

## Poznámky k cvičeniu č. 2

Peter Kostolányi

4. októbra 2017

### Zobrazenia, obrazy a inverzné obrazy

Nech  $f: X \rightarrow Y$  je zobrazenie. *Obraz prvku*  $x \in X$  pri zobrazení  $f$  sa tradične označuje symbolom  $f(x)$ . Pojem obrazu možno prirodzeným spôsobom rozšíriť aj na podmnožiny  $X$ .

**Definícia 1.** Nech  $f: X \rightarrow Y$  je zobrazenie a  $X' \subseteq X$ . *Obraz množiny*  $X'$  pri zobrazení  $f$  je množina

$$f(X') = \{f(x) \mid x \in X'\}.$$

Podobne možno definovať aj inverzný obraz množiny  $Y' \subseteq Y$  ako množinu všetkých prvkov z  $X$ , ktoré sa zobrazia na prvok z  $Y'$ . Formálne:

**Definícia 2.** Nech  $f: X \rightarrow Y$  je zobrazenie a  $Y' \subseteq Y$ . *Inverzný obraz množiny*  $Y'$  pri zobrazení  $f$  je množina

$$f^{-1}(Y') = \{x \in X \mid f(x) \in Y'\}.$$

V prípade, že je zobrazenie  $f: X \rightarrow Y$  bijektívne, zvykne sa symbolom  $f^{-1}$  označovať *inverzné zobrazenie* k zobrazeniu  $f$ . Táto notácia súhlasí s notáciou pre inverzné obrazy zavedenou v definícii 2: inverzný obraz množiny  $Y'$  pri bijektívnom zobrazení  $f$  je obraz množiny  $Y'$  pri inverznom zobrazení  $f^{-1}$ .

Inverzný obraz prvku  $y$  možno definovať pre ľubovoľné (teda nie len bijektívne) zobrazenia ako inverzný obraz jednoprvkovej množiny  $\{y\}$ .

**Definícia 3.** Nech  $f: X \rightarrow Y$  je zobrazenie a  $y \in Y$ . *Inverzný obraz prvku*  $y$  pri zobrazení  $f$  je množina

$$f^{-1}(y) = f^{-1}(\{y\}) = \{x \in X \mid f(x) \in \{y\}\} = \{x \in X \mid f(x) = y\}.$$

V prípade, že je zobrazenie  $f$  bijektívne, je inverzný obraz  $f^{-1}(y)$  jednoprvková množina. To úplne nesúhlasí s notáciou pre inverzné zobrazenia, kde  $f^{-1}(y)$  označuje priamo prvok tejto jednoprvkovej množiny. Tieto dva objekty sa však v matematike často vzájomne zamieňajú, takže uvedenú nejednoznačnosť nie je nutné prežívať príliš tragicky.

### Homomorfizmus

Pod pojmom homomorfizmus sa v matematike chápe štruktúru zachovávajúce zobrazenie (kde pod štruktúrou možno rozumieť napr. grupovú štruktúru, vektorovú štruktúru<sup>1</sup> a pod.). Štruktúra slov nad abecedou  $\Sigma$  je daná predovšetkým operáciou zretáženia a pod homomorfizmom teda rozumieme zobrazenie, ktoré túto operáciu zachováva.

**Definícia 4.** Nech  $\Sigma, \Gamma$  sú abecedy. *Homomorfizmus* zo  $\Sigma^*$  do  $\Gamma^*$  je zobrazenie  $h: \Sigma^* \rightarrow \Gamma^*$  také, že pre všetky  $u, v \in \Sigma^*$  platí

$$h(uv) = h(u)h(v).$$

Ak navyše pre každé  $w \in \Sigma^+$  platí  $h(w) \in \Gamma^+$ , nazýva sa homomorfizmus  $h$  *nevymazávajúci*.

Neskôr ukážeme, že takto definovaný homomorfizmus je v skutočnosti homomorfizmom monoidov. V rámci notačnej konvencie budeme homomorfizmy väčšinou označovať symbolom  $h$  s prípadnými indexmi alebo inými „ozdobami“.

