Úvod do diskrétnych štruktúr

1 Základy matematickej logiky (logické operácie, formuly, výrokové funkcie, kvantifikácia výrokov, tautológia, kontradikcia)

<u>Logické operácie:</u>

Logické spojky: negácia, konjunkcia, disjunkcia, implikácia, ekvivalencia, xor

1. Idempotentnosť $(p \wedge p) \leftrightarrow p$
   $(p \vee p) \leftrightarrow p$
2. Komutatívnosť $(p \wedge q) \leftrightarrow (q \wedge p)$
   $(p \vee q) \leftrightarrow (q \vee p)$
   $(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$
3. Asociatívnosť $(p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r)$
   $(p \wedge (q \wedge r)) \leftrightarrow ((p \wedge q) \wedge r)$
4. Distributívne zákony $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$
   $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$
5. Absorbčné zákony $(p \wedge (q \vee p)) \leftrightarrow p$
   $(p \vee (q \wedge p)) \leftrightarrow p$
6. Zákon dvojitej negácie $\neg\neg p \leftrightarrow p$
7. Zákon vylúčenia tretieho $(p \vee \neg p) \leftrightarrow 1$
8. Zákon o vylúčení sporu $(p \wedge \neg p) \leftrightarrow 0$
9. De Morganove zákony $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
   $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
10. Kontrapozícia negácie $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$
11. Reductio ad absurdum $(\neg p \rightarrow p) \rightarrow p$
12. $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$
13. $(p \rightarrow q) \leftrightarrow \neg(p \wedge \neg q)$
14. $(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q)$
15. $(p \vee q) \leftrightarrow (\neg p \rightarrow q)$
16. $(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$

<u>Tautológia:</u> výrok, ktorý je pravdivý pri akýchkoľvek významoch pravdivosti ich premenných

výrok p je pravdivý pre všetky možné kombinácie pravdivostných hodnôt výrokov, z ktorých je zložený

<u>Kontradikcia</u>: ak v(p) = 0 bez ohľadu na pravdivostné hodnoty výrokov, z ktorých pozostáva

<u>Kvantifikácia:</u> Existuje, Všetky

Existenčný kvantifikátor ∃ čítame „existuje“. Zápis (∃x) a(x) má význam „existuje aspoň jedno také x, pre ktoré platí a(x) “, t.j. existuje aspoň jeden taký prvok, ktorý keď dosadíme do výrokovej formy a(x) za premennú x, dostaneme pravdivý výrok. Všeobecný kvantifikátor ∀ čítame „pre všetky“, alebo „pre každé“. Zápis (∀x) a(x) má význam: „pre každé x platí a(x)“.

Výroky obsahujúce kvantifikátory nazývame kvantifikované výroky. Poznamenávame, že existenčný kvantifikátor niekedy nazývajú aj malý kvantifikátor a všeobecný kvantifikátor veľký alebo univerzálny kvantifikátor

Negovanie:

$$\neg(\exists x)a(x) \leftrightarrow (\forall x)(\neg a(x))$$
$$\neg(\forall x)a(x) \leftrightarrow (\exists x)(\neg a(x))$$

Výrokové funkcie: ???

2 Matematický dôkaz (logický dôsledok, základné typy matematických dôkazov)

Dôkazom ľubovoľného tvrdenia a rozumieme postupnosť logických úvah, ktoré ukazujú, že platnosť tvrdenia a logicky vyplýva z platnosti prijatých axióm a z tvrdení, ktoré už boli skôr dokázané. Deduktívnosť výstavby matematických teórií je v tom, že každé tvrdenie, ktoré chceme do teórie začleniť, musí byť najskôr dokázané (jedinou výnimkou sú axiómy). Teda zjednodušene, pod matematickým dôkazom tvrdenia a si budeme predstavovať konečnú postupnosť tvrdení a1 ,a2 ,...,an = a , kde ai sú nejaké výroky, alebo výrokové formy a pre všetky i, i = 1, 2, ..., n-1 sú implikácie ai → ai+1 tautológie. Pričom a1 je pravdivý výrok a nazývame ho predpoklad. Pri takomto poňatí matematického dôkazu si treba uvedomiť, že sme zohľadnili finitné hľadisko a odvolávame sa na sémantiku, uvažované implikácie sú tautológie.

Definícia 1.3.1 Nech sú dané výroky a a an , ,..., 1 2 a výrok a. Hovoríme, že výrok a je logickým dôsledkom výrokov a a an , ,..., 1 2 (alebo že a logicky vyplýva z a a an , ,..., 1 2), ak pre každú interpretáciu, v ktorej každý výrok a a an , ,..., 1 2 je pravdivý, výrok a je taktiež pravdivý. Výroky a a an , ,..., 1 2 nazývame postulátmi, alebo predpokladmi tvrdenia a.

Veta 1.3.1 Nech sú dané výroky a a an , ,..., 1 2 , a, potom výrok a je logickým dôsledkom a a an , ,..., 1 2 práve vtedy, keď ((a a a) a) 1 ∧ 2 ∧...∧ n → je tautológia.

Základné typy matematických dôkazov:

Priamy dôkaz tvrdenia a Pozostáva z konečného reťazca implikácií a1 → a2 → ... → an → a , ktorého prvý člen je axióma, alebo už dokázané tvrdenie, alebo pravdivé tvrdenie, výrok a každé ďalšie tvrdenie je logickým dôsledkom predchádzajúcich, pričom posledným členom reťazca (postupnosti) je dokazované tvrdenia a. Všimnime si, že ak v uvedenej postupnosti implikácií použijeme dostatočný počet krát pravidlo jednoduchého sylogizmu dostávame platnosť implikácie a1 → a . O tvrdení, výroku a1 predpokladáme, že je pravdivé, tak potom použitím pravidla modus ponens dostávame platnosť tvrdenia a.

Nepriamy dôkaz tvrdenia a sporom Založený je na zákone vylúčenia tretieho, podľa ktorého z dvojice výrokov a,¬a musí byť práve jeden pravdivý. Keď teda dokážeme, že výrok ¬a nie je pravdivý, vyplýva z toho pravdivosť tvrdenia a. Pri dôkaze sporom postupujeme takto:

Predpokladajme platnosť tvrdenia ¬a , odvodzujeme z neho logické dôsledky tak dlho, až sa nám podarí odvodiť tvrdenie b, o ktorom vieme, že je nepravdivé (pretože jeho negácia ¬b bola už skôr dokázaná). V tom prípade hovoríme, že sme dospeli ku sporu. Keby sme v tejto situácií pokladali ¬a za pravdivé tvrdenie, boli by v našej teórií dokázateľné tvrdenia b aj ¬b , a teda aj tvrdenie b Λ ¬b , ktoré je nepravdivé. Teória by bola preto sporná (všetky tvrdenia by v nej boli dokazateľné a teda aj pravdivé), ľahko to možno nahliadnuť takto, nech a je ľubovoľné tvrdenie, výrok, zložený výrok (¬b → (b → c)) je tautológia, použitím pravidla modus ponens, dvakrát, dostávame platnosť tvrdenia c, ktoré sme vzali ľubovoľné. Teda zhrnutím dostávame, že predpoklad o pravdivosti tvrdenia ¬a neplatí, z čoho vyplýva, že a je pravdivé tvrdenie

<u>Priamy dôkaz implikácie a → b</u> Predpokladajme, že tvrdenie a platí (v prípade, že a je nepravdivé je implikácia a → b pravdivá, niet čo dokazovať), nájdeme postupnosť implikácií začínajúcu tvrdením a, končiacu tvrdením b, v ktorej každý člen je logickým dôsledkom predchádzajúcich tvrdení a axióm, resp. skôr dokázaných tvrdení. Niekoľkonásobným použitím pravidla jednoduchého sylogizmu dostávame platnosť implikácie a → b.

