Теория и реализация языков программирования. Доказательство алгоритма Brzozowski ($\mathrm{DRDR}\mathcal{A} \cong \mathcal{A}_{\min}$)

Сергей Володин, 272 гр.

10 декабря 2013 г.

Доказательство основано на доказательстве со стр. 116-117 книги «Elements of Automata Theory», Jacques Sakarovitch

1. До того, как не указано обратное считаем, что у автоматов нет ε-переходов.
Обобщим определение конечного автомата: $\mathcal{A} = (Q, \Sigma, \delta, I, F)$, где I вместо q_0 — множесто начальных состояний.
$w \in L(\mathcal{A}) \overset{\text{def}}{\Leftrightarrow} \exists i \in I \colon (i, w) \vdash^* (q, \varepsilon), q \in F$, где $\vdash^*$ — из изначального определения. Автомат называем детерминированным, если $|I| = 1$, и он детерминированный в смысле изначального определения.

2. Определим $\mathrm{R}\mathcal{A} \overset{\text{def}}{=} (Q, \Sigma, \delta^r, F, I)$ — автомат с обращенными переходами, распознающий $L(\mathcal{A})^r$. $\delta^r(p, a) \ni q \Leftrightarrow \delta(q, a) \ni p$. (отличие от изначального алгоритма в том, что не создается ε-переходов и новых состояний).
   - Пусть $|I| = 1$. Тогда у $\mathrm{R}\mathcal{A}$ одно принимающее состояние.
   - По построению, $\mathrm{RR}\mathcal{A} = \mathcal{A}$.

3. Определим $\mathrm{D}\mathcal{A} \overset{\text{def}}{=} (Q', \Sigma, \delta, I', F')$ — автомат, полученный детерминизацией $\mathcal{A}$ по модифицированному алгоритму:
   - Пусть $|I| > 1$. В начале соединим ε-переходами все начальные состояния, и выберем в качестве нового начального какое-нибудь одно. Очевидно, полученный автомат будет эквивалентен исходному, но он уже будет иметь одно начальное состояние. Далее выполним исходный алгоритм.
   - В определении указана та же функция переходов, что и у $\mathcal{A}$. Имеется в виду, что δ доопределена следующим образом на множествах состояний исходного автомата: $\delta(X, a) = \bigcup\limits_{x \in X} \delta(x, a)$. Заметим, что именно такую функцию переходов даст алгоритм: $\delta^{\text{alg.}}(X, a) = \bigcup\limits_{x \in X} \varepsilon\text{-closure}(\delta(x, a))$, и ε-переходов в исходном автомате нет (кроме тех, которые соединяют старые начальные, но все эти состояния будут объединены в одно множество-состояние, поэтому равенство сохранится).

4. Пусть $\mathcal{A} = (Q, \Sigma, \delta, I, F)$ — НКА, причем $\mathrm{R}\mathcal{A}$ — детерминированный, и все его состояния достижимы. Тогда $\mathrm{D}\mathcal{A} \cong \mathcal{A}_{\min}$.
   (a) $L \overset{\text{def}}{=} L(\mathcal{A})$. $\mathrm{R}\mathcal{A}$ — детерминированный, поэтому имеет одно начальное состояние. Значит, $\mathcal{A}$ имеет одно принимающее состояние: $F = \{f\}$.
   (b) Пусть $x, y \in \Sigma^* \colon x \sim_L y$. Докажем, что $\delta(I, x) = \delta(I, y)$.
   Действительно, пусть $\underline{p \in \delta(I, x)}$. Тогда $\exists i \in I \colon i \xrightarrow{x} p$. Поскольку все состояния $\mathrm{R}\mathcal{A}$ достижимы по условию (из его начального состояния f), имеем слово z и путь $p \xrightarrow{z} f$ в $\mathcal{A}$. Получаем, $i \xrightarrow{x} p \xrightarrow{z} f \in F$, и $xz \in L$. Но $x \sim y$, значит, $yz \in L$. Значит, $\exists i' \in I \colon (i', yz) \vdash^* (f, \varepsilon)$. Пусть перед прочтением z автомат находился в p'. Тогда $p' \xrightarrow{z} f$. $\mathrm{R}\mathcal{A}$ — детерминированный, поэтому в нем путь из f по z единственный, поэтому $p = p'$. Значит, $i' \xrightarrow{y} p \xrightarrow{z} f$, т.е. $\delta(i', y) \ni p$, а, значит, $\underline{p \in \delta(I, y)}$. Аналогично доказывается обратное включение $\delta(I, y) \subseteq \delta(I, x)$.
   (c) Заметим, что задана функция φ, сопоставляющая классу эквивалентности некоторое состояние автомата $\mathrm{D}\mathcal{A}$: классу с представителем x сопоставлено состояние $\delta(I, x)$. Корректность (значение функции не зависит от выбора представителя класса) как раз доказана выше.
   (d) Поскольку все состояния $\mathrm{D}\mathcal{A}$ достижимы, φ — сюръективно: состояние $\delta(I, w)$ можно выразить как $\varphi(C(w))$. Отсюда следует, что количество состояний $\mathrm{D}\mathcal{A}$ не больше, чем $|\Sigma^* / \sim_L|$. Значит, эти числа равны.
   (e) Изоморфизм между каноническим минимальным автоматом и $\mathrm{D}\mathcal{A}$ уже построен: действительно, φ — биекция (сюръективность + равенство мощностей $\mathrm{E}\varphi$ и $\mathrm{D}\varphi$). Также φ сохраняет переходы:
      i. Пусть $C(w) \xrightarrow{a} C(wa)$ (переходы на классах эквивалентности).
      Тогда $\varphi(C(w)) = \delta(I, w) \xrightarrow{a} \delta(\delta(I, w), a) = \delta(I, wa) = \varphi(C(wa))$.
      ii. Пусть $X \xrightarrow{a} Y$ (переходы на состояниях).
      $X = \delta(I, w)$. Тогда $\delta(I, wa) = Y$, $X = \varphi(C(w))$, и $\varphi^{-1}(X) = C(w) \xrightarrow{a} C(wa) = \varphi^{-1}(Y)$.

   $\blacksquare$

5. Пусть дан НКА $\mathcal{A}$. Построим $\mathcal{B} \overset{\text{def}}{=} \mathrm{RDR}\mathcal{A}$. $\mathrm{R}\mathcal{B} \equiv \mathrm{DR}\mathcal{A}$ — детерминированный, все его состояния достижимы. Тогда $\mathrm{D}\mathcal{B} \cong \mathcal{B}_{\min} = \mathcal{A}_{\min}$, так как $L(\mathcal{B}) = L(\mathcal{A})^{R^R} = L(\mathcal{A})$, т.е. $\boxed{\mathrm{DRDR}\mathcal{A} \cong \mathcal{A}_{\min}}$

6. Заметим, что доказываемая изоморфность сохранится, если разрешить ε-переходы в $\mathcal{A}$, т.к. ε-переходов уже не будет после первой детерминизации $\mathrm{DR}\mathcal{A}$.