6 Zadania o hipotezie Černego

Kolejne zadania mają związek z – otwartą od ponad pół wieku – hipotezą Černego. Mówi ona, że jeśli zbiór $sync(Q)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $(|Q|-1)^2$ (znany jest automat, z niepustym $sync(Q)$, dla którego najkrótsze słowo w $sync(Q)$ ma długość dokładnie $(|Q|-1)^2$).

Definicja. Dla danego deterministycznego automatu skończonego $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$ i zbioru $S \subseteq Q$, przez $sync(S)$ oznaczmy zbiór $\{w \in \Sigma^* : \forall q, q' \in S \;\; \hat{\delta}(q, w) = \hat{\delta}(q', w)\}$. Zauważ, że definicja nie zależy od wyboru stanów q_0 i F a tylko od zbioru stanów Q, od alfabetu Σ i od funkcji przejścia δ.

Zadanie 31. Język $L \subseteq \Sigma^*$ nazywany jest regularnym ideałem jeśli jest regularny i jeśli dla każdego słowa $w \in L$ i każdych słów $v, v' \in \Sigma^*$ zachodzi $vwv' \in L$.

a. Czy dla każdego automatu $\mathcal{A}$ i zbioru S zawartego w zbiorze stanów automatu $\mathcal{A}$ język $sync(S)$ jest regularny?

b. Czy dla każdego automatu $\mathcal{A}$ i zbioru S zawartego w zbiorze stanów automatu $\mathcal{A}$ język $sync(S)$ jest regularnym ideałem?

c. Czy dla każdego automatu $\mathcal{A}$ język $sync(Q)$ jest regularnym ideałem? (Q jest ponownie zbiorem stanów automatu $\mathcal{A}$).

Zadanie 32. **a.** Udowodnij, że jeśli S jest dwuelementowy i zbiór $sync(S)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $|Q|^2$.

b. Udowodnij, że jeśli zbiór $sync(Q)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $|Q|^3$. *Wskazówka: skorzystaj z* **a.**

Zadanie 33. Udowodnij, że dla każdego dostatecznie dużego n naturalnego istnieje automat $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$, gdzie $\Sigma = \{a, b\}$, $n = |Q|$, i dwuelementowy zbiór $S \subseteq Q$, takie że zbiór $sync(S)$ jest niepusty, ale nie zawiera słowa o długości mniejszej niż $n^2/4$.

W kolejnych zadaniach rozważamy Częściowe Deterministyczne Automaty Skończone (PDFA). PDFA różni się od DFA tym, że funkcja przejścia δ może być w nim funkcją częściową, to znaczy $\delta(q, a)$ może nie być określona dla niektórych par $\langle q, a \rangle$, gdzie $q \in Q$ i $a \in \Sigma$. W rezultacie, dla niektórych słów $w \in \Sigma^*$ i stanów $q \in Q$, wartość $\hat{\delta}(q, w)$ może być nieokreślona.

Dla danego PDFA $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$ i zbioru $S \subseteq Q$, przez $csync(S)$ („zbiór słów ostrożnie synchronizujących S") oznaczmy zbiór takich słów $w \in \Sigma^*$ że dla każdego $q \in S$ wartość $\hat{\delta}(q, w)$ jest określona, oraz dla każdych dwóch stanów $q, q' \in S$ zachodzi $\hat{\delta}(q, w) = \hat{\delta}(q', w)$. Zauważ, że definicja nie zależy od wyboru stanów q_0 i F a tylko od zbioru stanów Q, od alfabetu Σ i od funkcji przejścia δ.

Zadanie 34. Załóżmy, że dla każdego dwuelementowego $S \subseteq Q$ zbiór $csync(S)$ jest niepusty. Czy wynika z tego, że $csync(Q)$ jest niepusty?

Zadanie 35. Niech $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$ będzie PDFA.

a. Załóżmy że dla pewnego trzyelementowego $S \subseteq Q$ zbiór $csync(S)$ jest niepusty. Pokaż, że w takim razie istnieje $w \in csync(S)$ o długości nie większej niż $2|Q|^3$.

b. Udowodnij, że jeśli zbiór $csync(Q)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $2^{|Q|}$.

Zadanie 36. (za 3 punkty - każda wersja za punkt) Udowodnij, że dla każdego (dostatecznie dużego) n istnieje PDFA $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$, taki że $|Q| = n$ i że...

Wersja M. ...istnieje trzylelementowy $S \subseteq Q$ taki że zbiór $csync(S)$ jest niepusty ale nie zawiera słowa krótszego niż $n^3/10000$.

Wersja L. ...$csync(Q)$ jest niepusty ale nie zawiera słowa krótszego niż $p(n)$, gdzie p jest dowolnym, ustalonym wcześniej, wielomianem. Zakładamy, że $\Sigma = \{0, 1, 2\}$.