<u>Nepriamy dôkaz implikácie a → b sporom</u>. Podobne ako v opísanej schéme dôkazu sporom predpokladáme platnosť negácie dokazovanej implikácie, t. j. predpokladáme platnosť tvrdenia ¬(a → b) , ktoré je ekvivalentné tvrdeniu a Λ ¬b . Z tohto tvrdenia postupne odvodzujeme logické dôsledky tak dlho, pokým dospejeme k sporu. Môžu tu nastať tri prípady: - dôjdeme do sporu s tvrdením a, - dôjdeme do sporu s tvrdením ¬b - napokon môžeme dokázať dve navzájom odporujúce si tvrdenia c, ¬c . Všetky tri prípady vedú na platnosť tvrdenia a → b

<u>Nepriamy dôkaz implikácie a → b pomocou obmeny</u>. Zakladá sa na skutočnosti, že implikácia a → b a jej obmena ¬b → ¬a sú ekvivalentné, t.j. majú vždy rovnakú pravdivostnú hodnotu. To znamená, že namiesto implikácie a → b , môžeme dokazovať jej obmenu ¬b → ¬a , ak je to výhodnejšie. Nepriamym dôkazom implikácie a → b je teda reťazec (postupnosť) implikácií ¬b → a1 → a2 → ... → an → ¬a . Do predpokladu sme dali ¬b a odvodili sme ¬a . Dokázali sme teda implikáciu ¬b → ¬a , ktorá je obmenou implikácie a → b , teda z a → b , a vyplýva b. Prakticky to znamená, že nepriamy dôkaz implikácie obmenou ukončíme odkazom na spor, pretože z negovaného tvrdenia ¬b sme odvodili platnosť nepravdivého tvrdenia ¬a . (Pritom sa neodvolávame na kontrapozíciu negácie). Náš spor spočíva v tom, že o tvrdení a v implikácií a → b predpokladáme, že je pravdivé (zo známych dôvodov), zároveň sme však dokázali, že aj a Λ ¬a je pravdivé tvrdenie, čo ale nie je pravda. Poznamenávame, že účinnosť nepriamych dôkazov závisí podstatne na tom, či okrem daných predpokladov sa naviac ako predpoklad príjme nepravdivosť toho, čo chceme dokázať a vychádzame z väčšieho počtu predpokladov. Vďaka tomu sa mnohé tvrdenia dokazujú ľahšie nepriamo, ako keby sme ich chceli dokázať priamo, neplatí to však všeobecne.

<u>Matematická indukcia.</u> Ak nám treba dokázať platnosť nejakého tvrdenia (vety), ktoré je typu (alebo sa dá sformulovať tak, aby bolo tohto typu) „pre každé prirodzené číslo platí ...“, budeme sa pridržiavať princípu na ktorom je založená metóda dokazovania tvrdení nazývaná matematická indukcia. Pričom pod prirodzenými číslami rozumieme 0,1,2,...,n, ..., teda aj 0 pokladáme za prirodzené číslo. Princíp môžeme sformulovať takto: Majme množinu M, ktorá

má tieto dve vlastnosti: 1) $0 \in M$ 2) Pre každé prirodzené číslo n platí: Ak $n \in M$, tak aj $n + 1 \in M$. Množina M obsahuje všetky prirodzené čísla. Ľahko sa o tom presvedčíme. Podľa 1) je $0 \in M$. Podľa 2) z toho vyplýva, že $1 \in M$. Z toho znovu podľa 2) vyplýva, že $2 \in M$, odtiaľ $3 \in M$, atď. Takto môžeme prísť postupne ku ktorémukoľvek prirodzenému číslu, takže množina M obsahuje všetky prirodzené čísla. Môžeme uvažovať aj inak. Predpokladajme, že existujú prirodzené čísla, ktoré do M nepatria, najmenšie z nich označme p. Podľa 1) je $p > 0$. Číslo $p - 1$ je teda prirodzené číslo a podľa toho ako sme zaviedli číslo p, je $p - 1 \in M$. Podľa 2) z toho vyplýva, že $p \in M$ a to je spor. Nech a(n) označuje výrokovú formu, definovanú na množine prirodzených čísel. Máme dokázať tvrdenie, že a(n) platí pre každé prirodzené číslo n, tak postupujeme nasledujúcim spôsobom: 1º Dokážeme, že a(n) platí pre $n = 0$. Tento krok nazývame báza matematickej indukcie. 2º Dokážeme nasledujúce tvrdenie. Pre každé prirodzené číslo n platí: ak platí a(n) pre číslo n, tak platí aj pre $n + 1$. Tvrdenie, ktoré dokazujeme v 2º nazývame indukčný krok a jej predpoklad „a(n) platí pre číslo n“ nazývame indukčný predpoklad. Záver: Výroková forma a(n) platí pre každé prirodzené číslo.

3 Intuitívny pojem množiny (základné pojmy a označenia, množinové operácie, množinové identity)

<u>Základné pojmy a označenia:</u>

Množiny budeme označovať veľkými písmenami latinskej abecedy A, B, C, ..., prípadne veľkými písmenami s indexami: , ,..., ,... A_1 A_2 A_n. Objekty, ktoré tvoria množinu nazývame prvkami danej množiny. Prvky množiny označujeme malými písmenami latinskej abecedy a,b,c,..., x, y,z,... , v prípade potreby ich tiež indexujeme. Skutočnosť, že prvok x patrí do množiny A zapisujeme symbolicky $x \in A$. (Znak $\in$ nazývame binárny predikát patričnosti, prináležitosti), hovoríme tiež, že prvok x je elementom množiny A (množina A obsahuje (prvok) x, x patrí do (množiny) A). Ak x nie je prvkom množiny A, zapisujeme $x \notin A$, alebo niekedy je výhodné zapísať $\neg(x \in A)$.

Opísať množinu možno v podstate dvomi spôsobmi a to buď vymenovaním jej prvkov, alebo charakterizáciou jej prvkov pomocou nejakej spoločnej vlastnosti. V prvom prípade do zložených zátvoriek vypíšeme všetky prvky danej množiny, v prípade, že množina je konečná, nie príliš veľká; zložené zátvorky môžeme použiť aj v prípade, keď množina je nekonečná spočítateľná.

N – množina prirodzených čísel

Z - množina celých čísel

Q – množina racionálnych čísel

I – množina iracionálnych čísel

R – množina reálnych čísel

C – množina komplexných čísel.

Množinové operácie:

Definícia 2.2.2 Nech sú A, B ľubovoľné množiny. Ak pre každý prvok $x \in A$ platí, že x je prvkom B, tak potom hovoríme, že množina ***A* je podmnožinou** množiny ***B*** alebo tiež, že A je v inklúzii s B, označenie $A \subseteq B$.

Ak $A \subseteq B$ a existuje prvok množiny B taký, ktorý nepatrí do množiny A (t.j. neplatí $B \subseteq A$), tak hovoríme, že ***A* je vlastná alebo pravá podmnožina** množiny ***B*** a označujeme $A \subset B$.

