\sigma}})$	indukčný predpoklad
2.		$\vdash \mathcal{C} \Rightarrow \neg\neg\mathcal{C}$	T3
3.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \neg\neg\mathcal{C}$	MP 1,2

      Ale $\neg\neg\mathcal{C} = \neg(\neg\mathcal{C}) = \neg\mathcal{A} = \mathcal{A}^{\tilde{\sigma}}$, čiže aj v tomto prípade
      $$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{A}^{\tilde{\sigma}}.$$

   (b) Nech $\mathcal{A} = \mathcal{C}_1 \Rightarrow \mathcal{C}_2$ Formuly $\mathcal{C}_1, \mathcal{C}_2$ sú formuly hĺbky menšej ako n, a preto podľa indukčného predpokladu pre ľubovoľný vektor $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_k)$ pravdivostných hodnôt premenných $B_1, \ldots, B_k$ formúl $\mathcal{C}_1, \mathcal{C}_2$ platí
   $$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{C}_1^{\tilde{\sigma}}.,$$
   $$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{C}_2^{\tilde{\sigma}}.$$
   Budeme rozlišovať tri prípady vzhľadom na pravdivostné hodnoty, ktoré nadobúdajú formuly $\mathcal{C}_1, \mathcal{C}_2$:

      i. $\mathcal{C}_1^{\tilde{\sigma}} = \neg\mathcal{C}_1$ (Všimnite si, že tento prípad zahŕňa dve možnosti: $\mathcal{C}_2^{\tilde{\sigma}} = \neg\mathcal{C}_2$ aj $\mathcal{C}_2^{\tilde{\sigma}} = \mathcal{C}_2$). Uvedomte si, že ide vlastne o tautológiu $(0 \Rightarrow \mathcal{C}_2)$. Potom zrejme $\mathcal{A}^{\tilde{\sigma}} = \mathcal{A}$. Ukážeme, že v tomto prípade tvrdenie vety platí:

1.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \mathcal{C}_1^{\tilde{\sigma}} \quad (= \neg\mathcal{C}_1)$	indukčný predpoklad
2.		$\vdash \neg\mathcal{C}_1 \Rightarrow (\mathcal{C}_1 \Rightarrow \mathcal{C}_2)$	T4
3.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash (\mathcal{C}_1 \Rightarrow \mathcal{C}_2)$	MP 1,2

      Ale $(\mathcal{C}_1 \Rightarrow \mathcal{C}_2) = \mathcal{A}$, $\mathcal{A} = \mathcal{A}^{\tilde{\sigma}}$.

ii. $\mathcal{C}_2^{\tilde{\sigma}} = \mathcal{C}_2$ (aj tento prípad zahŕňa dve možnosti: $\mathcal{C}_1^{\tilde{\sigma}} = \mathcal{C}_1$ a $\mathcal{C}_1^{\tilde{\sigma}} = \neg\mathcal{C}_1$). Ak $\mathcal{C}_2^{\tilde{\sigma}} = \mathcal{C}_2$, $\mathcal{A}^{\tilde{\sigma}} = \mathcal{A}$ (v podstate ide o tautológiu $(\mathcal{C}_1 \Rightarrow 1)$)

1.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \mathcal{C}_2^{\tilde{\sigma}} \quad (= \mathcal{C}_2)$	indukčný predpoklad
2.		$\vdash \mathcal{C}_2 \Rightarrow (\mathcal{C}_1 \Rightarrow \mathcal{C}_2)$	A1
3.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash (\mathcal{C}_1 \Rightarrow \mathcal{C}_2)$	MP 1,2

Ale $(\mathcal{C}_1 \Rightarrow \mathcal{C}_2) = \mathcal{A}, \quad \mathcal{A}^{\tilde{\sigma}} = \mathcal{A}$, a teda aj v tomto prípade tvrdenie vety platí. Ostáva nám dokázať posledný prípad:

iii. $\mathcal{C}_1^{\tilde{\sigma}} = \mathcal{C}_1$ a $\mathcal{C}_2^{\tilde{\sigma}} = \neg\mathcal{C}_2$. (Ide o prípad $(1 \Rightarrow 0) \equiv 0$). To znamená, že $\mathcal{A}^{\tilde{\sigma}} = \neg\mathcal{A} = \neg(\mathcal{C}_1 \Rightarrow \mathcal{C}_2)$.

1.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \mathcal{C}_1 \quad (= \mathcal{C}_1^{\tilde{\sigma}})$	indukčný predpoklad
2.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \neg\mathcal{C}_2 \quad (= \mathcal{C}_2^{\tilde{\sigma}})$	indukčný predpoklad
3.		$\vdash \mathcal{C}_1 \Rightarrow (\neg\mathcal{C}_2 \Rightarrow \neg(\mathcal{C}_1 \Rightarrow \mathcal{C}_2))$	T 7
4.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash (\neg\mathcal{C}_2 \Rightarrow \neg(\mathcal{C}_1 \Rightarrow \mathcal{C}_2))$	MP 1,3
5.	$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k}$	$\vdash \neg(\mathcal{C}_1 \Rightarrow \mathcal{C}_2)$	MP 2,4

□

Úloha 9.8. *Napíšte tabuľky pravdivostných hodnôt elementárnych logických funkcií: konjunkcie, disjunkcie,ekvivalencie, súčtu modulo 2 a ďalších a ukážte pre ne platnosť vety! Napríklad*

A_1	A_2	$A_1 \& A_2$		
0	0	0	$\neg A_1, \neg A_2$	$\vdash \neg(A_1 \& A_2)$
0	1	0	$\neg A_1, A_2$	$\vdash \neg(A_1 \& A_2)$
1	0	0	$A_1, \neg A_2$	$\vdash \neg(A_1 \& A_2)$
1	1	0	A_1, A_2	$\vdash (A_1 \& A_2)$

V predchádzajúcej vete sme vytvorili predpoklady potrebné pre dôkaz nasledujúcej vety, ktorá spolu s tvrdením vety 9.4 dokazuje jednoznačnosť vzťahu medzi teorémemi (formulami odvodenými z axióm) výrokového počtu na jednej strane a tautológiami (formulami algebry logiky, ktoré sú pravdivé pre všetky hodnoty svojich logických premenných.)

Veta 9.6. *(O úplnosti výrokového počtu.) Ak je formula $\mathcal{A}$ teórie $\mathcal{L}$ tautológiou, tak potom je teorémou teórie $\mathcal{L}$.*

Dôkaz. Nech je formula $\mathcal{A}$ teórie $\mathcal{L}$ s výrokovými premennými $B_1, \ldots, B_k$. Potom podľa vety 9.5

$$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{A}^{\tilde{\sigma}}.$$

Keďže $\mathcal{A}$ je tautológiou, tak pre ľubovoľný vektor pravdivostných hodnôt $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_k)$ svojich výrokových premenných $B_1, \ldots, B_k$ formula $\mathcal{A}$ nadobúda pravdivostnú hodnotu 1. To znamená, že pre ľubovoľný vektor pravdivostných hodnôt $\tilde{\sigma}$, $\mathcal{A}^{\tilde{\sigma}} = \mathcal{A}$ a teda

$$B_1^{\sigma_1}, \ldots, B_k^{\sigma_k} \vdash \mathcal{A}^{\tilde{\sigma}}.$$

Zoberieme teraz dva vektory pravdivostných hodnôt, ktoré majú prvých $k-1$ zložiek rovnakých a odlišujú sa len v poslednej zložke:

$$\tilde{\sigma} = (\sigma_1, \ldots, \sigma_{k-1}, 1),$$

$$\tilde{\sigma}' = (\sigma_1, \ldots, \sigma_{k-1}, 0).$$

Ukážeme,že formulu $\mathcal{A}$ možno odvodiť z predpokladov $B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}$. Pripomíname, že platí $B^0 = \neg B$ a $B^1 = B$. Potom

1.	$B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}, B_k, \neg B_k$		hypotézy
2.	$B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}, B_k$	$\vdash \mathcal{A}$	veta 9.5
3.	$B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}, \neg B_k$	$\vdash \mathcal{A}$	veta 9.5
4.	$B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}$	$\vdash B_k \Rightarrow \mathcal{A}$	VD 1,2
5.	$B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}$	$\vdash \neg B_k \Rightarrow \mathcal{A}$	VD 1,3
6.		$\vdash (B_k \Rightarrow \mathcal{A}) \Rightarrow ((\neg B_k \Rightarrow \mathcal{A}) \Rightarrow \mathcal{A})$	T 10
7.	$B_1^{\sigma_1}, \ldots, B_{k-1}^{\sigma_{k-1}}$	$\vdash \mathcal{A}$	$2\times$ VD 4,5,6

V predchádzajúcom odvodení sme zmenšili počet predpokladov na $(k-1)$. Ak celý postup zopakujeme ešte $(k-1)$-krát dostaneme požadovaný výsledok;

$$\vdash \mathcal{A}.$$

□

Úloha 9.9. *Spravte dôkaz vety 9.6 pre nejakú jednoduchú tautológiu!*

Úloha 9.10. *Njdite aspoň 10 rozličných tautológií. Zapíšte ich ako formuly teórie $\mathcal{L}$ a dokážte ich!*

Úloha 9.11. *Dokážte, že formula algebry logiky $\mathcal{B}$ obsahujúca logické operátory $\&, \vee, \equiv$ a prípadne iné, je tautológiou algebry logiky práve vtedy, keď formula $\mathcal{A}$, ktorú dostaneme z formuly $\mathcal{B}$ nahradením operátorov $\&, \vee, \equiv$ podľa pravidiel D1-D3 je teorémou teórie $\mathcal{L}$!*

Úloha 9.12. *Dokážte, že pre ľubovoľné formuly $\mathcal{A}, \mathcal{B}, \mathcal{C}$ teórie $\mathcal{L}$ sú nasledujúce formuly tautológiami algebry logiky a teda aj teorémami teórie $\mathcal{L}$:*

(a) $((A \vee \mathcal{B}) \& (A \Rightarrow \mathcal{C}) \& (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow \mathcal{C}$,

(b) $(A \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \equiv ((A \& \mathcal{B}) \Rightarrow \mathcal{C})$.

9.4 Neprotirečivosť výrokového počtu

Logické teórie sa vytvárali preto, lebo sa ukázalo, že prirodzený jazyk je nepresný a možno v ňom formulovať protirečivé tvrdenia (napríklad „táto veta je nepravdivá“). Zdalo sa, že matematická logika by mohla byť základom, na ktorom by bolo možné postaviť teórie, v ktorých by sa nevyskytovali protirečenia.[4] Ideálne by bolo mať pre nejakú

[4]Podrobnejšie sa týmito problémami budeme zaoberať v kapitole xxx.

oblasť teóriu, ktorá by umožnila preveriť ľubovoľné tvrdenie týkajúce sa danej oblasti a rozhodnúť, či je pravdivé, alebo nie. Vybudovať takúto teóriu, ale najmä dokázať, že má požadovanú vlastnosť, môže byť náročný alebo až nedosiahnuteľný cieľ. Isté však je, že teória, ktorá nerozlišuje medzi pravdivými a nepravdivými formulami, nebude použiteľná na odvodzovanie matematických tvrdení. Preto požadujeme, aby v logickej teórii nebolo možné odvodzovať nepravdivé tvrdenia. Teória, ktorá spĺňa takúto požiadavku, sa nazýva *neprotirečivá (bezposporná.)*

Upresníme najprv spomenuté pojmy a potom budeme skúmať, či je výrokový počet vyjadrený pomocou teórie $\mathcal{L}$ bezposporný.

Teória sa nazýva *absolútne bezospornou (neprotirečivou)*, ak v nej existuje formula, ktorá nie je teorémou. Teória sa nazýva *bezospornou (neprotirečivou) v relatívnom zmysle vzhľadom na negáciu*, ak neobsahuje takú formulu $\mathcal{A}$ takú, že formuly $\mathcal{A}$ a $\neg\mathcal{A}$ sú súčasne teorémy danej teórie.

Čo by sa stalo, ak by nejaké formuly $\mathcal{A}$ a $\neg\mathcal{A}$ boli teorémy teórie $\mathcal{L}$? Potom by ľubovoľná formula teórie $\mathcal{L}$ bola zároveň jej teorémou—stačí použiť teorému $\mathcal{A} \Rightarrow (\neg\mathcal{A} \Rightarrow \mathcal{B})$ a 2-krát pravidlo modus ponens). V takom prípade by sa pojem pravdivosti (obsah, sémantika formuly) stotožnil so syntaktickou správnosťou (forma, syntax formuly). Ukážeme, že sme teóriu $\mathcal{L}$ vybudovali dobre a že je bezosporná.

Veta 9.7. *Teória $\mathcal{L}$ je bezposporná v absolútnom aj relatívnom zmysle.*

Dôkaz. Najprv ukážeme, že teória $\mathcal{L}$ je bezposporná v relatívnom zmysle vzhľadom na negáciu. Nech je formula $\mathcal{A}$ teorémou teórie $\mathcal{L}$. Potom podľa vety 9.4 je aj tautológiou. Ale to znamená, že negácia tejto formuly, formula $\neg\mathcal{A}$ je *kontradikciou* (formulou, ktorá nie je pravdivá pre žiaden vektor hodnôt svojich výrokových premenných). Ak by formula $\neg\mathcal{A}$ bola teorémou teórie $\mathcal{L}$, tak potom by podľa vety 9.4 musela byť tautológiou, spor.

Predpokladajme že teória $\mathcal{L}$ nie je bezposporná v absolútnom zmysle. Potom každá jej formula je teorémou, a teda pre ľubovoľnú jej formulu $\mathcal{A}$ je aj formula $\neg\mathcal{A}$ teorémou teórie $\mathcal{L}$. Ale potom teória $\mathcal{L}$ nie je bezosporná v relatívnom zmysle. Spor. □

Tú istú axiomatickú teóriu (v našom prípade výrokový počet), možno vybudovať na rozličných systémoch axióm. Uvedieme niektoré alternatívne systémy axióm, pomocou ktorých sa dá vybudovať axiomatická teória pre výrokový počet. (V ďalšom budú označovať symboly $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E}$ ľubovoľné formuly):

$\mathcal{L}_1$ Logické spojky $\Rightarrow, \neg$, pravidlo odvodenia modus ponens, axiómy:

(A1) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$

(A2) $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$

(A3) $(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$

$\mathcal{L}_2$ Logické spojky $\Rightarrow, \neg, \&, \vee$, pravidlo odvodenia modus ponens, axiómy:

(A1) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$

(A2) $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$

(A3) $(\mathcal{A}\&\mathcal{B}) \Rightarrow \mathcal{A}$

(A4) $(\mathcal{A}\&\mathcal{B}) \Rightarrow \mathcal{B}$

(A5) $(\mathcal{A} \Rightarrow (\mathcal{B}) \Rightarrow (\mathcal{A}\&\mathcal{B})$

(A6) $\mathcal{A} \Rightarrow (\mathcal{A} \vee \mathcal{B})$

(A7) $\mathcal{B} \Rightarrow (\mathcal{A} \vee \mathcal{B})$

(A8) $(\mathcal{A} \Rightarrow \mathcal{C}) \Rightarrow ((\mathcal{B} \Rightarrow \mathcal{C}) \Rightarrow ((\mathcal{A} \vee \mathcal{B}) \Rightarrow \mathcal{C})$

(A9) $(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow ((\mathcal{A} \Rightarrow \neg\mathcal{B}) \Rightarrow \neg\mathcal{A})$

(A10) $\neg\neg\mathcal{A} \Rightarrow \mathcal{A}$

$\mathcal{L}_3$ Logické spojky $\Rightarrow, \neg, \&, \vee$, pravidlo odvodenia modus ponens, axióma:

(A1) $[(((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\neg\mathcal{C} \Rightarrow \neg\mathcal{D})) \Rightarrow \mathcal{C}) \Rightarrow \mathcal{E}] \Rightarrow [(\mathcal{E} \Rightarrow \mathcal{A}) \Rightarrow (\mathcal{D} \Rightarrow \mathcal{A})]$.

$\mathcal{L}_4$ Logické spojky $\Rightarrow, \neg$, axiómy:

(A1) $\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A})$

(A2) $(\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Rightarrow ((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}))$

(A3) $(\neg\mathrm{B} \Rightarrow \neg\mathrm{A})((\neg\mathrm{B} \Rightarrow \mathrm{A}) \Rightarrow \mathrm{B})$

kde $\mathrm{A}, \mathrm{B}, \mathrm{C}$ sú výrokové premenné. K pravidlu modus ponens pridáme pravidlo substitúcie, ktoré možno zapísať takto

$$\frac{\mathcal{B}(\mathrm{A})}{\mathcal{B}(\mathcal{A})},$$

t.j. vo formule $\mathcal{B}$ možno nahradiť všetky výskyty premennej A formulou $\mathcal{A}$.

Úloha 9.13. *Dokážte ekvivalentnosť teórií $\mathcal{L}$ a $\mathcal{L}_1$. Návod: odvoďte A3 teórie $\mathcal{L}$ pomocou axióm teórie $\mathcal{L}_1$.*

Úloha 9.14. *Dokážte teorémy T2-T10 v teórii $\mathcal{L}_1$.*

Úloha 9.15. *Vyjadrite axiómy teórie $\mathcal{L}_2$ ako formuly teórie $\mathcal{L}$ a zostrojte ich odvodenie!*

Úloha 9.16. *Zostrojte odvodenie axiómy (A1) teórie $\mathcal{L}_3$ v teórii $\mathcal{L}$!*

Úloha 9.17. *Odvoďte tautológie 1-40 z kapitoly 2 v teórii $\mathcal{L}_2$!*

9.5 Nezávislosť axióm výrokového počtu

Videli sme, že existuje viacero systémov axióm, ktoré umožňujú vybudovať axiomatickú teóriu výrokového počtu. Ak ste vyriešili úlohy z predchádzajúcej časti, zistili ste, že uvedené systémy axióm sú ekvivalentné; t.j. že axiómy jedného systému sú odvoditeľné pomocou axióm druhého systému a pravidla modus ponens. To znamená, že formuly, ktoré sú teorémami jednej z uvedených axiomatických teórií, sú aj teorémami ostatných axiomatických teórií. Ostáva otvorená jedna otázka: sú všetky axiómy a pravidlá

odvodenia potrebné? Veď teórie $\mathcal{L}$ a $\mathcal{L}_1$ majú 3 axiómy, teória $\mathcal{L}_2$ má až 10 axióm a teória $\mathcal{L}_3$ vystačí s jedinou axiómou. Koľko axióm a pravidiel odvodenia vlastne potrebujeme na to, aby sme vybudovali axiomatickú teóriu (v našom prípade výrokového počtu)? Uvedené otázky súvisia s dôležitou vlastnosťou axiomatických teórií—s nezávislosťou axióm. Zavedieme tento pojem formálne.

Nech je **AX** množina axióm a **P** je množina pravidiel odvodenia axiomatickej teórie $\mathcal{T}$ a nech $\mathbf{X} \subset \mathbf{AX}$. Budeme hovoriť, že množina **X** je nezávislá, ak existuje teoréma teórie $\mathcal{T}$, ktorá sa nedá odvodiť pomocou axióm $\mathbf{AX} - \mathbf{X}$ a pravidiel odvodenia **P**.

Nájsť teorému, ktorá sa nedá odvodiť z nejakej podmnožiny axióm, ale najmä dokázať, že takúto vlastnosť skutočne má, je vo všeobecnosti ťažká úloha. Jednoduchšie je ukázať, že žiadna z axióm teórie $\mathcal{T}$ sa nedá odvodiť pomocou ostatných axióm a pravidiel odvodenia. Na to sa používa nasledujúci postup: predpokladajme, že $\mathbf{AX} = \{A1, \ldots, An\}$ a potrebujeme ukázať nezávislosť napríklad axiómy $A1$. Nájdeme nejaké zobrazenie Φ, ktoré transformuje axiómu $A1$ ináč, ako ostatné axiómy a pravidlo modus ponens špecifickosť axióm $\{A2, \ldots, An\}$ zachováva. Presnejšie povedané, existuje vlastnosť $\mathcal{P}_\Phi$, taká, že

1. $\mathcal{P}_\Phi(\Phi(Ai))$ pre $i = 2, \ldots n$,
2. ak pre formuly $A, A \Rightarrow B$ teórie $\mathcal{T}$ platí $\mathcal{P}_\Phi(A), \mathcal{P}_\Phi(A \Rightarrow B)$, tak potom platí aj $\mathcal{P}_\Phi(B)$;
3. $\neg\mathcal{P}_\Phi(\Phi(A1))$.

Ak by $A1$ bola odvodená z axióm $\{A2, \ldots, An\}$ pomocou pravidla modus ponens, potom by musela mať vlastnosť $\mathcal{P}_\Phi$; keďže túto vlastnosť nemá, musí byť nezávislá od ostatných axióm.

Príklad 9.4. *Ukážeme, že axióma* **A3** *nezávisí od ostatných axióm a pravidiel odvodenia teórie $\mathcal{L}$. Nech je $\mathcal{A}$ ľubovoľná formula teórie $\mathcal{L}$. Zobrazenie Φ bude definované na množine formúl teórie $\mathcal{L}$ nasledovne:*

1. $\Phi(\neg\mathcal{A}) = \mathcal{A}$,
2. $\Phi(\mathcal{A} \Rightarrow \mathcal{B}) = \Phi(\mathcal{A}) \Rightarrow \Phi(\mathcal{B})$,
3. $\Phi(A) = A$, *kde* A *je logická premenná.*

Ináč povedané, zobrazenie Φ odstráni z formuly $\mathcal{A}$ všetky negácie; ak formula $\mathcal{A}$ negácie neobsahuje, tak potom $\Phi(\mathcal{A}) = \mathcal{A}$. Ak použijeme zobrazenie Φ na axiómy **A1** *a* **A2**, *dostávame* **A1** *a* **A2**; *t.j. formuly, ktoré sú tautológie. Použijeme teraz zobrazenie Φ na axiómu* **A3** *(kvôli jednoduchosti predpokladáme, že formuly $\mathcal{A}, \mathcal{B}$ už žiadne negácie neobsahujú):*

$$\Phi[(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})] = [(\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow ((\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})].$$

Transformáciou axiómy **A3** *dostávame formulu, ktorá nie je tautológiou (za formuly $\mathcal{A}, \mathcal{B}$ stačí dosadiť nepravidivé tvrdenia, napríklad $\neg(A \Rightarrow A)$ a dostávame dokonca kontradikciu).*

Ostáva ešte pravidlo modus ponens: ak sú formuly $\Phi(\mathcal{A} \Rightarrow \mathcal{B})$ a $\Phi(\mathcal{A})$ tautológie, potom je tautológiou aj formula $\Phi(\mathcal{B})$, pretože $\Phi(\mathcal{A} \Rightarrow \mathcal{B}) = \Phi(\mathcal{A}) \Rightarrow \Phi(\mathcal{B})$ a z $\Phi(\mathcal{A}) \Rightarrow \Phi(\mathcal{B})$ a $\Phi(\mathcal{A})$ vyplýva $\Phi(\mathcal{B})$. To znamená, že akékoľvek odvodenie z axióm **A1** *a* **A2** *pomocou pravidla modus ponens vedie k formulám, ktorých obrazy sú v zobrazení Φ tautológiami, zatiaľ čo obraz axiómy* **A3** *v zobrazení Φ tautológiou nie je.*

Aj pre ostatné axiómy a pravidlo modus ponens by sme museli nájsť podobné zobrazenia, ktoré by umožnili ukázať ich principiálnu odlišnosť od ostatných axióm (prípadne pravidiel odvodenia). Využívajú sa na to zobrazenia, ktoré zobrazujú formuly výrokového počtu na formuly troj- a viachodnotovej logiky. Keďže na konštrukcii týchto zobrazení nie je nič zaujímavého (okrem toho, že sa ich podarí nájsť), čitateľa odkazujeme na knihu [14] na nasledujúce cvičenie a na tomto mieste uvedieme akurát konečný výsledok.

Veta 9.8. *Schéma axióm* **A1**, **A2**, **A3** *ponens teórie $\mathcal{L}$ je nezávislá.*

Úloha 9.18. *Dokážte nezávislosť axióm* **A1** *a* **A2** *teórie $\mathcal{L}$! Návod ([14]): Na dôkaz nezávislosti axiómy* **A1** *zavedieme zobrazenie Φ_1, ktoré priraďuje formulám teórie $\mathcal{L}$ formuly trojhodnotovej logiky (formuly $\mathcal{A}, \mathcal{B}$ sú ľubovoľné formuly teórie $\mathcal{L}$)*

1. $\Phi_1(\neg\mathcal{A}) = \neg\Phi_1(\mathcal{A})$,
2. $\Phi_1(\mathcal{A} \Rightarrow \mathcal{B}) = \Phi_1(\mathcal{A}) \Rightarrow \Phi_1(\mathcal{B})$,
3. $\Phi_1(A) = x$, *kde* A *je výroková premenná teórie* $\mathcal{L}$ *a* x *je premenná trojhodnotovej logiky.*

Operácie negácia a implikácia v trojhodnotovej logike definujeme pre tento prípad nasledovne:

x	$\neg x$
0	1
1	1
2	0

x	y	$x \Rightarrow y$
0	0	0
1	0	2
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	0
2	2	0

Preskúmajte, aké hodnoty nadobúdajú formuly $\Phi_1(\mathbf{A1}), \Phi_1(\mathbf{A2}), \Phi_1(\mathbf{A3})$ ak ich premenné nadobúdajú hodnotu 0; a zistite, či aplikáciou pravidla modus ponens na formuly (trojhodnotovej logiky) nadobúdajúce hodnotu 0 dostávame formulu nadobúdajúcu hodnotu 0.

Podobne ako v predchádzajúcom prípade, zavedieme na dôkaz nezávislosti axiómy **A2** *zobrazenie* Φ_2*, ktoré priraďuje formulám teórie* $\mathcal{L}$ *formuly trojhodnotovej logiky. Operácie negácia a implikácia v trojhodnotovej logike definujeme v tomto prípade nasledovne:*

x	$\neg x$
0	1
1	0
2	1

x	y	$x \Rightarrow y$
0	0	0
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	1
1	2	0
2	2	0

Preskúmajte, ktoré hodnoty zachovávajú obrazy jednotlivých axióm a pravidlo modus ponens v trojhodnotovej logike a zistite, čím sa odlišuje axióma **A2** *od ostatných axióm!*

Úloha 9.19. *Čo by sa stalo, keby sme medzi axiómy teórie* $\mathcal{L}$ *zaradili formulu, ktorá*

1. *je tautológiou,*
2. *nie je tautológiou*

Úloha 9.20. *Čo by sa stalo, keby sme v systéme axióm teórie* $\mathcal{L}$ *nahradili niektorú z jej axióm jej negáciou?*

Aj keď sa na prvý pohľad môže zdať, že nezávislosť axoóm má zmysel skúmať len kvôli tomu, aby sme „nadbytočnú“ axiómu mohli vylúčiť a tak optimalizovať systém axióm danej teórie, nie je tomu tak. Prvou známou axiomatickou matematickou teóriou boli Euklidove Základy. Dvetisíc rokov sa diskutovalo o tom, či piata axióma (o rovnobežkách) je skutočnou axiómou alebo len teorémou odvoditeľnou z ostatných axióm. Potvrdenie piatej axiómy ako plnoprávnej axiómy euklidovskej geometrie začiatkom 19. storočia viedlo nielen k vytvoreniu nových neeuklidovských geometrií, ale aj k zmene pohľadu na axiomatizovateľnosť teórií. Namiesto hľadania toho správneho, najlepšieho systému axióm sa pripúšťa existenia rozličných (rovnako dobrých) systémov axióm a vytvárajú sa alternatívne matematické teórie v matematickej logike, teórii množín a inde.

Kapitola 10

Predikátový počet

Pomocou výrokového počtu možno úspešne popísať a odvodiť mnohé tvrdenia. Existujú však úsudky, na vyjadrenie ktorých výrokový počet nestačí. Preskúmajme napríklad klasický úsudok:

P: Každý človek je smrteľný.
Q: Sokrates je človek.
R: Sokratesje smrteľný.

Uvedený úsudok je úplne korektný, ale tvrdenie **R** nie je korektným dôsledkom tvrdení **P** a **Q** vo výrokovom počte. Výrokový počet nemá prostriedky na vyjadrenie tvrdení typu **P,Q,R**. V tejto kapitole zavedieme zložitejšiu logiku, ako je výrokovový počet; tzv. *logiku prvého rádu (predikátový počet)*. Predikátový počet bude rozšírením výrokového počtu a v porovnaní s ním bude mocť vyjadrovať vlastnosti prvkov, popisovať vytváranie nových prvkov a skúmať vlastnosti množín prvkov. Jazyk predikátového počtu bude obsahovať v porovnaní s výrokovým počtom ďalšie dve množiny (predikáty a termy) a množina logických spojok a pomocných symbolov sa rozšíri o všeobecný a existenčný kvantifikátor. Zavedieme aj nové odvodzovacie pravidlá a axiómy, ktoré umožnia pracovať s formulami, obsahujúcimi kvantifikátory, termy a predikáty. Logická teória, ktorú takýmto spôsobom vytvoríme, nebude podstatne zložitejšia ako výrokový počet. Ako ukážeme neskôr, pomocou tejto logiky bude možné formalizovať mnohé tvrdenia prirodzeného jazyka, ale čo je podstatnejšie, aj mnohé matematické teórie.

Prikročíme k systematickému budovaniu predikátového počtu.

10.1 Jazyk predikátového počtu 1. rádu

1. Abeceda Σ pozostáva z nasledujúcich množín:

(a) spočítateľná množina *predmetových premenných* $x, y, z, x_i, \ldots,$

(b) spočítateľná množina *predmetových konštánt* $a, b, c, a_i, \ldots,$

(c) nanajvýš spočítateľná množina *predikátových symbolov* $P_1, P_2, \ldots,$

(d) nanajvýš spočítateľná množina *funkcionálnych symbolov* $F_1, F_2, \ldots,$

(e) množina logických spojok, kvantifikátorov a pomocných symbolov $\{\forall, \exists, \neg, \Rightarrow, \equiv, \vee, \&, \vdash, "(", ")", ".", ", \ldots\}$.

Poznámka. Symboly pre označenie premenných, logické spojky, kvantifikátory a pomocné symboly nezávisia od konkrétnej teórie, ale využívajú sa vo všetkých teóriách, ktoré ako logický základ používajú predikátový počet. Preto ich nazývame *logickými symbolmi*. Predmetové konštanty, predikátové symboly a funkcionálne symboly určujú oblasť, v ktorej sa daná teória používa—nazývame ich preto *špeciálnymi symbolmi*, alebo o nich hovoríme ako o *signatúre* danej *formálnej teórie*.

Zavedené pojmy ilustrujeme na príklade.

Príklad 10.1. *Budeme formalizovať aritmetiku prirodzených čísel.*

1. *Predmetové premenné budú premenné definované na množine* $\mathbb{N}$,
2. *keďže potrebujeme vyjadriť rovnosť nejakých číselných výrazov, zavedieme binárny predikátový symbol* $P_1^2(x, y)$ *taký, že*

$$P_1^2(x, y) = \begin{cases} 0 & x \neq y; \\ 1 & x = y. \end{cases}$$

3. *Ak by sme sa chceli zaoberať usporiadaním na množine prirodzených čísel, mohli by sme zaviesť aj ďalší predikátový symbol* $P_2^2(x, y)$*, ktorý bude vyjadrovať reláciu* $\leq$ *na množine prirodzených čísel:*

$$P_2^2(x, y) = \begin{cases} 0 & x > y; \\ 1 & x \leq y. \end{cases}$$

4. *Aby sme mohli počítať s prirodzenými číslami, zavedieme pomocou funkcionálnych symbolov dve operácie na množine* $\mathbb{N}$*. Unárny funkcionálny symbol* $f_1^1(x) = x + 1$ *vyjadruje operáciu nasledovníka (kvôli ľahšiemu zapamätaniu sa zvykne označovať symbolom* $S(x)$*, successor.) Druhý funkcionálny symbol bude binárny a bude vyjadrovať operáciu sčítania prirodzených čísel:* $f_1^2(x, y) = x + y$*. Podobne by sme mohli zaviesť binárny funkcionálny symbol pre operáciu násobenia a pod.*
5. *Konštantným symbolom by sme mohli označiť ľubovoľné prirodzené číslo. Zavedieme dve konštanty,* a, b *ktoré budú reprezentovať prirodzené čísla* $0, 1$*, ktoré sú dôležité tak z hľadiska aritmetických operácií (násobenia a sčítania), ako aj usporiadania prirodzených čísel. V logickej teórii budeme kvôli prehľadnosti konštanty* $0, 1$ *vyjadrovať pomocou ich bežného číselného zápisu, t,j, ako* $0, 1$.

Zhrnieme to. Oblasť D, ktorú chceme popísať pomocou predikátového počtu 1. rádu pozostáva z nejakých prvkov, nad ktorými je možné uskutočňovať nejaké operácie a medzi ktorými existujú nejaké vzťahy. Konkrétnym prvkom, ktoré sú z nejakých dôvodov dôležité, priradíme predmetové konštanty, ostatné prvky

oblasti D môžu byť hodnotami predmetových premenných. Operácie nad prvkami popíšeme pomocou funkcionálnych prvkov; n-árnemu zobrazeniu $D^n \to D$ priradíme n-árny funkcionálny symbol f_i^n. Nakoniec, vzťahy medzi prvkami budeme popisovať pomocou relácií a tým budeme priraďovať predikátové symboly. Z tohoto hľadiska možno n-árny predikátový symbol P_i^n chápať aj ako reláciu na D^n, aj ako zobrazenie $P_i^n : D^n \to \{0, 1\}$.

2. Výrazy a termy predikátového počtu sú definované ako ľubovoľné konečné postupnosti symbolov abecedy Σ. Táto definícia si všíma akurát to, či je postupnosť symbolov konečná a či pozostáva zo správnych symbolov. Vôbec sa nezaoberá tým, či výraz spĺňa nejaká syntaktické požiadavky a už vôbec nie tým, či má nejaký zmysel. A tak popri rozumných výrazoch spĺňajú definíciu výrazu predikátového počtu aj postupnosti zjavne nezmyselné, ako sú napríklad:$\Rightarrow\Rightarrow \forall\neg\exists, \exists\exists\forall\exists z \& \vee P_2^2(x, y), ((()))$ a pod. Gramaticky správne vytvorené výrazy budú tvoriť formuly predikátového počtu. Formuly predikátového počtu dávajú po vyhodnotení logickú hodnotu. Vo výrokovom počte sa formuly vytvárali z logických premenných pomocou logických operátorov/operácií. Jedinými objektami logického charakteru (t.j. takými, ktoré po vyhodnotení dávajú logickú hodnotu), o ktorých sme doteraz v predikátovom počte hovorili, boli predikáty. Do predikátov môžeme zatiaľ dosadzovať predmetové premenné a konštanty. Ale pomocou funkcionálnych symbolov môžeme vytvárať komplikovanejšie objekty, ktoré v konečnom dôsledku nadobudnú hodnotu z množiny oblasti D. Všetky takéto objekty zahrnieme do pojmu *term*.

1. každá predmetová premenná a predmetová konštanta je term,
2. ak je $f_i^{(n)}$ n-árny funkcionálny symbol a $t_1, \ldots t_n$ sú termy, tak potom je aj $f_i^{(n)}(t_1, \ldots t_n)$ term,
3. výraz je termom práve vtedy, ak je termom podľa (a) alebo podľa (b). Iných termov nieto.

3. Formuly predikátového počtu Ak do predikátových symbolov dosadíme termy, dostávame výrazy, ktoré po vyhodnotení dávajú logickú hodnotu. Keďže predikátové symboly majú zo syntaktického hľadiska najjednoduchšiu štruktúru (neobsahujú logické spojky, ani kvantifikátory), predikátové symboly, do ktorých sme dosadili termy budeme nazývať *elementárnymi (atomárnymi, atomickými) formulami*: Nech P_i^n je n-árny predikátový symbol, $t_1, \ldots, t_n$ sú termy, potom $P_i^n(t_1, \ldots, t_n)$ je elementárna formula. Teraz môžeme zaviesť pojem formuly predikátového počtu.

(a) Každá elementárna formula je formula,

(b) Ak sú $\mathcal{A}, \mathcal{B}$ formuly a x je predmetová premenná, tak potom aj výrazy $\neg\mathcal{A}$, $(\mathcal{A} \Rightarrow \mathcal{A})$ a $(\forall x \mathcal{A})$ sú formuly (predikátového počtu).

(c) Výraz je formulou práve vtedy, ak je formulou podľa pravidla (a) alebo (b). Iných formúl predikátového počtu niet.

Formula $\mathcal{A}$ vo formule $(\forall x \mathcal{A})$ sa nazýva *oblasťou pôsobenia všeobecného kvantifikátora* $\forall x$. Chvíľu sa budeme dívať na formuly ako na reťazce znakov. Výskyt premennej x vo formule $\mathcal{A}$ budeme nazývať *viazaný*, ak

- sa x nachádza v oblasti pôsobenia kvantifikátora $\forall x$, (t.j. formula $\mathcal{A}$ obsahuje podreťazec $\forall x\mathcal{B}$ a všetky výskyty premennej x v takej podformule $\mathcal{B}$ sú viazané) alebo
- x sa nachádza bezprostredne za všeobecným kvantifikátorom.

Všetky výskyty premennej x vo formule $\mathcal{A}$, ktoré nie sú viazané, sa nazývajú *voľné*. Ak formula $\mathcal{A}$ neobsahuje voľné výskyty premennej x, tak potom sú formuly $\mathcal{A}$ a $\forall x\mathcal{A}$ ekvivalentné. (Takáto situácia nastáva aj v prípade, keď formula $\mathcal{A}$ neobsahuje premennú x). Ak chceme zdôrazniť, že premenná x vo formule $\mathcal{A}$ má (voľný) výskyt, zapisujeme formulu $\mathcal{A}$ v podobe $\mathcal{A}(x)$. Ako to vyzerá s oblasťou pôsobenia všeobecného kvantifikátora vo formule $\forall x\mathcal{A}$, ak formula $\mathcal{A}$ predstavuje negáciu, alebo implikáciu nejakých formúl? Ak má formula $\mathcal{A}$ tvar negácie; $\mathcal{A} = \neg\mathcal{B}$, tak potom je oblasťou pôsobenia kvantifikátora $\forall x\neg\mathcal{B}$ formula $\mathcal{B}$. Implikácia ukončuje oblasť pôsobenia kvantifikátora; ak má formula $\mathcal{A}$ tvar $\mathcal{B}_1 \Rightarrow \mathcal{B}_2$, tak vo formule $\forall x\mathcal{B}_1 \Rightarrow \mathcal{B}_2$ (a formula $\mathcal{B}_2$ neobsahuje všeobecný kvantifikátor $\forall x$) je oblasťou pôsobenia kvantifikátora $\forall x$ len formula $\mathcal{B}_1$.

Príklad 10.2. *Oblasť pôsobenia kvantifikátora môžeme ovplyvniť pomocou zátvoriek. Uvažujme formulu $\mathcal{A}$, ktorá má tvar $\mathcal{B}_1 \Rightarrow \mathcal{B}_2$ a vyznačme rôzne oblasti pôsobenia kvantifikátora $\forall x$:*

(a)	$\forall x\mathcal{B}_1 \Rightarrow \mathcal{B}_2$	$\forall x\boxed{\mathcal{B}_1} \Rightarrow \mathcal{B}_2$
(b)	$\forall x\mathcal{B}_1 \Rightarrow \forall x\mathcal{B}_2$	$\forall x\boxed{\mathcal{B}_1} \Rightarrow \forall x\boxed{\mathcal{B}_2}$
(c)	$\mathcal{B}_1 \Rightarrow \forall x\mathcal{B}_2$	$\mathcal{B}_1 \Rightarrow \forall x\boxed{\mathcal{B}_2}$
(d)	$\forall x(\mathcal{B}_1 \Rightarrow \mathcal{B}_2)$	$\forall x\boxed{\mathcal{B}_1 \Rightarrow \mathcal{B}_2}$

Poznámky. (1) Ostatné logické spojky, t.j. konjunkciu &, disjunkciu $\vee$ a ekvivalenciu $\equiv$ sme neuvádzali, pretože ich definujeme rovnako ako vo výrokovom počte pomocou negácie $\neg$ a implikácie $\Rightarrow$.

(2) Nezavádzali sme zvlášť existenčný kvantifikátor $\exists$, pretože ten môžeme vyjadriť pomocou všeobecného kvantifikátora a negácie:

$$\exists x\mathcal{A} \equiv \neg\forall x\neg\mathcal{A}.$$

Príklad 10.3. *Pozrieme sa na výskyty premenných v rozličných formulách. Kvôli jednoduchosti budeme predpokladať, že sa skúmané formuly skladajú z elementárnych formúl, ktoré už neobsahujú logické spojky ani kvantifikátory a elementárne formuly obsahujú len tie premenné, ktoré sú explicitne uvedené.*

(1)	$\mathcal{A}_1^2(x,y)$	$\mathcal{A}_1(x,y)$
(2)	$\forall x\mathcal{A}_1^2(x,y) \Rightarrow \forall y\mathcal{A}_1^1(y)$	$\mathcal{A}_2(x,y)$
(3)	$\forall x\mathcal{A}_1^2(x,y) \Rightarrow \forall y\mathcal{A}_2^2(x,y)$	$\mathcal{A}_3(x,y)$.