Wersja XL. ...$csync(Q)$ jest niepusty ale nie zawiera słowa krótszego niż $p(n)$, gdzie p jest dowolnym, ustalonym wcześniej, wielomianem. Zakładamy, że $\Sigma = \{0,1\}$.
Wskazówka. Rozwiązując wersję M warto może pamiętać, że między każdym naturalnym k a 2k znajdzie się liczba pierwsza. Rozwiązując wersje L i XL warto być może wiedzieć, że suma pierwszych n liczb pierwszych jest zawsze mniejsza niż $n^2 \log n$, zaś ich iloczyn zawsze jest większy od $2^{n \log n}$.

Zadanie 42. Czy język $L = \{w \in \{0,1\}^* : |w|_0 \leqslant |w|_1 \leqslant 2|w|_0\}$ jest bezkontekstowy?

Zadanie 43. Czy język $L = \{w \in \{0,1\}^* : \exists n \in \mathbb{N}\ 2n|w|_0 \leqslant |w|_1 \leqslant (2n+1)|w|_0\}$ jest bezkontekstowy?

Zadanie 44. Pokaż, że $L \subseteq \{0\}^*$ jest bezkontekstowy wtedy i tylko wtedy gdy jest regularny.

Zadanie 46. Czy język $L_3 = \{w \in \{0,1,2\}^* : \neg\exists x \in \{0,1,2\}^*\ w = xx\}$ jest bezkontekstowy?

Zadanie 42. Czy język $L = \{w \in \{0,1\}^* : |w|_0 \leqslant |w|_1 \leqslant 2|w|_0\}$ jest bezkontekstowy?

Rozważmy CFG G:

$E \to S \mid S0E1E1 \mid S1E0E1 \mid S1E1E0$

$S \to 1S0S \mid 0S1S \mid \varepsilon$

<u>Lemat</u>

$w \in L_S \iff |w|_0 = |w|_1$

($\Rightarrow$) widać z konstrukcji

($\Leftarrow$) indukcja po długości słowa (dla $n=0$ ok)

zał. że potrafimy wyprodukować słowa o dł. $\leq n-2$, pokażemy, że umiemy też n

$|w| = 2n$, $|w|_0 = |w|_1 = n$

bso $w[1] = 0$

weźmy teraz v, v' t.że $w = 0vv'$, gdzie v - najdłuższy prefiks t.że $|v|_0 = |v|_1$

zauważmy, że $|v'|_0 = |w|_0 - 1 - |v|_0$, $|v'|_1 = |w|_1 - |v|_1$, zatem $|v'|_0 = |v'|_1 - 1$

oraz skoro v jest najdłuższym takim prefiksem, to każdy prefiks v' ma więcej 1 niż 0 w szczególności $v[1]=1$

otrzymujemy podział $w = 0v1u$, gdzie $v = 1u$

$|v|, |u| < |w|$; $|v|_0 = |v|_1$, $|u|_1 = |u|_0$

Zatem są one produkowane przez gramatykę. $S \to 0S1S \to 0v1u = w$ $\square$

<u>Lemat</u>

$w \in L_G \Leftrightarrow |w|_0 \leqslant |w|_1 \leqslant 2|w|_0$

($\Rightarrow$) wynika z konstrukcji

($\Leftarrow$) indukcja po $|w|_1 - |w_0| = n$

1) dla $n = 0$ ok (Lemat 1)

2) założmy, że potrafimy wyprodukować wszystkie słowa o $|w|_1 - |w|_0 = n < |w|_0$

pokażemy, że umiemy $|w|_1 - |w|_0 = n+1 \leqslant |w|_0$

Weźmy takie w, że $|w|_1 - |w|_0 = n+1 \leqslant |w|_0$

Niech u - najdłuższy prefiks t. że $|u|_0 = |u_1|$ oraz $|w|_1 - |v|_1 \leqslant 2|w|_0 - 2|w|_1$

$w = uw_1$

Rozpatrzmy przypadki:

- $w_1 = 0w_2$

  Niech v - najdłuższy prefiks w_2 t. że $|v|_1 \leqslant 2|v|_0$

Zadanie 43. Czy język $L = \{w \in \{0,1\}^* : \exists n \in \mathbb{N}\ 2n|w|_0 \leqslant |w|_1 \leqslant (2n+1)|w|_0\}$ jest bezkontekstowy?

Załóżmy nie wprost, że jest.

Niech n - stała z LoP

Rozważmy słowo $(1^{2n+1}0)^{2n+1} = w$

Niech s, z, t, y, x będą słowami t.że $w = sztyx$, $|zty| \leqslant n$, $|zy| > 0$

Niech $k \in \{0, 1, 2, \dots\}$ - liczba pompowań; rozważmy przypadki:

1) $|zy|_0 = 0$

Rozważmy $k = 2$.