Poznamenávame, že niekedy namiesto $A \subseteq B$ sa v literatúre píše $A \subset B$. Vtedy namiesto $A \subset B$ píšeme $A \subsetneq B$.

Skutočnosť, že $A \subseteq B$ zapisujeme formálne takto:

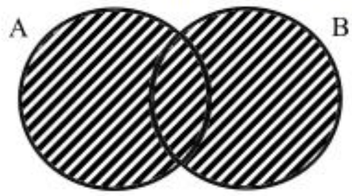
$$A \subseteq B \leftrightarrow (\forall x)((x \in A) \to (x \in B))$$

Definícia 2.2.3 Nech sú A a B ľubovoľné množiny. **Zjednotením množín *A*, *B*** nazveme množinu všetkých prvkov, ktoré patria aspoň do jednej z množín A, B. Označenie: $A \cup B$.

Formálne zapísané zjednotenie množín:

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

Pomocou Vennových diagramov zjednotenie znázorňujeme takto:

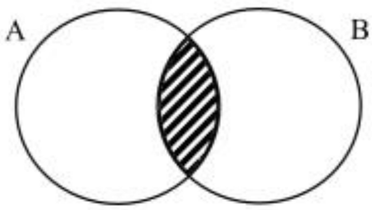


Definícia 2.2.4 Nech sú A a B ľubovoľné množiny. **Prienikom množín *A*, *B*** nazveme množinu všetkých prvkov, ktoré patria súčasne do oboch množín A, B. Označenie: $A \cap B$.

Formálne zapisujeme prienik množín:

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

Pomocou Vennových diagramov prienik množín znázorňujeme takto:



Definícia 2.2.5 Množina, ktorá neobsahuje žiaden prvok sa nazýva **prázdna množina** a označujeme ju $\emptyset$.

Poznamenávame, že prázdnu množinu môžeme definovať pomocou ľubovoľnej vlastnosti, ktorú nespĺňa žiaden prvok.

Veta 2.2.1 a) Prázdna množina je podmnožina ľubovoľnej množiny

b) Existuje práve jedna prázdna množina

Definícia 2.2.6 Nech A je ľubovoľná množina, $A \subseteq \mathrm{U}$. **Doplnkom množiny *A*** vzhľadom na množinu U nazývame množinu všetkých tých prvkov univerzálnej množiny U, ktoré nepatria do množiny A. Označenie A'.

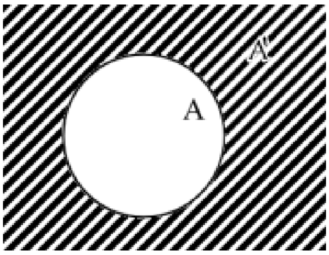
Formálny zápis:

$$A' = \{x \mid x \in \mathrm{U} \wedge x \notin A\}.$$

V literatúre označujú doplnok (komplement) množiny A aj ako $\overline{A}$ alebo A^C.

Keďže uvažujeme doplnok (komplement) množiny vzhľadom na univerzálnu množinu U, často používame aj skrátený formálny zápis

$$A' = \{x \mid x \notin A\}.$$

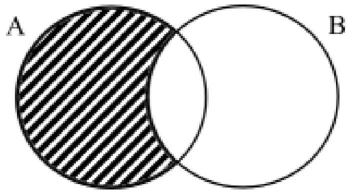


Definícia 2.2.7 Nech sú A, B ľubovoľné množiny. **Rozdielom množín *A*, *B*** nazveme množinu všetkých tých prvkov množiny A, ktoré nepatria do B. Označenie $A \setminus B$, alebo aj $A - B$.

Formálny zápis:

$$A - B = \{x \mid (x \in A) \wedge (x \notin B)\}.$$

Znázornenie pomocou Vennových diagramov:



Definícia 2.2.8 Nech sú A, B ľubovoľné množiny. **Symetrickou diferenciou množín *A*, *B*** nazveme množinu

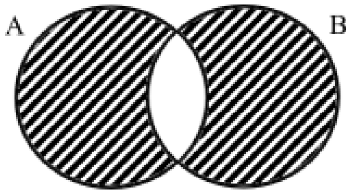
$$A \dot{-} B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}.$$

Symetrickú diferenciu množín A, B možno vyjadriť pomocou rozdielu a zjednotenia množín skrátene takto:

$$A \dot{-} B = (A - B) \cup (B - A).$$

Príklad 7. Nech $A = \langle 5,12 \rangle$, $B = \langle 7,15 \rangle$. Potom $A \dot{-} B = \langle 5,7) \cup (12,15 \rangle$.

Grafické znázornenie symetrickej diferencie množín A, B.



Definícia 2.2.9 Nech je daná množina A. **Potenčnou množinou** množiny ***A*** nazveme množinu všetkých podmnožín množiny A. Označenie $P(A)$. Teda

$$P(A) = \{X \mid X \subseteq A\}.$$

Vlastnosti množinových operácii:

Veta 2.3.1 Nech A, B, C sú ľubovoľné množiny, potom platia nasledujúce rovnosti:

1) $A \cup B = B \cup A$, $A \cap B = B \cap A$ **komutatívnosť**
2) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ **asociatívnosť**
3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ **distributívnosť**
4) $A \cup A = A$, $A \cap A = A$ **idempotentnosť**
5) $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$
6) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$ **de Morganove zákony**

Množinové identity:

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. $A \cup A^c = \mathcal{U}$
20. $A \cap (A \cup B) = A$ *(absorbčný zákon)*
21. $A \cup (A \cap B) = A$ *(absorbčný zákon).*

4 Karteziánsky súčin množín (definícia usporiadanej dvojice, KS dvoch a viacerých množín, množinové identity s KS, použitie KS)

Definícia usporiadanej dvojice:

Definícia 2.4.1 Nech sú a_1, a_2 ľubovoľné prvky. Množinu $\{\{a_1\},\{a_1,a_2\}\}$ nazývame **usporiadanou dvojicou**, označenie (a_1,a_2), pričom a_1 nazývame prvou súradnicou (zložkou), a_2 druhou súradnicou (zložkou).

Usporiadanú n-ticu, pre $n \geq 1$ môžeme teraz definovať induktívne takto:

$$(a_1) = a_1$$
$$(a_1,a_2) = \{\{a_1\},\{a_1,a_2\}\}$$
$$\vdots$$
$$(a_1,a_2,\dots,a_n) = ((a_1,\dots,a_{n-1}),a_n).$$

Platí nasledujúce tvrdenie, charakterizujúce základnú vlastnosť usporiadanej dvojice.

Veta 2.4.1 Nech (a_1,a_2), (b_1,b_2) sú dve usporiadané dvojice. $(a_1,a_2)=(b_1,b_2)$ práve vtedy, ak $a_1=b_1$, $a_2=b_2$.

KS:

Definícia 2.4.2 **Karteziánskym súčinom množín** A, B nazveme množinu

$$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}.$$

Pri definovaní karteziánskeho súčinu n – množín môžeme postupovať aj jednoduchšie, budeme vychádzať z pojmu usporiadanej n – tice, pričom budeme mať na zreteli základnú vlastnosť usporiadaných n – tíc, usporiadané n – tice $(a_1,a_2,\dots,a_n)=(b_1,b_2,\dots,b_n)$ práve vtedy, ak $a_i=b_i$, pre $i=1,2,\dots,n$, pričom všetky $a_1,a_2,\dots,a_n$ nemusia byť navzájom rôzne. **Karteziánsky súčin množín** A_1, A_2,..., A_n môžeme definovať ako množinu

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1,a_2,\dots,a_n) \mid a_i \in A_i, i=\overline{1,n}\}.$$

Množinové identity s KS: ???

