Cvičenie č. 2
Homomorfizmy a inverzné homomorfizmy

Peter Kostolányi

28. septembra 2022

1 Obraz a vzor množiny pri zobrazení

Obraz množiny $S \subseteq X$ pri zobrazení $f\colon X \to Y$ definujeme ako množinu

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

Ide teda o množinu všetkých obrazov prvkov množiny S.

Vzor – alebo *inverzný obraz* – množiny $T \subseteq Y$ pri zobrazení $f\colon X \to Y$ je množina

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

Vzor množiny T teda pozostáva z tých prvkov oboru zobrazenia, ktoré sa zobrazia do T.

Poznámka 1. V prípade, že je zobrazenie $f\colon X \to Y$ bijektívne, zvykne sa symbolom f^{-1} označovať *inverzné zobrazenie* k zobrazeniu f. Táto notácia súhlasí s práve zavedenou notáciou pre vzory: vzor množiny T pri bijektívnom zobrazení f je obraz množiny T pri inverznom zobrazení f^{-1}.

Vzor – alebo *inverzný obraz* – prvku $y \in Y$ možno pri ľubovoľnom – teda nie iba bijektívnom – zobrazení $f\colon X \to Y$ definovať ako vzor jednoprvkovej množiny $\{y\}$:

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

Ide teda o množinu prvkov X, ktoré sa zobrazia na y.

Poznámka 2. V prípade, že je zobrazenie $f\colon X \to Y$ bijektívne, je vzor $f^{-1}(y)$ každého prvku $y \in Y$ jednoprvková množina. To úplne nesúhlasí s notáciou pre inverzné zobrazenia, kde $f^{-1}(y)$ označuje priamo prvok tejto jednoprvkovej množiny. Krajšie by teda bolo zvoliť pre vzory inú notáciu – čo sa aj často robí.[1] My sa však budeme pridŕžať označenia zavedeného vyššie, ktoré je v oblasti jazykov a automatov zďaleka najbežnejšie. Požadovaná interpretácia symbolu $f^{-1}(y)$ navyše obyčajne býva zrejmá z kontextu, takže uvedenú nejednoznačnosť nie je nutné prežívať príliš tragicky.

2 Homomorfizmy

Pod *homomorfizmom* sa v matematike chápe štruktúru zachovávajúce zobrazenie (kde pod štruktúrou možno rozumieť napr. grupovú štruktúru, grafovú štruktúru, vektorovú štruktúru[2] a pod.). Štruktúra slov nad abecedou Σ je daná predovšetkým operáciou zreťazenia a pod homomorfizmom teda rozumieme zobrazenie, ktoré túto operáciu rešpektuje.

Definícia 1. Nech Σ, Γ sú abecedy. *Homomorfizmus* zo Σ^* do Γ^* je zobrazenie $h\colon \Sigma^* \to \Gamma^*$ také, že pre všetky $u, v \in \Sigma^*$ je

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

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

[1] Niektorí autori napríklad označujú obraz množiny S, vzor množiny T a vzor prvku y ako $f[S]$, $f^{-1}[T]$ a $f^{-1}[y]$; inde sa možno stretnúť s označeniami $f[S]$, $f^-[T]$ a $f^-[y]$, prípadne $f(S)$, $f^-(T)$ a $f^-(y)$.

[2] Homomorfizmy medzi vektorovými priestormi sú známejšie ako *lineárne zobrazenia*.

Dokážme najprv, že homomorfným obrazom prázdneho slova je vždy prázdne slovo.

Tvrdenie 1. *Nech Σ, Γ sú abecedy a $h\colon \Sigma^* \to \Gamma^*$ 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. □

Priamo z definície homomorfizmov dostávame jednoduchým induktívnym argumentom ich nasledujúcu vlastnosť.