V nasledujúcich troch tvrdeniach postupne dokážeme, že homomorfný obraz prázdneho slova je vždy prázdne slovo, že každé zobrazenie písmen zo  $\Sigma$  do  $\Gamma^*$  možno rozšíriť na homomorfizmus zo  $\Sigma^*$  do  $\Gamma^*$  a že každý homomorfizmus je jednoznačne určený obrazmi písmen.

<sup>1</sup>Homomorfizmy medzi vektorovými priestormi sú známe skôr ako *lineárne zobrazenia*.

**Tvrdenie 1.** Nech  $\Sigma, \Gamma$  sú abecedy a  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus. Potom  $h(\varepsilon) = \varepsilon$ .

*Dôkaz.* Sporom. Nech  $h(\varepsilon) = w$  pre nejaké  $w \in \Gamma^+$ . Z definície homomorfizmu potom vyplýva

$$w = h(\varepsilon) = h(\varepsilon\varepsilon) = h(\varepsilon)h(\varepsilon) = ww,$$

čo je spor, keďže rovnosť  $w = ww$  nemôže platiť pre žiadne neprázdne slovo  $w$ . □

**Tvrdenie 2.** Nech  $\Sigma, \Gamma$  sú abecedy a  $f: \Sigma \rightarrow \Gamma^*$  je zobrazenie. Potom existuje homomorfizmus  $h: \Sigma^* \rightarrow \Gamma^*$  taký, že pre všetky  $c \in \Sigma$  platí  $h(c) = f(c)$ .

*Dôkaz.* Matematickou indukciou by sme ľahko dokázali, že zobrazenie  $h: \Sigma^* \rightarrow \Gamma^*$ , dané pre všetky  $w = a_1 \dots a_k$ ,  $a_1, \dots, a_k \in \Sigma$  ako  $h(a_1 \dots a_k) = f(a_1) \dots f(a_k)$  – z uvedeného zápisu vyplýva aj  $h(\varepsilon) = \varepsilon$  – je homomorfizmus. □

**Tvrdenie 3.** Nech  $\Sigma, \Gamma$  sú abecedy a  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus. Nech  $h': \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus taký, že pre všetky  $c \in \Sigma$  platí  $h'(c) = h(c)$ . Potom  $h' = h$ .

*Dôkaz.* Treba dokázať, že pre všetky  $w \in \Sigma^*$  platí  $h'(w) = h(w)$ . Z tvrdenia 1 a predpokladu na homomorfizmus  $h'$  vyplýva, že rovnosť platí pre všetky  $w$  také, že  $|w| \leq 1$ . Nech teraz  $|w| = k > 1$ . Potom  $w = a_1 \dots a_k$  pre nejaké  $a_1, \dots, a_k \in \Sigma$ . Matematickou indukciou by sme ľahko dokázali, že z definície homomorfizmu vyplýva  $h(w) = h(a_1) \dots h(a_k)$  a  $h'(w) = h'(a_1) \dots h'(a_k)$ . Keďže ale pre všetky  $c \in \Sigma$  platí  $h'(c) = h(c)$ , z uvedených dvoch rovností vyplýva  $h'(w) = h(w)$ , čo bolo treba dokázať. □

Homomorfizmy budeme zvyčajne – vďaka tvrdeniu 2 zmysluplne a vďaka tvrdeniu 3 jednoznačne – zadávať práve homomorfnými obrazmi jednotlivých symbolov abecedy. Obraz jazyka  $L$  pri zobrazení homomorfizmom  $h$  je definovaný jednoducho ako obraz množiny  $L$  pri zobrazení  $h$  v zmysle definície 1.

**Definícia 5.** Nech  $\Sigma, \Gamma$  sú abecedy,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $L \subseteq \Sigma^*$  je jazyk. Obraz jazyka  $L$  pri zobrazení homomorfizmom  $h$  je jazyk  $h(L) = \{h(w) \mid w \in L\}$ .