Obe premenné x, y majú len voľné výskyty vo formule $\mathcal{A}_1(x,y)$. Premenná x má vo formule $\mathcal{A}_2(x,y)$ len viazané výskyty a premenná y má vo formule $\mathcal{A}_2(x,y)$ aj viazané výskyty (podformula $\forall y\mathcal{A}_1^1(y)$), aj voľné výskyty (podformula $\forall x\mathcal{A}_1^2(x,y)$). Napokon v poslednej formule $\mathcal{A}_3(x,y)$ majú obe premenné x, y aj voľné aj viazané výskyty: premenná x má viazané výskyty vo formule $\forall x\mathcal{A}_1^2(x,y)$ a voľné výskyty vo

formule $\forall y \mathcal{A}_2^2(x,y)$ *a naopak premenná* y *má voľné výskyty vo formule* $\forall x \mathcal{A}_1^2(x,y)$ *a viazané výskyty vo formule* $\forall y \mathcal{A}_2^2(x,y)$.

Premenná x sa nazýva *voľnou (viazanou)* premennou vo formule $\mathcal{A}$, ak v tejto formule existujú voľné (viazané) výskyty premennej x. To znamená, že tá istá premenná môže byť v jednej formule aj voľná aj viazaná. Ak chceme vyjadriť, že sú všetky výskyty premennej x vo formule $\mathcal{A}$, viazané (voľné), musíme použiť formuláciu: premenná x nemá vo formule $\mathcal{A}$, voľné, (viazané) výskyty. Pridávaním kvantifikátorov pred formulu môžeme dosiahnuť stav, keď formula nebude obsahovať voľné premenné, takáto formula sa nazýva *uzavretá formula*.

Za voľné premenné vo formulách môžeme dosadzovať termy. Nie každý term však možno dosadiť za ľubovoľnú voľnú premennú. Skôr ako sformulujeme všeobecné pravidlo, uvedieme príklad, na ktorom ukážeme, na čo si pri dosadzovaní treba dávať pozor:

Uvažujeme formulu $\mathcal{A}(x,y)$ definovanú nasledovne $\mathcal{A}(x,y) = \exists y(x \neq y)$. Premenná x vo formule $\mathcal{A}(x,y)$ je voľná. Ak však za ňu dosadíme term—premennú y, dostávame zjavne nepravdivé tvrdenie $\mathcal{A}(y,y) = \exists y(y \neq y)$.

Predpokladajme, že je daná formula $\mathcal{A}$; premenná x_i za ktorú chceme dosadzovať term t, ktorý obsahuje nejaké predmetové premenné. Term t môžeme dosadiť za premennú x_i vo formule $\mathcal{A}$ len vtedy, ak sa žiaden voľný výskyt premennej x_i nenachádza v oblasti pôsobenia kvantifikátora $\forall x_j$, kde x_j je voľná premenná termu t. Ak je táto podmienka splnená, hovoríme, že *term* t *je voľný vzhľadom na premennú* x_i *vo formule* $\mathcal{A}$.

Príklad 10.4. *Uvedieme niekoľko príkladov termov a formúl a pozrieme sa, kedy termy možno dosadzovať za premenná vo formulách a kedy nie.*

1. *Term* x *(predmetová premenná) je voľný vzhľadom na* x *vo formule* $\mathcal{A}(x)$.
2. *Každý term, ktorý neobsahuje premenné (napríklad konštanta) je voľný vzhľadom na ľubovoľnú premenné v ľubovoľnej formule.*
3. *Ak žiadna voľná premenná termu* t *nie je viazaná vo formule* $\mathcal{A}$*, term* t *je voľný vzhľadom na ľubovoľnú premennú vo formule* $\mathcal{A}$.
4. *Každý term je voľný vzhľadom na premennú* x_i*, ak formula* $\mathcal{A}$ *neobsahuje voľné výskyty premennej* x_i.
5. *Term* x_i *je voľný vzhľadom na* x_j *vo elementárnej formule* $\mathcal{A}(x_j)$*, ale nie je voľný vzhľadom na* x_j *vo formule* $\forall x_i \mathcal{A}(x_j)$.
6. *Term* $t^2(x_1,x_3)$ *je voľný vzhľadom na premennú* x_1 *vo formule*

$$\forall x_2 \mathcal{A}_1^2(x_1,x_2) \Rightarrow \mathcal{A}_1^1(x_1),$$

ale nie je voľný vzhľadom na premennú x_1 *vo formule*

$$\exists x_3 \forall x_2 \mathcal{A}_1^2(x_1,x_2) \Rightarrow \mathcal{A}_1^1(x_1).$$

4. Axiómy predikátového počtu. Nech sú $\mathcal{A}, \mathcal{B}, \mathcal{C}$ ľubovoľné formuly predikátového počtu. Potom sú nasledujúce formuly (logické) *axiómy predikátového počtu*:

(A1) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$

(A2) $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C}) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$

(A3) $(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$

(A4) $\forall x \mathcal{A}(x) \Rightarrow \mathcal{A}(t)$, kde t je term voľný vzhľadom na premennú x vo formule $\mathcal{A}(x)$

(A5) $\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \forall x \mathcal{B}(x))$ ak formula $\mathcal{A}$ neobsahuje voľné výskyty premennej x

Prvé tri axiómy poznáme z výrokového počtu. Zastavíme sa krátko pri posledných dvoch.

Ukážeme najprv, že požiadavka, by bol t term voľný vzhľadom na premennú x vo formule $\mathcal{A}(x)$ je podstatná. Uvažujme formulu $\forall x \exists y(x \neq y)$, ktorá je pravdivá, ak premenné x, y nadobúdajú aspoň dve rozličné hodnoty. Teraz použijeme axiómu (A4) a položíme $t = y$. Dostávame tvrdenie

$$\forall x \exists y(x \neq y) \Rightarrow \exists y(y \neq y),$$

čo je (stačí vziať napríklad $x, y \in \{0, 1\}$) zjavne nepravdivé tvrdenie.

Podobne, ak v axióme (A5) upustíme od predpokladu, že formula $\mathcal{A}$ neobsahuje voľné výskyty premennej x, dostávame sa do ťažkostí:

Vyberieme veľmi jednoduché formuly $\mathcal{A} = \mathcal{B} = P(x)$, pričom premenná x nadobúda dve hodnoty; $x \in \{0, 1\}$ a definujeme predikát $P(x)$ pomocou identického zobrazenia;

$$P(x) = \begin{cases} 0 & x = 0; \\ 1 & x = 1. \end{cases}$$

Formula $\forall x\,[P(x) \Rightarrow P(x)]$ je vždy pravdivá (dosaďte za premennú x hodnoty $0, 1$ a presvedčte sa o tom!), ale formula $\forall x P(x)$ je nepravdivá (lebo $P(0) = 0$) a formula $P(x)$ nadobúda aj hodnotu 0 aj hodnotu 1. Potom formula

$$\forall x\,[P(x) \Rightarrow P(x)] \Rightarrow [P(x) \Rightarrow \forall x P(x)]$$

nie je všeobecne pravdivá—stačí dosadiť za jediný voľný výskyt premennej x hodnotu 1.

5. Pravidlá odvodenia. V predikátovom počte vystačíme s dvoma pravidlami odvodenia.

(a) Modus ponens (MP): ak sú odvodené formuly $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$ predikátového počtu, tak potom je odvodená aj formula $\mathcal{B}$:

$$\frac{\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}}{\mathcal{B}}.$$

(b) Pravidlo zovšeobecnenia (generalizácie, GEN): Ak je odvodená formula $\mathcal{A}$ predikátového počtu, tak potom je odvodená aj formula $\forall x \mathcal{A}$:

$$\frac{\mathcal{A}}{\forall x \mathcal{A}}.$$

Poznámka. Formulu $\mathcal{B}$, ktorá bola odvodená z formúl $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$ pomocou pravidla modus ponens budeme nazývať bezprostredným dôsledkom formúl $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$ (na základe pravidla modus ponens). Podobne, formulu $\forall x \mathcal{A}$, odvodenú z formuly $\mathcal{A}$ pomocou pravidla zovšeobecnenia, budeme nazývať bezprostredným dôsledkom formuly $\mathcal{A}$ (na základe pravidla zovšeobecnenia).

V predikátovom počte zavádzame podobne ako vo výrokovom počte aj pojmy odvodenie, odvodená formula, hypotéza, formula odvodená z množiny hypotéz a teoréma. Týmto pojmom venujeme nasledujúcu podkapitolu.

10.2 Odvodzovanie v predikátovom počte

> You can only find truth with logic if you have already found truth without it.
> G.K. Chesterton

Keď už máme zavedené všetky základné pojmy predikátového počtu, naučíme v predikátovom počte formálne odvodzovať tvrdenia a potom ukážeme, ako možno použiť predikátový počet ako logický základ pri výstavbe matematických teórií. Odvodenie v predikátovom počte definujeme podobne ako odvodenie vo výrokovom počte.

Definícia 10.1. *Nech je Γ množina formúl predikátového počtu. Potom postupnosť formúl $\mathcal{A}_1, \ldots, \mathcal{A}_n$ predikátového počtu nazveme odvodením predikátového počtu (formuly $\mathcal{A}_n$) z množiny hypotéz Γ, ak pre ľubovoľnú formulu $\mathcal{A}_i$ tejto postupnosti platí*

1. *$\mathcal{A}_i$ je axióma predikátového počtu, alebo*
2. *$\mathcal{A}_i \in \Gamma$ ($\mathcal{A}_i$ je hypotéza z množiny Γ), alebo*
3. *$\mathcal{A}_i$ je bezprostredným dôsledkom formúl $\mathcal{A}_j, \mathcal{A}_k$; $j, k < i$ na základe pravidla modus ponens, alebo*
4. *$\mathcal{A}_i$ je bezprostredným dôsledkom formuly $\mathcal{A}_j, j < i$ na základe pravidla zovšeobecnenia.*

Skutočnosť, že pre formulu $\mathcal{A}_n$ existuje odvodenie (predikátového počtu) z množiny hypotéz Γ, zapisujeme symbolicky takto:

$$\Gamma \vdash \mathcal{A}_n.$$

Podobne ako vo výrokovom počte zavedieme pojem teorémy predikátového počtu.

Definícia 10.2. *Ak existuje odvodenie formuly $\mathcal{A}_n$ predikátového počtu z prázdnej množiny hypotéz, tak potom formulu $\mathcal{A}_n$ nazveme teorémou predikátového počtu.*

Poznámka. Keďže množina hypotéz Γ je prázdna, v odvodení teorémy $\mathcal{A}_n$ predikátového počtu s vyskytujú len axiómy a formuly odvodené z axióm pomocou pravidiel odvodenia, t.j. teorémy. Ak sme rozumne vybrali axiómy a pravidlá odvodenia, znamená to, že teorémy predikátového počtu sú formuly, ktoré majú rovnakú pravdivostnú hodnotu ako axiómy.[1]

Vo výrokovom počte nám veta o dedukcii veľmi pomáhala zjednodušovať dôkazy. Podobná veta platí aj v predikátovom počte, ale môžeme ju používať len za istých doplňujúcich predpokladov. Najprv ukážeme, že nejaké (aj keď zatiaľ nevieme aké) obmedzenia na použitie vety o dedukcii sú v predikátovom počte potrebné.

Príklad 10.5. *Uvažujme predikát* $P(x)$ *z predchádzajúceho príkladu, definovaný pomocou identického zobrazenia na množine* $\{0,1\}$. *Keďže* $P(0) = 0$, *tvrdenie (v tomto prípade dokonca výrok)* $\forall x P(x)$ *má pravdivostnú hodnotu* 0.

Pre ľubovoľnú formulu $\mathcal{A}$ predikátového počtu možno pomocou pravidla zovšeobecnenie odvodiť formulu $\forall x\mathcal{A}$. To znamená, že sa dá odvodiť aj $P(x) \vdash \forall x P(x)$. Ak by sme teraz použili vetu o dedukcii, dotstali by sme sa k tvrdeniu

$$P(x) \Rightarrow \forall x P(x)$$

ktoré je zjavne nepravdivé (stačí dosadiť $x = 1$.)

Ukážeme, za akých predpokladov možno v odvodeniach v predikátovom počte používať vetu o dedukcii. Na to potrebujeme zaviesť pojem *závislosti formúl*.

Definícia 10.3. *Nech je daná množina formúl (hypotéz) Γ, $\mathcal{A} \in \Gamma$ a nech $B_1, \ldots, B_n$ je nejaké odvodenie z Γ. Budeme hovoriť, že formula B_i závisí od formuly $\mathcal{A}$ v tomto odvodení, ak*

1. $\mathcal{B}_i = \mathcal{A}$,
2. *$\mathcal{B}_i$ je bezprostredným dôsledkom nejakých formúl $\mathcal{B}_j, \mathcal{B}_k, j, k < i$ tohto odvodenia na základe pravdidla modus ponens a aspoň jedna z formúl $\mathcal{B}_j, \mathcal{B}_k$ závisí v tomto odvodené od formuly $\mathcal{A}$,*
3. *$\mathcal{B}_i$ je bezprostredným dôsledkom formuly $\mathcal{B}_j, j < i$ na základe pravidla zovšeobecnenia a formula $\mathcal{B}_j$ v tomto odvodení závisí od formuly $\mathcal{A}$.*

Z definície závislosti formúl vyplýva, že ak v odvodení formula B_i závisí od formuly $\mathcal{A}$, tak sa v tomto odvodení musí formula $\mathcal{A}$ niekde vyskytnúť. Ak nie, tak je pre odvodenie formuly B_i zbytočná. Tento poznatok presnejšie formuluje nasledujúca veta.

Veta 10.1. *Ak formula $\mathcal{B}$ v odvodení nezávisí od formuly $\mathcal{A}$ a $\Gamma, \mathcal{A} \vdash \mathcal{B}$, tak potom $\Gamma \vdash \mathcal{B}$*

[1] Aj v predikátovom počte má význam skúmať také otázky ako je bezospornosť, úplnosť, nezávislosť systému axióm. Na rozdiel od výrokového počtu však získať odpovede na tieto otázky nebude jednoduché.

Dôkaz. Nech je $B_1, \ldots, B_n; B_n = B$ je také odvodenie formuly B z hypotéz $\Gamma, \mathcal{A}$ v ktorom formula $\mathcal{B}$ nezávisí od formuly $\mathcal{A}$. Matematickou indukciou vzhľadom na dĺžku odvodenia dokážeme, že potom $\Gamma \vdash \mathcal{B}$.

Nech $n = 1$. Potom $\mathcal{B}_1 = \mathcal{B}$ a $\mathcal{B}_1 \vdash \mathcal{B}$. Ale $\mathcal{B}_1 \neq \mathcal{A}$, a teda $\Gamma \vdash \mathcal{B}$.

Predpokladajme, že tvrdenie platí pre všetky $k < n$ a nech formula $\mathcal{B}$ má odvodenie dĺžky n. Podľa definície odvodenia formula $\mathcal{B}_n = \mathcal{B}$ môže byť:

1. axióma, alebo
2. $\mathcal{B}_n \in \Gamma$, alebo
3. $\mathcal{B}_n = \mathcal{A}$, alebo
4. $\mathcal{B}_n = \forall x B_l(x)$, alebo $\mathcal{B}_n$ je dôsledkom formúl $\mathcal{B}_j = (\mathcal{B}_i \Rightarrow \mathcal{B}_n)$ podľa pravidla modus ponens.

V prvých dvoch prípadoch zrejme $\Gamma \vdash \mathcal{B}$. Tretí prípad nemôže nastať, lebo $\mathcal{B}$ nezávisí od $\mathcal{A}$.

Konečne v poslednom prípade formuly $\mathcal{B}_i, \mathcal{B}_j, \mathcal{B}_l$ nemôžu závisieť od $\mathcal{A}$ (ináč by aj formula $\mathcal{B}$ závisela od $\mathcal{A}$). To znamená, že podľa indukčného predpokladu

$$\Gamma \vdash \mathcal{B}_i, \quad \Gamma \vdash \mathcal{B}_j, \quad \Gamma \vdash \mathcal{B}_l$$

pretože $i, j, l < n$. Potom však $\Gamma \vdash \mathcal{B}_n$, pretože formula $\mathcal{B}_n$ bola odvodená pomocou pravidla zovšeobecnenia, resp. modus ponens z formuly (formúl), ktoré nezáviseli od formuly $\mathcal{A}$. □

Veta 10.2. *(O dedukcii).veta!o dedukcii) Nech $\Gamma, \mathcal{A} \vdash \mathcal{B}$ a nech existuje také odvodenie formuly $\mathcal{B}$ z množiny hyptéz $\Gamma \bigcup \{\mathcal{A}\}$, v ktorom sa pri žiadnom použití pravidla zovšeobecnenia na formuly, ktoré v tomto odvodení závisia od formuly $\mathcal{A}$ kvantifikátorom neviaže žiadna voľná premenná vyskytujúca sa vo formule $\mathcal{A}$. Potom*

$$\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}.$$

Dôkaz. Nech $\mathcal{B}_1, \ldots, \mathcal{B}_n; \mathcal{B}_n = \mathcal{B}$ je odvodenie formuly $\mathcal{B}$, ktoré vyhovuje podmienkam vety. Matematickou indukciou dokážeme, že $\forall i \leq n$ platí

$$\Gamma \vdash \mathcal{B}_i.$$

Nech $i = 1$. Môžu nastať tieto 3 prípady:

1. $\mathcal{B}_1$ je axióma. Potom

1.		$\vdash \mathcal{B}_1$	
2.		$\vdash \mathcal{B}_1 \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_1)$	H1
3.		$\vdash (\mathcal{A} \Rightarrow \mathcal{B}_1)$	modus ponens 1,2
4.	Γ	$\vdash (\mathcal{A} \Rightarrow \mathcal{B}_1)$	

2. $\mathcal{B}_1 \in \Gamma$. Potom

1.	Γ	$\vdash \mathcal{B}_1$	
2.		$\vdash \mathcal{B}_1 \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_1)$	H1
3.	Γ	$\vdash (\mathcal{A} \Rightarrow \mathcal{B}_1)$	modus ponens 1,2

3. $\mathcal{B}_1 = \mathcal{A}$. V tomto prípade

$$\vdash \mathcal{A} \Rightarrow \mathcal{A} \qquad \text{T1}$$

a teda

$$\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{A}.$$

Predpokladáme, že tvrdenie platí pre prípady $i < n$. Ukážeme, že tvrdenie vety platí aj pre $i = n$. Podobne, ako pre $i = 1$ riešime prípady

1. formula $\mathcal{B}_n$ je axióma,
2. $\mathcal{B}_n \in \Gamma$,
3. $\mathcal{B}_n = \mathcal{A}$.

   K uvedeným trom pribúdajú však ďalšie možnosti:

4. formula $\mathcal{B}_n$ je dôsledkom formúl $\mathcal{B}_j = \mathcal{B}_k \Rightarrow \mathcal{B}_n, \mathcal{B}_k$ podľa pravidla modus ponens. Vtomto prípade však formuly $\mathcal{B}_j, \mathcal{B}_k$ majú odvodenia dĺžky menšej ako n a podľa indukčného predpokladu platí:

1.	Γ	$\vdash \mathcal{A} \Rightarrow (\mathcal{B}_k \Rightarrow \mathcal{B}_n)$	indukčný predpoklad
2.	Γ	$\vdash \mathcal{A} \Rightarrow \mathcal{B}_k$	indukčný predpoklad
3.		$\vdash (\mathcal{A} \Rightarrow (\mathcal{B}_k \Rightarrow \mathcal{B}_n)) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}_k) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_n))$	A2
4.	Γ	$\vdash ((\mathcal{A} \Rightarrow \mathcal{B}_k) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_n))$	MP 1,3
5.	Γ	$\vdash (\mathcal{A} \Rightarrow \mathcal{B}_n))$	MP 2,4.

5. Formula $\mathcal{B}_n$ bola odvodená pomocou pravidla zovšeobecnenia z formuly $\mathcal{B}_i : \mathcal{B}_n = \forall x \mathcal{B}_i(x)$. Keďže aj dĺžka odvodenia formuly $\mathcal{B}_i$ je kratšia ako n, podľa indukčného predpokladu platí

$$\Gamma \vdash (\mathcal{A} \Rightarrow \mathcal{B}_i).$$

   Pre formuly $\mathcal{B}_i$ a $\mathcal{A}$ môže nastať jedna z dvoch možností:

   - formula $\mathcal{B}_i$ nezávisí od formuly $\mathcal{A}$, alebo
   - x nie je voľná premenná vo formule $\mathcal{A}$.

   Rozoberieme obidve možnosti. Ak formula $\mathcal{B}_i$ nezávisí od formuly $\mathcal{A}$, tak potom podľa vety 10.1 dostávame

1.	Γ	$\vdash \mathcal{B}_i$	indukčný predpoklad
2.	Γ	$\vdash \forall x \mathcal{B}_i$	GEN 1
3.		$\vdash \forall x \mathcal{B}_i \Rightarrow (\mathcal{A} \Rightarrow \forall x \mathcal{B}_i)$	(A1)
2.	Γ	$\vdash \mathcal{A} \Rightarrow \forall x \mathcal{B}_i$	MP 2,3

Ostáva posledná možnosť, x nie je voľná premenná vo formule $\mathcal{A}$. Potom

1.	$\Gamma \vdash (\mathcal{A} \Rightarrow \mathcal{B}_i)$	indukčný predpoklad
2.	$\Gamma \vdash \forall x(\mathcal{A} \Rightarrow \mathcal{B}_i)$	GEN 1
3.	$\vdash \forall x(\mathcal{A} \Rightarrow \mathcal{B}_i) \Rightarrow (\mathcal{A} \Rightarrow \forall x\mathcal{B}_i)$	A5
4.	$\Gamma \vdash (\mathcal{A} \Rightarrow \forall x\mathcal{B}_i)$	MP 2,3.

□

Podmienky vety o dedukcii sú na prvý pohľad dosť komplikované. Niekedy vystačíme aj so slabšími ale jednoduchšími predpokladmi.

Dôsledok 1. *Ak $\Gamma, \mathcal{A} \vdash \mathcal{B}$ a existuje také odvodenie formuly $\mathcal{B}$, v ktorom sa nepoužíva pravidlo zovšeobecnenia na žiadne premenné, ktoré sú voľné vo formule $\mathcal{A}$, tak potom $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$.*

Dôsledok 2. *Ak je formula $\mathcal{A}$ uzavretá a $\Gamma, \mathcal{A} \vdash \mathcal{B}$, tak potom $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$.*

Teraz vyslovíme a dokážeme niekoľko teorém predikátového počtu.

Veta 10.3. *Nech sú $\mathcal{A}, \mathcal{B}$ ľubovoľné formuly predikátového počtu, potom nasledujúce formuly sú teorémy predikátového počtu:*

(a) $\forall x\forall y\mathcal{A}(x, y) \Rightarrow \forall y\forall x\mathcal{A}(x, y)$

(b) $\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\forall x\mathcal{A} \Rightarrow \forall x\mathcal{B})$

(c) $\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\exists x\mathcal{A} \Rightarrow \exists x\mathcal{B})$

(d) $\forall x_1 \ldots \forall x_n\mathcal{A}(x_1, \ldots, x_n) \Rightarrow \mathcal{A}$,

(e) $\mathcal{A}(x) \Rightarrow \exists x\mathcal{A}(x)$,

(f) $\forall x\mathcal{A}(x) \Rightarrow \exists x\mathcal{A}(x)$,

(g) $\exists x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\forall x\mathcal{A} \Rightarrow \exists x\mathcal{B})$,

(h) $(\forall x\mathcal{A} \Rightarrow \exists x\mathcal{B}) \Rightarrow \exists x(\mathcal{A} \Rightarrow \mathcal{B})$,

(i) $\forall x(\mathcal{A}\&\mathcal{B}) \equiv (\forall x\mathcal{A}\&\forall x\mathcal{B})$,

(j) $\exists x\exists y\mathcal{A}(x, y) \equiv \exists y\exists x\mathcal{A}(x, y)$,

(k) $\exists x\exists y\mathcal{A}(x, y) \Rightarrow \forall y\exists x\mathcal{A}(x, y)$.

Ak premenná x nie je voľná vo formule $\mathcal{A}$, tak

(l) $\mathcal{A} \equiv \forall x\mathcal{A}$,

(m) $\mathcal{A} \equiv \exists x\mathcal{A}$,

(n) $\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \equiv (\mathcal{A} \Rightarrow \forall x\mathcal{B})$

(o) $\forall x(\mathcal{B} \Rightarrow \mathcal{A}) \equiv (\exists x\mathcal{B} \Rightarrow \mathcal{A})$

Ak premenná y nie je voľná vo formule $\mathcal{B}$, ani vo formule $\mathcal{A}(x)$ tak

(p) $\forall x(\mathcal{A}(x) \Rightarrow \mathcal{B}) \equiv \exists y(\mathcal{A}(y) \Rightarrow \mathcal{B})$

(q) $\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}) \equiv \forall y(\mathcal{A}(y) \Rightarrow \mathcal{B})$

(r) $(\mathcal{B} \Rightarrow \forall x\mathcal{A}(x)) \equiv \forall y(\mathcal{B} \Rightarrow \mathcal{A}(y))$,

(s) $(\mathcal{B} \Rightarrow \exists x\mathcal{A}(x)) \equiv \exists y(\mathcal{B} \Rightarrow \mathcal{A}(y))$.

Dôkaz.

(a)

1.			$\forall x\forall y\mathcal{A}(x,y)$	H1
2.		$\vdash$	$\forall x\forall y\mathcal{A}(x,y) \Rightarrow \forall y\mathcal{A}(x,y)$	(A4)
3.		$\vdash$	$\forall y\mathcal{A}(x,y) \Rightarrow \mathcal{A}(x,y)$	(A4)
4.	H1	$\vdash$	$\forall y\mathcal{A}(x,y)$	(MP 1,2)
5.	H1	$\vdash$	$\mathcal{A}(x,y)$	(MP 4,3)
6.	H1	$\vdash$	$\forall x\mathcal{A}(x,y)$	(GEN 5)
7.	H1	$\vdash$	$\forall y\forall x\mathcal{A}(x,y)$	(GEN 6)
8.		$\vdash$	$\forall x\forall y\mathcal{A}(x,y) \Rightarrow \forall y\forall x\mathcal{A}(x,y)$	(VD 1,7)

(b)

1.			$\forall x(\mathcal{A} \Rightarrow \mathcal{B})$	H1
2.			$\forall x\mathcal{A}(x)$	H2
3.			$\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	(A4)
4.	H1	$\vdash$	$(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	(MP 1,3)
5.			$\forall x\mathcal{A}(x) \Rightarrow \mathcal{A}(x)$	(A4)
6.	H2	$\vdash$	$\mathcal{A}(x)$	(MP 2,5)
7.	H1,H2	$\vdash$	$\mathcal{B}(x)$	(MP 4,6)
8.	H1,H2	$\vdash$	$\forall x\mathcal{B}(x)$	(GEN 7)
9.		$\vdash$	$\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\forall x\mathcal{A} \Rightarrow \forall x\mathcal{B})$	2 krát VD 1,2,8

(c)

1.			$\forall x(\mathcal{A} \Rightarrow \mathcal{B})$	H1
2.			$\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	(A4)
3.	H1	$\vdash$	$(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	(MP 1,2)
4.		$\vdash$	$(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow (\neg\mathcal{B}(x) \Rightarrow \neg\mathcal{A}(x))$	kontrapozícia negácie
5.	H1	$\vdash$	$(\neg\mathcal{B}(x) \Rightarrow \neg\mathcal{A}(x))$	(MP 3,4)
6.	H1	$\vdash$	$\forall x(\neg\mathcal{B}(x) \Rightarrow \neg\mathcal{A}(x))$	(GEN 5)
7.		$\vdash$	$\forall x(\neg\mathcal{B}(x) \Rightarrow \neg\mathcal{A}(x)) \Rightarrow (\forall x\neg\mathcal{B}(x) \Rightarrow \forall x\neg\mathcal{A}(x))$	teoréma (b)
8.		$\vdash$	$(\forall x\neg\mathcal{B}(x) \Rightarrow \forall x\neg\mathcal{A}(x)) \Rightarrow (\neg\forall x\neg\mathcal{A}(x) \Rightarrow \neg\forall x\neg\mathcal{B}(x))$	kontrapozícia negácie
9.		$\vdash$	$\forall x(\neg\mathcal{B}(x) \Rightarrow \neg\mathcal{A}(x)) \Rightarrow (\exists x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x))$	sylog. 7,8
10.	H1	$\vdash$	$(\exists x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x))$	(MP 6,9)
11.		$\vdash$	$\forall x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\exists x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x))$	(VD 1,10)

V ďalších odvodeniach budeme stručnejší a uvedieme len kľúčové kroky odvodenia. Oporúčame čitateľovi, aby spravil aj tie kroky, ktoré sme v odvodeniach len naznačili.

(d) Stačí n-$\times$ použiť axiómu (A4) a pravidlo sylogizmu.

(e)

1.	$\vdash$	$\forall x\neg\mathcal{A}(x) \Rightarrow \neg\mathcal{A}(x)$	(A4)
2.	$\vdash$	$(\forall x\neg\mathcal{A}(x) \Rightarrow \neg\mathcal{A}(x)) \Rightarrow (\neg\neg\mathcal{A}(x) \Rightarrow \neg\forall x\neg\mathcal{A}(x))$	kontrapozícia negácie
3.	$\vdash$	$\mathcal{A}(x) \Rightarrow \exists x\mathcal{A}(x)$	(MP 1,2)

(g)

1.			$\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	H1
2.			$\exists x\mathcal{A}(x)$	H2
3.		$\vdash$	$\mathcal{A}(x) \Rightarrow (\neg\mathcal{B}(x) \Rightarrow \neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)))$	teoréma
4.		$\vdash$	$\forall x[\mathcal{A}(x) \Rightarrow (\neg\mathcal{B}(x) \Rightarrow \neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)))]$	GEN 3
5.		$\vdash$	$\forall x\mathcal{A}(x) \Rightarrow \forall x(\neg\mathcal{B}(x) \Rightarrow \neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)))$	teoréma (b)
6.	H2	$\vdash$	$\forall x(\neg\mathcal{B}(x) \Rightarrow \neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)))$	MP 2,5
7.	H2	$\vdash$	$\forall x\neg\mathcal{B}(x) \Rightarrow \forall x\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	teoréma (b)
8.	H2	$\vdash$	$[\forall x\neg\mathcal{B}(x) \Rightarrow \forall x\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))] \Rightarrow$	
			$[\neg\forall x\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \neg\forall x\neg\mathcal{B}(x)]$	kontrapozícia negácie
9.	H2	$\vdash$	$\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \exists x\mathcal{B}(x)$	MP 7,8
10.	H1,H2	$\vdash$	$\exists x\mathcal{B}(x)$	MP 1,9
11.		$\vdash$	$\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow (\forall x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x))$	$2\times$ VD 1,2,10

(h)

1.	$\forall x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x)$		H1
2.	$\neg\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	$(= \forall x\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}))$	H2

Všimnite si, že ako druhú hypotézu sme si dali negáciu formuly, ktorú chceme dokázať.

3.		$\vdash$	$\forall x\neg(\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x)) \Rightarrow \neg(\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x))$	(A4)
4.	H2	$\vdash$	$\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	MP 2,3
5.		$\vdash$	$\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \mathcal{A}(x)$	teoréma
6.		$\vdash$	$\neg(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \neg\mathcal{B}(x)$	teoréma
7.	H2	$\vdash$	$\mathcal{A}(x)$	MP 4,5
8.	H2	$\vdash$	$\neg\mathcal{B}(x)$	MP 4,6
9.	H2	$\vdash$	$\forall x\mathcal{A}(x)$	GEN 7
10.	H1,H2	$\vdash$	$\exists x\mathcal{B}(x)$	MP 1,9
11.	H2	$\vdash$	$\forall x\neg\mathcal{B}(x) \quad (= \neg\exists x\mathcal{B}(x))$	GEN 8
12.		$\vdash$	$[\neg\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \neg\exists x\mathcal{B}(x)] \Rightarrow$	
		$\Rightarrow$	$[[\neg\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \exists x\mathcal{B}(x)] \Rightarrow \exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))]$	(A3)
13.		$\vdash$	$[\neg\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))] \Rightarrow \neg\exists x\mathcal{B}(x)$	(VD 2,11)
14.		$\vdash$	$[[\neg\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \exists x\mathcal{B}(x)] \Rightarrow \exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	MP 12,13
15.	H1	$\vdash$	$\neg\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \Rightarrow \exists x\mathcal{B}(x)$	VD 10,2
16.	H1	$\vdash$	$\exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	MP 14,15
17.		$\vdash$	$(\forall x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x)) \Rightarrow \exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$	VD 1,16

(i) Konjunkciu môžeme vyjadriť pomocou implikácie a negácie takto: $\mathcal{A}\&\mathcal{B} \stackrel{\text{def}}{\equiv} \neg(\mathcal{A} \Rightarrow \neg\mathcal{B})$ a ekvivalenciu pomocou implikácie ne konjunkcie $\mathcal{A} \equiv \mathcal{B} \stackrel{\text{def}}{\equiv} \mathcal{A} \Rightarrow \mathcal{B}\&\mathcal{B} \Rightarrow \mathcal{A}$ a potom dokazovať ekvivalentnú formulu, obsahujúcu už len operácie implikácie a negácie. Zjednodušíme dôkaz tým, že využijeme teorémy (tautológie) výrokového počtu, popisujúce vlastnosti konjunkcie a dokážeme, že nasledujúce dve formuly (implikácie) sú teorémy:

- $\forall x(\mathcal{A}(x)\&\mathcal{B}(x)) \Rightarrow (\forall x\mathcal{A}\&\forall x\mathcal{B}(x))$
- $(\forall x\mathcal{A}\&\forall x\mathcal{B}(x)) \Rightarrow \forall x(\mathcal{A}(x)\&\mathcal{B}(x))$

1.			$\forall x(\mathcal{A}(x)\&\mathcal{B}(x))$	H1
2.			$\forall x(\mathcal{A}(x)\&\mathcal{B}(x)) \Rightarrow (\mathcal{A}(x)\&\mathcal{B}(x))$	A4
3.	H1	$\vdash$	$(\mathcal{A}(x)\&\mathcal{B}(x))$	MP 1,2
4.		$\vdash$	$(\mathcal{A}(x)\&\mathcal{B}(x)) \Rightarrow \mathcal{A}(x)$	teoréma
5.		$\vdash$	$(\mathcal{A}(x)\&\mathcal{B}(x)) \Rightarrow \mathcal{B}(x)$	teoréma
6.	H1	$\vdash$	$\mathcal{A}(x)$	MP 3,4
7.	H1	$\vdash$	$\mathcal{B}(x)$	MP 3,5
8.	H1	$\vdash$	$\forall x\mathcal{A}(x)$	GEN 6
9.	H1	$\vdash$	$\forall x\mathcal{B}(x)$	GEN 7
10.		$\vdash$	$\forall x\mathcal{A}(x) \Rightarrow (\forall x\mathcal{B}(x) \Rightarrow (\forall x\mathcal{A}\&\forall x\mathcal{B}(x)))$	teoréma
11.	H1	$\vdash$	$\forall x\mathcal{A}\&\forall x\mathcal{B}(x)$	$2\times$ MP 5,8,10
12.		$\vdash$	$\forall x(\mathcal{A}(x)\&\mathcal{B}(x)) \Rightarrow (\forall x\mathcal{A}\&\forall x\mathcal{B}(x))$	VD 1,11

Dokážeme opačnú implikáciu.

1.			$\forall x\mathcal{A}(x)\&\forall x\mathcal{B}(x)$	H1
2.		$\vdash$	$\forall x\mathcal{A}(x)\&\forall x\mathcal{B}(x) \Rightarrow \forall x\mathcal{A}(x)$	teoréma
3.		$\vdash$	$\forall x\mathcal{A}(x)\&\forall x\mathcal{B}(x) \Rightarrow \forall x\mathcal{B}(x)$	teoréma
4.	H1	$\vdash$	$\forall x\mathcal{A}(x)$	MP 1,2
5.	H1	$\vdash$	$\forall x\mathcal{B}(x)$	MP 1,3
6.		$\vdash$	$\forall x\mathcal{A}(x) \Rightarrow \mathcal{A}$	(A4)
7.		$\vdash$	$\forall x\mathcal{B}(x) \Rightarrow \mathcal{B}$	(A4)
8.	H1	$\vdash$	$\mathcal{A}(x)$	VD 4,6
9.	H1	$\vdash$	$\mathcal{B}(x)$	VD 5,7
10.		$\vdash$	$\mathcal{A}(x) \Rightarrow (\mathcal{B}(x) \Rightarrow (\mathcal{A}\&\mathcal{B}(x)))$	teoréma
11.	H1	$\vdash$	$(\mathcal{A}\&\mathcal{B}(x))$	$2\times$ VD 8,9,10
12.	H1	$\forall x \vdash$	$(\mathcal{A}\&\mathcal{B}(x))$	GEN 11
13.		$\vdash$	$(\forall x\mathcal{A}\&\forall x\mathcal{B}(x)) \Rightarrow \forall x(\mathcal{A}(x)\&\mathcal{B}(x))$	VD 1,12

(k)

1.	$\vdash$	$\forall y\mathcal{A}(x,y) \Rightarrow \mathcal{A}(x,y)$	A4
2.	$\vdash$	$\neg\mathcal{A}(x,y) \Rightarrow \neg\forall y\mathcal{A}(x,y)$	kontrapozícia negácie
3.	$\vdash$	$\forall x\neg\mathcal{A}(x,y) \Rightarrow \forall x\neg\forall y\mathcal{A}(x,y)$	GEN 2
4.	$\vdash$	$\neg\forall x\neg\forall y\mathcal{A}(x,y) \Rightarrow \neg\forall x\neg\mathcal{A}(x,y)$	kontrapozícia negácie
5.	$\vdash$	$\forall y(\exists y\mathcal{A}(x,y) \Rightarrow \exists x\mathcal{A}(x,y))$	GEN 4
6.	$\vdash$	$\exists y\mathcal{A}(x,y) \Rightarrow \forall y\exists x\mathcal{A}(x,y)$	(A5)

□

Úloha 10.1. *(1) Odvoďte ostávajúce teorémy z predchádzajúcej vety!*

(2) vyjadrite konjunkciu &, disjunkciu $\vee$ a ekvivalenciu $\equiv$ pomocou imlikácie $\Rightarrow$ a negácie $\neg$ a potom dokážte (alebo vyvráťte) nasledujúce formuly!

(a) $\forall x(\mathcal{A}(x) \vee \mathcal{B}(x)) \Rightarrow (\exists x\mathcal{A}(x) \vee \forall x\mathcal{B}(x))$,

(b) $\exists x(\mathcal{A}(x) \vee \mathcal{B}(x)) \Rightarrow (\exists x\mathcal{A}(x) \vee \exists x\mathcal{B}(x))$,

(c) $(\exists x\mathcal{A}(x)\&\exists x\mathcal{B}(x)) \Rightarrow \exists x(\mathcal{A}(x) \vee \mathcal{B}(x))$,

(d) $(\exists x\mathcal{A}(x)\&\exists x\mathcal{B}(x)) \Rightarrow \exists x(\mathcal{A}(x)\&\mathcal{B}(x))$.

10.3 Interpretácia, splniteľnosť a pravdivosť

V tejto kapitole sme sa už neraz snažili nájsť nejakú interpretáciu formúl, predikátových a funkcionálnych symbolov pri zdôvodňovaní toho, že nejaká formula nemôže byť teorémou predikátového počtu. Teraz skúsime tieto intuitívne predstavy postaviť na trochu pevnejší základ.

Formuly (nejakej teórie) majú zmysel len vtedy, ak existuje nejaká interpretácia symbolov, ktoré obsahujú. Pod interpretáciou budeme rozumieť ľubovoľný systém, ktorý pozostáva z neprázdnej množiny D, nazývanej oblasťou interpretácie a nejakého zobrazenia (korešpondencie) $\mathcal{I}$, ktoré

- každému n-árnemu predikátovému symbolu P_i^n priradí n-árnu reláciu na množine D (ktorá sa dá chápať aj ako zobrazenie $P_i^n : D^n \to \{0,1\}$,
- každému n-árnemu funkcionálnemu symbolu f_k^n priradí n-árnu operáciu na množine D; $f_k^n : D^n \to D$;
- každej predmetovej konštante a_i priradí nejaký konkrétny prvok z množiny D.

Predmetové premenné nadobúdajú hodnoty z množiny D, logické spojky a kvantifikátory majú obvyklý význam.

V danej interpretácii predstavuje každá uzavretá formula (formula bez voľných premenných) výrok, ktorý môže byť buď pravdivý alebo nepravdivý. Formula s voľnými premennými predstavuje nejakú reláciu na množine D (oblasti interpretácie), ktorá môže byť splnená pre jedny a nepravdivá pre iné hodnoty predmetových premenných.