Tvrdenie 2. *Nech Σ, Γ sú abecedy, $h\colon \Sigma^* \to \Gamma^*$ je homomorfizmus, $n \in \mathbb{N}$ a $w_1, w_2, \ldots, w_n \in \Sigma^*$. Potom $h(w_1 w_2 \ldots w_n) = h(w_1)h(w_2)\ldots h(w_n)$.*

Dôkaz. Pre $n = 0$ ide o dôsledok tvrdenia 1. Ak teraz dokazované tvrdenie platí pre $n = k \in \mathbb{N}$, pre ľubovoľné $w_1, \ldots, w_{k+1} \in \Sigma^*$ dostávame

$$h(w_1 \ldots w_k w_{k+1}) = h(w_1 \ldots w_k)h(w_{k+1}) = h(w_1)\ldots h(w_k)h(w_{k+1}),$$

kde prvá rovnosť je z definície homomorfizmu a druhá z indukčného predpokladu. □

Kľúčový význam má nasledujúca veta, podľa ktorej možno každé zobrazenie $f\colon \Sigma \to \Gamma^*$ rozšíriť na homomorfizmus $h\colon \Sigma^* \to \Gamma^*$, ktorý je navyše určený jednoznačne. Každý homomorfizmus $h\colon \Sigma^* \to \Gamma^*$ je teda jednoznačne určený obrazmi $h(c)$ jednotlivých písmen $c \in \Sigma$ a každé takéto priradenie obrazov písmenám naopak určuje homomorfizmus.

Veta 1. *Nech Σ, Γ sú abecedy a $f\colon \Sigma \to \Gamma^*$ je zobrazenie. Potom existuje* práve jeden *homomorfizmus $h\colon \Sigma^* \to \Gamma^*$ taký, že pre všetky $c \in \Sigma$ je $h(c) = f(c)$.*

Dôkaz. Uvažujme zobrazenie $h\colon \Sigma^* \to \Gamma^*$ dané pre všetky $k \in \mathbb{N}$ a všetky $a_1, a_2, \ldots, a_k \in \Sigma$ ako $h(a_1 a_2 \ldots a_k) = f(a_1)f(a_2)\ldots f(a_k)$. Evidentne $h(c) = f(c)$ pre všetky $c \in \Sigma$. Dokážeme, že ide o homomorfizmus. Nech $u, v \in \Sigma^*$; nech $m, n \in \mathbb{N}$ a $a_1, \ldots, a_m, b_1, \ldots, b_n \in \Sigma$ sú také, že $u = a_1 \ldots a_m$ a $v = b_1 \ldots b_n$. Potom skutočne

$$h(uv) = f(a_1)\ldots f(a_m)f(b_1)\ldots f(b_n) = h(u)h(v).$$

Pre ľubovoľný homomorfizmus $h'\colon \Sigma^* \to \Gamma^*$, všetky $k \in \mathbb{N}$ a všetky $a_1, a_2, \ldots, a_k \in \Sigma$ ďalej z tvrdenia 2 dostávame

$$h'(a_1 a_2 \ldots a_k) = h'(a_1)h'(a_2)\ldots h'(a_k).$$

Ak je teda $h'(c) = f(c)$ pre všetky $c \in \Sigma$, nutne

$$h'(a_1 a_2 \ldots a_k) = f(a_1)f(a_2)\ldots f(a_k) = h(a_1 \ldots a_k),$$

čo dokazuje jednoznačnosť homomorfizmu h. □

Homomorfizmy budeme zvyčajne zadávať práve homomorfnými obrazmi jednotlivých symbolov abecedy. Všimnime si tiež, že vďaka tvrdeniu 2 je homomorfizmus $h\colon \Sigma^* \to \Gamma^*$ nevymazávajúci práve vtedy, keď $h(c) \in \Gamma^+$ pre všetky $c \in \Sigma$. Ak je totiž táto podmienka splnená a $w = a_1 \ldots a_n$ pre nejaké $a_1, \ldots, a_n \in \Sigma$, je aj $h(w) = h(a_1 \ldots a_n) = h(a_1)\ldots h(a_n) \in \Gamma^+$.