Wtedy $|sz^2ty^2x|_0 = 2n+1$

$|sz^2ty^2x|_1 = (2n+1)^2 + |zy|_1 \leqslant (2n+1)^2 + 1$

oczywiście $(2n+1)^2 + 1 \geqslant (2n+1)^2$ oraz $(2n+2)(2n+1) \geqslant (2n+1)^2 + 1$ ↯

2) $|zy|_0 = 1$, $1 < b = |zy|_1 < n$

Wtedy dla $k = 0$ mamy

$|stx|_0 = 2n$

$|stx|_1 = (2n+1)^2 - b$

$$\underset{\substack{\vee \\ 4n^2+2n = 2n(2n+1)}}{\overset{\substack{4n^2+3n+1 \\ \parallel}}{(2n+1)^2 - n}} < |stx|_1 < \overset{\substack{2n(2n+2) \\ \parallel \\ 4n^2+4n \\ \parallel}}{(2n+1)^2 - 1}$$ ↯

3) $|zy|_0 = 1$, $|zy|_1 = 1$ lub $|zy|_1 = 0$

Wtedy dla $k = 3$ otrzymujemy

$\#0 = 2n+1+2$

$\#1 = (2n+1)(2n+1)\,[+2] = 4n^2+4n+1\,[+2]$

$$\underset{(2n+3)(2n-1)}{\overset{}{4n^2+4n-3}} \leqslant \#1 \leqslant \underset{2n(2n+3)}{4n^2+6n}$$ ↯

Zadanie 44. Pokaż, że $L \subseteq \{0\}^*$ jest bezkontekstowy wtedy i tylko wtedy gdy jest regularny.

($\Leftarrow$) było

($\Rightarrow$)

Niech n - stała z LoP dla języka L.

Oznaczmy $w_{k,l}$ - najkrótsze słowo t.że

- $|w_{k,l}| \bmod l = k$
- $\forall_{m \in \mathbb{N}}\ w_{k,l} 0^{ml} \in L$

Jeżeli takiego $w_{k,l}$ nie ma, to przyjmujemy za nie $\emptyset$

Rozważmy wyrażenie regularne:

$$\varphi = \bigoplus_{w \in L : |w| \leq n} w + \bigoplus_{k,l : 0 \leq k < l \leq p} w_{k,l} (0^l)^*$$

Pokażemy, że $L_\varphi = L$.

- $L_r \subseteq L$

Oczywiste, bo wszystkie składniki należą do L

- $L \subseteq L_r$

Weźmy dowolne $|w| \in L$

Jeśli $|w| \leq n$, to $w \in L_\varphi$

W przeciwnym razie niech s, z, t, y, x będą podziałem w z LoP.

Wtedy $\forall_{k \geq 1}\ s z^k t y^k x \in L$

Korzystając z $L \subseteq \{0\}^*$ otrzymujemy $sztyx(zy)^{k-1} \in L$

Zatem istnieje l t.że $\forall_d$ mamy $w 0^{ld} \in L$

Niech $k = |w| \bmod l$

Wtedy $w_{k,l} \neq \emptyset$, bo w spełnia warunki. Zatem $w \in L_{w_{k,l}(0^l)^*}$

Jeśli $|w_{k,l}| < |w|$ to

$|w| = |w_{k,l}| + m \cdot l$

$w = w_{k,l} (0^l)^m \in L_{w_{k,l}(0^l)^*}$

Zadanie 46. Czy język $L_3 = \{w \in \{0,1,2\}^* : \neg\exists x \in \{0,1,2\}^*\ w = xx\}$ jest bezkontekstowy?

Zauważmy, że L_3 składa się z dwóch części:

$L_P = \{wv : w, v \in \Sigma^*,\ |w| = |v| \wedge w \neq v\}$

$L_N = \{w : 2 \nmid |w|\}$

Pokażemy, że dwie części są CFL.

1) L_N jest CFL, bo jest regularne:

$$\varphi = (0+1+2)\left[(0+1+2)(0+1+2)\right]^*$$

$L_\varphi = L_N$.

2) L_P jest CFL. Skonstruujemy CFG G t.że $L_G = L$.

Zauważmy, że jeśli $w \in L_P$, $|w| = 2n$, to istnieje indeks $i \in \{0, \dots, n\}$ t.że $w[i] \neq w[n+i]$.