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* $(A \times B) \cap (B \times A) = \emptyset$.

5 Relácie (skladanie relácii, inverzná relácia, relácie na množinách, relácie ekvivalencie, rozklady množiny, tranzitívny uzáver relácie, reflexívno-tranzitívny uzáver – definície, vlastnosti)

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.

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* $A_1, \ldots, A_n$.

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*

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

Definícia 2.5.2 Nech φ je relácia na množine A.

a) Relácia φ je **reflexívna**, ak pre každé $x \in A$ platí $(x,x) \in \varphi$;
b) Relácia φ je **ireflexívna**, ak pre žiadne $x \in A$ neplatí $(x,x) \in \varphi$;
c) Relácia φ je **symetrická**, ak z podmienky $(x,y) \in \varphi$ vyplýva $(y,x) \in \varphi$;
d) Relácia φ je **asymetrická**, ak pre každé $(x,y) \in \varphi$ platí $(y,x) \notin \varphi$;
e) Relácia φ je **tranzitívna**, ak $(((x,y) \in \varphi \wedge (y,z) \in \varphi) \Rightarrow (x,z) \in \varphi)$
f) Relácia φ je **atranzitívna**, ak $((x,y) \in \varphi \wedge (y,z) \in \varphi) \Rightarrow (x,z) \notin \varphi$
g) Relácia φ je **trichotomická**, ak pre každé $x, y \in A$ platí:
$$x \neq y \Rightarrow ((x,y) \in \varphi \vee (y,x) \in \varphi)$$
$$[\ (x = y) \vee (x,y) \in \varphi \vee (y,x) \in \varphi\ ]$$
h) Relácia φ je **antisymetrická**, ak pre každé $x, y \in A$ platí:
$$((x,y) \in \varphi \wedge (y,x) \in \varphi) \Rightarrow x = y$$

Definícia 2.5.3 **a)** Nech φ je relácia medzi prvkami množín A, B a nech ψ je relácia medzi prvkami množín B, C. Potom
$$\{(a,c) \in A \times C : (\exists b)(b \in B \wedge (a,b) \in \varphi \wedge (b,c) \in \psi)\}$$
(je to relácia medzi prvkami množín A a C) sa nazýva **zložená relácia (zložená z relácií** φ **a** ψ **)** a označujeme ju $\psi \circ \varphi$.

b) Nech φ je relácia medzi prvkami množín A, B. Potom
$$\{(b,a) \in B \times A, (a,b) \in \varphi\}$$

(je to relácia medzi prvkami množín B a A) sa nazýva **inverzná relácia** k relácii φ a označujeme ju symbolom φ^{-1}.

Definícia 2.5.4 Nech φ je relácia na množine A. **Tranzitívnym**, resp. **reflexívno-tranzitívnym uzáverom relácie** φ nazývame relácie φ^+, resp. φ^* definované nasledujúcimi vzťahmi:

$$\varphi^+ = \varphi^1 \cup \varphi^2 \cup \ldots = \bigcup_{k\geq 1} \varphi^k$$
$$\varphi^* = I_A \cup \varphi^1 \cup \varphi^2 \cup \ldots = \bigcup_{k\geq 0} \varphi^k$$

$I_A = \{(x,x) \mid x \in A\}$, $\varphi^0 = I_A$, $\varphi^i = \varphi^{i-1} \circ \varphi$ pre $i > 0$, t.j. $(x,y) \in \varphi^k$ pre nejaké $k > 0$ $\Leftrightarrow$ ak existuje postupnosť prvkov $x = x_0, x_1, \ldots, x_{k-1}, x_k = y$ taká, že platí $(x_0,x_1) \in \varphi$, $(x_1,x_2) \in \varphi$, ..., $(x_{k-1},x_k) \in \varphi$

Tranzitívny uzáver bin. relácie

$R \cup R \circ R = R \cup R^2$

$R \cup R\circ R\circ R = R \cup R^3$

$R^+ = R \cup R^2 \cup R^3 \cup \ldots = \bigcup_{k\geq 1} R^k$ tranzitívny uzáver relácie R

Veta: nech R je ľub. b.r. na mn. A
potom $\exists$ (a jediná) tranzitívna relácia R^+
s vlastnosťami:
(1) $R \subseteq R^+$
(2) Ak S je ľub. tranz. b.r. na A taká, že $R \subseteq S$, tak potom aj $R^+ \subseteq S$ (z toho vyplýva aj jednoznačnosť)

D:
$R \subseteq A\times A$ $\quad$ $A\times A$ je tranzitívna
$\mathcal{T} = \{S \subseteq A\times A \ ; \ S \text{ je tranz.} \wedge R \subseteq S\}$
$\mathcal{T} \neq \emptyset$ $\quad$ $A\times A \in \mathcal{T}$

Def: bin. rel. R^+ spĺňajúca (1) a (2) z vety je tranz. uzáver relácie R.
platí, že $R^+ = \bigcup_{k\geq 1} R^k$

$R^* \rightarrow$ reflexívna - tranz. uzáver
R $\quad$ $R^+ \cup Id_A = R^*$ reflex. - tranz. uzáver
$id_A = \{(a,a) \ ; \ a \in A\}$
R je reflex $\quad id_A \subseteq R$

Inverzná relácia:

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

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

Relácie na množinách:

Definícia 6.1. *Nech je* A *ľubovoľná množina,* A^n *označuje karteziánsky súčin* $\underbrace{\mathrm{A} \times \cdots \times \mathrm{A}}_{n}$. *Ľubovoľnú podmnožinu karteziánskeho súčinu* A^n *nazveme* n*-árnou reláciou na množine* A.

Relácia ekvivalencie:

Relácia R je reláciou ekvivalencie, ak R je reflexívna, symetrická, tranzitívna

Rozklad množiny:

Definícia 2.6.2 Nech A je neprázdna množina. Systém $S \subseteq P(A)$ sa nazýva **rozklad množiny** A, ak každá množina systému S je neprázdna. Pričom S je systém po dvoch disjunktných množín s vlastnosťou $\bigcup_{M \in S} M = A$.

Teda rozklad množiny A je taký systém neprázdnych podmnožín množiny A, že každý prvok $x \in A$ patrí práve do jednej množiny tohto systému.

nech A je ľub. mn. Systém $\mathcal{Y}$ podmnožín mn. A
$\mathcal{Y} \subseteq P(A)$

sa nazýva rozkladom mn. A, ak spĺňa:

(1) $X \in \mathcal{Y}$ $\quad X \neq \emptyset$

(2) $X, Y \in \mathcal{Y}$ $\quad X \neq Y$ $\quad X \cap Y = \emptyset$

(3) $\bigcup \mathcal{Y} = \{a \in A, \exists X \in \mathcal{Y}$ také, že $a \in X\} = A$

6 Usporiadania (definícia čiastočného a úplného usporiadania množiny, ostré a neostré usporiadanie, minimálny, maximálny, prvý a posledný prvok množiny, lexikografické usporiadanie karteziánskeho súčinu)

Definícia 2.7.1 Relácia na množine A sa nazýva **čiastočné usporiadanie množiny** A, ak je asymetrická a tranzitívna. Relácia na množine A sa nazýva **(lineárne) usporiadanie množiny** A, ak je asymetrická tranzitívna a trichotomická. Teda usporiadanie množiny A je každé čiastočné usporiadanie, ktoré je trichotomické na množine A.

