Лесен пример за разбиране на коректност на автомат

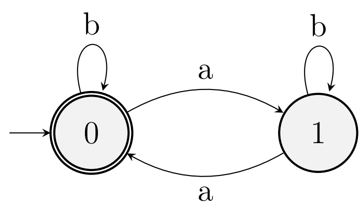
Иво Стратев

9 юни 2020 г.

Разглеждаме един от най-простите езици

$$\mathcal{L} = \{\omega \in \{a, b\}^* \mid \mathcal{N}_a(\omega) \equiv 0 \pmod 2\}$$

Един очевиден автомат за този език е



Формално $\mathcal{A} =< \{a, b\}, \{0, 1\}, 0, \delta, \{0\} >$, където

$$\begin{aligned}
\delta(0, b) &= 0 \\
\delta(0, a) &= 1 \\
\delta(1, b) &= 1 \\
\delta(1, a) &= 0
\end{aligned}$$

Искаме да докажем, че автомата $\mathcal{A}$ разпознава точно езика $\mathcal{L}$. Тоест $\mathcal{L}(\mathcal{A}) = \{\omega \in \{a, b\}^* \mid \delta^*(0, \omega) \in \{0\}\} = \mathcal{L}$. За тази цел формулираме по една лема за всяко състояние, с която целим да докажем кои са езиците съотвестващи на всяко състояние. Тоест как изглеждат думите, които стигат (привършват) до конкретно състояние. Конкретно за разглеждания пример лемите са следните:

$$(\forall \omega \in \{a, b\}^*)(\delta^*(0, \omega) = 0 \longleftrightarrow \mathcal{N}_a(\omega) \equiv 0 \pmod 2)$$
$$(\forall \omega \in \{a, b\}^*)(\delta^*(0, \omega) = 1 \longleftrightarrow \mathcal{N}_a(\omega) \equiv 1 \pmod 2)$$

Сега ако $q \in \{0, 1\}$ (е състояние на дадения автомат), то езика съответстващ на това състояние ще бележим с $\mathcal{L}_{\mathcal{A}}(q)$ и

$$\mathcal{L}_{\mathcal{A}}(q) = \{\omega \in \{a, b\}^* \mid \delta^*(0, \omega) = q\}$$

Съответно ако означим с $L_i = \{\omega \in \{a, b\}^* \mid \mathcal{N}_a(\omega) \equiv i \pmod 2\}$ за $i \in \{0, 1\}$. То двете твърдения, които искаме да докажем можем да запишем като

$$(\forall \omega \in \{a, b\}^*)(\omega \in \mathcal{L}_{\mathcal{A}}(0) \longleftrightarrow \omega \in L_0)$$
$$(\forall \omega \in \{a, b\}^*)(\omega \in \mathcal{L}_{\mathcal{A}}(1) \longleftrightarrow \omega \in L_1)$$

, които са еквивалетни с $\mathcal{L}_{\mathcal{A}}(0) = L_0$ & $\mathcal{L}_{\mathcal{A}}(1) = L_1$. Вземайки предвид, че $\mathcal{L} = L_0$ и $\mathcal{L}(\mathcal{A}) = \mathcal{L}_{\mathcal{A}}(0)$. Ще получим желаното твърдение $\mathcal{L}(\mathcal{A}) = \mathcal{L}$.

Забележка:

В общия случай, когато автомата има повече от едно финално състояние и искаме да докажем, че $\mathcal{L}(\mathcal{A}) = \mathcal{L}$. То преди да докажем, че $\mathcal{L}_{\mathcal{A}}(q) = L_q$ е добре да докажем, че $\mathcal{L} = \bigcup\limits_{q \in F} L_q$, за да сме сигурни, че не изпускаме нещо. Това трябва задължително да се докаже, но ако започнем с него може да хванем някой бъг предварително ;). Равенството $\mathcal{L}(\mathcal{A}) = \bigcup\limits_{q \in F} \mathcal{L}_{\mathcal{A}}(q)$ е винаги в сила. Ето бързо доказателство:

$$\mathcal{L}(\mathcal{A}) = \{\omega \in \{a, b\}^* \mid \delta^*(0, \omega) \in F\} =$$
$$\bigcup_{q \in F} \{\omega \in \{a, b\}^* \mid \delta^*(0, \omega) = q\} = \bigcup_{q \in F} \mathcal{L}_{\mathcal{A}}(q)$$