Korzystając z tego stworzymy gramatykę G:

$S \to AB \mid BA \mid AC \mid CA \mid BC \mid CB$

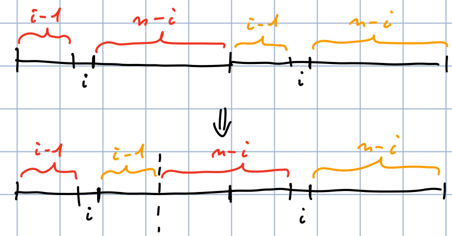
$A \to xAy \mid 0 \qquad x, y \in \Sigma$

$B \to xBy \mid 1 \qquad x, y \in \Sigma$

$C \to xCy \mid 2 \qquad x, y \in \Sigma$

$L_P \subseteq L_G$

$w \in L_P$, $|w| = 2n$



Niech i - indeks t.że $w[i] \neq w[n+i]$

BSO przyjmijmy $w[i] = 0$, $w[n+i] = 1$

Skonstruujemy w:

$S \to AB \to w[1]\,A\,w[2i-1]\,B \to \dots \to w[1:i-1]\,A\,w[i+1:2i-1]\,B \to w[1:i-1]\,0\,w[i+1:2i-1]\,B$

$\to w[1:2i-1]\,w[2i]\,B\,w[2n] \to \dots \to w[1:2i-1]\,w[2i:n+i-1]\,B\,w[n+i+1:2n] \to \underbrace{w[1:n+i-1]\,1\,w[n+i+1:2n]}_{= w}$

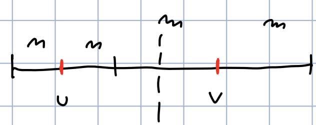
$L_G \subseteq L_P$

BSO przyjmijmy $w \in L_G$ powstało z $S \to AB$.

Niech $w = uv$ t.że $A \xrightarrow{*} u$, $B \xrightarrow{*} v$

Wtedy $|u|, |v|$ są nieparzyste, czyli $2 \mid |w|$

Przyjmijmy $|u| = 2n+1$, $|v| = 2m+1$



Z konstrukcji wiemy, że $u[n+1] \neq v[m+1]$
(środkowe litery są różne)

Zauważmy, że w oryginalnym słowie mamy

$$w[n+1] = u[n+1] \neq v[m+1] = w[2n+1+m+1] = w\left[\frac{|w|}{2} + n + 1\right]$$

Czyli pierwsza połowa w różni się od drugiej, zatem $w \in L_P$.

Skoro $L_3 = L_P \cup L_N$, i oba są CFL, to L_3 też jest CFL □

Zadanie 31. Język $L \subseteq \Sigma^*$ nazywany jest regularnym ideałem jeśli jest regularny i jeśli dla każdego słowa $w \in L$ i każdych słów $v, v' \in \Sigma^*$ zachodzi $vwv' \in L$.

a. Czy dla każdego automatu $\mathcal{A}$ i zbioru S zawartego w zbiorze stanów automatu $\mathcal{A}$ język $sync(S)$ jest regularny?

b. Czy dla każdego automatu $\mathcal{A}$ i zbioru S zawartego w zbiorze stanów automatu $\mathcal{A}$ język $sync(S)$ jest regularnym ideałem?

c. Czy dla każdego automatu $\mathcal{A}$ język $sync(Q)$ jest regularnym ideałem? (Q jest ponownie zbiorem stanów automatu $\mathcal{A}$).

a) Tak. Skonstruujemy automat $\mathcal{A}'$ rozpoznający $sync(S)$.

Niech $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$

$\mathcal{A}' = \langle \Sigma, Q', q_0', \delta', F' \rangle$

$S = \{ s_0, s_1, \dots, s_{n-1} \}$

Niech $Q' = Q^{|S|}$, $q_0' = \langle s_0, \dots, s_{n-1} \rangle$

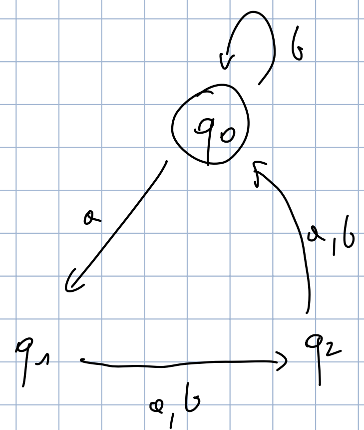
$F' = \{ \langle q, q, \dots, q \rangle : q \in Q \}$

$\delta'(\langle q_1, q_2, \dots, q_n \rangle, a) = \langle \delta(q_1, a), \delta(q_2, a), \dots, \delta(q_n, a) \rangle$

Pokażemy, że $L_{\mathcal{A}'} = sync(S)$

$w \in L_{\mathcal{A}'} \Leftrightarrow \hat{\delta}'(q_0', w) \in F \Leftrightarrow \hat{\delta}(s_0, w) = \hat{\delta}(s_1, w) = \dots = \hat{\delta}(s_{n-1}, w) \Leftrightarrow w \in sync(S)$ □

b) Nie. Rozważmy następujący automat $\mathcal{A}$:



Niech $S = \{q_0, q_2\}$

Wtedy do $sync(S)$ należy słowo b.

Przyjmijmy $u = a$, $v = \varepsilon$

Wtedy $\hat{\delta}(q_0, ab) = q_2 \neq q_0 = \hat{\delta}(q_2, ab)$

Czyli $sync(S)$ nie jest regularnym ideałem.

c) Tak.

z a) wiemy, że $sync(Q)$ jest regularny.