Príklad 10.6. *Nech $\mathcal{A}^2(x_1, x_2)$ označuje reláciu usporiadania na množine prirodzených čísel: $\mathcal{A}^2(x_1, x_2) \stackrel{\text{def}}{\equiv} x_1 \leq x_2$. Potom*

- $\mathcal{A}^2(5,7)$ *predstavuje pravdivý výrok,*
- $\mathcal{A}^2(3,1)$ *je nepravdivý výrok,*

- $\mathcal{A}^2(x,3)$ *je relácia* $x \leq 3$*, ktorá pozostáva zo* 4 *usporiadaných dvojíc;* $\mathcal{A}^2(x,3) = \{(0,3),(1,3),(2,3),(03,3)$;
- $\forall x \exists y \mathcal{A}^2(x,y)$ *je pravdivý výrok, pretože skutočno pre každé prirodzené číslo existuje väčšie prirodzené číslo,*
- $\exists y \forall x \mathcal{A}^2(x,y)$ *je nepravdivý výrok, ktorý tvrdí, že existuje maximálne prirodzené číslo,*
- $\exists x \forall y \mathcal{A}^2(x,y)$ *je pravdivý výrok, pretože skutočne existuje minimálne (súčasne najmenšie) prirodzené číslo (*0*),*
- $\forall y \exists x \mathcal{A}^2(x,y)$ *je pravdivý výrok, pretože pretože ku každému prirodzenému číslu existuje prirodzené číslo menšie alebo rovné ako dané číslo. (Keďže platí* $\mathcal{A}^2(0,0)$*, výrok* $\forall y \exists x \mathcal{A}^2(x,y)$ *je pravdivý aj pre* $y = 0$*.)*

Intuitívne je zrejmé, že formula je tautológiou vtedy, ak je za každých okolností (t.j. nech sa interpretujú funkcionálne a predikátové symboly ktoré obsahuje akokoľvek a keď sa dosadia za predmetové premenné ľubovoľné hodnoty); a kotradikciou, ak jej negácia je tautológiou. Niektoré formuly môžu však byť za istých okolností pravdivé, za iných nie. Upresníme najprv intuitívne predstavy o pravdivosti formúl predikátového počtu a potom sa budeme zaoberať úplnosťou a bezospornosťou predikátového počtu.

Definícia 10.4. *Nech je daná oblasť interpretácie* D*, interpretácia* $\mathcal{I}$ *a množina všetkých spočítateľných postupností prvkov z oblasti interpretácie* D*, ktorú označíme symbolom* Σ*. Potom formula* $\mathcal{A}$ *je splnená na postupnosti* $s, \in \Sigma$; $s = b_1, b_2, \ldots$ *práve vtedy, keď po dosadení prvku* b_i *na miesto všetkých voľných výskytov premennej* x_i, $i = 1, 2, \ldots$ *vo formule* $\mathcal{A}$*, dostávame pravdivé tvrdenie (v danej interpretácii).*

Formula $\mathcal{A}$ *sa nazýva splniteľnou v danej interpretácii práve vtedy, ak existuje taká postupnosť* $s \in \Sigma$*, na ktorej je formula* $\mathcal{A}$ *splnená.*

Formula $\mathcal{A}$ *sa nazýva pravdivou v danej interpretácii práve vtedy, ak je splnená na každej postupnosti* $s \in \Sigma$*.*

Formula $\mathcal{A}$ *sa nazýva nepravdivou v danej interpretácii práve vtedy, ak nie je splnená na žiadnej postupnosti* $s \in \Sigma$*.*

Nech je daná množina formúl Γ*. Interpretácia* $\mathcal{I}$ *sa nazýva modelom danej množiny formúl, ak je v danej interpretácii každá formula z množinay formúl* Γ *pravdivá.*

Poznámka. V predchádzajúcej definícii sme pevne spojili pojmy interpretácie a oblasti interpretácie. Je možné uvažovať tú istú interpretáciu a rozličné oblasti interpretácie. Vzhľadom na to, aké úlohy v predikátovom počte riešime, vystačíme s našou menej všeobecnou definíciou.

Úloha 10.2. *Dokážte platnosť nasledujúcich tvrdení:*

(a) *Formula* $\mathcal{A}$ *je nepravdivá v danej interpretácii práve vtedy, ak je formula* $\neg\mathcal{A}$ *pravdivá v danej interpretácii. Opačne formula* $\mathcal{A}$ *je pravdivá v danej interpretácii práve vtedy aj je formula* $\neg\mathcal{A}$ *nepravdivá v danej interpretácii.*

(b) *Žiadna formula nemôže byť v súčasne pravdivá aj nepravdivá v tej istej interpretácii.*

(c) *Ak sú v danej interpretácii pravdivé formuly $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B}$, tak je v danej interpretácii pravdivá aj formula $\mathcal{B}$.*

(d) *Formula $\mathcal{A} \Rightarrow \mathcal{B}$ je nepravdivá v danej interpretácii práve vtedy, ak je formula $\mathcal{A}$ je pravdivá a formula $\mathcal{B}$ je nepravdivá v danej interpretácii.*

(e) *Formula $\mathcal{A}$ je pravdivá v danej interpretácii práve vtedy, ak je formula $\forall x \mathcal{A}$ pravdivá v danej interpretácii.*

(f) *Každá tautológia je pravdivá v ľubovoľnej interpretácii.*

(g) *Ak je formula $\mathcal{A}$ uzavretá, tak potom v ľubovoľnej interpretácii je pravdivá buď formula $\mathcal{A}$ alebo formula $\neg\mathcal{A}$; resp. formula $\mathcal{A} \vee \neg\mathcal{A}$ je v každej interpretácii pravdivá.*

Definícia 10.5. *Formula $\mathcal{A}$ sa nazýva* všeobecne pravdivou formulou predikátového počtu*, ak je pravdivá v každej interpretácii.*

Formula $\mathcal{A}$ sa nazýva splniteľnou formulou predikátového počtu*, ak existuje interpretácia, v ktorej je formula $\mathcal{A}$ splniteľná.*

Formula $\mathcal{A}$ sa nazýva kontradikciou predikátového počtu*, ak je formula $\neg\mathcal{A}$ všeobecne pravdivá.*

Podobne ako pre výrokový počet, má zmysel skúmať aj v predikátovom počte také otázky, ako je bezospornosť, úplnosť a nezávislosť axióm a pravidiel odvodenia. Štúdium týchto problémov v predikátovom počte je technicky pomerne náročné a presahuje úroveň základného kurzu. Preto uvedieme bez dôkazov len odpovede na uvedené otázky. Podrobnejší výklad (a samozrejme aj dôkazy) daných tvrdení čitateľ nájde napríklad v knihe [14].

Veta 10.4. *Predikátový počet 1. rádu je bezosporný.*

Veta 10.5. *(Gödelova veta o úplnosti predikátového počtu.) V predikátovom počte 1. rádu sú teorémemi práve tie formuly, ktoré sú všeobecne pravdivé.*

Veta 10.6. *Systém axióm (A1)—(A5), odvodzovacích pravidiel modus ponens a zovšeobecnenia predikátového počtu je bezosporný.*

Z praktického hľadiska[2] má veľký význam Gödelova veta. Ak je nejaká formula teorémou predikátového počtu, tak musí byť všeobecne pravdivou formulou. Dokázať o nejakej formule, že je teorémou, znamená zostrojiť jej dôkaz. Ak sa to nedarí, môžeme skúsiť ukázať, že formula nie je všeobecne pravdivá. Na to stačí nájsť interpretáciu, v ktorej daná formula nebude pravdivá.

Príklad 10.7. *(1) Uvažujme formulu $\mathcal{C} = \exists x(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\exists x \mathcal{A} \Rightarrow \exists x \mathcal{B})$. Zvolíme dvojprvkovú oblasť interpretácie $D = \{a, b\}$ a formuly $\mathcal{A}, \mathcal{B}$ interpretujeme pomocou unárnych*

[2] o teoretickom ani nehovoriac

predikátov; $\mathcal{A} = P_1^1(x), \mathcal{B} = P_2^1(x)$*, ktoré sú definované nasledovne*

x	$P_1^1(x)$	$P_2^1(x)$
a	0	0
b	1	0

Potom je formula $\exists x\mathcal{A}$ *pravdivá, lebo* $P_1^1(b) = 1$*, ale formula* $\exists x\mathcal{B}$ *je nepravdivá. To znamená, že formula* $(\exists x\mathcal{A} \Rightarrow \exists x\mathcal{B})$ *je v danej interpretácii nepravdivá. Na druhej strane formula* $\exists x(\mathcal{A} \Rightarrow \mathcal{B})$ *je v danej interpretácii pravdivá, pretože pre* $x = a$ *nadobúdajú obe formuly pravdivostnú hodnotu* 0*:* $\mathcal{A}(a) = P_1^1(a) = 0$*;* $\mathcal{B}(a) = P_2^1(a) = 0$*. To znamená, že formula* $\mathcal{C}$ *nie je pravdivá v danej interpretácii, a teda nemôže byť teorémou predikátového počtu.*

(2) Preskúmame formulu $\exists x\mathcal{A}(x) \Rightarrow \forall x\mathcal{A}$*. Zvolíme tú istú interpretáciu ako v predchádzajúcom príklade; oblasť interpretácie* $D = \{a, b\}$*, formule* $\mathcal{A}$ *priradíme predikát* $P_1^1(x)$*. Keďže* $P_1^1(b) = 1$*, formula* $\exists x\mathcal{A}(x)$ *je pravdivá. Na druhej strane z toho, že* $P_1^1(a) = 0$ *vyplýva, že formula* $\forall x\mathcal{A}$*. je v danej interpretácii nepravdivá. To znamená, že formula* $\exists x\mathcal{A}(x) \Rightarrow \forall x\mathcal{A}$ *nie je všeobecne pravdivá, a preto nemôže byť teorémou predikátového počtu.*

Poznámka. Všimnite si, že v jednoprvkovej oblasti interpretácie je formula $\exists x\mathcal{A}(x) \Rightarrow \forall x\mathcal{A}$ pravdivá.

Úloha 10.3. *Zistite, či sú nasledujúce formuly teorémami predikátového počtu:*

1. $\forall x\exists y\mathcal{A}(x, y) \equiv \exists y\forall x\mathcal{A}(x, y)$
2. $(\exists x\mathcal{A}(x) \Rightarrow \exists x\mathcal{B}(x)) \Rightarrow \exists x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x))$
3. $\forall x(\mathcal{A}(x) \Rightarrow \mathcal{B}(x)) \equiv (\forall x\mathcal{A}(x) \Rightarrow \exists\forall x\mathcal{B}(x))$.

Kapitola 11

Teórie 1. rádu

Štúdium matematickej logiky nie je samoúčelné. Matematická logika slúži (okrem iného) na vytváranie matematických teórií. Ukážeme, ako pomocou už známeho predikátového počtu 1. rádu možno vybudovať matematickú teóriu opisujúcu niektoré zaujímavé vlastnosti celých čísel. Predikátový počet bude tvoriť logický základ našej teórie (využijeme syntaktické pravidlá na vytváranie formúl, axiómy a odvodzovacie pravidlá a odvodzovanie teorém v predikátovom počte.) Problém však spôsobuje to, že samotný predikátový počet 1. rádu nič nehovorí o celých číslach, a tak z neho žiadne vlastnosti celých čísel neodvodíme. Preto musíme zaviesť minimálne niektoré konkrétne predikáty a funkcionálne symboly; možno aj konštanty na množine celých čísel a pomocou axióm popísať ich základné vlastnosti. Výber predikátov, funkcionálnych konštánt a následne axióm závisí od toho, na čo chceme vytváranú teóriu použiť. Existuje však vzťah, ktorý sa vyskytuje v mnohých teóriách a nemôže chýbať ani v našej—rovnosť (v našom prípade rovnosť celých čísel). Rovnosť, ako sme to videli v 7. kapitole, je relácia ekvivalencie. Vyjadríme reláciu rovnosti (na množine celých čísel) pomocou predikátového symbolu $P^2_=(x,y) \stackrel{\text{def}}{=} (x = y)$. Vlastnosti rovnosti popíšeme pomocou nových axióm, ktoré pridáme k axiómam (A1)—(A5) predikátového počtu. Aké axiómy by to mali byť? Na prvý pohľad sa zdá, že by bolo rozumné zachytiť v nich to, že rovnosť je ekvivalencia, t.j. že je reflexívna, symetrická a tranzitívna relácia. Tieto vlastnosti rovnosti by sa formálne dali zapísať takto:

1. $\forall x P^2_=(x,x)$,
2. $\forall x \forall y (P^2_=(x,y) \Rightarrow P^2_=(y,x)$,
3. $\forall x \forall y \forall z [(P^2_=(x,y) \& P^2_=(y,z)) \Rightarrow P^2_=(x,z)]$.

Ale rovnosť má jednu dôležitú vlastnosť, ktorú z týchto troch „axióm“ neodvodíme. Ak $x = y$, tak potom možno za istých podmienok x a y zamieňať. Preto medzi axómy rovnosti spomedzi vyššie uvedených kandidátov zaradíme prvú formulu a druhú a tretiu nahradíme novou formulou. Axiómy rovnosti budú potom vyzerať nasledovne (namiesto trocha ťažkopádneho zápisu $P^2_=(x,y)$ budeme používať štandardný zápis $x = y$):

(A6) $\forall x (x = x)$

(A7) $(x = y) \Rightarrow [\mathcal{A}(x, x) \Rightarrow \mathcal{A}(x, y)]$,

Kde x, y sú predmetové premenné, $\mathcal{A}(x, y)$ je ľubovoľná formula, ktorú dostávame z formuly $\mathcal{A}(x, x)$ nahradením niektorých (nemusia to byť všetky) voľných výskytov premennej x premennou y za predpokladu, že y je voľná vzhľadom na tie výskyty x, za ktoré ju dosadzujeme.

Úloha 11.1. *Odvoďte z axióm (A1)—(A7) nasledujúce tvrdenia*

1. $t = t$ *pre ľubovoľný term* t *definovaný na množine* $\mathbb{Z}$*,*
2. $(x = y) \Rightarrow (y = x)$,
3. $(x = y)\&(y = z) \Rightarrow (x = z)$,
4. $\forall x[\mathcal{A}(x) \equiv \exists y((x = y)\&\mathcal{A}(y))]$,
5. $\forall x[\mathcal{A}(x) \equiv \forall y((x = y) \Rightarrow \mathcal{A}(y))]$,
6. $\forall x \exists y(x = y)$.

Budeme pokračovať v budovaní teórie celých čísel. Zavedieme funkcionálny symbol $f^2_+(x, y) \stackrel{\text{def}}{=} (x + y)$.[1] Vlastnosti súčtu definujeme (napríklad) takto:

(A8) $x + (y + z) = (x + y) + z$,

(A9) $x + y = y + x$,

Význačné postavenie pri sčítaní celých čísel má prvok 0. Tento prvok budeme definovať takto:

(A10) $\exists x \forall y(x + y = x)$,

Dá sa ukázať, že prvok x definovaný formulou (A10) je jediný, a teda ho môžeme označiť zvláštnym symbolom (0). Prvok 0 predstavuje predmetovú konštantu. K danému celému číslu existuje opačné číslo. Jeho existenciu popíšeme pomocou nasledujúcej axiómy:

(A11) $\forall x \exists y(x + y = 0)$.

Ak by sme zaviedli ešte predikát $P^1_{\in\mathbb{Z}}(x) \stackrel{\text{def}}{=} (x \in \mathbb{Z})$ a pomocou neho vyjadrili uzavretosť množiny $\mathbb{Z}$ na súčet[2] :

(A12) $(x \in \mathbb{Z})\&(y \in \mathbb{Z}) \Rightarrow ((x + y) \in \mathbb{Z})$,

pomocou axióm (A1)—(A12) by sme definovali aditívnu grupu na množine $\mathbb{Z}$.

[1] Kvôli sprehľadneniu zápisu budeme však v ďalšom zapisovať súčet čísel štandardným spôsobom.

[2] aj v tomto prípade budeme na vyjadrenie množinovej príslušnosti používať štandardné označenia

Úloha 11.2. *Zoberte namiesto množiny* $\mathbb{Z}$ *množinu* $\mathbb{R}-\{0\}$. *Definujte funkcionálny symbol* $f^2_{\otimes}(x,y) \stackrel{\text{def}}{=} (x \otimes y)$ *(súčin reálnych čísel).*

1. *Čo vyjadrujú axiómy (A8)—(A12) v tomto prípade?*
2. *Aká konštanta je definovaná pomocou axiómy (A10)?*
3. *Čo popisuje systém axióm (A1)—(A12) v tomto prípade?*
4. *Platia axiómy (A8)—(A12) aj v prípade, ak je oblasťou interpretácie množina* $\mathbb{Z}$*?*

Úloha 11.3. *Zaveďte na množine* $\mathbb{R}$ *operácie sčítania a násobenia a pomocou axióm popíšte ich vlastnosti!*

Úloha 11.4. *Na mnžine celých čísel je definovaný funkcia* $f^2_{\otimes}(x,y) \stackrel{\text{def}}{=} (x \otimes y)$ *(súčin celých čísel). Napíšte formuly, ktoré budú vyjadrovať: „*x *delí* y*“, „*x *je prvočíslo“, „*x *je štvorcom nejakého celého čísla“„*x *je najväčší spoločný deliteľ čísel* y, z*“, „*x *je najmenší spoločný násobok čísel* y, z*“, „čísla* y, z *sú nesúdeliteľné“, a pod.*

Vytvoríme ešte jednu (dôležitú) teóriu prvého rádu. Teória $\mathcal{S}$ bude mať

1. binárny predikátový symbol $P^2_{=}(x,y) \stackrel{\text{def}}{=} (x = y)$ reprezentujúci reláciu rovnosti;
2. predmetovú konštantu 0;
3. tri funkcionálne symboly
   (a) unárny funkcionálny symbol reprezentujúci operáciu nasledovníka: $f^1_1(x) \stackrel{\text{def}}{=} s(x)$;
   (b) binárny funkcionálny symbol reprezentujúci operáciu sčítania: $f^2_{\oplus}(x,y) \stackrel{\text{def}}{=} (x \oplus y)$;
   (c) binárny funkcionálny symbol reprezentujúci operáciu násobenia: $f^2_{\otimes}(x,y) \stackrel{\text{def}}{=} (x \otimes y)$;

Vlastnosti relácie rovnosti, konštanty 0 a troch operácií sú v teórii $\mathcal{S}$ definované pomocou nasledujúcich deviatich axióm.

S1 $(x = y) \Rightarrow [(x = z) \Rightarrow (y = z)]$

S2 $(x = y) \Rightarrow (s(x) = s(y))$

S3 $0 \neq s(x)$

S4 $(s(x) = s(y)) \Rightarrow (x = y)$

S5 $(x \oplus 0) = x$

S6 $x \oplus s(y) = s(x \oplus y)$

S7 $x \otimes 0 = 0$

S8 $x \otimes s(y) = (x \otimes y) \oplus x$

S9 $\mathcal{A}(0) \Rightarrow [\forall x(\mathcal{A}(x) \Rightarrow \mathcal{A}(s(x))) \Rightarrow \forall x(\mathcal{A}(x)]$

kde x, y sú predmetové premenné, $\mathcal{A}(x)$ je ľubovoľná formula teórie $\mathcal{S}$. Prvých osem axióm je zrejmých, ťažkosti by na prvý pohľad mohla spôsobovať posledná axióma. Keď sa však na ňu lepšie pozrieme, zistíme že vyjadruje *princíp matematickej indukcie.*

Ak interpretujeme konštantu 0 ako prirodzené číslo 0, funkciu nasledovníka $s(x)$ ako $x + 1$, sčítanie $x \oplus y$ ako sčítanie prirodzených čísel $x + y$, násobenie $x \otimes y$ ako násobenie prirodzených čísel $x \cdot y$,a za oblasť interpretácie teórie $\mathcal{S}$ zvolíme množinu prirodzených čísel, $\mathbb{N}$[3], teória $\mathcal{S}$ popisuje aritmetiku prirodzených čísel.[4]

Úloha 11.5. *Dokážte, že teória $\mathcal{S}$ je teória prvého rádu s rovnosťou; t.j. že pomocou axióm (A1)—(A5), S1—S9, pravidla modus ponens a pravidla zovšeobecnenia možno odvodiť axiómy (A6) a (A7)!*

Úloha 11.6. *Nech sú q, r, t ľubovoľné termy teórie $\mathcal{S}$. Dokážte, že potom sú nasledujúce formuly teorémy teórie $\mathcal{S}$:*

(a) $t = t$

(b) $t = r \Rightarrow r = t$

(c) $t = r \Rightarrow (r = q \Rightarrow t = q)$

(d) $r = t \Rightarrow (q = t \Rightarrow r = q)$

(e) $t = r \Rightarrow (t \oplus q = r \oplus q)$

(f) $t = 0 \oplus t$

(g) $s(t) \oplus r = s(t \oplus r)$

(h) $t \oplus r = r \oplus t$

(i) $t = r \Rightarrow (q \oplus t = q \oplus r)$

(j) $(t \oplus r) \oplus q = t \oplus (r \oplus q)$

(k) $t = r \Rightarrow t \otimes q = r \otimes q$

(l) $0 \otimes t = 0$

(m) $s(t) \otimes r = (t \otimes r) + r$

(n) $t \otimes r = r \otimes t$

(o) $t = r \Rightarrow (q \otimes t = q \otimes r)$

[3] takáto interpretácia sa nazýva štandardnou interpretáciou teórie $\mathcal{S}$

[4] samozrejme spolu s predikátovým počtom prvého rádu, ktorý tvorí logický základ teórie $\mathcal{S}$.

(p) $t \otimes (r \oplus q) = t \otimes r \oplus t \otimes q$

(q) $(r \oplus q) \otimes t = r \otimes t \oplus q \otimes t$

(r) $(q \otimes r) \otimes t = q \otimes (r \otimes t)$

(s) $(t \oplus q = r \oplus q) \Rightarrow t = r$

Zhrnieme naše poznatky o vytváraní (matematických) teórií prvého rádu:

1. Za logický základ teórie 1. rádu zoberieme predikátový počet 1. rádu.
2. Pomocou predikátových symbolov zavedieme základné vzťahy medzi objektami, ktoré chceme popisovať; pomocou funkcionálnych symbolov zavedieme operácie nad popisovanými objektami.
3. Vlastnosti relácií a operácií, ktoré sú popísané pomocou predikátových a funkcionálnych symbolov popíšeme pomocou axióm. Pomocou axióm definujeme aj potrebné konštanty.
4. Pomocou odvodzovacích pravidiel odvodzujeme z axióm teórémy.

Všimnite si, že tie isté axiómy (A1)—(A5) sa používali aj pri vytváraní aritmetiky prirodzených čísel, aj pri vytváraní teórie grúp. Tieto axiómy nazývame logickými axiómami a sú spoločné pre všetky teórie 1. rádu, ktoré využívajú ako svoj logický základ predikátový počet 1. rádu. Axiómy (A6), (A7) sa vyskytujú v mnohých axiomatických teóriách. Preto sa im niekedy priznáva status logických axióm a predikátový počet 1. rádu s predikátom $x = y$ a axiómami(A6), (A7) nazývame *predikátovým počtom s rovnosťou*.

Axiómy (A8)—(A12), resp. S1—S9, ktoré v skutočnosti určujú obsah teórie, sa nazývajú vlastnými axiómami teórie.

Aj v teóriách 1. rádu sa skúmajú také otázky, ako je úplnosť (možnosť dokázať všetky pravdivé tvrdenia danej teórie z jej axióm), bezospornosť (v teórii neexistuje taká formula, ktorá by bola teorémou a súčasne jej negácia by bola teorémou danej teórie), nezávislosť axióm (žiadna axióma teórie nie je nadbytočná, t.j. nedá sa odvodiť z ostatných axióm). Skúmanie týchto nesporne veľmi zaujímavých otázok však presahuje rámec tejto knihy. Čitateľovi odporúčame [14].

Poznámka. Číslo 1 v názve predikátový počet 1. rádu, resp. teórie 1. rádu naznačuje existenciu logík (teórií) iných rádov. O teórii prvého rádu hovoríme vtedy, keď je jej logickým základom logika (predikátový počet) 1. rádu. Logika 1. rádu sa od logík vyšších rádov odlišuje tým, že používa len logické pojmy, kým napr. v logike 2. rádu sa používajú také pojmy, ako je množina, prirodzené číslo. Rozdiel je aj v používaní kvantifikátorovm kým v logike 1. rádu kvantifikátory pôsobia na nejakej (danej) množine M, v logike 2. rádu sa kvantifikátory vzťahujú na podmnožiny množiny M a na funkcie, v logike 3. rádu kvantifikátory pôsobia na množiny funkcií, atď.

Mnohí logici predpokladajú, že neexistuje iná logika okrem logiky 1. rádu; t.j. ak sa pokúsime vyjadriť všetky matematické (nie logické) predpoklady o objektoch teórie pomocou axióm, axiómy, ktoré dostaneme, možno vyjadriť v logike 1. rádu. To by znamenalo, že neformálny pojem dokázateľnosti (matematického tvrdenia), by sa presne zhodoval s formálnym pojmom dokázateľnosti v logike 1. rádu. Toto hľadisko sa nazýva *Hilbertovou tézou*. Nie všetci logici prijímajú Hilbertovu tézu. Ale aj tí, ktorí s ňou súhlasia, zďaleka nie sú ochotní uplatňovať ju v praxi, pretože logika 1. rádu je pomerne chudobná na výrazové prostriedky a niektoré mimologické pojmy by sa v nej vyjadrovali komplikovane. [5]

Čitateľa, ktorý by si želal oboznámiť sa hlbšie s formálnymi axiomatickými teóriami, odkazujeme na početnú literatúru (my sme čerpali z klasických zdrojov [14], [**?**],[**?**], [**?**]; z novších [], resp. internetové zdroje). Teória množín je prístupnou formou spracovaná v knihe [14] a [3], formálnu aritmetiku možno nájsť v skoro každej knihe o matematickej logike, my sme čerpali z [14].

[5] Aj pri programovaní by bolo možné používať priamo strojový kód, ale z praktického hľadiska je rozumnejšie a pohodlnejšie napísať program vo vyššom jazyku a ten nechať automaticky spracovať (kompilátorom, assemblerom) do podoby strojového kódu. Na rozdiel od programovania, v logike naviac nie je isté, či sa teória vyššieho rádu dá „skompilovať“ do podoby teórie 1. rádu.

Kapitola 12

Booleovské funkcie

V tejto kapitole sa znova budeme zaoberať výrokovou logikou, tentoraz však nebudeme odvodzovať teorémy, ale študovať (zloženým) výrokom priradené logické (Booleovské) funkcie.[1] Ukážeme, že pomocou logických (binárnych) hodnôt možno jednoznačne zapisovať (kódovať) ľubovoľnú informáciu vyjadrenú pomocou reťazcov znakov nad nejakou konečnou abecedou. Ak sa obmedzíme na informáciu zapísanú v podobe konečných reťazcov znakov nad nejakou konečnou abecedou (textovú informáciu), tak spracovanie informácie v podstate predstavuje nejakú transformáciu, ktorá jednému konečnému reťazcu znakov priradí iný (alebo ten istý) konečný reťazec znakov. Ak je takáto transformácia dobre popísaná (napríklad pomocou zobrazenia), tak sa dá popísať aj pomocou logických (Booleovských) funkcií. Booleovské funkcie sa zasa dajú realizovať pomocou fyzikálnych (možno aj biologických) systémov. To znamená, že ak sa dá riešenie nejakého problému popísať pomocou Booleovských funkcií, tak potom (aspoň principiálne[2]) sa dá zostrojiť fyzikálny systém (logický obvod) na riešenie tohto problému. Ako neskôr zistíte pri štúdiu informatiky, Booleovské funkcie nemožno preceňovať; podstata riešenia problému spočíva v nájdení vhodnej transformácie a nie vo vyjadrení tejto transformácie pomocou Booleovských funkcií. Napriek tomuto obmedzeniu sú Booleovské funkcie jedným zo základných objektov, ktoré sa v informatike študujú, a to tak kvôli ich širokému uplatneniu v teoretických disciplínach (výpočtová zložitosť, teória riadiacich systémov, teória testov a iné), ale aj—ako sme už naznačili vyššie—ich úlohe pri návrhu súčasných počítačov a iných digitálnych systémov.

12.1 Základné pojmy

Nech $\mathbb{E} = \{0, 1\}$. *Booleovskou (logickou) premennou* budeme nazývať ľubovoľnú premenú, ktorá nadobúda hodnoty z množiny $\mathbb{E}$ (a žiadne iné). Booleovské premenné budeme označovať symbolmi x, y, z a indexovať. Hodnoty $0, 1$ sa nazývajú *binárne, logické* alebo *Booleovské hodnoty*, alebo aj *logické konštanty*. n*-árnou Booleovskou funkciou* budeme

[1] Táto oblasť diskrétnej matematiky sa nazýva výroková algebra, alebo algebra logiky; zrejme preto, že Booleovské funkcie skúma ako algebraické objekty.

[2] neskôr ukážeme, že takéto riešenia môžu byť tak zložité, že nie sú prakticky realizovateľné

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Tabuľka 12.1: Booleovské funkcie dvoch premenných

nazývať ľubovoľné zobrazenie $f : E^n \to E$. n-árna Booleovská funkcia teda priraďuje n-ticiam binárnych hodnôt opäť binárne hodnoty. n-tice vstupných hodnôt Booleovskej funkcie chápeme ako hodnoty n-tice Booleovských premenných. To, že Booleovská funkcia f závisí od premenných $x_1, \ldots, x_n$, zapisujeme symbolicky nasledovne $f(x_1, \ldots, x_n)$. Keďže množina vstupných hodnôt n-árnej Booleovskej funkcie (binárnych vektorov dĺžky n) je konečná a konečná je aj množina hodnôt Booleovskej funkcie, n-árnych Booleovských funkcií je konečne veľa. Označme množinu všetkých n-árnych Booleovských funkcií symbolom $\mathcal{P}_2^n$. Binárnych vektorov dĺžky n je 2^n a n-árnych Booleovských funkcií je toľko, koľko je binárnych vektorov dĺžky 2^n, čiže 2^{2^n}. Pre $n = 2$ teda $|\mathcal{P}_2^2| = 16$ a všetky Booleovské funkcie dvoch premenných sú uvedené v tabuľke 12.1.

Zavedieme niektoré konvencie, ktoré nám zjednodušia zápis Booleovských funkcií. Nech je i prirodzené číslo, $0 \leq i < 2^n$, potom symbolom $\sigma(n, i)$ budeme označovať n-bitový binárny zápis čísla i. Aby sme mohli určiť hodnoty jednotlivých bitov čísla $\sigma(n, i)$, označíme symbolom $\sigma(n, i, j)$, $1 \leq j \leq n$ j-ty bit čísla $\sigma(n, i)$. Tak napríklad $\sigma(4, 12) = 1100, \sigma(4, 7) = 0111, \sigma(3, 7) = 111$; resp. $\sigma(4, 12, 1) = \sigma(4, 12, 2) = 1, \sigma(4, 12, 3) = \sigma(4, 12, 4) = 0$. Je zrejmé, že ak je daný binárny vektor $(x_1, \ldots, x_n)$, tak tomuto vektoru zodpovedá binárne číslo $\sum_{k=1}^{n} x_k * 2^{n-k}$. Na druhej strane binárnemu číslu i môžeme priradiť n-ticu (binárny vektor) $(\sigma(n, i, 1), \sigma(n, i, 2), \ldots, \sigma(n, i, n))$. Túto vzájomne jednoznačnú korešpondenciu medzi binárnymi vektormi dĺžky n a binárnymi číslami budeme využívať tak, že v prípadoch, kde to nepovedie k nedorozumeniu, nebudeme rozlišovať medzi binárnym zápisom n-bitového čísla a jemu zodpovedajúcim n-bitovým vektorom. Potom napríklad $f(\sigma(2, 3))$ bude predstavovať zápis $f(1, 1)$.

Všimnite si tabuľku 12.1, ktorá predstavuje štandardnú tabuľku pravdivostných hodnôt Booleovských funkcií. Riadky tabuľky sú usporiadané vzostupne podľa číselných hodnôt vektorov hodnôt jednotlivých premenných. Ak sa dohodneme na konvencii, že n-árnu Booleovskú funkciu budeme zadávať pomocou štandardnej tabuľky pravdivostných hodnôt 12.2, tak potom je zbytočné zapisovať premenné a ich hodnoty a n-árnu Booleovskú f funkciu možno jednoznačne zadať vektorom hodnôt $(f(\sigma(n, 0)), \ldots, \ldots, f(\sigma(n, 2^n - 1)))$. (Takýto zápis je úsporný a vhodný pre teoretické výpočty a najmä na reprezentáciu Booleovských funkcií v počítači, ale pri väčších hodnotách n je trocha ne-

$\tilde{x}$	$f(\tilde{x})$
$\sigma(n, 0)$	$f(\sigma(n, 0))$
$\vdots$	$\vdots$
$\sigma(n, 2^n - 1)$	$f(\sigma(n, 2^n - 1))$

Tabuľka 12.2: Pravdivostná tabuľka n-árnej Booleovskej funkcie

prehľadný, a preto budeme na zápis Booleovskej funkcie pri „ručnom“ spracovaní väčšinou používať štandardnú pravdivostnú tabuľku.) Aj vektor hodnôt Booleovskej funkcie predstavuje prirodzené číslo; túto skutočnosť sme využili aj v tabuľke 12.1, kde vektor hodnôt Booleovskej funkcie f_i je $\sigma(4, i)$, čo nám zjednoduší odvolávanie sa na jednotlivé funkcie.

Prikročíme teraz ku skúmaniu Booleovských funkcií dvoch premenných. Ak sa pozrieme na tabuľku 12.1, zistíme, že obsahuje Booleovské funkcie, ktoré „nereagujú“ na zmeny svojich vstupných premenných. Krajným prípadom sú funkcie f_0, f_{15}; prvá nadobúda pre všetky vstupné hodnoty 0, druhá 1. Tieto funkcie nezávisia od hodnôt svojich premenných a predstavujú *konštantné funkcie*, alebo stručne—*konštanty* 0 a 1. Iným príkladom je funkcia f_3, ktorá na výstupe kopíruje hodnoty vstupnej premennej x_1. To znamená, že medzi Booleovskými funkciami dvoch premenných existujú aj funkcie, ktoré by sa dali zapísať ako Booleovské funkcie jednej, resp. žiadnej premennej.

Definícia 12.1. *Nech je daná n-árna Booleovská funkcia $f(x_1, \ldots, x_n)$. Potom budeme hovoriť, že Booleovská funkcia $f(x_1, \ldots, x_n)$* podstatne závisí od premennej x_i, $i \in \{1, \ldots, n\}$, *ak existuje taký vektor hodnôt $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ premenných $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, že*

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Ak Booleovská funkcia f podstatane závisí od premennej x_i, tak premennú x_i nazývame podstatnou premennou *Booleovskej funkcie f. V opačnom prípade premennú x_i nazývame fiktívnou premennou Booleovskej funkcie f.*

Príklad 12.1. *Funkcia $f_{12}(x_1, x_2)$ má podstatnú premennú x_1, lebo $f_{12}(0, 0) = 1$ a $f_{12}(1, 0) = 0$, ale premenná x_2 je fiktívna, lebo $f_{12}(0, x_2) = 1$ a $f_{12}(1, x_2) = 0$.*

Úloha 12.1. *Zistite, ktoré z Booleovských funkcií $f_0, \ldots, f_{15}$ podstatne závisia od dvoch, jednej a žiadnej premennej!*

Príklad 12.2. *Čo sa stane, ak n-árnu Booleovskú funkciu, ktorá podstatne závisí od všetkých svojich premenných. rozšírime o jednu fiktívnu premennú? Ilustrujeme to na príklade, ktorý potom zovšeobecníme. Uvažujme napríklad Booleovskú funkciu $f = f_7$ s premennými x, y a pridajme k nim tretiu premennú, z. Pridanie fiktívnej premennej spôsobilo, že sa každý riadok pôvodnej pravdivostnej tabuľky nahradil dvoma riadkami, v ktorých sú hodnoty premenných x, y rovnaké a tretia premenná z v prvom riadku*

x	y	z	$g(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Tabuľka 12.3: Pridanie fiktívnej premennej

nadobúda hodnotu 0 *a v druhom hodnotu* 1*, ale hodnota funkcie* f *závisí len od hodnôt premenných* x, y*, tabuľka 12.3.*

Úloha 12.2. *Koľko je ternárnych Booleovských funkcií? Koľko z nich podstatne závisí od všetkých troch premenných?*

Zistili sme, že pridávaním, či vyškrtávaním fiktívnych premenných sa síce zväčšuje (zmenšuje) veľkosť tabuľky pravdivostných hodnôt funkcie, ale samotná funkcia sa nemení: pre ten istý súbor hodnôt svojich podstatných premenných dáva vždy tú istú hodnotu bez ohľadu na to, aké hodnoty nadobúdajú jej fiktívne premenné. To nám umožňuje zjednodušiť skúmanie Booleovských funkcií; namiesto toho, aby sme uvažovali Booleovské funkcie s rozličným počtom premenných, môžeme ich doplniť fiktívnymi premennými a skúmať ich všetky napríklad ako n-árne Booleovské funkcie.

Skôr ako prikročíme ku skúmaniu vlastností Booleovských funkcií, ukážeme ako možno pomocou Booleovských funkcií zapísať funkciu definovanú na konečných, ale nie binárnych množinách.

Príklad 12.3. *Nech je* $A = \{a, b, c, d, e, f\}, B = \{✠, ♠, †, ♢\}$ *a zobrazenie* $F : A \to B$ *je definované pomocou nasledujúcej tabuľky:*

x	a	b	c	d	e	f
$F(x)$	✠	♠	†	♢	†	✠

Každému prvku množiny A *priradíme binárny vektor dĺžky* 3 *a prvky množiny* B *zakódujeme pomocou binárnych vektorov dĺžky* 2*:*

x	a	b	c	d	e	f
	000	001	010	011	100	101

y	✠	♠	†	♢
	00	01	10	11

Zobrazenie $F : A \to B$ *vyjadríme pomocou dvoch ternárnych Booleovských funkcií* g_1, g_2*: Všimnite si posledné dva riadky tabuľky 12.4. Definičný obor zobrazenia* F *je 6 prvkový. Na rozlíšenie 6 hodnôt potrebujeme binárne vektory dĺžky 3. Ale binárnych vektorov dĺžky 3 je 8. Prvých 6 riadkov tabuľky 12.4 popisuje pomocou dvoch ternárnych*

x	x_1	x_2	x_3	g_1	g_2	$F(x)$
a	0	0	0	0	0	✠
b	0	0	1	0	1	♠
c	0	1	0	1	0	†
d	0	1	1	1	1	♢
e	1	0	0	1	0	†
f	1	0	1	0	0	✠
–	1	1	0	–	–	–
–	1	1	1	–	–	–

Tabuľka 12.4: Zobrazenie F vyjadrené pomocou Booleovských funkcií g_1, g_2

a_1	a_0	b_1	b_0	c_2	c_1	c_0	$a+b=c$		
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	1	0	1	1
0	0	1	0	0	1	0	0	2	2
0	0	1	1	0	1	1	0	3	3
0	1	0	0	0	0	1	1	0	1
0	1	0	1	0	1	0	1	1	2
0	1	1	0	0	1	1	1	2	3
0	1	1	1	1	0	0	1	3	4
1	0	0	0	0	1	0	2	0	2
1	0	0	1	0	1	1	2	1	3
1	0	1	0	1	0	0	2	2	4
1	0	1	1	1	0	1	2	3	5
1	1	0	0	0	1	1	3	0	3
1	1	0	1	1	0	0	3	1	4
1	1	1	0	1	0	1	3	2	5
1	1	1	1	1	1	0	3	3	6

Tabuľka 12.5: Súčet binárne kódovaných čísel

funkcií g_1, g_2 *zobrazenie* F*, posledné dva riadky zodpovedajú tým vektorom hodnôt premenných* x_1, x_2, x_3*, na ktorých nie sú funkcie* g_1, g_2 *definované. Ako sa takýto problém rieši, budeme skúmať pri konštrukcii disjuntívnych normálnych foriem pre neúplne zadané Booleovské funkcie.*

V úvode tejto kapitoly sme sa zaoberali reprezentáciou celých čísel pomocou binárnych vektorov. V nasledujúcom príklade popíšeme sčítanie prirodzených čísel pomocou Booleovských funkcií 4 premenných.