*Príklad 1.* Nech  $\Sigma = \{a, b\}$  a  $h: \Sigma^* \rightarrow \Sigma^*$  je homomorfizmus daný ako  $h(a) = ab$  a  $h(b) = \varepsilon$ . Nech  $L_1 = \{b, bb\}$ ,  $L_2 = \{b, bb, abb\}$ ,  $L_3 = \{a^n b^n \mid n \in \mathbb{N}\}$  a  $L_4 = \{w \in \{a, b\}^* \mid \#_a(w) = \#_b(w)\}$ . Obrazy týchto jazykov pri zobrazení homomorfizmom  $h$  sú dané nasledovne:

$$\begin{aligned} h(L_1) &= \{\varepsilon\}, \\ h(L_2) &= \{\varepsilon, ab\}, \\ h(L_3) &= \{ab\}^*, \\ h(L_4) &= \{ab\}^*. \end{aligned}$$

**Úloha 1.** Nech  $L_1, L_2$  sú jazyky,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $\Sigma_{L_1}, \Sigma_{L_2} \subseteq \Sigma$ . Porovnajzte jazyky  $h(L_1 \cup L_2)$  a  $h(L_1) \cup h(L_2)$ .

*Riešenie.* Dokážeme, že platia obidve inklúzie, a teda  $h(L_1 \cup L_2) = h(L_1) \cup h(L_2)$ .

⊆: Nech  $u \in h(L_1 \cup L_2)$ . Z definície 5 vyplýva, že existuje  $v \in L_1 \cup L_2$  také, že  $u = h(v)$ . Keďže  $v \in L_1 \cup L_2$ , musí platiť  $v \in L_1$  alebo  $v \in L_2$  (alebo oboje). Ak  $v \in L_1$ ,  $u = h(v) \in h(L_1)$ . Ak  $v \in L_2$ ,  $u = h(v) \in h(L_2)$ . Keďže ale  $h(L_1), h(L_2) \subseteq h(L_1) \cup h(L_2)$ , v oboch prípadoch máme  $u \in h(L_1) \cup h(L_2)$ .

⊇: Nech  $u \in h(L_1) \cup h(L_2)$ . Potom  $u \in h(L_1)$  alebo  $u \in h(L_2)$ . Bez ujmy na všeobecnosti, nech  $u \in h(L_1)$ . Potom z definície 5 vyplýva, že existuje  $v \in L_1$  také, že  $u = h(v)$ . Keďže  $v \in L_1$ , platí aj  $v \in L_1 \cup L_2$ . Preto  $u = h(v) \in h(L_1 \cup L_2)$ , čo bolo treba dokázať.

Tvrdenie je dokázané. □

**Úloha 2.** Nech  $L_1, L_2$  sú jazyky,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $\Sigma_{L_1}, \Sigma_{L_2} \subseteq \Sigma$ . Porovnajete jazyky  $h(L_1 \cdot L_2)$  a  $h(L_1) \cdot h(L_2)$ .

*Riešenie.* Dokážeme, že platia obidve inklúzie, a teda  $h(L_1 \cdot L_2) = h(L_1) \cdot h(L_2)$ .

$\subseteq$ : Nech  $u \in h(L_1 \cdot L_2)$ . Potom existuje  $v \in L_1 \cdot L_2$  také, že  $h(v) = u$ . Keďže  $v \in L_1 \cdot L_2$ , existujú slová  $x \in L_1$  a  $y \in L_2$  tak, že  $v = xy$ . Z definície homomorfizmu potom vyplýva  $u = h(v) = h(xy) = h(x)h(y) \in h(L_1) \cdot h(L_2)$ .

$\supseteq$ : Nech  $u \in h(L_1) \cdot h(L_2)$ . Potom existujú slová  $x \in L_1$  a  $y \in L_2$  také, že  $u = h(x)h(y)$ . Z definície homomorfizmu potom vyplýva  $u = h(x)h(y) = h(xy) \in h(L_1 \cdot L_2)$ .

Tvrdenie je dokázané. □

### Inverzný homomorfizmus

Obraz jazyka pri zobrazení inverzným homomorfizmom je inverzný obraz v zmysle definícií 2 a 3, kde príslušné zobrazenie je homomorfizmus.