Pokażemy, że $sync(Q)$ jest regularnym ideałem.

Weźmy dowolne $w \in sync(Q)$ oraz dowolne $u, v \in \Sigma^*$.

Niech $p, q \in Q$

Wtedy $\hat{\delta}(p, uwv) = \hat{\delta}(\hat{\delta}(\hat{\delta}(p,u), w), v) \overset{w \in sync(Q)}{=} \hat{\delta}(\hat{\delta}(\hat{\delta}(q,u), w), v) = \hat{\delta}(q, uwv)$

Czyli $\forall_{p,q \in Q}\ \hat{\delta}(p, uwv) = \hat{\delta}(q, uwv) \Rightarrow uwv \in sync(Q)$

Zadanie 32. **a.** Udowodnij, że jeśli S jest dwuelementowy i zbiór $sync(S)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $|Q|^2$.

b. Udowodnij, że jeśli zbiór $sync(Q)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $|Q|^3$. *Wskazówka: skorzystaj z* **a.**

Lemat 1

$\forall_{w,x,y \in \Sigma^k} \forall_{q \in S}\ \hat{\delta}(q,w) = \hat{\delta}(q,wy) \Rightarrow \hat{\delta}(q,wx) = \hat{\delta}(q,wyx)$

D-d

Ustalmy $q \in S$

Wtedy $\hat{\delta}(q,wx) = \hat{\delta}(\hat{\delta}(q,w),x) = \hat{\delta}(\hat{\delta}(q,wy),x) = \hat{\delta}(q,wyx)$

Lemat 2

Niech $w \in S$, w - najkrótsze.

Wtedy $\forall_{1 \le i < j \le |w|} \exists_{q \in S}\ \hat{\delta}(q, w[1:i]) \neq \hat{\delta}(q, w[1:j])$

D-d:

Załóżmy n.c. że $i<j$ t.że $\forall_{q \in S}\ \hat{\delta}(q, w[1:i]) = \hat{\delta}(q, w[1:j])$

Wtedy z L1 wynika, że

$$\hat{\delta}(q, w[1:i]) = \hat{\delta}(q, w[1:i]\,w[i+1:j])$$
$$\Downarrow$$
$$\hat{\delta}(q, w[1:i]\,w[j+1:|w|]) = \hat{\delta}(q,w)$$

Zatem $w[1:i]\,w[j+1:|]$ synchronizuje automat $\lightning$

a) Wiemy, że $|S| = 2$.

Zatem wystarczy policzyć ile różnych stanów przyjmują $v_i = w[1:i]$ dla $i \le |w|$

Razem mamy ich $\le |Q|^2 - |Q| < |Q|^2$

Czyli $|w| < |Q|^2$

Lemat 3

$$\forall_{w\in\Sigma^*} \exists_{i,j,k} \left(\hat{\delta}(q_i, w[1:k]) = \hat{\delta}(q_j, w[1:k])\right) \Rightarrow \forall_{l>k} \ \hat{\delta}(q_i, w[1:l]) = \hat{\delta}(q_j, w[1:l])$$

Wniosek: $\forall_{w,v\in\Sigma^*} \ \hat{\delta}(q_i, w) = \hat{\delta}(q_j, w) \Rightarrow \hat{\delta}(q_i, wv) = \hat{\delta}(q_j, wv)$

Lemat 4

Dla $Q = \{q_0, q_1, \dots, q_{n-1}\}$ dla każdego $k \leq n$ istnieje $w \in \Sigma^*$, $|w| \leq k|Q|^2$, $w \in sync(\{q_0, \dots, q_{k-1}\})$

Indukcja po k:

1) dla $k=2$ punkt a)

2) zał. że dla $n<k$ zachodzi, pokażemy k.

Niech v - najkrótsze słowo z $sync(\{q_0, \dots, q_{k-2}\})$

Wtedy $|v| \leq (k-1)|Q|^2$.

Oraz $\forall_{0\leq i<j\leq k-2} \ \hat{\delta}(q_i, v) = \hat{\delta}(q_j, v) = q$

Oznaczmy $p = \hat{\delta}(q_{k-1}, v)$

Niech w - najkrótsze słowo z $sync(\{p, q\})$; $|w| \leq |Q|^2$

Wtedy $|vw| \leq (k-1)|Q|^2 + |Q|^2 = k|Q|^2$

Oraz z lematu 3 $vw \in sync(\{q_0, \dots, q_{k-2}\})$

Widzimy, że $\hat{\delta}(q_{k-1}, vw) = \hat{\delta}(p, w) = \hat{\delta}(q, w) = \hat{\delta}(q_i, vw)$ dla $i \leq k-2$

Czyli $vw \in sync(\{q_0, \dots, q_{k-1}\})$ $\square$

Stąd dla $k = |Q|$ otrzymujemy b)

Zadanie 33. Udowodnij, że dla każdego dostatecznie dużego n naturalnego istnieje automat $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$, gdzie $\Sigma = \{a, b\}$, $n = |Q|$, i dwuelementowy zbiór $S \subseteq Q$, takie że zbiór $sync(S)$ jest niepusty, ale nie zawiera słowa o długości mniejszej niż $n^2/4$.

