Teoretické základy informatiky

M. Nehéz D. Chudá I. Polický M. Čerňanský

september 2006

Obsah

Kapitola 1

Teória množín

1.1 Základné pojmy a označenia

$P, Q, \ldots$	vlasnosti objektov, t.j. *predikáty*
$a, b, c, \ldots$	jednotlivé objekty (napr. čísla).
$\neg$, **not**	negácia
$\vee$	disjunkcia ("alebo")
$\wedge$	konjunkcia ("súčasne")
$\Rightarrow$	implikácia ("z toho vyplýva")
$\Leftrightarrow$	ekvivalencia ("vtedy a len vtedy")
$\forall$	všeobecný kvantifikátor ("pre všetky ...")
$\exists$	existenčný kvantifikátor ("existuje ...")
$\ln x$	prirodzený logaritmus (so základom e)
$\log x$	dekadický logaritmus
$\lg x$	logaritmus pri základe 2
$\lfloor x \rfloor$	dolná celá časť čísla x
$\lceil x \rceil$	horná celá časť čísla x

1.2 Naivná teória množín

Pojem množiny bol najprv používaný iba intuitívne, prípadne vychádzal z niektorých filozofických pojmov. Nakoniec sa vymedzenie tohto pojmu ustálilo (približne) na nasledujúcej formulácii.

Množina je súhrn nejakých objektov, jednoznačne rozlíšiteľných, ktoré nazývame *prvky*.

Slovo "súhrn" je vágne - poznáme len jeho intuitívny význam. Uvedenú formuláciu preto nemožno považovať za definíciu v pravom slova zmysle.

Množina sa najčastejšie zapisuje dvoma spôsobmi:

- vymenovaním prvkov,
- určením vlastností jej prvkov.

Príklad 1.2.1 *Zápis množiny vymenovaním prvkov.*

$$A = \{a, c, d, f\}$$

Príklad 1.2.2 *Zápis množiny určením vlastností jej prvkov.*
Nech predikáty $P(x)$, $Q(x)$ a $R(x)$ označujú postupne nasledujúce vlastnosti: "x je párne číslo", "$x \geq 1$", "$x \leq 5$". Nech:

$$B = \{\ x \mid P(x) \wedge Q(x) \wedge R(x)\ \}.$$

Potom platí: $B = \{2, 4\}$.

Paradoxy naivnej teórie množín

Russelov paradox. Majme danú nasledujúcu množinu:

$$X = \{\ y \mid y \notin y\ \}.$$

V tomto prípade ide o zápis množiny určením vlastností jej prvkov, pričom predikát $P(y)$ je určený logickou podmienkou $y \notin y$. Neformálne sa táto podmienka vyjadrí takto: "množina y nie je prvkom množiny y". Skúmajme platnosť tvrdenia $X \in X$.

1. Z predpokladu $X \in X$ vyplýva, že X má spĺňať podmienku P, teda že $X \notin X$.
2. Z predpokladu $X \notin X$ zase vyplýva, že X nespĺňa podmienku P, teda $X \in X$.

Obidva prípady sú sporné, z čoho vyplýva, že naivná teória množín je nekorektná. Znamená to, že sa v nej dajú odvodiť sporné tvrdenia.

Po Russellovom paradoxe boli objavené ešte ďalšie paradoxy, napr. Richardov, z r. 1905. Tieto skutočnosti viedli k tomu, že teória množín začala byť budovaná na tzv. axiomatickom princípe. O ňom sa zmienime v nasledujúcej podkapitole.

Vysvetlenie Russellovho paradoxu je jednoduché. Nejde o rozpor, ale sme dokázali, že množina X neexistuje. Presnejšie, X nie je množina.

1.3 Axiomatická teória množín

Axiomatická teória množín sa najčastejšie buduje z axióm, ktoré navrhli E. Zermelo (1871-1956) a A. A. Fraenkel (1891-1956) a zvykne sa označovať skratkou ZF. Okrem nej poznáme aj iné axiomatické systémy, nimi sa však zaoberať nebudeme.

Každý predikát $P(x)$ prirodzeným spôsobom určuje súbor

$$\{x \mid P(x)\} ,$$

ktorý budeme nazývať *trieda.* Nie každá trieda je množina. Vlastnosti množín sú stanovené axiómami, ktoré určujú aj to, akým spôsobom môžeme z už známych množín konštruovať nové množiny.

Axiómy ZF teórie množín

1. Axióma existencie množín
Existuje aspoň jedna množina.

2. Axióma extenzionality
Množiny, ktoré majú tie isté prvky, sa rovnajú.

3. Schéma axióm vydelenia
Z každej množiny je možné vydeliť množinu všetkých prvkov, ktoré spĺňajú danú vlastnosť.

4. Axióma dvojice
Ľubovoľné dve množiny určujú dvojprvkovú množinu.

5. Axióma sumy
Ku každej množine A je daná množina všetkých prvkov, ktoré patria do nejakého prvku množiny A.

6. Axióma potencie
Ku každej množine je daná množina všetkých podmnožín.

7. Schéma axióm nahradenia
Definovateľné zobrazenie zobrazuje množinu na množinu.

8. Axióma nekonečna
Existuje nekonečná množina.

9. Axióma fundovanosti
Axióma fundovanosti sa používa zriedkavo a slovne sa formuluje komplikovane. Jej znenie vynechávame.

Pre samotnú ZF teóriu sú postačujúce axiómy č. 2, 5, 6, 7, 8 a 9, pričom ostatné axiómy sa z týchto dajú odvodiť. Všimnite si, že axióma č. 1 priamo vyplýva z axiómy č. 8.

V ZF teórii množín sú odstránené všetky známe paradoxy. Z uvedených axióm vyplýva, že súbor X z Russellovho paradoxu nie je množina.

Axióma existencie množín zaručuje, že pojem množiny má neprázdny obsah.

Axióma extenzionality určuje význam a vlastnosti dvoch základných symbolov v teórii množín: symbolu $\in$ ("... je prvkom ...") a symbolu rovnosti $=$. Každý objekt (prvok) sa môže v množine vyskytovať iba raz. Na jeho poradí nezáleží.

Definícia 1.3.1 Podmnožina
Množina A je podmnožinou *množiny B, píšeme $A \subseteq B$, ak každý prvok množiny A je aj prvkom množiny B.*

Množina A je vlastnou podmnožinou *množiny B, píšeme $A \subset B$, ak platí:* $A \subseteq B \wedge A \neq B$.

Platí, že každá množina je podmnožinou samej seba. Vzťah označovaný symbolom $\subseteq$ sa nazýva *inklúzia.* Vzťah označovaný symbolom $\subset$ sa nazýva *vlastná inklúzia.*

Definícia 1.3.2 Prázdna množina
Množina, do ktorej nepatrí žiadny prvok, sa nazýva prázdna*, označuje sa $\emptyset$. Teda:*

$$\forall x \quad x \notin \emptyset \ .$$

Existuje jediná prázdna množina.

Lema 1.3.1 *Pre ľubovoľné množiny A, B platí:*

$$A = B \quad \Leftrightarrow \quad A \subseteq B \wedge B \subseteq A \ . \tag{1.1}$$

Zo schémy axióm vydelenia sa odvodzujú množinové operácie prienik a rozdiel.

Definícia 1.3.3 Prienik množín
Prienikom množín *A a B nazývame množinu*

$$A \cap B = \{ \ x \mid x \in A \ \wedge \ x \in B \ \} \ . \tag{1.2}$$

Množiny C, D sa nayývajú *disjunktné*, ak $C \cap D = \emptyset$.

Definícia 1.3.4 Rozdiel množín
Rozdielom množín *A a B nazývame množinu*

$$A \setminus B = \{ \ x \mid x \in A \ \wedge \ x \notin B \ \} \ . \tag{1.3}$$

Alternatívou k použitiu axióm v teórii množín sú pravidlá na konštrukciu množín. Pomocou nich možno z daných množín utvorit' d'alšie množiny. Budeme používat' nasledujúcich pät' princípov tvorby množín.

P1. Ak x, y sú nejaké objekty, tak:

$$\exists X \ \ \forall z \ \ z \in X \quad \Leftrightarrow \quad (z = x \ \vee \ z = y) \ .$$

P2. Ak A, B sú nejaké množiny, tak:

$$\exists C \ \ \forall z \ \ z \in C \quad \Leftrightarrow \quad (z \in A \ \vee \ z \in B) \ .$$

P3. Ak A, B sú nejaké množiny, tak:

$$\exists D \ \ \forall z \ \ z \in D \quad \Leftrightarrow \quad (\exists x \in A)(\exists y \in B) \ z = (x, y) \ .$$

P4. Ak A je množina, tak:

$$\exists E \ \ \forall z \ \ z \in E \quad \Leftrightarrow \quad z \subseteq A \ .$$

P5. Ak A je množina a P je vlastnost' (predikát), tak:

$$\exists F \ \ \forall z \ \ z \in F \quad \Leftrightarrow \quad (z \in A \ \wedge \ P(z)) \ .$$

Uvedené princípy sú odvodené z jednotlivých axióm teórie množín. Konkrétne, princíp P1 je odvodený z axiómy dvojice, princíp P2 je špeciálnym prípadom axiómy sumy, princíp P4 je ekvivalentný s axiómou potencie a princíp P5 je odvodený zo schémy axióm vydelenia.

Z princípov P2 a P3 sa odvodzujú množinové operácie zjednotenia a karteziánskeho súčinu.

Definícia 1.3.5 Zjednotenie množín
Nech A a B sú množiny. Zjednotenie množín *A a B je množina*

$$A \cup B = \{ \ x \mid x \in A \ \vee \ x \in B \ \} \ . \tag{1.4}$$

Operáciu zjednotenia je možné aplikovat' aj viackrát. V takom prípade budeme používat' nasledujúce označenie. Nech k je kladné celé číslo a nech $A_1, \ldots, A_k$ sú množiny. Potom budeme používat' nasledujúce označenie:

$$A_1 \cup \cdots \cup A_k = \bigcup_{i=1}^{k} A_i \ .$$

Definícia 1.3.6 Karteziánsky súčin množín
Nech A a B sú množiny. Karteziánskym súčinom množín *A a B nazývame množinu*

$$A \times B = \{ \ (a,b) \mid a \in A \ \wedge \ b \in B \ \} \ . \tag{1.5}$$

Prvkami množiny $A \times B$ sú *usporiadané dvojice* prvkov, ktoré budeme označovať symbolom (a,b). Ak $a \neq b$, tak $(a,b) \neq (b,a)$. Neusporiadané dvojice prvkov a, b budeme označovať symbolom $\{a,b\}$.

Analogickým spôsobom možno definovať karteziánsky súčin k množín - jeho prvkami sú usporiadané k-tice.

Definícia 1.3.7 Binárna relácia
Nech A a B sú množiny. Ľubovoľnú podmnožinu R karteziánskeho súčinu $A \times B$ budeme nazývať binárnou reláciou*, teda:*

$$R \subseteq A \times B \ .$$

Prvkami relácií sú usporiadané dvojice. Ak $(a,b) \in R$, tak používame tiež zápis aRb. Najdôležitejšou operáciou na binárnych reláciach je kompozícia relácií.

Definícia 1.3.8 Kompozícia relácií
Nech R_1 a R_2 sú binárne relácie. Kompozícia (binárnych) relácií*, označuje sa $R_1 \circ R_2$, skrátene $R_1 R_2$, je definovaná nasledovne:*

$$R_1 \circ R_2 = R_1 R_2 = \{ \ (x,z) \mid \exists y \ \ (x,y) \in R_1 \ \wedge \ (y,z) \in R_2 \ \} \ . \tag{1.6}$$

Ak $R \subseteq A \times A$ pre nejakú množinu A, tak hovoríme, že R je *relácia na množine A*. *Identická relácia* $I = \{ \ (a,a) \mid a \in A \ \}$ je tiež takou reláciou. Pre reláciu R na množine A definujeme operácie *mocniny, reflexívneho a tranzitívneho uzáveru.*

Mocnina relácie R, označuje sa R^i, ak i je nezáporné celé číslo, sa definuje

1. $R^0 = I$,
2. $R^i = R \circ R^{i-1}$ pre $i \geq 1$.

Reflexívny uzáver relácie R je $R^0 \cup R$.

Tranzitívny uzáver relácie R, označuje sa R^+, je:

$$R^+ = \bigcup_{i=1}^{\infty} R^i$$

Reflexívny a tranzitívny uzáver relácie R, označuje sa R^*, je:

$$R^* = \bigcup_{i=0}^{\infty} R^i$$

Špeciálnym prípadom relácií sú zobrazenia (funkcie).

Definícia 1.3.9 Zobrazenie
Nech A a B sú množiny. Binárna relácia $\varphi \subseteq A \times B$ sa nazýva zobrazenie*, ak $\forall x \in A$ a $\forall u \in B$, $\forall v \in B$ platí:*

$$[\ (x,u) \in \varphi \ \wedge \ (x,v) \in \varphi\ ] \Rightarrow u = v\ .$$

Ak $\varphi \subseteq X \times Y$ je zobrazenie, tak píšeme $\varphi : X \to Y$ a $\varphi(x) = y$, ak $(x,y) \in \varphi$ pre $x \in X$ a $y \in Y$.

Zobrazenie $\varphi : X \to Y$ sa nazýva:

- *injektívne*, ak $\forall x_1, x_2 \in X$, $x_1 \neq x_2$ platí: $\varphi(x_1) \neq \varphi(x_2)$,
- *surjektívne*, ak $\forall y \in Y \ \ \exists x \in X$ tak, že $\varphi(x) = y$,
- *bijektívne*, ak je injektívne a súčasne surjektívne.

Analogicky ako pri reláciách, aj pre zobrazenia je možné definovat' ich kompozíciu.

Definícia 1.3.10 Kompozícia zobrazení
Nech $\varphi_1 : X \to Y$ a $\varphi_2 : Y \to Z$ sú zobrazenia. Kompozícia zobrazení *φ_1 a φ_2 je zobrazenie $(\varphi_2 \circ \varphi_1) = \psi : X \to Z$, ak:*

$$\forall x \in X \quad \psi(x) = (\varphi_2 \circ \varphi_1)(x) = \varphi_2(\varphi_1(x))\ . \tag{1.7}$$

Platí, že kompozícia dvoch injektívnych zobrazení je tiež injektívne zobrazenie, dvoch surjektívnych zobrazení je surjektívne zobrazenie a dvoch bijektívnych zobrazení je bijektívne zobrazenie.

Z princípu P4 sa odvodzuje vytvorenie potenčnej množiny.

Definícia 1.3.11 Potenčná množina
Nech A je množina. Potenčná množina $\mathcal{P}(A)$ je množina všetkých podmnožín množiny A, teda:

$$\mathcal{P}(A) = \{\ X \mid X \subseteq A\ \}\ . \tag{1.8}$$

Potenčná množina sa zvykne označovať dvoma spôsobmi: $\mathcal{P}(A)$, alebo 2^A.

Na záver uvedieme niekoľko poznámok k pojmom množina a trieda.
Každý predikát $P(x)$ prirodzeným spôsobom určuje triedu

$$T = \{ \ x \mid P(x) \ \} \ , \tag{1.9}$$

pričom trieda nemusí byť množina.
Z axiómy vydelenia a z princípu P5 vyplýva, že ak A je množina, tak trieda

$$M = \{ \ x \mid x \in A \ \wedge \ P(x) \ \} \tag{1.10}$$

je množina. Pritom podmienka "$x \in A \wedge P(x)$" v (1.10) sa nemôže zoslabiť na tvar vo vzťahu (1.9). Voľbou termu $x \notin x$ za predikát $P(x)$ v (1.9) by sme totiž dostali Russellov paradox.

Uvedomme si, že všetky triedy, o ktorých tvrdíme, že sú množiny, musia byť preukázateľne množinami. Znamená to, že o každej množine by sme mali dokázať, že bola vytvorená korektnými množinovými operáciami. Platí napr., že princípmi P1 až P5 nie je možné zostrojiť súbor X z Russellovho paradoxu. V axiomatickej ZF teórii množín doteraz nie je známy žiaden paradox, preto sa považuje za korektnú.

1.4 Konečné a nekonečné množiny

Existencia aspoň jednej nekonečnej množiny je zaručená axiómou č. 8 - axiómou nekonečna. Ako prvú nekonečnú množinu definujeme množinu prirodzených čísel.

Definícia 1.4.1 Množina prirodzených čísel
Množina prirodzených čísel $\mathbb{N}$ *je najmenšia množina (vzhľadom na inklúziu), pre ktorú platí:*

1. $0 \in \mathbb{N}$,

2. *ak* $x \in \mathbb{N}$, *tak* $(x+1) \in \mathbb{N}$.

Z definície množiny prirodzených čísel je možné odvodiť korektnosť dôkazu matematickou indukciou.

Veta 1.4.1 O matematickej indukcii
Nech $P(x)$ je predikát vyjadrujúci nejakú vlastnosť čísel. Nech $k \in \mathbb{N}$. Predpokladajme, že platí:

1. $P(0)$,

2. *ak* $P(k)$, *tak* $P(k+1)$.

Potom pre všetky $n \in \mathbb{N}$ platí $P(n)$, teda vlastnosť P majú všetky prirodzené čísla.

Ďalšie nekonečné množiny zostrojíme tak, že využijeme vlastnosti množiny prirodzených čísel.