**Definícia 6.** Nech  $\Sigma, \Gamma$  sú abecedy,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $L \subseteq \Gamma^*$  je jazyk. *Obraz jazyka  $L$  pri zobrazení inverzným homomorfizmom  $h^{-1}$  je jazyk  $h^{-1}(L) = \{u \in \Sigma^* \mid h(u) \in L\}$ .*

**Definícia 7.** Nech  $\Sigma, \Gamma$  sú abecedy,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $v \in \Gamma^*$  je slovo. *Obraz slova  $v$  pri zobrazení inverzným homomorfizmom  $h^{-1}$  je jazyk*

$$h^{-1}(v) = h^{-1}(\{v\}) = \{u \in \Sigma^* \mid h(u) \in \{v\}\} = \{u \in \Sigma^* \mid h(u) = v\}.$$

O niečo presnejšie by bolo namiesto o „obraz pri zobrazení inverzným homomorfizmom  $h^{-1}$ “ hovoriť o „inverznom obraze pri homomorfizme  $h$ “, prípadne o „inverznom homomorfizmom obraze“. Ide však o zaužívanú terminológiu súvisiacu s predstavou inverzného homomorfizmu ako zobrazenia  $h^{-1}: \Gamma^* \rightarrow 2^{\Sigma^*}$ . Takáto predstava môže byť občas užitočná, podobne ako predstava o zobrazeniach  $h: 2^{\Sigma^*} \rightarrow 2^{\Gamma^*}$  a  $h^{-1}: 2^{\Gamma^*} \rightarrow 2^{\Sigma^*}$ .

Z uvedených definícií je zrejmé, že pre každý homomorfizmus  $h: \Sigma^* \rightarrow \Gamma^*$  a jazyk  $L \subseteq \Gamma^*$  platí

$$h^{-1}(L) = \bigcup_{w \in L} h^{-1}(w).$$

*Príklad 2.* Nech  $\Sigma = \{a, b, c\}$ ,  $\Gamma = \{a, b\}$  a  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus daný ako  $h(a) = ab$ ,  $h(b) = a$  a  $h(c) = ab$ . Potom napríklad  $h^{-1}(aab) = \{ba, bc\}$  a  $h^{-1}(b) = h^{-1}(bb) = \emptyset$ . V dôsledku toho napríklad pre  $L = \{b, aab\}$  platí  $h^{-1}(L) = \{ba, bc\}$ .

**Úloha 3.** Nech  $h: \{a, b\}^* \rightarrow \{c, d\}^*$  je homomorfizmus daný ako  $h(a) = c$  a  $h(b) = cd$ . Nájdite nasledujúce jazyky:

- $h^{-1}(L_1)$ , kde  $L_1 = \{c^n d^n \mid n \in \mathbb{N}\}$ .
- $h^{-1}(L_2)$ , kde  $L_2 = \{c^n d^n \mid n \in \mathbb{N}; n \geq 1\}$ .
- $h^{-1}(L_3)$ , kde  $L_3 = \{c^n d^n \mid n \in \mathbb{N}; n \geq 2\}$ .

*Riešenie.* Ľahko možno nahliadnuť, že jazyk  $h^{-1}(w)$  je pre slovo  $w \in \{c, d\}^*$  neprázdny vtedy a len vtedy, keď sa pred každým výskytom symbolu  $d$  v slove  $w$  nachádza symbol  $c$ . Pre všetky  $n \in \mathbb{N}$  také, že  $n \geq 2$  teda platí  $h^{-1}(c^n d^n) = \emptyset$ . Ďalej,  $h^{-1}(cd) = \{b\}$  a  $h^{-1}(\varepsilon) = \{\varepsilon\}$ . Preto:

- $h^{-1}(L_1) = \bigcup_{w \in L_1} h^{-1}(w) = \{\varepsilon, b\}$ .
- $h^{-1}(L_2) = \bigcup_{w \in L_2} h^{-1}(w) = \{b\}$ .
- $h^{-1}(L_3) = \bigcup_{w \in L_3} h^{-1}(w) = \emptyset$ . □

**Úloha 4.** Nech  $L_1, L_2$  sú jazyky,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $\Sigma_{L_1}, \Sigma_{L_2} \subseteq \Gamma$ . Porovnajete jazyky  $h^{-1}(L_1 \cdot L_2)$  a  $h^{-1}(L_1) \cdot h^{-1}(L_2)$ .

*Riešenie.* Dokážeme, že  $h^{-1}(L_1 \cdot L_2) \supseteq h^{-1}(L_1) \cdot h^{-1}(L_2)$ , kým opačná inklúzia vo všeobecnosti neplatí.