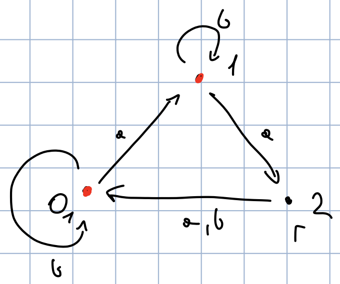
Niech $Q = \{q_0, q_1, \dots, q_{n-1}\}$

$$\delta(q_i, a) = q_{(i+1) \bmod n}$$

$$\delta(q_0, b) = q_1$$

$$\delta(q_i, b) = q_i \text{ dla } i = 1, 2, \dots, n-1$$

Rozważmy $S = \{q_0, q_{\lfloor \frac{n}{2} \rfloor}\}$



Obserwacja:

Tylko raz w całym cyklu możemy zmniejszyć odległość między $\hat{\delta}(q_0, w)$ i $\hat{\delta}(q_{\lfloor \frac{n}{2} \rfloor}, w)$

Cykl ma długość n, zatem będziemy potrzebować słowa o przynajmniej $n(\lfloor \frac{n}{2} \rfloor - 1)$ literach.

Pytamy się dla jakich n zachodzi $n(\lfloor \frac{n}{2} \rfloor - 1) \geqslant \frac{n^2}{4}$

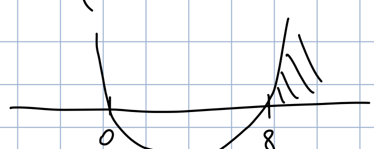
Szacujemy $\lfloor \frac{n}{2} \rfloor - 1 \geqslant \frac{n}{2} - 2$

Zatem $n(\lfloor \frac{n}{2} \rfloor - 1) \geqslant n(\frac{n}{2} - 2) \geqslant \frac{n^2}{4}$

$$\frac{n^2}{2} - 2n \geqslant \frac{n^2}{4}$$

$$\frac{n^2}{4} - 2n \geqslant 0$$

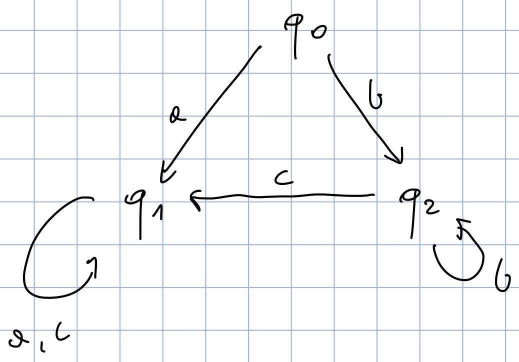
$$n\left(\frac{n}{4} - 2\right) \geqslant 0$$



Zatem $n \geqslant 8$ □

Zadanie 34. Załóżmy, że dla każdego dwuelementowego $S \subseteq Q$ zbiór $csync(S)$ jest niepusty. Czy wynika z tego, że $csync(Q)$ jest niepusty?

Nie. Rozważmy automat



Wtedy $a \in csync(\{q_0, q_1\})$

$b \in csync(\{q_0, q_2\})$

$c \in csync(\{q_1, q_2\})$

Ale $\delta(q_0, c)$, $\delta(q_2, a)$ i $\delta(q_1, b)$ nie są określone, więc słowo z $csync(\{q_1, q_2, q_3\})$ musi być puste.

Zadanie 35. Niech $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$ będzie PDFA.

a. Załóżmy że dla pewnego trzyelementowego $S \subseteq Q$ zbiór $csync(S)$ jest niepusty. Pokaż, że w takim razie istnieje $w \in csync(S)$ o długości nie większej niż $2|Q|^3$.

b. Udowodnij, że jeśli zbiór $csync(Q)$ jest niepusty, to zawiera on jakieś słowo o długości nie większej niż $2^{|Q|}$.

a) Niech $w \in csync(S)$. $S = \{s_1, s_2, s_3\}$

Zał. nie wprost, że $|w| > 2|Q|^3$

oznaczmy $k = |w|$.

Rozważmy ciąg $(\langle s_1, s_2, s_3 \rangle, \langle \delta(s_1, w[1]), \delta(s_2, w[1]), \delta(s_3, w[1]) \rangle,$

$\langle \hat{\delta}(s_1, w[1{:}2]), \hat{\delta}(s_2, w[1{:}2]), \hat{\delta}(s_3, w[1{:}2]) \rangle,$

$\dots$

$\langle \hat{\delta}(s_1, w), \hat{\delta}(s_2, w), \hat{\delta}(s_3, w) \rangle)$

Mamy $k+1$ krotek. Łącznie wszystkich możliwych jest $|Q|^3$.

