

Deklaracja						
Zad	1	2	5	6	7	9
Rozwiązane	1	1	0	1	0	0

W życiu bowiem istnieją rzeczy, o które warto walczyć do samego końca.

– Paulo Coelho

Zadanie 1

Zad 1

Rozważmy język $L = \{w0s : |s| = 9\}$, złożony z tych słów nad alfabetem $\{0, 1\}$ których dziesiąty symbol od końca to 0. Udowodnij, że DFA rozpoznający ten język ma co najmniej 1024 stany.

Dowód. Niech $M = \langle Q, \Sigma, \delta, q_0, F \rangle$ będzie DFA akceptującym podany język. Przypuśćmy, że $|Q| < 1024$.

Rozważmy zbiór słów $S = \{w : |w| = 10 \wedge w \in \{0, 1\}^*\}$. Ponieważ $|S| = 1024$ to z zasady szufladkowej Dirichleta istnieją dwa różne słowa u, v które kończą się w tym samym stanie. Przyjrzyjmy się następującym przypadkom:

- u jest w stanie akceptującym, a v w stanie nieakceptującym (analogicznie u jest w stanie nieakceptującym, a v w stanie akceptującym).

Nie może być tak, gdyż stan nie może być na raz akceptujący i nieakceptujący.

- u, v jest w stanie akceptującym (analogicznie u, v są w stanie nieakceptującym).

Ponieważ $u \neq v$ to istnieje takie i , że $u[i] \neq v[i]$. Weźmy najmniejsze takie i i nazwijmy je i_0 . Rozważmy słowa $u' = u \underbrace{000 \dots 0}_{i_0}$ oraz $v' = v \underbrace{000 \dots 0}_{i_0}$. Z faktu, że u, v były w tym samym stanie wynika, że u', v' też są w tym samym stanie. Jednak patrząc na 10-literowy sufix u', v' możemy zauważyć, że jeden zaczyna się cyfrą 0, a drugi 1. Zatem jeden z nich jest w pozycji akceptującej, a drugi w pozycji nieakceptującej. Dostajemy sprzeczność.

Zatem DFA akceptujący język z treści zadania ma co najmniej 1024 stany.

□

Zadanie 2

Zad 2

Jaką minimalną liczbę stanów musi mieć deterministyczny automat skończony rozpoznający zbiór tych wszystkich słów nad alfabetem $\{a, b, c\}$, które wśród ostatnich trzech znaków mają po jednym wystąpieniu każdej z liter alfabetu.

Rozwiązanie: Rysujemy sobie automat w którym „stanami” będą wszystkie różnowartościowe ciągi o długości ≤ 3 : $\varepsilon, a, b, c, ab, ba, ca, ac, bc, cb, abc, abc, bac, bca, cab, cba$ oraz odpowiednie przejścia np. z ba dostając a przechodzimy do tego samego, dostając b do ab , a dostając c do bac .

Twierdzę, że 16 to minimalna liczba stanów. Dlaczego?

Zakładamy nie wprost, że jest ich mniej. Wtedy istnieje jakaś para różnych słów z tego zbioru, która ma ten sam stan. Pałujemy wszystkie możliwości (robiąc to analogicznie jak w przykładzie wyżej) i pokazujemy, że taka sytuacja nie może mieć miejsca.

Zadanie 6**Zad 6**

Udowodnij, że język L tych słów, które są zapisem binarnym liczby pierwszej, nie jest regularny.

Rozwiązanie:

Lemat 1. Dla dowolnego języka regularnego L istnieje takie K , że dla dowolnych x, y, z takich, że $xyz \in L$ oraz $|y| \geq K$ istnieją u, v, w takie, że $y = uvw$ (gdzie $v \neq \varepsilon$) oraz dla każdego k $xuv^k wz \in L$.

Twierdzenie 1. Ciąg $\{an + d\}$ dla $(a, d) = 1$ zawiera nieskończenie wiele liczb pierwszych.

Niech $\text{Bin}(n)$ oznacza zapis liczby n w systemie binarnym. Załóżmy, że L jest regularny. Niech m będzie stałą z lematu o pompowaniu. Z twierdzenia Dirichleta o postępie arytmetycznym wiemy, że istnieje takie $p \in \mathbb{P}$ postaci $\text{Bin}(n) \underbrace{000 \dots 0}_m 1$ (inaczej $p = 2^{m+1}n + 1$). Podstawmy do lematu o pompowaniu $x = \text{Bin}(n)$, $y = \underbrace{000 \dots 0}_m$, $z = 1$.

Wtedy wiemy, że $y = uvw$ i możemy pompować v . Znaczy to też że dla dowolnego k liczba postaci $\text{Bin}(n)0^{m+k|v|}1$ jest pierwsza (bo z lematu o pompowaniu należy do języka).

Niech $q = n2^{m+k|v|+1} + 1 = (p-1)2^{k|v|} + 1 = 2^{k|v|}p - (2^{k|v|} - 1)$. Weźmy $k = p-1$. Wtedy z małego twierdzenia Fermata $2^k \equiv 1 \pmod{p}$. Podstawiając to do równania wyżej dostajemy, że p dzieli q co jest sprzeczne z tym, że q jest pierwsze.