$\not\subseteq$ : Uvažujme napríklad homomorfizmus  $h: \{a\}^* \rightarrow \{a\}^*$  daný ako  $h(a) = aa$  a jazyky  $L_1 = L_2 = \{a\}$ . Potom  $h^{-1}(L_1 \cdot L_2) = h^{-1}(\{aa\}) = \{a\}$ , kým  $h^{-1}(L_1) \cdot h^{-1}(L_2) = \emptyset \cdot \emptyset = \emptyset$ .

$\supseteq$ : Nech  $w \in h^{-1}(L_1) \cdot h^{-1}(L_2)$ . Potom  $w = uv$  pre nejaké  $u \in h^{-1}(L_1)$  a  $v \in h^{-1}(L_2)$ . Z definície inverzného homomorfizmu vyplýva  $h(u) \in L_1$  a  $h(v) \in L_2$ . Preto dostávame  $h(w) = h(uv) = h(u)h(v) \in L_1 \cdot L_2$ , a teda  $w \in h^{-1}(L_1 \cdot L_2)$ .

Tvrdenie je dokázané. □

**Úloha 5.** Nech  $L$  je jazyk,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $\Sigma_L \subseteq \Gamma$ . Porovnajete jazyky  $L$  a  $h(h^{-1}(L))$ .

*Riešenie.* Dokážeme, že  $L \supseteq h(h^{-1}(L))$ , pričom opačná inklúzia vo všeobecnosti neplatí.

$\not\subseteq$  Nech  $L = \{a\}$  a  $h: \{a\}^* \rightarrow \{a\}^*$  je daný ako  $h(a) = aa$ . Potom  $h(h^{-1}(L)) = h(\emptyset) = \emptyset$ , čo nie je nadjazyk jazyka  $L$ .

$\supseteq$  Nech  $w \in h(h^{-1}(L))$ . Potom existuje  $u \in h^{-1}(L)$  také, že  $w = h(u)$ . Keďže  $u \in h^{-1}(L)$ , z definície inverzného homomorfizmu máme  $h(u) \in L$  a z rovnosti  $w = h(u)$  potom vyplýva  $w \in L$ . □

**Úloha 6.** Nech  $L$  je jazyk,  $h: \Sigma^* \rightarrow \Gamma^*$  je homomorfizmus a  $\Sigma_L \subseteq \Sigma$ . Porovnajete jazyky  $L$  a  $h^{-1}(h(L))$ .

*Riešenie.* Dokážeme, že  $L \subseteq h^{-1}(h(L))$ , pričom opačná inklúzia vo všeobecnosti neplatí.

$\subseteq$ : Nech  $w \in L$ . Potom  $h(w) \in h(L)$ , z čoho  $w \in h^{-1}(h(L))$ .

$\not\supseteq$ : Nech  $L = \{a\}$  a  $h: \{a, b\}^* \rightarrow \{a\}^*$  je definovaný ako  $h(a) = h(b) = a$ . Potom dostávame  $h^{-1}(h(L)) = h^{-1}(\{a\}) = \{a, b\}$ , čo nie je podjazyk jazyka  $L$ . □

### \* Voľný monoid

Zreťazenie slov je zjavne asociatívne a  $\varepsilon$  je neutrálny prvok vzhľadom na túto operáciu. Pre každú abecedu  $\Sigma$  tak jazyk  $\Sigma^*$  tvorí s operáciou zretiazovania monoid, tzv. *voľný monoid* nad  $\Sigma$  (systematickejší výklad súvisiacich pojmov čitateľ nájde napríklad v [2]).

**Definícia 8.** *Grupoid* (niekde tiež *magma*) je usporiadaná dvojica  $(X, \circ)$ , kde  $X$  je množina a  $\circ: X \times X \rightarrow X$  je binárna operácia na  $X$ . *Pologrupa* je grupoid, pre ktorý navyše platí:

(i) Asociatívnosť:  $\forall x, y, z \in X : x \circ (y \circ z) = (x \circ y) \circ z$ .

*Pologrupa s jednotkou* alebo *monoid* je pologrupa, pre ktorú navyše platí:

(ii) Existencia neutrálneho prvku:  $\exists e_X \in X \forall x \in X : x \circ e_X = e_X \circ x = x$ .

*Grupa* je monoid, pre ktorý navyše platí:

(iii) Existencia inverzných prvkov:  $\forall x \in X \exists x^{-1} \in X : x \circ x^{-1} = x^{-1} \circ x = e_X$ .