Zatem przynajmniej jedna krotka musiała się powtórzyć.

Przyjmijmy, że $\hat{\delta}(s_1, w[1:i]) = \hat{\delta}(s_1, w[1:j]), \dots \quad i<j$

Wtedy $\hat{\delta}(s_1, w) = \hat{\delta}(s_1, w[1:j]\, w[j+1:k]) = \hat{\delta}(s_1, w[1:i]\, w[j+1:k])$

czyli $w[1:i]\, w[j+1:k]$ synchronizuje automat,

co jest sprzeczne z minimalnością w. ↯

b) Niech $w \in csync(S)$, $|w|$ - minimalne

Załóżmy nie wprost, że $|w| > 2^{|Q|}$

Niech $Q = \{q_0, \dots, q_{n-1}\}$

Tworzymy tablicę stanów osiągalnych:

Niech $T_{0,i} = 1$ dla wszystkich $i = 0, \dots, n-1$

$T_{j,i} = 1 \iff$ istnieje stan q t. że $\hat{\delta}(q, w[1:j]) = q_i$, $j = 1, \dots, k$

Mamy $k+1$ wierszy w tabeli,

wszystkich możliwych wierszy jest $2^{|Q|} < k+1$

Zatem któryś wiersz musiał się powtórzyć

Przyjmijmy $i < i'$; $\forall_j\ T_{j,i} = T_{j,i'}$

Wiemy, że automat się zsynchronizował po wczytaniu w,

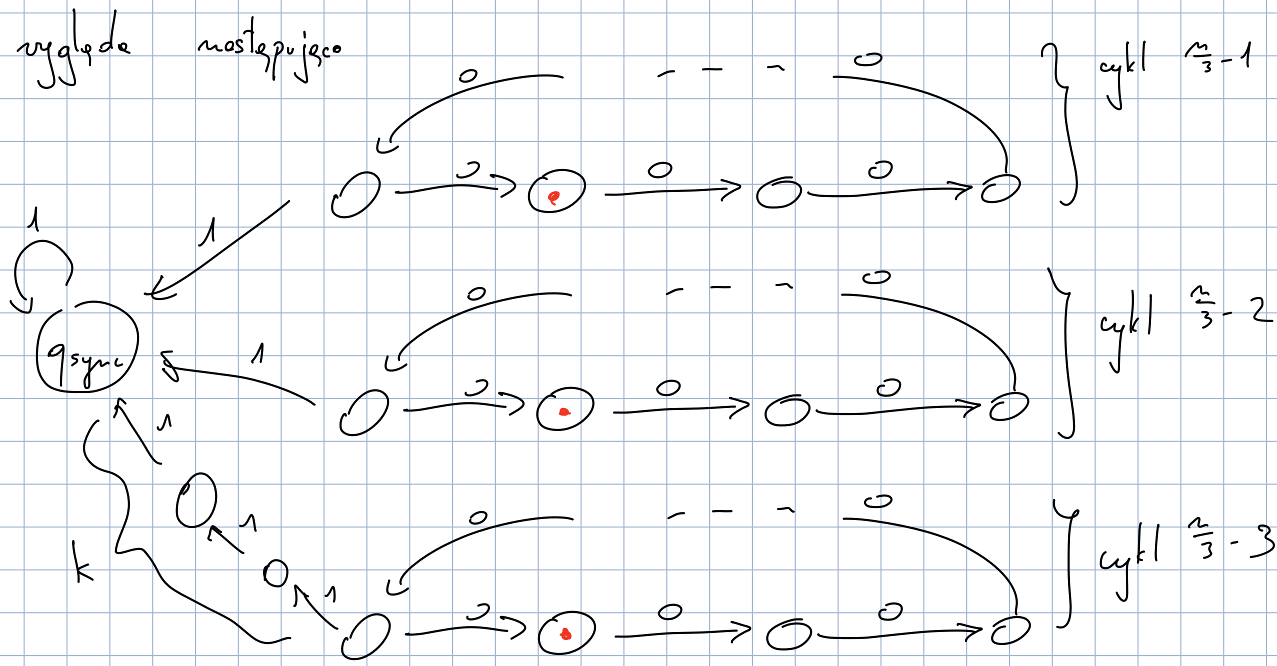
zatem zsynchronizuje się również po wczytaniu $w[1:i]\, w[i'+1:k]$

Ale to słowo jest krótsze ↯.

Zadanie 36. (za 3 punkty - każda wersja za punkt) Udowodnij, że dla każdego (dostatecznie dużego) n istnieje PDFA $\mathcal{A} = \langle \Sigma, Q, q_0, F, \delta \rangle$, taki że $|Q| = n$ i że...

Wersja M. ...istnieje trzylelementowy $S \subseteq Q$ taki że zbiór $csync(S)$ jest niepusty ale nie zawiera słowa krótszego niż $n^3/10000$.