Množina kladných celých čísel $\mathbb{N}^+$

$$\mathbb{N}^+ = \mathbb{N} \setminus \{0\} \tag{1.11}$$

Množina (nezáporných) párnych čísel $\mathbb{E}v$ (*Even*)

$$\mathbb{E}v = \{\ 2 \cdot k \mid k \in \mathbb{N}\ \} \tag{1.12}$$

Množina (kladných) nepárnych čísel $\mathbb{O}dd$

$$\mathbb{O}dd = \{\ 2 \cdot k + 1 \mid k \in \mathbb{N}\ \} \tag{1.13}$$

Množina celých čísel $\mathbb{Z}$

$$\mathbb{Z} = \mathbb{N} \cup \{\ -k \mid k \in \mathbb{N}\ \} \tag{1.14}$$

Definovanie množín všetkých prvočísel, racionálnych čísel a reálnych čísel je komplikovanejšie. My uvedieme ich neformálny opis.

Množina všetkých prvočísel $\mathbb{P}r$
Je to množina všetkých takých čísel z $\mathbb{N}^+$, ktoré majú iba dva rôzne kladné delitele.

Množina racionálnych čísel $\mathbb{Q}$
Každé racionálne číslo sa dá zapísať v tvare *zlomku*, teda v tvare $\frac{p}{q}$, pričom $p \in \mathbb{Z}, q \in \mathbb{N}^+$. Avšak rôzne zlomky môžu vyjadrovať to isté číslo (napr. $\frac{1}{5} = \frac{3}{15}$). Preto sa množina $\mathbb{Q}$ definuje ako množina všetkých zlomkov v tzv. vykrátenom (resp. kanonickom) tvare.

Množina reálnych čísel $\mathbb{R}$
Množina reálnych čísel vznikne tzv. zúplnením množiny racionálnych čísel. Okrem všetkých čísel z $\mathbb{Q}$ obsahuje aj ďalšie čísla, ako napr. $\sqrt{2}, \sqrt{3}, \pi$ a iné.

Pre jednotlivé množiny je vymenovaných niekoľko (resp. niekoľko prvých) prvkov:

- $\mathbb{N}\ \ = \{0,\ 1,\ 2,\ 3,\ 4,\ \dots\}$,
- $\mathbb{N}^+ = \{1,\ 2,\ 3,\ 4,\ 5,\ \dots\}$,
- $\mathbb{E}v = \{0,\ 2,\ 4,\ 6,\ 8,\ \dots\}$,

- $\mathbb{O}dd = \{1,\ 3,\ 5,\ 7,\ 9,\ \dots\}$,
- $\mathbb{P}r = \{2,\ 3,\ 5,\ 7,\ 11,\ \dots\}$,
- $\mathbb{Z}\ = \{\dots, -3, -2, -1, 0,\ 1,\ 2,\ 3,\ \dots\}$.

Lema 1.4.1 *Platí:*

$$\mathbb{P}r \subset \mathbb{N}^+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}\ . \tag{1.15}$$

Množiny $\mathbb{E}v$ a $\mathbb{O}dd$ sú disjunktné (t.j. $\mathbb{E}v \cap \mathbb{O}dd = \emptyset$) a platí, že $\mathbb{E}v \cup \mathbb{O}dd = \mathbb{N}$. Podmnožinami množiny reálnych čísel sú tiež *intervaly.* Poznáme 9 druhov intervalov (pozri cvičenie 1.5.5). Na tomto mieste zavedieme iba jeden z nich - otvorený interval. (Definovanie ostatných ponechávame ako cvičenie.)

Otvorený interval reálych čísel (a, b), ak $a, b \in \mathbb{R}$

$$(a, b) = \{\ x \in \mathbb{R} \mid a < x\ \wedge\ x < b\ \} \tag{1.16}$$

Namiesto pojmu "počet prvkov množiny" budeme používat' termín "mohutnost' množiny". Pri definovaní mohutnosti budeme vychádzat' z pojmu zobrazenia.

Mohutnost' množiny
Symbolom $|A|$ budeme označovat' *mohutnost'* (*kardinalitu*) *množiny* A.

Definícia 1.4.2 Porovnávanie mohutností
Nech A, B *sú množiny. Budeme hovorit', že* množiny A a B majú rovnakú mohutnost'*, ak existuje bijektívne zobrazenie* $\varphi : A \to B$*. Túto skutočnost' budeme zapisovat' označením* $|A| = |B|$ *alebo* $A \approx B$*.*

Aby sme mohli mohutnosti množín porovnávat' efektívnejšie, zavedieme pre mohutnosti ešte aj relácie $\leq$ a $<$.

Definícia 1.4.3 Porovnávanie mohutností
Nech A, B *sú množiny. Budeme hovorit', že množina* A má mohutnost' menšiu alebo rovnakú ako množina B*, píšeme* $|A| \leq |B|$*, ak existuje injektívne zobrazenie* $\psi : A \to B$*.*
Množina A má mohutnost' menšiu ako množina B*, píšeme* $|A| < |B|$*, ak* $|A| \leq |B|$ *a neplatí* $|A| = |B|$*.*

Pomocou relácie $<$ definujeme pojem konečnej množiny.

Definícia 1.4.4 Konečná množina
Množina A *sa nazýva* konečná*, ak* $|A| < |\mathbb{N}|$*.*

Mohutnosť konečných množín je možné vyjadriť prirodzeným číslom. Toto číslo sa rovná tomu, čo intuitívne chápeme ako počet prvkov danej množiny. Exaktne sa tento pojem zavádza nasledujúcim spôsobom.

Nech $k \in \mathbb{N}$. Mohutnosť konečnej množiny A označíme číslom k, píšeme $|A| = k$, ak $|A| = |\{1, 2, \ldots, k\}|$. Mohutnosť prázdnej množiny sa označuje nulou.

Nasledujúca veta vyčísľuje mohutnosť rôznych konečných množín vo vzťahu k niektorým množinovým operáciam.

Veta 1.4.2 *Pre konečné množiny A, B platí:*

$$|A \times B| = |A| \cdot |B| \tag{1.17}$$

$$|A \cup B| \leq |A| + |B| \tag{1.18}$$

$$|A \cap B| \leq \min\{|A|, |B|\} \tag{1.19}$$

$$|A \setminus B| \leq |A| \tag{1.20}$$

$$|\mathcal{P}(A)| = 2^{|A|} \ . \tag{1.21}$$

V ďalšej časti budeme skúmať mohutnosti nekonečných množín. Ako prvý výsledok ukážeme fakt, že množina nepárnych čísel a množina prirodzených čísel majú rovnakú mohutnosť. Táto skutočnosť je v rozpore s našou intuitívnou predstavou, že "menšia množina má menšiu mohutnosť"'.

Príklad 1.4.1 *Dokážeme, že platí* $|\mathbb{O}dd| = |\mathbb{N}|$.
Definujme zobrazenie $\varphi : \mathbb{O}dd \to \mathbb{N}$ tak, že každé nepárne číslo sa zobrazí na dolnú celú časť jeho polovice, t.j.:

$$\varphi(k) = \lfloor k/2 \rfloor \qquad \textit{pre všetky} \quad k \in \mathbb{O}dd \ .$$

Konkrétne, $\varphi(1) = 0$, $\varphi(3) = 1$, $\varphi(5) = 2$, $\varphi(7) = 3$, atď.
Uvedené zobrazenie je bijektívne. (Zdôvodnite, prečo.) Z toho vyplýva, že platí $|\mathbb{O}dd| = |\mathbb{N}|$. □

Napriek tomu, že množiny $\mathbb{O}dd$ a $\mathbb{E}v$ sú vlastnými podmnožinami množiny $\mathbb{N}$, všetky tri majú rovnakú mohutnosť. Podobne $\mathbb{N}^+ \subset \mathbb{N}$, pričom obidve množiny majú rovnakú mohutnosť.

Príklad 1.4.2 *Dokážeme, že platí* $|\mathbb{N}^+| = |\mathbb{N}|$.
Nech $\varphi : \mathbb{N}^+ \to \mathbb{N}$ je zobrazenie, definované ako

$$\varphi(k) = k - 1 \qquad \textit{pre všetky} \ \ k \in \mathbb{N}^+ \ .$$

Zobrazenie φ je bijektívne. (Zdôvodnite.) Z toho vyplýva platnosť rovnosti $|\mathbb{N}^+| = |\mathbb{N}|$. □

Vidíme, že intuitívna predstava "menšia množina má aj menej prvkov", je v prípade nekonečných množín veľmi zavádzajúca. Existuje veľa množín, ktoré majú rovnakú mohutnosť ako množina $\mathbb{N}$. Ich mohutnosť sa, na rozdiel od konečných množín, nedá vyjadriť prirodzeným číslom. Preto budeme mohutnosť množiny $\mathbb{N}$ označovať symbolom $\aleph_0$ (alef nula), čo sa označuje $|\mathbb{N}| = \aleph_0$.

Dokázali sme, že mohutnosť $\aleph_0$ majú okrem množiny $\mathbb{N}$ aj množiny $\mathbb{E}v$, $\mathbb{O}dd$ a $\mathbb{N}^+$. Ďalšou množinou s uvedenou mohutnosťou je množina celých čísel.

Veta 1.4.3 *Platí:* $|\mathbb{N}| = |\mathbb{Z}|$.

Dôkaz Definujme zobrazenie $\varphi : \mathbb{N} \to \mathbb{Z}$ tak, že sa všetky párne čísla z $\mathbb{N}$ zobrazia na nezáporné zo $\mathbb{Z}$ a všetky nepárne čísla z $\mathbb{N}$ sa zobrazia na záporné zo $\mathbb{Z}$. Formálne:

$$\varphi(k) = \begin{cases} k/2\ , & \text{ak } \ k \in \mathbb{E}v \\ -\lceil k/2 \rceil\ , & \text{ak } \ k \in \mathbb{O}dd. \end{cases}$$

Konkrétne: $\varphi(0) = 0$, $\varphi(2) = 1$, $\varphi(4) = 2$, $\ldots$ a tiež: $\varphi(1) = -1$, $\varphi(3) = -2$, $\varphi(5) = -3$, $\ldots$
Nie je ťažké dokázať, že zobrazenie φ je bijektívne. Z toho vyplýva platnosť dokazovanej rovnosti. $\square$

Lema 1.4.2 *Nech A, B sú disjunktné nekonečné množiny, pre ktoré platí:* $|\mathbb{N}| = |A| = |B|$. *Potom platí:*

$$|\mathbb{N}| = |A \cup B|.$$

Dôkaz Z predpokladu $|\mathbb{N}| = |A|$ vyplýva, že existuje bijektívne zobrazenie $\varphi_1 : \mathbb{N} \to A$, ktoré každé prirodzené číslo zobrazí na nejaký prvok z množiny A. Konkrétne, prirodzené číslo $n \in \mathbb{N}$ sa zobrazí na prvok $\varphi_1(n) \in A$. Podobne, z rovnosti $|\mathbb{N}| = |B|$ vyplýva, že existuje bijektívne zobrazenie $\varphi_2 : \mathbb{N} \to B$, ktoré prirodzené číslo $m \in \mathbb{N}$ zobrazí na prvok $\varphi_2(m) \in B$. Keďže množiny A a B sú disjunktné, môžeme definovať nové zobrazenie $\psi : \mathbb{N} \to (A \cup B)$ nasledujúcim spôsobom:

$$\psi(k) = \begin{cases} \varphi_1(k/2), & \text{ak } k \in \mathbb{E}v \\ \varphi_2(\lfloor k/2 \rfloor), & \text{ak } k \in \mathbb{O}dd. \end{cases}$$

Teda platí: $\psi(0) = \varphi_1(0)$, $\psi(2) = \varphi_1(1)$, $\psi(4) = \varphi_1(2)$, $\psi(6) = \varphi_1(3)$, atď.
To znamená, že v zobrazení ψ sa napr. číslo 4 zobrazí na ten prvok z množiny A, na ktorý bolo v zobrazení φ_1 zobrazené číslo 2.
Tiež platí, že $\psi(1) = \varphi_2(0)$, $\psi(3) = \varphi_2(1)$, $\psi(5) = \varphi_2(2)$, $\psi(7) = \varphi_2(3)$, atď.
Zobrazenie ψ je bijektívne. Tým sme dokázali, že platí $|\mathbb{N}| = |A \cup B|$. $\square$

Poznámka 1.4.1 *Tvrdenie z lemy 1.4.2 platí aj vtedy, ak v predpokladoch vynecháme podmienku disjunktnosti množín A a B.*

Ukázali sme, že zjednotením dvoch nekonečných množín s mohutnosťami $\aleph_0$ dostaneme množinu, ktorej mohutnosť je taktiež $\aleph_0$. Analogická situácia nastáva aj v prípade operácie karteziánskeho súčinu. Nasledujúca veta reprezentuje uvedený výsledok v zjednodušenej podobe.

Veta 1.4.4 *Platí:* $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Dôkaz Myšlienka dôkazu je založená na nasledujúcej úvahe. Prvkami množiny $\mathbb{N} \times \mathbb{N}$ sú usporiadané dvojice prirodzených čísel, ktoré usporiadame do dvojrozmernej tabuľky (viď Tabuľka 1.1), ohraničenej ľavým a horným okrajom.

$\mathbb{N} \times \mathbb{N}$	0	1	2	3	$\cdots$
0	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$\cdots$
1	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$\cdots$
2	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$\cdots$
3	$(3,0)$	$(3,1)$	$(3,2)$	$(3,3)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tabuľka 1.1: Usporiadané dvojice z $\mathbb{N} \times \mathbb{N}$.

Prvky v tejto tabuľke očíslujeme prirodzenými číslami tak, aby uvedené očíslovanie reprezentovalo bijektívne zobrazenie $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Dvojiciam v tabuľke budeme priraďovať prirodzené čísla v smere diagonály, zhora-dole a sprava-doľava tak, ako je to naznačené v tabuľke (viď Tabuľka 1.2).

$\mathbb{N}$	0	1	2	3	$\cdots$
0	0	1	3	6	$\cdots$
1	2	4	7	11	$\cdots$
2	5	8	12	17	$\cdots$
3	9	13	18	24	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tabuľka 1.2: Spôsob očíslovania prvkov z $\mathbb{N} \times \mathbb{N}$.

Platí: $f(0,0) = 0$, $f(0,1) = 1$, $f(1,0) = 2$, $f(0,2) = 3$, $f(1,1) = 4$, $f(2,0) = 5$, atď. Funkčný predpis potom možno vyjadriť nasledovne:

$$f(m,n) = \frac{1}{2}(m+n)(m+n+1) + m \ .$$

Takto definované zobrazenie je bijektívne, a teda požadovaná rovnosť je dokázaná. $\square$

Poznámka 1.4.2 *Spôsob očíslovania prvkov z $\mathbb{N} \times \mathbb{N}$ podľa Tabuľky 1.2 nie je jediný. Je možné nájsť nekonečne veľa rôznych očíslovaní.*

Aplikovaním myšlienky dôkazu predchádzajúcej vety je možné dokázať, že aj množina $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ má mohutnosť $\aleph_0$. Matematickou indukciou sa dá dokázať, že aj karteziánsky súčin k množín $\mathbb{N}$ má mohutnosť $\aleph_0$ pre $k \in \mathbb{N}^+$.
Množina všetkých prvočísel a množina racionálnych čísel majú tiež mohutnosť $\aleph_0$. Hovorí o tom nasledujúca veta, ktorú uvádzame bez dôkazu.

Veta 1.4.5 *Platí:*

$$|\mathbb{N}| = |\mathbb{P}r| \ ,$$

$$|\mathbb{N}| = |\mathbb{Q}| \ .$$

Všetky nekonečné množiny, ktoré sme doteraz spomenuli v súvislosti so skúmaním mohutnosti množín, mali rovnakú mohutnosť. Konkrétne sme uviedli, že množiny $\mathbb{E}v$, $\mathbb{O}dd$, $\mathbb{P}r$, $\mathbb{N}^+$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{N} \times \mathbb{N}$ majú mohutnosť $\aleph_0$. Z týchto množín sa napr. operáciami $\cup$ a $\times$ dajú zostrojiť ďalšie množiny s takou istou mohutnosťou. Vzniká preto prirodzená otázka, či existuje vôbec nejaká nekonečná množina, ktorej mohutnosť nie je $\aleph_0$. Nasledujúca veta dáva pozitívnu odpoveď na túto otázku. Ako prvý túto vetu dokázal nemecký matematik Georg Cantor (1845 - 1918) a prvýkrát pri tom použil novú metódu dôkazu, neskôr nazvanú *metóda diagonalizácie.*

Veta 1.4.6 *Mohutnosť množiny prirodzených čísel je menšia ako mohutnosť množiny reálnych čísel, teda platí nasledujúca nerovnosť:*

$$|\mathbb{N}| < |\mathbb{R}| \ .$$

Dôkaz Vetu dokážeme sporom. Sleduje skutočne pôvodný Cantorov dôkaz. Vieme, že $|\mathbb{N}| \leq |\mathbb{R}|$. Predpokladajme, že platí $|\mathbb{N}| = |\mathbb{R}|$ a budeme sa snažiť dostať spor, z ktorého by potom hneď vyplynulo tvrdenie vety. Ak by platilo $|\mathbb{N}| = |\mathbb{R}|$, tak potom z príkladu 1.4.3 máme $(0,1) \approx \mathbb{N}$. To by znamenalo, že interval $(0,1)$ možno zoradiť do postupnosti:

$$(0,1) = \{ \ a_n \mid n \in \mathbb{N}, \ n > 0 \ \} \ .$$

Každé číslo a_n má dekadický zápis

$$a_n = \sum_{k=1}^{\infty} a_{n,k} \cdot 10^{-k} \ .$$

Ak číslo a_n má dva rôzne dekadické zápisy (napr. $\frac{1}{2} = 0,50000\ldots$ a $\frac{1}{2} = 0,49999\ldots$), tak vyberieme nekonečný zápis, t.j. taký, že pre nekonečne veľa k je $a_{n,k} \neq 0$ (ten druhý zápis musí byt' konečný). Čísla a_n a ich dekadické zápisy môžeme zoradit' do nasledujúcej tabuľky:

$$\begin{array}{lllllll}
a_1 & = & 0, & a_{1,1} & a_{1,2} & \dots & a_{1,n} & \dots \\
a_2 & = & 0, & a_{2,1} & a_{2,2} & \dots & a_{2,n} & \dots \\
\vdots & & & \vdots & & \ddots & \vdots & \vdots \\
a_n & = & 0, & a_{n,1} & a_{n,2} & \dots & a_{n,n} & \dots \\
\vdots & & & \vdots & & \vdots & \vdots & \ddots
\end{array}$$

Teraz použijeme metódu diagonalizácie. Zostrojíme číslo

$$b = 0, b_1 b_2 \dots b_n \dots$$

nasledovne. Nech:

$$b_k = \begin{cases} 1\ , & ak \quad a_{k,k} \neq 1 \\ 9\ , & ak \quad a_{k,k} = 1\ . \end{cases}$$

ak $a_{k,k} = 1$ položíme $b_k = 9$; ak $a_{k,k} \neq 1$ položíme $b_k = 1$. Konštrukcia čísla b je znázornená v nasledujúcej tabuľke:

$$\begin{array}{lllllllll}
a_1 & = & 0, & \mathbf{1} & 2 & 3 & \dots & 9 & \dots \\
a_2 & = & 0, & 2 & \mathbf{0} & 1 & \dots & 2 & \dots \\
a_3 & = & 0, & 5 & 2 & \mathbf{4} & \dots & 7 & \dots \\
\vdots & & & \vdots & & & \ddots & & \vdots \\
a_n & = & 0, & 3 & 1 & 2 & \dots & \mathbf{1} & \dots \\
\vdots & & & \vdots & & & \vdots & \vdots & \ddots \\
\hline
b & = & 0, & \mathbf{9} & \mathbf{1} & \mathbf{1} & \dots & \mathbf{9} & \dots
\end{array}$$

Potom číslo b patrí do intervalu $(0,\ 1)$, teda existuje také m, že $a_m = b$. Špeciálne, musí byt' $a_{m,m} = b_m$. Ale číslo b bolo zostrojené tak, aby pre každé k bolo $b_k \neq a_{k,k}$, teda aj $a_{m,m} \neq b_m$. To je hľadaný spor.