Príklad 12.4. *Nech* $0 \leq a, b \leq 3$ *sú dve prirodzené čísla; a nech* $a+b=c$ *Zapíšeme všetky tri čísla binárne;* $a = (a_1a_2)_2; b = (b_1b_2)_2$ *a* $c = (c_2c_1c_0)_2$*. Súčet binárne kódovaných čísel* a, b *je popísaný v tabuľke 12.5*

12.2 Skladanie Booleovských funkcií

Ako sme videli v predchádzajúcom príklade, pomocou Booleovských funkcií je možné popísať sčítanie celých čísel. Podobne by sme mohli realizovať násobenie celých čísel, celočíselné delenie (DIV) a modulárne delenie (MOD). Vhodným kódovaním (napríklad vyhradením jedného bitu na kódovanie znamienka) by sme mohli zaviesť záporné čísla a rozšíriť aritmetiku z prirodzených čísel na obor celých čísel. Ak by sme sa dohodli, že (napríklad) v $2n$-bitovom vektore bude prvých n bitov reprezentovať celočíselnú časť a ostávajúcich n bitov—zlomkovú časť čísla, môžeme kódovať racionálne čísla[3] a pomocou Booleovských funkcií popísať aritmetické operácie nad racionálnymi číslami. Principiálne s tým nie sú žiadne problémy. Tie vznikajú, keď by sa teoretické riešenie malo

[3] v programovacích jazykoch sa označujú ako reálne čísla, t.j. typ REAL

funkcia	# premenných	názov	formula	označenie
$f_0(x,y)$	0	konštanta 0	0	0
$f_1(x,y)$	2	konjunkcia	$x\&y$	AND
$f_3(x,y)$	1	identita/projekcia	x	n.a.
$f_6(x,y)$	2	súčet modulo 2	$x \oplus y$	XOR
$f_7(x,y)$	2	disjunkcia	$x \vee y$	OR
$f_8(x,y)$	2	Pierceova funkcia	$\neg(x \vee y)$	NOR
$f_9(x,y)$	2	ekvivalencia	$x \equiv y$	n.a.
$f_{12}(x,y)$	1	negácia	$\neg x$	NOT
$f_{13}(x,y)$	2	implikácia	$x \Rightarrow y$	n.a.
$f_{14}(x,y)$	2	Shefferova funkcia	$\neg(x\&y)$	NAND
$f_{14}(x,y)$	0	konštanta 1	1	1

Tabuľka 12.6: Elementárne Booleovské funkcie

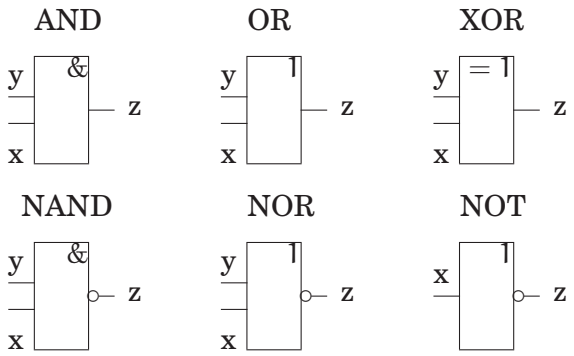
prakticky implementovať. Pomocou 16 bitov môžeme zapísať celé čísla bez znamienka z intervalu $0,\ldots,65535$, čo na praktické účely asi nebude stačiť. Ak by sme chceli popísať sčítanie dvoch 16 bitových čísel spôsobom uvedeným v príklade 12.5, potrebovali by sme na to 17 Booleovských funkcií o 32 premenných a tabuľku, ktorá by mala $2^{32} = 4.294.967.296$ riadkov. To asi nie je schodné riešenie. Naviac, ak by sa mal pre každú Booleovskú funkciu navrhovať systém (logický obvod), ktorý by ju realizoval, bolo by potrebné navrhnúť a vyrobiť veľký počet rozličných špecifických obvodov. To je neekonomické a prakticky nerealizovateľné. V praxi[4] sa preto používa iný prístup: hľadá sa nejaká rozumná množina základných Booleovských funkcií, pomocou ktorých je možné vyjadriť všetky ostatné Booleovské funkcie. Pre tieto základné Booleovské funkcie sa zostroja *logické obvody*, ktoré ich realizujú. Pre Booleovskú funkciu, ktorú potrebujeme realizovať, sa najprv nájde vyjadrenie pomocou elementárnych Booleovských funkcií a na základe tohto vyjadrenia sa z logických obvodov realizujúcich príslušné základné Booleovské funkcie poskladá logický obvod realizujúci danú Booleovskú funkciu. V ďalších častiach tejto kapitoly budeme hľadať odpovede na dve základné otázky

1. ako vybrať množinu základných Booleovských funkcií, aby pomocou nich bolo možné vyjadriť všetky ostatné Booleovské funkcie;
2. keď už je daná množina základných Booleovských funkcií, ako nájsť čo najefektívnejšie vyjadrenie Booleovskej funkcie pomocou základných Booleovských funkcií?

Niektoré spomedzi 16 Booleovských funkcií dvoch premenných[5] sa v matematike a informatike bežne používajú a považujú sa za *elementárne (Booleovské funkcie)*. Ide o Booleovské funkcie $f_0, f_1, f_3, f_6, f_7, f_{12}, f_{13}, f_{15}$ z tabuľky 12.1. Pre jednotlivé elementárne Booleovské funkcie sa zaužívali menej formálne označenia, ktoré budeme aj my v ďalšom výklade používať. Booleovské funkcie f_0, f_{15} budeme nazývať logickými konštantami a označovať symbolmi 0, resp. 1; funkciu f_1 budeme nazývať konjunkciou, atď; kvôli

[4] ani teória sa neuspokojila konštatovaním, že nejaká úloha je principiálne riešiteľná, ale skúmala zložitosť úloh a hľadala metódy ich optimálneho riešenia.

[5] v skutočnosti medzi nimi sú aj konštanty a funkcie jednej premennej



Obrázok 12.1: Hradlá realizujúce elementárne Booleovské funkcie

stručnosti a prehľadnosti uvádzame elementárne Booleovské funkcie, ich názvy a symbolické označenia príslušných operátorov v tabuľke 12.6. V tabuľke 12.6 nie sú funkcie f_5, f_{10}, predstavujúce identitu $f_5(x, y) = y$ a negáciu $f_{10}(x, y) = \neg y$, pretože tieto sú už zastúpené funkciami f_3, f_{12}. Na druhej strane, kvôli úplnosti sme medzi elementárne funkcie zaradili aj funkcie f_8, f_{14}, ktorými sa budeme zaoberať až v poslednej časti tejto kapitoly. Operátory pre Shefferovu $|$ a Pierceovu funkciu $\downarrow$ sa bežne nepoužívajú, a preto sme obe funkcie vyjadrili pomocou konjunkcie, disjunkcie a negácie. Pre väčšinu elementárnych Booleovských funkcií existujú logické obvody (hradlá, logické členy), ktoré ich realizujú. To znamená, že ak napríklad na vstupy logického obvodu AND (ktorý má dva vstupy a jeden výstup) privedieme signály zodpovedajúce logickým hodnotám p, q, na výstupe AND sa objaví signál zodpovedajúci logickej hodnote $p\&q$. Schématické označenie jednotlivých hradiel je uvedené na obrázku 12.1.

Zložitejšie Booleovské funkcie môžeme dostať skladaním základných Booleovských funkcií.

Definícia 12.2. *Nech sú* $f(x_1, x_2, \ldots, x_n), g_1(y_1, \ldots, y_m), g_2(y_1, \ldots, y_m), \ldots, g_n(y_1, \ldots, y_m)$ *Booleovské funkcie. Booleovskú funkciu*

$$F(y_1, \ldots, y_m) = f(g_1(y_1, \ldots, y_m), g_2(y_1, \ldots, y_m), \ldots, g_n(y_1, \ldots, y_m)) \qquad (12.1)$$

nazveme zloženou funkciou funkcií $f, g_1, g_2, \ldots, g_n$. *Booleovská funkcia* $f(x_1, x_2, \ldots, x_n)$ *sa nazýva vonkajšou a Booleovské funkcie* $g_1(y_1, \ldots, y_m), g_2(y_1, \ldots, y_m), \ldots, g_n(y_1, \ldots, y_m)$ *vnútornými funkciami zloženej Booleovskej funkcie* F.

Poznámka. Keďže Booleovská funkcia je zobrazenie $\{0,1\}^n \to \{0,1\}$ skladaním Booleovských funkcií dostaneme opäť Booleovskú funkciu. Vnútorné funkcie zloženej Booleovskej funkcie by mohli mať rozličné počty rôznych premenných. Zjednotením množín vstupných premenných jednotlivých Booleovských funkcií sme dostali množinu $\{y_1, \ldots, y_m\}$ a potom sme jednotlivé Booleovské funkcie g_i doplnili fiktívnymi premennými na m-árne Booleovské funkcie. Preto sme pri definícii skladania Booleovských funkcií mohli

x_1	x_2	f_6	f_{11}	f_{14}	F
0	0	0	1	1	0
0	1	1	0	1	1
1	0	1	1	1	0
1	1	0	1	0	1

Tabuľka 12.7: Zložená Booleovská funkcia

predpokladať, že všetky vnútorné Booleovské funkcie majú rovnaký počet rovnakých premenných (aj keď v niektorých prípadoch fiktívnych).

Zloženú Boleovskú funkciu 12.1 môžeme opäť zadať pomocou tabuľky pravdivostných hodnôt, ktorú vyplníme nasledovne: aby sme vypočítali hodnotu zloženej Booleovskej funkcie $F(y_1, \ldots, y_m)$ na vektore vstupných hodnôt $\sigma_1, \ldots, \sigma_m$ potrebujeme najprv vypočítať hodnoty $g_1(\sigma_1, \ldots, \sigma_m), \ldots, g_n(\sigma_1, \ldots, \sigma_m)$, dosadiť ich za premenné $x_1, \ldots, x_n$ funkcie f a potom (napríklad pomocou tabuľky pravdivostných hodnôt Booleovskej funkcie f) vypočítame hodnotu zloženej Booleovskej funkcie.

Príklad 12.5. *Nech* $F(x_1, x_2) = f_6(f_{11}(x_1, x_2), f_{14}(x_1, x_2))$. *Pravdivostné tabuľky čiastkových funkcií* f_6, f_{11}, f_{14} *a zloženej funkcie* F *sú uvedené v tabuľke 12.7*

Všimnite si, že zložená funkcia $F(x_1, x_2) = f_5(x_1, x_2)$*; t.j. skladaním Booleovských funkcií, ktoré záviseli od oboch premenných sme dostali Booleovskú funkciu s jednou fiktívnou premennou.*

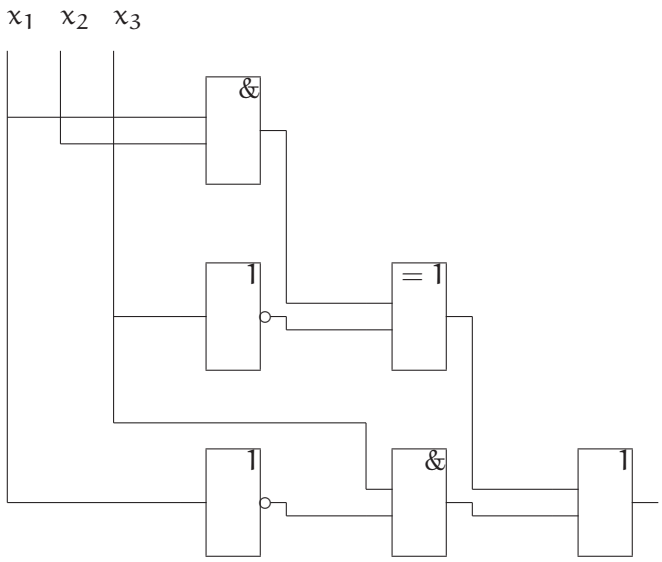
Úloha 12.3. *Zopakujte si základné vlastnosti elementárnych Booleovských funkcií z 2. kapitoly (asociatívnosť, komutatívnosť, idempotentnosť a i.) a preskúmajte, ktoré z nich sa zachovávajú pri skladaní Booleovských funkcií!*

V zápise Booleovskej funkcie pomocou pravdivostnej tabuľky sa stráca informácia o čiastkových Booleovských funkciách, pomocou ktorých je daná Booleovská funkcia vyjadrená. Táto informácia môže však byť užitočná pri skúmaní vlastností Booleovskej funkcie ako aj pri konštruovaní logického obvodu, ktorý ju realizuje. Preto sa popri zápise Booleovských funkcií pomocou pravdivostných tabuliek používa aj ich vyjadrenie v podobe formúl nad nejakou množinou základných Booleovských funkcií. Zavedieme najprv pojem *formuly (algebry logiky)*[6] a potom sa pozrieme na vzťah medzi Booleovskými funkciami a formulami.

Definícia 12.3. *Nech je daná množina Booleovskch funkcií* $\mathcal{D} \subseteq \mathcal{P}_2$.

1. *Každý výraz tvaru* $f(x_1, \ldots, x_n)$*, kde* $f \in \mathcal{D}$ *sa nazýva formulou nad* $\mathcal{D}$
2. *Nech je* $f(x_1, \ldots, x_n)$ *Booleovská funkcia z* $\mathcal{D}$ *a* $\mathbf{A_1}, \ldots, \mathbf{A_1}$ *sú formuly nad* $\mathcal{D}$*, potom aj výraz* $f(\mathbf{A_1}, \ldots, \mathbf{A_1})$ *je formulou nad* $\mathcal{D}$
3. *Formulou nad* $\mathcal{D}$ *je ľubovoľný konečný výraz, spĺňajúci podmienky (1) alebo (2). Iné formuly nad* $\mathcal{D}$ *nie sú.*

[6] V tejto kapitole sa budeme takmer výlučne zaoberať foremulami algebry logiky. Ak to však nepovedie k nedorozumeniu, budem slová „algebry logiky“ kvôli stručnosti vynechávať



Obrázok 12.2: Logický obvod počítajúci Booleovskú funkciu F

Formuly algebry logiky budeme označovať písmenami $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$. Ak budeme potrebovať vyjadriť, z akých funkcií formula skladaním vznikla, uvedieme ich zoznam v hranatých zátvorkách za názvom formuly; ak potrebujeme vedieť, aké premenné obsahuje, uvedieme ich zoznam v okrúhlych zátvorkách za názvom formuly. Napríklad, ak zloženej funkcii F (12.1) priradíme formulu $\mathbf{A}$, tak potom formulu $\mathbf{A}$ môžeme zapísať ako $\mathbf{A}[f, g_1, \ldots, d_n]$ alebo $\mathbf{A}(y_1, \ldots, y_m)$. Ak ako množinu $\mathcal{D}_1$ zoberieme podmnožinu elementárnych Booleovských funkcií, napríklad

$$\mathcal{D}_1 = \{x\&y, x \vee y, x \oplus y, \neg x\},$$

tak potom formuly nad $\mathcal{D}_1$ zodpovedajú zloženým výrokom, v ktorých premenné x_i zohrávajú úlohu logických premenných alebo elementárnych výrokov. Pravdivostnú hodnotu zložených výrokov vieme bez problémov určiť. Naviac, ak sa nám podarí vyjadriť nejakú funkciu pomocou formuly nad danou množinou $\mathcal{D}_1$, tak potom vieme navrhnúť logický obvod, ktorý bude počítať hodnoty danej Booleovskej funkcie.

Príklad 12.6. *Uvažujme Booleovskú funkciu* $F(x_1, x_2, x_3)$ *zadanú nasledujúcou formulou:*

$$F(x_1, x_2, x_3) = ((x_1\&x_2) \oplus \neg x_3) \vee (x_3\&\neg x_1).$$

Hodnoty tejto Booleovskej funkcie bude počítať logický obvod uvedený na obrázku 12.2.

Teraz upresníme intuitívne chápanie súvislosti medzi Booleovskými funkciami a formulami algebry logiky. Upravíme najprv definíciu hĺbky formuly, ktorú sme zaviedli pre formuly výrokového počtu:

1. Nech $\mathbf{A}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, kde $f(x_1, \ldots, x_n) \in \mathcal{D}$. Potom $\mathbf{hl}(\mathbf{A}) = 0$.

2. Nech $\mathbf{A}(x_1, \ldots, x_n) = f(\mathbf{A}_1, \ldots \mathbf{A}_m)$, kde $f \in \mathcal{D}$. Potom $\mathbf{hl}(\mathbf{A}) = \max_i \mathbf{hl}(\mathbf{A})_i + 1$.

Teraz matematickou indukciou vzhľadom na hĺbku formuly ukážeme, že každej formule algebry logiky možno jednoznačne priradiť Booleovskú funkciu. Nech $\mathbf{A}(x_1, \ldots, x_n)$ je formula nad $\mathcal{D}$.

1. Ak $\mathbf{hl}(\mathbf{A}) = 0$, potom existuje funkcia $f(x_1, \ldots, x_n) \in \mathcal{D}$ taká, že $\mathbf{A}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Funkcia $f(x_1, \ldots, x_n)$ je Booleovská funkcia priradená formule $\mathbf{A}$.

2. Predpokladajme, že každej formule $\mathbf{A}(x_1, \ldots, x_n)$ nad $\mathcal{D}$, ktorá má hĺbku menšiu ako N dokážeme jednoznačne priradiť Booleovskú funkciu.

3. Nech $\mathbf{hl}(\mathbf{A}) = N$, potom $\mathbf{A}(x_1, \ldots, x_n) = f(\mathbf{A}_1, \ldots, \mathbf{A}_m)$, kde $f(x_1, \ldots, x_m) \in \mathcal{D}$ a $\mathbf{A}_1, \ldots, \mathbf{A}_m$ sú formuly nad $\mathcal{D}$. Keďže hĺbka formúl $\mathbf{A}_1, \ldots, \mathbf{A}_m$ je menšia ako N, každej z týchto formúl dokážeme jednoznačne priradiť Booleovskú funkciu. Označme tieto funkcie (v poradí) $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)$. Potom zložená Booleovská funkcia $f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$, ktorá je zadaná jednoznač ne funkciami $f, g_1, \ldots, g_m$ je Booleovskou funkciou priradenou formule $\mathbf{A}(x_1, \ldots, x_n)$.

Nech $\mathbf{A}(x_1, \ldots, x_n)$ je formula algebra logiky a $f(x_1, \ldots, x_n)$—Booleovská funkcia priradená formule $\mathbf{A}(x_1, \ldots, x_n)$. Potom pre ľubovoľný súbor hodnôt $\sigma_1, \ldots, \sigma_n$ premenných $x_1, \ldots, x_n$ platí $\mathbf{A}(\sigma_1, \ldots, \sigma_n) = f(\sigma_1, \ldots, \sigma_n)$. Preto hovoríme, že formula $\mathbf{A}$ realizuje Booleovskú funkciu $f(x_1, \ldots, x_n)$. Ukážeme teraz na príklade, ako sa formule priraďuje Booleovská funkcia.

Príklad 12.7. *Uvažujme formulu* $\mathbf{A}(x_1, x_2, x_3) = f_7(f_2(x_1, x_3), f_9(x_1, f_{10}(x_2, x_3)))$ *nad množinou všetkých binárnych Booleovských funkcií z tabuľky 12.1. Nájdeme Booleovskú funkciu* $f(x_1, x_2, x_3)$ *priradenú formule* $\mathbf{A}$ *a zapíšeme ju pomocou tabuľky pravdivostných hodnôt. Budeme postupovať nasledovne*

- *najprv vytvoríme tabuľku pravdivostných hodnôt Booleovských funkcií* $f_2(x_1, x_3)$ *a* $f_{10}(x_2, x_3)$. *Obe funkcie doplníme na funkcie troch premenných fiktívnymi premennými (v prvom prípade premennou* x_2*, v druhom —* x_1*) a rozšírené (ternárne) funkcie označíme symbolmi* $y_1(x_1, x_2, x_3) = f_2(x_1, x_3)$*, resp.* $y_2(x_1, x_2, x_3) = f_{10}(x_2, x_3)$.

- *Pre jednotlivé súbory hodnôt* $\sigma_1, \sigma_2, \sigma_3$ *premenných* x_1, x_2, x_3 *vypočítame hodnoty* $y_2(\sigma_1, \sigma_2, \sigma_3)$ *a zostrojíme tabuľku pravdivostných hodnôt funkcie* $f_9(x_1, f_{10}(x_2, x_3))$*, ktorú kvôli stručnosti označíme symbolom* $y_3(x_1, x_2, x_3) = f_9(x_1, y_2)$.

- *Nakoniec v tabuľke pravdivostných hodnôt nájdeme hodnoty* $y_1(\sigma_1, \sigma_2, \sigma_3)$ *a* $y_3(\sigma_1, \sigma_2, \sigma_3)$*, dosadíme ich do funkcie* $f_7 : f_7(y_1, y_3)$ *a na základe hodnôt, ktoré pre hodnoty* $\sigma_1, \sigma_2, \sigma_3$ *funkcia* f_7 *nadobúda, zostrojíme pravdivostnú tabuľku funkcie* $f(x_1, x_2, x_3)$.

Každej formule nad množinou $\mathcal{D}$ možno teda jednoznačne priradiť Booleovskú funkciu. Ak by sme dokázali realizovať jednotlivé funkcie z množiny $\mathcal{D}$ logickými obvodmi, potom by sme dokázali vytvoriť aj logický obvod, ktorý by realizoval (počítal hodnoty) danej Booleovskej fukncie. Z tohoto hľadiska je zaujímavá nasledujúca otázka—možno pre danú Booleovskú funkciu nájsť formulu nad množinou $\mathcal{D}$, ktorá ju realizuje? Odpoveď na túto otázku budeme hľadať v nasledujúcich častiach tejto kapitoly.

x_1	x_2	x_3	y_1	x_1	y_2	y_3	f_7
0	0	0	0	0	1	0	0
0	0	1	0	0	1	0	0
0	1	0	0	0	0	1	1
0	1	1	0	0	0	1	1
1	0	0	1	1	1	1	1
1	0	1	0	0	0	0	0
1	1	0	0	1	0	0	0
1	1	1	0	1	0	0	0

Tabuľka 12.8: Tabuľka pravdivostných hodnôt funkcie priradenej formule $\mathbf{A}(x_1, x_2, x_3)$

12.3 Rozklad Booleovských funkcií podľa premenných. Normálne formy

Uvažujme množinu Boleovských funkcií $\mathcal{D}_2 = \{x\&y, x\vee y, \neg x\}$. Ukážeme, že pre ľubovoľnú Booleovskú funkciu možno zostrojiť formulu nad $\mathcal{D}_2$, ktorá danú Booleovskú funkciu realizuje. Podobne ako pre formuly výrokového počtu zavedieme aj pre logické premenné nasledujúce označenie:

$$x^\sigma = x\&\sigma \vee (\neg\sigma)\&(\neg x), \text{kde } \sigma \in \{0,1\}.$$

Platí

$$x^\sigma = \begin{cases} \neg x & \text{ak } \sigma = 0, \\ x & \text{ak } \sigma = 1, \end{cases}$$

čo sa dá vyjadriť aj nasledovne:

$$x^\sigma = \begin{cases} x & \text{ak } x = \sigma, \\ \neg x & \text{ak } x \neq \sigma. \end{cases}$$

Veta 12.1. *(O disjunktívnom rozklade Booleovskej funkcie podľa premenných) Nech je* $f(x_1, \ldots, x_n)$ *ľubovoľná Booleovská funkcia a nech* $0 < m \leq n$. *Potom platí*

$$\begin{aligned} &f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = \\ &\quad = \bigvee_{\sigma_1,\ldots,\sigma_m} x_1^{\sigma_1}\& \ldots \&x_m^{\sigma_m}\&f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n) \end{aligned} \tag{12.2}$$

pričom disjunkcia sa berie cez všetky možné vektory hodnôt premenných $x_1, \ldots, x_m$.

Dôkaz. Nech je $(a_1, \ldots, a_n)$ ľubovoľný vektor hodnôt premenných $x_1, \ldots, x_n$. Dosadením do 12.2 dostávame:

$$\begin{aligned} &f(a_1, \ldots, a_n) = \\ &\quad = \bigvee_{\sigma_1,\ldots,\sigma_m} a_1^{\sigma_1}\& \ldots \&a_m^{\sigma_m}\&f(\sigma_1, \ldots, \sigma_m, a_{m+1}, \ldots, a_n). \end{aligned} \tag{12.3}$$

Ak pre nejaké i, $1 \leq i \leq m$ $a_i \neq \sigma_i$, tak $a_i^{\sigma_i} = 0$ a každá konjunkcia vo formule 12.3, ktorá obsahuje člen $a_i^{\sigma_i}$ nadobúda hodnotu 0. Pre disjunkciu platí $x \vee 0 \equiv 1$. Ak je funkcia $f(x_1, \ldots, x_n)$ identicky rovná 0, tak vďaka členu $f(\sigma_1, \ldots, \sigma_m, a_{m+1}, \ldots, a_n)$ je každý člen disjunkcie 12.3 nulový a tvrdenie vety je v tomto prípade pravdivé.

Nech $f(x_1, \ldots, x_n)$ nie je konštanta 0. Z disjunkcie vypadnú všetky konjunkcie obsahujúce členy $a_i^{\sigma_i}$ také, že $a_i \neq \sigma_i$ a zostane v nej len člen

$$a_1^{\sigma_1} \& \ldots \& a_m^{\sigma_m} \& f(\sigma_1, \ldots, \sigma_m, a_{m+1}, \ldots, a_n), \text{ kde } a_i = \sigma_i,\ i = 1, \ldots, m.$$

Potom však $a_1^{\sigma_1} \& \ldots \& a_m^{\sigma_m} \equiv 1$ a

$$f(a_1, \ldots, a_n) = 1 \& f(a_1, \ldots, a_n) = f(a_1, \ldots, a_n).$$

□

Poznámka. Hoci sme rozklad Booleovskej funkcie robili vzhľadom na premenné $x_1, \ldots, x_m$, rovnako dobre sme mohli Booleovskú funkciu rozložiť aj podľa premenných $x_{i_1}, \ldots, x_{i_m}$.

Príklad 12.8. *Rozložíme funkciu* $x_1 \Rightarrow x_2$ *vzhľadom na obe premenné:*

$$\begin{aligned} x_1 \Rightarrow x_2 &= [x_1^0 \& (0 \Rightarrow x_2)] \vee [x_1^1 \& (1 \Rightarrow x_2)] = \\ &= [\neg x_1 \& (0 \Rightarrow x_2)] \vee [x_1 \& (1 \Rightarrow x_2)]. \end{aligned} \tag{12.4}$$

Ale aj funkcie $(0 \Rightarrow x_2)$ *a* $(1 \Rightarrow x_2)$ *z formuly 12.4 možno rozložiť vzhľadom na premennú* x_2*:*

$$\begin{aligned} 0 \Rightarrow x_2 &= [x_2^0 \& (0 \Rightarrow 0)] \vee [x_2^1 \& (0 \Rightarrow 1)] = \\ &= [\neg x_2 \& (0 \Rightarrow 0)] \vee [x_2 \& (0 \Rightarrow 1)]. \end{aligned} \tag{12.5}$$

Podobne

$$\begin{aligned} 1 \Rightarrow x_2 &= [x_2^0 \& (1 \Rightarrow 0)] \vee [x_2^1 \& (1 \Rightarrow 1)] = \\ &= [\neg x_2 \& (1 \Rightarrow 0)] \vee [x_2 \& (1 \Rightarrow 1)]. \end{aligned} \tag{12.6}$$

Dosadíme teraz formuly 12.6 a 12.5 do formuly 12.4 a upravíme:

$$\begin{aligned} (\cancel{x_1} \Rightarrow x_2) &= [\neg x_1 \& [(\neg x_2 \& (0 \Rightarrow 0)) \vee (x_2 \& (0 \Rightarrow 1))]] \vee [x_1 \& [(\neg x_2 \& (1 \Rightarrow 0)) \vee (x_2 \& (1 \Rightarrow 1))] \\ &= [\neg x_1 \& \neg x_2 \& (0 \Rightarrow 0)] \vee [\neg x_1 \& x_2 \& (0 \Rightarrow 1)] \vee [x_1 \& \neg x_2 \& (1 \Rightarrow 0)] \vee [x_1 \& x_2 \& (1 \Rightarrow 1)]. \end{aligned}$$

Keďže $(0 \Rightarrow 0) \equiv (1 \Rightarrow 1) \equiv (0 \Rightarrow 1) \equiv 1$, $(1 \Rightarrow 0) \equiv 0$, $(p \& 0) \equiv 0, (p \& 1) \equiv p$ *a napokon* $(p \vee 0) \equiv p$, *pre funkciu* $(x_1 \Rightarrow x_2)$ *po posledných úpravách dostávame nasledujúcu formulu:*

$$(x_1 \Rightarrow x_2) = (\neg x_1 \& \neg x_2) \vee (x_1 \& \neg x_2) \vee (x_1 \& x_2).$$

Poznámka. Zápis negácie a konjunkcie v predchádzajúcich formulách je trochu neprehľadný. Vo výrokovej algebre sa používa jednoduchšie označenie. Operátor konjunkcie sa zvykne tam kde to nespôsobí nedorozumenie vynechávať a konjunkcia $x\&y$ sa zapisuje ako xy. Negácia premennej (ale vo všeobecnosti aj formuly) sa označuje vodorovnou čiarou nad premennou (formulou), na ktorú sa negácia vzťahuje: tak napríklad $\neg x_1$ sa zapisuje ako $\overline{x_1}$. Formula, ktorú dostaneme rozkladom implikácie z predchádzajúceho príkladu podľa oboch premenných, bude mať tvar:

$$(x_1 \Rightarrow x_2) = \overline{x_1}\,\overline{x_2} \vee \overline{x_1}x_2 \vee x_1x_2.$$

Dôsledky vety 12.1 Uvažujme dva krajné prípady vzhľadom na počet premenných, podľa ktorých sa robí rozklad:

$m = 1$ (Rozklad funkcie podľa jednej premennej)

$$\begin{aligned} &f(x_1,\ldots,x_i,\ldots,x_n) = \\ &\quad = \overline{x_i}\&f(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n) \vee x_i\&f(x_1,\ldots,x_{i-1},1,x_{i+1},\ldots,x_n). \end{aligned} \tag{12.7}$$

$m = n$ (Rozklad funkcie podľa všetkých premenných)

$$f(x_1,\ldots,x_n) = \bigvee_{\sigma_1,\ldots,\sigma_n} x_1^{\sigma_1}\ldots x_n^{\sigma_n}\&f(\sigma_1,\ldots,\sigma_n). \tag{12.8}$$

Ak do Booleovskej funkcie $f(x_1,\ldots,x_n)$ dosadíme za všetky premenné nejaké hodnoty, napríklad $\sigma_1,\ldots,\sigma_n$, dostávame nulárnu funkciu, čiže konštantu: $f(\sigma_1,\ldots,\sigma_n)$. Ak však $f(\sigma_1,\ldots,\sigma_n) \equiv 0$, potom aj

$$x_1^{\sigma_1}\ldots x_n^{\sigma_n}\&f(\sigma_1,\ldots,\sigma_n) \equiv 0$$

a preto z formuly 12.8 môžeme vynechať všetky konjunkcie, pre ktoré $f(\sigma_1,\ldots,\sigma_n) \equiv 0$. V disjunkcii zostávajú tie členy (konjunkcie),

$$x_1^{\sigma_1}\ldots x_n^{\sigma_n}\&f(\sigma_1,\ldots,\sigma_n) \text{ pre ktoré } f(\sigma_1,\ldots,\sigma_n) = 1.$$

Ale $p\&1 \equiv p$, a preto môžeme výraz $f(\sigma_1,\ldots,\sigma_n)$ v konjunkcii

$$x_1^{\sigma_1}\ldots x_n^{\sigma_n}\&f(\sigma_1,\ldots,\sigma_n)$$

vynechať. Po týchto úpravách dostávame pre Booleovskú funkciu $f(x_1,\ldots,x_n)$ formulu

$$f(x_1,\ldots,x_n) = \bigvee_{\substack{(\sigma_1,\ldots,\sigma_n)\\ f(\sigma_1,\ldots,\sigma_n)=1}} x_1^{\sigma_1}\ldots x_n^{\sigma_n}, \tag{12.9}$$

ktorá sa nazýva *úplnou disjunktívnou normálnou formou (ÚDNF) Booleovskej funkcie* $f(x_1,\ldots,x_n)$.

x_1	x_2	x_3	f	elementárna konjunkcia
0	0	0	1	$\overline{x}_1\overline{x}_2\overline{x}_3$
0	0	1	0	
0	1	0	1	$\overline{x}_1x_2\overline{x}_3$
0	1	1	1	$\overline{x}_1x_2x_3$
1	0	0	0	
1	0	1	1	$x_1\overline{x}_2x_3$
1	1	0	0	
1	1	1	0	

Tabuľka 12.9: Konštrukcia ÚDNF pre Booleovskú funkciu $f(x_1, x_2, x_3)$

Skôr ako ukážeme, ako sa pre Booleovskú funkciu zostrojuje ÚDNF, zavedieme niekoľko užitočných pojmov, ktoré budeme pri popise a skúmaní disjunktívnych normálnych foriem používať. Výraz $x_i^{\sigma_i}$ ktorý predstavoval premennú x_i alebo jej negáciu $\overline{x}_i$ budeme nazývať *literálom*. Nech sú $x_1, \ldots, x_n$ premenné (nejakej Booleovskej funkcie) a nech

$$x_{i_1}^{\sigma_{i_1}}, \ldots, x_{i_r}^{\sigma_{i_r}}, \text{ kde } 0 \leq r \leq n,$$

sú ľubovoľné literály premenných $x_1, \ldots, x_n$. Potom budeme výraz

$$K = x_{i_1}^{\sigma_{i_1}} \& \ldots \& x_{i_r}^{\sigma_{i_r}}$$

nazývať *elementárnou konjunkciou*[7]. Tam, kde to nepovedie k nedorozumeniu, budeme operátory konjunkcie (&) vynechávať. Hodnotu r nazveme *rangom konjunkcie* K, ak $r = 0$, hovoríme, že konjunkcia K je prázdna a jej hodnota je 1. Nech sú $K_1, \ldots, K_m$ navzájom rôzne konjunkcie. Výraz $\mathbf{D} = K_{i_1} \vee \cdots \vee K_{i_m}$ sa nazýva *disjunktívnou normálnou formou (DNF)*. Hodnota m sa nazýva *dĺžkou disjunktívnej normálnej formy* $\mathbf{D}$. Ak $m = 0$, DNF $\mathbf{D}$ je prázdna a jej hodnota je rovná 0. Úplná disjunktívna normálna forma sa vyznačuje tým, že všetky jej konjunkcie sú elementárne a obsahujú literály všetkých n premenných. V nasledujúcom príklade ukážeme, ako sa konštruuje ÚDNF Booleovskej funkcie.

Príklad 12.9. *Nech je daná Booleovská funkcia* $f(x_1, x_2, x_3) = 10110100$. *Zapíšeme Booleovskú funkciu* f *pomocou tabuľky pravdivostných hodnôt. Jednotkovým (nulovým) riadkom pravdivostnej tabuľky nazveme riadky zodpovedajúce tým vektorom hodnôt premenných, na ktorých Booleovská funkcia* f *nadobúda pravdivostnú hodnotu* 1 *(resp.* 0*). Jednotkovému riadku zodpovedajúcemu vektoru* $\sigma_1, \sigma_2, \sigma_3$ *priradíme elementárnu konjunkciu* $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}$. *Tieto elementárne konjunkcie pospájame disjunkciami a formula, ktorú takto vytvoríme, je úplnou disjunktívnou normálnou formou Booleovskej funkcie* $f(x_1, x_2, x_3)$

$$f(x_1, x_2, x_3) = \overline{x}_1\overline{x}_2\overline{x}_3 \vee \overline{x}_1x_2\overline{x}_3 \vee \overline{x}_1x_2x_3 \vee \overline{x}_2x_3.$$

Všimnite si, že elementárna konjunkcia $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}$ *nadobúda pravdivostnú hodnotu* 1 *len na jedinom vektore;* $\sigma_1, \sigma_2, \sigma_3$. *Úplná disjunktívna normálna forma Booleovskej funkcie*

[7] Elementárnosť konjunkcie spočíva v tom, že jej operandami sú literály. Ak by operandom konjunkcie bola iná zložená formula, výraz by predstavoval konjunkciu, ktorá by však nebola elementárnou konjunkciou, napríklad: $x_1\&(x_2 \Rightarrow x_3$.)

x_1	x_2	x_3	$\overline{x}_1\overline{x}_2\overline{x}_3$	$\overline{x}_1x_2\overline{x}_3$	$\overline{x}_1x_2x_3$	$x_1\overline{x}_2x_3$	$f(x_1,x_2,x_3)$
0	0	0	1	0	0	0	1
0	0	1	0	0	0	0	0
0	1	0	0	1	0	0	1
0	1	1	0	0	1	0	1
1	0	0	0	0	0	0	0
1	0	1	0	0	0	1	1
1	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0

Tabuľka 12.10: ÚDNF Booleovskej funkcie $f(x_1,x_2,x_3)$

x_1	x_2	x_3	$\overline{x}_1\overline{x}_3$	$\overline{x}_1x_2$	$x_1\overline{x}_2x_3$	$f(x_1,x_2,x_3)$
0	0	0	1	0	0	1
0	0	1	0	0	0	0
0	1	0	1	1	0	1
0	1	1	0	1	0	1
1	0	0	0	0	0	0
1	0	1	0	0	1	1
1	1	0	0	0	0	0
1	1	1	0	0	0	0

Tabuľka 12.11: Realizácia Booleovskej funkcie $f(x_1,x_2,x_3)$ pomocou DNF $\mathbf{D}^*$

v podstate predstavuje zoznam vektorov hodnôt, na ktorých daná Booleovská funkcia nadobúda hodnotu 1. *Pre Booleovskú funkciu* $f(x_1,x_2,x_3)$ *to názorne ukazuje tabuľka 12.10.*

Je úplná disjunktívna normálna forma jedinou formulou, ktorá realizuje Booleovskú funkciu $f(x_1,x_2,x_3)$ z predchádzajúceho príkladu? Ukážeme, že nie. Keďže

$$\overline{x}_1\overline{x}_2\overline{x}_3 \vee \overline{x}_1x_2\overline{x}_3 = \overline{x}_1\overline{x}_3(x_2 \vee \overline{x}_2) = \overline{x}_1\overline{x}_3$$

a

$$\overline{x}_1x_2\overline{x}_3 \vee \overline{x}_1x_2x_3 = \overline{x}_1x_2,$$

Ako je dobre vidieť z tabuľky 12.11 Booleovskú funkciu $f(x_1,x_2,x_3)$ možno realizovať aj pomocou disjunktívnej normálnej formy

$$\mathbf{D}^* = \overline{x}_1\overline{x}_3 \vee \overline{x}_1x_2 \vee x_1\overline{x}_2x_3.$$

Úloha 12.4. *Zostrojte logický obvod realizujúci Booleovskú funkciu* $f(x_1,x_2,x_3)$*!*

Úloha 12.5. *Zostrojte ÚDNF aspoň pre 5 rozličných Booleovských funkcií troch premenných!*

Keďže pre väčšinu Booleovských funkcií existuje viacero disjunktívnych normálnych foriem, ktoré ich realizujú, na realizáciu danej Booleovskej funkcie sa zvyčajne vyberá

optimálna DNF. Existuje viacero kritérií, pomocou ktorých možno posudzovať DNF. Uvedieme dve najčastejšie používané: DNF realizujúca danú Booleovskú funkciu f sa nazýva

1. *minimálnou*, ak zo všetkých DNF realizujúcich danú Booleovskú funkciu obsahuje minimálny počet literálov;
2. *najkratšou*, ak zo všetkých DNF realizujúcich danú Booleovskú funkciu má minimálnu dĺžku (obsahuje minimálny počet konjunkcií).

Zjednodušene povedané, výber minimálnej DNF minimalizuje počet spojení medzi hradlami a výber najkratšej DNF zasa minimalizuje počet hradiel v logickom obvode realizujúcoum danú Booleovskú funkciu f.[8] Základmi optimalizácie DNF sa budeme zaoberať v nasledujúcej časti tejto kapitoly.

Úloha 12.6. *Zostrojte minimálne a najkratšie DNF pre funkcie*

1. $x_1 \Rightarrow x_2$,
2. $f(x_1, x_2, x_3) = (01011011)$,
3. $f(x_1, x_2, x_3) = (11011001)$.

Čo spravíme v prípade, keď máme realizovať konštantu 0? Pre tú síce neexistuje ÚDNF (ak za ÚDNF nepovažujeme prázdnu DNF), ale konštantu 0 môžeme vyjadriť napríklad pomocou formuly $x\&\overline{x}$, Týmto sme uzavreli dôkaz nasledujúcej vety:

Veta 12.2. *Ľubovoľnú Booleovskú funkciu možno realizovať pomocou formuly nad množinou Booleovských funkcií* $\{x_1\&x_2, x_1 \vee x_2, \neg x\}$.

Okrem disjunktívnej normálnej formuly existujú aj iné spôsoby vyjadrenia Booleovských funkcií v podobe formúl nad množinou $\{x_1\&x_2, x_1 \vee x_2, \neg x\}$. Jednou z nich je tzv. *konjuktívna normálna forma.*

Veta 12.3. *(O konjuktívnom rozklade Booleovskej funkcie) Nech je* $f(x_1, \ldots, x_n)$ *ľubovoľná Booleovská funkcia a nech* $1 \leq m \leq n$. *Potom platí*

$$f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = \\ = \bigwedge_{\sigma_1, \ldots, \sigma_m} x_1^{\overline{\sigma}_1} \vee \cdots \vee x_m^{\overline{\sigma}_m} \vee f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n) \tag{12.10}$$

kde symbol $\wedge$ *označuje konjunkciu a konjunkcia sa berie cez všetky možné vektory hodnôt premenných* $x_1, \ldots, x_n$.

Dôkaz. Veta sa dokazuje analogický ako veta 12.1. □

[8] zjednodušenie spočíva v predpoklade, že sa v logickom obvode použijú hradlá, ktoré majú dostatočný počet vstupov na realizáciu elementárnej konjunkcie, resp. disjunkcie všetkých konjunkcií danej DNF. Ak sa použijú hradlá AND a OR s dvoma vstupmi a jedným výstupom, vzťah medzi dĺžkou DNF a počtom hradiel bude zložitejší.