Formálnejšie, relácia φ na množine A je čiastočné usporiadanie množiny A, ak pre každé $x, y, z \in A$ platí:

1. $(x, y) \in \varphi \rightarrow (y, x) \notin \varphi$
2. $(x, y) \in \varphi \wedge (y, z) \in \varphi \rightarrow (x, z) \in \varphi$.

Ak navyše pre každé $x, y \in A$ platí:

3. $(x = y) \vee (x, y) \in \varphi \vee (y, x) \in \varphi$, čo je ekvivalentné

3´. $x \neq y \rightarrow ((x, y) \in \varphi \vee (y, x) \in \varphi)$,

tak φ je **usporiadanie množiny *A***.

Ak A je množina a φ je jej usporiadanie (resp. čiastočné usporiadanie), tak hovoríme, že **množina *A* je usporiadaná** (resp. čiastočne usporiadaná) **reláciou** φ a zapisujeme to v tvare (A, φ), alebo $(A, <)$, ak namiesto $(x, y) \in \varphi$ píšeme $x < y$. Uvedený zápis je motivovaný tým, že pre tú istú množinu možno vo všeobecnosti definovať viacero čiastočných usporiadaní. Presnejšie, usporiadaná množina A je vlastne usporiadaná dvojica (A, φ), kde relácia φ je usporiadanie množiny A.

Ak namiesto $(x, y) \in \varphi$ píšeme $x < y$, tak je prirodzené stotožniť znak φ so znakom <, teda napr. $(<) \subseteq A \times A$, ak < je usporiadanie množiny A a pod.

<u>Lexikografické usporiadanie:</u>

Definícia 2.7.2 Nech $(A, \leq)$ je usporiadaná množina a n je prirodzené číslo.

Usporiadanie $\leq$ na množine $A^n = \underbrace{A \times A \times \cdots \times A}_{n-krát}$: $(a_1, a_2, ..., a_n) \leq (b_1, b_2, ..., b_n)$ práve vtedy, keď existuje taký index $i = 1,2,...,n$, že $a_i < b_i$ a pre $j < i$ platí $a_j = b_j$ sa nazýva **lexikografické usporiadanie množiny** A^n (lexikografické preto, lebo prvky $(a_1, a_2, ..., a_n)$ sú usporiadané ako slová v slovníku – lexikóne)

Lexikografické usporiadanie:

A ľub. mn. $(A, \leq)$ úplne usp. množina $\{a, b, c, \dots, x, y, z\}$

symboly = prvky mn. A

$A^n = \underbrace{A \times A \times \dots \times A}_{n\text{-krát}}$ $a = (a_1, a_2, \dots, a_n)$ slovo dĺžky n

$a = a_1 a_2 \dots a_n$

$A^* = \bigcup_{n \geq 0} A^n$ množina všetkých slov nad "abecedou"

$A^0 = \{\theta\}$

$(A^*, \leq_L)$ lexikografické uspo. $(A, \leq)$ je úplné uspo.

nech $x = x_1 x_2 \dots x_m$

$y = y_1 y_2 \dots y_n$

položíme $x \leq_L y$

(1) existuje index i taký, že $x_i < y_i$

$x_j = y_j$ pre každé $j < i$

$\underbrace{\text{rukách}} \leq \underbrace{\text{rukami}}$

nerozlišujeme dĺžku

(2) $m \leq n$ a zároveň

$x_i = y_i \quad \forall i \in \{1, 2, \dots, m\}$

~~$y = x_1 x_2$~~

$y = x_1 x_2 \dots x_m y_{m+1} y_{m+2} \dots y_n$

$(A, \leq)$ $R = \leq$

$\hat{R} = \geq$

$\hookrightarrow$ vymeníme prvky

<u>Minimálny maximálny prvok:</u>

Minimálne a najmenšie prvky:

def: prvok $a \in A$ je najmenší prvok mn. A, ak $\forall x \in A$: $a \leq x$

prvok $a \in A$ je minimálny prvok mn. A, ak neexistuje prvok $b \in A$ $b < a$ ekvivalentne pre každé $x \in A$, pre kt. platí $x \leq a$, platí, že $x = a$

najväčší $\geq$ <-> najmenší

maximálny <-> minimálny

$a \in A$ najmenší $a \leq x \quad \forall x \in A \quad a \leq b$

$b \in A$ najmenší ~~$b \leq x \quad \forall x \in A \Rightarrow a \leq b$~~

$b \leq x \quad \forall x \in A \quad b \leq a$

$\Rightarrow$ antisym. $a = b$

$(A, \leq)$ $\quad R = \leq$

$R^{-} = \{(b,a) \,;\, (a,b) \in R\}$

$a \in A$ je najmenší ak $\forall b \in A: \; a \leq b$

$a \in A$ je minimálny ak $\forall b \in A: \; b \leq a \Rightarrow b = a$

$b \neq a \Rightarrow b \not\leq a$

Nakoniec ešte zavedieme dva dôležité pojmy. Prvok a čiastočne usporiadanej množiny $(A,<)$ sa nazýva **minimálny** (resp. **maximálny**) **prvok**, ak pre žiadne $x \in A$ neplatí $x < a$ (resp. $a < x$). Prvok b čiastočne usporiadanej množiny $(A,<)$ sa nazýva **prvý** alebo **najmenší prvok** množiny A, ak pre každý prvok $x \in A$, $x \neq b$ platí $b < x$. Podobne b je **najväčší** alebo **posledný prvok** množiny A, ak pre každé $x \in A$, $x \neq b$ platí $x < b$.

Všimnime si, že najmenší (najväčší) prvok čiastočne usporiadanej množiny je súčasne jej minimálnym (resp. maximálnym) prvkom. Obrátené tvrdenie neplatí, ako vidieť z tohto príkladu.

$A \quad R \subseteq A \times A$ - usporiadanie:

je reflex $aRa \quad \forall a \in A$

je trancitívne $aRb \wedge bRc \Rightarrow aRc \quad \forall a,b,c \in A$

je antisymetrické $aRb \wedge bRa \Rightarrow a = b$

$a \leq b \quad b \leq c \Rightarrow a \leq c$

$a \leq b \quad b \leq a \Rightarrow a = b$

$(A, \leq)$ usporiadaná množina

$A \rightarrow$ nosič

$\leq \rightarrow$ relácia uspo. mn.

$a \leq b \vee b \leq a \quad \forall a,b \in A \rightarrow$ dichotómia

↳ úplne usporiadané ; lineárne usporiadané

7 Zobrazenia (definícia pomocou relácií, injektívne, bijektívne, surjektívne)

Definícia 2.8.1 Zobrazením f z množiny X do množiny Y nazývame reláciu $f \subseteq X \times Y$ ak ku každému $x \in X$ existuje práve jedno také $y \in Y$, že dvojica $(x, y) \in f$.

Podrobnejšie: relácia f z množiny X do množiny Y (alebo medzi prvkami množín X a Y v uvedenom poradí) sa nazýva **zobrazenie (funkcia)** množiny X do Y, ak platí:

1. $\forall_{x \in X} \exists_{y \in Y} (x, y) \in f$
2. $\forall_{x \in X} \forall_{y \in Y} \forall_{y' \in Y} ((x, y) \in f \wedge (x, y') \in f) \rightarrow y = y'$.