3 Homomorfné obrazy jazykov a inverzný homomorfizmus

Nech Σ, Γ sú abecedy a $h\colon \Sigma^* \to \Gamma^*$ je homomorfizmus. V súlade s označeniami z oddielu 1 potom pre všetky jazyky $L \subseteq \Sigma^*$ kladieme

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

a jazyk $h(L)$ nazývame *homomorfným obrazom* jazyka L. Podobne možno definovať *inverzný homomorfný obraz* jazyka $L \subseteq \Gamma^*$ ako

$$h^{-1}(L) = \{w \in \Sigma^* \mid h(w) \in L\}$$

a *inverzný homomorfný obraz* slova $v \in \Gamma^*$ ako

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

Označenia $h(L)$ resp. $h^{-1}(L)$ vedú k predstave *homomorfizmu* a *inverzného homomorfizmu* ako „operácií“ na jazykoch, ktoré pre daný homomorfizmus $h\colon \Sigma^* \to \Gamma^*$ spočívajú v prechode od jazyka $L \subseteq \Sigma^*$ k jazyku $h(L)$ resp. od jazyka $L \subseteq \Gamma^*$ k jazyku $h^{-1}(L)$. Tento pohľad sa v teórii jazykov miestami objavuje v zaužívanej terminológii.

Príklad 1. Nech $\Sigma = \{a, b, c\}$ a $h\colon \Sigma^* \to \Sigma^*$ je homomorfizmus daný ako $h(a) = ac$, $h(b) = \varepsilon$ a $h(c) = b$. Potom napríklad

$$\begin{aligned} h(\{b, bb\}) &= \{\varepsilon\}, & h^{-1}(ac) &= b^*ab^*, \\ h(\{b, abb\}) &= \{\varepsilon, ac\}, & h^{-1}(abc) &= \emptyset, \\ h(\Sigma^*) &= \{ac, b\}^*, & h^{-1}(\{ac, b, bb\}) &= b^*ab^* \cup b^*cb^* \cup b^*cb^*cb^*, \\ h(\{a^nb^n \mid n \in \mathbb{N}\}) &= (ac)^*, & h^{-1}(\{a^nc^n \mid n \in \mathbb{N}\}) &= b^* \cup b^*ab^*. \end{aligned}$$

Dokážte uvedené rovnosti.

4 Ešte k definícii homomorfizmu

Monoid alebo *pologrupa s jednotkou* je trojica $(M, \cdot, 1)$, kde $\cdot\colon M \times M \to M$ je asociatívna binárna operácia na M – je teda $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pre všetky $a, b, c \in M$ – a 1 je neutrálny prvok vzhľadom na operáciu $\cdot$ – čiže $a \cdot 1 = 1 \cdot a = a$ pre všetky $a \in M$. Na rozdiel od definície *grupy* tu nevyžadujeme existenciu inverzných prvkov; od *pologrúp* sa zas monoidy odlišujú tým, že vždy musia obsahovať neutrálny prvok. Namiesto $(M, \cdot, 1)$ často píšeme len $(M, \cdot)$, alebo – ak je uvažovaná binárna operácia zrejmá z kontextu – iba M.

Už minule sme si všimli, že zreťazenie slov je nad ľubovoľnou abecedou asociatívne a prázdne slovo ε je neutrálnym prvkom vzhľadom na túto operáciu. Pre každú abecedu Σ teda dostávame monoid $(\Sigma^*, \cdot, \varepsilon)$. Tento monoid v literatúre obvykle dostáva prívlastok *voľný* nad Σ; dôvod tohto pomenovania pochádza z univerzálnej algebry a do jeho vysvetľovania sa tu púšťať nebudeme.