Dôsledok. Pre ľubovoľnú Booleovskú funkciu $f(x_1,\ldots,x_n) \neq 1$ platí

$$f(x_1,\ldots,x_n) = \bigwedge_{\substack{\sigma_1,\ldots,\sigma_n \\ f(\sigma_1,\ldots,\sigma_n)=0}} x_1^{\overline{\sigma}_1} \vee \cdots \vee x_n^{\overline{\sigma}_n}. \tag{12.11}$$

Formula 12.11 sa nazýva *úplná konjuktívna forma* (ÚKNF) Booleovskej funkcie $f(x_1,\ldots,x_n)$. ÚKNF pre danú Booleovskú funkciu zostrojíme tak, že každému nulovému riadku pravdivostnej tabuľky (t.j. riadku, prislúchajúcemu vektoru $(\sigma_1,\ldots,\sigma_n)$, pre ktorý $f(\sigma_1,\ldots,\sigma_n)=0$) priradíme tzv. elementárnu disjunkciu $x_1^{\overline{\sigma}_1} \vee \cdots \vee x_n^{\overline{\sigma}_n}$ a potom tieto elementárne disjunkcie pospájame konjunkciami. ÚKNF pre Booleovskú funkciu z príkladu 12.16 má tvar

$$(x_1 \vee x_2 \vee \overline{x}_3)\&(\overline{x}_1 \vee x_2 \vee x_3)\&(\overline{x}_1 \vee \overline{x}_2 \vee x_3)\&(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3).$$

Úloha 12.7. *Vyberte si aspoň 5 Booleovských funkcií troch premenných a zostrojte pre ne ÚKNF!*

Úloha 12.8. *Zostrojte konjunktívny rozklad funkcie $x_1 \Rightarrow x_2$ podľa oboch premenných!*

Ako je výhodnejšie zadávať Booleovské funkcie—formulami, alebo pravdivostnými tabuľkami? Formuly nad $\{x_1\&x_2, x_1 \vee x_2, \neg x\}$ nebudú rozhodne zložitejšie ako pravdivostné tabuľky, pretože ÚDNF a ÚKNF zložitosťou približne zodpovedajú pravdivostným tabuľkám. Existujú však Booleovské funkcie, ktoré sa zapisujú pomocou formúl podstatne jednoduchšie v porovnaní so zápisom pomocou pravdivostných tabuliek. Napríklad funkcia $f(x_1,\ldots,x_{100}) = x_1\&\ldots\&x_{100}$. Formula pre realizujúca túto funkciu má 100 literálov a 99 znakov konjunkcie, zatiaľ čo pravdivostná tabuľka (ktorá mimochodom obsahuje jediný jednotkový riadok) má $2^{100} = 1267650600228229401496703205376$ riadkov.

12.4 Minimalizácia disjunktívnych normálnych foriem

V predchádzajúcej časti tejto kapitoly sme ukázali dve podstatné skutočnosti: každú[9] Booleovskú funkciu možno realizovať pomocou disjunktívnej normálnej formy a pre danú Booleovskú funkciu spravidla existuje viacero DNF, ktoré ju realizujú. Keďže priemerná n-árna Booleovská funkcia má približne polovicu jednotkových vektorov, jej ÚDNF bude mať dĺžku $\approx 2^{n-1}$ a bude obsahovať $\approx n2^{n-1}$ literálov. V praktických aplikáciách sa pracuje s binárnymi veličinami o veľkosti niekoľko desiatok bitov (čísla, znaky, inštrukcie). Popísať spracovanie (napríklad) dvoch 32-bitových čísel pomocou Booleovských funkcií a tie realizovať pomocou ÚDNF je príliš zložité a neefektívne. V praxi sa na návrh logických obvodov používa iná metóda: zložitý problém sa rozloží na jednoduchšie, tie sa popíšu pomocou Booleovských funkcií, navrhnú sa pre ne efektívne obvody a riešenie globálneho problému sa „poskladá“ z čiastkových riešení. Rozsah čiastkových problémov je taký malý, že je možná optimalizácia ich riešení. Napríklad

[9] Pripomíname, že konštantu 0 možno realizovať pomocou prázdnej DNF a konštantu 1 pomocou ÚDNF $x_1 \vee \overline{x}_1$.

a_i	b_i	r_{i-1}	r_i	c_i
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Tabuľka 12.12: Jednobitová sčítačka

sčítanie dvoch n-bitových čísel sa dá realizovať pomocou n jednobitových sčítačiek, z ktorých každá vypočítava súčet troch jednobitových čísel (dvoch jednobitových sčítancov a prenosu z nižšieho rádu). Výsledný $2n$-bitový sumátor bude mať zložitosť (vyjadrenú počtom literálov) $10n$ (pozri príklad 12.10). Ak by sme sčítanie realizovali pomocou logických obvodov vychádzajúcich z DNF $2n$-árnych Booleovských funkcií, potrebovali by sme $n+1$ takýchto Booleovských funkcií a zložitosť takto zostrojeného logického obvodu by bola $\approx n^2 \cdot 2^n$.

Príklad 12.10. *Sumátor so sériovým prenosom. Vstupom sú dve binárne hodnoty* a_i, b_1 *a prenos z predchádzajúceho nižšieho rádu* r_{i-1}. *Výstupom sumátora je súčet* $c_i = a_i \oplus b_1 = a_i\overline{b}_i \vee \overline{a}_i b_i$ *a prenos do vyššieho rádu:* $r_i = a_i b_i \vee a_i r_{i-1} \vee b_i r_{i-1}$. *Počet literálov vo formulách pre výstupnú hodnoty* c_i, r_i *je zhora ohraničený*[10] *číslom* 10.

Ako však nájdeme optimálnu DNF pre danú Booleovskú funkciu? Uvažujme n-árnu Booleovskú funkciu $f(x_1, \ldots, x_n)$. Existuje 3^n rozličných elementárnych konjunkcií premenných $x_1, \ldots, x_n$; pretože pre ľubovoľné $1 \leq i \leq n$ elementárna konjunkcia

- premennú x_i neobsahuje, alebo
- obsahuje premennú x_i, alebo
- obsahuje negáciu premennej x_i; $\overline{x}_i$.

Každá disjunktívna normálna forma je jednoznačne určená výberom konjunkcií—je zrejmé, že každá z 3^n rozličných elementárnych konjunkcií buď patrí alebo nepatrí do DNF. Celkovo je teda možných 2^{3^n} DNF premenných $x_1, \ldots, x_n$. Teoreticky by sme teda mohli postupovať nasledovne: usporiadali by sme všetky DNF (napríklad najprv podľa počtu literálov a potom lexikograficky) a potom by sme postupne preverovali, či DNF realizuje zadanú Booleovskú funkciu alebo nie. Prvá DNF, ktorú by sme takýmto spôsobom našli, by bola minimálna DNF danej Booleovskej funkcie. Žiaľ, principiálne jednoduchá metóda je použiteľná nanajvýš pre funkcie troch premenných, pretože množina konjunkcií, ktoré môžu patriť do DNF je príliš veľká. Prakticky sa tento problém rieši tak, že sa najprv podstatne zúži množina kandidátov na konjunkcie v DNF a potom sa na zúženú

[10] riešenie, ktoré sme zostrojili, potrebovalo 10 literálov. Nie je vylúčené, že existuje lepšie riešenie, ktoré vystačí s menším počtom literálov. Ale naša konštrukcia zaručuje, že 10 literálov bude určite stačiť.

množinu aplikujú sofistikované metódy preberania. Optimalizácia (minimalizácia) DNF je mimoriadne zaujímavá tak z praktického (konštrukcia logických obvodov) ako aj teoretického hľadiska. Mnohé optimalizačné problémy možno previesť na minimalizáciu DNF a tak nájdenie efektívnej metódy na minimalizáciu DNF by pomohlo vyriešiť aj celý rad ťažkých, užitočných a zaujímavých optimalizačných úloh. Preto sa minimalizácia DNF intenzívne študuje od polovice minulého storočia a návrhom rozličných schém realizujúcich Booleovské funkcie a skúmaniu ich zložitosti sa zaoberá samostatná disciplína. My sa teoretických poznatkov o zložitosti Booleovských funkcií dotkneme len okrajovo a sústredíme sa na prezentáciu dvoch metód konštrukcie optimálnych a suboptimálnych DNF Booleovských funkcií; metódu Quine-McCluskey a metódu založenú na Karnaughových mapách.

12.4.1 Geometrické princípy minimalizácie DNF

Minimalizcia DNF má veľmi názornú geometrickú interpretáciu—zodpovedá konštrukcii pokrytia grafu Booleovskej funkcie špeciálnymi podgrafmi. Zavedieme najprv niektoré potrebné pojmy a potom sa budeme zaoberať minimalizáciou DNF.

Definícia 12.4. *Nech* $\mathbf{u} = (a_1, \ldots, a_n), \mathbf{v} = (b_1, \ldots, b_n)$ *sú binárne vektory dĺžky* n.

(a) *Počet jednotkových zložiek vektora* $\mathbf{u}$ *budeme nazývať Hammingovou váhou vektora a označovať symbolom* $\mathbf{wt}(\mathbf{u})$.

(b) *Počet zložiek, v ktorých sa vektory* $\mathbf{u}, \mathbf{v}$ *odlišujú, budeme nazývať Hammingovou vzdialenosťou vektorov* $\mathbf{u}, \mathbf{v}$ *a označovať symbolom* $\mathbf{d}(\mathbf{u}, \mathbf{v})$.

Poznámka. Je zrejmé, že $= \mathbf{wt}(\mathbf{u} \oplus \mathbf{v})$.

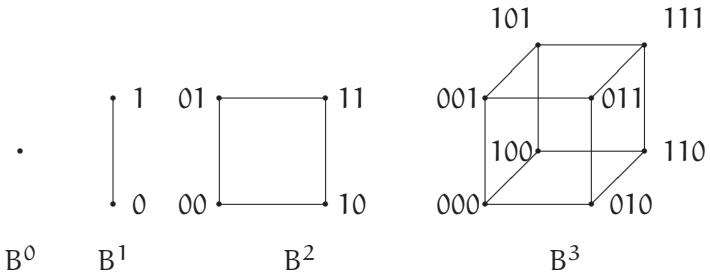
Definícia 12.5. *(Graf Booleovskej funkcie).*

(a) n*-rozmernou Booleovskou kockou nazveme graf* $B^n = (V, U)$*, kde* $V = \{\sigma(n, 0), \ldots, \ldots, \sigma(n, 2^n - 1)\}$ *a* $U = \{(v_i, v_j); \mathbf{d}(\sigma(\mathbf{n}, \mathbf{i}), \sigma(\mathbf{n}, \mathbf{j}) = \mathbf{1})\}$.

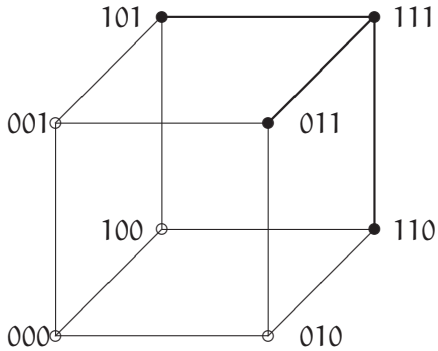
(b) *Nech* $f(x_1, \ldots, x_n)$ *je* n*-árna Booleovská funkcia,* $N_f = \{(a_1, \ldots, a_n); f(a_1, \ldots, a_n) = 1\}$ *je množina jednotkových vektorov funkcie* f. *Vrcholom* $\sigma(n, i)$ *Booleovskej kocky* B^n *priradíme hodnoty* $f(\sigma(n, i))$*; vrcholy zodpovedajúce vektorom z množiny* N_f *nazveme jednotkovými vrcholmi. Grafom Booleovskej funkcie* f *nazveme podgraf indukovaný množinou jej jednotkových vrcholov.*[11]

Príklad 12.11. *Na obrázku 12.16 sú uvedené* $0, 1, 2, 3$ *rozmerné Booleovské kocky. Uvažujme napríklad funkciu* r_i *z tabuľky 12.23. Graf tejto funkcie je znázornený na obrázku 12.4 hrubými čiarami.*

[11] Nech je daný graf $G = (V, U)$ a $V_1 \subseteq V$ je nejaká podmnožina nbožiny vrcholov grafu G. Podgrafom grafu G indukovaným množinou vrcholov V_1 je graf $G_1 = (V_1, U_1)$, kde $U_1 = (V_1 \times V_1) \cap U$ t.j. hranami podgrafu G_1 sú práve tie hrany grafu G, ktoré sú incidentné s vrcholmi z množiny V_1. Graf Booleovskej funkcie je potom $B^n(f) = (V(f), U(f))$; $V(f) = \{\sigma(n, i) \in V; \sigma(n, i) \in N_f$, $U(f) = U \cap V(f) \times V(f)$.



Obrázok 12.3: Booleovské kocky



Obrázok 12.4: Graf Booleovskej funkcie r_i

Pozrieme sa, ako sa operácie s funkciami prejavia na ich grafoch. Nech sú f, g dve n-árne Booleovské funkcie premenných $x_1, \ldots, x_n$; $B^n(f) = (V_f, U_f)$ a $B^n(g) = (V_g, U_g)$ sú grafy týchto funkcií. Potom

(a) grafom funkcie $\neg f$ je podgraf B^n indukovaný množinou vrcholov $\{0,1\}^n - V_f$;

(b) grafom funkcie $f\&g$ je podgraf B^n indukovaný množinou vrcholov $V_f \cap V_g$;

(c) grafom funkcie $f \vee g$ je podgraf B^n indukovaný množinou vrcholov $V_f \cup V_g$.

Ako sme ukázali v predchádzajúcom príklade, graf Booleovskej funkcie predstavuje iný spôsob reprezentácie Booleovskej funkcie. Určiť hodnotu Booleovskej funkcie f na vektore $\sigma_1, \ldots, \sigma_n$ znamená, zistiť, či jej graf $B^n(f)$ obsahuje vrchol $\sigma_1, \ldots, \sigma_n$. Efektívnosť takéhoto výpočtu závisí od toho, ako efektívne sa podarí charakterizovať graf $B^n(f)$. Jeden z možných spôsobov je zostaviť zoznam všetkých jednotkových vrcholov grafu $B^n(f)$. Takýto prístup však (vzhľadom na počet jednotkových vektorov priemernej Booleovskej funkcie) už pre relatívne malé hodnoty n vedie k značne rozsiahlym zoznamom. Preto sa hľadajú vzťahy medzi jednotkovými vrcholmi grafu $B^n(f)$, ktoré by umožnili zaradiť ich do takých skupín (podmnožín) spĺňajúcich nasledujúce prirodzené požiadavky

- každý jednotkový vrchol grafu $B^n(f)$ patrí do aspoň jednej skupiny vrcholov,
- každá skupina vrcholov sa dá jednoducho charakterizovať a príslušnosť vrcholu do skupiny sa dá efektívne určiť.

Implicitne sa predpokladá, že žiadna skupina neobsahuje nejaký nulový vrchol, pretože to by znamenalo zmenu pôvodnej Booleovskej funkcie.

Takéto riešenie zodpovedá konštrukcii zvláštneho pokrytia grafu $B^n(f)$.

Definícia 12.6. *(Vrcholové pokrytie) Nech je daný graf* $G = (V, U)$ *a nech sú* $G_i = (V_i, U_i), i = 1 \ldots, k$ *podgrafy grafu* G. *Potom hovoríme, že*

(a) *graf* $G_i = (V_i, U_i)$ *pokrýva množinu vrcholov* V_i *grafu* G,

(b) *grafy* G_i *tvoria (vrcholové) pokrytie grafu* G, *ak* $\bigcup_i V_i = V$.

Pokrytie na prvý pohľad pripomína rozklad množiny vrcholov na triedy ekvivalencie. Od rozkladu sa však odlišuje tým, že jednotlivé skupiny vrcholov nemusia byť disjunktné.

Teraz je dôležité nájsť podgrafy, pomocou ktorých by bolo možné pokryť graf $B^n(f)$. Pozrieme sa najprv na to, aký je vzťah medzi formulou (DNF) a grafom Booleovskej funkcie, resp. čo zodpovedá elementárnym konjunkciám z DNF Booleovskej funkcie v jej grafe $B^n(f)$. Kvôli názornosti budeme pracovať s trojrozmernou Booleovskou kockou z obrázka 12.16 a budeme vytvárať DNF a grafy rozličných Booleovských funkcií. Začneme konštantou 0. Konštanta 0 nemá žiadne jednotkové vektory a teda jej graf neobsahuje žiadne vrcholy a je prázdny. Ľubovoľnej elementárnej konjunkcii $x_1^{\sigma_2} x_2^{\sigma_2} x_3^{\sigma_3}$

zodpovedá jediný jednotkový vektor $\sigma_1, \sigma_2, \sigma_3$ a jemu prislúchajúci jednotkový vrchol v Booleovskej kocke B^3. Zaujímavá situácia nastane vtedy, keď sa v kocke vyskytujú susedné (t.j. spojené hranou) jednotkové vrcholy. Napríklad, dvojici susedných (jednotkových) vrcholov $111, 110$ v kocke B^3 odpovedajú elementárne konjunkcie $x_1x_2x_3$ a $x_1x_2\overline{x}_3$ a ÚDNF danej funkcie by mala tvar $x_1x_2x_3 \vee x_1x_2\overline{x}_3$. Použijeme distributívny zákon a upravíme ÚDNF nasledovne:

$$x_1x_2x_3 \vee x_1x_2\overline{x}_3 = x_1x_2(x_3 \vee \overline{x}_3) = x_1x_21 = x_1x_2.$$

Z hľadiska pokrytia to znamená, že dvojicu (jednotkových) vrcholov $111, 110$ môžeme pokryť hranou (jednorozmernou Booleovskou kockou). Zoberne napokon štvoricu (jednotkových) vrcholov ležiacich napríklad na prednej stene kocky B^3: $000, 010, 011, 001$. Táto štvorica je pokrytá dvojrozmernou kockou. V ÚDNF bude uvedenej štvorici jednotkových vrcholov zodpovedať formula

$$\overline{x}_1\overline{x}_2\overline{x}_3 \vee \overline{x}_1x_2\overline{x}_3 \vee \overline{x}_1x_2x_3 \vee \overline{x}_1\overline{x}_2x_3$$

Opakovaným použitím distributívneho zákona túto formulu upravíme na tvar

$$\overline{x}_1(\overline{x}_2\overline{x}_3 \vee x_2\overline{x}_3 \vee \overline{x}_2x_3 \vee x_2x_3) = \overline{x}_1.$$

Teraz už vieme dosť na to, aby sme mohli popísať vzťahy medzi geometrickým modelom Booleovskej funkcie a jej DNF.

(a) elementárnej konjunkcii $x_{i_1}^{\sigma_{i_1}}, \ldots, x_{i_r}^{\sigma_{i_r}}$ zodpovedá množina vrcholov/vektorov tvoriacich jednotkovú podkocku dimenzie $n - r$. Vrcholy/vektory tejto podkocky majú fixované zložky $i_1, \ldots, i_r$, na ktorých nadobúdajú hodnoty $\sigma_{i_1}, \ldots, \sigma_{i_r}$.

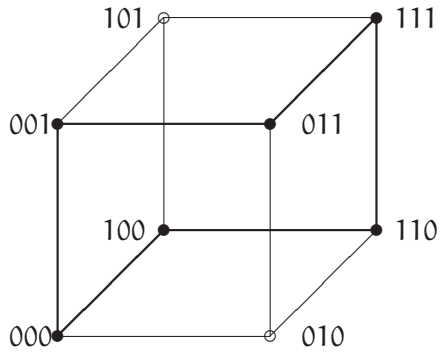
(b) DNF Booleovskej funkcie zodpovedá pokrytie vrcholov jej grafu jednotkovými podkockami.

(c) ÚDNF Booleovskej funkcie zodpovedá pokrytie vrcholov jej grafu jednotkovými podkockami dimenzie 0.

Konštrukcia DNF teda zodpovedá konštrukcii pokrytia vrcholov grafu Booleovskej funkcie jednotkovými podkockami. Jednotkový vrchol však môže byť pokrytý podkockami rozličných dimenzií. Uvažujme napríklad Booleovskú funkciu $f(x_1, x_2, x_3) = (01111111)$. Potom vrchol 111 možno pokryť 0-rozmernou podkockou zodpovedajúcou elementárnej konjunkcii $x_1x_2x_3$, 1-rozmernou podkocou (hranou) zodpovedajúcou elementárnej konjunkcii x_1x_2, dvojrozmernou podkockou zodpovedajúcou elementárnej konjunkcii x_1.[12] Videli sme, že čím väčšia je dimenzia podkocky, tým jednoduchšia je jej prislúchajúca konjunkcia a tým viac jednotkových vrcholov pokrýva. Ak máme možnosť pokryť nejaký jednotkový vrchol podkockami viacerých rozmerov, vyberieme z nich preto podkocku maximálneho rozmeru. Tento pojem je pre ďalší výklad taký dôležitý, že si zaslúži formálnu definíciu.

Definícia 12.7. *Nech je* $B^n(f)$ *graf (nejakej) Booleovskej funkcie* f. *Jednotková podkocka* C *grafu* $B^n(f)$ *sa nazýva maximálnou jednotkovou podkockou grafu* $B^n(f)$, *ak v grafe* $B^n(f)$ *neexistuje jednotková podkocka* C' *taká, že* C *je podgrafom* C'.

[12] vrchol 111 možno pokryť aj inými podkockami rozličných rozmerov.



Obrázok 12.5: Maximálne podkocky

V teórii DNF sa elementárne konjunkcie zodpovedajúce jednotkovým podkockám grafu $B^n(f)$ nazývajú aj *implikanty*. Tento názov vyplýva z toho, že ak K_i je elementárna konjunkcia zodpovedajúca jednotkovej podkocke C_i grafu $B^n(f)$, tak potom je implikácia $K_i \Rightarrow f$ pravdivá. Uvažujme postupnosť jednotkových podkociek $C_1, \ldots, C_m$ grafu $B^n(f)$, pričom C_i je zároveň podkockou C_{i+1} a postupnosť im prislúchajúcich elementárnych konjunkcií $K_1, \ldots, K_m$. Potom platia implikácie $K_i \Rightarrow K_{i+1}, 1 \leq i < m$ a $K_m \Rightarrow f$. Ak v grafe $B^n(f)$ neexistuje jednotková podkocka, ktorá by obsahovala podkocku C_m, tak potom je C_m maximálna podkocka. Elementárna konjunkcia zodpovedajúca maximálnej podkocke sa nazýva *prostým implikantom* (prime implicant). Význam pojmu implikant si najlepšie uvedomíme vtedy, keď v implikácii $K_i \Rightarrow f$ nahradíme elementárnu konjunkciu K_i elementárnou konjunkciou $K_i' \neq K_i$. Nech $K_i'(a_1 \ldots, a_n) = 1$ a $K_i(a_1 \ldots, a_n) = 0$, potom je implikácia $K_i \Rightarrow f$ na vektore $a_1 \ldots, a_n)$ pravdivá ($0 \Rightarrow 0 \equiv 1$), ale implikácia $K_i' \Rightarrow f$ na vektore $a_1 \ldots, a_n)$ je nepravdivá ($1 \Rightarrow 0 \equiv 0$). Dobrou stratégiou (aspoň na prvý pohľad) pri konštrukcii minimálnej DNF by mohlo byť vytvorenie zoznamu všetkých prostých implikantov Booleovskej funkcie f (resp. maximálnych podkociek grafu $B^n(f)$). Vzhľadom na to, ako sme definovali implikanty, resp. prosté implikanty Booleovskej funkcie, tvorí aj ich disjunkcia DNF Booleovskej funkcie.

Definícia 12.8. *Nech je* f *ľubovoľná Booleovská funkcia a* $K_1, \ldots, K_s$ *je množina všetkých prostých implikantov funkcie* f. *Disjunktívna normálna forma*

$$K_1 \vee \cdots \vee K_s$$

sa nazýva skrátenou disjunktívnou normálnou formou Booleovskej funkcie f.

Príklad 12.12. *Na obrázku 12.5 je uvedený graf Booleovskej funkcie* $f(x_1, x_2, x_3) = (11011011)$. *Booleovská funkcia má 6 prostých implikantov a jej skrátená DNF vyzerá nasledovne:*

$$f(x_1, x_2, x_3) = x_1x_2 \vee x_2x_3 \vee \overline{x}_1x_3 \vee \overline{x}_1\overline{x}_2 \vee \overline{x}_2\overline{x}_3 \vee x_1\overline{x}_3.$$

Predchádzajúci príklad ukazuje, že všetky prosté implikanty zo skrátenej DNF nemusia byť potrebné na realizáciu Booleovskej funkcie. Booleovskú funkciu z predchádzajúceho príkladu by bolo možné realizovať DNF obsahujúcou tri prosté implikanty:

$$f(x_1, x_2, x_3) = x_1x_2 \vee \overline{x}_1x_3 \vee \overline{x}_2\overline{x}_3.$$

Na vylúčenie nadbytočných prostých implikantov zo skrátenej DNF a na konštrukciu novej DNF sa používa nasledujúca induktívna metóda, pri ktorej využijeme korešpondenciu medzi prostými implikantami K_i a maximálnymi podkockami C_i grafu príslušnej Booleovskej funkcie:

1. vyberieme nejaký prostý implikant K_{i_1} a zaradíme ho do DNF;
2. predpokladáme, že v DNF sú už nejaké implikanty $K_{i_1}, \ldots, K_{i_{m-1}}$, $m > 1$ a nech K_{i_m} je nejaký prostý implikant zo skrátenej DNF. Ak existuje vrchol podkocky C_{i_m} ktorý nie je pokrytý podkockami $C_{i_1}, \ldots, C_{i_{m-1}}$, zaradíme K_{i_m} do DNF, v opačnom prípade ho do DNF nezaradíme. Tento krok opakujeme pre všetky prosté implikanty zo skrátenej DNF.

Po ukončení vyššie uvedenej procedúry dostávame DNF, z ktorej nemožno vyradiť žiaden prostý implikant, pretože výsledná DNF by potom už nerealizovala danú Booleovskú funkciu. Takáto DNF, v ktorej sa nevyskytujú nadbytočné prosté implikanty, sa nazýva *iredudantnou DNF*. Je zrejmé, že iredudantných DNF danej Booleovskej funkcie môže byť viacero (pozri 12.5). Napriek tomu konštrukcia minimálnej DNF vyzerá principiálne jednoducho—najprv zostrojíme ÚDNF, potom z ÚDNF skrátenú DNF a eleináciou nadbytočných prostých implikantov dostaneme niekoľko iredudantných DNF, medzi ktorými bude jedna alebo niekoľko minimálnych. Teória je však neúprosná—principiálne jednoduchá metóda sa vo všeobecnom prípade nedá použiť, pretože

- skrátená DNF je veľmi zložitá,
- iredudantných DNF je veľmi veľa,
- univerzálne a efektívne metódy preberania množiny prostých implikantov nie sú známe.

K týmto výsledkom sa ešte vrátime v závere tejto časti, zatiaľ sa však nimi nebudeme zaťažovať a pozrieme sa na prakticky použiteľné metódy konštrukcie skrátenej DNF.[13]

12.4.2 Quine-McCluskeyova metóda

Quineho-McCluskey-ova metóda sa výhodne používa pre funkcie závisiace od 5 a väčšieho počtu premenných. My ju vysvetlíme na príklade funkcie 4 premenných. Nech je daná Booleovská funkcia $f(x_1, x_2, x_3, x_4)$ zadaná pravdivostnou tabuľkou 12.13

Z konštrukcie pokrytí grafov Boleovských funkcií vieme, že spájať možno len susedné vrcholy, t.j. také, ktorých Hammingovská vzdialenosť je 1. Zostrojíme preto zoznam všetkých jednotkových vektorov Booleovskej funkcie f usporiadaných podľa ich Hammingovej váhy. V zozname budeme mať 5 skupín vrcholov: vrcholy/vektory váhy $0, \ldots, 4$, pozri tabuľka 12.14. Výhodou tohto usporiadania je, že susedné vrcholy/vektory

[13] Existencia takýchto metód vôbec nespochybňuje pesimistické teoretické výsledky. Znamená len to, že existujú prípady, pre ktoré sa minimálna DNF dá efektívne zostrojiť a že mnohé praktické problémy patria do tejto kategórie.

x_1	x_2	x_3	x_4	f	x_1	x_2	x_3	x_4	f
0	0	0	0	1	1	0	0	0	1
0	0	0	1	1	1	0	0	1	1
0	0	1	0	1	1	0	1	0	0
0	0	1	1	1	1	0	1	1	0
0	1	0	0	1	1	1	0	0	1
0	1	0	1	0	1	1	0	1	0
0	1	1	0	1	1	1	1	0	0
0	1	1	1	0	1	1	1	1	1

Tabuľka 12.13: Pravdivostná tabuľka Booleovskej funkcie f.

x_1	x_2	x_3	x_4	implikant	číslo	kontrola
0	0	0	0	$\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4$	0	
0	0	0	1	$\overline{x}_1\overline{x}_2\overline{x}_3x_4$	1	✓
0	0	1	0	$\overline{x}_1\overline{x}_2x_3\overline{x}_4$	2	✓
0	1	0	0	$\overline{x}_1x_2\overline{x}_3\overline{x}_4$	4	✓
1	0	0	0	$x_1\overline{x}_2\overline{x}_3\overline{x}_4$	8	✓
0	0	1	1	$\overline{x}_1\overline{x}_2x_3x_4$	3	✓
0	1	1	0	$\overline{x}_1x_2x_3\overline{x}_4$	6	✓
1	0	0	1	$x_1\overline{x}_2\overline{x}_3x_4$	9	✓
1	1	0	0	$x_1x_2\overline{x}_3\overline{x}_4$	12	✓
1	1	1	1	$x_1x_2x_3x_4$	15	

Tabuľka 12.14: Quine-McCluskey

sa nachádzajú v susedných skupinách. Všimneme si, že nám vypadla skupina vektorov váhy 3. Teraz budeme kombinovať vektory: v geometrickej interpretácii to znamená, že budeme susedné jednotkové vrcholy pokrývať hranami. Algebraická interpretácia „kombinovania“ vektorov znamená použitie distributívneho zákona a nahradenie dvojice konjunkcií $xK \vee \overline{x}K$ jednou konjunkciou K. Aby sme nestratili prehľad o tom, ktoré premenné sme vynechali, v príslušnom vektore hodnôt nahradíme hodnotu vynechanej premennej znakom "(don't care). Výsledky 1. kola „kombinovania“ vektorov sú uvedené v tabuľke 12.15. Pripomenieme ešte, že ak sme úspešne skombinovali dvojicu vektorov z tabuľky 12.14, oba vektory označíme znakom ✓.

V 1. kole sme našli všetky dvojice jednotkových vrcholov, ktoré bolo možné pokryť hranami. V 2.kole budeme hľadať možnosti pokrytia vrcholov 2-rozmernými jednotkovými kockami; t.j. možnosti nahradenia dvojice susedných jednotkových hrán dvojrozmernou jednotkovou kockou. To znamená, že v tabuľke 12.15 budeme opäť hľadať dvojice vektorov s Hammingovou vzdialenosťou 1, nahrádzať zložku, v ktorej sa odlišujú symbolom don't care a vyškrtávať z implikantov literál v ktorom sa odlišujú. Kedže vektory v tabuľke 12.15 obsahujú symboly don't care, kombinovať možno len tie vektory, ktoré majú symbol don't care na tom istom mieste, pozri tabuľku 12.16

Výsledky 2. kola kombinovania vektorov uvádzame v tabuľke 12.20. V predchádzajúcej tabuľke 12.15 označíme tie vektory, ktoré boli použité v 2. kole-ide o vektory, ktoré boli pokryté dvojrozmernými kockami. Keďže dvojrozmerná kocka sa skladá z

x_1	x_2	x_3	x_4	implikant	kombinácia	kontrola
0	0	0	–	$\overline{x}_1\overline{x}_2\overline{x}_3$	0, 1	✓
0	0	–	0	$\overline{x}_1\overline{x}_2\overline{x}_4$	0, 2	✓
0	–	0	0	$\overline{x}_1\overline{x}_3\overline{x}_4$	0, 4	✓
–	0	0	0	$\overline{x}_2\overline{x}_3\overline{x}_4$	0, 8	✓
0	0	–	1	$\overline{x}_1\overline{x}_2x_4$	1, 3	✓
0	0	1	–	$\overline{x}_1\overline{x}_2x_3$	2, 3	✓
0	–	1	0	$\overline{x}_1x_3\overline{x}_4$	2, 6	✓
0	1	–	0	$\overline{x}_1x_2\overline{x}_4$	4, 6	✓
–	0	0	1	$\overline{x}_2\overline{x}_3x_4$	1, 9	✓
1	0	0	–	$x_1\overline{x}_2\overline{x}_3$	8, 9	✓
–	1	0	0	$x_2\overline{x}_3\overline{x}_4$	4, 12	✓
1	–	0	0	$x_1\overline{x}_3\overline{x}_4$	8, 12	✓

Tabuľka 12.15: Quine-McCluskey, 1.kolo

x_1	x_2	x_3	x_4	implikant	kombinácia
0	0	0	–	$\overline{x}_1\overline{x}_2\overline{x}_3$	0, 1
0	0	1	–	$\overline{x}_1\overline{x}_2x_3$	2, 3
0	0	–	–	$\overline{x}_1\overline{x}_2$	0, 1, 2, 3

Tabuľka 12.16: kombinácie vektorov obsahujúcich don't care

dvoch dvojíc hrán, možno ju vytvoriť dvoma rozličnými spôsobmi. Preto v každom kroku budeme kontrolovať, či sme nevytvorili implikant, ktorý sa už v našom zozname nachádza; ak áno, nebudeme ho zapisovať ešte raz, ale označíme ako použitú (pokrytú) aj druhú dvojicu vektorov, ktorej kombináciou daný implikant vznikol.

Vektory z tabuľky 12.20 už nemáme s čím kombinovať. (Inak povedané, v grafe Booleovskej funkcie sa nevyskytujú jednotkové podkocky dimenzie 3 a vyššej.) V neoznačených riadkoch predchádzajúcich troch tabuliek 12.14, 12.15 a 12.20 sa nachádzajú všetky prosté implikanty Booleovskej funkcie f. Skrátená DNF Booleovskej funkcie f vyzerá nasledovne:

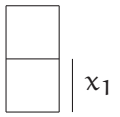
$$\overline{x}_1\overline{x}_2 \vee \overline{x}_2\overline{x}_3 \vee \overline{x}_1\overline{x}_4 \vee \overline{x}_3\overline{x}_4 \vee x_1x_2x_3x_4.$$

x_1	x_2	x_3	x_4	implikant	kombinácia
0	0	–	–	$\overline{x}_1\overline{x}_2$	0, 1, 2, 3
–	0	0	–	$\overline{x}_2\overline{x}_3$	0, 1, 8, 9
0	–	–	0	$\overline{x}_1\overline{x}_4$	0, 2, 4, 6
–	–	0	0	$\overline{x}_3\overline{x}_4$	0, 4, 8, 12

Tabuľka 12.17: Quine-McCluskey, 2. kolo

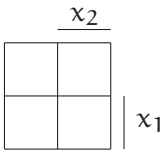
12.4.3 Karnaughove mapy

Pre Booleovské funkcie menšieho počtu premenných (≤ 4) možno na konštrukciu skrátenej DNF a často aj na konštrukciu minimálnej DNF použiť metódu založenú na inom geometrickom modeli Booleovskej funkcie, na tzv. Karnaughových mapách. Karnaughova mapa je tabuľka, do ktorej sa zapisujú hodnoty Booleovskej funkcie. Namiesto toho, aby sme ich definovali formálne, ukážeme, ako sa Karnaughove mapy konštruujú. Tieto mapy má zmysel konštruovať aspoň pre funkcie jednej premennej. Booleovská funkcia jednej premennej má pravdivostnú tabuľku s dvomi riadkami, to znamená, že Karnaughova mapa musí mať dve políčka. Aby sme nemuseli popisovať jednotlivé políčka tabuľky, označíme to políčko, pre ktoré nadobúda jediná premenná Booleovskej funkcie hodnotu 1. Je zrejmé, že na druhom políčku nadobúda hodnotu 0.



Obrázok 12.6: (Prázdna) Karnaughova mapa funkcie jednej premennej

Karnaughovu mapu pre funkciu dvoch premenných ($f(x_1, x_2)$) dostaneme tak, že spojíme dve Karnaughove mapy pre funkcie jednej premennej—$f(x_1, 1)$ a $f(x_1, 0)$, obrázok 12.7.



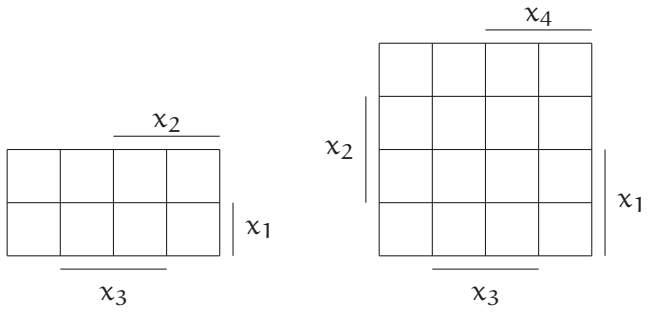
Obrázok 12.7: (Prázdna) Karnaughova mapa funkcie dvoch premenných

Karnaughovu mapu pre funkciu troch premenných $f(x_1, x_2, x_3)$ dostaneme spojením dvoch Karnaughových máp pre funkcie dvoch premenných $f(x_1, x_2, 0)$ a $f(x_1, x_2, 1)$, podobne ako Karnaughovu mapu pre funkciu štyroch premenných dostaneme spojením dvoch Karnaughových máp pre funkcie troch premenných, obrázok 12.8.

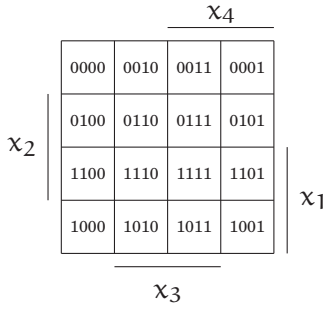
Dajú sa zostrojiť aj Karnaughove mapy pre Booleovské funkcie piatich a väčšieho počtu premenných, ale v týchto mapách už oblasti, v ktorých sú jednotlivé premenné jednotkové, nie sú súvislé. V ďalšom sa budeme podrobnejšie zaberať Karnaughovou mapou pre funkciu 4 premenných. Najprv explicitne uvedieme akým vektorom hodnôt zodpovedajú jednotlivé políčka Karnaughovej mapy, Obr. 12.9.

Zapíšme teraz do Karnaughovej mapy hodnoty Booleovskej funkcie. Podobne ako v prípade grafu Booleovskej funkcie, kde sme sa zaoberali len jednotkovými vrcholmi a ich pokrytím, budeme aj do Karnaughovej mapy zapisovať len jednotkové hodnoty Booleovskej funkcie. Na obrázku 12.10 je Karnaughova mapa funkcie 4 premenných, ktorú sme použili na ilustráciu Quine-McCluskeyovej metódy.

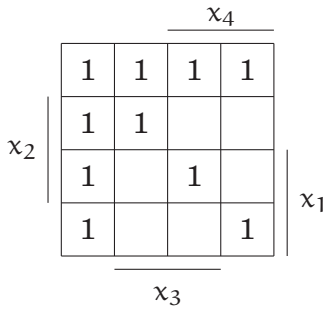
Priamo na základe Karnaughovej mapy možno zostrojiť ÚDNF Booleovskej funkcie.



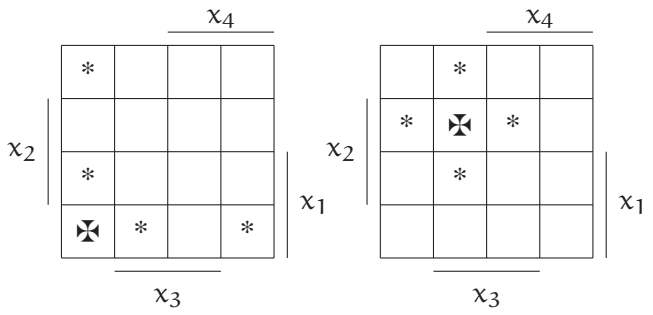
Obrázok 12.8: (Prázdne) Karnaughove mapy funkcie troch a štyroch premenných



Obrázok 12.9: „Adresy“ políčok v Karnaughovej mape štyroch premenných



Obrázok 12.10: Karnaughova mapa Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$



Obrázok 12.11: Susednosť v Karnaughovej mape

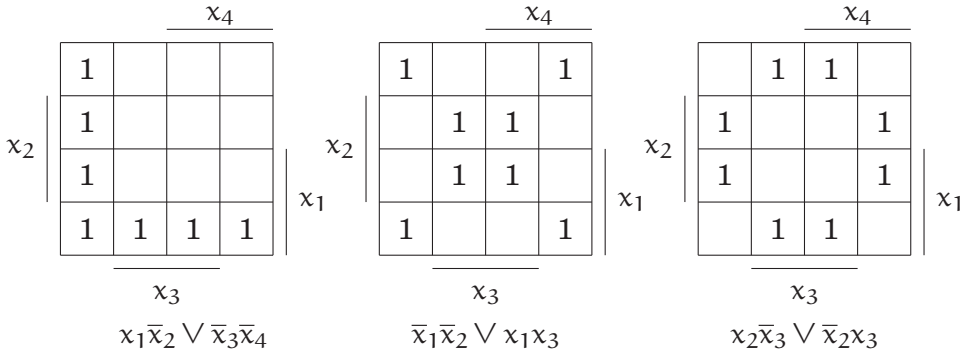
Každému jednotkovému políčku priradíme elementárnu konjunkciu na základe jeho „adresy"—napríklad jednotkové políčko s adresou 0111 leží v prieniku oblastí v ktorých premenné x_2, x_3, x_4 nadobúdajú hodnoty 1 a premenná x_1 hodnotu 0; jednotkovému vektoru 0111 teda priradíme elementárnu konjunkciu $\overline{x}_1 x_2 x_3 x_4$.[14] Na konštrukciu ÚDNF by sme nepotrebovali konštruovať Karnaughovu mapu, ale vystačili by sme s pravdivostnou tabuľkou Booleovskej funkcie. Karnaughova mapa nám umožňuje viac—nájsť prosté implikanty Booleovskej funkcie. Všimneme si vektory-adresy políčok Karnaughovej mapy na obrázku 12.9; každé políčko susedí so štyrmi ďalšími-políčkom nad, pod, napravo a naľavo, pričom susednosť presahuje cez okraj Karnaughovej mapy, prozri obrázok 12.11

Susedné jednotkové políčka možno spojiť do väčších jednotkových oblastí s 2, 4, 8, 16 políčkami. Jednotkovému políčku zodpovedá elementárna konjunkcia (v tomto prípade) rangu 4. Dve susedné jednotkové políčka tvoria oblasť, ktorej prislúcha elementárna konjunkcia rangu 3. Na obrázku 12.12 sú znázornené rozličné jednotkové oblasti so 4 políčkami a im prislúchajúce implikanty. Implikant (elementárnu konjunkciu) zodpovedajúcu jednotkovej oblasti Karnaughovej mapy určíme tak, že do konjunkcie zaradíme literály určujúce oblasti, do prieniku ktorých daná jednotková oblasť patrí. Ak sa v jednotkovej oblasti nachádzajú políčka z oblasti x_i aj $\overline{x}_i$, literál premennej x_i sa v konjunkcii nebude vyskytovať; ak daná jednotková oblasť leží celá v oblasti x_i, jej konjunkcia bude obsahovať premennú x_i a napokon, ak jednotková oblasť leží mimo oblasti x_i jej konjunkcia bude obsahovať negáciu tejto premennej— $\overline{x}_i$.