$R \subseteq A \times B$

1\. všade def: $\forall a \in A \quad \exists b \in B \quad aRb$

2\. jednoznačné: $\forall a \in A \quad b, c \in B$

ak $aRb \wedge aRc \Rightarrow$ ~~a~~ $b = c$

zobrazenie $A \rightarrow B$

f, g, h

funkcie = zobrazenie

A = definičný obor ; obor

B = obor hodnôt ; koobor

1\. $f: A \rightarrow B$ (injekcia) „vstrekmutie do" — sa nazýva injekcia / injektívne / (jednoznačné) ak platí:

$f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \quad \forall a_1, a_2 \in A$

$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

2\. $f: A \rightarrow B$ (surjekcia) zobrazenie „na" mn. B — sa nazýva surjekcia / surjektívne zobr., ak pre: $\forall b \in B \; \exists a \in A : f(a) = b$

každý prvok b je obrazom prvku a

00:35:0v

$P : A_1 \times A_2 \times \ldots \times A_n \longrightarrow A_i$

3. $f : A \longrightarrow B$ je bijekcion: - injektívnu
- surjektívnu

$$\begin{array}{ccc} A & f & B \\ a_1 & \longrightarrow & b_1 \\ a_2 & \longrightarrow & b_2 \\ \vdots & & \vdots \\ a_n & & b_n \\ \vdots & & \vdots \end{array}$$

injektívnu
každé ide do iného

$f \subseteq A \times B$ $\qquad f^{-} \subseteq B \times A$

$f^{-} = \{(b, a);\ (a, b) \in f\}$ $\qquad a_1 \longleftarrow b_1$

<u>Veta 2.8.1</u> Ak f je injektívne zobrazenie množiny *X* do *Y*, tak f^{-1} je bijektívne zobrazenie množiny $f(X)$ do *X*.

<u>Veta 2.8.2</u> Ak je f bijekcia množiny *X* na *Y*, tak f^{-1} je bijekcia množiny Y do *X*.

Poznamenávame, že $f^{-1} = \{(y, x) \in Y \times X, (x, y) \in f\}$.

<u>Veta 2.8.3</u> Nech $f : X \to Y$ a $g : Y \to Z$. Potom zložená relácia $g \circ f$ je zobrazenie množiny *X* do *Z*. Poznamenávame, že $g \circ f = \{(x, z) \in (X, Z) \mid \exists y, y \in Y, (x, y) \in f \wedge (y, z) \in g\}$.

Zobrazenie $g \circ f$ sa nazýva **zložené zobrazenie** alebo **kompozícia zobrazení** f a g.

<u>Veta 2.8.4</u> Nech $f : X \to Y$ a $g : Y \to Z$

a) Ak f, g sú injektívne zobrazenia, tak aj $g \circ f$ je injektívne zobrazenie
b) Ak f, g sú surjektívne zobrazenia, tak aj $g \circ f$ je surjektívne zobrazenie
c) Ak f, g sú bijektívne zobrazenia, tak aj $g \circ f$ je bijektívne zobrazenie

8 Mohutnosť množiny (základné vlastnosti mohutnosti a nerovnosti, počítane s mohutnosťami, súčet, súčin, moznina)

Definícia 2.9.1 Nech A, B sú dve množiny. Budeme hovoriť, že množiny ***A*, *B* majú rovnakú mohutnosť** alebo rovnaký počet prvkov, píšeme $|A|=|B|$, ak existuje prosté zobrazenie množiny A na množinu B, teda bijekcia.

Veta 2.9.1:

a) Pre každú množinu A platí $|A|=|A|$,

b) Ak $|A|=|B|$, potom $|B|=|A|$,

c) Ak $|A|=|B|$, $|B|=|C|$, tak $|A|=|C|$.

Definícia 2.9.2 Nech A, B sú množiny. Budeme hovoriť, že množina A má **mohutnosť menšiu alebo rovnú ako** množina B a písať $|A|\le|B|$, ak existuje injektívne zobrazenie $f: A \to B$. Množina A má **mohutnosť menšiu ako** množina B, píšeme $|A|<|B|$, ak $|A|\le|B|$ a nie je $|A|=|B|$.

Veta 2.9.2 Nech A, B, C sú množiny potom platí:

a) Ak $|A|=|B|$, tak $|A|\le|B|$,

b) Ak $|A|\le|B|$ a $|B|\le|C|$, tak $|A|\le|C|$,

c) Ak $|A|=|B|$ a $|B|<|C|$, tak $|A|<|C|$.

Počítanie:

Definícia 2.10.1 Nech A, B, C sú množiny. Budeme hovoriť, že **mohutnosť** množiny ***C* je súčet mohutností** množín ***A*** a ***B***, písať $|C|=|A|+|B|$, ak existujú množiny A_1, B_1 také že

$$A_1 \cup B_1 = C \tag{1a}$$

$$A_1 \cap B_1 = \emptyset \tag{1b}$$

$$|A|=|A_1|,\ |B|=|B_1| \tag{1c}$$

Definícia 2.10.2 Budeme hovoriť, že mohutnosť množiny C je **mohutnosť** množiny A **umocnená na mohutnosť** množiny B, písať $|C|=|A|^{|B|}$, ak $|C|=\left|A^B\right|$. Pričom A^B označujeme množinu všetkých zobrazení množiny B do množiny A.

Podobne ako v prípade súčtu mohutností, ukážeme korektnosť definície. Máme ukázať, že ak $|X|=|A|,\ |Y|=|B|$ a $|D|=\left|X^Y\right|$, tak $|D|=|C|$. K tomu stačí ukázať toto: ak $|A|=|X|,\ |B|=|Y|$, tak $\left|A^B\right|=\left|X^Y\right|$.

Definícia 2.10.3 Budeme hovoriť, že mohutnosť množiny C je **súčin mohutností** množín A a B, písať $|C|=|A|\cdot|B|$, ak platí

$$|C|=|A\times B|.$$

Aj tu je potrebné overiť korektnosť definície. Stačí ukázať, že ak $|A|=|X|,\ |B|=|Y|$, tak $|A\times B|=|X\times Y|$.

Pre sčítanie a násobenie mohutností platia zákony aritmetiky, napr.

Sčítanie je *komutatívne* $|A|+|B|=|B|+|A|$, (3a)

asociatívne $|A|+(|B|+|C|)=(|A|+|B|)+|C|$. (3b)

Násobenie je *komutatívne* $|A|\cdot|B|=|B|\cdot|A|$, (3c)

asociatívne: $|A|\cdot(|B|\cdot|C|)=(|A|\cdot|B|)\cdot|C|$. (3d)

Platí *distributívny zákon*

$$|A|\cdot(|B|+|C|)=(|A|\cdot|B|)+(|A|\cdot|C|). \tag{3e}$$

Dokážeme napríklad asociatívnosť násobenia. Zrejme stačí ukázať:

$$|A\times(B\times C)|=|(A\times C)\times C|.$$

Pre umocňovanie platia tiež zákony aritmetiky

$$|A|^{|B|+|C|}=|A|^{|B|}\cdot|A|^{|C|}$$

$$(|A|\cdot|B|)^{|C|}=|A|^{|C|}\cdot|B|^{|C|}$$

$$\left(|A|^{|B|}\right)^{|C|}=|A|^{|B||C|}$$

Lema 2.10.1 Pre ľubovoľnú množinu X platí $|P(X)|=2^{|X|}$.