Обрато към нашия пример. Нека с $\varphi(\alpha)$ означим свойството

$$((\alpha \in \mathcal{L}_{\mathcal{A}}(0) \longleftrightarrow \alpha \in L_0) \mathbin{\&} (\alpha \in \mathcal{L}_{\mathcal{A}}(1) \longleftrightarrow \alpha \in L_1))$$

. Доказателството на $\mathcal{L}_{\mathcal{A}}(0) = L_0$ & $\mathcal{L}_{\mathcal{A}}(1) = L_1$ ще направим чрез индукция по построението на $\{a, b\}^*$. Тоест доказваме твърденията едновременно по следната схема:

1. $\varphi(\varepsilon)$

2. Ако $\omega \in \{a,b\}^*$ и $u \in \{a,b\}$ и за ω твърдението е в сила, тоест $\varphi(\omega)$ е истина, то показваме и че за $\omega.u$ е в сила, тоест $\varphi(\omega.u)$ е истина

, с което същност доказваме

$$(\forall\omega \in \{a,b\}^*)((\omega \in \mathcal{L}_{\mathcal{A}}(0) \longleftrightarrow \omega \in L_0) \: \& \: (\omega \in \mathcal{L}_{\mathcal{A}}(1) \longleftrightarrow \omega \in L_1))$$

, от където вече следва желаното.

Доказателство (стигнахме и до него ...)

За ε:

По дефиниция $\delta^*(0,\varepsilon) = 0$. От друга страна $\mathcal{N}_a(\varepsilon) = 0$ и $0 \equiv 0 \pmod 2$. Така очевидно е вярно твърдението $\varepsilon \in \mathcal{L}_{\mathcal{A}}(0) \longleftrightarrow \varepsilon \in L_0$. От друга страна $\delta^*(0,\varepsilon) = 1$ не е вярно и значи от това следва $\mathcal{N}_a(\varepsilon) \equiv 1 \pmod 2$ (тривиално следствие). Тоест вярно е $\varepsilon \in \mathcal{L}_{\mathcal{A}}(1) \longrightarrow \varepsilon \in L_1$. По аналогични причини директно следва $\varepsilon \in L_1 \longrightarrow \varepsilon \in \mathcal{L}_{\mathcal{A}}(1)$. Значи $\varphi(\epsilon)$ е истина.

Стъпка:

Нека $\omega \in \{a,b\}^*$ и $u \in \{a,b\}$ и за ω твърдението е в сила, тоест $\varphi(\omega)$ е истина. Ще покажем $\varphi(\omega.u)$. Ще докажем двете твърдения в двете посоки. Като първо ще докажем двете посоки от ляво на дясно, след това двете от дясно на ляво.

1. Нека $\delta^*(0,\omega.u) = 0$. Понеже $\delta^*(0,\omega.u) = \delta(\delta^*(0,\omega),u) = 0$, то са възможни само два случая $\delta^*(0,\omega) = 0 \: \& \: u = b$ или $\delta^*(0,\omega) = 1 \: \& \: u = a$. Другите два случая не са възможни, няма как да се реализират заради дефиницията на δ функцията и δ^*. Ако $\delta^*(0,\omega) = 0$ и $u = b$, то от $\varphi(\omega)$, имаме че $\mathcal{N}_a(\omega) \equiv 0 \pmod 2$, тогава очевидно $\mathcal{N}_a(\omega.b) \equiv 0 \pmod 2$ и значи $\omega \in L_0$. Ако $\delta^*(0,\omega) = 1$ и $u = a$, то от $\varphi(\omega)$, имаме че $\mathcal{N}_a(\omega) \equiv 1 \pmod 2$, тогава очевидно $\mathcal{N}_a(\omega.a) \equiv 1 + 1 \equiv 0 \pmod 2$ и значи $\omega \in L_0$. Така получава, че е вярно твърдението $\omega \in \mathcal{L}_{\mathcal{A}}(0) \longrightarrow \omega \in L_0$.