Grupoid  $(X, \circ)$  je *komutatívny*, ak platí:  $\forall x, y \in X : x \circ y = y \circ x$ . Táto definícia nám umožňuje hovoriť aj o komutatívnej pologrupe, komutatívnom monoide a komutatívnej (abelovskej) grupe.

**Tvrdenie 4.** Nech  $\Sigma$  je abeceda. Potom  $(\Sigma^*, \cdot)$  je monoid, ktorý sa nazýva voľný monoid nad  $\Sigma$ .

*Dôkaz.* Zrejme z definície zretiazovania. □

*Homomorfizmus* medzi monoidmi  $(X, \circ)$  a  $(Y, \bullet)$  je ľubovoľné zobrazenie  $h: X \rightarrow Y$  spĺňajúce  $h(e_X) = e_Y$  a  $h(x \circ y) = h(x) \bullet h(y)$  pre všetky  $x, y \in X$ . Homomorfizmus slov  $h: \Sigma^* \rightarrow \Gamma^*$  by sme teda mohli – vďaka tvrdeniu 1 – definovať jednoducho ako homomorfizmus medzi monoidmi  $(\Sigma^*, \cdot)$  a  $(\Gamma^*, \cdot)$ .

Zvyčajná definícia voľného monoidu je ale o niečo všeobecnejšia – kľúčová je pri nej vlastnosť homomorfizmov slov, ktorú sme sformulovali v tvrdeniach 2 a 3: každé zobrazenie priradujúce písmenám abecedy slová jednoznačne určuje homomorfizmus. Ľahko možno nahliadnuť, že táto vlastnosť zostáva v platnosti aj pre homomorfizmy z voľného monoidu do ľubovoľného monoidu. Formálne potom definujeme voľný monoid  $(X, \circ)$  nad podmnožinou  $X' \subseteq X$  nasledovne.

**Definícia 9.** Nech  $(X, \circ)$  je monoid a  $X' \subseteq X$ . Monoid  $(X, \circ)$  je *voľný nad  $X'$* , ak pre každý monoid  $(Y, \bullet)$  a každé zobrazenie  $f: X' \rightarrow Y$  existuje práve jeden homomorfizmus  $h: X \rightarrow Y$  taký, že pre všetky  $x \in X'$  platí  $h(x) = f(x)$ .

Dá sa dokázať, že ľubovoľný monoid voľný nad  $\Sigma$  v zmysle definície 9 je generovaný množinou  $\Sigma$  a izomorfný s voľným monoidom  $(\Sigma^*, \cdot)$ . Pomenovanie „voľný monoid“ pritom pochádza z jeho vlastnosti, že „jedinými rovnosťami platnými medzi prvkami voľného monoidu nad  $\Sigma$  sú tie, ktoré priamo vyplývajú z definície monoidu generovaného množinou  $\Sigma$ “. Voľný monoid teda „nie je zväzovaný“ žiadnymi „zbytočnými“ rovnosťami medzi jeho prvkami. Napríklad monoid  $(\mathbb{N}^2, +)$  nie je voľný nad svojou generujúcou množinou  $\{(1, 0), (0, 1)\}$ , lebo v ňom okrem iného platí rovnosť  $(1, 0) + (0, 1) = (0, 1) + (1, 0)$ , ktorá očividne nemusí byť splnená v každom monoide s generátormi  $\{(1, 0), (0, 1)\}$ ; monoid  $(\mathbb{N}^2, +)$  v skutočnosti nie je voľný nad *žiadnou* svojou generujúcou množinou. Monoid  $(\mathbb{N}, +)$  naopak *je* voľný nad  $\{1\}$  – tento monoid je zjavne izomorfný s monoidom  $(\{a\}^*, \cdot)$ . Dá sa tiež ukázať, že ľubovoľný monoid možno získať z voľného monoidu faktorizáciou podľa nejakej kongruencie (kde kongruencia a faktorový monoid sú definované analogicky ako pri grupách).

