Komutující a konjugovaná slova

Věta. Nechť $u, v \in \Sigma^+$. Následující podmínky jsou ekvivalentní:

(a) $uv = vu$,
(b) $u^i = v^j$ pro nějaká $i, j \in \mathbb{N}$,
(c) $u = t^k$ a $v = t^\ell$ pro nějaké $t \in \Sigma^+$ a nějaká $k, \ell \in \mathbb{N}$.

Důkaz. (a) $\Longrightarrow$ (c). Pokud $|u| = |v|$, je $t = u = v$ a $k = \ell = 1$. Postupujme nyní indukcí podle $|uv|$. Je-li $|uv| = 2$, je $|u| = |v| = 1$ a jsme hotovi. BÚNO předpokládejme, že $|u| < |v|$, a nechť $w = u^{-1}v$. Pak $uuw = uwu$, a tedy $uw = wu$. Podle indukčního předpokladu tedy $u = t^k$ a $w = t^{\ell'}$ pro nějaké t a nějaká $k, \ell' \in \mathbb{N}$. Pak $v = uw = t^{k+\ell}$.

(c) $\Longrightarrow$ (b). Stačí volit $i = \ell$ a $j = k$.

(b) $\Longrightarrow$ (a). Pokud $|u| = |v|$, je také $u = v$ a $uv = vu$. Opět BÚNO předpokládejme, že $|u| < |v|$ a $v = uw$. Pak $v^j = (uw)^j = u^i = u^{-1}u^iu = (wu)^j$, a tedy $uw = wu$. Pak také $vu = uwu = uuw = uv$. □

Důsledek. Každé neprázdné slovo w je mocninou jediného primitivního slova t.

Slovo t z předchozího tvrzení se nazývá *primitivní kořen* slova w. Větu lze výrazně zesílit pomocí následujícího lemmatu. Symbolem $u \wedge v$ značíme nejdelší společný prefix slov u a v.

Lemma. Nechť $uv \neq vu$. Označme $z = uv \wedge vu$. Pak $z = uw_1 \wedge vw_2$ pro libovolná slova $w_1, w_2 \in \langle u, v\rangle$ taková, že $|uw_1| \geq |z|$ a $|vw_2| \geq |z|$.

Důkaz. Nechť $za \leq uv$ a $zb \leq vu$, kde a, b jsou písmena. Stačí ukázat, že $za \leq u^iv$ a $zb \leq v^iu$ pro každé $i \in \mathbb{N}$. Pro $i = 1$ to je zřejmé a dále postupujme indukcí. Slovo $u^{i+1}v$ má podle indukčního předpokladu prefix uz, což je také prefix uvu. Všechna tři slova mají tedy stejný prefix délky $|z| + 1$, tedy za, jak je vidět na slově uvu. Podobně ukážeme, že $zb \leq v^iu$. □

Příklad. Nechť $u = aaba$ a $v = aab$. Pak $z = uv \wedge vu = aabaa$. Vidíme tedy, že z může být delší obě slova u a v.

Důsledek. Pokud slova u a v splňují netriviální relaci, pak komutují.

Netriviální relací v předchozím důsledku formálně míníme dvojici (U, V) posloupností $U = (u_1, u_2, \ldots, u_n)$ a $V = (v_1, v_2, \ldots, v_m)$ takových, že $U \neq V$, a přesto $u_1u_2 \cdots u_n = v_1v_2 \cdots v_m$.

Množina slov, která žádnou netriviální relaci nesplňuje, se nazývá *kód*. Každé slovo generované kódem lze totiž jednoznačně „dekódovat“ do posloupnosti generátorů. Důsledek výše tedy říká, že dvě slova tvoří kód právě když nekomutují.

Pro tři slova žádné omezení na délku společného netriviální rovnosti neexistuje. Uvažme např. slova $x = ab$, $y = aba$ a $z = baa$, pro která platí $xy^\omega = yz^\omega$. Všimněme si navíc, že x, y, z tvoří kód. Slova, která nesplňují žádnou konečnou relaci, tedy mohou splňovat relaci nekonečnou. Taková relace je však pro tři slova nejvýše jedna, jak lze ukázat.

Můžeme si také všimnout, že konjugovaná slova x, y splňují „oboustranně nekonečnou“ relaci: $x^\mathbb{Z}$ a $y^\mathbb{Z}$ jsou až na posunutí stejná oboustranně nekonečná slova.

