Dominik Wawszczak
numer indeksu: 440014
numer grupy: 6

Zadanie 1.1

Rozpatrzmy dowolny język regularny $L \subseteq A^*$. Udowodnimy, że język EvenLen(L) również jest regularny.

Weźmy automat deterministyczny $\mathcal{A} = (A, Q, q_0, F, \delta)$ taki, że $L(\mathcal{A}) = L$. Wskażemy automat deterministyczny $\mathcal{A}' = (\{1\}, Q', q_0', F', \delta')$, dla którego $L(\mathcal{A}') = \text{EvenLen}(L)$.

Niech:

- $Q' = 2^Q$,
- $q_0' = \{q_0\}$,
- $F' = \{X \in Q' \ : \ |X \cap F| \mod 2 = 0\}$,
- $\delta'(X, 1) = \bigoplus_{(q,a) \in X \times A} \{\delta(q, a)\}$.

Wprowadźmy następującą definicję:

$$f_n(q) \ = \ \left|\left\{w \in A^* \ : \ |w| = n \ \wedge \ \hat{\delta}(q_0, w) = q\right\}\right|.$$

Innymi słowy, $f_n(q)$ jest liczbą słów $w \in A^*$ o długości n spełniających $\hat{\delta}(q_0, w) = q$.

Lemat 1

$$f_{n+1}(r) \ = \sum_{\{(q,a) \in Q \times A \ : \ \delta(q,a) = r\}} f_n(q).$$

Warto zwrócić uwagę, że $f_n(q)$ pojawi się w tej sumie tyle razy, ile jest liter $a \in A$ spełniających $\delta(q, a) = r$.

Dowód lematu 1

Każde słowo $v \in A^*$ o długości $n + 1$ spełniające $\hat{\delta}(q_0, v) = r$ możemy przedstawić w postaci $v = wa$, gdzie $a \in A$ jest jego ostatnią literą. Wtedy $\hat{\delta}(q_0, w) = q$, dla pewnego stanu $q \in Q$ spełniającego $\delta(q, a) = r$. Dla konkretnego stanu $q \in Q$ oraz konkretnej litery $a \in A$, słów $w \in A^*$ o długości n spełniających $\hat{\delta}(q_0, w) = q$ jest dokładnie $f_n(q)$. Wynika z tego, że jest dokładnie $f_n(q)$ słów o długości $n + 1$ postaci wa takich, że $\hat{\delta}(q_0, w) = q$, dlatego należy zsumować $f_n(q)$ dla każdej pary $(q, a) \in Q \times A$ spełniającej $\delta(q, a) = r$, co kończy dowód lematu.

Wprowadźmy teraz kolejną definicję:

$$g_n(q) \ = \ f_n(q) \mod 2.$$

Innymi słowy, $g_n(q) = 0$, jeśli jest parzyście wiele słów $w \in A^*$ o długości n spełniających $\hat{\delta}(q_0, w) = q$, albo $g_n(q) = 1$, jeżeli jest nieparzyście wiele takich słów.

Lemat 2

$$g_{n+1}(r) \ = \ |\{(q, a) \in Q \times A \ : \ \delta(q, a) = r \ \wedge \ g_n(q) = 1\}| \mod 2.$$

Dowód lematu 2

Zgodnie z definicją:

$$
\begin{aligned}
g_{n+1}(r) &= f_{n+1}(r) \mod 2 = \left(\sum_{\{(q,a)\in Q\times A \;:\; \delta(q,a)=r\}} f_n(q) \right) \mod 2 = \\
&= \left(\sum_{\{(q,a)\in Q\times A \;:\; \delta(q,a)=r\}} g_n(q) \right) \mod 2 = \\
&= \left(\sum_{\{(q,a)\in Q\times A \;:\; \delta(q,a)=r \;\wedge\; g_n(q)=1\}} 1 \right) \mod 2 = \\
&= |\{(q,a) \in Q \times A \;:\; \delta(q,a) = r \;\wedge\; g_n(q) = 1\}| \mod 2,
\end{aligned}
$$

co kończy dowód lematu.

Lemat 3

$$q \in \hat{\delta}'(q_0', 1^n) \iff g_n(q) = 1.$$

Dowód lematu 3

Skorzystamy z indukcji po n.

Pierwszy krok: Dla $n = 0$ mamy

$$\hat{\delta}'\left(q_0', 1^0\right) = \hat{\delta}'(q_0', \varepsilon) = q_0' = \{q_0\}.$$

Rzeczywiście, $g_0(q_0) = 1$, ponieważ jedyne słowo w A^* o długośći 0 to ε i spełnia ono $\hat{\delta}(q_0, \varepsilon) = q_0$. Wynika z tego, że $g_0(q) = 0$, dla każdego $q \neq q_0$.