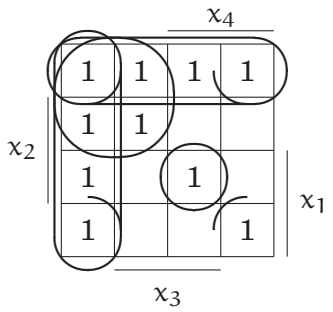
Vrátime sa ku Karnaughovej mape Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$. V Karnaughovej mape vyznačíme jednotkové oblasti a im prislúchajúce prosté implikanty (obrázok 12.13):

1. 1. stĺpec zľava: $\overline{x}_3\overline{x}_4$
2. 1. riadok zhora: $\overline{x}_1\overline{x}_2$
3. ľavý horný kvadrant: $\overline{x}_1\overline{x}_4$

[14] Inak povedané, jednotkovému vektoru $\sigma_1, \sigma_2\sigma_3, \sigma_4$ priradíme (ako sa dalo očakávať) elementárnu konjunkciu $x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} x_4^{\sigma_4}$. Pointa je v tom, že v Karnaughovej mape sú vyznačené len oblasti, v ktorých nadobúdajú jednotlivú premenné jednotkové hodnoty a nie vektory hodnôt premenných.



Obrázok 12.12: Jednotkové oblasti v Karnaughovej mape



Obrázok 12.13: Prosté implikanty Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$

4. všetky 4 rohy: $\overline{x}_2\overline{x}_3$
5. izolovaná jednotka v pravom dolnom kvadrante: $x_1x_2x_3x_4$

Skrátená a zároveň minimálna DNF Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$ je

$$\overline{x}_1\overline{x}_2 \vee \overline{x}_2\overline{x}_3 \vee \overline{x}_1\overline{x}_4 \vee \overline{x}_3\overline{x}_4 \vee x_1x_2x_3x_4.$$

12.4.4 Výber pokrytia

Predpokladajme, že sme úspešne zostrojili skrátenú DNF; t.j. našli všetky prosté implikanty Booleovskej funkcie. Ďalším krokom je odstránenie nadbytočných prostých implikantov a konštrukcia iredudantnej DNF. Ako sa ukáže v nasledujúcej časti, Booleovská funkcia môže mať veľký počet prostých implikantov a vybrať z nich tie, ktoré tvoria minimálnu DNF je vo všeobecnosti veľmi náročná úloha. Pre malý počet[15] premenných sa pokrytie dá zostrojiť pomocou tabuľky pokrytia a niekoľkých relatívne jednoduchých pravidiel. Tabuľka pokrytia Booleovskej funkcie f vyzerá nasledovne: každému jednotkovému vektoru funkcie f je priradený stĺpec (kvôli zjednodušeniu označenia sa namiesto $\sigma(n, i)$ označuje stĺpec len symbolom m_i a nulové vektory do tabuľky pokrytia nezapisujeme). Riadkom matice pokrytia sú priradené prosté implikanty Booleovskej funkcie f. Ak implikant K_j pokrýva vrchol/vektor m_i, na priesečníku riadka K_j a stĺpca m_i je v tabuľke pokrytia jednotka. V opačnom prípade ponecháme kvôli prehľadnosti políčko tabuľky prázdne. Na ilustráciu uvádzame tabuľku pokrytia funkcie $f(x_1, x_2, x_3, x_4)$ z predchádzajúceho príkladu, tabuľka 12.18.

	m_0	m_1	m_2	m_3	m_4	m_6	m_8	m_9	m_{12}	m_{15}	cena
$\overline{x}_1\overline{x}_2$	1	1	1	1							2
$\overline{x}_2\overline{x}_3$	1	1					1	1			2
$\overline{x}_1\overline{x}_4$	1		1		1	1					2
$\overline{x}_3\overline{x}_4$	1				1		1		1		2
$x_1x_2x_3x_4$										1	4

Tabuľka 12.18: Tabuľka pokrytia Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$

Každému prostému implikantu sme priradili cenu, v tomto prípade vyjadrenú počtom jeho literálov. Cena môže byť stanovená aj ináč a zohráva dôležitú úlohu pri rozhodovaní, ktorý z prostých implikantov zaradíme do pokrytia a ktorý vylúčime. Je zrejmé, že na to, aby výsledná DNF realizovala danú Booleovskú funkciu, je potrebné vybrať do DNF (resp. jej zodpovedajúceho pokrytia) prosté implikanty tak, že ak ponecháme v tabuľke len riadky zodpovedajúce vybraným prostým implikantom, každom stĺpci tabuľky pokrytia bude aspoň jedna jednotka. Pri výbere prostých implikantov budeme využívať nasledujúce pravidlá:

[15] pojem malý je relatívny. Pred niekoľkými rokmi sa študenti naprogramovali konštrukciu minimálnej DNF. Program sám o sebe nebol zložitý, ale keď ho testovali na vtedy modernej 286-ke, problémy sa prejavili už pri funkciách 8 premenných. Efektívnejšie kódovanie implikantov umožnilo zvýšiť počet premenných o 1, ale podstatné vylepšenie neprinieslo.

Pravidlo podstatného prostého implikantu. Prvé pravidlo je jednoduché a logické: **ak je v niektorom sĺpci tabuľky pokrytia jediná jednotka, príslušný prostý implikant musí byť zaradený do DNF** (a to bez ohľadu na jeho cenu) do DNF, pretože bez neho sa DNF realizujúca danú Booleovskú funkciu zostrojiť nedá. Takýto prostý implikant sa nazýva *podstatný*. Z tabuľky 12.14 vidíme, že sú všetky implikanty podstatné a teda skrátená DNF je zároveň aj minimálnou DNF danej Booleovskej funkcie. Vo všeobecnom prípade to také jednoduché nebude. Nájdenie podstatného implikantu (napríklad K_j) nám však umožní zjednodušiť tabuľku pokrytia—môžeme z nej odstrániť všetky stĺpce, ktoré majú v riadku zodpovedajúcemu K_j jednotky. Vektory/vrcholy prislúchajúce týmto stĺpcom sú už pokryté vybraným prostým implikantom

Pravidlo dominujúceho riadka. Pre pravidlo dominujúceho riadka je podstatné rozmiestnenie jednotkových prvkov v riadku a cena riadka. Nech má riadok r_j jednotkové hodnoty v stĺpcoch $i_1, \ldots, i_s$; cenu c_j a riadok r_k jednotkové hodnoty v stĺpcoch $l_1, \ldots, l_t$ a cenu c_k . Budeme hovoriť, že riadok r_j dominuje nad riadkom r_k práve vtedy, ak $\{l_1, \ldots, l_t\} \subseteq \{i_1, \ldots, i_s\}$ a $c_j \leq c_k$; t.j. riadok r_k pokrýva len nejakú podmnožinu tých vektorov, ktoré pokrýva riadok r_j a má vyššiu alebo rovnakú cenu ako riadok r_j. Pravidlo dominujúceho riadka potom znie **ak v tabuľke pokrytia riadok r_j dominuje nad riadkom r_k, možno z nej riadok r_k vynechať.**

	m_0	m_1	m_2	m_3	m_4	m_6	m_{12}	m_{15}	cena
$\overline{x}_1\overline{x}_2$	1	1	1	1					2
$\overline{x}_2\overline{x}_3$	1	1							2

Tabuľka 12.19: Dominujúci riadok

Na začiatku konštrukcie DNF obsahuje tabuľka pokrytia len prosté implikanty a pravidlo dominujúceho riadka nemožno uplatniť. Po uplatnení iných pravidiel z tabuľky vypadnú niektoré riadky a stĺpce a môžu sa objaviť aj dominujúce riadky. Ilustrujeme to na príklade, ktorý sme dostali modifikáciou[16] tabuľky 12.14. Predpokladajme, že nejakým spôsobom už boli pokryté vektory m_8, m_9. Potom riadok $\overline{x}_1\overline{x}_2$ dominuje nad riadkom $\overline{x}_2\overline{x}_3$ a teda riadok $\overline{x}_2\overline{x}_3$ možno z tabuľky pokrytia vylúčiť.

Pravidlo dominujúceho stĺpca Nech stĺpce m_r, m_s tabuľky pokrytia, majú jednotkové hodnoty v riadkoch $i_1, \ldots, i_k$, resp. $j_1, \ldots, j_l$ Stĺpec m_r dominuje nad stĺpcom m_s práve vtedy, ak $\{i_1, \ldots, i_k\} \subseteq \{j_1, \ldots, j_l$; t.j. každý implikant, ktorý pokrýva m_r, pokrýva aj m_s. Pravidlo dominujúceho stĺpca: **ak stĺpec m_r dominuje nad stĺpcom m_s, tak stĺpec m_s možno z tabuľky pokrytia vyradiť.** Napríklad v tabuľke 12.14 dominuje stĺpec m_3 nad stĺpcami m_0, m_1, m_2, m_6 nad m_4 a pod.

Pri konštrukcii pokrytia (minimalizácii DNF) sa pokúšame opakovane používať jednotlivé pravidlá. Niekedy sa stáva, že sa už žiadne z uvedených pravidielnedá použiť ale konštrukcia DNF nie je ukončená (ostali nepokryté stĺpce a niekoľko prostých implikantov, z ktorých je potrebné vyberať.). Vtedy je potrebné rozumným spôsobom prebrať

[16] pripomíname, že teraz už nejde o minimalizáciu pôvodnej Booleovskej funkcie

všetky možnosti: vyberieme stĺpec, ktorý obsahuje najmenej jednotiek (napríklad 2), vyberieme prostý implikant zodpovedajúci prvej jednotke, zaradíme ho do DNF a pokračujeme v konštrukcii DNF. Potom vyberieme prostý implikant zodpovedajúci druhej jednotke, zostrojíme DNF, napokon porovnáme obe DNF a vyberieme z nich tú, ktorá má nižšiu cenu.

Pri návrhu logických obvodov bývajú transformácie, ktoré je potrebné realizovať, často popísané pomocou *Booleovských operátorov.* (Pripomíname, že Booleovský operátor je zobrazenie $F^{n,m} : \{0,1\}^n \to \{0,1\}^m$, ktoré sa dá interpretovať ako m-tica n-árnych Booleovských funkcií.) Booleovský operátor by sme mohli realizovať pomocou DNF jeho jednotlivých Booleovských funkcií. Takáto realizácia však nevyužíva to, že čiastkové funkcie Booleovského operátora nemusia byť nezávislé (môžu sa medzi nimi dokonca vyskytovať rovnaké funkcie) a pre každú z nich konštruuuje samostatnú DNF. Quineho-McCluskeyova metóda konštrukcie prostých implikantov a uvedená metóda konštrukcie DNF sa dá upraviť aj na konštrukciu disjunktívnych normálnych foriem realizujúcich Booleovské operátory. Modifikácia Quineho-McCluskeyovej metódy spočíva vo vyhľadávaní všetkých spoločných (skupinových) prostých implikantov pre všetky možné kombinácie čiastkových Booleovských funkcií Boolovského operátora. To potom pri konštrukcii pokrytia (DNF) umožňuje rozhodovať o tom, ktoré jednotkové vrcholy jednotlivých čiasktových Booleovských funkci sa budú pokrývať individuálne a u ktorých sa pokrytie bude zdieľať. Konštrukcia skupinových prostých implikantov nie je principiálne zložitá, problém spočíva v tom, že netriviálnych kombinácii m Booleovských funkcií je $2^m - 2$ a rozličných skupinových prostých implikantov môže byť už pre malé hodnoty n, m netriviálne veľa.

12.4.5 *Odhady parametrov DNF

V predchádzajúcich častiach tejto kapitoly sme neraz narazili na problém, že principiálne jednoduchá konštrukcia nemusí byť prakticky použiteľná. Jednoduchým príkladom je ÚDNF. n-árna Booleovská funkcia je zadaná vektorom svojich pravdivostných hodnôt, ktorý má dĺžku 2^n. Typická Booleovská funkcia f má približne polovicu jednotiek a polovicu núl; presnejší odhad dostaneme pomocou Čebyševovej nerovnosti:

$$2^{n-1} - \phi(n) \cdot 2^{n/2} < |N_f| < 2^{n-1} + \phi(n) \cdot 2^{n/2},$$

kde $\phi(n) \to \infty$ pre $n \to \infty$ je ľubovoľná pomaly rastúca funkcia. To znamená, že dĺžka ÚDNF typickej n-árnej Booleovskej funkcie bude približne 2^{n-1}. Problémy spojené s minimalizáciou DNF viedli k skúmaniu dlžok a počtov rozličných DNF Booleovských funkcií. Dosiahnuté výsledky umožnili vytvoriť si ucelenejšiu predstavu o zložitosti problémov, na ktorý pri minimalizácii DNF narážame a posúdeniu efektívnosti metód minimalizácie. Výsledky sú prebraté z [9] a uvádzame ich bez dôkazov. Budeme používať nasledujúce označenie: ak λ označuje nejaký parameter Booleovských funkcií, tak $\lambda(f)$ označuje hodnotu tohto parametra na funkcii f a $\lambda(n) = \max_f \lambda(f)$, pričom maximum sa berie cez všetky n-árne Booleovské funkcie.

Dĺžka skrátenej DNF. Nech $l_S(f)$ označuje dĺžku skrátenej DNF Booleovskej funkcie f. Potom[17]

$$\frac{3^n}{n} \preccurlyeq l_S(n) \preccurlyeq \frac{3^n}{\sqrt{n}}.$$

Pritom pre skoro všetky n-árne Booleovské funkcie platí

$$n^{(1-\delta'_n)\lg\lg n} \cdot 2^n \leq l_S(f) \leq n^{(1+\delta''_n)\lg\lg n} \cdot 2^n,$$

kde $\delta'_n, \delta''_n \to 0$ pre $n \to \infty$.

Počet iredudantných DNF. Nech $t(f)$ označuje počet iredudantných DNF Booleovskej funkcie f. Najprv uvedieme odhad maximálnej hodnoty:

$$\left(2^{2^n}\right)^{c'_n\sqrt{n}} \leq t(n) \leq \left(2^{2^n}\right)^{c''_n n},$$

kde veličiny c'_n (pre $n \geq 3$) sú zdola a c''_n zhora ohraničené kladnými konštantami. Pre skoro všetky n-árne Booleovské funkcie je počet iredudantných DNF ohraničený nasledovne:

$$\left(2^{2^{n-1}}\right)^{(1-\varepsilon'_n)\lg n\lg\lg n} \leq t(f) \leq \left(2^{2^{n-1}}\right)^{(1+\varepsilon''_n)\lg n\lg\lg n},$$

kde $\varepsilon'_n, \varepsilon''_n \to 0$ pre $n \to \infty$. To znamená, že prehľadávanie množiny iredudantných DNF na to, aby sme našli minimálnu DNF je mimoriadne náročné.

Počet najkratších DNF. Najkratšia DNF má minimálnu dĺžku, t.j. počet konjunkcií. Dá sa očakávať, že pre jednu Booleovskú funkciu bude existovať viacero najkratších DNF. Označme symbolom $q(f)$ počet najkratších DNF Booleovskej funkcie f. Je známy len dolný odhad maximálnej hodnoty parametra $q(n)$:

$$\left(2^{2^n}\right)^{c'_n\sqrt{n}} \leq t(n).$$

Dĺžka iredudantnej DNF. Nech $l_T(f)$ je maximálna dĺžka iredudantnej DNF a $l_K(f)$ dĺžka najkratšej DNF. Potom

$$l_K(n) \sim 2^n,$$

a pre skoro všetky Booleovské funkcie

$$l_K(f) \sim 2^{n-1}$$

.

Dĺžka najkratšej DNF. Označme symbolom $l_K(f)$ dĺžka najkratšej DNF. Potom

$$l_K(n) = 2^{n-1},$$

a pre skoro všetky n-árne Booleovské funkcie

$$\frac{2^{n-1}}{\lg n \lg\lg n} \lesssim l_K(f) < \frac{2^n}{\lg n}.$$

[17] Symbol $\preccurlyeq$ vyjadruje vzťah menší alebo rádovo rovný.

Relatívna dĺžka iredudantnej DNF. Pre danú Booleovskú funkciu existuje—ako sme videli—veľa iredudandntých DNF. Bolo by zaujímavé vedieť, do akej miery sa ich dĺžky odlišujú od optima, ktoré predstavuje dĺžka najkratšej DNF. Relatívnou dĺžkou iredudantnej DNF sa nazýva pomer jej dĺžky k dĺžke najkratšej DNF. Pre funkciu f zavádzame parameter $\Upsilon(f)$, nazývaný rozptylom, ktorý je definovaný ako maximálna relatívna dĺžka iredudantnej DNF Booleovskej funkcie f. Pre maximálnu hodnotu rozptylu dĺžok platí

$$\Upsilon(n) = 2^{n(1-\varepsilon)},$$

kde $\varepsilon \to 0$, pre $n \to \infty$. Pre typickú Booleovskú funkciu je rozptyl dĺžok DNF podstatne menší, aj keď rastie vzhľadom na veľkosť n:

$$\lg n \preceq F(f) \precsim \lg n \lg\lg n.$$

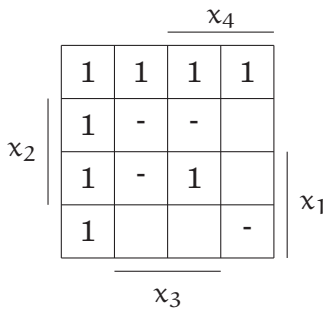
Keďže iredudantných DNF je príliš veľa na úplné preberanie, alternatívou úplného preberania by mohol byť náhodný výber a následné úplné preberanie podmnožiny iredudantných DNF. Posledný odhad hovorí, že takýmto spôsobom by sme mohli dostať iredudantnú DNF, ktorej dĺžka by bola minimálne $\lg n$-krát dlhšia, ako je dĺžka najkratšej DNF.

12.4.6 Neúplne určené Booleovské funkcie

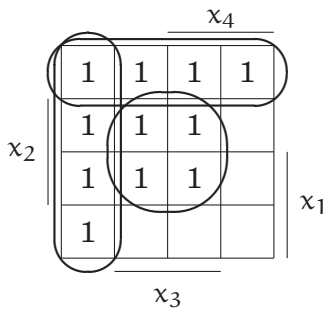
V niektorých úlohách sa stretávame s Booleovskými funkciami, ktoré nie sú definované pre všetky hodnoty svojich vstupných premenných (pozri napríklad tabuľku 12.4). Dalo by sa očakávať, že táto neurčitosť bude pri realizácii Booleovských funkcií spôsobovať problémy. Prekvapujúce je, že nie a dokonca realizácia neúplne určených Booleovských funkcií môže byť jednoduchšia, ako v prípade plne definovaných funkcií. Čo vlastne—z hľadiska realizácie—znamená, že Booleovská funkcia je na nejakom vektore svojich hodnôt neurčená? Môže sa to chápať dvojako: buď je z nejakých dôvodov jedno, akú hodnotu Booleovská funkcia na danom vektore nadobúda; alebo je daná vstupná hodnota zakázaná a tak je v konečnom dôsledku tiež jedno, akú hodnotu bude Booleovská funkcia na zakázanom vstupe nadobúdať. Ošetrenie vstupov formuly alebo obvodu realizujúceho Booleovskú funkciu nie je našou úlohou. Budeme predpokladať, že tento problém je vyriešený a pre nás neurčená hodnota znamená, že ju môžeme definovať ako sa nám hodí. Rozumné je ponechať si možnosť dodefinovať funkciu otvorenú čo najdlhšie. To sa dá spraviť tak, že sa neurčeným hodnotám priradí symbol - (don't care). Pri hľadaní prostých implikantov s "don't care" narábame tak, ako keby predstavoval hodnotu 1, s výnimkou prípadov, keď by sme mali zostrojiť prostý implikant, ktorý by pokrýval samé "don't care" -vektory. To však ošetríme pri konštrukcii pokrytia; v záhlaví tabuľky pokrytia uvedieme len jednotkové vrcholy, a to znamená, že prosté implikanty, ktoré by pokrývali len "don't care" vrcholy sa do tabuľky nedostanú, resp. vypadnú automaticky na základe pravidla o dominujúcom riadku. Metódu ilustrujeme na príklade. Na obrázku 12.14 je uvedená Karnaughova mapa neúplne určenej Booleovskej funkcie 4 premenných.

Na základe Karnaughovej mapy zostrojíme priamo DNF Booleovskej funkcie:

$$\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4 \vee x_2x_3.$$



Obrázok 12.14: Karnaughova mapa neúplne určenej Booleovskej funkcie



Obrázok 12.15: Doplnenie neúplne určenej Booleovskej funkcie

Tri "don't care" -vektory sme definovali ako jednotkové, jeden ako nulový—obrázok 12.15

Zostrojíme teraz pomocou Qiune-McCluskeyovej metódy zoznam všetkých prostých implikantov neúplne určenej Booleovskej funkcie a potom zostrojíme pokrytie jednotkových vektorov, resp. jemu zodpovedajúcu minimálnu DNF danej Booleovskej funkcie.

Teraz zostrojíme tabuľku pokrytia. Vektor m_{15} je pokrytý jedine prostým implikantom x_2x_3; t.j. implikant x_2x_3 je podstatný. 1. riadok $(\overline{x}_1\overline{x}_2)$ dominuje nad 5. riadkom $(\overline{x}_1x_3)$, 4. riadok $(\overline{x}_3\overline{x}_4)$ nad 6. riadkom $(x_2\overline{x}_4)$. Po odstránení 7. riadka a stĺpca m_{15}, 5. a 6. riadku dostávame nasledujúcu tabuľku pokrytia: Z tabuľky pokrytia vyplýva, že podstatné implikanty sú $\overline{x}_1\overline{x}_2$, ktorý pokrýva vektor m_3 a $\overline{x}_3\overline{x}_4$, ktorý pokrýva vektor m_{12}. Tieto dva implikanty však pokrývajú všetky ostávajúce jednotkové vektory, a teda minimálna DNF pre neúplne určenú Booleovskú funkciu f bude:

$$\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4 \vee x_2x_3.$$

Pripomenieme, že túto istú DNF sme dostali podstatne jednoduchším spôsobom pomocou karnaughovej mapy.

x_1	x_2	x_3	x_4	implikant	číslo	kontrola
0	0	0	0	$\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4$	0	✓
0	0	0	1	$\overline{x}_1\overline{x}_2\overline{x}_3x_4$	1	✓
0	0	1	0	$\overline{x}_1\overline{x}_2x_3\overline{x}_4$	2	✓
0	1	0	0	$\overline{x}_1x_2\overline{x}_3\overline{x}_4$	4	✓
1	0	0	0	$x_1\overline{x}_2\overline{x}_3\overline{x}_4$	8	✓
0	0	1	1	$\overline{x}_1\overline{x}_2x_3x_4$	3	✓
0	1	1	0	$\overline{x}_1x_2x_3\overline{x}_4$	6	✓
1	0	0	1	$x_1\overline{x}_2\overline{x}_3x_4$	9	✓
1	1	0	0	$x_1x_2\overline{x}_3\overline{x}_4$	12	✓
0	1	1	1	$\overline{x}_1x_2x_3x_4$	7	✓
1	1	1	0	$x_1x_2x_3\overline{x}_4$	14	✓
1	1	1	1	$x_1x_2x_3x_4$	15	✓
0	0	0	–	$\overline{x}_1\overline{x}_2\overline{x}_3$	0, 1	✓
0	0	–	0	$\overline{x}_1\overline{x}_2\overline{x}_4$	0, 2	✓
0	–	0	0	$\overline{x}_1\overline{x}_3\overline{x}_4$	0, 4	✓
–	0	0	0	$\overline{x}_2\overline{x}_3\overline{x}_4$	0, 8	✓
0	0	–	1	$\overline{x}_1\overline{x}_2x_4$	1, 3	✓
0	0	1	–	$\overline{x}_1\overline{x}_2x_3$	2, 3	✓
0	–	1	0	$\overline{x}_1x_3\overline{x}_4$	2, 6	✓
0	1	–	0	$\overline{x}_1x_2\overline{x}_4$	4, 6	✓
–	0	0	1	$\overline{x}_2\overline{x}_3x_4$	1, 9	✓
1	0	0	–	$x_1\overline{x}_2\overline{x}_3$	8, 9	✓
–	1	0	0	$x_2\overline{x}_3\overline{x}_4$	4, 12	✓
1	–	0	0	$x_1\overline{x}_3\overline{x}_4$	8, 12	✓
0	–	1	1	$\overline{x}_1x_3x_4$	3, 7	✓
0	1	1	–	$\overline{x}_1x_2x_3$	6, 7	✓
–	1	1	0	$x_2x_3\overline{x}_4$	6, 14	✓
1	1	–	0	$x_1x_2\overline{x}_4$	12, 14	✓
–	1	1	1	$x_2x_3x_4$	7, 15	✓
1	1	1	–	$x_1x_2x_3$	14, 15	✓
0	0	–	–	$\overline{x}_1\overline{x}_2$	0, 1, 2, 3	
–	0	0	–	$\overline{x}_2\overline{x}_3$	0, 1, 8, 9	
0	–	–	0	$\overline{x}_1\overline{x}_4$	0, 2, 4, 6	
–	–	0	0	$\overline{x}_3\overline{x}_4$	0, 4, 8, 12	
0	–	1	–	$\overline{x}_1x_3$	2, 3, 6, 7	
–	1	–	0	$x_2\overline{x}_4$	4, 6, 12, 14	
–	1	1	–	x_2x_3	6, 7, 14, 15	

Tabuľka 12.20: Prosté implikanty Booleovskej funkcie f

implikant	m_0	m_1	m_2	m_3	m_4	m_8	m_{12}	m_{15}	cena
$\overline{x}_1\overline{x}_2$	1	1	1	1					2
$\overline{x}_2\overline{x}_3$	1	1				1			2
$\overline{x}_1\overline{x}_4$	1		1		1				2
$\overline{x}_3\overline{x}_4$	1				1	1	1		2
$\overline{x}_1x_3$			1	1					2
$x_2\overline{x}_4$					1		1		2
x_2x_3								1	2

Tabuľka 12.21: Tabuľka pokrytia (1)

implikant	m_0	m_1	m_2	m_3	m_4	m_8	m_{12}	cena
$\overline{x}_1\overline{x}_2$	1	1	1	1				2
ï$\overline{x}_2\overline{x}_3$	1	1				1		2
$\overline{x}_1\overline{x}_4$	1		1		1			2
$\overline{x}_3\overline{x}_4$	1				1	1	1	2

Tabuľka 12.22: Tabuľka pokrytia (2)

12.5 Úplnosť a uzavretosť systému Booleovských funkcií

Podľa vety 12.2 stačia Booleovské funkcie $\{x_1\&x_2, x_1 \vee x_2, \neg x\}$ na vyjadrenie všetkých ostatných Booleovských funkcií. Existujú aj iné množiny Booleovských funkcií s touto vlastnosťou? Ak je daná množina Booleovských funkcií, vieme určiť, či sa pre ľubovoľnú Booleovskú funkciu dá vytvoriť formula nad touto množinou, ktorá danú Booleovskú funkciu realizuje? Odpovede na tieto otázky budeme hľadať v tejto časti. Začneme upresnením niektorých základných pojmov.

Definícia 12.9. *Nech je $\mathcal{M}$ množina Booleovských funkcií. Budeme hovoriť, že $\mathcal{M}$ je úplná ($\mathcal{M}$ tvorí úplný systém Booleovských funkcií), práve vtedy ak ľubovoľnú Booleovskú funkciu možno realizovať pomocou formuly nad $\mathcal{M}$.*

Príklad 12.13. *Nasledujúce množiny Booleovských funkcí tvoria úplné systémy.*

1. *Množina $\mathcal{P}_2$ všetkých Booleovských funkcií,*
2. *Množina $\{x_1\&x_2, x_1 \vee x_2, \neg x\}$,*
3. *Ľubovoľná množina Booleovských funkcií, ktorá je nadmnožinou množiny $\{x_1\&x_2, x_1 \vee x_2, \neg x\}$ alebo inej úplnej množiny Booleovských funkcií.*

Na druhej strane nie všetky množiny Booleovských funkcií sú úplné. Napríklad $\neg x$ nestačí na vyjadrenie konjunkcie; obe konštanty 0 a 1 sú nulárne (nemajú podstatné premenné), a preto z nich nemožno vyjadriť ani funkciu s apoň jednou podstatnou premennou. Nasledujúca veta dáva návod na to, ako zistiť, či nejaká množina Booleovských funkcí tvorí úplný systém.

Veta 12.4. *Nech sú dané dve množiny Booleovských funkcií z $\mathcal{P}_2$, $\mathcal{F} = \{f_1, f_2, \ldots, f_s\}$ a $\mathcal{G} = \{g_1, g_2, \ldots, g_t\}$ také že:*

1. *$\mathcal{F}$ tvorí úplný systém Booleovských funkcií a*
2. *každá funkcia z $\mathcal{F}$ sa dá realizovať pomocou formuly nad množinou $\mathcal{G}$.*

Potom množina $\mathcal{G}$ tvorí úplný systém Booleovských funkcií.

Dôkaz. Nech je h ľubovoľná funkcia z $\mathcal{P}_2$. Potom existuje formula $\mathbf{A}[\mathcal{F}]$, ktorá realizuje funkciu h; $\mathbf{A} = f_{i_0}(f_{i_1}, \ldots, f_{i_m})$, $\forall k f_{i_k} \in \mathcal{F}$. Podľa predpokladu vety možno každú funkciu $f_i \in \mathcal{F}$ realizovať pomocou formuly nad $\mathcal{G}$; $f_j = \mathbf{B}_j[\mathcal{G}]$; $\mathbf{B}_j = g_{j_0}(g_{j_1}, \ldots, g_{j_n})$. Ak vo formule $\mathbf{A}$ nahradíme každú funkciu z $\mathcal{F}$, formulou nad $\mathcal{G}$, ktorá ju realizuje, dostávame formulu $\mathbf{A}'[\mathcal{G}] \equiv \mathbf{A}[\mathcal{F}]$. Keďže $\mathcal{F}$ tvorí úplný systém Booleovských funkcií, každú Booleovskú funkciu z $\mathcal{P}_2$ môžeme realizovať pomocou formuly nad $\mathcal{F}$ a túto formulu zasa môžeme vyjadriť pomocou funkcií z $\mathcal{G}$. To znamená, že aj $\mathcal{G}$ tvorí úplný systém Booleovských funkcií. □

Využijeme tvrdenie vety 12.4 a zostrojíme niekoľko ďalších úplných systémov Booleovských funkcií.

Príklad 12.14. 1. *Množina Booleovských funkcií $\{\neg x, x_1 \& x_2\}$ tvorí úplný systém, pretože $x_1 \vee x_2 \equiv \neg(\neg x_1 \& \neg x_2)$, podobne*

2. *množina Booleovských funkcií $\{\neg x, x_1 \vee x_2\}$ tvorí úplný systém, pretože $x_1 \& x_2 \equiv \neg(\neg x_1 \vee \neg x_2)$.*

Úloha 12.9. *Zistite, či nasledujúce množiny Booleovských funkcií tvoria úplné systémy:*

1. $\{\neg x_1, x_1 \Rightarrow x_2\}$;
2. $\{1, x_1 \Rightarrow x_2\}$;
3. $\{0, x_1 \Rightarrow x_2\}$;
4. $\{x_1 \& x_2, x_1 \Rightarrow x_2\}$;
5. $\{f_{14}\}$, *Pierceova funkcia;*
6. $\{f_8\}$, *Shefferova funkcia.*

Zaujímavý úplný systém Booleovských funkcií predstavuje nasledujúca množina:

$$\mathcal{D}_3 = \{x_1 \& x_2, x_1 \oplus x_2, 1\}.$$

Podľa predchádzajúcej vety na dôkaz úplnosti stačí ukázať, že pomocou funkcií z $\mathcal{D}_3$ vyjadríme všetky funkcie nejakého úplného systému, napríklad $\{\neg x, x_1 \& x_2\}$. Množina $\mathcal{D}_3$ obsahuje konjunkciu, ale neobsahuje negáciu. Negácia sa však dá vyjadriť takto:

$$\neg x \equiv x \oplus 1. \tag{12.12}$$

To znamená, že množina $\mathcal{D}_3$ tvorí skutočne úplný systém Booleovských funkcií. Konjunkcia a sčítanie modulo 2 sú komutatívne operácie a platí pre ne distributívny zákon (operátor & kvôli zjednodušeniu zápisu vynechávame):

$$x_1(x_2 \oplus x_3) \equiv x_1 x_2 \oplus x_1 x_3. \tag{12.13}$$

Ak využijeme vzťahy 12.12 a 12.13, môžeme ľubovoľnú formulu[18] nad množinou $\mathcal{D}_3$ vyjadriť v *algebraickej normálnej forme* (ANF), nazývanej aj *Žegalkinovým polynómom*:

$$f(x_1, \ldots, x_n) = \bigoplus_{i_1,\ldots,i_s} a_{i_1,\ldots,i_s} x_{i_1} \& \ldots \& x_{i_s}, \tag{12.14}$$

kde znak $\oplus$ označuje súčet modulo 2 a suma sa berie cez všetky možné podmnožiny množiny $\{1, \ldots, n\}$ a koeficienty $a_{i_1,\ldots,i_s}$ nadobúdajú hodnotu z množiny $\{0, 1\}$.

Skôr, ako sa budeme zaoberať ANF Booleovských funkcií podrobnejšie, ilustrujeme na príklade, čo sa skrýva za trocha neprehľadným zápisom 12.14.

Príklad 12.15. *Zapíšeme všeobecný tvar algebraickej normálnej formy Booleovskej funkcie 3 premenných.*

$$\begin{aligned} &f(x_1, x_2, x_3) = \\ &\quad = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus a_{2,3}x_2x_3 \oplus a_{1,2,3}x_1x_2x_3. \end{aligned}$$

Všimnite si, že zložitý index $i_1, \ldots, i_s$ konštanty $a_{i_1,\ldots,i_s}$ nevyjadruje nič iné, len indexy premenných, ktoré vystupujú v príslušnej konjunkcii $a_{i_1,\ldots,i_s} x_{i_1} \& \ldots \& x_{i_s}$. Takéto označenie konštánt je dobré pri teoretickom skúmaní vlastností algebraických normálnych foriem. Pri konštrukcii ANF pre konkrétne Booleovské funkcie menšieho počtu premenných sa obvykle používa jednoduchšie označenie, napríklad ANF Booleovskej funkcie 3 premenných sa dá zapísať aj v tvare:

$$f(x, y, z) = a_0 \oplus a_1x \oplus a_2y \oplus a_3z \oplus a_4xy \oplus a_5xz \oplus a_6yz \oplus a_7xyz.$$

Zápis Booleovskej funkcie v ANF je vhodný na skúmanie viacerých vlastností Booleovských funkcií. My ho budeme používať pri zisťovaní linearity Booleovskej funkcie. Z úplnosti systému $\mathcal{D}_3$ vyplýva, že každú Booleovskú funkciu možno zapísať v ANF. Nasledujúca veta tvrdí, že tento zápis je jednoznačný.

Veta 12.5. *Pre ľubovoľnú Booleovskú funkciu $f \in \mathcal{P}_2$ existuje práve jedna formula v algebraickej normálnej forme, ktorá realizuje Booleovskú funckiu f.*

Dôkaz. V ANF n-árnej Booleovskej funkcie je 2^n binárnych koeficientov. Ak sa dohodneme na pevnom poradí členov v ANF, môžeme ANF Booleovskej funkcie jednoznačne zadať pomocou binárneho vektora dĺžky 2^n. ANF n-árnych Booloevských funkcií je práve toľko, koľko je n-árnych Booloevských funkcií. Z úplnosti systému $\mathcal{D}_3$ vyplýva, že každú Booleovskú funkciu možno zapísať v ANF. Predpokladajme, že tento zápis nie je jednoznačný, t.j. jednej Booleovskej funkcii by boli priradené dve rozličné formuly v ANF. Potom by

- existovala n-árna Booleovská funkcia, pre ktorú neexistuje formula v ANF. To je v spore s úplnosťou systému $\mathcal{D}_3$.
- alebo by jedna formula v ANF realizovala dve rozličné n-árne Booleovské funkcie, čo je v spore s jednoznačnosťou Booleovskej funkcie realizovanej formulou.

□

[18] a teda aj ľubovoľnú Booleovskú funkciu

Poznámka. Dokážeme jednoznačnosť priradenia ANF Boleovskej funkcii iným spôsobom. Nech sú Booleovskej funkcii $f(x_1,\dots,x_n)$ priradené dve rozličné formuly v ANF:

$$\begin{aligned} f(x_1,\dots,x_n) &= a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n \oplus a_{1,2}x_1x_2 \oplus \cdots \oplus a_{1,\dots,n}x_1\dots x_n \\ f(x_1,\dots,x_n) &= b_0 \oplus b_1x_1 \oplus \cdots \oplus b_nx_n \oplus b_{1,2}x_1x_2 \oplus \cdots \oplus b_{1,\dots,n}x_1\dots x_n. \end{aligned}$$

Sčítame modulo 2 pravé i ľavé strany posledných dvoch rovností. Dostávame

$$0 = c_0 \oplus c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c_{1,2}x_1x_2 \oplus \cdots \oplus c_{1,\dots,n}x_1\dots x_n, \tag{12.15}$$

kde

$$c_{i_1,\dots,i_s} = a_{i_1,\dots,i_s} \oplus b_{i_1,\dots,i_s}.$$

Zistíme, aké hodnoty nadobúdajú koeficienty c_i ANF konštantej funkcie 0.[19] Vo vzťahu 12.15 položíme $x_1 = x_2 = \cdots = x_n = 0$. Potom $c_0 = 0$ a

$$0 = c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c_{1,2}x_1x_2 \oplus \cdots \oplus c_{1,\dots,n}x_1\dots x_n, \tag{12.16}$$

Dosadíme $x_1 = 1$ a $x_2 = \cdots = x_n = 0$ do vzťahu 12.16. Dostávame $c_1 = 0$ a

$$0 = c_2x_2 \oplus \cdots \oplus c_nx_n \oplus c_{1,2}x_1x_2 \oplus \cdots \oplus c_{1,\dots,n}x_1\dots x_n,$$

Podobným spôsobom určíme hodnoty koeficientov $c_2 = \dots c_n = 0$ a pre ANF dostávame

$$0 = c_{1,2}x_1x_2 \oplus \cdots \oplus c_{n-1,n}x_{n-1}x_n \oplus c_{1,2,3}x_1x_2x_3 \oplus \cdots \oplus c_{1,\dots,n}x_1\dots x_n.$$

Dosadíme do posledného vzťahu: $x_1 = x_2 = 1; x_3 = \cdots = x_n = 0$ a dostávame $c_{1,2} = 0$. Takto postupne určíme hodnoty všetkých koeficientov:

$$c_0 = c_1 = \cdots = c_n = c_{1,2} = \cdots = c_{1,\dots,n} = 0.$$

To ale znamená, že

$$a_0 = b_0, a_1 = b_1, \dots, a_{1,\dots,n} = b_{1,\dots,n},$$

a obe ANF Booleovskej funkcie $f(x_1,\dots,x_n)$ sa zhodujú.