Na úplnost' dôkazu si treba ešte uvedomit', že sa nemôže stat', že $0, a_{n,1} a_{n,2} \dots a_{n,n} \dots$ a $0, b_1 b_2 \dots b_n \dots$ sú dva rôzne dekadické zápisy toho istého čísla. Jeden z nich by totiž musel byt' konečný, no prvý nie je konečný podľa dohody a druhý nie je konečný, lebo obsahuje len číslice 1 a 9. □

Uvedená veta patrí medzi jeden z naslávnejších Cantorových výsledkov. Okrem nekonečných množín s mohutnost'ou $\aleph_0$ existuje teda aspoň jedna množina s mohutnost'ou "väčšou" ako $\aleph_0$.

Príklad 1.4.3 $(0, 1) \approx \mathbb{R}$

Dôkaz prevedieme v dvoch krokoch: postupne ukážeme, že

- $(-\pi/2, \pi/2) \approx \mathbb{R}$

- $(0,1) \approx (-\pi/2, \pi/2)$

Pri dôkaze prvého tvrdenia si stačí uvedomit', že funkcia

$$tg : (-\pi/2, \pi/2) \to \mathbb{R}$$

je bijekciou. Na dôkaz druhého tvrdenia si stačí zobrat' lineárnu funkciu

$$f : (0,1) \to (-\pi/2, \pi/2)$$

s predpisom

$$f(x) = \pi \cdot x - \pi/2 \ ,$$

ktorá je tiež samozrejme bijekciou. Zložením týchto dvoch funkcií dostaneme funkciu

$$g(x) = (tg \circ f)(x) = tg(f(x)) = tg(\pi \cdot x - \pi/2) \ ,$$

ktorá zobrazuje interval $(0,1)$ *na* $\mathbb{R}$ *a musí byt' tiež bijekciou.* $\square$

Príklad 1.4.4 *Dokážte, že množiny* $(0,1\rangle \times \{1,2,3\}$ *a* $(0,1\rangle$ *majú rovnakú mohutnost'.*
Zdá sa, že prvá množina má "trikrát viac" prvkov ako druhá, no ukážeme, že to je naozaj len zdanie. Rozdelíme si druhú množinu - interval $(0,1\rangle$ *na tri menšie podintervaly* $(0,\frac{1}{3}\rangle$, $(\frac{1}{3},\frac{2}{3}\rangle$, $(\frac{2}{3},1\rangle$. *Tieto podintervaly sú navzájom disjunktné a ich zjednotením je pôvodný interval* $(0,1\rangle$. *Množina* $(0,1\rangle \times \{1,2,3\}$ *ako keby pozostávala z troch kópií intervalu* $(0,1\rangle$ *a každú z nich bijektívne zobrazíme na jeden z vyššie vymenovaných podintervalov. Využijeme pri tom fakt, že dĺžka intervalov reálnych čísel nehrá pri ich mohutnostiach úlohu. Teda hl'adaná bijekcia* f *bude zjednotením troch zobrazení:*

$$f_1 : (0,1\rangle \times \{1\} \to (0, \frac{1}{3}\rangle$$

$$f_2 : (0,1\rangle \times \{2\} \to (\frac{1}{3}, \frac{2}{3}\rangle$$

$$f_3 : (0,1\rangle \times \{3\} \to (\frac{2}{3}, 1\rangle \ .$$

Predpis pre zobrazenie f *môže potom vyzerat' nasledovne:*

$$f(x,i) = \frac{x+i-1}{3} \ , \quad x \in (0,1\rangle, \ \ i \in \{1,2,3\} \ .$$

L'ahko sa možno presvedčit', že f *je bijektívne zobrazenie, čím je tvrdenie dokázané.*
$\square$

Príklad 1.4.5 *Dokážte, že intervaly* $(0,1\rangle$ *a* $(0,1)$ *majú rovnakú mohutnost'.*
Prvý interval má o jeden prvok "viac" ako druhý, a ten chceme pri hl'adaní bijekcie niekde "stratit'". Zobrazíme číslo 1 na $\frac{1}{2}$. *Tým si vytvoríme nový "dlh", lebo nemáme*

kam zobrazit' $\frac{1}{2}$. *Tú zobrazíme na* $\frac{1}{3}$. *Urobíme si d'alší dlh, no ten vieme splatit' na úkor nového dlhu. Takto budeme pokračovat' do nekonečna. Teda zostrojené zobrazenie bude vyzerat' takto:*

$$f\left(\frac{1}{n}\right) = \frac{1}{n+1} \quad \textit{pre} \quad n = 1, 2, \ldots$$

$$f(x) = x \quad \textit{pre} \quad x \in (0,1\rangle \ , \quad x \neq \frac{1}{n} \ , \quad n = 1, 2, \ldots$$

Zobrazenie f *je bijektívne z* $(0,1\rangle$ *na* $(0,1)$. $\square$

Existuje mnoho príkladov nekonečných množín s mohutnost'ou $\aleph_0$. Taktiež existuje vel'a množín s mohutnost'ou zhodnou s $|\mathbb{R}|$. Patria medzi ne napr. intervaly reálnych čísel. Vzhl'adom k tejto situácii uvedieme definíciu, pomocou ktorej je možné klasifikovat' množiny vo vzt'ahu k ich mohutnosti.

Definícia 1.4.5 Spočítatel'ná a nespočítatel'ná množina
Množina A *sa nazýva* spočítatel'ná, *ak* $|A| \leq |\mathbb{N}|$. *(T. j.* $|A| \leq \aleph_0$*)*
Množina, ktorá nie je spočítatel'ná, sa nazýva nespočítatel'ná.

V nasledujúcom tvrdení dokážeme, že aj množina iracionálnych čísel je nespočítatel'ná.

Veta 1.4.7 *Množina* $\mathbb{R} \setminus \mathbb{Q}$ *iracionálnych čísel je nespočítatel'ná.*

Dôkaz Vetu dokážeme sporom. Predpokladajme, že množina $\mathbb{R}\setminus\mathbb{Q}$ je spočítatel'ná. V tom prípade je bud' konečná alebo nekonečná spočítatel'ná.
Predpokladajme najprv, že množina $\mathbb{R}\setminus\mathbb{Q}$ je konečná. Ked'že podl'a vety 1.4.5 platí, že $|\mathbb{Q}| = \aleph_0$, dalo by sa zostrojit' bijektívne zobrazenie $(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} \to \mathbb{N}$. (Pozri cvičenie 1.5.6.) To by ale znamenalo, že množina $(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$ je nekonečná spočítatel'ná, čo je spor s vetou 1.4.6!

V prípade, keby bola množina $\mathbb{R} \setminus \mathbb{Q}$ nekonečná spočítatel'ná, dostaneme taktiež spor. Množina $\mathbb{Q}$ je nekonečná spočítatel'ná, pričom množiny $\mathbb{Q}$ a $\mathbb{R}\setminus\mathbb{Q}$ sú disjunktné. Podl'a lemy 1.4.2 potom ich zjednotenie, teda množina $\mathbb{R}$, musí byt' spočítatel'ná. Opät' sme dostali spor s vetou 1.4.6! Tým je tvrdenie dokázané. $\square$

Pri skúmaní mohutnosti množín sme dospeli k záveru, že okrem konečných množín poznáme aj nekonečné spočítatel'né a nespočítatel'né množiny. V nasledujúcej schéme sú tieto fakty vyjadrené názornou formou.

$$\text{Množiny} \begin{cases} \text{Spočítateľné} & \begin{cases} \text{Konečné} \\ \text{Nekonečné} \end{cases} \\ \text{Nespočítateľné} & \text{Nekonečné} \end{cases}$$

1.5 Cvičenia

Cvičenie 1.5.1 *Dokážte lemu 1.3.1.*

Cvičenie 1.5.2 *Matematickou indukciou dokážte , že pre každú konečnú množinu* A *platí:* $|\mathcal{P}(A)| = 2^{|A|}$.

Cvičenie 1.5.3 *Na príkladoch konkrétnych množín si overte platnosť vzťahov (1.17) až (1.21) z vety 1.4.2.*

Cvičenie 1.5.4 *Analogickým spôsobom, ako vo vzťahoch (1.11)až (1.14) definujte nasledujúce množiny:*

- *množinu* $\mathbb{E}v^-$ *všetkých záporných párnych čísel,*
- *množinu* $\mathbb{Q}^+$ *všetkých kladných racionálnych čísel,*
- *množinu* $\mathbb{R}^+$ *všetkých kladných reálnych čísel.*

Cvičenie 1.5.5 *Nech* $a, b \in \mathbb{R}$. *Existuje nasledujúcich* 9 *druhov intervalov:*

$$(a,b) \qquad (a,b\rangle \qquad \langle a,b) \qquad \langle a,b\rangle$$

$$(-\infty,b) \qquad (-\infty,b\rangle \qquad (a,\infty) \qquad \langle a,\infty)$$

$$(-\infty,\infty) = \mathbb{R}\ .$$

Analogicky ako bol definovaný otvorený interval (pozri vzťah 1.16), definujte ostatné typy intervalov.
Zistite, medzi ktorými typmi intervalov platí vzťah (vlastnej) inklúzie.

Cvičenie 1.5.6 *Dané sú dve disjunktné množiny,* A *a* B. A *je konečná množina a* B *je nekonečná spočítateľná množina. Dokážte, že platí* $|A \cup B| = \aleph_0$.

Cvičenie 1.5.7 *Analogickým spôsobom ako v príklade 1.4.1 dokážte, že platí* $|\mathbb{E}v| = \mathbb{N}$.

Cvičenie 1.5.8 *Dokážte, že platia nasledujúce vzťahy.*

a) $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$
b) $\mathbb{N}^k \approx \mathbb{N}\ , \quad k \in \mathbb{N}^+$
c) $(\mathbb{N} \times \mathbb{Z}) \approx \mathbb{N}$
d) $(\mathbb{N} \times \mathbb{Z}) \approx \mathbb{Z}$
e) $\mathbb{Q} \approx \mathbb{N}$ *(Využite cvičenie c).)*
f) $\mathbb{P}r \approx \mathbb{N}$

Cvičenie 1.5.9 *Dokážte, že platia nasledujúce vzťahy.*

a) Ak $A = \{\ 7k+1 \mid k \in \mathbb{N}\ \}$, $B = \{\ 7k+5 \mid k \in \mathbb{N}\ \}$, tak $A \cup B \approx \mathbb{N}$

b) Platí $\{\ \alpha k + \beta \mid k \in \mathbb{N}\ \} \approx \mathbb{N}$, ak $\alpha, \beta \in \mathbb{Z}$, $\alpha \neq 0$.

c) $\{\ 5k \mid k \in \mathbb{Z}\ \} \cup \{\ 7k \mid k \in \mathbb{Z}\ \} \approx \mathbb{N}$

d) $\mathbb{N} \times \{2,4,6\} \approx \mathbb{N}$

e) $\mathbb{N} \times \{2,4,6\} \approx \mathbb{Z}$

Cvičenie 1.5.10 *Dokážte, že nasledujúce dvojice množín majú rovnakú mohutnosť.*

a) $(0,1) \approx (0,2)$

b) $(0,1) \approx (a,b)$, ak $a,b \in \mathbb{R}$

c) $\langle 0,1 \rangle \approx \langle a,b \rangle$, ak $a,b \in \mathbb{R}$

d) $(-\frac{\pi}{2}, \frac{\pi}{2}) \approx \mathbb{R}$

e) $(0,1) \approx (0,\infty)$

f) $(0,1) \approx (-\infty,\infty)$

g) $(0,1) \approx (0,2\rangle \cup (4,7)$

h) $\langle 2,3 \rangle \approx \langle 0,1 \rangle \cup (5,8) \cup \langle 10,11 \rangle$

Cvičenie 1.5.11 *Dokážte, že nasledujúce dvojice množín majú rovnakú mohutnosť.*

a) $(0,1) \approx \langle 0,1)$

b) $(0,1) \approx \langle 0,1 \rangle$

c) $(a,b) \approx \langle a,b \rangle$, ak $a,b \in \mathbb{R}$

d) $(0,1\rangle \approx (0,1\rangle \times \{0,1,2,3\}$

e) $(0,1\rangle \approx (0,1\rangle \times \mathbb{N}$

f) $\langle 0,1) \approx \langle 0,1) \times \mathbb{N}$

Cvičenie 1.5.12 *Nech A a B sú spočítateľné množiny také, že $A \cap B = \emptyset$. Dokážte, že $A \cup B$ je tiež spočítateľná množina.*

Cvičenie 1.5.13 *Jednoduchými aritmetickými operáciami dokážte, že platí $\frac{1}{2} = 0.49999\ldots$. Tento fakt sa využíva v dôkaze vety 1.4.6.*

Cvičenie 1.5.14 *Nech $X = \{\ 2^{-k} \mid k \in \mathbb{Z}\ \}$. Dokážte, že množina $\mathbb{R} \setminus X$ je nespočítateľná. (Návod: postupujte podobne ako vo vete 1.4.7.)*

Cvičenie 1.5.15 *Nech $Y = \{\ 7^{-k},\ 3^{2k} \mid k \in \mathbb{Z}\ \}$. Dokážte, že množina $\mathbb{R} \setminus Y$ je nespočítateľná.*

Cvičenie 1.5.16 *Dokážte lemu 1.4.1. Pri dôkaze inklúzie $\mathbb{Q} \subset \mathbb{R}$ využite poznatok, že číslo π nie je racionálne.*

Kapitola 2

Jazyky a gramatiky

Teória formálnych jazykov, ktorú v pät'desiatych rokoch 20. storočia inicioval americký lingvista Noam Chomsky, predstavuje súhrn poznatkov, ktoré sa v informatike uplatňujú najmä pri tvorbe prekladačov a textových procesorov. Na princípoch teórie formálnych jazykov sú založené napr. kompilátory programovacích jazykov, ako aj prehliadače www stránok.

Na abstraktnej úrovni rozlišujeme 3 základné typy jazykov:

- *prirodzené (lingvistické)*,
- *umelé*,
- *formálne.*

Prirodzené jazyky sú jazyky, ktorými sa l'udia dorozumievajú. Do najvýznamnejšej triedy umelých jazykov zarad'ujeme jazyky používané v informatike, ako sú napr. počítačové jazyky, jazyky na tvorbu www stránok, jazyky pre textové procesory (napr. LaTeX) a d'alšie (napr. jazyk Postscript, používaný v súboroch pre tlačiarne). Formálne jazyky sú zjednodušenou podobou predchádzajúcich dvoch typov jazykov, pričom zachytávajú podstatné črty obidvoch typov.

Každý jazyk je možné skúmat' z dvoch hl'adísk. Podl'a toho má každý jazyk svoju:

- *syntax*,
- *sémantiku.*

Syntax jazyka je jeho štruktúra a stavba. Sémantika jazyka je jeho význam a obsah. Kým prirodzené jazyky majú dôraz kladený na svoju sémantiku, pre umelé jazyky je dôležitejšia ich syntaktická stránka.

2.1 Slová a jazyky

Abeceda, označuje sa Σ, je konečná množina prvkov, ktoré nazývame *symboly* alebo *znaky*. *Slovo* (resp. *ret'azec*) nad abecedou Σ je l'ubovol'ná (môže byt' aj opakujúca sa) postupnost' symbolov zo Σ. Slová budeme označovat' najčastejšie písmenami u, v, w, x, y alebo ako postupnosti znakov, teda napr.:

$$w = a_1 a_2 \ldots a_k \ ,$$

kde w je slovo, $k \in \mathbb{N}^+$ a a_i sú symboly z abecedy Σ, kde $i = 1, \ldots, k$.

