Slova s více periodami

Nejprve ukažme alternativní důkaz periodického lemmatu.

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

Důkaz. Nechť je $q < p$ a nechť má slovo $w = a_0 a_1 \cdots a_{p+q-\mathrm{NSD}(p,q)-1}$ periody p a q.

Předpokládejme nejprve, že p a q jsou nesoudělná. Na indexech, tedy na přirozených číslech $0, 1, 2, \ldots, p + q - 2$, definujme nejmenší ekvivalenci splňující $i \approx j$, pokud $i \equiv j \mod p$ nebo $i \equiv j \mod q$. 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 $0, 1, \ldots, q - 1$.

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

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

Nechť je nyní $\mathrm{NSD}(p, q) = d$. Pro $r \in \{0, 1, \ldots, d - 1\}$ 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 má periody p a q, právě když w_r má periody p' a q' pro všechna $r = 0, 1, \ldots, d-1$. Protože slova w_r mají délku $p' + q' - 1$, jsou podle první části důkazu mocninou téhož písmene. Slovo w má proto periodu d. □

A podobně získáme optimalitu.

Věta. Pokud $p \not| q$, pak existuje slovo délky $p + q - \mathrm{NSD}(p, q) - 1$, které má periody p i q, ale nemá periodu $\mathrm{NSD}(p, q)$.

Důkaz. Uvažujme slovo $w = a_0 a_1 \cdots a_{p+q-\mathrm{NSD}(p,q)-2}$ 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 $\{0, 1, \ldots, q - 1\}$ a chápejme je jako vrcholy orientovaného grafu G, ve kterém $i \longrightarrow j$, právě když $i + p < p + q - 2$ a $i + p \equiv j \mod q$. Je snadné si rozmyslet, že třídy $\approx$ omezené na množinu $\{0, 1, \ldots, q - 1\}$ 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 $p - 1 \mod q$ a $p - 2 \mod q$ vstupní stupeň nula. Z toho plyne, že G má více než jednu komponentu a slovo w je netriviální.

Nechť je nyní $\mathrm{NSD}(p, q) = d$. 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. □

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 $\mathrm{NSD}(P)$. Pro $1 \in P$ definujeme $\mathcal{L}_P := 0$. Výše jsme ukázali, že $\mathcal{L}_{\{p,q\}} = p + q - \mathrm{NSD}(p, q) - 1$. Pro jednoduchost se dále omezíme na nesoudělné množiny period, obecný případ se získá obdobně jako výše.

Věta. Buď P množina přirozených čísel, jejichž největší společný dělitel je jedna. Nechť $1 < m = \min P$ a definujme množinu

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

Pak

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

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

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

Nechť $i \equiv j \mod q$ pro $0 \le i < j \le k-1$ a nějaké $q \in Q$. Pokud $q = m$, je jistě $i \approx_{P,k+m} j$. Pokud $q \ne m$, je $i \equiv j + m \mod q + m$ a $j \equiv j + m \mod m$. Protože $i, j, j + m \in \{0, 1, \ldots, m + k - 1\}$ a $m, q + m \in P$, je opět $i \approx_{P,k+m} j$. Tím je dokázána přímá implikace.

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

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

Celá tato posloupnost leží v intervalu $\{0, \ldots, k-1\}$ a pro každé $t = 0, 1, \ldots s - 1$ zřejmě platí buď $i'_t \equiv i'_{t+1} \mod p$ pro nějaké $p \in P$, nebo $i'_t \equiv i'_{t+1} \mod q$ 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 $\mathcal{L}_P \ge 2m - 1$ a $\mathcal{L}_P \ge m + \mathcal{L}_Q$.

Podle $(*)$ dále platí, že pro $k \ge \mathcal{L}_Q + 1$ jsou v $\approx_{P,m+k}$ ekvivalentní všechny prvky $0, 1, \ldots, k-1$. Je-li $\mathcal{L}_Q \ge m - 1$, 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 $\mathtt{FW}(P, n)$, které definujeme jako slovo délky n s největší možnou abecedou a periodami P. Pokud $n \le \min P$, platí

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

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

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

*

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 $\mathbb{Z} \to \mathbb{C}$, pro které platí

$$w(j) = w(j \mod p).$$

Taková zobrazení tvoří p-dimenzionální vektorový prostor nad $\mathbb{C}$, který má také bázi

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

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

Současně vidíme, že hodnoty v bodech $j = 1, 2, \ldots, p+q-\mathrm{NSD}(p,q)-1$ umožňují i jiná řešení.