Príklad 12.16. *Zostrojíme ANF pre Booleovskú funkciu* $f(x_1,x_2,x_3) = 10110100$ *z príkladu . Všeobecný tvar ANF Booleovskej funkcie troch premenných je*

$$\begin{aligned} &f(x_1,x_2,x_3) = \\ &\quad = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus a_{2,3}x_2x_3 \oplus a_{1,2,3}x_1x_2x_3. \end{aligned}$$

Položíme $x_1 = x_2 = x_3 = 0$. *Všetky členy ANF, ktoré obsahovali aspoň jednu premennú, sa anulovali a ostal len absolútny člen,* a_0. *Keďže* $f(0,0,0) = 1$, $a_0 = 1$ *a*

$$\begin{aligned} &f(x_1,x_2,x_3) = \\ &\quad = 1 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus a_{2,3}x_2x_3 \oplus a_{1,2,3}x_1x_2x_3. \end{aligned}$$

[19] resp. funkcie $f(x_1,\dots,x_n) \oplus f(x_1,\dots,x_n)$

	x_1	x_2	x_3	$f(x_1,x_2,x_3)$		koeficient
0.	0	0	0	1	$a_0 = 1$	$a_0 = 1$
1.	1	0	0	0	$1 \oplus a_1 = 0$	$a_1 = 1$
2.	0	1	0	1	$1 \oplus a_2 = 1$	$a_2 = 0$
3.	0	0	1	0	$1 \oplus a_3 = 0$	$a_3 = 1$
4.	1	1	0	0	$1 \oplus 1 \oplus a_{1,2} = 0$	$a_{1,2} = 0$
5.	1	0	1	1	$1 \oplus 1 \oplus a_{1,3} = 1$	$a_{1,3} = 1$
6.	0	1	1	1	$1 \oplus 1 \oplus 1 \oplus a_{2,3} = 1$	$a_{2,3} = 0$
7.	1	1	1	0	$1 \oplus 1 \oplus 1 \oplus 1 \oplus a_{1,2,3} = 0$	$a_{1,2,3} = 0$

Tabuľka 12.23: Konštrukcia ANF

Teraz určíme koeficient a_1. *Dosadíme do posledného vzťahu* $x_1 = 1, x_2 = x_3 = 0$. *Dostávame rovnosť* $f(1,0,0) = 1 \oplus a_1$, *pretože vypadli všetky členy ANF, ktoré obsahovali premenné* x_2, x_3. *Z pravdivostnej tabuľky funkcie zistíme, že* $f(1,0,0) = 0$, *to znamená, že* $a_1 = 1$. *Odvodenie ďalších koeficientov ANF Booeleovskej funkcie uvádzame kvôli stručnosti a prehľadnosti v tabuľke 12.23. Výsledná ANF Booleovskej funkcie* $f(x_1,x_2,x_3)$ *má tvar:*

$$1 \oplus x_1 \oplus x_3 \oplus x_1x_3.$$

Úloha 12.10. *Zostrojte ANF pre funkcie* $f_0, \ldots, f_{15}$*!*

Úloha 12.11. *Zadajte pomocou tabuľky pravdivostných hodnôt 5 funkcií troch premenných a zostrojte pre ne ANF!*

ANF pre Booleovské funkcie môžeme konštruovať aj tak, že transformujeme niektorú vhodnú formulu realizujúcu danú Booleovskú funkciu na ANF. Napríklad

$$x_1 \vee x_2 \equiv \neg(\neg x_1)\&(\neg x_2)) \equiv [1 \oplus (1 \oplus x_1)(1 \oplus x_2)] \equiv [1 \oplus (1 \oplus x_1 \oplus x_2 \oplus x_1x_2)] \equiv x_1 \oplus x_2 \oplus x_1x_2.$$

Doterajšie poznatky o úplnosti systémov Booleovských funkcií stačia na to, aby sme pre systém, ktorý je úplný vedeli jeho úplnosť dokázať. Aby sme vedeli exaktne zdôvodniť, že nejaký systém Booleovských funkcií nie je úplný a povedať prečo, potrebujeme vytvoriť aparát, ktorý nám umožní efektívne popísať všetky funkcie, ktoré môžeme dostať skladaním funkcií zo skúmaného systému Booleovských funkcií. Zavedieme preto dva dôležité pojmy: *uzáveru množiny* a *uzavretej množiny Booleovských funkcií*.

Definícia 12.10. *Nech je* $\mathcal{M}$ *ľubovoľná množina Booleovských funkcií;* $\mathcal{M} \subseteq \mathcal{P}_2$. *Množinu všetkých Booleovských funkcií, ktoré možno realizovať pomocou formuly nad* $\mathcal{M}$ *nazveme uzáverom množiny* $\mathcal{M}$ *a označíme ju symbolom* $[\mathcal{M}]$. *Množinu Booleovských funkcií* $\mathcal{M}$ *budeme nazývať (funkcionálne) uzavretou, ak* $[\mathcal{M}] = \mathcal{M}$.

Základné vlastnosti uzáveru množiny funkcií popisuje nasledujúca veta.

Veta 12.6. *Nech sú* $\mathcal{M}, \mathcal{M}_1, \mathcal{M}_2$ *ľubovoľné množiny Booleovských funkcií, potom*

1. $\mathcal{M} \subseteq [\mathcal{M}]$,
2. $[[\mathcal{M}]] = [\mathcal{M}]$,

3. *ak* $\mathcal{M}_1 \subseteq \mathcal{M}_2$*, tak potom* $[\mathcal{M}_1] \subseteq [\mathcal{M}_2]$,
4. $[\mathcal{M}_1] \cup [\mathcal{M}_2] \subseteq [\mathcal{M}_1 \cup \mathcal{M}_2]$.

Dôkaz. Ponechávame čitateľovi ako cvičenie. □

Úloha 12.12. *Dokážte vetu 12.6!*

Úloha 12.13. *Nájdite príklady množín Booleovských funkcií, pre ktoré vo vzťahoch uvedených vo vete 12.6 rovnosť nastáva (nenastáva)!*

Príklad 12.17. *Uvedieme niekoľko príkladov množín funkcií, ktoré sú / nie sú funkcionálne uzavreté.*

1. $\mathcal{P}_2$ *je uzavretá trieda Booleovských funkcií, lebo skladaním Booleovských dostaneme opäť Booleovskú funkciu.*
2. $\{\neg x\}$ *nie je uzavretá trieda Booleovských funkcií, lebo* $\neg\neg x = x \in [\{\neg x\}]$,
3. $\{1, x \oplus y\}$ *nie je uzavretá trieda Booleovských funkcií, lebo* $1 \oplus 1 = 0 \notin \{1, x \oplus y\}$
4. *množina* $[\mathcal{M}]$ *je uzavretá pre ľubovoľnú množinu Booleovských funkcií* $\mathcal{M}$.

Úloha 12.14. *Vytvorte aspoň 10 rozličných uzavretých množín Booleovských funkcií!*

Pomocou pojmu uzáver môžeme jednoducho definovať úplnosť množiny Booleovských funkcií $\mathcal{M}$: množina $\mathcal{M}$ tvorí úplný systém práve vtedy, ak $[\mathcal{M}] = \mathcal{P}_2$.

Veta 12.4 obsahovala kritérium, na základe ktorého bolo možné rozhodnúť, či je nejaká množina Booleovských funkcií úplná. Ak však úplná množina $\mathcal{F}$ obsahuje viacero Booleovských funkcií, toto kritérium nemusí byť pre praktické účely vhodné. Naviac, ak sa nám nepodarí vyjadriť nejakú funkciu z $\mathcal{F}$ pomocou formuly nad $\mathcal{G}$, nevieme povedať, či je to naša neschopnosť, alebo sa daná funkcia objektívne nedá vyjadriť pomocou formuly nad $\mathcal{G}$. V nasledujúcej časti preto odvodíme jednoduchšie kritérium úplnosti, ktoré pre danú množinu Booleovských funkcií dá jednoznačnú odpoveď, resp. lepšie povedané, ak sa jedná o množinu konkrétnych Booleovských funkcií, spomínanú kritérium úplnosti dá odpoveď áno, množina je úplná alebo nie, daná množina Booleovských funkcií netvorí úplný systém. Množina Booleovských funkcií $\mathcal{M}$ však nemusí byť zadaná len vymenovaním všetkých svojich prvkov, ale možno ju vyjadriť pomocou množinových operácií nad množinami Booleovských funkcií, resp. špecifikovaním vlastností, ktoré by Booleovské funkcie z danej množiny mali mať. V tomto prípade nemusí byť informácia o prvkoch množiny $\mathcal{M}$ (Booleovských funkciách) dostatočná a odpoveď môže znieť: ak v množine $\mathcal{M}$ existujú funkcie s takýmito vlastnosťami, tak potom (nie) je úplná.

12.6 Predúplné triedy. Veta o úplnosti

Pri zisťovaní úplnosti množiny Booleovských funkcií sa využíva 5 zvláštnych uzavretých množín Booleovských funkcií. Teraz tieto množiny charakterizujeme a potom vyslovíme a dokážeme vetu o úplnosti.

12.6.1 Triedy T_0 a T_1

Definícia 12.11. *Trieda*[20] *Booleovských funkcií*

$$T_0^n = \{f(x_1, \ldots, x_n) \in \mathcal{P}_2; f(0, \ldots, 0) = 0\}$$

sa nazýva triedou (n*-árnych) Booleovských funkcií zachovávajúcich* 0*. Trieda* n*-árnych Booleovských funkcií*

$$T_1^n = \{f(x_1, \ldots, x_n) \in \mathcal{P}_2; f(1, \ldots, 1) = 1\}$$

sa nazýva triedou (n*-árnych) Booleovských funkcií zachovávajúcich* 1*. Triedy Booleovských funkcií zachovávajúcich* 0*, resp.* 1 *potom definujeme nasledovne:*

$$T_0 = \bigcup_n T_0^n, \qquad T_1 = \bigcup_n T_1^n.$$

Tabuľka hodnôt n-árnej Booleovskej funkcie patriacej do triedy T_0 sa vyznačuje tým, že v prvom riadku má hodnotu 0, zatiaľ čo v ostatných $2^n - 1$ riadkoch môže nadobúdať ľubovoľné hodnoty. Z toho výplýva, že, že trieda T_0 obsahuje 2^{2^n-1} n-árnych Booleovských funkcií. Podobne, n-árne Booleovské funkcie z triedy T_1 majú v poslednom riadku svojej pravdivostnej tabuľky hodnotu 1 a v ostatných $2^n - 1$ riadkoch možu nadobúdať ľubovoľné hodnoty. Potom zrejme T_1 obsahuje rovnako ako trieda T_0 2^{2^n-1} n-árnych Booleovských funkcií. Ukážeme, že trieda T_0 je uzavretá. Nech $f, g_1, \ldots, g_n \in T_0$ (bez ujmy na všeobecnosti môžeme predpokladať, že funkcie $f, g_1, \ldots, g_n$ sú n-árne a závisia od premenných $(x_1, \ldots, x_n)$. Nech je $F(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_1n(x_1, \ldots, x_n))$ zložená Booleovská funkcia. Potom

$$F(0, \ldots, 0) = f(g_1(0, \ldots, 0), \ldots, g_n(0, \ldots, 0)) = f(0, \ldots, 0) = 0,$$

a Booleovská funkcia $F(x_1, \ldots, x_n)$ patrí do T_0. To znamená, že trieda T_0 je uzavretá vzhľadom operáciu skladania Booleovských funkcií. Podobne by sme dokázali aj uvavretosť triedy T_1. Z elementárnych Booleovských funkcií patrí do triedy T_0 napríklad konjunkcia, disjunkcia, identická funkcia, súčet modulo 2; do triedy T_1 patrí konjunkcia, disjunkcia, indentická funkcia, ekvivalencia, implikácia. Negácia nepatrí ani do T_0 ani do T_1, implikácia nepatrí do T_0.

12.6.2 Trieda lineárnych funkcií, L

Definícia 12.12. *Booleovská funkcia* $f(x_1, \ldots, x_n)$ *sa nazýva* n*-árnou lineárnou Booleovskou funkciou, ak jej algebraická normálna forma obsahuje len lineárne členy; t.j.*

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$$

Triedou L^n *nazveme množinu všetkých* n*-árnych lineárnych Booleovských funkcií. Triedu* L *lineárnych Booleovských funkcií definujeme ako*

$$L = \bigcup_n L^n.$$

[20] v teórii Booleovských funkcií na označenie množiny funkcií často používa pojem trieda alebo systém Booleovských funkcií. Tejto konvencie sa budeme pridŕžať aj my.

Poznámka. Pri štúdiu kryptografických vlastností Booleovských funkcií sa Booleovské funkcie z triedy L nazývajú afinnými Booleovskými funkciami a pojem lineárna Booleovská funkcia sa rezervuje pre takú Booleovskú funkciu, ktorej AFN má tvar $f(x_1,\ldots,x_n) = a_1x_1 \oplus \cdots \oplus a_nx_n$; t.j. koeficient a_0 v ANF je nulový. My sa budeme pridržiavať štandardného označenia.

Keďže ANF lineárnej Booleovskej funkcie má $n+1$ koeficientov, $|L^n| = 2^{n+1}$. Ukážeme ešte, že tieda lineárnych funkcií je uzavretá. Nech sú $f, g_1, \ldots, g_n \in L$ n-árne Booleovské funkcie;

$$\begin{aligned} f(y_1,\ldots,y_n) &= a_0 \oplus a_1y_1 \oplus \cdots \oplus a_ny_n, \\ g_1(x_1,\ldots,x_n) &= b_{1,0} \oplus b_{1,1}x_1 \cdots \oplus b_{1,n}x_n, \\ g_2(x_1,\ldots,x_n) &= b_{2,0} \oplus b_{2,1}x_1 \cdots \oplus b_{2,n}x_n, \\ &\ldots \\ g_n(x_1,\ldots,x_n) &= b_{n,0} \oplus b_{n,1}x_1 \cdots \oplus b_{n,n}x_n. \end{aligned}$$

Potom

$$\begin{aligned} &F(x_1,\ldots,x_n) = f(g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)) = \\ &= a_0 \oplus a_1(b_{1,0} \oplus b_{1,1}x_1 \cdots \oplus b_{1,n}x_n) \oplus \cdots \oplus a_n(b_{n,0} \oplus b_{n,1}x_1 \cdots \oplus b_{n,n}x_n) = \\ &= (a_0 \oplus a_1b_{1,0} \oplus \cdots \oplus a_nb_{n,0}) \oplus x_1(a_1b_{1,1} \oplus a_2b_{2,1} \oplus \cdots \oplus a_nb_{n,1}) \oplus \\ &\oplus\ x_2(a_1b_{1,2} \oplus a_2b_{2,2} \oplus \cdots \oplus a_nb_{n,2}) \oplus \cdots \oplus x_n(a_1b_{1,n} \oplus a_2b_{2,n} \oplus \cdots \oplus a_nb_{n,n}) = \\ &= c_0 \oplus c_1x_1 \oplus \cdots \oplus c_nx_n. \end{aligned}$$

To znamená, že zložená funkcia F je lineárna, resp. trieda L je uzavretá vzhľadom na operáciu skladania Booleovských funkcií.

Úloha 12.15. *Dokážte uzavretosť tried* T_0, T_1, L *bez predpokladov, že*

- *všetky čiastkové funkcie sú* n*-árne,*
- *čiastkové funkcie závisia od tých istých premenných.*

12.6.3 Trieda monotónnych funkcií, M

V matematickej analýze sme sa stretli s pojmami monotónne rastúcej reálnej funkcie; $f(x)$ bola monotónne rastúca, ak platilo $\forall x_0, x_1 \in \mathbb{R}[(x_0 < x_1) \Rightarrow (f(x_0) < f(x_1))]$. Zavedenie monotónnosti pre Booleovské funkcie naráža na problém—ako porovnávať binárne vektory? Ani lexikografické usporiadanie, ani usporiadanie založení na tom, že binárne vektory reprezentujú prirodzené čísla nebolo použiteľné. Preto na množine binárnych vektorov dĺžky n najprv definujeme reláciu čiastočného usporiadania a potom pomocou neho zavedieme pojem monotónnej Booleovskej funkcie.

Definícia 12.13. *Nech* $\alpha, \beta \in \{0,1\}^n$*;* $\alpha = (a_1, \ldots, a_n), \beta = (b_1, \ldots, b_n)$*. Budeme hovoriť, že vektor* α *predchádza vektor* β *práve vtedy, ak* $a_i \leq b_i \quad i = 1 \ldots, n$*. Tto skutočnosť budeme symbolicky zapisovať nasledovne:* $\alpha \preceq \beta$

Príklad 12.18. *Vektor* $(0,0,1)$ *predchádza vektor* $0,1,1$*. Medzi vektormi* $(0,1)$ *a* $(1,0)$ *neexistuje vzťah predchádzania, pretože* $a_1 < b_1$ *a* $a_2 > b_2$*. Takéto vektory sa nazývajú neporovnateľné. Keďže relácia* $\preceq$ *je definovaná na vektoroch rovnakej dĺžky, nedá sa aplikovať na vektory rozličnej dĺžky: napr.* $(0,0,1)$ *a* $(0,0)$*.*

Úloha 12.16. *Ilustrujte reláciu* $\preceq$ *na množine* $\{0,1\}^3$ *pomocou orientovaného grafu rádu 8. (Návod: vrcholu* v_i *priradíte vektor* $\sigma(3,i),\ i = 0, \ldots, 7$*. Ak* $\sigma(3,i) \preceq \sigma(3,j)$*, vrcholy* v_i, v_j *spojte orientovanou hranou* (v_i, v_j)*!)*

Teraz zavedieme pojem *monotónnej Booleovskej funkcie*.

Definícia 12.14. *(*n*-árna)Booleovská funkcia* $f(x_1, \ldots, x_n)$ *sa nazýva monotónna, ak pre ľubovoľné dva vektory* $\alpha = (a_1, \ldots, a_n), \beta = (b_1, \ldots, b_n)$ *také, že* $\alpha \preceq \beta$ *platí* $f(a_1, \ldots, a_n) \leq f(b_1, \ldots, b_n)$*. Triedu všetkých* n*-árnych monotónnych Booleovských funkcií budeme označovať symbolom* M^n *a triedu všetkých monotónnych Booleovských funkcií budeme označovať symbolom* M*.*

Monotónnosť Booleovskej funkcie sa neprejavuje tak jednoducho v tabuľke pravdivostných hodnôt (ako v prípade funkcií zachovávajúcich hodnotu 0 alebo 1) ani v tvare ANF Booleovskej funkcie (ako v prípade afinných/lineárnych Booleovských funkcií.) Preto sa zatiaľ nepodarilo nájsť presné vyjadrenie pre mohutnosť M^n Pre veľké n platí tento asymptotický odhad: **??**

$$|M^n| \sim 2^{\binom{n}{n/2}} \exp\left[\binom{n}{(n/2)-1} \cdot \left(\frac{1}{2^{n/2}} + \frac{n^2}{2^{n+5}} + \frac{n}{2^{n+4}}\right)\right] \quad n \text{ je párne,}$$

resp. pre nepárne n

$$|M^n| \sim 2 \cdot 2^{\binom{n}{(n-1)/2}} \times$$
$$\times \quad \exp\left[\binom{n}{(n-3)/2} \cdot \left(\frac{1}{2^{(n+3)/2}} - \frac{n^2}{2^{n+6}} - \frac{n}{2^{n+3}}\right) + \binom{n}{(n-1)/2} \cdot \left(\frac{1}{2^{(n+1)/2}} + \frac{n^2}{2^{n+4}}\right)\right]$$

Zápis $a_n \sim b_n$ vyjadruje skutočnosť, že $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$ a číta sa „a_n je asymptoticky rovné b_n.“

Dokážeme uzavretosť triedy M. Nech $f(y_1, \ldots, y_m), g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n) \in M$. Potom zložená funkcia

$$F(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

je monotónnou funkciou. Skutočne, nech sú $\alpha =, \beta = (b_1, \ldots, b_n)$ ľubovoľné dva binárne vektory také, že $\alpha \preceq \beta$. Keďže $g_1, \ldots d_m$ sú monotónne funkcie, platí pre ne

$$\begin{aligned} c_1 = g_1(a_1, \ldots, a_n) &\leq g_1(b_1, \ldots, b_n) = d_1 \\ c_2 = g_2(a_1, \ldots, a_n) &\leq g_2(b_1, \ldots, b_n) = d_2 \\ &\ldots \\ c_m = g_m(a_1, \ldots, a_n) &\leq g_m(b_1, \ldots, b_n) = d_m \end{aligned}$$

To však znamená, že $(c_1, \ldots, c_m) \preceq (d_1, \ldots, d_m)$. Ale aj funkcia $f(y_1, \ldots, y_m)$ je monotónna, a teda

$$f(c_1, \ldots, c_m) \leq f(d_1, \ldots, d_m).$$

Pre zloženú funkciu F postupne dostávame:

$$F(a_1, \ldots, a_n) = f(g_1(a_1, \ldots, a_n), \ldots, g_m(a_1, \ldots, a_n) =$$
$$= f(c_1, \ldots, c_m) \leq f(d_1, \ldots, d_m) = f(g_1(b_1, \ldots, b_n), \ldots, g_m(b_1, \ldots, b_n)) = F(b_1, \ldots, b_n).$$

Príklad 12.19. *Konjunkcia, disjunkcia, obidve konštanty a identická funkcia sú monotónne funkcie, negácia, implikácia, ekvivalencia, súčet modulo 2 nie sú monotónne funkcie.*

12.6.4 Trieda samoduálnych funkcií S

Samoduálna funkcia sa vyznačuje takou veľkou symetriou svojej tabuľky pravdivostných hodnôt, že na úplné zadanie samoduálnej Booleovskej funkcie stačí polovica jej tabuľky pravdivostných hodnôt. Na druhej strane, samoduálnosť je menej názorná ako ostatné vlastnosti Booleovských funkcií. Začneme preto jednoduchším pojmom duálnosti Booleovských funkcií.

Definícia 12.15. *Booleovská funkcia* $f(x_1, \ldots, x_n)$ *sa nazýva duálnou funkciou k Booleovskej funkcii* $g(x_1, \ldots, x_n)$*, ak*

$$f(x_1, \ldots, x_n) = \overline{g}(\overline{x}_1, \ldots, \overline{x}_n).$$

Ilustrujeme si pojem duálnosti funkcií na príkladoch.

Príklad 12.20. *1. Funkcia* $f_1(x, y)$ *(konjunkcia) je duálna ku funkcii* $f_7(x, y)$ *(disjunkcii):*

$$\overline{\overline{x} \& \overline{y}} = (x \vee y)$$

a opačne disjunkcia je duálnou funkciou konjunkcie, lebo

$$\overline{\overline{x} \vee \overline{y}} = (x \& y)$$

2. funkcia $f_{12}(x, y)$ *(negácia) je duálna k sebe samej, lebo* $\neg\neg(\neg x) = \neg x$ *a funkcia* $f_3(x, y)$ *(identita) je duálna k sebe samej, lebo* $\neg(\neg x) = x$.

Zavedieme pojem samoduálnej funkcie:

Definícia 12.16. *Booleovská funkcia* $f(x_1, \ldots, x_n)$ *sa nazýva samoduálnou funkciou, ak*

$$f(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n);$$

t.j. ak je duálna k sebe samej.

Trieda samoduálnych funkcií je neprázdna, pretože podľa predchádzajúceho príkladu medzi samoduálne funkcie patria napríklad identická funkcia x a negácia $\neg x$. Tabuľka pravdivostných hodnôt samoduálnej funkcie sa vyznačuje tým, že v riadkoch prislúchajúcich opačným vektorom vstupných hodnôt sú opačné hodnoty. Názorne si to ukážeme na nasledujúcom príklade.

x_1	x_2	x_3	$\overline{x}_1$	$\overline{x}_2$	$\overline{x}_3$	$f(x_1,x_2,x_3)$	$\overline{f}(\overline{x}_1,\overline{x}_2,\overline{x}_3)$
0	0	0	1	1	1	1	0
0	0	1	1	1	0	0	1
0	1	0	1	0	1	0	1
0	1	1	1	0	0	1	0

Tabuľka 12.24: Tabuľka samoduálnej funkcie

Príklad 12.21. *Definujme samoduálnu funkciu* $fx_1,x_2,x_3)$ *troch premenných. Aby sme dosiahli samoduálnosť funkcie* f *musíme zaistiť komplementárnosť hodnôt na opačných vektoroch. V tabuľke 12.24 sú kvôli názornosti uvedené opačné vektory v susedných stĺpcoch.*

Nech napríklad $f(0,0,0)=1$. *Potom* $f(1,1,1)=1$ *a* $\neg f(1,1,1)=0$. *Zvolíme hodnoty funkcie* $fx_1,x_2,x_3)$ *na prvých 4 vektoroch, napríklad* $f(0,0,0)=1, f(0,0,1)=0, f(0,1,0)=0, f(0,1,1)=1$ *Tým sú jednoznačne definované hodnoty funkcie* $fx_1,x_2,x_3)$ *aj na opačných vektoroch—pozri tabuľku 12.24.*

Ako sme videli v predchádzajúcom príklade, na jednoznačné určenie samoduálnej Booleovskej funkcie stačí určiť jej hodnotu na jednom z každej dvojice opačných vektorov. To znamená, že n-árna samoduálna Booleovská funkcia je zadaná napr. prvou polovicou tabuľky, resp. binárným vektorom dĺžky 2^{n-1}. Z uvedeného faktu potom vyplýva, že n-árnych samoduálnych Booleovských funkcií je $2^{2^{n-1}}=\sqrt{2^{2^n}}$. Ukážeme, že aj trieda S samoduálnych funkcií je uzavretá na skladanie Booleovských funkcií. Nech sú $f(y_1,\ldots,y_m), g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n)\in S$. Potom zložená funkcia

$$F(x_1,\ldots,x_n)=f(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n))$$

je samoduálnou funkciou. Negujeme najprv premenné zloženej funkcie F:

$$F(\overline{x}_1,\ldots,\overline{x}_n)=f(g_1(\overline{x}_1,\ldots,\overline{x}_n),\ldots,g_m(\overline{x}_1,\ldots,\overline{x}_n))$$

Keďže funkcie $g_1,\ldots,g_m$ sú samoduálne, platí pre ne

$$g_i(\overline{x}_1,\ldots,\overline{x}_n)=\overline{g}_i(x_1,\ldots,x_n).$$

Vonkajšia čiastková funkcia zloženej funkcie F, funkcia f je tiež samoduálna, preto

$$f(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n))=\overline{f}(\overline{g}_1(x_1,\ldots,x_n),\ldots,\overline{g}_m(x_1,\ldots,x_n)),$$

resp.

$$f(\overline{g}_1,\ldots,\overline{g}_m)=\overline{f}(g_1,\ldots,g_m).$$

Z vyššie uvedených vzťahov vyplýva, že

$$F(\overline{x}_1,\ldots,\overline{x}_n)=\overline{f}(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n))=\overline{F}(x_1,\ldots,x_n),$$

a teda trieda samoduálnych Booleovských funkcií je uzavretá.

Teraz môžeme sformulovať kritérium úplnosti systému Booleovských funkcií.

Veta 12.7. *(O funkcionálnej úplnosti) Množina Booleovských funkcií* D *tvorí úplný systém Booleovských funkcií práve vtedy, ak nie je podmnožinou žiadnej z tried* T_0, T_1, L, S, M.

Dôkaz. Nutnosť. Triedy T_0, T_1, L, S, M sú uzavreté a žiadna z nich nie je úplná (pre každú z nich vieme nájsť Booleovskú funkciu, ktorú neobsahuje). Ak by D bola úplná a zároveň bola podmnožinou niektorej z tried T_0, T_1, L, S, M, napríklad $D \subseteq M$, potom by podľa tvrdenia 3 vety 12.6 muselo platiť

$$D \subseteq M \Rightarrow [M] = M \supseteq [D] = \mathcal{P}_2.$$

Spor.

Ukážeme, že podmienka je aj postačujúca; t.j. ak D nie je podmnožinou žiadnej z tried T_0, T_1, L, S, M, tak dokážeme vytvoriť formuly nad D realizujúce funkcie $\neg x, x\&y$, ktoré tvoria úplný systém Booleovských funkcií.

Keďže D nie je podmnožinou žiadnej z tried T_0, T_1, L, S, M, môžeme predpokladať, že obsahuje funkcie $f_0 \notin T_0, f_1 \notin T_1, f_S \notin S, f_M \notin M$. Funkcie f_0, f_1, f_M, f_L, f_S nemusia byť nutne rôzne a f_0, f_1 sa nezhodujú s funkciami f_0, f_1 z tabuľky 12.1. Bez ujmy na všeobecnosti môžeme predpokladať, že všetky uvedené funkcie sú n-árne.

1. Najprv zoberieme funkciu f_0. Keďže $f_0 \notin T_0$, $f_0(0, \ldots, 0) = 1$. Stotožníme všetky premenné funkcie f_0 a vytvoríme novú funkciu jednej premennej: $\phi(x) = f_0(x, \ldots, x)$. Je zrejmé, že $\phi(0) = 1$. Pozrieme sa na opačný koniec tabuľky pravdivostných hodnôt Booleovskej funkcie f_0, aby sme zistili, akú hodnotu nadobúda funkcia $\phi(x)$ pre $x = 1$. Sú dve možnosti:

   (a) $f_0(1, \ldots, 1) = 1$. V tomto prípade funkcia $\phi(x) \equiv 1$ nemá podstatné premenné a predstavuje konštantu 1.

   (b) V druhom prípade $f_0(1, \ldots, 1) = 0$, a teda $\phi(1) = 0$, resp. $\phi(x) = \neg x$.

2. Teraz využijeme funkciu $f_1 \notin T_1$. Tak ako v predchádzajúcom prípade stotožníme všetky premenné funkcie f_1 a vytvoríme novú funkciu jednej premennej: $\psi(x) = f_1(x, \ldots, x)$. Platí $\psi(1) = f_1(1, \ldots, 1) = 0$. Zaujma nás hodnota $\psi(0) = f_1(0, \ldots, 0)$. Podobne ako v prípade funkcie $\phi(x)$, môžu aj tu nastať dve možnosti

   (a) $\psi(0) = f_1(0, \ldots, 0) = 0$. V tomto prípade $\psi(x) \equiv 0$ predstavuje konštantu 0.

   (b) Ak $\psi(0) = f_1(0, \ldots, 0) = 1$, $\psi(x) = \neg x$.

   V optimálnom prípade sme z funkcií f_0, f_1 vytvorili obe konštanty a negáciu, v horšom prípade buď obe konštanty alebo samotnú negáciu (Obr.12.16). Ukážeme, že v prípade, keď sme skonštruovali „len“ obe konštanty, vytvoríme pomocou nemonotónnej funkcie negáciu.

3. Keďže $f_M \notin M$, existujú také dva vektory hodnôt $\alpha = (a_1, \ldots, a_n), \beta = (b_1, \ldots, b_n)$ také, že $\alpha \preceq \beta$ a

   $$f(a_1, \ldots, a_n) = 1, \quad f(b_1, \ldots, b_n) = 0.$$

   Keďže $\alpha \preceq \beta$, potom existujú také hodnoty $i_1, \ldots, i_k$, že $a_{i_j} = 0, b_{i_j} = 1, \quad j = 1, \ldots, k$ a $a_i = b_i$ pre $i \notin \{i_1, \ldots, i_k\}$. Bez ujmy na všeobecnosti môžeme predpokladať, že sa vektory α, β odlišujú na prvých k miestach a na zostávajúcich $n - k$ miestach majú rovnaké hodnoty, t.j.:

   $$\alpha = (0, \ldots, 0, a_{k+1}, \ldots, a_n), \qquad \beta = (1, \ldots, 1, a_{k+1}, \ldots, a_n).$$

Definujeme teraz funkciu $\vartheta(x) = f_M(x, \ldots, x, a_{k+1}, \ldots, a_n)$. Pre funkciu $\vartheta(x)$ platí

$$\begin{aligned} \vartheta(0) &= f_M(0, \ldots, 0, a_{k+1}, \ldots, a_n) = 1 \\ \vartheta(1) &= f_M(1, \ldots, 1, a_{k+1}, \ldots, a_n) = 0. \end{aligned}$$

Potrebné konštanty sme vytvorili z funkcií f_0, f_1. Funkcia jednej premennej $\vartheta(x)$ predstavuje negáciu.

Ak sa nám z funkcií f_0, f_1 podarilo vytvoriť len negáciu, obe konštanty získame pomocou negácie a funkcie f_S, ktorá nie je samoduálna.

4. Keďže $f_S \notin S$, existujú také dva navzájom opačné vektory hodnôt $\alpha = (a_1, \ldots, a_n)$ $\overline{\alpha} = (\overline{a}_1, \ldots, \overline{a}_n)$, na ktorých funkcia f_S nadobúda rovnakú hodnotu;

$$f_S(a_1, \ldots, a_n) = f_S(\overline{a}_1, \ldots, \overline{a}_n).$$

(Pripomenieme význam označenia x^σ, ktoré sme zaviedli na začiatku tejto kapitoly: $x^\sigma = \overline{x}$ ak $\sigma = 0$ a $x^\sigma = x$ ak $\sigma = 1$.) Podobne ako v predchádzajúcich prípadoch využijeme funkciu f_S na vytvorenie Booleovskej funkcie jednej premennej. Položíme

$$\omega(x) = f_S(x^{a_1}, \ldots, x^{a_n}).$$

Takúto funkciu dokážeme zostrojiť pomocou negáciu, ktorú sme už vytvorili. Z definície výrazu x^σ vyplýva, že $1^\sigma = \sigma$ a $0^\sigma = \neg\sigma$. Pomocou týchto vzťahov vyjadríme hodnoty funkcie $\omega(x)$ (jednej premennej):

$$\omega(1) = f_S(1^{a_1}, \ldots, 1^{a_n}) = f_S(a_1, \ldots, a_n) = f_S(\overline{a}_1, \ldots, \overline{a}_n) = f_S(0^{a_1}, \ldots, 0^{a_n}) = \omega(0).$$

Funkcia $\omega(x)$ teda predstavuje konštantu. Z funkcie $\omega(x)$ nedokážeme síce zostrojiť predpísanú konštantu, ale to nepredstavuje žiaden problém, pretože druhú konštantu poľahky vytvoríme pomocou negácie a funkcie $\omega(x)$.

5. Výsledkom našich doterajších snažení sú funkcie $0, 1, \neg x$. Z tchto troch funkcií a nelineárnej funkcie $f_L \notin L$ vytvoríme konjunkciu. Z toho, že funkcia f_L nie je lineárna, vyplýva že v jej ANF sa vyskytuje konjunkcia aspoň dvoch premenných. Bez ujmy na všeobecnosti môžeme predpokladať, že ide o premenné x_1, x_2. Využijeme komutatívnosť a asociatívnosť sčítania modulo 2, distributívny zákon pre konjunkciu a súčet modulo 2 a upravíme ANF Booleovskej funkcie f_L na nasledujúci tvar:

$$\begin{aligned} f_L(x_1, \ldots, x_n) &= x_1x_2 \& f_{(1,2)}(x_3, \ldots, x_n) \oplus x_1 \& f_{(1)}(x_3, \ldots, x_n) \oplus \\ &\oplus \quad x_2 \& f_{(2)}(x_3, \ldots, x_n) \oplus f_{(\emptyset)}(x_3, \ldots, x_n). \end{aligned} \tag{12.17}$$

Preusporiadali sme všetky členy ANF Boleovskej funkcie $f_L(x_1, \ldots, x_n)$ a rozdelili ich do 4 skupín (zátvoriek) tak, že prvá skupina pozostáva zo všetkých tých členov ANF, ktoré obsahujú konjunkciu x_1x_2, druhú tvoria tie členy ANF, ktoré obsahujú premennú x_1 ale nie x_2, tretiu—tie členy ANF, ktoré obsahujú premennú x_2 ale nie x_1 a napokon, do poslednej sme zaradili tie členy ANF, ktoré neobsahujú ani x_1, ani x_2. Zo všetkých členov prvej skupiny sme na základe distributívneho zákona vyňali pred zátvorku konjunkciu x_1x_2 a výraz v zátvorke vyjadrili pomocou Booleovskej funkcie $f_{(1,2)}(x_3, \ldots, x_n)$. Rovanako sme upravili ostatné tri skupiny členov ANF.

Všimnite si, že po vyňatí x_1x_2, x_1, x_2 z prvej, druhej, resp. tretej skupiny členov pred zátvorku, zostávajúce výrazy v zátvorkách už neobsahovali premenné x_1, x_2. Posledná, štvrtá skupina pozostávala z členov ANF, ktoré nezáviseli od x_1, x_2. To znamená, že výrazy v zátvorkách predstavujú funkcie premenných $x_3, \ldots, x_n$.

Nakoľko ANF Booleovskej funkcie f_L obsahuje konjunkciu x_1x_2, musí existovať aspoň jeden taký súbor hodnôt $(a_3, \ldots, a_n)$ premenných $x_3, \ldots, x_n$, že $f_{(1,2)}(a_3, \ldots, a_n) = 1$. Vytvoríme novú Booleovskú funkciu dvoch premenných $\Phi(x_1, x_2)$ dosadením konštánt $(a_3, \ldots, a_n)$ do funkcie f_L:

$$\Phi(x_1, x_2) = f_L(x_1, x_2, a_3, \ldots, a_n).$$

Zo zápisu funkcie f_L 12.17 vyplýva, že

$$\begin{aligned} \Phi(x_1, x_2) &= x_1x_2 \& f_{(1,2)}(a_3, \ldots, a_n) \oplus x_1 \& f_{(1)}(a_3, \ldots, a_n) \oplus x_2 \& f_{(2)}(a_3, \ldots, a_n) \oplus \\ &\oplus f_{(\emptyset)}(a_3, \ldots, a_n) = d_0x_1x_2 \oplus d_1x_1 \oplus d_2x_2 \oplus d_3. \end{aligned} \tag{12.18}$$

Koeficienty d_0, d_1, d_2, d_3 sú kontanty—hodnoty funkcií $f_{(1,2)}, f_{(1)}, f_{(2)}, f_{(\emptyset)}$ na vektore $(a_3, \ldots, a_n)$. Je zrejmé, že $d_0 = 1$. Ak by boli ostatné koeficienty d_1, d_2, d_3 nulové, funkcia $\Phi(x_1, x_2)$ by už predstavovala potrebnú konjunkciu. Ale konjunkciu z $\Phi(x_1, x_2)$ ľahko vytvoríme aj v prípade, keď je aspoň jeden z koeficientov d_1, d_2, d_3 nenulový. Na základe hodnôt d_1, d_2 transformujeme premenné funkcie $\Phi(x_1, x_2)$ a výslednú funkciu ešte v prípade potreby negujeme. Dostávame opäť funkciu dvoch premenných $\Theta(x_1, x_2)$:

$$\Theta(x_1, x_2) = \Phi(x_1 \oplus d_2, x_2 \oplus d_1) \oplus d_1d_2 \oplus d_3. \tag{12.19}$$

Pripomíname, že $x \oplus 1 = \neg x$ a $x \oplus 0 = x$. Dokážeme, že $\Theta(x_1, x_2) = x_1 \& x_2$. Vyjadríme $\Theta(x_1, x_2)$ pomocou vzťahov 12.18 a 12.19.

$$\begin{aligned} \Theta(x_1, x_2) &= (x_1 \oplus d_2)(x_2 \oplus d_1) \oplus d_1(x_1 \oplus d_2) \oplus d_2(x_2 \oplus d_1) \oplus d_3 \oplus d_1d_2 \oplus d_3 = \\ &= x_1x_2 \oplus x_1d_1 \oplus x_2d_2 \oplus d_1d_2 \oplus x_1d_1 \oplus d_1d_2 \oplus x_2d_2 \oplus d_1d_2 \oplus d_3 \oplus d_1d_2 \oplus d_3 = \\ &= x_1 \& x_2. \end{aligned}$$

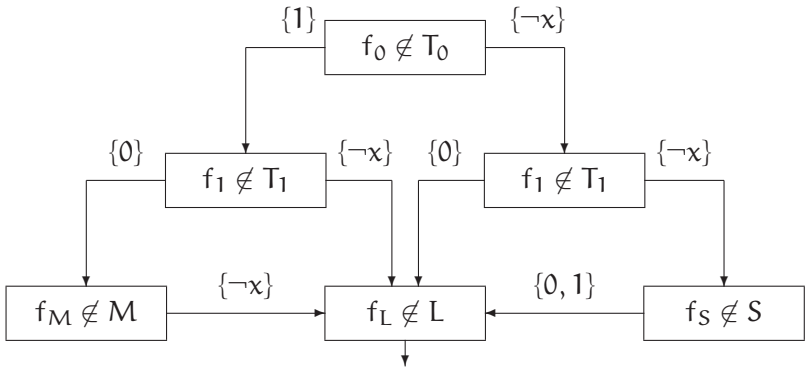
Všetky úpravy funkcie f_L, ktoré sme robili, sa dali realizovať pomocou dosadzovania konštánt a negácie premenných, resp. negácie funkcie. To znamená, že pomocou konštánt $0, 1$, negácie $\neg x$ a nelineárnej funkcie možno vytvoriť konjunkciu.

Pomocou pätice funkcií f_0, f_1, f_M, f_L, f_S sme vytvorili funkcie $\neg x, x_1 \& x_2$, ktoré tvoria úplný systém Booleovských funkcií. To znamená, že tak funkcie f_0, f_1, f_M, f_L, f_S, ako aj trieda/množina D tvoria úplný systém Booleovských funkcií. Prehľadná schéma dôkazu tejto vety je zobrazená na obrázku 12.16. □

Príklad 12.22. *Dôkaz vety 12.7 je pomerne dlhý a zložitý. Kvôli lepšiemu pochopeniu ho teraz ilustrujeme na dvoch konkrétnych príkladoch.*

1. *Ukážeme najprv, že množina Booleovských funkcií $\{x \Rightarrow y, 0\}$ tvorí úplný systém.*

   (a) *Funkcia $x \Rightarrow y$ nepatrí do triedy T_0, lebo $0 \Rightarrow 0 = 1$. Keďže $1 \Rightarrow 1 = 1$, funkcia $x \Rightarrow x$ predstavuje konštantu 1,*



Obrázok 12.16: Schéma dôkazu vety 12.7

(b) Funkcia 0 *nepatrí do triedy* T_1.

(c) Implikácia nie je monotónnou funkciou, lebo $0 \Rightarrow 0 = 1$, *ale* $1 \Rightarrow 0 = 0$. *Skonštruujeme pomocou nej a konštanty* 0 *negáciu:* $x \Rightarrow 0 \equiv \neg x$.