Homomorfizmus monoidov $(M, \cdot, 1_M)$ a $(N, \circ, 1_N)$ je zobrazenie $h\colon M \to N$ spĺňajúce nasledujúce dve podmienky:

(*i*) $h(1_M) = 1_N$,

(*ii*) $h(a \cdot b) = h(a) \circ h(b)$ pre všetky $a, b \in M$.

Na rozdiel napríklad od definície homomorfizmov grúp je nutné explicitne uviesť aj podmienku (*i*), pretože tá vo všeobecnosti nie je dôsledkom vlastnosti (*ii*).

Pre danú dvojicu abecied Σ a Γ teda zisťujeme, že homomorfizmus $h\colon \Sigma^* \to \Gamma^*$ nie je ničím iným, než homomorfizmom voľných monoidov $(\Sigma^*, \cdot, \varepsilon)$ a $(\Gamma^*, \cdot, \varepsilon)$ – vlastnosť (*i*) je tu dôsledkom tvrdenia 1 a vlastnosť (*ii*) vyplýva priamo z definície homomorfizmov.

5 Riešené úlohy

Úloha 1. Nech Σ, Γ sú abecedy, $L_1, L_2 \subseteq \Sigma^*$ jazyky a $h\colon \Sigma^* \to \Gamma^*$ homomorfizmus. Porovnajte jazyky $h(L_1 \cup L_2)$ a $h(L_1) \cup h(L_2)$.

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

- $\subseteq$: Nech $u \in h(L_1 \cup L_2)$. Potom existuje $v \in L_1 \cup L_2$ také, že $u = h(v)$. Keďže $v \in L_1 \cup L_2$, nutne $v \in L_1$ alebo $v \in L_2$ (prípadne aj oboje naraz). Ak $v \in L_1$, tak $u = h(v) \in h(L_1)$. Ak $v \in L_2$, tak $u = h(v) \in h(L_2)$. V oboch prípadoch $u \in h(L_1) \cup h(L_2)$.
- $\supseteq$: 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 existuje $v \in L_1$ také, že $u = h(v)$. Keďže $v \in L_1$, je aj $v \in L_1 \cup L_2$. Preto $u = h(v) \in h(L_1 \cup L_2)$, čo bolo treba dokázať. □

Úloha 2. Nech Σ, Γ sú abecedy, $L_1, L_2 \subseteq \Sigma^*$ jazyky a $h\colon \Sigma^* \to \Gamma^*$ homomorfizmus. Porovnajte jazyky $h(L_1 \cdot L_2)$ a $h(L_1) \cdot h(L_2)$.

Riešenie. Dokážeme, že $h(L_1 \cdot L_2) = h(L_1) \cdot h(L_2)$.

- $\subseteq$: 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 $u = h(x)h(y) = h(xy) \in h(L_1 \cdot L_2)$. □

Úloha 3. Nech Σ, Γ sú abecedy, $L_1, L_2 \subseteq \Gamma^*$ jazyky a $h\colon \Sigma^* \to \Gamma^*$ homomorfizmus. Porovnajte 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 homomorfizmus $h\colon a^* \to a^*$ 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 toho $h(u) \in L_1$ a $h(v) \in L_2$, takže $h(w) = h(uv) = h(u)h(v) \in L_1 \cdot L_2$, a teda $w \in h^{-1}(L_1 \cdot L_2)$. □

Úloha 4. Nech Σ, Γ sú abecedy, $L \subseteq \Gamma^*$ jazyk a $h\colon \Sigma^* \to \Gamma^*$ homomorfizmus. Porovnajte 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 $h\colon a^* \to a^*$ 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 $u \in h^{-1}(L)$, je $h(u) \in L$, a teda aj $w = h(u) \in L$. □

Úloha 5. Nech Σ, Γ sú abecedy, $L \subseteq \Sigma^*$ jazyk a $h\colon \Sigma^* \to \Gamma^*$ homomorfizmus. Porovnajte 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 $h\colon \{a, b\}^* \to a^*$ 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. □