0.0.1 Jak dokázat, že daný automat přijímá daný jazyk.

Obvykle není problém vymyslet si pro daný regulární jazyk L *nějaký* automat, problém je *dokázat*, že funguje, tj. že přijímá správný jazyk.

Vyzkoušením činnosti automatu na několika příkladech lze prokázat, že automat funguje špatně (přijímá, co nemá, nebo nepřijímá, co má), ale nelze už tak snadno prokázat, že na všech nekonečně mnoha slovech funguje dobře.

Jednou z možností, jak dokázat, že automat přijímá daný jazyk, je využití Nerodovy věty — metoda invariantů.

Každému stavu q přiřadíme přesný popis všech slov, které převedou počáteční stav q_0 do stavu q. Tím popíšeme jednotlivou třídu ekvivalence T z Nerodovy věty. To se většinou dělá pomocí formule $I_q(u)$ (kde slovo u je proměnná); a tuto formuli nazveme *invariantem* pro stav q. Abychom opravdu dokázali, že náš automat pracuje správně, musí

1. Prázdné slovo splňovat invariant pro počátečního stavu q_0 (I_{q_0}).
2. Každé slovo u nad vstupní abecedou musí splňovat právě jeden invariant (tj. každé slovo u leží v právě jedné třídě ekvivalence T).
3. Pro každý stav q a každý vstupní symbol x platí implikace *Jestliže slovo u odpovídá invariantu $I_q(u)$, pak slovo ux odpovídá invariantu $I_{\delta(q,x)}(ux)$.* Tj.
$$I_q(u) \Rightarrow I_{\delta(q,x)}(ux) \quad .$$
4. Pro každé slovo nad vstupní abecedou platí, že $u \in L$ právě tehdy, když u splňuje invariant pro některý koncový stav $q \in F$ (tj. platí $I_q(u)$ pro nějaký koncový stav q).

Vymyslet invarianty nemusí být úplně snadné, ale jsou-li již vymyšleny, pak ověření výše uvedených podmínek je již rutinní záležitostí.

0.0.2 Věta o invariantech.

Mějme konečný automat $M = (Q, \Sigma, \delta, q_0, F)$. Pro každý stav $q \in Q$ mějme formuli (které budeme říkat *invariant*) $I_q(u)$, s proměnnou u. Předpokládejme, že množina všech invariantů splňuje tyto tři předpoklady:

I1: Platí $I_{q_0}(\varepsilon)$, tj. prázdné slovo ε splňuje invariant počátečního stavu q_0.

I2: Pro každý stav $q \in Q$, každé písmeno $x \in \Sigma$ a každé slovo $u \in \Sigma^\star$ platí implikace

$$I_q(u) \;\Rightarrow\; I_{\delta(q,x)}(ux)$$

tj. když jakékoli slovo u splňovalo invariant I_q, pak slovo ux splňuje invariant $I_{\delta(q,x)}$ následujícího stavu $\delta(q, x)$.

I3: Pro každé slovo $u \in \Sigma^\star$ existuje právě jeden stav $q \in Q$ takový, že $I_q(u)$, tj. takový, že slovo u splňuje invariant I_q.

Pak pro každé slovo $u \in \Sigma^\star$ platí

$$\delta^\star(q_0, u) = q \quad\Longleftrightarrow\quad I_q(u)\ , \tag{1}$$

jinak řečeno, po přečtení libovolného slova u se automat převede do přesně toho stavu q, jehož invariant slovo u splňuje.

Důkaz. Nejprve indukcí podle délky slova u dokážeme implikci „$\Rightarrow$“, tedy implikaci

$$\delta^\star(q_0, u) = q \;\Rightarrow\; I_q(u) \tag{2}$$

Pro prázdné slovo $u = \varepsilon$ tvrzení (2) vyplývá z předpokladu I1.

Předpokládejme nyní, že tvrzení (2) platí pro všechna slova délky n, a dokážeme, že potom tvrzení (2) platí také pro slova délky $n + 1$. Vezměme libovolné slovo u délky $n + 1$, označme x jeho poslední písmeno a označme v počáteční úsek slova takový, že $u = vx$. Dále označme $p = \delta^\star(q_0, v)$ a také $q = \delta(p, x) = \delta^\star(q_0, u)$.

Délka slova v je n, proto podle indukčního předpokladu pro slovo v platí implikace (2), tedy slovo v splňuje invariant I_p, tj. platí $I_p(v)$.

Podle předpokladu I2 platí implikace $I_p(v) \Rightarrow I_{\delta(p,x)}(vx)$. Slovo $u = vx$ tedy splňuje invariant $I_{\delta(p,x)} = I_q$. Tím je dokázán druhý krok indukce. Implikace (2) je tedy dokázána pro slova u libovolné délky.

Obrácenou implikaci dokážeme s využitím předpokladu I3. Předpokládejme, že slovo u splňuje invariant I_q, tj. platí $I_q(u)$. Označme $p = \delta(q_0, u)$. Podle již dokázaného tvrzení (2) pak slovo u splňuje také invariant I_p. Podle předpokladu I3 pak musí platit $p = q$, tedy $\delta(q_0, u) = q$.

Důsledek. Za stejných předpokladů pak platí

$$u \in L \quad\Longleftrightarrow\quad \exists q_f \in F \;\; (I_{q_f}(u))\ ,$$

tj. slovo u je přijímáno automatem právě tehdy, když splňuje invariant I_{q_f} některého koncového stavu $q_f \in F$.

Tento důsledek lze využít k důkazu, že daný automat přijímá jazyk definovaný nějakou předepsanou vlastností.