

SLOVA S VÍCE PERIODAMI

Podle definice má každé slovo w nekonečně mnoho period: každé přirozené číslo $p \geq |w|$ je jeho periodou. Dalším triviálním případem jsou násobky nejkratší periody: je-li nejkratší perioda p , je periodou i každé kp , bez ohledu na délku slova.

Slovo ale může mít více period i netriviálním způsobem. Např. slovo *abaababaaba* má periody 5 a 8, aniž by mělo periodu $\text{NSD}(5, 8) = 1$. Kdy k takové situaci může dojít, určuje následující věta pocházející od Finea a Wilfa, nazývaná také *Periodické lemma*.

Věta. Má-li slovo délky alespoň $p + q - \text{NSD}(p, q)$ periody p a q , má také periodu $\text{NSD}(p, q)$.

Důkaz. Necht' je $q < p$ a necht' má slovo $w = a_0 a_1 \cdots a_{p+q-\text{NSD}(p,q)-1}$ periody p a q .

Předpokládejme nejprve, že p a q jsou nesoudělná. Na indexech, tedy na přirozených číslech $0, 1, 2, \dots, p + q - 2$, definujeme nejmenší ekvivalenci splňující $i \approx j$, pokud $i \equiv j \pmod p$ nebo $i \equiv j \pmod q$. Zřejmě platí, že pokud $i \approx j$, pak také $a_i = a_j$. Chceme tedy ukázat, že jsou všechna čísla \approx -ekvivalentní. Zjevně to stačí ukázat pro čísla $0, 1, \dots, q - 1$.

Označme $i_k \equiv (k + 1)p - 1 \pmod q$. Protože jsou čísla p a q nesoudělná, je $\{i_0, i_1, \dots, i_{q-1}\} = \{0, 1, \dots, q - 1\}$, přičemž $i_{q-1} \equiv -1 \equiv q - 1 \pmod q$. Pro $k = 0, 1, \dots, q - 2$ tedy platí $i_k < q - 1$, tedy $i_k + p < p + q - 1$, a tedy

$$i_k \approx i_k + p \approx (i_k + p \pmod q) = i_{k+1}.$$

Necht' je nyní $\text{NSD}(p, q) = d$. Pro $r \in \{0, 1, \dots, d - 1\}$ definujme slovo $w_r = a_r a_{r+d} a_{r+2d} \cdots a_{r+(p'+q'-2)d}$, kde $p' = p/d$ a $q' = q/d$. Je snadné si uvědomit, že w_r má periody p a q , právě když w_r má periody p' a q' pro všechna $r = 0, 1, \dots, d - 1$. Protože slova w_r mají délku $p' + q' - 1$, jsou podle první části důkazu mocninou téhož písmene. Slovo w má proto periodu d . \square

Nyní ukážeme, že mez v předchozí větě je optimální.

Věta. Pokud $p \nmid q$, pak existuje slovo délky $p + q - \text{NSD}(p, q) - 1$, které má periody p i q , ale nemá periodu $\text{NSD}(p, q)$.

Důkaz. Uvažujme slovo $w = a_0 a_1 \cdots a_{p+q-\text{NSD}(p,q)-2}$ a opět nejprve předpokládejme, že $q < p$ a slova p a q jsou nesoudělná. Pokud má ekvivalence \approx alespoň dvě třídy, můžeme identifikovat každé a_i s třídou, ve které leží i , a dostaneme slovo s požadovanými vlastnostmi.

Uvažujme opět pouze čísla $\{0, 1, \dots, q - 1\}$ a chápejme je jako vrcholy orientovaného grafu G , ve kterém $i \rightarrow j$, právě když $i + p < p + q - 2$ a $i + p \equiv j \pmod q$. Je snadné si rozmyslet, že třídy \approx omezené na množinu $\{0, 1, \dots, q - 1\}$ jsou právě (slabě souvislé) komponenty grafu G . Každý vrchol má zjevně vstupní i výstupní stupeň nejvýše jedna. Přitom vrcholy $q - 1$ a $q - 2$ mají výstupní stupeň nula. Podobně mají vrcholy $p - 1 \pmod q$ a $p - 2 \pmod q$ vstupní stupeň nula. Z toho plyne, že G má více než jednu komponentu a slovo w je netriviální.

