Podpologrupy volné pologrupy a věta o defektu

Na rozdíl od grup nejsou podpologrupy volné pologrupy nutně volné. Například pologrupa $S = \langle X \rangle$ generovaná množinou $X = \{a, ab, ba\}$ není volná, protože $ab{\cdot}a = a \cdot ba$. Přitom platí, že X je nejmenší množina generátorů S. To je speciální případ následujícího obecného pravidla:

Lemma. Je-li S podpologrupa volné pologrupy, pak S má nejmenší (vzhledem k inkluzi) množinu generátorů $B = S \setminus S^2$.

Důkaz. Ukažme nejprve, že B generuje S. Předpokládejme pro spor, že w leží v S, ale neleží v $\langle B \rangle$, a nechť w je nejkratší možné. Protože $w \notin S \setminus S^2$, je $w \in S^2$, a tedy je součinem dvou slov $u, v \in S$. Protože $|u|, |v| < |w|$, platí $u, v \in \langle B \rangle$, a tedy také $w \in \langle B \rangle$, spor.

Nechť nyní $S = \langle B' \rangle$. Z definice B plyne, že žádný z jeho prvků není součinem dvou prvků z B'. Odtud plyne $B \subseteq B'$. $\square$

Množinu B z předchozího lemmatu nazýváme *bazí* pologrupy S a její velikost *hodností* pologrupy S. Jak ukazuje podpologrupa T pologrupy $\{a, b\}^*$ sestávající ze slov začínajících písmenem a, může mít pologrupa konečné hodnosti podpologrupu hodnosti nekonečné. Bazí takové pologrupy je totiž množina $\{ab^i \mid i \geq 0\}$.

Zopakujme, že báze je sice nejmenší generující množina dané pologrupy, ale výsledná pologrupa nemusí být volná. Generuje-li množina slov B volnou pologrupu, říkáme, že B je *kód*. Pokud navíc platí, že prvky B jsou po dvou prefixově (sufixově) nesrovnatelné, říkáme, že B je *prefixový* (*sufixový*) *kód*.

Následující lemmata charakterizují, kdy je pologrupa volná a kdy je generována prefixovým kódem.

Lemma. Pologrupa $S \subseteq \Sigma^+$ je volná, právě když pro libovolná slova $p, q, w \in \Sigma^+$ platí

$$p, q, pw, wq \in S \Longrightarrow w \in S\,. \tag{f}$$

Důkaz. Nechť je S volná a nechť $p, q, pw, wq \in S$. Pak také $pwq \in S$ a slova pw, wq a pwq mají jednoznačnou faktorizaci do prvků báze B_S pologrupy S. Nechť tedy $p = p_1 p_2 \cdots p_{i_p}$, $q = q_1 q_2 \cdots q_{i_q}$, $pw = b_1 b_2 \cdots b_{j_1}$ a $wq = c_1 c_2 \cdots c_{j_2}$ jsou takové faktorizace (tedy všechna p_i, q_i, b_i a c_i leží v B_S). Pak z rovnosti

$$p_1 p_2 \cdots p_{i_p} c_1 c_2 \cdots c_{j_2} = pwq = b_1 b_2 \cdots b_{j_1} q_1 q_2 \cdots q_{i_q}$$

dostáváme $p_k = b_k$, $k = 1, 2, \ldots, i_p$, a tedy $w = b_{i_p+1} b_{i_p+2} \cdots b_{j_1} \in S$.

Nechť nyní S není volná a nechť $b_1 b_2 \cdots b_j = c_1 c_2 \cdots c_k$ je nějaká co nejkratší netriviální relace mezi prvky B_S. Můžeme bez újmy na obecnosti předpokládat $b_1 < c_1$. Pak $p = b_1$, $q = c_2 c_3 \cdots c_k$ a $w = b_1^{-1} c_1$ nesplňují implikaci (`f`). $\square$

Podmínka (`f`) z předchozího lemmatu se nazývá *podmínka stability.*

Lemma. Pologrupa $S \subseteq \Sigma^+$ je generovaná prefixovým kódem, právě když pro libovolná slova $p, w \in \Sigma^+$ platí

$$p, pw \in S \Longrightarrow w \in S\,. \tag{p}$$

Důkaz. Nechť je S generována prefixovým kódem a nechť $p, pw \in S$. Nechť $p = b_1 b_2 \cdots b_j$ a $pw = c_1 c_2 \cdots c_k$ je faktorizace p a pw v bázi B_S. Protože B_S je prefixový kód, platí $b_i = c_i$, $i = 1, 2, \ldots, j$, a tedy $w = c_{j+1} c_{j+2} \cdots c_k \in S$.

Nechť B_S není prefixový kód. Pak existují prvky $b, b' \in B_S$ takové, že $b < b'$. Protože B_S je báze, platí $b^{-1}b' \notin B_S$ a důkaz je hotov. $\square$

Protože množiny splňující (f) jsou zjevně uzavřené na průnik, existuje minimální (vzhledem k inkluzi) volná pologrupa F obsahující danou množinu X. Takovou pologrupu nazýváme *volný obal* množiny X a píšeme $F = \langle X \rangle_{\mathtt{f}}$. Bázi F nazýváme *volnou bazí* množiny X a její kardinalitu, kterou značíme $\mathrm{rank}_{\mathtt{f}}(X)$, nazýváme *volnou hodností* množiny X.