Podslovo slova u je nejaká jeho čast' po sebe nasledujúcich symbolov. *Prázdne slovo* je slovo, ktoré neobsahuje žiaden znak a budeme ho označovat' ϵ.

Rovnost' slov sa definuje nasledovne. Nech $k, l \in \mathbb{N}^+$ a nech $u = a_1 \ldots a_k$, $v = b_1 \ldots b_l$ sú slová. Platí, že $u = v$, ak $k = l$ a súčasne $a_i = b_i$ pre všetky $i = 1, \ldots, k$.

Naopak, slová u, v *sa nerovnajú* (píšeme $u \neq v$), ak $k \neq l$ alebo existuje také j $(1 \leq j \leq k)$, že $a_j \neq b_j$.

Zret'azenie slov $u = a_1 \ldots a_k$, $v = b_1 \ldots b_l$ je operácia (označuje sa $\cdot$), ktorej výsledkom je slovo $u \cdot v = a_1 \ldots a_k b_1 \ldots b_l$. Ak u, v, w sú l'ubovol'né slová nad danou abecedou Σ, tak operácia zret'azenia splňa nasledujúce vlastnosti:

1. (*uzavretost'*) $u \cdot v$ je tiež slovo nad abecedou Σ,
2. (*asociativita*) $(u \cdot v) \cdot w = u \cdot (v \cdot w)$,
3. (*existencia neutrálneho prvku*) $u \cdot \epsilon = \epsilon \cdot u = u$.

Poznámka 2.1.1 *Z vlastnotí 1-3 vyplýva, že množina všetkých slov nad danou abecedou tvorí tzv.* nekomutatívny monoid. *Ked'že operácia zret'azenia nesplňa komutatívny zákon a ani vlastnost' inverzného prvku, nemôže množina všetkých slov nad danou abecedou tvorit' grupu.*

Nad slovami je možné definovat' aj d'alšie operácie. Operácie *mocnina slova, zrkadlový obraz, dĺžka slova a počet výskytov symbolu* opíšeme pomocou tzv. *induktívnych definícií.* Budeme predpokladat', že je daná nejaká abeceda Σ, nech $a, z \in \Sigma$ a nech u je slovo nad abecedou Σ.

Mocnina slova u, označuje sa u^i, ak $i \in \mathbb{N}$.

1. $u^0 = \epsilon$,
2. $u^i = u^{i-1} \cdot u$ pre $i \in \mathbb{N}^+$.

Špeciálne, ak $b \in \Sigma$ a $k \in \mathbb{N}^+$, tak:

$$\underbrace{b \dots b}_{k} = b^k \ .$$

Zrkadlový obraz slova, označuje sa ^{R}.

1. $\epsilon^R = \epsilon$,
2. $(a \cdot u)^R = u^R \cdot a$.

Slovo, pre ktoré platí $u^R = u$, sa nazýva *palindróm*.

Dĺžka slova, označuje sa $|\_|$.

1. $|\epsilon| = 0$,
2. $|a \cdot u| = 1 + |u|$.

Dĺžka slova spĺňa nasledujúce vlastnosti.

Lema 2.1.1 *Pre všetky slová u, v platí:*

- $|u^R| = u$,
- $|u \cdot v| = |u| + |v|$.

Počet výskytov daného symbolu v slove, označuje sa #.

1. $\#_z \ \epsilon = 0$,
2. $\#_z \ (a \cdot u) = \begin{cases} \#_z \ u, & ak \ \ z \neq a \\ 1 + \#_z \ u, & ak \ \ z = a \ . \end{cases}$

Homomorfizmus nad slovami, označuje sa h, definujeme nasledovne. Ak Σ_1 a Σ_2 sú abecedy, tak homomorfizmus h je zobrazenie z množiny všetkých slov nad abecedou Σ_1 do množiny všetkých slov nad abecedou Σ_2, pričom pre ľubovoľné slová u, v nad abecedou Σ_1 platí:

$$h(u \cdot v) = h(u) \cdot h(v) \ .$$

Každý homomorfizmus spĺňa nasledujúcu vlastnosť.

Lema 2.1.2 *Platí:*

$$h(\epsilon) = \epsilon \ .$$

Pri označovaní operácie zreťazenia sa niekedy zvykne symbol $\cdot$ vynechávať. Preto budeme v nasledujúcom texte často používať označenie:

$$u \cdot v = uv \ .$$

V naseldujúcej časti zevedieme pojem jazyka a operácie nad jazykmi.

Definícia 2.1.1 Jazyk *je množina slov.*

Z definície vyplýva, že všetky poznatky z teórie množín je možné aplikovať aj na jazyky. Napr. podľa mohutnosti môžu byť jazyky konečné a nekonečné (prevažne spočítateľné). Taktiež všetky množinové operácie je možné aplikovať na jazyky. Najčastejšie budeme používať operácie zjednotenia, prieniku, rozdielu, rovnosti, nerovnosti a podmnožín ($\subseteq$ a $\subset$). Okrem týchto operácií zavedieme ďalšie, ktoré sú rozšírením niektorých operácií používaných nad slovami, pre jazyky.

Zreťazenie jazykov, označuje sa "$\cdot$". Nech L_1 a L_2 sú jazyky, potom ich zreťazenie je definované nasledovne:

$$L_1 \cdot L_2 = L_1 L_2 = \{ \ uv \mid u \in L_1, v \in L_2 \ \} \ .$$

Ani pre zreťazenie jazykov neplatí komutatívny zákon, preto je potrebné rozlišovať jazyky $L_1 \cdot L_2$ a $L_2 \cdot L_1$.

Mocnina jazyka L, označuje sa L^i, ak $i \in \mathbb{N}$. Nech L je jazyk, potom:

1. $L^0 = \{\epsilon\}$,
2. $L^i = L^{i-1} \cdot L$ pre $i \in \mathbb{N}^+$.

Kleeneho iterácia alebo *uzáver jazyka* L, označuje sa L^*. Ak L je jazyk, tak:

$$L^* = \bigcup_{i=0}^{\infty} L^i \ .$$

Kladný uzáver jazyka L, označuje sa L^+. Ak L je jazyk, tak:

$$L^+ = \bigcup_{i=1}^{\infty} L^i \ .$$

Doplnok (*komplement*) *jazyka* L, označuje sa L^C. Ak L je jazyk, tak:

$$L^C = \Sigma_L^* \setminus L \ ,$$

kde Σ_L označuje abecedu, nad ktoru sú vytvorené slová z jazyka L. Pre niektoré jazyky je možné doplnok charakterizovať aj iným spôsobom.

Lema 2.1.3 *Nech Σ je abeceda a nech Q je predikát určujúci nejakú vlastnosť slov. Ak je možné jazyk L napísať v tvare*

$$L = \{\ w \in \Sigma^* \mid Q(w)\ \}\ ,$$

tak platí, že:

$$L^C = \{\ w \in \Sigma^* \mid \neg Q(w)\ \}\ .$$

Homomorfizmus jazyka L, označuje sa $h(L)$. Nech Σ_1 a Σ_2 sú abecedy, nech L je jazyk nad abecedou Σ_1 a nech $h : \Sigma_1^* \to \Sigma_2^*$ je homomorfizmus. Potom:

$$h(L) = \{\ h(w) \mid w \in L\ \}\ .$$

2.2 Gramatiky a Chomského hierarchia

Gramatika predstavuje jednu z možností, ako sa konečným spôsobom dá určiť nekonečný jazyk. Pri opise jazykov prostredníctvom gramatík sa využíva tzv. *generatívna paradigma.* Znamená to, že slová jazka sa postupne vytvárajú (generujú) z kratších/jednoduchších na dlhšie/zložitejšie. Použitie gramatík našlo široké uplatnenie pri definovaní umelých (najmä počítačových) jazykov.

Definícia 2.2.1 Frázová gramatika
Frázová gramatika *je štvorica $G = (N, T, P, S)$, kde N a T sú abecedy* terminálnych *resp.* neterminálnych symbolov*, pričom platí: $(N \cap T) = \emptyset$, d'alej*

$$P \subseteq_{KON} \ (N \cup T)^* N (N \cup T)^* \times (N \cup T)^*$$

je konečná množina pravidiel *a $S \in N$ je* počiatočný (štartovací) neterminálny symbol.

Krok odvodenia *v gramatike G je binárna relácia $\Rightarrow_G$ na množine $(N \cup T)^* \times (N \cup T)^*$ definovaná nasledovne:*

$$x \Rightarrow_G y\ ,$$

ak existujú $w_1, w_2 \in (N \cup T)^*$ a pravidlo $(u \to v) \in P$, že platí:

$$x = w_1 u w_2 \qquad a \qquad y = w_1 v w_2\ .$$

Jazyk definovaný gramatikou G *je množina $L(G)$ daná nasledovne:*

$$L(G) = \{\ w \in T^* \mid S \Rightarrow_G^* w\ \}\ ,$$

pričom $\Rightarrow_G^*$ je reflexívny a tranzitívny uzáver relácie $\Rightarrow_G$.

Reťazec $x \in (N \cup T)^*$ sa nazýva *vetná forma* v gramatike $G = (N, T, P, S)$, ak $S \Rightarrow_G^* x$.

Definícia 2.2.2 Chomského hierarchia gramatík
Frázová gramatika *je gramatika v zmysle definície 2.2.1.*
Kontextová gramatika *je taká frázová gramatika, v ktorej všetky pravidlá majú tvar:*

$$u \to v \ , \quad kde \ \ |u| \leq |v| \ .$$

Bezkontextová gramatika *je taká frázová gramatika, v ktorej všetky pravidlá majú tvar:*

$$A \to w \ , \quad kde \ \ A \in N \ , \quad w \in (N \cup T)^* \ .$$

Regulárna gramatika *je taká frázová gramatika, v ktorej všetky pravidlá majú tvar:*

$$A \to wB \ , \quad alebo \quad A \to w \ ,$$

$$kde \quad A, B \in N \ , \quad w \in T^* \ .$$

Chomského hierarchia gramatík indukuje hierarchiu jazykov.

Definícia 2.2.3 Chomského hierarchia jazykov
Jazyk sa nazýva kontextový *(*bezkontextový, *resp.* regulárny*), ak je generovaný kontextovou (bezkontextovou, resp. regulárnou) gramatikou.*
Jazyk sa nazýva rekurzívne vyčísliteľný*, ak je generovaný frázovou gramatikou.*

Pre označenie tried jazkov patriacich do Chomského hierarchie sa používajú nasledujúce symboly:

- $\mathcal{L}_{RE}$ - trieda všetkých rekurzívne vyčísliteľných jazykov,
- $\mathcal{L}_{CS}$ - trieda všetkých kontextových jazykov,
- $\mathcal{L}_{CF}$ - trieda všetkých bezkontextových jazykov,
- $\mathcal{R}$ - trieda všetkých regulárnych jazykov.

Poznámka 2.2.1 *Označenia jednotlivých tried sa odvodzujú z príslušných anglických názvov:*
RE - recursive enumerable,
CS - context sensitive,
CF - context free,
R - regular.

Uvedomme si, že žiadne pravidlo kontextovej gramatiky nemôže generovať jazyk, ktorý by obsahoval prázdne slovo. Naprotitomu všetky ostatné typy gramatík takýto jazyk generovať môžu. Preto zavedieme ešte jednu triedu jazykov, $\mathcal{L}_{CSE}$, ktorá obsahuje spolu so všetkými kontextovými jazyky aj všetky kontextové jazyky obohatené o prázdne slovo.

$$\mathcal{L}_{CSE} = \mathcal{L}_{CS} \cup \bigcup_{L \in \mathcal{L}_{CS}} (L \cup \{\epsilon\}) \ .$$

Veta 2.2.1 *Medzi triedami jazkov Chomského hierarchie platia nasledujúce vzťahy:*

$$\mathcal{R} \subset \mathcal{L}_{CF} \subset \mathcal{L}_{CSE} \subset \mathcal{L}_{RE} \ . \tag{2.1}$$

2.3 Vlastnosti regulárnych a bezkontextových jazykov

Najskôr uvedieme vlastnosti, týkajúce sa regulárnych gramatík a jazykov.

Veta 2.3.1 *Každý konečný jazyk je regulárny.*

Dôsledok 2.3.1 *Umelé jazyky C, C++, Pascal, UML sú nekonečné.*

Poznámka 2.3.1 *Platnosť tohoto dôsledku sa dá rozšíriť aj pre mnoho iných umelých jazykov.*

Veta 2.3.2 *Ku každej regulárnej gramatike G existuje regulárna gramatika G' taká, že platí:*

- *dĺžka pravej strany každého pravidla v G' je nanajvýš 2,*
- $L(G') = L(G)$.

Ďalšie vlastnosti sa vzťahujú k bezkontextovým gramatikám a jazykom.

Veta 2.3.3 *K ľubovoľnej bezkontextovej gramatike G existuje gramatika G' taká, že platí:*

- *G' neobsahuje pravidlo $A \to \epsilon$ pre žiadny neterminálny symbol A,*
- $L(G') = L(G) \setminus \{\epsilon\}$.

Veta 2.3.4 *K ľubovoľnej bezkontextovej gramatike G existuje gramatika G' taká, že platí:*

- G' *neobsahuje pravidlá v tvare* $A \to B$ *pre žiadne neterminálne symboly* A, B,
- $L(G') = L(G)$.

Definícia 2.3.1 *Gramatika* $G = (N, T, P, S)$ *je v* Chomského normálnom tvare, *ak každé pravidlo z* P *má jeden z týchto tvarov:*

1. $A \to BC$, *kde* $A, B, C \in N$, *alebo*
2. $A \to a$, *kde* $A \in N$, $a \in T$, *alebo*
3. $S \to \epsilon$, *pričom* $S \in N$ *sa nevyskytuje na pravej strane žiadneho pravidla.*

Veta 2.3.5 *K ľubovoľnej bezkontextovej gramatike* G *existuje gramatika* G' *v Chomského normálnom tvare taká, že platí:* $L(G') = L(G)$.

Definícia 2.3.2 *Gramatika* $G = (N, T, P, S)$ *je v* Greibachovej normálnom tvare, *ak každé pravidlo z* P *má tvar:*

$$A \to a\beta \ , \quad kde \quad a \in T, \ \beta \in N^* \ .$$

Veta 2.3.6 *K ľubovoľnej bezkontextovej gramatike* G *existuje gramatika* G' *v Greibachovej normálnom tvare taká, že platí:* $L(G') = L(G) \setminus \{\epsilon\}$.

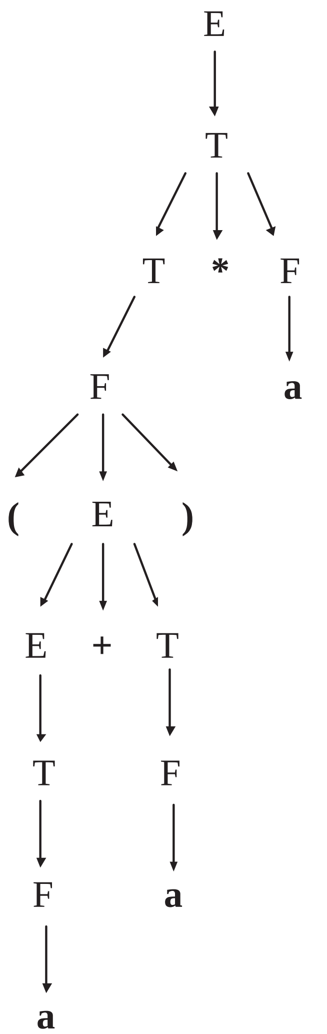
Pojem *strom odvodenia* nebudeme uvádzať definíciou, ale ho znázorníme na príklade.

Príklad 2.3.1 Strom odvodenia
Nech $G_E = (N, T, P, E)$ *je gramatika, kde:*
$N = \{E, T, F\}$, $T = \{a, +, *, (,)\}$, P *sú:*

$$E \to E + T \ | \ T \ ,$$
$$T \to T * F \ | \ F \ ,$$
$$F \to (E) \ | \ a \ .$$

Slovo $(a+a)*a$ *má strom odvodenia znázornený na obrázku 2.3.1. Platí, že ku každému slovu, odvodenému v danej gramatike, existuje nejaký strom odvodenia. Listy každého stromu odvodenia zodpovedajú jednotlivým terminálnym symbolom daného slova, ostatné vrcholy stromu zodpovedajú neterminálnym symbolom v príslušnom odvodení.*

Stromy odvodenia je možné použiť napr. na zisťovanie, či je daná gramatika tzv. viacznačná.



Definícia 2.3.3 Viacznačnosť

Gramatika G sa nazýva viacznačná, *ak existuje slovo* $w \in L(G)$ *s aspoň dvoma rôznymi stromami odvodenia.*

Ak gramatika nie je viacznačná, nazýva sa jednoznačná.

Jazyk je jednoznačný, *ak existuje jednoznačná gramatika, ktorá ho generuje.*

Ak jazyk nie je jednoznačný, nazýva sa vnútorne viacznačný.