Necht' je nyní $\text{NSD}(p, q) = d$. Slovo w_{d-1} definované podobně jako v důkazu předchozí věty má délku $p' + q' - 2$, protože $(d - 1) + (p' - q' - 2)d = p + q - d - 1$. Podle první části důkazu tedy může obsahovat alespoň dvě písmena a w tedy nemá periodu d . \square

Předchozí úvahy lze zobecnit pro libovolný počet period. Pro množinu $P \subset \mathbb{N}$ označme \mathcal{L}_P délku nejdelšího slova, které má periodu p pro každé $p \in P$ a nemá periodu $\text{NSD}(P)$. Pro $1 \in P$ definujeme $\mathcal{L}_P := 0$. Výše jsme ukázali, že $\mathcal{L}_{\{p,q\}} = p + q - \text{NSD}(p, q) - 1$. Pro jednoduchost se dále omezíme na nesoudělné množiny period, obecný případ se získá obdobně jako výše.

Věta. Bud' P množina přirozených čísel, jejichž největší společný dělitel je jedna. Necht' $1 < m = \min P$ a definujeme množinu

$$Q = \{p - m \mid p \in P\} \cup \{m\}.$$

Pak

$$\mathcal{L}_P = m + \max\{m - 1, \mathcal{L}_Q\}.$$

Důkaz. Definujeme $\approx_{P,k}$ nejmenší ekvivalenci na číslech $0, 1, \dots, k - 1$ takovou, že $i \approx_{P,k} j$, pokud $i \equiv j \pmod p$ pro nějaké $p \in P$. Ukážeme, že pro libovolná k a libovolné $i, j \in \{0, \dots, k - 1\}$ platí

$$(*) \quad i \approx_{Q,k} j, \quad \text{právě když} \quad i \approx_{P,k+m} j.$$

Necht' $i \equiv j \pmod q$ pro $0 \leq i < j \leq k - 1$ a nějaké $q \in Q$. Pokud $q = m$, je jistě $i \approx_{P,k+m} j$. Pokud $q \neq m$, je $i \equiv j + m \pmod{q+m}$ a $j \equiv j + m \pmod{q+m}$. Protože $i, j, j + m \in \{0, 1, \dots, m + k - 1\}$ a $m, q + m \in P$, je opět $i \approx_{P,k+m} j$. Tím je dokázána přímá implikace.

Necht' naopak $i \approx_{P,k+m} j$ pro $0 \leq i < j \leq k - 1$. Pak existuje posloupnost $i = i_0, i_1, \dots, i_{s-1}, i_s = j$ čísel z $\{0, 1, \dots, k + m - 1\}$ taková, že pro každé $t = 0, 1, \dots, s - 1$ platí pro nějaké $p \in P$ vztah $i_t \equiv i_{t+1} \pmod p$. Uvažujme posloupnost $i = i'_0, i'_1, \dots, i'_{s-1}, i'_s = j$ definovanou

$$i'_t = \begin{cases} i_t, & \text{pokud } i_t \in \{0, \dots, k - 1\}, \\ i_t - m, & \text{pokud } i_t \in \{k, \dots, k + m - 1\}. \end{cases}$$

Celá tato posloupnost leží v intervalu $\{0, \dots, k - 1\}$ a pro každé $t = 0, 1, \dots, s - 1$ zřejmě platí buď $i'_t \equiv i'_{t+1} \pmod p$ pro nějaké $p \in P$, nebo $i'_t \equiv i'_{t+1} \pmod q$ pro nějaké $q \in Q$. Protože $p = q' + m$ pro nějaké $q' \in Q$ a současně $m \in Q$, dovoluje uvedená posloupnost uzavřít, že $i \approx_{Q,k} j$. Tím je dokončen důkaz tvrzení (*).