Ještě jiná situace nastává pro slova $x = aba$ a $y = b$: slovo $(xy)^\mathbb{Z}$ je rovno samo sobě při netriviálním posunu o dvě písmena.

Definice. Řekneme, že neprázdná slova x a y jsou konjugovaná, pokud existují slova u a v taková, že $x = uv$ a $y = vu$.

Všimněme si, že konjugovaná slova z definice splňují rovnost $xz = zy$, kde $z = u$. Toto pozorování lze obrátit na následující řešení jednoduché rovnice o třech neznámých.

Věta. Pro slova x, y a z, kde x je neprázdné, platí $xz = zy$, právě když existují slova u a v a přirozené číslo i takové, že $x = uv$, $y = vu$ a $z = (uv)^i u$.

Důkaz. Nechť $xz = zy$. Pokud je z kratší než x, existuje v takové, že $x = zv$ a $y = vz$, a tvrzení platí pro $u = z$ a $i = 0$. Je-li naopak x (ostře) kratší z, máme $z = xz'$ a $xz' = z'y$ a indukcí podle $|z|$ dostáváme slova u a v a číslo j splňující $x = uv$, $y = vu$ a $z' = (uv)^j u$. Nyní stačí uvážit, že $z = (uv)^{j+1}u$.

Obrácená implikace je zřejmá. □

Následující věta upřesňuje vlastnosti konjugovaných slov.

Věta. Nechť jsou slova x a y konjugovaná.

(a) Slovo x je primitivní, právě když je y primitivní.
(b) Slova x a y mají konjugované primitivní kořeny.
(c) Existuje právě jedna dvojice slov $(t_1, t_2) \in \Sigma^+ \times \Sigma^*$ taková, že t_1t_2 je primitivní kořen x a t_2t_1 je primitivní kořen y.

Důkaz. Nechť $x = uv = t^i$, kde t je primitivní kořen uv a $y = vu$. Pak existuje neprázdný prefix t_1 slova t a exponent $0 \leq j < i$ takové, že $u = t^j t_1$ a $v = t_2 t^{i-j-1}$, kde $t_2 = t_1^{-1}u$. Pak $y = (t_2t_1)^i$. Podobně dostaneme, že $x = (s_2s_1)^{i'}$, kde $s = s_1s_2$ je primitivní kořen y a $y = s^{i'}$. Z věty o komutujících slovech dostáváme $i = i'$ a $s = t_2t_1$, čímž je dokázáno (a) a (b).

Nechť nyní $t = t'_1t'_2$ a $s = t'_2t'_1$. BÚNO předpokládejme, že $|t_1| \leq |t'_1|$. Pak $t'_1 = t_1r$ a $t_2 = rt'_2$ pro nějaké r. Dostáváme $rs = rt'_2t'_1 = t_2t'_1 = t_2t_1r = sr$. Protože r je kratší než primitivní slovo s a komutuje s ním, musí být prázdné, což ukazuje (c). □

Následující věta dává ekvivalentní charakteristiku konjugovanosti.

Věta. Pro slova x, y, z platí $zx = yz$, právě když jsou x a y konjugovaná a $z \in t_2(t_1t_2)^*$, kde $(t_1, t_2) \in \Sigma^+ \times \Sigma^*$ je taková dvojice, že t_1t_2 je primitivní kořen slova x a t_2t_1 je primitivní kořen slova y.

Důkaz. Přímou implikaci dokážeme indukcí podle délky z. Předpokládejme nejprve $0 \leq |z| < |y|$. Pak $y = zz'$, kde $z = t_2(t_1t_2)^j$ a $z' = (t_1t_2)^{j'}t_1$ pro nějaké $0 \leq j$ a nějaký neprázdný sufix t_1 primitivního kořene $t = t_2t_1$ slova y. Pak $zx = zz'z = yz$ a $x = z'z = (t_1t_2)^{j+j'+1}$. Podle předchozí věty je t_1t_2 primitivní kořen x.

Je-li $|z| > |y|$, pak $z = yz' = z'x$ pro $z' = y^{-1}z$. Podle indukčního předpokladu platí $z' \in t_2(t_1t_2)^*$, kde $x \in (t_1t_2)^*$, a tedy také $z = z'x \in t_2(t_1t_2)^*$.

Obrácenou implikaci snadno ověříme. □