Principiální řešení a kanonický rozklad

Hovoříme-li o nějakém řešení α nějaké rovnice (u, v), budeme vždy předpokládat, že α zobrazuje jakoukoli neznámou, která se nevyskytuje v (u, v), na prázdné slovo.

Nechť $\alpha : \Xi^* \to A^*$ a $\beta : \Xi^* \to B^*$ jsou dvě řešení rovnice (u, v). Řekneme, že β *dělí* α, pokud existuje homomorfismus $\vartheta : \mathrm{alph}(\beta(u))^+ \to A^+$ takový, že $\alpha = \vartheta \circ \beta$.

Řešení α rovnice (u, v) nazveme *principiální*, pokud je minimální ve výše definovaném uspořádání dělitelnosti. Znamená to, že pokud $\alpha = \vartheta \circ \beta$, kde $\vartheta : \mathrm{alph}(\beta(u)) \to A^+$, pak ϑ je přejmenování písmen a $\beta = \vartheta^{-1} \circ \alpha$. Řešení, která se navzájem dělí, tj. taková, která se liší jen přejmenováním písmen, nazýváme *asociovaná* a budeme je ztotožňovat. Speciálně je přejmenování písmen asociované s identitou.

Všimněme si, že z principiálního řešení α lze získat neprincipiální řešení $\beta = \vartheta \circ \alpha$, pokud ϑ nezachovává délku, ale také pokud ji zachovává, ale není prosté (ztotožňuje různá písmena).

Indukcí lze snadno ukázat, že každé řešení je dělitelné nějakým principiálním řešením. Dále navíc ukážeme, že takové principiální řešení je dáno jednoznačně.

Nejprve se vypořádáme s mazacími řešeními tím, že je převedeme na nemazací řešení jiné rovnice, totiž té bez smazaných proměnných.

Věta. Buď $\alpha : \Xi^* \to \Sigma^*$ řešení rovnice (u, v). Označme Ξ' množinu neznámých x, pro které je $\alpha(x)$ neprázdné. Nechť π je projekce Ξ^* na $(\Xi')^*$ a nechť α' je restrikce α na Ξ'.

Pak je α principiální řešení (u, v), právě když je α' principiální řešení $(\pi(u), \pi(v))$.

Důkaz. Je-li $\alpha' = \vartheta \circ \beta'$, pak $\alpha = \vartheta \circ \beta$, kde

$$\beta(x) = \begin{cases} \beta'(x) & \text{pro } x \in \Xi', \\ \varepsilon & \text{pro } x \in \Xi \setminus \Xi'. \end{cases}$$

Z toho plyne přímá implikace.

Je-li $\alpha = \vartheta \circ \beta$, pak $\alpha' = \vartheta \circ \beta'$, kde β' je restrikce β na Ξ'. Z toho plyne, opačná implikace. □

Pro každé dva prvky $x, y \in \Xi$ definujeme homomorfismus $\varphi_{xy} : \Xi^+ \to \Xi^+$ takto:

$$\varphi_{xy}(z) = \begin{cases} xy, & \text{pokud } z = y \\ z, & \text{pokud } z \neq y\,. \end{cases}$$

Homomorfismy φ_{xy} nazýváme *regulární elementární transformace*. Dále definujeme *singulární elementární transformace* $\varepsilon_{xy} : \Xi^+ \to \Xi^+$ předpisem

$$\varepsilon_{xy}(z) = \begin{cases} x, & \text{pokud } z = y \\ z, & \text{pokud } z \neq y\,. \end{cases}$$

Řekneme, že elementární transformace φ je *příslušná* rovnici (u, v), pokud $u \neq v$ a $\varphi \in \{\varphi_{xy}, \varphi_{yx}, \varepsilon_{xy}\}$, kde $x \neq y$ jsou proměnné a platí $u = zxu'$ a $v = zyv'$ (tedy x a y jsou první proměnné, na kterých se strany rovnice liší).