Existujú jazyky, ktoré je možné generovať viacerými rôznymi gramatikami, pričom jedna z nich môže byť viacznačná, kým ďalšia naopak jednoznačná. Táto skutočnosť sa musí brať do úvahy, ak máme rozhodnúť, či je nejaký jazyk jednoznačný alebo nie. Ako príklad vnútorne viacznačného jazyka uvádzame jazyk L_V:

$$L_V = \{\ a^i b^j c^j \mid i,j \in \mathbb{N}^+\ \} \cup \{\ a^k b^k c^l \mid k,l \in \mathbb{N}^+\ \}\ .$$

2.4 Riešené príklady

2.4.1 Slová a jazyky

Príklad 2.4.1 *Nech* $L_1 = \{\ w \in \{a,b\}^* \mid \#_b\, w < 2\ \}$*. Ukážeme, že* $L_1 = \{\ a^k \mid k \in \mathbb{N}\ \} \cup \{\ a^i b a^j \mid i,j \in \mathbb{N}\ \}$*.*

$$L_1 = \{\ w \in \{a,b\}^* \mid \#_b\, w < 2\ \} =$$

$$= \{\ w \in \{a,b\}^* \mid \#_b\, w = 0 \vee \#_b\, w = 1\ \} =$$
$$= \{\ w \in \{a,b\}^* \mid \#_b\, w = 0\ \} \cup \{\ w \in \{a,b\}^* \mid \#_b\, w = 1\ \} =$$
$$= \{\ a^k \mid k \in \mathbb{N}\ \} \cup \{\ a^i b a^j \mid i,j \in \mathbb{N}\ \}$$

Príklad 2.4.2 *Nech* $L_2 = \{\ w \in \{a,b\}^* \mid |w| = 3k+1, k \in \mathbb{N}\ \}$*. Ukážeme, že* $L_2^C = \{\ w \in \{a,b\}^* \mid |w| = 3k, k \in \mathbb{N}\ \} \cup \{\ w \in \{a,b\}^* \mid |w| = 3k+2, k \in \mathbb{N}\ \}$*. Použijeme lemu 2.1.3.*

$$L_2^C = \{\ w \in \{a,b\}^* \mid |w| \neq 3k+1, k \in \mathbb{N}\ \} =$$

$$= \{\ w \in \{a,b\}^* \mid |w| = 3k \vee |w| = 3k+2, k \in \mathbb{N}\ \} =$$
$$\{\ w \in \{a,b\}^* \mid |w| = 3k, k \in \mathbb{N}\ \} \cup \{\ w \in \{a,b\}^* \mid |w| = 3k+2, k \in \mathbb{N}\ \}$$

2.4.2 Gramatiky a Chomského hierarchia

Pri vytváraní gramatík pre konkrétne jazyky predvedieme niekoľko rôznych používaných techník, pričom jednotlivé techniky sú často charakteristické pre konkrétnu triedu garamtiky/jazyka v Chomského hierarchii. Tieto techniky sme pomenovali nasledujúcimi názvami:

- *princíp viacerých neterminálnych symbolov,*
- *princíp cyklicky sa opakujúcich neterminálnych symbolov* (regulárne garamatiky),
- *princíp vnútorného neterminálneho symbolu* (bezkontextové gramatiky),
- *princíp znásobovania symbolov,*
- *princíp postupného prepisovania neterminálnych symbolov na terminálne* (kontextové gramatiky).

Regulárne gramatiky

Príklad 2.4.3 *Nech* $G_1 = (N,T,P,A)$*, kde* $N = \{A\}$*,* $T = \{c\}$*,*
$P = \{$

1. $A \to cccA$

2. $A \to \epsilon$

}.
Platí, že $L(G_1) = \{\ c^{3n} \mid n \in \mathbb{N}\ \}$.

Príklad 2.4.4 *Nech* $G_2 = (N, T, P, A)$, *kde* $N = \{A, B, C\}$, $T = \{a, b, c\}$,
$P = \{$

$A \to aA \mid B$

$B \to bB \mid C$

$C \to cC \mid \epsilon$

}.

Platí, že $L(G_2) = \{\ a^i b^j c^k \mid i, j, k \in \mathbb{N}\ \}$.

Príklad 2.4.5 *Nech* $G_3 = (N, T, P, S)$, *kde* $N = \{S\}$, $T = \{a, b\}$,
$P = \{$

$$\begin{array}{llll} S \to aaaS & \mid\ aabS & \mid\ abaS & \mid\ baaS \\ S \to abbS & \mid\ babS & \mid\ bbaS & \mid\ bbbS \\ S \to \epsilon & & & \end{array}$$

}.
Platí, že $L(G_3) = \{\ u \in \{a, b\}^* \mid |u| = 3k, k \in \mathbb{N}\ \}$.

Príklad 2.4.6 *Nech* $G_4 = (N, T, P, A)$, *kde* $N = \{A, B, C, D\}$, $T = \{a, b, c\}$,
$P = \{$

$$\begin{array}{lll} A \to aA & \mid\ bA & \mid\ cB \\ B \to aB & \mid\ bB & \mid\ cC \\ C \to aC & \mid\ bC & \mid\ cD \\ D \to aD & \mid\ bD & \mid\ cA \\ B \to \epsilon & & \end{array}$$

}.
Platí, že $L(G_4) = \{\ u \in \{a, b, c\}^* \mid \#_c u = 4k + 1, k \in \mathbb{N}\ \}$.

Bezkontextové gramatiky

Príklad 2.4.7 *Jazyk* $L_5 = \{\ a^n b^n \mid n \in \mathbb{N}\ \}$ *predstavuje najjednoduchší príklad bezkontextového jazyka. Napíšeme gramatiku, ktorá ho generuje. Nech* $G_5 = (N, T, P, S)$, *kde* $N = \{S\}$, $T = \{a, b\}$,
$P = \{$

1. $S \to aSb$

2. $S \to \epsilon$

}.

Príklad 2.4.8 *Nech* $G_6 = (N, T, P, S)$, *kde* $N = \{S\}$, $T = \{c, d\}$,
$P = \{$
$S \to c^5Sd^3$
$S \to cdd$
}.

Platí, že $L(G_6) = \{\ c^{5n+1}d^{3n+2} \mid n \in \mathbb{N}\ \}$.

Príklad 2.4.9 *Nech* $G_7 = (N, T, P, A)$, *kde* $N = \{A, B\}$, $T = \{1, 2, 3, a, b, c\}$,
$P = \{$
$A \to 1B3$
$B \to aBa$
$B \to bBb$
$B \to cBc$
$B \to 2$
}.

Platí, že $L(G_7) = \{\ 1w2w^R3 \mid w \in \{a, b, c\}^*\ \}$.

Príklad 2.4.10 *Nech* $G_8 = (N, T, P, S)$, *kde* $N = \{S, B\}$, $T = \{a, b\}$,
$P = \{$

1. $S \to aSB$
2. $S \to \epsilon$
3. $B \to b$
4. $B \to bb$

}.

Platí, že $L(G_8) = \{\ a^ib^j \mid i \leq j \leq 2i,\ i \in \mathbb{N}\ \}$.

Príklad 2.4.11 *Nech* $G_9 = (N, T, P, S)$, *kde* $N = \{S, A, B\}$, $T = \{a, b, c, d, 5, 6\}$,
$P = \{$

1. $S \to A56B$
2. $A \to aAb$

3. $A \to \epsilon$

4. $B \to cBd$

5. $B \to \epsilon$

}.

Platí, že $L(G_9) = \{\ a^i b^i 56 c^j d^j \mid i, j \in \mathbb{N}\ \}$.

Kontextové gramatiky

Príklad 2.4.12 *Jazyk* $L_{10} = \{\ a^n b^n c^n \mid n \in \mathbb{N}^+\ \}$ *je typický kontextový jazyk. Napíšeme gramatiku, ktorá ho generuje.*
Nech $G_{10} = (N, T, P, S)$, *kde* $N = \{S, A, B, C\}$, $T = \{a, b, c\}$,
$P = \{$

1. $S \to aBC$

2. $S \to aSBC$

3. $CB \to BC$

4. $aB \to ab$

5. $bB \to bb$

6. $bC \to bc$

7. $cC \to cc$

}.

2.4.3 Vlastnosti regulárnych a bezkontextových jazykov

Príklad 2.4.13 *Nech* $G_{11} = (N, T, P, A)$, *kde* $N = \{A, B\}$, $T = \{a, b\}$,
$P = \{$
$A \to \epsilon$
$A \to a^3 B$
$B \to b^2 A$
}.
Platí, že $L(G_{11}) = \{\ (aaabb)^n \mid n \in \mathbb{N}\ \}$.

Príklad 2.4.14 *Gramatika G_9 z príkladu 2.4.11 generuje jazyk*

$$\{\ a^i b^i 56 c^j d^j \mid i, j \in \mathbb{N}\ \}\ .$$

Táto gramatika je bezkontextová a obsahuje 2 tzv. epsilonové pravidlá, konkrétne:

$$A \to \epsilon\ , \qquad B \to \epsilon\ .$$

Podľa vety 2.3.3 sa G_9 dá upraviť tak, aby neobsahovala epsilonové pravidlá. Výsledkom je gramatika $G_{12} = (N, T, P, S)$, kde $N = \{S, A, B\}$, $T = \{a, b, c, d, 5, 6\}$,
$P = \{$

$$\begin{array}{lllll} S \to A56B & \mid\ A56 & \mid\ 56B & \mid\ 56 \\ A \to aAb & \mid\ ab \\ B \to cBd & \mid\ cd \end{array}$$

$\}$.

Platí, že $L(G_{12}) = \{\ a^i b^i 56 c^j d^j \mid i, j \in \mathbb{N}\ \}$.

Príklad 2.4.15 *Nech $G_{13} = (N, T, P, S)$, kde $N = \{S\}$, $T = \{a,$ `if`, `else`, $1, (,)\}$,*
$P = \{$

$S \to$ `if` $(1)\ S$

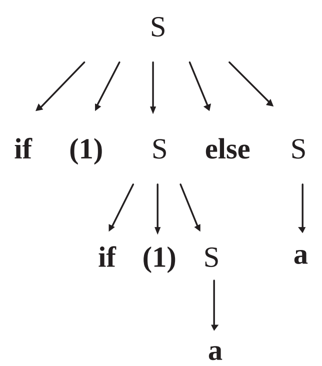
$S \to$ `if` $(1)\ S$ `else` S

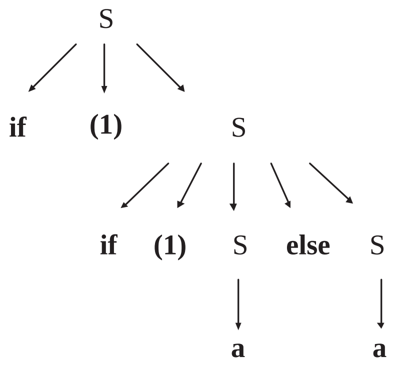
$S \to a$

$\}$.
Dokážeme, že gramatika G_{13} je viacznačná. Viacznačnosť vyplýva z faktu, že pre slovo

`if` (1) `if` $(1)\ a$ `else` a

existujú dva rôzne stromy odvodenia. Znázornené sú na obrázkoch 2.4.15 a 2.4.15.





2.5 Cvičenia

Cvičenie 2.5.1 *Dokážte lemu 2.1.2.*

Cvičenie 2.5.2 *Dokážte, že nasledujúce jazyky sú regulárne.*

a) $L_1 = \{\ a^i b^j \mid i, j \in \mathbb{N}^+\ \}$

b) $L_2 = \{\ a^i b^j c^k d^n \mid i, k \in \mathbb{N}^+, j, n \in \mathbb{N}\ \}$

c) $L_3 = \{\ u \in \{1, 2, 3, 4, 5\}^* \mid |u| = 2k + 1, k \in \mathbb{N}\ \}$

d) $L_4 = \{\ u \in \{0, 1, 2\}^* \mid |u| = 5k, k \in \mathbb{N}\ \} \cup$
$\cup\ \{\ u \in \{0, 1, 2\}^* \mid |u| = 5k + 1, k \in \mathbb{N}\ \}$

e) $L_5 = \{\ u \in \{a, b, c, d\}^* \mid \#_b u = 2k, k \in \mathbb{N}\ \}$

f) $L_6 = \{\ u \in \{a, b, c, d\}^* \mid \#_c u + \#_d u = 5k + 2, k \in \mathbb{N}\ \}$

Cvičenie 2.5.3 *Je daná gramatika* $G = (N, T, P, A)$*, kde* $N = \{A\}$*,* $T = \{0, 1, 2\}$*,* $P = \{$

$A \to x, \quad x \in \{0, 1, 2\}^3$

$A \to yA, \quad y \in \{0, 1, 2\}^5$

$\}$

1. *Zistite, do akej triedy v Chomského hierarchii patrí gramatika* G*.*
2. *Zistite, aký jazyk generuje gramatika* G*.*
3. *Napíšte garamatiku* G' *tak, aby dĺžka pravej strany každého pravidla v* G' *bola nanajvýš* 2 *a súčasne platilo, že* $L(G') = L(G)$*.*

Cvičenie 2.5.4 *Napíšte gramatiky, ktoré vytvárajú nasledujúce číselné množiny. Zdôvodnite, že všetky garmatiky sú regulárne. (Ako terminálne symboly použite vhodné číslice/cifry.)*

1. *Všetky čísla v štvorkovej číselnej sústave.*
2. *Všetky čísla v dvojkovej číslenej sústave deliteľné dvoma.*
3. *Všetky čísla v desiatkovej číslenej sústave deliteľné piatimi.*
4. *Všetky čísla v desiatkovej číslenej sústave deliteľné štyrmi.*
5. *Všetky čísla v sedmičkovej číslenej sústave začínajúce sa ciframi* $2, 4, 6$ *a končiace sa ciframi* $1, 3, 5$.
6. *Všetky čísla v desiatkovej číslenej sústave deliteľné tromi.*

Cvičenie 2.5.5 *Alternatívna definícia regulárnej gramatiky obmedzuje jej pravidlá na nasledujúce dva tvary:*

$$A \to Bw \ , \quad \textit{alebo} \quad A \to w \ ,$$

$$\textit{kde} \quad A, B \in N \ , \quad w \in T^* \ .$$

Dokážte, že ak by nejaká gramatika obsahovala súčasne pravidlá nasledujúcich troch typov:

$$A \to wB \ , \qquad A \to Bw \ , \qquad A \to w \ ,$$

$(A, B \in N, w \in T^*)$*, tak by už mohla generovať aj iný ako regulárny jazyk. Pri dôkaze využite fakt, že nasledujúce dva jazyky sú bezkontextové:*

$L_1 = \{ \ a^n b^n \mid n \in \mathbb{N} \ \}$,
$L_2 = \{ \ ww^R \mid w \in \{a, b\}^* \ \}$.

Cvičenie 2.5.6 *Pre nasledujúce jayzky napíšte gramatiky, ktoré ich generujú. Zistite, do akej triedy v Chomského hierarchii tieto gramatiky patria.*

a) $L_1 = \{ \ a^n b^n \mid n \in \mathbb{N}^+ \ \}$
b) $L_2 = \{ \ 0^{4i+3} a^j c b^j 1^{3i} \mid i, j \in \mathbb{N} \ \}$
c) $L_3 = \{ \ ww^R \mid w \in \{a, b\}^+ \ \}$
d) $L_4 = \{ \ wcw^R \mid w \in \{1, 2, 3, 4\}^* \ \}$
e) $L_5 = \{ \ uw \mid u \in \{a, c\}^*, \ v \in \{b, c\}^*, \ \#_a u = \#_b v \ \}$
f) $L_6 = \{ \ w \in \{a, b, c\}^* \mid \#_a w = \#_b w + \#_c w \ \}$
g) $L_7 = \{ \ awbw^R cudu^R \mid w \in \{1, 2, 3\}^*, u \in \{4, 5\}^* \ \}$
h) $L_8 = \{ \ 2^i 3^{2i} ab 4^j 5^{3k} 6^k 7^j \mid i, j \in \mathbb{N} \ \}$

Cvičenie 2.5.7 *Nech* $h : \{c, d\}^* \to \{4, 6\}^*$ *je nasledújuci homomorfizmus:*

$$h(c) = 4 \ , \qquad h(d) = 6 \ .$$

Napíšte gramatiky, ktoré generujú nasledujúce jayzky.

a) $L_1 = \{\ u^R h(u) \mid u \in \{c,d\}^*\ \}$
b) $L_2 = \{\ uh(u^R)avh(v^R) \mid u \in \{c,d\}^*,\ v \in \{c,d\}^+\ \}$
c) $L_3 = \{\ 9a^{2n}w0h(w^R)b^{3n}87 \mid n \in \mathbb{N},\ w \in \{c,d\}^*\ \}$

Cvičenie 2.5.8 *Nech $\alpha, \beta \in \mathbb{N}^+$ sú parametre. Napíšte gramatiky, ktoré generujú nasledujúce jazyky.*
a) $L_1 = \{\ a^{\alpha n} b^{\beta n} \mid n \in \mathbb{N}^+\ \}$
b) $L_2 = \{\ c^{\alpha n+1} b^{\beta n+2} \mid n \in \mathbb{N}\ \} \qquad (\alpha > 1, \beta > 2)$

Cvičenie 2.5.9 *Je daná gramatika $G = (N, T, P, S)$, kde $N = \{S, A, B\}$, $T = \{0, 1\}$,*
$P = \{$

$$\begin{array}{lll} S \to 0B & \mid 1A & \mid \epsilon \\ A \to 0S & \mid 1AA & \\ B \to 1S & \mid 0BB & \end{array}$$

$\}$.