Krok indukcyjny: Zauważmy, że

$$\hat{\delta}'\left(q_0', 1^{n+1}\right) = \delta'\left(\hat{\delta}'(q_0', 1^n), 1\right) = \bigoplus_{(q,a)\in\hat{\delta}'\left(q_0',1^n\right)\times A} \{\delta(q,a)\}.$$

Wynika z tego, że następujące warunki są równoważne:

1. $r \in \hat{\delta}'\left(q_0', 1^{n+1}\right)$,
2. $r \in \bigoplus_{(q,a)\in\hat{\delta}'\left(q_0',1^n\right)\times A} \{\delta(q,a)\}$,
3. $\left|\left\{(q,a) \in \hat{\delta}'(q_0', 1^n) \times A \;:\; \delta(q,a) = r\right\}\right| \mod 2 = 1$,
4. $\left|\left\{(q,a) \in Q \times A \;:\; \delta(q,a) = r \;\wedge\; q \in \hat{\delta}'(q_0', 1^n)\right\}\right| \mod 2 = 1$,
5. $|\{(q,a) \in Q \times A \;:\; \delta(q,a) = r \;\wedge\; g_n(q) = 1\}| \mod 2 = 1$,
6. $g_{n+1}(r) = 1$,

co kończy dowód lematu.

Na podstawie powyższego wnioskujemy równoważność następujących warunków:

1. $1^n \in L(\mathcal{A}')$,
2. $\hat{\delta}'(q_0', 1^n) \in F'$,
3. $\left|\left\{q : q \in \hat{\delta}'(q_0', 1^n) \wedge q \in F\right\}\right| \mod 2 = 0$,
4. $|\{q : g_n(q) = 1 \wedge q \in F\}| \mod 2 = 0$,
5. $\left(\sum_{q \in F} g_n(q)\right) \mod 2 = 0$,
6. $\left(\sum_{q \in F} f_n(q)\right) \mod 2 = 0$,
7. $\left|\left\{w \in A^* : |w| = n \wedge \hat{\delta}(q_0, w) \in F\right\}\right| \mod 2 = 0$,
8. $|\{w \in L : |w| = n\}| \mod 2 = 0$,

co kończy rozwiązanie zadania.

$\square$

Zadanie 1.2

Rozpatrzmy język regularny $L = a^*ba^*$ nad alfabetem $\{a, b\}$. Zauważmy, że dla każdego $k \in \mathbb{Z}^+ \cup \{0\}$ zachodzi

$$\{w \in L : |w| = k\} = \left\{a^i b a^{k-1-i} : i \in [0, k-1] \cap \mathbb{Z}\right\},$$

czyli w L jest dokładnie k słów o długości k.

Z powyższego wynika, że

$$\mathrm{SquareLen}(L) = \left\{1^k : \underset{l \in \mathbb{Z}^+ \cup \{0\}}{\exists} k = l^2\right\}.$$

Udowodnimy, że język ten nie jest regularny. W tym celu skorzystamy z lematu o pompowaniu.

Niech n będzie stałą z lematu o pompowaniu. Weźmy dowolne słowo $w \in \mathrm{SquareLen}(L)$ spełniające $|w| \geqslant n$. Wtedy $w = xyz$, gdzie $|y| > 0$, przy czym dla każdego $m \in \mathbb{Z}^+$ zachodzi $xy^m z \in \mathrm{SquareLen}(L)$. Niech $x = 1^a$, $y = 1^b$ oraz $z = 1^c$. Wówczas

$$\underset{m \in \mathbb{Z}^+}{\forall} \; \underset{l \in \mathbb{Z}^+ \cup \{0\}}{\exists} a + mb + c = l^2.$$

Rozpatrzmy $m = b$. Wtedy $a + b^2 + c = l_b^2$, dla pewnego $l_b \in \mathbb{Z}^+ \cup \{0\}$, przy czym $l_b \geqslant b$, gdyż $l_b^2 = a + b^2 + c \geqslant b^2$. Z drugiej strony, biorąc $m = b + 1$ otrzymamy, że istnieje $l_{b+1} \in \mathbb{Z}^+ \cup \{0\}$ spełniające $a + b(b+1) + c = l_{b+1}^2$. Łatwo zauważyć, że $l_{b+1} \geqslant l_b + 1$, ponieważ

$$l_{b+1}^2 = a + b(b+1) + c > a + b^2 + c = l_b^2.$$

Z powyższego wynika, że

$$b = l_{b+1}^2 - l_b^2 \geqslant (l_b + 1)^2 - l_b^2 = 2l_b + 1 \geqslant 2b + 1,$$

czyli sprzeczność, co kończy rozwiązanie zadania.

$\square$