Pro každé řešení α rovnice (u, v) definujeme jeho *kanonický rozklad příslušný rovnici* (u, v) jako

$$\alpha = \vartheta \circ \alpha_n \circ \alpha_{n-1} \cdots \circ \alpha_1 \circ \pi,$$

kde platí (prázdným homomorfismem rozumíme identitu):

- π je projekce,
- $\alpha_n \circ \alpha_{n-1} \circ \cdots \circ \alpha_1$ je řešení (u, v);
- ϑ je nemazací na abecedě slova $\alpha_n \circ \alpha_{n-1} \circ \cdots \circ \alpha_1(u)$.
- Pro každé $1 \leq k \leq n$ je α_k elementární transformace příslušná rovnici $(\alpha_{k-1} \circ \cdots \circ \alpha_1(u), \alpha_{k-1} \circ \cdots \circ \alpha_1(v))$.

Věta. Pro každé nemazací řešení existuje jednoznačný kanonický rozklad.

Důkaz. Pokud $u = v$, plyne z definic $n = 0$, a tedy $\alpha = \vartheta$ je jediný kanonický rozklad α.

Pokud $u \neq v$, máme $n \neq 1$ a $\alpha_1 \in \{\varphi_{xy}, \varphi_{yx}, \varepsilon_{xy}\}$, kde x a y jsou proměnné, na kterých se u a v poprve liší. Protože α je řešení (u, v), je α_1 jednoznačně určeno znaménkem $|\alpha(x)| - |\alpha(y)|$. Pokud totiž např. $\alpha_1 = \varphi_{xy}$, pak z rovností

$$\alpha(x) = \vartheta \circ \alpha_n \circ \cdots \circ \alpha_2(x) \quad \text{a} \quad \alpha(y) = \vartheta \circ \alpha_n \circ \cdots \circ \alpha_2(xy)$$

plyne, že $\alpha(x)$ je vlastní prefix $\alpha(y)$. Podobně v ostatních dvou případech.

Označme α' řešení rovnice $(u', v') := (\alpha_1(u), \alpha_1(v))$ splňující $\alpha' \circ \alpha_1 = \alpha$. Je-li $\alpha_1 = \varphi_{cd}$, jednoduše ověříme, že existuje jediné takové α', a to

$$\alpha'(z) = \begin{cases} \alpha(c)^{-1}\alpha(d) & \text{pokud } z = d, \\ \alpha(z) & \text{pro jiná } z \in \operatorname{alph}(\alpha_1(uv)). \end{cases}$$

Je-li $\alpha_1 = \varepsilon_{cd}$, pak výše uvedené tvrzení platí za předpokladu konvence, že $\alpha'(d) = \varepsilon$ pro d, které se nevyskytuje v (u', v').

Protože

$$\sum_{x \in \operatorname{alph}(u'v')} |\alpha'(x)| < \sum_{x \in \operatorname{alph}(uv)} |\alpha(x)|,$$

dostáváme indukcí existenci i jednoznačnost kanonického rozkladu. □

Předchozí věta umožňuje identifikovat jediné principiální řešení, které dělí dané řešení.

Věta. Nechť je α řešení rovnice (u, v). Pak existuje jediné principiální řešení β, které dělí α, a jediné ϑ takové, že $\alpha = \vartheta \circ \beta$ (jednoznačnost je až na asociovanost).

Navíc je kanonický rozklad α tvaru

$$\alpha = \vartheta \circ \alpha_n \circ \alpha_{n-1} \circ \cdots \circ \alpha_1 \circ \pi,$$

kde $\beta = \alpha_n \circ \alpha_{n-1} \circ \cdots \circ \alpha_1 \circ \pi$.

Důkaz. Nechť $\alpha = \vartheta \circ \beta$, kde β je principiální, a nechť $\vartheta' \circ \beta_m \circ \beta_{m-1} \circ \cdots \circ \beta_1 \circ \pi'$ je kanonický rozklad β. Protože je β principiální, můžeme předpokládat, že ϑ' je identita.

Zbývá ukázat, že $\vartheta \circ \beta_m \circ \beta_{m-1} \circ \cdots \circ \beta_1 \circ \pi'$ je kanonický rozklad α.

Zřejmě α a β mažou stejnou množinu neznámých, a proto $\pi' = \pi$.

Pokud $\pi(u) = \pi(v)$, je $m = n = 0$ a tvrzení platí. Je-li $\pi(u) \neq \pi(v)$, je $\beta_1 = \alpha_1$ elementární transformace příslušná rovnici $(\pi(u), \pi(v))$ jednoznačně určená α jako v předchozím důkazu. Tvrzení dokončíme indukcí.

□