1. *Zistite, do akej triedy v Chomského hierarchii patrí gramatika G.*
2. *Zdôvodnite, že platí: $L(G) = \{\ w \in \{0,1\}^* \mid \#_0 w = \#_1 w\ \}$.*
3. *Napíšte garamatiku G' tak, aby neobsahovala žiadne ëpsilonové"pravidlá a súčasne platilo, že $L(G') = L(G) \setminus \{\epsilon\}$.*

Cvičenie 2.5.10 *Pre nasledujúce jayzky napíšte gramatiky, ktoré ich generujú. Zistite, do akej triedy v Chomského hierarchii tieto gramatiky patria.*
a) $L_1 = \{\ a^n b^n c^n \mid n \in \mathbb{N}, n \geq 2\ \}$
b) $L_2 = \{\ a^{2n} b^n c^n \mid n \in \mathbb{N}^+\ \}$
c) $L_3 = \{\ a^n b^{3n} c^n \mid n \in \mathbb{N}^+\ \}$
d) $L_4 = \{\ a^{3n} b^{2n} c^n \mid n \in \mathbb{N}^+\ \}$
e) $L_5 = \{\ a^n b^n c^n d^n \mid n \in \mathbb{N}^+\ \}$
f) $L_6 = \{\ a^n b^n c^{2n} d^n \mid n \in \mathbb{N}^+\ \}$

Cvičenie 2.5.11 *Pre nasledujúce jayzky napíšte gramatiky, ktoré ich generujú. Zistite, do akej triedy v Chomského hierarchii tieto gramatiky patria.*
a) $L_1 = \{\ a^i b^j c^i d^j \mid i, j \in \mathbb{N}^+\ \}$
b) $L_2 = \{\ a^{2i} b^j c^i d^j \mid i, j \in \mathbb{N}^+\ \}$
c) $L_3 = \{\ a^i b^{2j} c^{3i} d^{2j} \mid i, j \in \mathbb{N}^+\ \}$

Cvičenie 2.5.12 *Pre nasledujúci jazyk napíšte takú gramatiku, aby dĺžka pravej strany každého pravidla bola nanajvýš 4.*

$$L = \{\ a^n b^{2n} c^n \mid n \in \mathbb{N}^+\ \}$$

Cvičenie 2.5.13 *Je daná gramatika* $G = (N, T, P, S)$, *kde* $N = \{S, A, B\}$, $T = \{a\}$,
$P = \{$

$$\begin{array}{lll} S \to aAaBa & \mid & a \\ A \to aS & \mid & a \\ B \to S & \mid & a \end{array}$$

$\}$.
Dokážte, že G *je viacznačná.*

Cvičenie 2.5.14 *Vymyslite* 5 *rôznych viacznačných gramatík. O každej dokážte, že je viacznačná.*

Cvičenie 2.5.15 *Je daná gramatika* $G = (N, T, P, S)$, *kde* $N = \{S, A, B\}$, $T = \{a\}$,
$P = \{$

$$\begin{array}{lllll} S \to abA & \mid & & & \\ A \to cS & \mid & dbB & \mid & b \\ B \to cBd & \mid & bA & \mid & cA \end{array}$$

$\}$.
Nájdite homomorfizmus h *tak, aby gramatika* $G' = (N, h(T), P', S)$ *bola viacznačná. Množina* P' *vznikne z množiny* P *aplikovaním homomorfizmu* h *na každý terminálny symbol z* T.

Cvičenie 2.5.16 *Dokážte, že jazyk* L_V *je vnútorne viacznačný, ak platí:*

$$L_V = \{\ a^i b^j c^j \mid i, j \in \mathbb{N}^+\ \} \cup \{\ a^k b^k c^l \mid k, l \in \mathbb{N}^+\ \}\ .$$

(Návod: najprv napíšte gramatiku, ktorá generuje L_V*).*

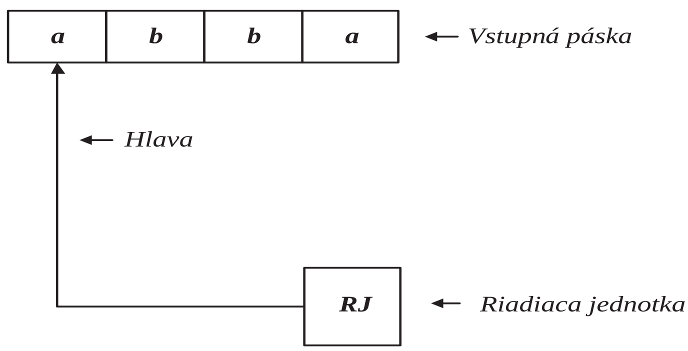
Kapitola 3

Konečné automaty a regulárne jazyky

Jazyky môžeme reprezentovať troma spôsobmi:

- množinami,
- gramatikami,
- výpočtom.

V tejto kapitole opíšeme spôsob reprezentácie jazyka výpočtom. Výpočtový model, ktorý budeme používať, bude reprezentovaný konečným automatom.



Obrázok 3.1: Schéma konečného automatu.

Schéma konečného automatu je zobrazená na obr.1 a pozostáva z nasledujúcich častí:

- riadiaca jednotka,
- čítacia hlava, čítajúca symboly, každý symbol raz,
- vstupná páska.

3.1 Deterministické konečné automaty

Rozlišujeme dva druhy konečných automatov:

- deterministické,
- nedeterministické.

Ako prvý formálne opíšeme deterministický konečný automat.

Definícia 3.1.1 Deterministický konečný automat
Deterministický konečný automat *(DFA - deterministic finite automaton) je pätica* $A = (K, \Sigma, \delta, q_0, F)$, *kde:*
K *je konečná množina stavov,*
Σ *je vstupná abeceda,*
δ *je prechodová funkcia, pričom platí*

$$\delta : K \times \Sigma \to K$$

$q_0 \in K$ *je počiatočný stav,*
$F \subseteq K$ *je množina koncových (akceptačných) stavov.*
Konfigurácia deterministického konečného automatu *je dvojica*

$$(q, w) \ \in \ K \times \Sigma^*,$$

kde:
q *je momentálny stav,*
w *je zvyšok vstupu.*
Krok výpočtu deterministického konečného automatu *je relácia* $\vdash_A$ *na konfigurácii definovaná nasledovne:*

$$(q, au) \vdash_A (p, u), \qquad ak \qquad \delta(q, a) = p,$$

pričom $p, q \in K$, $a \in \Sigma \cup \{\epsilon\}$, $u \in \Sigma^*$.
Jazyk rozpoznávaný deterministickým konečným automatom *(koncovým stavom) je množina*

$$L(A) = \{ \ w \in \Sigma^* \mid (q_0, w) \vdash_A^* (q, \epsilon), \ q \in F\}.$$

Riešené príklady

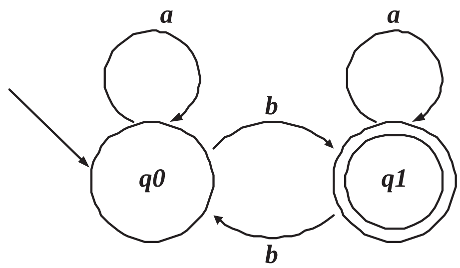
Konečný automat môžeme reprezentovať':

- stavovým diagramom,

- formálnym zápisom,
- maticou prechodových funkcií.

Ukážeme si to na nasledujúcom príklade.

Príklad 3.1.1 *Deterministický konečný automat A_1 je definovaný nasledujúcim stavovým diagramom:*



Obrázok 3.2: Deterministický konečný automat A_1.

Konečný automat graficky reprezentujeme stavovým diagramom, v ktorom sú jednotlivé stavy graficky znázornené kružnicami. Každý stav má svoje jednoznačné označenie. Koncové stavy sú reprezentované dvoma sústrednými kružnicami. Konečný automat na obrázku 3.2 má dva stavy q_0, q_1, pričom stav q_1 je koncový stav. Počiatočný stav je reprezentovaný počiatočnou šipkou. V našom prípade je to počiatočný stav q_0. Stavy sú navzájom graficky spojené šipkami, ktoré reprezentujú prechodovú funkciu δ .

Konečný automat A_1 môžeme opísať' nasledujúcim formálnym zápisom.
Nech $A_1 = (K, \Sigma, \delta, q_0, F)$, kde:
$K = \{q_0, q_1\}$,
$\Sigma = \{a, b\}$,
$\delta(q_0, a) = q_0$
$\delta(q_0, b) = q_1$
$\delta(q_1, a) = q_1$
$\delta(q_1, b) = q_0$
$F = \{q_1\}$.

Konečný automat A_1 môžeme opísať' maticou prechodových funkcií.

	a	b
q_0	q_0	q_1
q_1	q_1	q_0

V jednotlivých riadkoch je prepísaná prechodová funkcia automatu A_1. *V prvom riadku matice prechodových funkcií sú jednotlivé znaky, ktoré sa môžu nachádzať na vstupe. V prvom stĺpci matice prechodových funkcií sú jednotlivé stavy automatu. V druhom riadku matice prechodových funkcií si môžeme všimnúť, že ak sa automat nachádza v stave* q_0 *a na vstupe analyzuje znak a zostáva v stave* q_0, *ak sa automat nachádza v stave* q_0 *a na vstupe analyzuje znak b prechádza do stavu* q_1. *Tretí riadok je analogický pre stav* q_1.

Opíšme si ako je realizovaný výpočet deterministického konečného automatu A_1. *V stavovom diagrame šipky reprezentujú prechodovú funkciu* δ. *Pri každej šipke je naznačený nejaký znak vstupnej abecedy* Σ. *Predpokladajme, že automat je v stave* q_0 *a na vstupe je znak a, potom automat zostáva v stave* q_0, *ak je na vstupe znak b, tak automat prechádza do nasledovného stavu v smere šipky, do stavu* q_1. *Ak je na vstupe slovo abbb, tak deterministický konečný automat* A_1 *prechádza z počiatočného stavu* q_0 *nasledovnou postupnosťou stavov:* q_0,q_1,q_0,q_1, *čo je akceptujúci koncový stav. Automat akceptuje slovo vtedy, ak je prečítané celé slovo zo vstupu a automat sa nachádza v jednom z koncových stavov.*
Stavový diagram korešponduje s formálnym zápisom a využíva sa na grafické znázornenie konečného automatu. Pri formálnom zápise podľa definície 3.1.1, definujeme súvis prechodovej funkcie a kroku výpočtu, pričom a je čítaný znak a u je zvyšok slova na vstupe, p a q sú jednotlivé stavy. Pričom ľubovolný akceptujúci výpočet končiaci v koncovom stave predstavuje slovo patriace do jazyka $L(A)$ *rozpoznávaného automatom A.*
Pri formálnom zápise môžeme opísať výpočet ako postupnosť krokov výpočtu, postupnosť jednotlivých relácií. Predpokladajme, že na vstupe je slovo abbb , ktoré čítacia hlava číta zľava doprava po jednom znaku. Simulovanie výpočtu automatu A_1 *pre vstupné slovo abbb je vyjadrené nasledujúcou postupnosťou krokov:*

$$(q_0, abbb) \vdash (q_0, bbb) \vdash (q_1, bb) \vdash (q_0, b) \vdash (q_1, \epsilon).$$

Základná myšlienka činnosti automatu A_1 *spočíva v tom, že pri čítaní vstupného (páskového) symbolu a v počiatočnom stave* q_0, *zostáva v stave* q_0 *a pri čítaní páskového symbolu b sa preklopí do stavu* q_1. *Pri ďalšom čítaní páskového symbolu b sa preklopí do stavu* q_0 *a pri poslednom čítaní páskového symbolu b sa preklopí do stavu* q_1. *Ak na vstupe už nie je žiadny symbol a automat sa nachádza v stave* q_1 *(ktorý je koncovým stavom), tak môžeme konštatovať, že automat akceptuje slovo abbb, pretože po prečítaní celého slova sa dostal do akceptujúceho stavu. Slovo abbb patrí do jazyka* L_1 *rozpoznávaného automatom* A_1.
Predpokladajme, že je na vstupe slovo abba. Simulovanie výpočtu automatu A_1 *pre vstupné slovo abba je vyjadrené nasledujúcou postupnosťou krokov:*

$$(q_0, abba) \vdash (q_0, bba) \vdash (q_1, ba) \vdash (q_0, a) \vdash (q_0, \epsilon).$$

Ak na vstupe už nie je žiadny symbol a po prečítaní slova abba sa automat nachádza v stave q_0, *ktorý nie je koncovým stavom, tak automat neakceptuje, resp. dané slovo*

abba zamietne. Platí, že slovo abba nepatrí do jazyka L_1 rozpoznávaného automatom A_1.
Keď analyzujeme jednotlivé slová na vstupe, vidíme, že automat A_1 rozpoznáva slová, v ktorých je počet znakov b nepárny.

$$A(L_1) = \{\ w \in \{a,b\}^* \mid \#_b w = 2k+1,\ k \in \mathbb{N}\ \}$$

V nasledujúcich príkladoch budeme automaty reprezentovať iba stavovým diagramom.

Nasledujúca formálna formulácia vyjadruje všeobecný postup konštrukcie konečného automatu z jazyka.

Lema 3.1.1 *Formálna formulácia postupu konštrukcie konečného automatu z jazyka. Nech Σ je vstupná abeceda, $\alpha,\ \beta \in \mathbb{N}$,*

$$L = \{\ w \in \Sigma^* \mid f(a_1, a_2, ..., a_s) = \alpha k + \beta,\ k \in \mathbb{Z}\ \}, s \leq |\Sigma|, 0 \leq \beta < \alpha,$$

potom $A = (K, \Sigma, \delta, q_0, F)$, $|K| = \alpha$, $F = \{q_\beta\}$, $|\delta| = \alpha.|\Sigma|$.

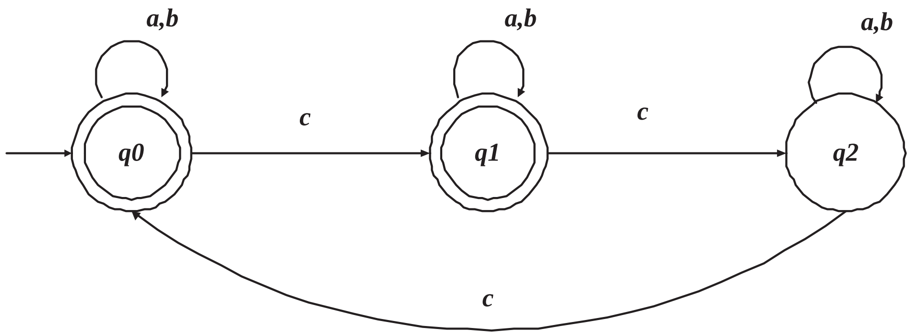
V popise jazyka vystupuje obmedzujúca podmienka $f(a_1, a_2, ..., a_s) = \alpha k+\beta$. Obmedzujúca podmienka je v tvare rovnosti, pričom jej ľavá strana je tvorená výrazom obsahujúcim výskyty jednotlivých znakov. Pravá strana je (lineárny) výraz v tvare $\alpha k + \beta$, kde α, β sú nezáporné celočíselné koeficienty, pričom $0 \leq \beta < \alpha$. Postup konštrukcie deterministického konečného automatu pozostáva z nasledovných krokov:

- určíme počet stavov, ak konštruujeme konečný automat rozpoznávajúci takýto jazyk, tak počet jeho stavov sa rovná koeficientu α.

- určia sa koncové stavy, ak stavy označujeme q_0, q_1, ..., $q_\alpha - 1$, tak koncový stav je určený koeficientom β, tak, že $q_\beta \in F$.

- konštruujeme prechodovú funkciu, realizujú sa prechody pre jednotlivé znaky. V prípade, že v ľavej strane obmedzujúcej podmienky sa daný znak vyskytuje s koeficientom nula, prechodová funkcia zostáva v tom istom stave, ak sa daný znak vyskytuje s koeficientom +1 prechodová funkcia sa preklápa do nasledovného stavu, ak sa ak sa daný znak vyskytuje s koeficientom -1 prechodová funkcia sa preklápa do predošlého stavu, ak sa daný znak vyskytuje s koeficientom +2 prechodová funkcia sa preklápa ob 2 do nasledovného stavu, s výskytmi ďalších znakov konštruujeme prechodovú funkciu analogicky.

Formálnu formuláciu postupu konštrukcie konečného automatu z jazyka si ukážeme v nasledujúcom príklade.



Obrázok 3.3: Konečný automat A_2.

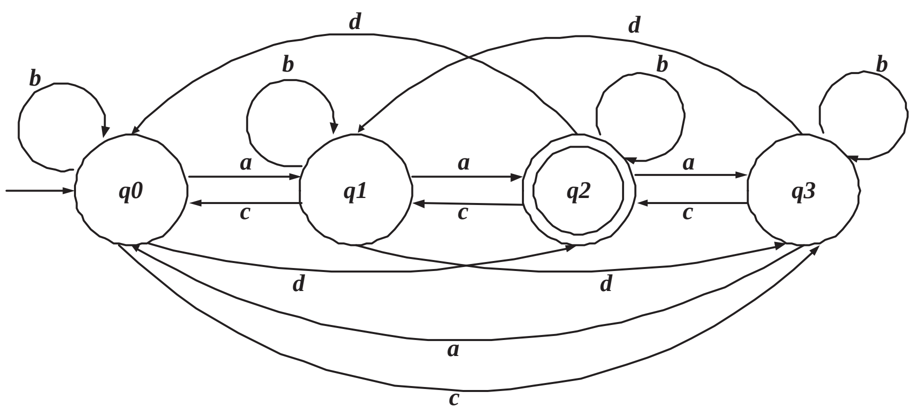
Príklad 3.1.2 *Skonštruujeme konečný automat A_2, ktorý rozpoznáva jazyk*

$$L_2 = \{ \ w \in \{a, b, c\}^* \mid \#_c w = 3k \vee \#_c w = 3k + 1, \ k \in \mathbb{N} \ \}.$$

Skonštruovaný stavový diagram pre automat A_2 je na obrázku 3.3.

Príklad 3.1.3 *Skonštruujme konečný automat A_3 pre jazyk*

$$L_3 = \{ \ w \in \{a, b, c, d\}^* \mid \#_a w - \#_c w + 2\#_d w = 4k + 2, \ k \in \mathbb{Z} \ \}$$

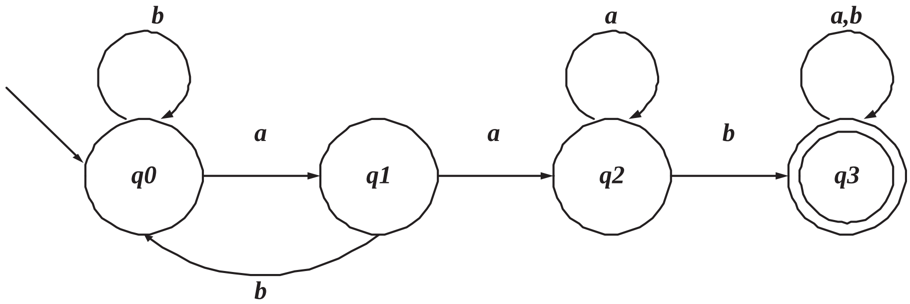


Obrázok 3.4: Konečný automat A_3.