2. Нека $\delta^*(0,\omega.u) = 1$. Аналогично понеже $\delta^*(0,\omega.u) = \delta(\delta^*(0,\omega),u) = 1$, то са възможни само два случая $\delta^*(0,\omega) = 1 \: \& \: u = b$ или

$\delta^*(0,\omega) = 0$ & $u = a$. Другите два случая не са възможни, няма как да се реализират заради дефиницията на δ функцията и δ^*. Ако $\delta^*(0,\omega) = 1$ и $u = b$, то имаме, че $\mathcal{N}_a(\omega) \equiv 1 \pmod 2$, тогава очевидно $\mathcal{N}_a(\omega.b) \equiv 1 \pmod 2$ и значи $\omega \in L_1$. Ако $\delta^*(0,\omega) = 0$ и $u = a$, то имаме, че $\mathcal{N}_a(\omega) \equiv 0 \pmod 2$, тогава очевидно $\mathcal{N}_a(\omega.a) \equiv 0 + 1 \equiv 1 \pmod 2$ и значи $\omega \in L_1$. Така получава, че е вярно твърдението $\omega \in \mathcal{L}_{\mathcal{A}}(1) \longrightarrow \omega \in L_1$.

3. Нека $\mathcal{N}_a(\omega.u) \equiv 0 \pmod 2$. Тогава са възможни само два случая $\mathcal{N}_a(\omega) \equiv 0 \pmod 2$ & $u = b$ или $\mathcal{N}_a(\omega) \equiv 1 \pmod 2$ & $u = a$. Ако $\mathcal{N}_a(\omega) \equiv 0 \pmod 2$ и $u = b$. Тогава понеже $\varphi(\omega)$, то $\delta^*(0,\omega) = 0$. Тогава $\delta^*(0,\omega.u) = \delta(\delta^*(0,\omega), b) = \delta(0,b) = 0$. Ако $\mathcal{N}_a(\omega) \equiv 1 \pmod 2$ и $u = a$. Тогава понеже $\varphi(\omega)$, то $\delta^*(0,\omega) = 1$. Тогава $\delta^*(0,\omega.u) = \delta(\delta^*(0,\omega), a) = \delta(1,a) = 0$. Така получаваме, че е в сила $\omega \in L_0 \longrightarrow \omega \in \mathcal{L}_{\mathcal{A}}(0)$.

4. Нека $\mathcal{N}_a(\omega.u) \equiv 1 \pmod 2$. По аналогични на разсъжденията за предното получаваме $\omega \in L_1 \longrightarrow \omega \in \mathcal{L}_{\mathcal{A}}(1)$ ...

Така очевидно е вярно $\varphi(\omega.u)$. Така както вече казахме получаваме $\mathcal{L}(\mathcal{A}) = \mathcal{L}_{\mathcal{A}}(0) = L_0 = \mathcal{L}$.

За формалистите:

Формално се възползваме от това, че в множеството $\{a,b\}^*$ можем да правим индукция. Защо ще разберете когато стигнете 3-ти курс в някой от курсовете по СЕП или Теория на множествата! Иначе правилото за индукция в случая на произволна азбука Σ и произволно свойство φ на думите над Σ изглежда така

$$(\varphi(\varepsilon) \ \& \ (\forall\omega \in \Sigma^*)(\varphi(\omega) \longrightarrow (\forall u \in \Sigma)\varphi(\omega.u)) \longrightarrow (\forall\omega \in \Sigma^*)\varphi(\omega)$$