Automat wygląda następująco



Zaczynamy w czerwonych stanach

Wtedy najmniejszym słowem synchronizującym jest $0^{NWW(\frac{n}{3}-1,\frac{n}{3}-2,\frac{n}{3}-3)-1}1^k$

Niech c_1, c_2, c_3 będą równe odp. $\frac{n}{3}-1$, $\frac{n}{3}-2$, $\frac{n}{3}-3$

Wtedy

$$NWW(c_1, c_2, c_3) = NWW\left(c_1, \frac{c_2 c_3}{NWD(c_2, c_3)}\right)$$

$$= NWW(c_1, c_2 c_3) \qquad NWD(c_2 c_3) = 1$$

$$= \frac{c_1 c_2 c_3}{NWD(c_1, c_2 c_3)}$$

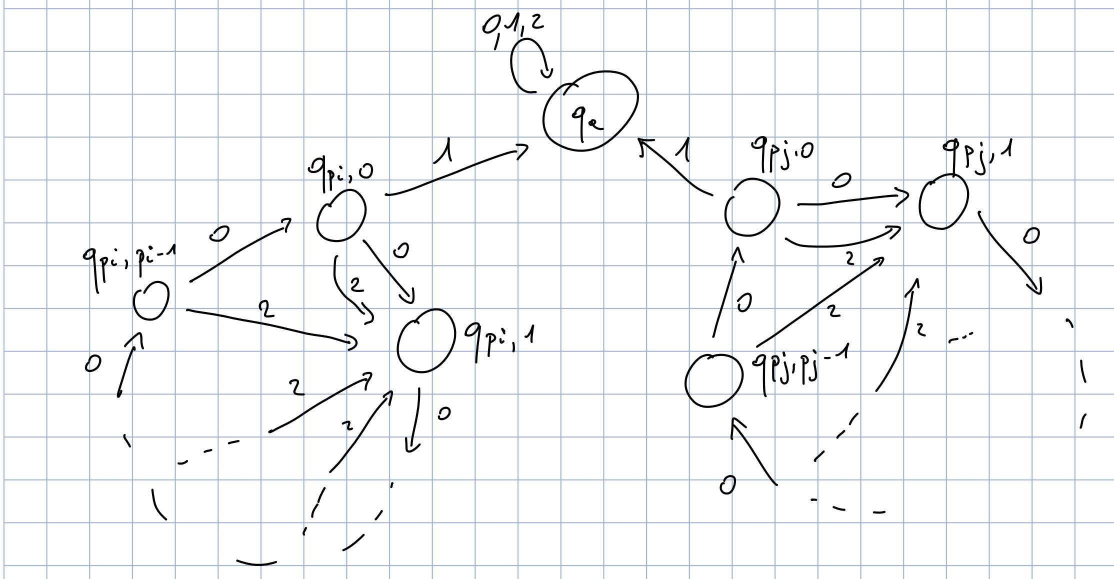
Wstawiając wartości otrzymujemy

$$= \frac{n^3 - 9n^2 + 18n}{27 \cdot NWD(c_1, c_2 c_3)} \geqslant \frac{n^3}{27 \cdot 2} > \frac{n^3}{1000}$$

dla dużych n

Wersja L. ...$csync(Q)$ jest niepusty ale nie zawiera słowa krótszego niż $p(n)$, gdzie p jest dowolnym, ustalonym wcześniej, wielomianem. Zakładamy, że $\Sigma = \{0, 1, 2\}$.

Niech $\mathbb{P}_k$ – k pierwszych l. pierwszych.



Obs: 1 nie może wystąpić przed 2, samymi 0 nie zsynchronizujemy cykli

Zatem słowo będzie postaci $0^{l} 2 0^{l'} 1$

Ale krótsze będzie $2 0^{l'} 1$, bo po 2 cykle się synchronizują

Wtedy $l' = NWW(\mathbb{P}_k) - 1$

Wtedy mamy $l' = \prod_{i=1}^{k} p_i - 1$

Czyli $|w| = \prod_{i=1}^{k} p_i + 1$

Więc $|w| \geq 2^{k \log k}$

Liczba stanów to $\sum_{i=1}^{k} p_i + 1 \leq k^2 \log k + 1$

Szukamy k t.że

$$k^2 \log k + 1 \leq n \quad i \quad 2^{k \log k} \geq n^m \geq p(n)$$

$$2^{k \log k} - k^2 \log k - 1 \geq n^m - n$$

dla odpowiednio dużych k to będzie zachodzić.

Zatem znajdziemy N t.że $n \geq N$ istnieje k dla których to zachodzi

Zadanie 42. Czy język $L = \{w \in \{0,1\}^* : |w|_0 \leqslant |w|_1 \leqslant 2|w|_0\}$ jest bezkontekstowy?

Automat ze stosem