Skonštruovaný stavový diagram pre automat A_3 je na obrázku 3.4.

V nasledujúcom príklade ukážeme, ako sa dá použit' konečný automat pri rozpoznávaní ret'azcov.

Príklad 3.1.4 *Rozpoznávanie ret'azcov.*
Skonštruujeme konečný automat, ktorý rozpoznáva všetky slová, v ktorých sa nachádza podslovo aab. Takýto automat bude rozpoznávat' jazyk:
$L_4 = \{xaaby \mid x, y \in \{a, b\}^*\}$



Obrázok 3.5: Konečný automat A_4.

Skonštruovaný stavový diagram pre automat A_4 je na obrázku 3.5.

3.2 Nedeterministické konečné automaty

Nedeterminizmus je formálna abstrakcia takých výpočtov, v ktorých nie je jednoznačne určený nasledujúci krok. Ako príklady môžu slúžit' konkurentné procesy, distribuované výpočty.

Definícia 3.2.1 Nedeterministický konečný automat
Nedeterministický konečný automat *(NFA - nondeterministic finite automaton) je pätica $A = (K, \Sigma, \delta, q_0, F)$, kde:*

K *je konečná množina stavov,*

Σ *je vstupná abeceda,*

δ *je prechodové zobrazenie, pričom platí*

$$\delta : K \times (\Sigma \cup \{\epsilon\}) \rightarrow 2^K,$$

$q_0 \in K$ *je počiatočný stav,*

$F \subseteq K$ *je množina koncových (akceptačných) stavov.*

Konfigurácia nedeterministického konečného automatu *je dvojica*

$$(q, w) \ \in \ K \times \Sigma^*,$$

kde:

q je momentálny stav,

w je zvyšok vstupu.

Krok výpočtu nedeterministického konečného automatu *je relácia* $\vdash_A$ *na konfigurácii definovaná nasledovne:*

$$(q, au) \vdash_A (p, u), \qquad ak \qquad p \in \delta(q, a),$$

kde $a \in \Sigma \cup \{\epsilon\}$, $u \in \Sigma^*$.

Jazyk rozpoznávaný deterministickým konečným automatom *(koncovým stavom) je množina*

$$L(A) = \{\ w \in \Sigma^* \mid (q_0, w) \vdash_A^* (q, \epsilon),\ q \in F\}.$$

Poznámka 3.2.1 *Pri konečných automatoch rozoznávame dva zdroje nedeterminizmu:*

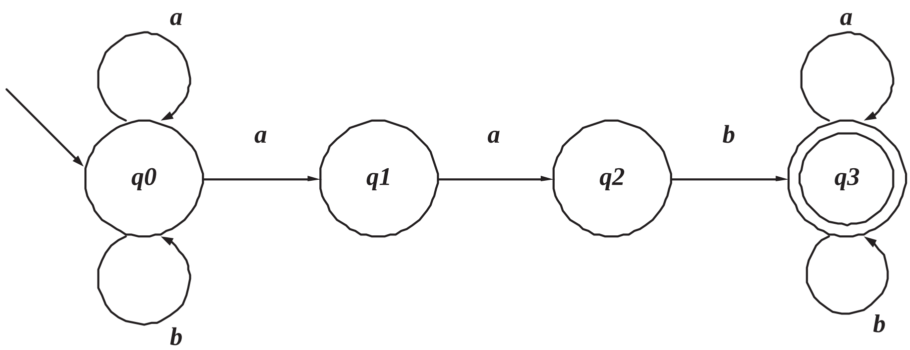
1. *epsilonové kroky,*

2. *prechodové zobrazenie, nie je funkcia.*

Riešené príklady

Na nasledovnom príklade si ukážeme využitie druhého zdroja nedeterminizmu.

Príklad 3.2.1 *Rozpoznávanie ret'azcov - nedeterministická verzia.*
Skonštruujme konečný automat A_5, pre jazyk L_4 z príkladu 3.1.4, ktorý rozpoznáva všetky slová v ktorých sa nachádza podslovo aab .
$L_5 = \{xaaby \mid x, y \in \{a, b\}^*\}$
Skonštruovaný stavový diagram pre automat A_5 je na obrázku 3.6.



Obrázok 3.6: Konečný automat A_5.

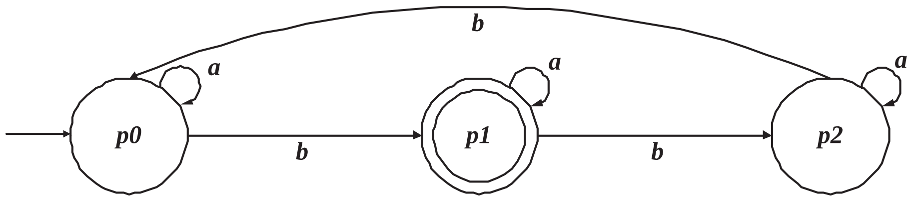
Prvým zdrojom nedeterminizmu sú epsilonové kroky, ktorý si ukážeme v nasledovnom príklade.

Príklad 3.2.2 *Skonštruujme konečný automat A_6, ktorý rozpoznáva zjednotenie jazykov*

$$L_6 = L_{2b} \cup L_{3b},$$

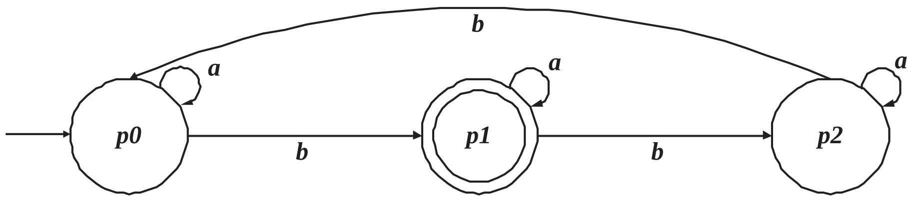
pričom $L_{2b} = \{ \ w \in \{a,b\}^* \mid \#_b w = 3k+1, \ k \in \mathbb{N} \ \}$, $L_{3b} = \{ \ w \in \{a,b\}^* \mid \#_b w = 4k+2, \ k \in \mathbb{N} \ \}$.

Riešením pariciálneho jazyka L_{2b} je automat A_{2b} skonštruovaný analogicky podľa príkladu 3.1.2. Skonštruovaný stavový diagram pre automat A_{2b} je na obrázku 3.7.



Obrázok 3.7: Konečný automat A_{2b}.

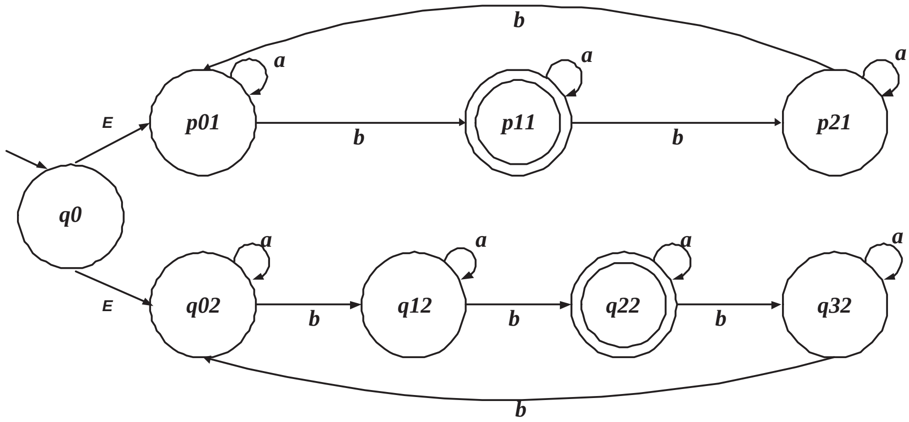
Riešením pariciálneho jazyka L_{3b} je automat A_{3b} skonštruovaný analogicky podľa príkladu 3.1.3. Skonštruovaný stavový diagram pre automat A_{3b} je na obrázku 3.8.



Obrázok 3.8: Konečný automat A_{3b}.

Zjednotenie dvoch jazykov L_{2b} a L_{3b} môžeme skúsiť skonštruovať ako zjenotenie dvoch automatov A_{2b} a A_{3b}. Musíme však myslieť na možnosť, aby sa tvorba slov z výsledného jazyka nemiešala navzájom medzi jazykmi.

Správne nedeterministrické riešenie skonštruujeme prepojením oboch automatov A_{2b} a A_{3b} pomocou epsilonových krokov, ktoré nám zabezpečia nemiešanie pôvodných automatov navzájom. Skonštruovaný stavový diagram pre automat A_6 je na obrázku 3.9.



Obrázok 3.9: Konečný automat A_6 správne riešenie.

3.3 Trieda jazykov rozpoznávaných konečnými automatmi

Pre skúmanie triedy jazykov rozpoznávaných konečnými automatmi zaveďme nasledovné označenia:

- trieda jazykov rozpoznávaných deterministickými konečnými automatmi L(DFA),
- trieda jazykov rozpoznávaných nedeterministickými konečnými automatmi L(NFA),
- trieda jazykov rozpoznávaných konečnými automatmi L(FA).

Veta 3.3.1 *Trieda jazykov rozpoznávaných deterministickými konečnými automatmi je ekvivalentná s triedou jazykov rozpoznávaných nedeterministickými konečnými automatmi. Formálne:*

$$\mathcal{L}(DFA) = \mathcal{L}(NFA) \ . \tag{3.1}$$

Poznámka 3.3.1 *Ku každému nedeterministickému konečnému automatu môžeme zostrojiť deterministický konečný automat.*

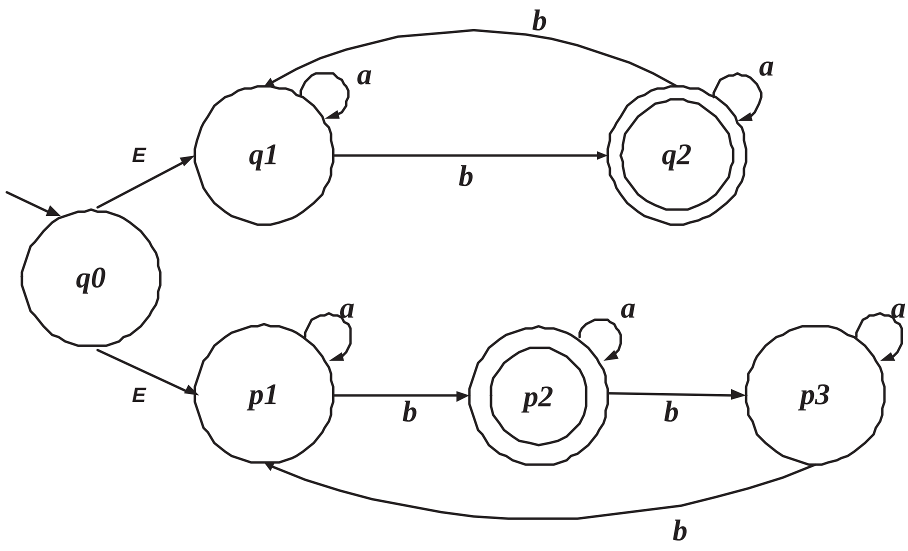
Veta 3.3.2 *Trieda jazykov rozpoznávaných konečnými automatmi je zhodná s triedou všetkých regulárnych jazykov. Formálne:*

$$\mathcal{L}(FA) = \mathcal{R} \ . \tag{3.2}$$

Riešené príklady

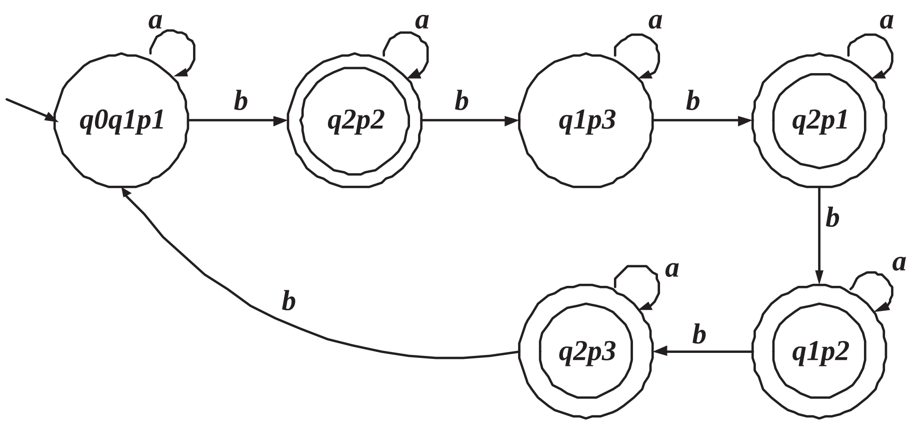
Príklad 3.3.1 *Príklad na prevod nedeterministického konečného automatu na deterministický konečný automat.*

Majme nedeterministický automat A_{7N}, ktorý je na obrázku 3.10. Nedeterministický automat $A_{7N} = A_1 \cup A_{2b}$. Jednotlivé automaty A_1 a A_{2b} nájdeme na obrázkoch 3.2 a 3.7.
$A(L_1) = \{\ w \in \{a,b\}^* \mid \#_b w = 2k+1,\ k \in \mathbb{N}\ \}$
$A(L_{2b}) = \{\ w \in \{a,b\}^* \mid \#_b w = 3k+1,\ k \in \mathbb{N}\ \}$



Obrázok 3.10: Konečný automat A_{7N}.

Skonštruujme deterministický konečný automat A_{7D} ku automatu A_{7N}.



Obrázok 3.11: Konečný automat A_{7D}, epsilonový uzáver.

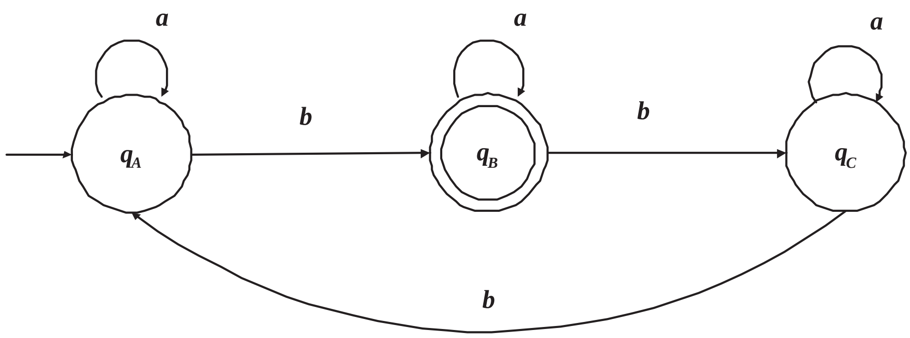
Deterministický konečný automat A_{7D} je skonštruovaný na obrázku 3.11.

Ukážme si vzt'ah konečných automatov a regulárnych gramatík. Nasledujúci príklad znázorňuje jednojednoznačnú korešpondenciu medzi regulárnymi gramatikami a konečnými automatmi.

Príklad 3.3.2 *Vzt'ah konečných automatov a regulárnych gramatík.*
Majme regulárnu gramatiku G_8.
Nech $G_8 = (N, T, P, A)$, *kde* $N = \{A, B, C\}$, $T = \{a, b\}$,
$P = \{$

$$\begin{array}{lcl} A \rightarrow aA & | & bB \\ B \rightarrow aB & | & bB \\ C \rightarrow aC & | & bA \\ B \rightarrow \epsilon & & \end{array}$$

$\}$.
Gramatika G_8 *generuje jazyk* $L(G_8) = \{\ w \in \{a, b\}^* \mid \#_b w = 3k + 1,\ k \in \mathbb{N}\ \}$.
Skonštruujme konečný automat A_8, *taký že* $L(A_8) = L(G_8)$.



Obrázok 3.12: Konečný automat A_8.

Skonštruovaný konečný automat A_8 *vidíme na obrázku 3.12.*

3.4 Uzáverové vlastnosti triedy regulárnych jazykov

Definícia 3.4.1 Uzavretost'
Trieda jazykov $\mathcal{L}$ *je uzavretá vzhl'adom na operáciu* $\Box : \mathcal{L} \times \mathcal{L} \rightarrow \mathcal{L}$ *ak platí:*

$$\forall\ L_1, L_2 \in \mathcal{L} \quad (L_1 \Box L_2) \in \mathcal{L}\ .$$

Veta 3.4.1 *Trieda* $\mathcal{R}$ *je uzavretá vzhl'adom nasledujúce na operácie:*

1. *zjednotenie* ($\cup$),

2. *zreťazenia* $(\cdot)$,

3. *prieniku* $(\cap)$,

4. *Kleeneho iterácie* $(^*)$,

5. *doplnku* $(^C)$,

6. *kladný uzáver* $(^+)$,

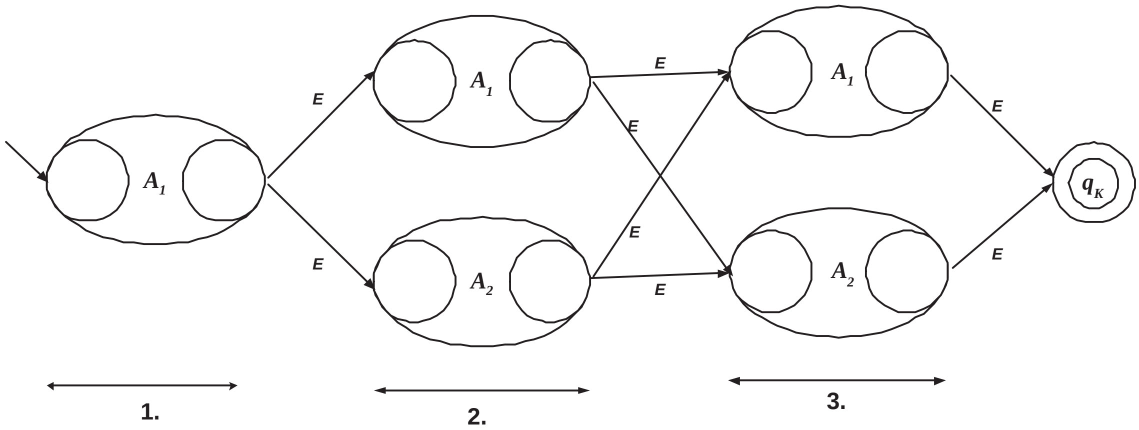
7. *zrkadlový obraz* (R).

