

Syntaktická kongruence a syntaktický monoid. Řekneme, že *monoid* M *rozeznává jazyk* $L \subseteq \Sigma^*$, pokud existuje množina $F \subseteq M$ a homomorfismus $\varphi : \Sigma^* \rightarrow M$ takové, že $w \in L$, právě když $\varphi(w) \in F$; neboli $L = \varphi^{-1}(F)$. Množinu F přitom nemusíme předem zmiňovat, protože zjevně $F = \varphi(L)$. Stačí tedy požadovat existenci homomorfismu φ , pro který je $L = \varphi^{-1}\varphi(L)$.

Připomeňme, že *jádrem* homomorfismu φ rozumíme ekvivalenci $\sim_\varphi$ definovanou:

$$u \sim_\varphi v, \text{ právě když } \varphi(u) = \varphi(v).$$

Přitom platí, že jádro homomorfismu je vždy kongruence; a naopak, každá kongruence $\sim$ na Σ^* definuje homomorfismus

$$\varphi : \Sigma^* \rightarrow \Sigma^* / \sim$$

vztahem $\varphi(u) = [u]$, jehož jádrem je právě $\sim$ ($[u]$ značí třídu, ve které leží u).

Je tedy vidět, že monoidy rozeznávající jazyk L jsou dány kongruencemi monoidu Σ^* , pro které platí, že L se rozkládá na třídy této kongruence. Necht' je $\sim$ taková kongruence. Pak $u \sim v$ implikuje $rus \sim rvs$ pro každé r a s , neboli

$$(1) \quad \forall r, s \in \Sigma^* : rus \in L \Leftrightarrow rvs \in L.$$

Přímočaře lze ověřit, že pokud definujeme ekvivalenci $u \sim_s v$ vztahem (1), dostaneme kongruenci. Ta se nazývá *syntaktická kongruence* jazyka L . Z definice je vidět, že je to největší kongruence, pro kterou se jazyk L rozkládá na třídy. („Největší“ znamená, že má nejmenší počet tříd a všechny ostatní jsou jejím zjemněním.) Monoid $\Sigma^* / \sim_s$ se nazývá *syntaktický monoid* jazyka L , a je to tedy nejmenší monoid rozeznávající jazyk L . Uvidíme, že jazyk je regulární, právě když je jeho syntaktický monoid konečný.

Pravá kongruence a minimální automat. Definujeme

$$C_L(u) = \{(r, s) \mid rus \in L\}$$

množinu *kontextů* slova u v jazyce L . Syntaktická kongruence spojuje právě ta slova, která mají stejnou množinu kontextů. Tuto podmínku můžeme oslabit a definovat ekvivalenci $\sim_R$ (nazývanou též *Myhillova-Nerodova ekvivalence*) pouze pomocí pravých kontextů, tedy podmínkou

$$(2) \quad u \sim_R v \quad \text{právě když} \quad \forall s \in \Sigma^* : us \in L \Leftrightarrow vs \in L.$$

Tato ekvivalence nemusí být kongruencí (ověřte!). Je to ale tzv. *pravá kongruence* (nebo též *doprava invariantní ekvivalence*), tedy ekvivalence splňující, že $u \sim v$ implikuje $us \sim vs$ pro všechna s . Že $\sim_R$ je pravá kongruence, plyne přímočaře z (2) (ověřte!).

Je také snadné ověřit, že $\sim_R$ je největší pravá kongruence taková, že L se rozkládá na její třídy. Mějme totiž nějakou takovou pravou kongruenci $\sim$. Pak $u \sim v$ implikuje $(\forall s : us \sim vs)$, tedy z rozložitelnosti L na třídy dostáváme $(\forall s : us \in L \Leftrightarrow vs \in L)$, a proto $u \sim_R v$.

Uvažujme nyní nějaký konečný automat s počátečním stavem q_0 . Pokud $q_0 \cdot u = q_0 \cdot v$, pak i pro každé s platí $q_0 \cdot us = q_0 \cdot vs$, tedy $u \sim_R v$. Ekvivalence $\sim_R$ identifikuje slova, která vedou ke stejnému stavu. Tím je dokázáno, že pro každý regulární jazyk má ekvivalence $\sim_R$ konečný index (tj. konečný počet tříd): tříd je nejvýše tolik, kolik je stavů automatu (tedy automat má alespoň tolik stavů, kolik je tříd).