Ilustrujme to na příkladu $p = 2$ a $q = 3$. Funkce s periodou dva jsou tvaru

$$c_0\varphi_{2,0} + c_1\varphi_{2,1}$$

a funkce s periodou tři jsou tvaru

$$d_1\varphi_{3,0} + d_1\varphi_{3,1} + d_2\varphi_{3,2},$$

přičemž $\varphi_{3,0} = \varphi_{2,0}$ je konstantní jednička, označme ji φ_0. Mají-li se nyní dvě takové funkce rovnat (všude), musí platit

$$(c_0 - d_0)\varphi_0 + c_1\varphi_{2,1} - d_1\varphi_{3,1} - d_2\varphi_{3,2} = 0\,.$$

Protože prvky Fourierovy báze jsou lineárně nezávislé, dostáváme

$$c_0 - d_0 = c_1 = d_1 = d_2 = 0,$$

a hledaná funkce má tedy tvar $a\varphi_0$, kde $a = c_0 = d_0$. To je ovšem případ, kdy se funkce mají rovnat všude. Pokud se mají rovnat jen v bodech $1, \ldots, p+q-\mathrm{NSD}(p-q)$, tedy v našem příkladu v bodech $1, 2, 3, 4$, pak dostáváme soustavu

$$\begin{aligned}
(c_0 - d_0)\varphi_0(1) + c_1\varphi_{2,1}(1) - d_1\varphi_{3,1}(1) - d_2\varphi_{3,2}(1) &= 0\\
(c_0 - d_0)\varphi_0(2) + c_1\varphi_{2,1}(2) - d_1\varphi_{3,1}(2) - d_2\varphi_{3,2}(2) &= 0\\
(c_0 - d_0)\varphi_0(3) + c_1\varphi_{2,1}(3) - d_1\varphi_{3,1}(3) - d_2\varphi_{3,2}(3) &= 0\\
(c_0 - d_0)\varphi_0(4) + c_1\varphi_{2,1}(4) - d_1\varphi_{3,1}(4) - d_2\varphi_{3,2}(4) &= 0\,,
\end{aligned}$$

která má pouze triviální řešení. Klíčové je tedy pozorování, že soustava je regulární: jedná se o Vandermondovu matici. Jednoznačné řešení má např. i soustava

$$\begin{aligned}
(c_0 - d_0)\varphi_0(1) + c_1\varphi_{2,1}(1) - d_1\varphi_{3,1}(1) - d_2\varphi_{3,2}(1) &= 0\\
(c_0 - d_0)\varphi_0(2) + c_1\varphi_{2,1}(2) - d_1\varphi_{3,1}(2) - d_2\varphi_{3,2}(2) &= 0\\
(c_0 - d_0)\varphi_0(3) + c_1\varphi_{2,1}(3) - d_1\varphi_{3,1}(3) - d_2\varphi_{3,2}(3) &= 0\\
(c_0 - d_0)\varphi_0(4) + c_1\varphi_{2,1}(4) - d_1\varphi_{3,1}(4) - d_2\varphi_{3,2}(4) &= 1\,,
\end{aligned}$$

existují tedy dvě různé funkce, které mají periodu dva a tři, ale nemají periodu jedna (protože se liší v bodě 4).

*

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

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

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 komlexních kořenů), že největší společný dělitel polynomů $1 - x^p$ a $1 - x^q$ je $1 - x^d$, kde $d = \mathrm{NSD}(p, q)$. Platí tedy

$$\overline{w_1} - \overline{w_2} = \frac{P_1}{1 - x^p} - \frac{P_2}{1 - x^q} = \frac{(1 - x^d)}{(1 - x^p)(1 - x^q)} \left(P_1 \frac{(1 - x^q)}{(1 - x^d)} - P_2 \frac{(1 - x^p)}{(1 - x^d)} \right),$$

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 $\overline{w_1} - \overline{w_2}$ 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

$$\overline{w_1} = \overline{w_2} = \frac{P}{1 - x^d},$$

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 $p + q - d - 1$.