Monoid nie je jedinou algebraickou štruktúrou, pre ktorú sa dá definovať voľnosť chápaná ako v definícii 9. Analogicky by sa dala definovať napríklad *voľná pologrupa* alebo *voľná grupa*. V skutočnosti dokonca možno voľnosť definovať konzistentne pre všetky „druhy algebraických štruktúr“, čo už je parketa univerzálnej algebry [3], alebo ešte všeobecnejšie na úrovni teórie kategórií [1], odkiaľ pochádza prívlastok „univerzálna“, ktorý je často používaný pre vlastnosť z definície 9.

### \* Polokruh formálnych jazykov

Nech  $\Sigma$  je abeceda. Množina  $2^{\Sigma^*}$  všetkých formálnych jazykov nad abecedou  $\Sigma$  tvorí s aditívnou operáciou zjednotenia a multiplikatívnou operáciou zretazovania polokruh, čo je algebraická štruktúra definovaná nasledovne:

**Definícia 10.** *Polokruh* je usporiadaná trojica  $(S, +, \cdot)$ , kde  $S$  je množina,  $+: S \times S \rightarrow S$  a  $\cdot: S \times S \rightarrow S$  sú binárne operácie na  $S$  a kde platí:

- (i)  $(S, +)$  je komutatívny monoid s neutrálnym prvkom  $0_S$ .
- (ii)  $(S, \cdot)$  je monoid s neutrálnym prvkom  $1_S$ .
- (iii) Platia distributívne zákony:  $\forall x, y, z \in S : (x + y) \cdot z = x \cdot z + y \cdot z$  a  $z \cdot (x + y) = z \cdot x + z \cdot y$ .
- (iv) Pre každé  $x \in S$  platí  $x \cdot 0_S = 0_S \cdot x = 0_S$ .

*Poznámka 1.* Takto definovaná štruktúra sa niekedy nazýva aj *polokruh s jednotkou*, pričom u všeobecného polokruhu sa nepožaduje existencia multiplikatívneho neutrálného prvku (teda v podmienke (ii) sa iba vyžaduje, aby  $(S, \cdot)$  bola pologrupa).<sup>2</sup> V teoretickej informatike sa však takmer výhradne používa horeuvedená definícia.

<sup>2</sup>Rovnaká situácia je aj pri definíciách okruhu, kde je ale obvyklejšia definícia bez jednotky.

**Tvrdenie 5.** *Nech  $\Sigma$  je abeceda. Potom  $(2^{\Sigma^*}, \cup, \cdot)$  je polokruh nazývaný polokruh formálnych jazykov nad  $\Sigma$ , s aditívnym neutrálnym prvkom  $\emptyset$  a multiplikatívnym neutrálnym prvkom  $\{\varepsilon\}$ .*

*Dôkaz.* Prenechávame čitateľovi ako elementárne cvičenie. □

*Homomorfizmus* medzi dvojicou polokruhov  $(S, +_S, \cdot_S)$  a  $(T, +_T, \cdot_T)$  je ľubovoľné zobrazenie  $h: S \rightarrow T$  také, že  $h(0_S) = 0_T$ ,  $h(1_S) = 1_T$  a pre všetky  $x, y \in S$  platí  $h(x +_S y) = h(x) +_T h(y)$  a  $h(x \cdot_S y) = h(x) \cdot_T h(y)$ . Ak homomorfizmus jazykov chápeme ako zobrazenie  $h: 2^{\Sigma^*} \rightarrow 2^{\Gamma^*}$ , je takto definované zobrazenie aj homomorfizmom v polokruhu formálnych jazykov. To platí vďaka identite  $h(L_1 \cup L_2) = h(L_1) \cup h(L_2)$  dokázanej v úlohe 1 a vďaka identite  $h(L_1 \cdot L_2) = h(L_1) \cdot h(L_2)$  dokázanej v úlohe 2.

### Literatúra

- [1] Adámek, J., Herrlich, H., Strecker, G. E.: *Abstract and Concrete Categories: The Joy of Cats*. Mineola, New York : Dover Publications, 2009. ISBN 978-0-486-46934-8. Dostupné online: <http://katmat.math.uni-bremen.de/acc/acc.pdf>.
- [2] Sakarovitch, J.: *Elements of Automata Theory*. Cambridge : Cambridge University Press, 2009. ISBN 978-0-521-84425-3.
- [3] Wechler, W.: *Universal Algebra for Computer Scientists*. Berlin, Heidelberg : Springer, 1992. ISBN 978-3-642-76773-9.