Veta 2.10.1 $\aleph_0=\aleph_0+\aleph_0$.

Veta 2.10.2 $\aleph_0=\aleph_0 . \aleph_0$.

Veta 2.10.3 (Cantor) Pre každú množinu X platí $|X|<|P(X)|$.

Dôsledok 1. Pre každú množinu X platí $|X|<2^{|X|}$.

Dôsledok 2. Neexistuje množina všetkých množín.

9 Cantor-Bernsteinova veta a jej dôsledky (formulácia vety, idea dôkazu, usporiadanie kardinálnych čísiel)

Veta 2.9.3 (Cantor - Bernstein) Nech A, B sú množiny. Ak platí $|A| \le |B|$ a súčasne $|B| \le |A|$, tak $|A| = |B|$.

Dôkaz 1: Nech platí $|A| \le |B|$, $|B| \le |A|$. Potom existujú injektívne zobrazenia f, g také, že $f : A \to B$ a $g : B \to A$. Podľa predchádzajúcej lemy existujú množiny A_1, A_2, B_1, B_2 také, že platí (1a) – (1c). Podľa (1c) zobrazenie g zobrazuje množinu B_2 injektívne na A_2. Teda existuje inverzné zobrazenie $g^{-1} : A_2 \to B_2$. Definujme zobrazenie h takto:

$$h(x) = f(x) \text{ pre } x \in A_1 \tag{4a}$$

$$h(x) = g^{-1}(x) \text{ pre } x \in A_2 \tag{4b}$$

Ukážeme, že h je prosté zobrazenie množiny A na množinu B. Nech $x_1, x_2 \in A$, $x_1 \ne x_2$. Máme štyri možnosti: 1) $x_1, x_2 \in A_1$, 2) $x_1, x_2 \in A_2$, 3) $x_1 \in A_1, x_2 \in A_2$ a 4) $x_1 \in A_2, x_2 \in A_1$. V prípadoch (1) a (2) je $h(x_1) \ne h(x_2)$ lebo f a g^{-1} sú injektívne zobrazenia. V prípadoch (3) a (4) jeden z prvkov $h(x_1), h(x_2)$ patrí do B_1 a druhý do B_2, teda sú rôzne. Z uvedeného vyplýva, že h je prosté zobrazenie.

Nech $y \in B$. Ak $y \in B_1$ tak podľa (1c) a (4a) je $y = f(x) = h(x)$ pre nejaké $x \in A_1$. Ak $y \in B_2$ potom podľa (1c) je $x = g(y) \in A_2$ a podľa (4b) je $h(x) = g^{-1}(x) = y$. Teda zobrazenie h je surjektívne zobrazenie množiny A na B.

Veta 2.9.4 Nech A, B, C sú množiny. Ak $|A| \le |B|$ a $|B| < |C|$ (alebo $|A| < |B|$ a $|B| \le |C|$), tak $|A| < |C|$.

Dôkaz: Ak $|A| \le |B|$ a $|B| < |C|$, tak $|A| \le |C|$ vyplýva z vety, ktorú sme dokázali skôr. Keby platilo $|A| = |C|$ a teda aj $|C| \le |A|$, tak dostávame $|C| \le |B|$ a súčasne $|B| < |C|$, podľa Cantorovej-Bersteinovej vety je $|B| = |C|$, čo je v spore s predpokladom vety.

V súlade s tým, čo sme povedali na úvod o mohutnostiach, uvažovali sme vzťah „dve množiny majú rovnakú mohutnosť“ alebo vzťah „mohutnosť jednej množiny je menšia ako mohutnosť druhej množiny“ bez toho, aby sme vedeli čo je to „mohutnosť“. Zatiaľ sme to nepotrebovali a ani to potrebovať nebudeme. V niektorých špeciálnych prípadoch budeme postupovať zdanlivo inak, ale vždy to bude len vyjadrenie (skratka) pre vzťah „mať rovnakú mohutnosť“.

Vo filozofii sa hovorí o definícií abstrakciou, „mohutnosť“ je to čo je spoločné všetkým množinám rovnakej mohutnosti, nepotrebujeme tento pojem mať ako presne definovaný matematický pojem. S podobnou situáciou sa stretávame v bežnom živote často: asi by ste ťažko vysvetlili, čo je to „pekné“, ale viete posúdiť, či je hudba pekná, či sú pekné kvety na lúke, alebo či je pekné dievča, mládenec. „Pekné“ je tá vlastnosť týmto všetkým spoločná. Preto mnohí matematici často pod mohutnosťou množiny A nazývajú symbol, priradený všetkým množinám s rovnakou mohutnosťou ako množina A. Ak sa vrátime do matematiky, môžeme si všimnúť, že nevieme, čo je to prirodzené číslo, ale vieme (aspoň čiastočne), čo je to množina všetkých prirodzených čísel. Príslušné pojmy (mohutnosť, číslo) vieme posúdiť v súvislostiach a nie oddelene.

10 Konečné nekonečné množiny (definícia (ne)konečnej množiny, existencia nekonečných množín, vlastnosti (ne)konečných množín)

Definícia 2.10.4 Množina $\boldsymbol{A}$ sa nazýva **konečná**, ak $|A| < \aleph_0$, t.j. ak $|A| < |N|$. Množina sa nazýva nekonečná, ak nie je konečná.

Definícia 2.10.5 Budeme hovoriť, že množina $\boldsymbol{A}$ **má $\boldsymbol{n}$ prvkov**, písať $|A| = n$, kde $n \in N$, ak $|A| = |N_n|$.

Chceme ukázať, že n prvková množina je konečná. K tomu bude užitočná nasledujúca lema.

Lema 2.10.2 Pre každé $n \in N$ platí

$$|N_n| < |N_{n+1}| \qquad (3)$$

Veta 2.10.4 Ak má množina n prvkov, $n \in N$, tak je konečná.

Veta 2.10.5 Pre $n, m \in N$ je $|N_n| = |N_m|$ vtedy a len vtedy, keď $n = m$.

Lema 2.10.3 Ak $A \subseteq N_n$, tak existuje k také, že $|A| = k$.

Lema 2.10.4 Ak množina $A \subseteq N$ je zhora neohraničená, tak $|A| = |N|$.

Veta 2.10.6 Ak množina A je konečná, tak existuje také prirodzené číslo n, že $|A| = n$.

Dôsledok 1. Množina A je konečná vtedy a len vtedy, ak existuje prirodzené číslo $n \in N$ také, že A má n prvkov.

Veta 2.10.7 Nech A, B sú konečné množiny, $|A| = n$, $|B| = m$.

a) Ak A, B sú disjunktné, tak $|A \cup B| = n + m$

b) $|A \times B| = n \cdot m$

c) $|A^B| = n^m$

Dôsledok 2. Ak A, B sú konečné množiny, potom $A \cup B$, $A \times B$, A^B, $P(A)$ sú konečné množiny .

Dôkaz: Ak A, B sú konečné, aj $B - A$ je konečná. Podľa vety je $|A \cup B| = |A| + |B - A|$. Podobne $|A \times B| = |A| \cdot |B|$ a $|A^B| = |A|^{|B|}$. $P(A)$ je konečná, lebo $|P(A)| = 2^{|A|}$.