Analogicky definujeme *prefixový obal* $\langle X \rangle_{\mathtt{p}}$, *prefixovou bázi* a *prefixovou hodnost* $\mathrm{rank}_{\mathtt{p}}(X)$ množiny X.

Následující lemma ukazuje další charakterizaci volné pologrupy.

Lemma. Nechť S je podpologrupa Σ^+. Označme S^* monoid $S \cup \{\varepsilon\}$ a definujme

$$L(S) = \left\langle \{u \in \Sigma^+ \mid uS^* \cap S^*u \cap S \neq \emptyset\} \right\rangle .$$

Pak S je volná, právě když $L(S) = S$.

Důkaz. Jistě $S \subseteq L(S)$. Nechť S není volná a nechť p, q, w splňují $p, q, pw, wq \in S$ a $w \notin S$. Pak

$$w \cdot (q \cdot pw) = (wq \cdot p) \cdot w = wq \cdot pw$$

implikuje $w \in L(S)$, a tedy $S \neq L(S)$.

Nechť naopak $L(S) \neq S$. Pak existuje $w \notin S$ takové, že $pw = wq \in S$ pro nějaká $p, q \in S$. Tedy S nesplňuje podmínku stability. $\square$

Lemma. Nechť X je konečná množina slov a B je volná báze $\langle X \rangle$. Pak pro každé $b \in B$ existuje $x \in X$ takové, že b je prvním (posledním) prvkem B-faktorizace slova x.

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že X je báze $\langle X \rangle$. Budeme postupovat indukcí podle celkové délky X, tedy podle $\sum_{u \in X} |u|$. Je-li celková délka X rovna jedné, tvrzení platí. Platí také, je-li X kód, tedy pokud $X = B$. Nechť X není kód a nechť $b_1 b_2 \cdots b_j = c_1 c_2 \cdots c_k$ je nějaká netriviální relace prvků z X. Můžeme bez újmy na obecnosti předpokládat, že $b_1 < c_1$. Nechť m je takový index, že $b_1 b_2 \cdots b_m < c_1$ a $c_1 < b_1 b_2 \cdots b_{m+1}$.

Označme $w = (b_1 b_2 \cdots b_m)^{-1} c_1$ a $X' = X \setminus \{c_1\} \cup \{w\}$.

Platí $\langle X \cup \{w\} \rangle = \langle X' \rangle$ a z podmínky stability plyne, že w je prvkem každé volné pologrupy obsahující X. Tedy $\langle X \rangle_{\mathtt{f}} = \langle X' \rangle_{\mathtt{f}}$.

Podle indukčního předpokladu je tedy každé $b \in B$ prvním prvkem B-faktorizace nějakého prvku $x \in X'$. Je-li $x \in X$, jsme hotovi. Je-li $x = w$, je b prvním prvkem B-faktorizace slova b_{m+1}. $\square$

Ukážeme jiný důkaz, který nevyžaduje, aby X byla konečná množina.

Důkaz. Předpokládejme, že $b \in B$ není prvním prvkem B-faktorizace žádného slova z $\langle X \rangle$. Označme

$$Z = (B \setminus \{b\})b^* = \{cb^i \mid b \neq c \in B\}.$$

Platí, že Z je kód, protože jednoznačná B-faktorizace každého slova $w \in \langle Z \rangle$ určuje jednoznačnou Z-faktorizaci slova w. Protože $\langle X \rangle \subseteq \langle Z \rangle \subsetneq \langle B \rangle$, dostáváme spor s minimalitou $\langle B \rangle$. $\square$

Předchozí lemma je základem pro důležitou větu, nazývanou „Věta o defektu“ nebo „Grafové lemma“.

Věta. Nechť slova z množiny $X = \{w_1, w_2, \dots, w_n\}$ splňují relace $(u_i, v_i) \in \Xi^+ \times \Xi^+$, $i \in I$, kde $\Xi = \{x_1, \dots, x_n\}$. Nechť $G = (X, H)$ je neorientovaný graf s hranami

$$H = \{\{\mathrm{pref}_1(u_i), \mathrm{pref}_1(v_i)\} \mid i \in I\}.$$

Pak $\mathrm{rank}_{\mathtt{f}}(X)$ je nejvýše roven počtu souvislých komponent grafu G.

Speciálně, volný rank množiny splňující netriviální relaci je menší než její kardinalita.

Důkaz. Nechť je B volná báze $\langle X \rangle$ a nechť b_i je první prvek B-faktorizace slova u_i. Podle předchozího lemmatu je $B = \{b_1, b_2, \dots, b_n\}$.

Označme $\psi : \Xi^+ \to X^+$ homomorfismus definovaný $\psi(x_i) = w_i$. Nechť je $\{x_j, x_k\}$ hrana v G a nechť $x_j = \mathrm{pref}_1(u_i)$ a $x_k = \mathrm{pref}_1(v_i)$. Protože slovo $\psi(u_i) = \psi(v_i)$ má jednoznačnou B-faktorizaci, paltí $b_j = b_k$. Odtud tvrzení plyne. $\square$