Języki Formalne i Złożoność Obliczeniowa
Lista zadań nr 2

Kwiatek

28 marca 2020

Zadanie 29. Język $L \subseteq \{0,1\}^*$ jest regularny. Czy wynika z tego, że język $\sqrt{L} = \{w \in \{0,1\}^* : \exists x \in \{0,1\}^* \; \exists y \in L \; wx = y \wedge |y| = |w|^2\}$ jest regularny?

- Najpierw podzielimy zupełnie przestrzeń słów nad alfabetem $\Sigma = \{0,1\}^*$ na regularne języki P_q (tak, by wszystkie języki P sumowały się do Σ, oraz by każdy P był językiem regularnym).
- Następnie postaramy się przemianować zbiór podany w zadaniu na język, do którego potrafimy prosto skonstruować automat.
- Skonstruujemy automat rozpoznający $\sqrt{L} \cap P_q$.
- Ostatecznie wywnioskujemy, $\sqrt{L}$ jest regularny.

1 Podział przestrzeni

Weźmy automat $A = \langle Q, \Sigma, q_0, F, \delta \rangle$ rozpoznający L. Nieprawda.
Niech $P_q = \{w \in \Sigma : \delta(q_0, w) = q\}$.
Czyli, P_q jest zbiorem tych prefiksów pewnych słów w L, że po wczytaniu dowolnego z nich do automatu A dostajemy stan q.
Zauważmy, że $\bigcup_{q \in Q} P_q = \Sigma$.
Ponieważ dla dowolnego słowa wczytanego do automatu, skończy się ono w pewnym stanie q. A oczywiście P_q jest podzbiorem Σ^*.
Zauważmy też, że P_q jest regularny, ponieważ możemy stworzyć automat podobny do A, ale z jednym stanem akceptującym $F = \{q\}$.
Zdefiniujmy przy okazji język S_q, który bierze sufiksy słów z L, zaczynając od stanu q. Możemy zatem stworzyć automat podobny do A, ale stan początkowy $q_0 = q$. Regularność języka wynika z konstrukcji automatu.

Dlaczego (prawie) każde zdanie jest w osobnym akapicie?

2 Język $\sqrt{L}$

Weźmy przekrój języka $\sqrt{L}$ oraz P_q. Uzasadnimy następujący ciąg przejść:
$\sqrt{L} \cap P_q = \{w \in P_q : \exists x \in \{0,1\}^* \ \exists y \in L \ wx = y \wedge |y| = |w|^2\}$
Pierwsze przejście jest przepisaniem definicji w nowy sposób - mówimy, że szukamy y równego słowu w skonkatenowanym z elementem z Σ^*.
$\sqrt{L} \cap P_q = \{w \in P_q : \exists y \in L \ y \in w\Sigma^* \wedge |y| = |w|^2\}$
Dalej, zapewniamy, że y ma odpowiednią długość, wybierając tylko niektóre elementy z Σ^*.
$\sqrt{L} \cap P_q = \{w \in P_q : \exists y \in L \ y \in w\Sigma^{|w^2-w|}\}$
Zamiast szukać y należących do języka, szukamy słów s, które pod skonskatenowaniu z w dadzą nam słowo z L.
$\sqrt{L} \cap P_q = \{w \in P_q : \exists s \in \Sigma^* \ |s| = |w^2 - w| \wedge \delta(q, s) \in F\}$
Ostatecznie aplikujemy definicję języka sufiksów. Jako że startujemy w q wiemy, że s należy do S_q.
$\sqrt{L} \cap P_q = \{w \in P_q : \exists s \in S_q \ |s| = |w^2 - w|\}$

3 Konstrukcja automatu rozpoznającego $\sqrt{L} \cap P_q$

Mamy już automat A_q rozpoznający P_q - został opisany w części pierwszej.
Szukamy automatu, którym po wczytaniu słowa w sprawdzi, czy istnieje słowo długości $|w^2 - w|$ w języku S_q.
Łatwo możemy stworzyć automat sprawdzający, czy słowo długości $|w|$ należy do S_q. Mianowicie weźmy automat rozpoznający S_q i wszystkie krawędzie przemianujmy na cały alfabet Σ. Wtedy po wczytaniu dowolnych n liter będziemy w zbiorze stanów. Jeżeli do tego zbioru należy stan akceptujący, to istnieje słowo o długości n akceptowane przez S_q.
Oznaczmy na moment S_q jako DFA rozpoznające tenże język. Wiemy, że w S_q istnieje cykl, lub jest skończony. Ustalmy, że cykl ten ma długość p. Ale wynika z tego, że ciąg $B'_q = \{|w|^2 : w \in S_q\}$ też ma cykl. Zatem istnieje język B_q który jest przesunięciem każdego słowa języka B'_q o pierwiastek jego długości. Czyli $B_q = \{|w|^2 - |w| : w \in S_q\}$.
Aby to uzasadnić zauważmy, że:
$n^2 = (n+p)^2 \ mod \ p$
$n^2 = n^2 + 2np + p^2 \ mod \ p$
$n^2 = n^2 \ mod \ p$

Nic nie rozumiem :(

Weźmy zatem przekrój języków P_q i S_q. Przekrój języków regularnych także jest regularny.
Zatem zaakceptujemy tylko takie słowa, które są w P_q oraz mają odpowiednią długość czyli są w S_q.

4 Wniosek

Weźmy zatem sumę wszystkich języków przedstawionych powyżej:
$\bigcup_{q \in Q} \sqrt{L} \cap P_q = \sqrt{L}$
Co wynika z dowolności doboru pośredniego stanu p. A skoro jest to język, który jest sumą języków regularnych, to sam jest regularny.