Obraťme se nyní k důkazu věty. Ekvivalence $\approx_{Q, \mathcal{L}_Q}$ je netriviální (tj. obsahuje alespoň dvě třídy), a podle (*) je tedy také ekvivalence $\approx_{P, m + \mathcal{L}_Q}$ netriviální. Současně platí, že ekvivalence $\approx_{P, 2m-1}$ je netriviální, protože prvek $m - 1$ je v relaci pouze sám se sebou. Odtud $\mathcal{L}_P \geq 2m - 1$ a $\mathcal{L}_P \geq m + \mathcal{L}_Q$.

Podle (*) dále platí, že pro $k \geq \mathcal{L}_Q + 1$ jsou v $\approx_{P, m+k}$ ekvivalentní všechny prvky $0, 1, \dots, k - 1$. Je-li $\mathcal{L}_Q \geq m - 1$, je tedy $\approx_{P, m + \mathcal{L}_Q + 1}$ triviální, protože m leží v P . Pak tedy $\mathcal{L}_P = m + \mathcal{L}_Q$. Je-li $\mathcal{L}_Q < m - 1$, pak je $\approx_{P, 2m}$ triviální a $\mathcal{L}_P = 2m - 1$. \square

Předcházející věta dává rekurzivní předpis na výpočet \mathcal{L}_P (terminující podmínka je $\min Q = 1$). Její důkaz současně dává návod na konstrukci slova $\text{FW}(P, n)$, které definujeme jako slovo délky n s největší možnou abecedou a periodami P . Pokud $n \leq \min P$, platí

$$\text{FW}(P, n) = 0 \cdot 1 \cdots (n - 1).$$

Jinak je $\text{FW}(P, n)$ dáno svým prefixem w délky $m = \min P$, který lze získat rekurzivně ze slova $u = \text{FW}(Q, n - m)$ takto:

$$w = \begin{cases} \text{pref}_m(u), & \text{pokud } m \leq n - m, \\ u \cdot |u| \cdot (|u| + 1) \cdots (m - 1) & \text{jinak.} \end{cases}$$

*

Důkaz periodického lemmatu indukcí. Pokud q dělí p , pak tvrzení zjevně platí. Necht' $q < p$, $d = \text{NSD}(p, q)$, necht' $w = a_0 a_1 \cdots a_{p+q-d-1}$ má periody p a q , a necht' $w' = a_0 a_1 \cdots a_{p-d-1}$ je prefix w délky $p - d$. Slovo w' má zjevně periodu q . Necht' $i + (p - q) \leq p - d - 1$. Pak $i + p \leq p + q - d - 1$, a proto $a_i = a_{i+p} = a_{i+p-q}$. Tím jsme ukázali, že slovo w' má periodu $p - q$. Protože $d = \text{NSD}(p - q, q)$ a w' má délku $q + (p - q) - d$, dostáváme z indukčního předpokladu, že w' má periodu d . Protože w má periodu q a prefix w' délky nejméně q , který má periodu d dělící q , má i w periodu d .

Optimalitu dokážeme indukcí podle $(p - q)/d$. Necht' je nejprve $q = kd$ a $p = (k + 1)d$, kde $k > 1$. Pak $(a^{d-1}b)^{k-1}a^{d-1}c(a^{d-1}b)^{k-1}a^{d-1}$ je slovo délky $p + q - d - 1$, které má periody p a q a nemá periodu d .

Necht' nyní $p - q > d$. Podle indukčního předpokladu existuje slovo w' délky $q + (p - q) - d - 1$, které má periody q a $p - q$ a nemá periodu d . Zvolme slovo w jako prefix délky $p + q - d - 1$ slova z^ω , kde z je prefix w' délky q (w je prodloužením slova w' s periodou q). Protože w nemá periodu d (jinak by ji mělo i w'), zbývá ukázat, že w má periodu p . Necht' tedy $w = a_0 a_1 \cdots a_{p+q-d-2}$ a necht' $i + p \leq p + q - d - 2$. Pak $a_i = a_{i+p-q} = a_{i+p}$, kde druhá rovnost plyne z q -periodicity w a první z $(p - q)$ -periodicity slova w' díky $i + p - q \leq q + (p - q) - d - 2$.