(d) Funkcia $x \Rightarrow y$ *nie je lineárna. Zostrojíme jej ANF a z nej vytvoríme konjunkciu. Všeobecný tvar ANF Booleovskej funkcie dvoch premenných je:*

$$f(x, y) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 xy.$$

Určíme hodnoty jednotlivých koefcientov funkcie $f(x, y) = x \Rightarrow y$. *Jednotlivé kroky odvodenia sú uvedené v nasledujúcej tabuľke*

hodnota	*rovnica*	*koeficient*
$f(0,0) = 1$	$a_0 = 1$	$a_0 = 1$
$f(1,0) = 0$	$1 \oplus a_0 = 0$	$a_1 = 1$
$f(0,1) = 1$	$1 \oplus a_2 = 1$	$a_2 = 0$
$f(1,1) = 1$	$1 \oplus 1 \oplus a_3 = 1$	$a_3 = 1$

ANF implikácie $x \Rightarrow y$ *má teda tvar:*

$$x \Rightarrow y = 1 \oplus x \oplus xy \qquad (= \Phi(x, y)).$$

Zostrojili sme funkciu $\Phi(x, y)$, *v ktorej koeficienty* d_i *nadobúdajú nasledujúce hodnoty:* $d_0 = d_1 = d_3 = 1$ *a* $d_2 = 0$. *Vytvoríme funkciu* $\Theta(x, y)$*:*

$$\Theta(x, y) = \Phi(x, y \oplus 1) \oplus 1 = \neg\Phi(x, \neg y) = [(x \Rightarrow (y \Rightarrow 0)) \Rightarrow 0].$$

2. Ukážeme, ako sa upravuje zložitejšia ANF.

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= 1 \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4 = \\ &= x_1x_2(1 \oplus x_3 \oplus x_3x_4) \oplus x_1(1 \oplus x_3x_4) \oplus x_2(x_1 \oplus x_3) \oplus (1 \oplus x_3x_4). \\ f(x_1, x_2, 0, 1) &= \Phi(x_1, x_2) = x_1x_2 \oplus x_1 \oplus x_2 \oplus 1, \\ f(\overline{x}_1, \overline{x}_2, 0, 1) &= \Theta(x_1, x_2) = x_1x_2. \end{aligned}$$

funkcia	T_0	T_1	L	S	M
0	+	−	+	−	+
1	−	+	+	−	+
x	+	+	+	+	+
$\neg x$	−	−	+	+	−
$x\&y$	+	+	−	−	+
$x \vee y$	+	+	−	−	+
$x \Rightarrow y$	−	+	−	−	−
$x \equiv y$	−	+	+	−	−
$x \oplus y$	+	−	+	−	−
$x\mathrm{NAND}y$	−	−	−	−	−
$x\mathrm{NOR}y$	−	−	−	−	−

Tabuľka 12.25: Príslušnosť elementárnych Booleovských funkcií do tried T_0, T_1, L, S, M.

Všimnite si, že rovnica

$$(1 \oplus x_3 \oplus x_3x_4) = 1$$

má tri riešenia:

(a) $x_3 = x_4 = 0$,

(b) $x_3 = 0, x_4 = 1$,

(c) $x_3 = x_4 = 1$.

Úloha 12.17. *Každá uzavretá trieda* $A \subsetneq \mathcal{P}_2$ *je obsiahnutá v aspoň jednej z tried* T_0, T_1, L, S, M.

Úloha 12.18. *Zostrojte Vennov diagram pre množiny* n*-árnych Booleovských funkcií* T_0^n, T_1^n, L^n, S^n *a určte mohutnosti všetkých 16 množín, ktoré sú pomocou neho definované!*

Pri skúmaní úplnosti nejakej množiny Booleovských funkcií, resp. pri konštrukcii úplného systému Booleovských funkcií môže byť užitočná nasledujúca tabuľka: Aby bola nejaká množina Booleovských funkcií úplná, musí mať v každom zo stĺpcov T_0, T_1, L, S, M aspoň jeden znak –. Preto sú napríklad množiny $\{\neg x, x \vee y\}, \{x \Rightarrow y, x \oplus y\}$ úplné, ale $\{x\&y, x \vee y\}$ nie je úplná. Rozhodnúť o tom, či nejaká zložitejšia Booleovská funkcia patrí/nepatrí do tried L, S, M na základe definícií tried môže byť pomerne náročné. Pre praktické použitie však často vystačíme so slabšími ale podstatne jednoduchšími kritériami. Na ich zavedenie potrebujeme jeden jednoduchý pojem.

Definícia 12.17. n*-árna Booleovská funkcia* f *je balancovaná, ak má množina jej jednotkových vektorov (vektorov pravdivostných hodnôt, na ktorých* f *nadobúda hodnotu* 1*) mohutnosť* $2^{2^{n-1}}$.

- Ak je Booleovská funkcia samoduálna, tak je balancovaná.
- Ak je Booleovská funkcia lineárna, tak je buď konštantná, alebo balancovaná.

- Ak je n-árna Booleovská funkcia $f(x_1, \ldots, x_n)$ monotónna a $f(0, \ldots, 0) = 1$, alebo $f(1, \ldots, 1) = 0$, tak $f(x_1, \ldots, x_n)$ je konštantná.

Podľa týchto kritérií rýchle zaradíme napríklad implikáciu: nie je to ani konštantná, ani balancovaná funkcia, preto nemôže patriť do tried L, S, na vektore $(0, 0)$ nadobúda hodnotu 1, a teda nie je monotónna.

Triedy Booleovských funkcií T_0, T_1, L, S, M sú výnimočné, predstavujú jediné tzv. predúplné triedy Booleovských funkcií v $\mathcal{P}_2$. Preskúmame ich vlastnosti podrobnejšie.

Definícia 12.18. *Množina Booleovských funkcií $A \subseteq \mathcal{P}_2$ sa nazýva predúplnou triedou (Booleovských funkcií), ak $[A] \neq \mathcal{P}_2$, ale pre ľubovoľnú Booleovskú funkciu f, ktorá nepatrí do A platí $[A \cup \{f\}] = \mathcal{P}_2$.*

Poznámka. Predúplnosť triedy A znamená:

1. A je uzavretá, pretože ináč by sme mohli zobrať Booleovskú funkciu $f \in [A] - A$, pre ktorú by potom platilo: $[A \cup \{f\}] = [A] \neq \mathcal{P}_2$.
2. A je neúplná trieda, lebo $[A] \neq \mathcal{P}_2$, ale
3. triede A chýba k úplnosti tak málo, že stačí zobrať ľubovoľnú Booleovskú funkciu, ktorá do triedy A nepatrí, pridať ju k A, aby sme dostali úplný systém.

Zdôrazňujeme ešte raz, že poslednú uvedenú vlastnosť musí mať ľubovoľná a nie špeciálne vybraná funkcia z A^c. V opačnom prípade by totiž ľubovoľná uzavretá neúplná množina Booleovských funkcií tvorila predúplný systém, ktorý by sa dal „zúplniť“ pridaním napríklad Shefferovej alebo Pierceovej funkcie (NAND alebo NOR).

Nasledujúca veta je fakticky dôsledkom vety 12.7. Kvôli závažnosti jej obsahu ju formulujeme ako samostatnú vetu.

Veta 12.8. *V triede $\mathcal{P}_2$ existuje práve päť predúplných tried;* T_0, T_1, L, S, M.

Dôkaz Všetky triedy T_0, T_1, L, S, M sú neúplné a uzavreté. Stačí, aby sme o každej z nich ukázali, že nie je podmnožinou inej (predúplnej) triedy. Tento dôkaz ponechávame čitateľovi ako cvičenie. My pri dôkaze budeme vychádzať priamo z definície predúplnej triedy, vety 12.7 a tabuľky 12.25.

Predúplnosť triedy T_0. Trieda T_0 obsahuje okrem iných Booleovských funkcií aj funkcie $x, x\&y, x \oplus y$. Vyberieme ľubovoľnú funkciu $f \notin T_0$. Potom na základe tejto funkcie buď vytvoríme negáciu, ktorá spolu s konjunkciou tvorí úplný systém, alebo zostrojíme konštantu 1, dosadíme ju do funkcie $x \oplus y$ a dostávame negáciu $x \oplus 1$, ktorá potom spolu s konjunkciou tvorí úplný systém.

Predúplnosť triedy T_1. Vyberieme ľubovoľnú funkciu $f \notin T_1$. Ak z tejto funkcie vytvoríme negáciu, tak už máme úplný systém, lebo konjunkcia patrí do triedy T_1. Ak pomocou f vytvoríme „len“ konštantu 0, tak použijeme implikáciu z triedy T_1 a vytvoríme negáciu v tvare $x \Rightarrow 0$.

Predúplnosť triedy M Obe koštanty, konjunkcia a disjunkcia sú monotónne funkcie. Z nemonotónnej Booleovskej funkcie $f \notin M$ dosadzovaním konštánt zostrojíme negáciu, ktorá spolu s (monotónnou) konjunkciou tvorí úplný systém.

Predúplnosť triedy L Trieda lineárnych funkcií obsahuje obe konštanty aj negáciu. Z nelineárnej Booleovskej funkcie $f \notin L$ vytvoríme konjunkciu.

Predúplnosť triedy S Trieda samoduálnych funkcií obsahuje negáciu. Pomocou negácie a nesamoduálnej funkcie $f \notin S$ vytvoríme obe konštanty. Trieda n-árnych samoduálnych funkcií obsahuje $2^{2^{n-1}}$ a trieda n-árnych lineárnych funkcií obsahuje len 2^{n+1} Booleovských funkcií. To znamená, že v triede S existuje samoduálna a zároveň nelineárna funkcia aspoň troch premenných, z ktorej vytvoríme konjunkciu.

Predpokladajme, že v triede $\mathcal{P}_2$ existuje ďalšia predúplná trieda, označme ju X. Trieda X je uzavretá a nesmie byť obsiahnutá v žiadnej z predúplných tried T_0, T_1, L, S, M. To však znamená, že X je úplná. Spor. □

Úloha 12.19. *Zistite či sú nasledujúce množiny Booleovských funkcií úplné:*

1. $x\&y, 0, 1, x \oplus y \oplus z$
2. $x\&y, x \Rightarrow y, 1$
3. $x \oplus y, x \equiv y, x \Rightarrow y$
4. $x \Rightarrow (y\&\neg z)$
5. $x \oplus (y \vee z), x \Rightarrow z$
6. $\neg x \vee \neg y$
7. $\neg x\&\neg y$
8. $x \Rightarrow \neg y$
9. $x \vee \neg y$

Úloha 12.20. *Dokážte, že neexistuje samoduálna nelineárna funkcia dvoch premenných!*

Úloha 12.21. *Nájdite všetky samoduálne nelineárne Booleovské funkcie troch premenných! Návod: vytvorte ANF Booleovskej funkcie 3 premenných* $f(x, y, z)$ *a riešte rovnosť* $f(x, y, z) = \overline{f}(\overline{x}, \overline{y}, \overline{z})$ *vzhľadom na koeficienty* $a_0, \ldots, a_7$.

Hoci množiny Booleovských funkcií môžu byť veľmi rozsiahle, ale ako sa ukázalo v predchádzajúcich vetách, úplnosť množiny Booleovských funkcií môže zaistiť už jej malá podmnožina. V ideálnom prípade bude obsahovať jednu Booleovskú funkciu—NAND, NOR alebo podobnú Booleovskú funkciu tvoriacu úplný systém. V najhoršom prípade by to nemalo byť viac, ako vetou 12.7 garantovaných 5 funkcií. Nasledujúca veta ukazuje, že sa horný odhad na počet funkcií tvoriacich minimálny úplný podsystém dá ešte trocha stlačiť.

Veta 12.9. *Z každej úplnej množiny* D *Booleovských funkcií možno vybrať úplnú podmnožinu ubsahujúcu najviac 4 Booleovské funkcie.*

Dôkaz. Ponechávame čitateľovi ako cvičenie. □

Zatiaľ sme uvažovali o úplnosti vzhľadom na triedu všetkých Booleovských funkcií, $\mathcal{P}_2$. Pojem úplnosti je však možné zovšeobecniť aj na ľubovoľnú inú uzavretú triedu.

Definícia 12.19. *Množina Booleovských funkcií* $\{f_1, \ldots, f_k, \ldots\}$ *uzavretej triedy* A *sa nazýva úplnou v triede* A*, ak sa jej uzáver rovná* A.

Definícia 12.20. *Množina Booleovských funkcií* $\{f_1, \ldots, f_k, \ldots\}$ *uzavretej triedy* A *sa nazýva bázou triedy* A*, ak je úplná v triede* A *a žiadna jej vlastná podmnožina nie je úplná v triede* A.

Príklad 12.23. *Bázy tried Booleovských funkcií.*

1. $\{x\&y, \neg x\}$ *tvorí bázu* $\mathcal{P}_2$*,*
2. $\{0, 1, x \vee y, x\&y\}$ *tvorí bázu* M*,*
3. $\{1, x \oplus y\}$ *tvorí bázu* L.

Na záver tejto kapitoly uvedieme dva výsledky, ktoré pre uzavreté triedu Booleovských funkcií dokázal americký matematik Emil Post.

Veta 12.10. *Každá uzavretá trieda z* $\mathcal{P}_2$ *má konečnú bázu.*

Veta 12.11. *Mohutnosť množiny uzavretých tried v* $\mathcal{P}_2$ *je spočítateľná.*

Kapitola 13

Diskrétna matematika a informatika

13.1 Niektoré aplikácie funkcií v informatike

13.1.1 Šifrovanie informácie

Pomocou komunikačných sietí sa často prenášajú dôverné správy, ktorých prezradenie nepovolaným osobám by mohlo spôsobiť problémy. Keďže prístupu nepovolaných osôb ku komunikačným kanálom spravidla nie je možné zabrániť, dôvernosť prenášanej informácie sa chráni pomocou šifrovania. Existuje veľa šifrovacích algoritmov[1] my ilustrujeme použitie funkcií na príklade klasickej substitučnej šifry. Podstata šifrovania spočíva v nahradení údajov zapísaných v otvorenom tvare *(otvoreného textu) šifrovým textom*. Nech je M množina všetkých otvorených textov, C množina všetkých šifrových textov, potom šifru (šifrovací systém, kryptosystém) možno definovať pomocou zobrazenie (šifrovacej funkcie) $E : M \to C$, ktoré každému otvorenému textu priradí šifrový text[2] a opačnej funkcie k šifrovacej funkcii (dešifrovacej funkcie)$D : C \to M$. Podobne ako pri kódovaní je najdôležitejšou požiadavkou, ktorú kladieme na šifrovaciu a dešifrovaciu funkciu je jednoznačnosť dešifrovania, ktorá sa dá vyjadriť nasledovne:

$$\forall m[(m \in M) \to D(E(m)) = m].$$

Bezpečnosť takejto šifry by však bola pochybná, spočívala by v utajení dešifrovacej funkcie D. Ak by sa nepovolaná osoba dostala k dešifrovacej funkcii, bola by schopná úspešne dešifrovať ľubovoľnú zachytenú šifrovú správu. Preto sa volí iný prístup—kryptosystém nepozostáva z jedinej dvojice (E, D) ale dostatočne veľkej množiny dvojíc kryptografických funkcií (E_k, D_k), parametrizovanej pomocou parametra k, nazývaného kryptografickým kľúčom. Na šifrovanie/dešifrovanie informácie sa síce používa ten istý kryptosystém, ale zakaždým iná dvojica kryptografických funkcií (E_k, D_k). Klasický

[1] histórii kryptológie je venovaná skvelá kniha [10], dobrým úvodom do kryptológie je [16].

[2] existujú tzv polyalfabetické šifry, kde sa namiesto šifrovacej funkcie používa len relácia, ale takýmito šiframi sa teraz nebudeme zaoberať

kryptosystém využíva na šifrovanie nahrádzanie znakov inými znakmi (najčastejšie tej istej abecedy). Šifrovacia a dešifrovacia funkcia sú permutácie abecedy, nad ktorou sa zapisujú otvorené aj šifrové texty a možno ich zadať pomocou tabuľky. Substitučnú šifru ilustrujeme na príklade tzv Cézarovej šifry, keď je znak abecedy nahradený znakom, ktorý v abecede nasleduje bezprostredne za ním a ako nasledovník znaku 'z' je definovaný znak 'a'. Tabuľka šifrovacej funkcie vyzerá nasledovne:

α	a	b	c	d	e	f	g	h	i	j	k	l	m
$E(\alpha)$	b	c	d	e	f	g	h	i	j	k	l	m	n
α	n	o	p	q	r	s	t	u	v	w	x	y	z
$E(\alpha)$	o	p	q	r	s	t	u	v	w	x	y	z	a

Šifrový text [16] je rozdelený do blokov dĺžky 5 (zachovanie dĺžok pôvodných slov by protivníkovi veľmi uľahčilo kryptoanalýzu)

```
uifsf  bsfux  pljoe  tpgds  zquph  sbqiz  jouij  txpsm  edszq  uphsb
qizui  buxjm  mtupq  zpvsl  jetjt  ufsgs  pnsfb  ejohz  pvsgj  mftbo
edszq  uphsb  qizui  buxjm  mtupq  nbkps  hpwfs  onfou  gspns  fbejo
hzpvs  gjmft  uijtc  ppljt  bcpvu  uifmb  uufs
```

13.1.2 Hašovacie funkcie

13.1.3 Primitívne rekurzívne funkcie

13.1.4 Lexikografické usporiadanie

Pri spracovaní textov potrebujeme definovať usporiadanie na množine slov nad nejakou abecedou. Nie je problém usporiadať jednotlivé symboly abecedy napríklad takto: najprv písmená, potom číslice a nakoniec špeciálne znaky. Ťažkosti spôsobuje porovnávanie slov nerovnakej dĺžky. Tento problém sa dá riešiť rozličnými spôsobmi, prirodzeným riešením je však tzv. *lexikografické usporiadanie*.

Definícia 13.1. *Nech je* $(A, \leq_A)$ *usporiadaná množina. Lexikografickým usporiadaním množiny* $A^* = \bigcup_{i\geq 0} A^i$ *indukovaným usporiadaním* $\leq_A$ *nazývame reláciu* $\leq_L$ *definovanú takto: pre* $x, y \in A^*$; $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_n)$ *platí*

$$x \leq_L y \equiv$$
$$\equiv \exists i[(i \leq m)\&(x_i <_A y_i)\&\forall j[(j < i) \rightarrow (x_j = y_j)]] \vee [(m \leq n)\&\forall j[(j \leq m) \rightarrow (x_j = y_j)]].$$

Poznámka. V definícii lexikografického usporiadania treba rozlišovať relácie usporiadania $\leq_A, <_A$; to sú usporiadania množiny A, $\leq_L$ je lexikografické usporiadanie množiny A^* a $\leq$ je prirodzené usporiadanie množiny $\mathbb{N}$. Pripomíname, že A^* označuje množinu všetkých reťazcov nad abecedou A. Formálna definícia lexikografického usporiadania je na prvý pohľad dosť komplikovaná. Skutočnosť, ktorú vyjadruje, je však pomerne jednoduchá: slovo (reťazec) x predchádza slovo (reťazec) y ak

1. x je prefixom slova y, alebo
2. slová x, y majú nejaký spoločný prefix dĺžky r ($0 \leq r < \min(\lambda(x), \lambda(y))$ a $(r+1)$-vý symbol slova x, x_{r+1} predchádza v usporiadaní $\leq_A$ $(r+1)$-vý symbol y_{r+1} slova y.

Príklad 13.1. *Uvažujme slová „demokracia“, „demonštrácia“ a „demon“. Všetky tri majú spoločný prefix „demo“, o usporiadaní bude rozhodovať piaty symbol. V slove „demokracia“ je piaty symbol „k“ a v slovách „demonštrácia“ a „demon“ je piaty symbol „n“. Keďže „k“<„n“, v lexikografickom usporiadaní uvedených troch slov bude na prvom mieste „demokracia“. Slovo „demon“ je prefixom slova „demonštrácia“, a preto ho v lexikografickom usporiadaní bude predchádzať. V lexikografickom usporiadaní bude teda poradie „demokracia“, „demon“, „demonštrácia“.*

Úloha 13.1. *Nech $\leq_A$ nie je úplné usporiadanie na množine A. Bude lexikografické usporiadanie na množine A^*, $\leq_L$ indukované usporiadaním $\leq_A$ úplné? Zdôvodnite!*

Úloha 13.2. *Dokážte, že lexikografické usporiadanie $\leq_L$ indukované usporiadaním $\leq_A$ je usporiadaním na množine A^*. (Návod: ukážte, že $\leq_L$ je reflexívna, tranzitívna a antisymetrická relácia!)*

Úloha 13.3. *(Pokračovanie.) Dokážte, že ak je relácia $\leq_A$ úplné usporiadanie na množine A., tak potom relácia $\leq_L$ je úplným usporiadaním na množine A^*!*

Úloha 13.4. *Nech $E = \{0, 1\}$. Na množine vektorov E^3 definujeme usporiadanie takto:*

$$(a_1, a_2, a_3) \leq_E (b_1, b_2, b_3) \equiv (a_1 \leq b_1)\&(a_2 \leq b_2)\&(a_3 \leq b_3),$$

pričom $0 \leq 0, 0 \leq 1, 1 \leq 1$. Zostrojte Hasseho diagram pre $(E^3, \leq_E)$!

Úloha 13.5. *Zostrojte Hasseho diagram pre lexikografické usporiadanie množiny E^3 a porovnajte ho s Hasseho diagramom z predchádzajúceho príkladu!*

Úloha 13.6. *Usporiadajte lexikograficky nasledujúce slová: a, ano, ale, aba, alebo, ani, abraham, anna, andrej, ada,adalin, adolf, andrea, adrenalin, anton, aldo, alf, alfa, august, aurel, augustus, atom, axis, avenarius, alveola, aorta, ascendentny; za predpokladu, že $a < b < c \ldots < z$.*

Zoznam potenciálnych tém pre túto kapitolu

1. Usporiadania a triedenia
2. algoritmy ako funkcie. Rekurzívna vyčísliteľnosť
3. spočítateľnosť algoritmicky riešiteľných problémov potenciálne vs. aktuálne nekonečno (konštruktivistická matematika)
4. dátové štuktúry
5. relácie, databázy
6. reprezentácia množín, relácií, zobrazení,... v programovacích jazykoch

Kapitola 14

Prílohy

14.1 Zermelo-Fraenkelov systém axióm

Zermel-Fraenkelov systém axióm je najrozšírenejší axiomatický systém teórie množín. Zermel-Fraenkelov systém axióm sa označuje skratkou ZF, ak sa k jeho axiómam pridáva axióma výbery, označuje sa ako ZFC (Zermel-Fraenkelov systém axióm s axiómou výberu). Axiómy ZF, aj rozšíreného systému ZFC zaručujú existenciu dostatočne bohatého univera množín, postačujúceho pre potreby súčasne matematiky. Zermel-Fraenkelov systém axióm je uvedený prakticky v každej monografii alebo učebnici teórie množín, my sme ho prebrali z práce [4].

Axióma existencie množín

$$\exists x(x = x)$$

(existuje aspoň jedna množina.)

Axióma extenzionality

$$\forall x \forall y \left[(x = y) \Leftrightarrow z : (z \in x \Leftrightarrow z \in y)\right]$$

(Axióma extenzionality vyjadruje, že dve množiny (x, y) sa rovnajú práve vtedy, ak obsahujú tie isté prvky.)

Axióma dvojice

$$\forall x \forall y \exists z \Rightarrow (z = \{x, y\}).$$

(ľubovoľné dve množiny x, y určujú dvojprvkovú množinu $\{x, y\}$.

Axióma Schéma separácie

$$\forall x \forall y (z \in y \Leftrightarrow (z \in x \& \phi(x)))$$

(Ak je x množina a ϕ formula, tak existuje množina z tých prvkov množiny x, ktoré majú vlastnosť ϕ.)

Axióma sumy

$$\forall a \exists z \forall x (x \in z \Leftrightarrow \exists y (x \in y \& y \in a))$$

(pre každú množinu a existuje množina všetkých prvkov, ktoré patria do niektorého z prvkov množiny a.)

Axióma regularity

$$A \neq \emptyset \Rightarrow (\exists x)\,[x \in A \& (\forall y)(y \in x \Rightarrow y \notin A)])$$

Žiadna množina nie je porvkom seba samej.

Axióma nekonečnej množiny

$$\exists x (\emptyset \in x \& \forall y \in x : (S(y) \in x))$$

Nasledovník množiny x je definovaný ako množina $x \cup \{x\}$. Axióma nekonečnej množiny tvrdí, že existuje množina obsahujúca prázdnu množinu a je uzavretá vzhľadom na operáciu nasledovníka.

$$\forall x \exists y (z \in y \Leftrightarrow z \subset x).$$

Inými slovami, ak je x množina, tak aj súbor všetkých jej podmnožín je množina (nazývaná potenčnou množinou).

Schéma axióm nahradenia Nech $\psi(u, v)$ je formula, ktorá neobsahuje voľné premenné w, z. Potom formula

$$\forall u \forall v \forall w ((\psi(u, v) \& \psi(u, w)) \rightarrow (v = w)) \rightarrow \forall a \exists z \forall v (v \in z \Leftrightarrow \exists u (u \in a \& \psi(u, v)))$$

(definovateľné zobrazenie zobrazuje množinu na množinu.)

Axióma výberu

$$(I \neq \emptyset) \& (x_i : i \in I) \Rightarrow \prod_{i \in I} x_i \neq \emptyset$$

Prvok množiny $\prod_{i \in I} x_i$ sa nazýva výberová funkcia. Axióma výberu sa dá formulovať aj jednoduchšie. Jedno z tvrdení ekvivalentných axióme výberu tvrdí, že karteziánsky súčin neprázdnych množín je neprázdna množina. Iná formulácia axiómy výberu znie, že pre ľubovoľnú množinu neprázdnych množín existuje množina, ktorá obsahuje po jednom prvku z každej množiny danej množiny množín.

Zoznam obrázkov

2.1 Vennov diagram pre $A \subseteq B$ 33

3.1 Karteziánsky súčin množín $\{1,2,3,4,5\} \times \{2,3\}$ 57
3.2 Karteziánsky súčin množín $\{1,2,3,4,5\} \times \{y \in \mathbf{R}; 2 \leq y \leq 3\}$ 57
3.3 Karteziánsky súčin množín $\{x \in \mathbf{R}; 1 \leq x \leq 5\} \times \{y \in \mathbf{R}; 2 \leq y \leq 3\}$ 57

4.1 Graf $G = (V, U)$. 64
4.2 Graf binárnej relácie R 64
4.3 Rodokmeň rodiny Medici, slepá vetva Chiarissima II 65
4.4 Zložená relácia RS 66
4.5 Graf relácie RS 67
4.6 Skladanie relácií RST 67

5.1 Grafy relácií R_1, R_2, R_3, R_4, R_5. 85

6.1 Graf relácie $|$ 105
6.2 Hasseho diagram množiny M 106
6.3 Hasseho diagram množiny M 107
6.4 Hasseho diagram množiny M 108

12.1 Hradlá realizujúce elementárne Booleovské funkcie 201
12.2 Logický obvod počítajúci Booleovskú funkciu F 203
12.3 Booleovské kocky 214
12.4 Graf Booleovskej funkcie r_i 214
12.5 Maximálne podkocky 217
12.6 (Prázdna) Karnaughova mapa funkcie jednej premennej 221

12.7 (Prázdna) Karnaughova mapa funkcie dvoch premenných 221
12.8 (Prázdne) Karnaughove mapy funkcie troch a štyroch premenných 222
12.9 „Adresy“políčok v Karnaughovej mape štyroch premenných 222
12.10 Karnaughova mapa Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$ 222
12.11 Susednosť v Karnaughovej mape 223
12.12 Jednotkové oblasti v Karnaughovej mape 224
12.13 Prosté implikanty Booleovskej funkcie $f(x_1, x_2, x_3, x_4)$ 224
12.14 Karnaughova mapa neúplne určenej Booleovskej funkcie 230
12.15 Doplnenie neúplne určenej Booleovskej funkcie 230
12.16 Schéma dôkazu vety 12.7 246

Index

(, 179

abeceda, 35
  kódová, 87
  zdrojová, 87
alternatíva, 10
ANF, 234
antitéza, 20
aritmetika
  kardinálna, 131
  ordinálna, 131, 141
asociatívnosť
  disjunkcie , 12
  konjunkcie , 12
  prieniku, 39
  skladania binárnych relácií, 68
  zjednotenia, 39
axióma, 6, 7
  špecifikácie, 30
  fundovanosti, 139
  logická, 8
  matematickej teórie, 8
  regularity, 139, 140
  výberu, 116, 150
  vlastná, 8
axiómy
  predikátového počtu, 175
  rovnosti, 8
axiomatická teória, 151

bijekcia, 85

cesta, 63
cyklus, 63
číslo
  alef nula ($\aleph_0$), 128
  kardinálne, 127, 128
  ordinálne, 137, 139
  ordinálne, izolované, 141
  ordinálne, konečné, 140
  ordinálne, limitné, 141
  ordinálne, nekonečné, 140
  ordinálne, transfinitné, 140, 142

dĺžka
  DNF, 208
  odvodenia, 153
  slova, 35
dôkaz
  deduktívny, 18
  implikácie nepriamy, 21
  matematický, 18
  nepriamy, 20
  priamy, 19
  sporom, 20
diagonála
  matice hlavná, 94
diagram
  Hasseho, 105
  pokrytia, 105
  Vennov, 33
disjunkcia, 10
DNF
  iredudantná, 218
  minimálna, 210
  najkratšia, 210
  skrátená, 217

ekvivalencia, 11
  množín, 123

forma
  úplná normálna disjunktívna, ÚDNF, 207
  úplná normálna konjuktívna, ÚKNF, 211
  algebraická normálna, 234
  normálna disjunktívna, DNF, 208
  normálna konjuktívna, KNF, 210
formula
  algebry logiky, 202

elementárna, 7, 173
PP nepravdivá v interpretácii, 186
PP pravdivá v interpretácii, 186
PP splnená v interpretácii, 186
PP splniteľná, 187
PP splniteľná v interpretácii, 186
PP všeobecne pravdivá, 187
predikátového počtu, 173
uzavretá, 175
výrokovej logiky, 7
formula algebry logiky, 164
funkcia, 81
množiny charakteristická, 129
Booleovská, 82
Booleovská (BF), 195
Booleovská balancovaná, 247
Booleovská, elementárna, 200
Booleovská, zložená, 201
dekódovacia, 87
hašovacia, 252
kódovacia, 87
množiny charakteristická, 82
pravdivostná, 82
primitívne rekurzívna, 252
totálna, 83
funkcia neúplne zadaná, 199
funkcionálny symbol, 172

graf, 63
BF, 213
neorientovaný, 63
orientovaný, 63
súvislý, 63
grafová reprezentácia binárnej relácie, 62

hĺbka formuly, 160, 203
hodnota
Booleovská, 195
pravdivostná, 9
hradlo, 201
hrana
grafu, 63
grafu neorientovaná, 63
grafu orientovaná, 63
incidentná, 63
hypotéza, 153

idempotentnosť
disjunkcie, 12
konjunkcie, 12
prieniku, 39
zjednotenia, 39
identity
množinové, 38
implikácia, 11
implikant, 217
prostý , 217
prostý, podstatný, 226
indukcia
úplná, 24
báza, 24
matematická, 24
predpoklad, 24
transfinitná, 139
záver, 24
injekcia, 85
interpretácia, 186
iterácia
jazyka kladná, 36
jazyka nezáporná , 36
izomorfizmus
množín, 137

jazyk, 36
teórie, 6

Karnaughova
mapa, 221
mapa BF, 221
karteziánsky súčin, 56, 61
kocka Booleovská, 214
kompozícia
binárnych relácií, 65
komutatívnosť
prieniku, 39
zjednotenia, 39
konštanta
logická, 195
konjunkcia, 10
elementárna, 208
konkatenácia
jazykov, 36
slov, 36
kontradikcia, 11, 165
PP, 187

kontrapozícia
    negácie, 12
kontrapozícia negácie, 159
kontrapríklad, 23
koobor
    binárnej relácie, 61
    zobrazenia, 81
kvantifikátor, 15
    existenčný, 15
    všeobecný, 15

literál, 208
logika
    výroková, 7

matematická indukcia, 192
matica, 56
    binárna, 62
    Booleovská, 62
    transponovaná, 73
maticová reprezentácia binárnej relácie, 62
metóda
    Cantorova diagonalizačná, 124
    Quine-McCluskey, 218
    rozlišovacia, 23
metóda Karnaughova, 213
metóda Quine-McCluskey, 213
metajazyk, 6
minimaliz8cia DNF, 213
minimalizácia DNF, 211
množina, 29
    BF uzavretá, 236
    celých čísel, 30
    dobre usporiadaná, 108, 138
    komplexných čísel, 30
    konečná, 119
    nekonečná, 119
    nespočítateľná, 120, 124
    potenčná, 50, 129
    prázdna, 33
    prirodzených čísel, 30, 120
    prvočísel, 121
    racionálnych čísel, 30
    reálnych čísel, 30
    spočítateľná, 120
    univerzálna, 33
    usporiadaná, 103
    všetkých množín, 31
množiny
    disjunktné, 33
    izomorfné, 137
    podobné, 137
model, 186
mohutnosť
    kontinua, 128
    množiny, 120
    množiny prirodzených čísel, 128
    množiny reálnych čísel, 128

nasledovník ordinálneho čísla, 142
negácia, 10
neprotirečivosť
    absolútna, 165
    relatívna, 165
    teórie, 165
neprotirečivosť výrokového počtu, 164

oblasť interpretácie, 186
oblasť pôsobenia kvantifikátora, 173
obor
    binárnej relácie, 61
    zobrazenia, 81
obvod
    logický, 200
obvod logický, 195
odvodenie
    formuly, 153
    v teórii, 152
operácia
    binárna, 82
    nasledovníka, 131
    zreťazovania slov, 36
operácie množinové
    doplnok, 33
    prienik, 33
    rozdiel, 33
    symetrická diferencia, 35
    zjednotenie, 33
operátor
    Booleovský, 227
    logický, 7
operátor nasledovníka, 172
ordinálny typ, 139

paradox

Burali-Forti, 140
Burali-Fortiho, 149
Russellov, 31, 50, 149
permutácia, 85
počet
predikátový, 151
predikátový s rovnosťou, 193
počet predikátový, 171
podgraf indukovaný, 213
podkocka maximálna, 216
podmnožina, 32
podobnosť
množín, 137
podslovo, 36
koncové (sufix), 36
počiatočné (prefix), 36
pokrytie grafu vrcholové, 215
polynóm
Žegalkinov, 234
pravidlo
modus ponens, 18
modus tolens, 19
negácie ∃, 16
negácie ∀, 16
negácie kvantifikátora, 16
odlúčenia, 18
odvodzovacie, 7, 8
sylogizmu, 19
výberu, 75
pravidlo modus ponens, 152
pravidlo zovšeobecnenia, 176
predikátový počet, 171
predikátový symbol, 171
predmetová konštanta, 171
predmetová premenná, 171
premenná
Booleovská, 195
fiktívna, 197
logická, 195
podstatná, 197
výroková, 7, 10
viazaná , 175
voľná, 175
premisa, 11
princíp
dvojhodnotovosti, 9
matematickej indukcie, 23
priorita logických operátorov, 153
projekcia
relácie, 74
relácie prvá,druhá, 74
prvky
porovnateľné, 103
prvok
matice, 56
maximálny, 107
minimálny, 107
množiny, 29
najmenší, 107
najväčší, 107

rang konjunkcie, 208
reductio ad absurdum, 12
rekurzia
transfinitná, 140
relácia
n-árna, 62
antisymetrická, 95
asymetrická, 96
atranzitívna, 96
binárna, 61
ekvivalencie, 95
identická, 73, 94
inklúzie množín, 32
inverzná, 69
ireflexívna, 96
jednoznačná, 77
na množine, 94
opačná, 69
pokrytia, 105
prázdna, 94
redukcia, 105
reflexívna, 95
rozšírenie, 80
symetrická, 95
symetrizácia, 100
tolerancie, 96
tranzitívna, 95
trichotomická, 96
usporiadania, 103
všade definovaná, 77
zúženie, 80
zložená, 65
rovnosť

množín, 32
rozklad
BF, 205
BF konjunktívny, 210
indukovaný ekvivalenciou, 101
množiny, 100

súčet
kardinálnych čísel, 131
logický, 10
ordinálnych čísel, 141
súčin
binárnych matíc, 68
kardinálnych čísel, 132
logický, 10
ordinálnych čísel, 144
šifra
substitučná, 251
šifrovanie, 251
signatúra teórie, 172
skladanie
binárnych relácií, 64
Booleovských funkcií, 201
skladanie BF, 199
sled, 63
slovo
konečné, 35
nad abecedou, 35
nekonečné, 35
prázdne, 35
sumátor jednobitový, 212
surjekcia, 85
symbol
špeciálny, 172
logický, 172
symetrizácia relácie, 100
systém
indexovaný, 111
množín indexovaný, 112

téza Hilbertova, 194
tabuľka
pravdivostná, 10
pravdivostných hodnôt, 196
tautológia, 11, 160
teória
efektívne axiomatizovateľná, 152
logická, 7
matematická, 6
neprotirečivá, 165
teoréma, 160
teórie, 153
teorémy
matematickej teórie, 8
výrokového počtu, 154
term, 173
text
šifrový, 251
otvorený, 251
trieda
čiastočne usporiadaných množín, 138
množín, 32
ordinálnych čísel, 140
rozkladu, 100
ťah, 63

umocňovanie
kardinálnych čísel, 133
ordinálnych čísel, 146
usporiadaná
n-tica, 54, 55
dvojica, 54
usporiadaná dvojica, 61
usporiadanie, 103
dobré, 137, 150
lexikografické, 144, 252
lineárne, 103
ostré, 104
totálne, 103
uzáver, 11
relácie reflexívno-tranzitívny, 98
relácie tranzitívny, 98
uzáver množiny, 236
úplnosť
výrokového počtu, 160

váha Hammingova, 213
výrok, 9
elementárny, 10
kvantifikovaný, 15
zložený, 10
výroková
forma, 14
funkcia, 14

výroky
ekvivalentné, 11
výskyt premennej
viazaný, 173
voľný, 174
Vennov diagram, 33
verifikácia, 23
veta
Cantor-Bernsteinova , 125
o úplnosti výrokového počtu, 163
o dedukcii, 155
o disjunktívnom rozklade BF, 205
o funkcionálnej úplnosti, 242
o konjuktívnom rozklade BF, 210
vrchol
izolovaný, 74
stupeň, 82
vrchol grafu, 63
vzdialenosť Hammingova, 213

základ
logický, 7
zákon
o vylúčení sporu, 9
vylúčenia tretieho, 9
absorbcie, 12, 39
asociatívny zovšeobecnený, 114
de Morganov, 12, 39
de Morganov zovšeobecnený, 113
distributívny, 12, 39
distributívny zovšeobecnený, 114
dvojitej negácie, 12
komutatívny zovšeobecnený, 114
vylúčenia sporu, 12
vylúčenia tretieho, 12
ZFC, 255
znak abecedy, 35
zobrazenie, 81
čiastočné, 83
bijektívne, 85
injektívne, 85
jedno-jednoznačné, 85
na množinu, 85
parciálne, 83
prosté, 85
surjektívne, 85
zachovávajúce usporiadanie, 137
zreťazenie
jazykov, 36
slov, 36

Literatúra

[1] *Encyclopedia Britannica*. Britannica.com Inc, cd rom edition, 2001.

[2] P.S. Aleksandrov. *Úvod do teórie množín a všeobecnej topológie*. Nauka, Moskva, 1-st edition, 1974. v ruštine.

[3] Šalát, T. and Smítal, J. *Teória množín*. Alfa, Bratislava, 1-st edition, 1986.

[4] B. Balcar and P Štepánek. *Teorie množin*. Academia, Praha, 1-st edition, 1986.

[5] L. Bukovský. *Množiny a všeličo okolo nich*. Epsilon. Alfa, Bratislava, 1-st edition, 1985.

[6] Čechák, V., Berka, K., and Zapletal I. *Co víte o moderní logice*. Horizont, Praha, 1-st edition, 1981.

[7] I. Černý. *Analýza v komplexním oboru*. Academia, Praha, 1-st edition, 1983.

[8] S.V. Jablonský. *Úvod do diskrétnej matematiky*. Alfa, Bratislava, 1982.

[9] Jablonský, S.V. and Lupanov, O.B. *Diskrétna matematika a matematické otázky kybernetiky*. Mir, 1974, Moskva. (V ruštine).

[10] D. Kahn. *The Codebreakers*. Scribner, 3-rd edition, 1996.

[11] M. Kline. *Mathematics, the Loss of Certainty*. Oxford University Press, New York, 1980.

[12] J. Kolář, O. Štepánková, and M. Chytil. *Logika, algebry a grafy*. SNTL, Praha, 1-st edition, 1989. Spoločné vydanie s vydavateľstvom Alfa, Bratislava.

[13] Kolmogorov, A.N. and Fomin, S.V. *Základy teorie funkcí a funkcionální analýzy*. SNTL, Praha, 1-st edition, 1975.

[14] E. Mendelson. *Introduction to Mathematical Logic*. Nauka, Moskva, 1 edition, 1976. v ruštine.

[15] D. Olejár and M. Škoviera. *Diskrétna matematika I.* Univerzita Komenského, Bratislava, 1 edition, 1992.

[16] B. Schneier. *Applied Cryptography*. John Wiley, 2-nd edition, 1996.

[17] R. Thiele. *Matematické dôkazy*. SNTL, Praha, 1986.