11 Spočítateľné a nespočítateľné množiny (zjednotenie a karteziánsky súčin spočítateľných množín, existencia nespočítateľných množín, Cantorova diagonálna metóda)

Definícia 2.11.1 Množina A sa nazýva **spočítateľná**, ak platí $|A| \leq \aleph_0$, t.j. ak existuje prosté zobrazenie množiny A do množiny N – prirodzených čísel. Množina sa nazýva **nespočítateľná**, ak nie je spočítateľná.

Definícia 2.11.2 Budeme hovoriť, že množina **A sa dá zoradiť do postupnosti**, ak existuje zobrazenie množiny N na množinu A, t.j. ak existuje postupnosť $\{a_n\}_{n=0}^{\infty}$ taká, že $A = \{a_n, n \in N\}$.

Veta 2.11.1 Neprázdna množina je spočítateľná vtedy a len vtedy, keď sa dá zoradiť do postupnosti.

Veta 2.11.2 Zjednotenie a karteziánsky súčin dvoch spočítateľných množín sú spočítateľné množiny.

Veta 2.11.3 Zjednotenie spočítateľne mnoho spočítateľných množín je spočítateľná množina.

Príklad 8. Ukážeme, že interval $\langle 0,1 \rangle$ nie je spočítateľná množina.

Dokážeme to sporom, predpokladajme, že interval $\langle 0,1 \rangle$ je spočítateľná množina a možno ho zoradiť do postupnosti

$$\langle 0,1 \rangle = \{a_n, n \in N\}.$$

Každé číslo a_n má dekadický zápis $a_n = \sum_{k=0}^{\infty} a_{nk}.10^{-k-1}$. Ak $a_n \neq 0$, tak vyberieme ten zápis, ktorý nemá samé nuly od určitého miesta, t.j. nie je konečný. Čísla $a_n, n \in N$ môžeme zoradiť do tabuľky – pozri obr.č.2. Teraz použijeme ***metódu Cantorovej diagonály***.

$$\begin{array}{lccccccccc}
a_0 = 0 & a_{00} & a_{01} & a_{02} & a_{03} & a_{04} & \cdots & a_{0n} & \cdots \\
a_1 = 0 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & \cdots & a_{1n} & \cdots \\
. & . & . & . & . & . & & & \\
. & . & . & . & . & . & & & \\
. & . & . & . & . & . & & & \\
a_n = 0 & a_{n0} & a_{n1} & a_{n2} & a_{n3} & a_{n4} & \cdots & a_{nn} & \cdots \\
. & . & . & . & . & . & & . & \\
. & . & . & . & . & . & & . & \\
. & . & . & . & . & . & & . &
\end{array}$$

Obr. 2

Nech $b_n = 9$ ak $a_{nn} = 1$ a $b_n = 1$ ak $a_{nn} \neq 1$. Teda pre každé n platí

$$b_n \neq a_{nn} \qquad (*)$$

Číslo $b = \sum_{k=0}^{\infty} b_k . 10^{-k-1}$ patrí do intervalu $\langle 0,1 \rangle$. Teda existuje $m \in N$, že $b = a_m$. Dekadický zápis čísla b je $0, b_0 \, b_1 \, b_2 \ldots b_n \cdots$ a neobsahuje nulu vôbec. Dekadický zápis čísla a_m je $0, a_{m0} \, a_{m1} \, a_{m2} \cdots a_{mn} \cdots$.Číslo a_m síce môže mať dva rôzne dekadické zápisy, my sme však vybrali ten, ktorý nie je konečný. Ani zápis $0, b_0 \, b_1 \, b_2 \ldots b_n \cdots$ nie je konečný (neobsahuje 0 vôbec). Keďže $a_m = b$, tak z uvedeného vyplýva, že obidva zápisy musia byť totožné, t.j. $b_k = a_{mk}$ pre každé $k \in N$. Pre $k = m$ dostávame

$$b_m = a_{mm} ,$$

čo je spor s (*).

<u>Veta 2.11.4 (Cantorova)</u> Množina všetkých reálnych čísel je nespočítateľná.

<u>Dôkaz</u>: Predpokladajme, že množina R je spočítateľná., keďže $|R| = |(0,1)|$ a $|(0,1)| = |\langle 0,1 \rangle|$, platilo by, že aj interval $\langle 0,1 \rangle$ je spočítateľná množina, čo je spor s predchádzajúcim príkladom.

<u>Existencia nespočítateľných množín:</u>

Cantorova veta????

12 Potenčná množina a jej kardinalita (formulácia Cantorovej vety o potenčnej množine, idea dôkazu, dôsledky pre nekonečné množiny)

<u>***Definícia 2.2.9***</u> Nech je daná množina A. **Potenčnou množinou** množiny A nazveme množinu všetkých podmnožín množiny A. Označenie $P(A)$. Teda

$$P(A) = \{X \mid X \subseteq A\}.$$

<u>***Veta 2.10.3 (Cantor)***</u> Pre každú množinu X platí $|X| < |P(X)|$.

<u>*Dôkaz:*</u> Vieme už, že existuje prosté zobrazenie $f : X \to P(X)$, stačí položiť $f(x) = \{x\}$. Teda $|X| \leq |P(X)|$. Ukážeme, že neplatí rovnosť $|X| = |P(X)|$. Budeme dokazovať sporom. Nech platí $|X| = |P(X)|$. Potom existuje prosté zobrazenie f množiny X na množinu $P(X)$. Uvažujme množinu:

$$E = \{x \in X,\ x \notin f(x)\}.$$

Zrejme $E \subseteq X$ a teda $E \in P(X)$, keďže f je zobrazenie na množinu $P(X)$, tak existuje $k \in X$ taký, že $f(k) = E$. Máme dve možnosti:

1) $k \in E$. Potom podľa definície množiny E platí, že $k \notin f(k)$. To však nie je možné, lebo $f(k) = E$.

Teda nutne platí:

2) $k \notin E$. Keďže $E = f(k)$, tak to znamená, že $k \notin f(k)$. Potom podľa definície množiny E platí $k \in E$. A to je hľadaný spor.

<u>***Dôsledok 1.***</u> Pre každú množinu X platí $|X| < 2^{|X|}$.

<u>***Dôsledok 2.***</u> Neexistuje množina všetkých množín.

<u>*Dôkaz:*</u> Vykonáme sporom. Nech A je množina, ktorá obsahuje všetky množiny, tak každá množina množín je jej podmnožina. Špeciálne $P(A) \subseteq A$. Potom by však bola $|P(A)| \leq |A|$, čo je spor s Cantorovou vetou.

Vzniká otázka, ktoré množiny nazvať konečné a ktoré nazvať nekonečné. Mnohé vlastnosti nekonečna sa ponúkajú za definíciu: napríklad zrejme „nekonečná“ množina R má rovnakú mohutnosť ako „jej časť“ $(0,1)$. To by sa konečnej množine nemalo stať. Za vyše sto rokov bádania v teórii množín sa však ukázalo, že práve uvedená vlastnosť nie je najvhodnejšia pre definíciu. Pojem nekonečna je schovaný vo vlastnostiach prirodzených čísel a princíp matematickej indukcie zaručuje, že ${}_0\aleph$ je v určitom zmysle najmenšie nekonečno.

<u>Dôsledky pre nekonečné množiny:</u>

???