To vede k nápadu, vytvořit automat, jehož stavy budou naopak pro daný jazyk odpovídat třídám ekvivalence $\sim_R$. Takový automat skutečně existuje a je to nejmenší automat rozeznávající daný jazyk. Nechť je tedy L regulární jazyk. Deterministický automat

$$\mathcal{A} = (\Sigma^*/\sim_R, \Sigma, [\varepsilon], \delta, L/\sim_R),$$

kde přechodová funkce δ je dána vztahem $[w] \cdot a = [wa]$, se nazývá *minimální automat jazyka L* . Ověřit, že $\mathcal{A}$ rozeznává L , je přímočaré (proved'te!). Výše jsme viděli, že počet stavů automatu nemůže být menší než index $\sim_R$, a $\mathcal{A}$ je tedy opravdu minimální, co do počtu stavů.

Je-li $\mathcal{A}'$ nějaký deterministický automat se stejným počtem stavů jako minimální automat (a počátečním stavem q_0), je snadné ověřit (proved'te!), že zobrazení $\psi : \mathcal{A}' \rightarrow \mathcal{A}$ dané předpisem $\psi : q \mapsto [u]$, kde u je nějaké slovo splňující $q_0 \cdot u = q$, je isomorfismus automatů. Takové slovo určitě existuje, protože jinak by byl stav q nedosažitelný a bylo by možné ho ve sporu s minimalitou automatu vynechat. Minimální automat je tedy jediný až na isomorfismus.

Syntaktický monoid a přechody minimálního automatu. Viděli jsme, že syntaktická kongruence definuje minimální monoid rozeznávající daný jazyk, zatímco Myhillova-Nerodova ekvivalence definuje minimální takový automat. Ukážeme, jaká je mezi oběma objekty souvislost.

Uvažujme deterministický automat $A = (Q, \Sigma, q_0, \delta, F)$. Každé slovo $u \in \Sigma^*$ určuje zobrazení $\tau_u : Q \rightarrow Q$ dané vztahem $\tau_u(q) = q \cdot u$, tzv. *transformací množiny stavů*. Na transformacích definujeme operaci skládání zleva:

$$\tau_u \circ \tau_v(q) := \tau_v(\tau_u(q)),$$

čímž vznikne *transformační monoid automatu $\mathcal{A}$* :

$$T := (\{\tau_u \mid u \in \Sigma^*\}, \circ).$$

Souvislost mezi syntaktickým monoidem a minimálním automatem je nyní dána následujícím tvrzením.

Věta. *Syntaktický monoid jazyka L je isomorfní transformačnímu monoidu jeho minimálního automatu.*

Důkaz. Ukážeme, že zobrazení $\psi : [u] \mapsto \tau_u$ je hledaný isomorfismus $\Sigma/\sim$ a T . Nejprve ověříme, že ψ je dobře definované, tj. $u \sim v$ implikuje $\tau_u = \tau_v$. Nechť $\tau_u \neq \tau_v$. Existuje tedy $[s] \in \Sigma/\sim$ takové, že $\tau_u([s]) \neq \tau_v([s])$. Z definic dostáváme

$$\tau_u([s]) = [s] \cdot u = [su] \neq \tau_v([s]) = [s] \cdot u = [sv].$$

Tedy $su \not\sim sv$, a proto také $u \not\sim v$.

Platí $\tau_{uv} = \tau_u \circ \tau_v$ (ověřte!), a ψ je tedy homomorfismus. Protože je zjevně na, zbývá ukázat, že je prostý. Nechť $[u] \neq [v]$. Pak existují slova r, s taková, že $rus \in L$ není ekvivalentní $rvs \in L$. Tudíž $[rus] \neq [rvs]$, proto i $[ru] \neq [rv]$, a tedy $[r] \cdot u \neq [r] \cdot v$. To znamená, že $\tau_u([r]) \neq \tau_v([r])$, a tedy $\tau_u \neq \tau_v$. $\square$