*

Důkaz periodického lemmatu pomocí Fourierovy transformace. Zvolíme-li jako abecedu nějakou množinu komplexních čísel (např. nějaká přirozená čísla), můžeme slovo w s periodou p chápat jako zobrazení $\mathbb{Z} \rightarrow \mathbb{C}$, pro které platí $w(j) = w(j \bmod p)$. Taková zobrazení tvoří p -dimenzionální vektorový prostor nad \mathbb{C} , který má také bázi

$$\Phi_p = \{\varphi_{p,k} \mid k = 0, 1, \dots, p - 1\},$$

kde

$$\varphi_{p,k}(j) = \omega_{p,k}^j = e^{2\pi i \frac{kj}{p}}.$$

Platí tedy $w = \sum_{k=0}^{p-1} c_k \varphi_{p,k}$ pro jednoznačně určené koeficienty c_k . Uvažme nyní slovo $w' = \sum_{\ell=0}^{q-1} d_\ell \varphi_{q,\ell}$ s periodou q . Všimněme si, že množina

$$\Phi_p \cup \Phi_q$$

obsahuje přesně $p + q - \text{NSD}(p, q)$ různých (lineárně nezávislých) funkcí. Hodnoty $w(j) = w'(j)$, $j = 1, 2, \dots, p + q - \text{NSD}(p, q)$ tedy jednoznačně určují koeficienty c_k a d_ℓ , přičemž nenulové mohou být pouze koeficienty u funkcí z průniku $\Phi_p \cap \Phi_q = \Phi_{\text{NSD}(p,q)}$.

Současně vidíme, že hodnoty v bodech $j = 1, 2, \dots, p + q - \text{NSD}(p, q) - 1$ umožňují v bodě $p + q - \text{NSD}(p, q)$ libovolnou hodnotu.

*

Důkaz periodického lemmatu pomocí formálních řad. Zvolme jako abecedu podmnožinu racionálních čísel a reprezentujme nekonečné slovo $w = a_0a_1\dots$ formální řadou $\bar{w} = \sum_{i=1}^{\infty} a_i x^i$. Má-li w periodu p , pak

$$\bar{w} = \frac{P}{1 - x^p},$$

kde $P = a_0 + a_1x + \dots + a_{p-1}x^{p-1}$. Uvažujme dvě slova w_1 a w_2 s periodami p a q . Všimněme se (například srovnáním komplexních kořenů), že největší společný dělitel polynomů $1 - x^p$ a $1 - x^q$ je $1 - x^d$, kde $d = \text{NSD}(p, q)$. Platí tedy

$$\bar{w}_1 - \bar{w}_2 = \frac{P_1}{1 - x^p} - \frac{P_2}{1 - x^q} = \frac{(1 - x^d)}{(1 - x^p)(1 - x^q)} \left(P_1 \frac{(1 - x^q)}{(1 - x^d)} - P_2 \frac{(1 - x^p)}{(1 - x^d)} \right),$$

což je součin formální řady s nenulovým absolutním členem a polynomu R stupně nejvýše $p + q - d - 1$. Pokud se w_1 a w_2 shodují na prvních $p + q - d$ místech, je $\bar{w}_1 - \bar{w}_2$ dělitelné x^{p+q-d} , což je možné pouze pokud je polynom R nulový. Pak je P_1 dělitelné

$$\frac{1 - x^p}{1 - x^d} = 1 + x^d + x^{2d} + x^{3d} + \dots + x^{p-d}$$

a

$$\bar{w}_1 = \bar{w}_2 = \frac{P}{1 - x^d},$$

kde

$$P = P_1 \left(\frac{1 - x^p}{1 - x^d} \right)^{-1} = P_2 \left(\frac{1 - x^q}{1 - x^d} \right)^{-1}$$

je polynom stupně nejvýše $d - 1$.

Můžeme naopak zvolit polynomy P'_1 a P'_2 stupňů nejvýše $p - 1$ a $q - 1$ takové, že

$$P'_1 \frac{(1 - x^q)}{(1 - x^d)} - P'_2 \frac{(1 - x^p)}{(1 - x^d)} = x^{p+q-d-1}.$$

Potom slova odpovídající řadám $P'_1(1 - x^p)^{-1}$ a $P'_2(1 - x^q)^{-1}$ mají periody p a q a společný začátek délky $p + q - d - 1$.