Lema 3.4.1 *Jediný koncový stav konečného automatu.*
Ku každému konečnému automatu A existuje konečný automat A' taký, ktorý má jediný koncový stav a platí:

$$L(A) = L(A')$$

Riešené príklady

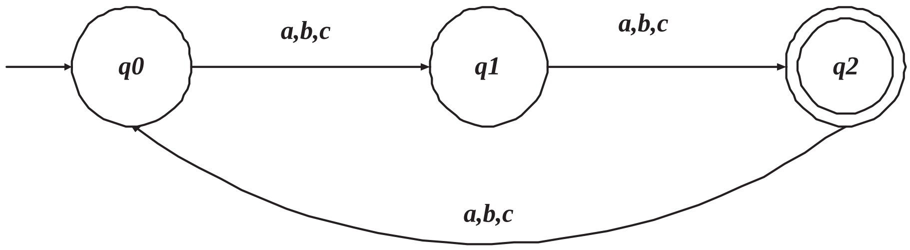
Príklad 3.4.1 *Nech $\triangle$ je binárna operácia nad jazykmi definovaná nasledovne: $L_1 \triangle L_2 = L_1.(L_1 \cup L_2)^2$. Zistite, či je trieda regulárnych jazykov $\mathcal{R}$ uzavretá vzhľadom na operáciu $\triangle$. Odpoveď zdôvodnite.*
Dokážme, že trieda regulárnych jazykov $\mathcal{R}$ je uzavretá vzhľadom na operáciu $\triangle$. Využijeme vetu 3.3.2 $\mathcal{L}(FA) = \mathcal{R}$. Stačí skonštruovať konečný automat, ktorý reprezentuje jazyk $L_1 \triangle L_2$.
Rozpíšme jazyk
$L_1 \triangle L_2 = L_1.(L_1 \cup L_2)^2 = L_1.(L_1 \cup L_2).(L_1 \cup L_2)$.
Keď využijeme fakt
$L(A_1) = L_1$
$L(A_2) = L_2$
potom sa dá jazyk reprezentovať automatom B skonštruovaným na obrázku 3.13. Vidíme, že celý obrázok 3.13 reprezentuje konečný automat B, ktorý rozpoznáva nejaký jazyk a po aplikácii vety 3.3.2 $\mathcal{L}(FA) = \mathcal{R}$ vyplýva, že tento jazyk je regulárny.



Obrázok 3.13: Konečný automat B.

Cvičenia

Cvičenie 3.4.1 *Skontrolujte, či sú nasledujúce dané konečné automaty skonštruované správne. Ku daným konečným automatom simulujte ich výpočet pre rôzne vstupné slová, ktoré jednak patria a jednak nepatria do daného jazyka.*

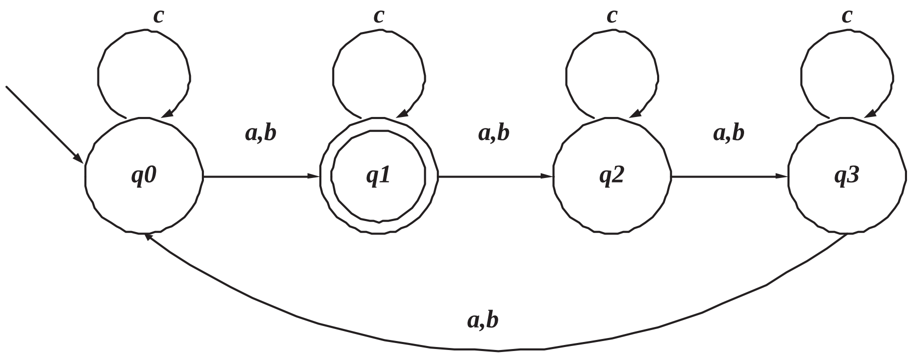


Obrázok 3.14: Cvičenia, automat A_1.

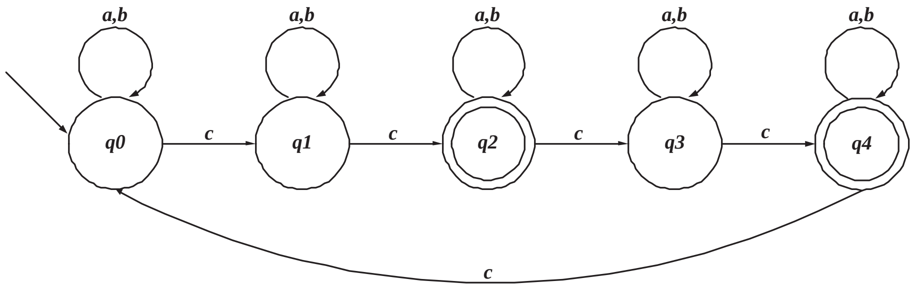
1. *konečný automat A_1 je nakreslený na obrázku 3.14 , jazyk $L_1 = \{ w \in \{a,b,c\}^* \mid |w| = 3k+2, k \in \mathbb{N}\}$*
2. *konečný automat A_2 je nakreslený na obrázku 3.15, jazyk $L_2 = \{ w \in \{a,b,c\}^* \mid \#_a w + \#_b w = 4k+1, k \in \mathbb{N}\}$*

Cvičenie 3.4.2 *Skontrolujte, či sú nasledujúce dané konečné automaty skonštruované správne. Daný konečný automat popíšte formálnym zápisom. Definujte jazyk rozpoznávaný daným konečným automatom. Simulujte výpočet automatu pre rôzne vstupné slová, ktoré jednak patria a jednak nepatria do jazyka.*

1. *konečný automat A_1 je nakreslený na obrázku 3.16 , definujte jazyk L_1*



Obrázok 3.15: Cvičenia, automat A_2.



Obrázok 3.16: Cvičenia, automat A_1.

2. konečný automat A_2 je nakreslený na obrázku 3.17, definujte jazyk L_2

Cvičenie 3.4.3 *Navrhnite konečné automaty pre jazyky:*

1. $L_1 = \{\ w \in \{b, c, d, e\}^* \mid 2\#_b w - \#_c w - 3\#_d w = 5k + 1, k \in \mathbb{Z}\}$

2. $L_2 = \{\{\ w \in \{a, b, c\}^* \mid \#_c w = 5k + 2, k \in \mathbb{N}\} \cup \{\ w \in \{a, b, c\}^* \mid \#_c w = 5k + 4, k \in \mathbb{N}\}\}^C$

3. $L_3 = \{\ w \in \{a, b\}^* \mid \#_b w = 4k + 3, k \in \mathbb{N}\} \cup \{w \in \{c, d\}^* \mid \#_c w + \#_d w = 3k + 1, k \in \mathbb{N}\}$

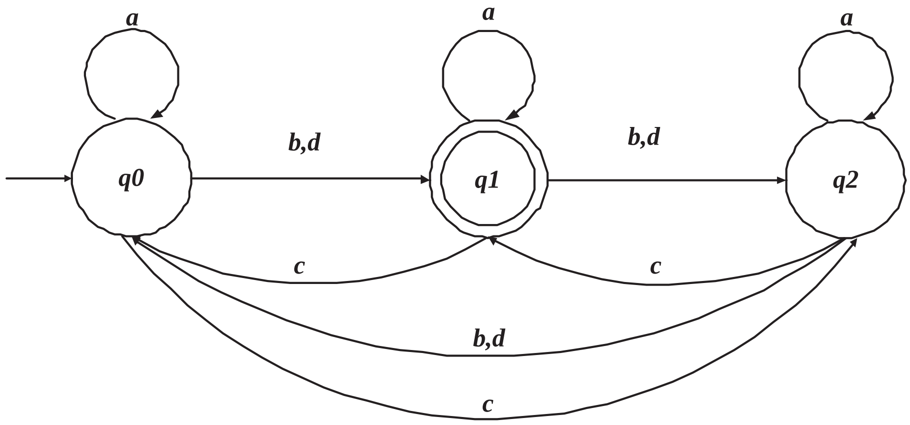
4. $L_4 = \{\ 67w8 \mid w \in \{a, b\}^* \mid \#_b w = 3k + 1, k \in \mathbb{N}\}$

5. $L_5 = \{\ abwc \mid w \in \{3, 4, 5\}^* \mid \#_4 w + \#_5 w = 4k + 2, k \in \mathbb{N}\}$

6. $L_6 = \{\ w \in \{a, b, c\}^* \mid \#_a w + \#_b w = 4k + 1, k \in \mathbb{N}\}^C$

Cvičenie 3.4.4 *Navrhnite konečné automaty pre jazyky:*

1. $L_1 = \{\ abbabx \mid x \in \{a, b\}^*\}$



Obrázok 3.17: Cvičenia, automat A_2.

2. $L_2 = \{\ xabbab \mid x \in \{a,b\}^*\}$
3. $L_3 = \{\ xaaby \mid x,y \in \{a,b\}^*\}$
4. $L_4 = \{\ xaabby \mid x,y \in \{a,b\}^*\}$
5. $L_5 = \{\ xaaby \mid x,y \in \{a,b,c\}^*\}$
6. $L_6 = \{\ xababcy \mid x,y \in \{a,b,c\}^*\}$
7. $L_7 = \{\ xcbbaby \mid x,y \in \{a,b,c\}^*\}$
8. $L_8 = \{\ xabcdaby \mid x,y \in \{a,b,c,d\}^*\}$
9. $L_9 = \{\ x777865y \mid x,y \in \{5,6,7,8\}^*\}$
10. $L_{10} = \{\ xabbaby \mid x,y \in \{a,b\}^*\}$
11. $L_{11} = \{\ w \mid w \in \{a,b\}^*,\ \textit{slovo } w \textit{ neobsahuje podslovo } abbab\ \}$

Cvičenie 3.4.5 *Navrhnite konečné automaty pre jazyky:*

1. $L_1 = \{\ w = xbbay\ \vee\ w = xabay \mid x,y \in \{a,b\}^*\}$
2. $L_2 = \{\ w = xaaay\ \vee\ w = xbbby \mid x,y \in \{a,b\}^*\}$
3. $L_3 = \{\ w = xaby\ \wedge\ \#_b w = 2k+1 \mid x,y \in \{a,b\}^*, k \in \mathbb{N}\}$

Cvičenie 3.4.6 *Navrhnite konečné automaty pre jazyky:*

1. $L_1 = \{\ a^i b^j c^k \mid i,j,k \in \mathbb{N}^+\ \}$

2. $L_2 = \{\ a^i b^j c^k \mid i, j, k \in \mathbb{N}\ \}$

3. $L_3 = \{\ (ab)^n \mid n \in \mathbb{N}\ \}$

4. $L_3 = \{\ (ab)^n c^i \mid i, n \in \mathbb{N}\ \}$

5. $L_3 = \{\ (ab)^n c^i \mid i, n \in \mathbb{N}^+\ \}$

Cvičenie 3.4.7 *Navrhnite konečné automaty pre jazyky:*

1. $L_1 = \{\ w = uv, |u| = |v| = n, u \neq v \mid u, v \in \{0,1\}^*,\ n \in \mathbb{N}\ \}$

2. $L_2 = \{\ w \mid w \in \{0,1\}^*,$ *v slove w je na posledných dvoch pozíciách práve jedna 0* $\}$

3. $L_3 = \{\ w \mid w \in \{0,1\}^*,$ *v slove w za každou 0 nasleduje 1* $\}$

4. $L_4 = \{\ w \mid w \in \{a,b\}^*,$ *slovo w začína aj končí tým istým písmenom* $\}$

5. $L_5 = \{\ w \mid w \in \{a,b\}^*,$ *slovo w je aspoň štvorpísmenové a druhé aj predposledné písmeno je rovnaké* $\}$

Cvičenie 3.4.8 *Navrhnite konečné automaty, ktoré rozpoznávajú čísla (predpokladáme konečný počet cifier):*

1. *prirodzené bez nuly,*

2. *prirodzené s nulou,*

3. *celé,*

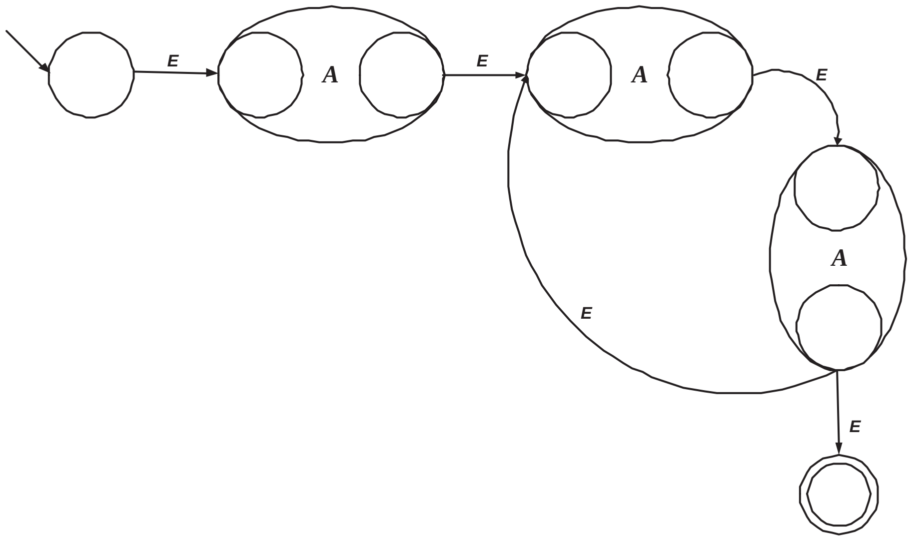
4. *kladné racionálne,*

5. *celé párne,*

6. *záporné deliteľné piatimi.*

Cvičenie 3.4.9 *Je daný deterministický konečný automat $A = (K, \Sigma, \delta, q_z, F)$, ktorý rozpoznáva jazyk L, pričom $\Sigma = \{a, c\}$, $F = \{q_k\}$. Na obrázku 3.18 je nakreslený konečný automat B_1, ktorý vznikol "poskladaním"niekoľkých konečných automatov A. Zistite aký jazyk rozpoznáva konečný automat B_1.*

Cvičenie 3.4.10 *Je daný deterministický konečný automat $A = (K, \Sigma, \delta, q_z, F)$, ktorý rozpoznáva jazyk L, pričom $\Sigma = \{b, d\}$, $F = \{q_k\}$. Na obrázku 3.19 je nakreslený konečný automat B_2, ktorý vznikol "poskladaním"niekoľkých konečných automatov A. Zistite aký jazyk rozpoznáva konečný automat B_2.*



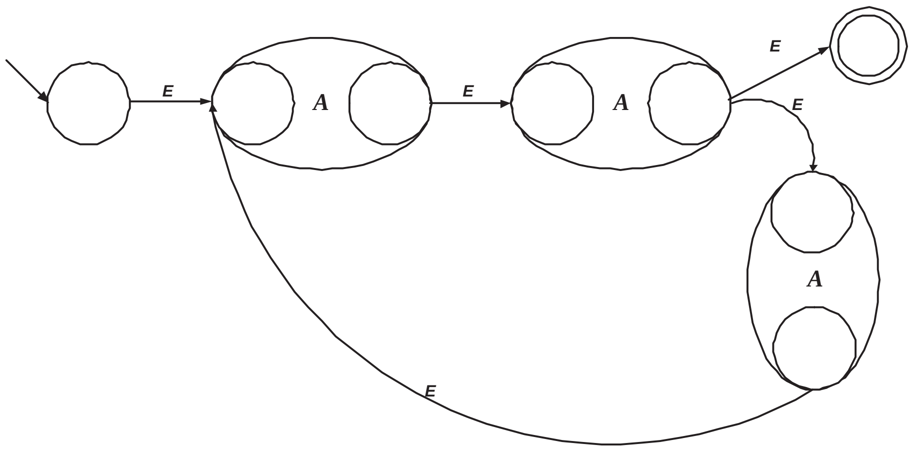
Obrázok 3.18: Cvičenia, automat B_1.

Cvičenie 3.4.11 *Dokážte tvrdenie, že ku každému konečnému automatu A existuje konečný automat A' taký, ktorý má jediný koncový stav a platí:*

$$L(A) = L(A')$$

Cvičenie 3.4.12 *Nech $\heartsuit$ je binárna operácia nad jazykmi definovaná nasledovne: $L_1 \heartsuit L_2 = (L_1 \cup L_2).(L_1)^+$. Zistite, či je trieda regulárnych jazykov $\mathcal{R}$ uzavretá vzhľadom na operáciu $\heartsuit$. Odpoveď zdôvodnite.*

Cvičenie 3.4.13 *Definujte konečný automat so zásobníkom a s počítadlom tak, že definujete konfiguráciu, krok odvodenia a krok výpočtu.*



Obrázok 3.19: Cvičenia, automat B_2.