Algorithms on Strings

Problems Set 1

Aleksander Czeszejko-Sochacki

October 2018

1

Proof.

$$\begin{aligned} |w| - p \textit{ is a border } &\equiv w[1, |w| - p] = w[|w| - (|w| - p), |w|] \\ &\equiv w[1, |w| - p] = w[p, |w|] \\ &\equiv w[i] = w[i + p] \textit{ for } i \in \{1, 2, \ldots, |w| - p\} \\ &\equiv \ p \textit{ is a period of } w \end{aligned} \tag{1}$$

□

2

2.1

Proof.

$$\begin{aligned} p \textit{ is a period of } w &\equiv w \textit{ is a subword of some } x^k \textit{ with } |x| = p \textit{ and } k > 0 \\ &\equiv w = ux^jv \textit{ where } j \leq k, u \sqsubset x \textit{ and } v \sqsupset x \end{aligned} \tag{2}$$

Since u and v - suffix and prefix of x, respectively, we can proceed as follows:

$$w = ux^jv = u(zu)^jv = (uz)^juv \tag{3}$$

Hence, the period condition holds for i $\in \{1, 2, \ldots, |w| - p - |v|\}$. On the other hand:

$$w = ux^jv = ux^{j-1}vyv \tag{4}$$

So the period condition holds for i $\in \{|w| - p - |v|, |w| - p - |v| + 1, \ldots, |w| - p\}$. From 3 and 4 the proof is done. □

2.2

Proof. Assume $|w| = kp + l$. From the period condition we have:

$$w[1,p] = w[p+1,2p] = \cdots = w[(k-1]p+1,kp] \tag{5}$$

and

$$w[kp+1,kp+l] = w[(k-1)p+1,(k-1)p+l] \tag{6}$$

Basing on 5, we can write $w = y^k u$, such that $|y| = p$ and $|u| = l$. On the other hand, by 6, we have $w = xuvu$, where $|u| = l$, $|v| = p - l$, $|x| = |w| - p - l$. Combining these two conclusions, $y = uv$, so $w = (uv)^k u$. □

2.3

Proof.

$$\begin{aligned} p \textit{ is a period of } w &\equiv |w| - p \textit{ is a border of } w \textit{ (1)} \\ &\equiv \exists_{x,\ y,\ z}(|y| = |w| - p \land xy = yz = w) \\ &\equiv \exists_{x,\ y,\ z}(|x| = |y| = p \land xy = yz = w) \end{aligned} \tag{7}$$

□

Lemma 1 (uv periods)**.** *For any unempty u, v and some $k \in \mathbb{N}$, if $uv = vu$, then $|u|, |v|$ are periods of $(uv)^k$.*

Proof.

$$\begin{aligned} |v| \textit{ is a period of } (uv)^k &\equiv |uv|^k - |v| \textit{ is a border of } (uv)^k (1) \\ &\equiv (uv)^{k-1}u \textit{ is both prefix and suffix of } (uv)^k \end{aligned} \tag{8}$$

Indeed, $(uv)^{k-1}u \sqsubset (uv)^k$ and $(uv)^{k-1}u \sqsupset (vu)^k = (uv)^k$ For $|u|$ the proof is simmilar. □

3

Proof. The thesis is equivalent to the following implication:

$$p,\ q \textit{ are periods of } w \implies q \textit{ mod } p,\ p \textit{ are periods of } w$$

Let $w[1,p] = P$, $p < q$ ($p = q$ does not make any sense). We can write:

$$w = w[1,q]w[q+1,|w|] = \underbrace{P^k u}_{w[1,q]}\ \underbrace{vP^k y}_{w[q+1,|w|]}$$

where $uv = P$, $k, l \in \mathbb{N}$.

$$
\begin{aligned}
q \textit{ is a period of } w &\implies |w| - q \textit{ is a border of } w \\
&\implies w[q+1, |w|] \sqsubset w \\
&\equiv vP^k y \sqsubset w
\end{aligned} \tag{9}
$$

As we know from the problem conditions, $p + q < |w|$, so $p < |w| - q$, implies, that $P \sqsubset vP^k y$, what is equivalent to $uv \sqsubset v(uv)^k y$, especially $uv \sqsubset vuv$, what gives us

$$uv = vu \tag{10}$$

Basing on uv periods lemma and that $|u| = q \ mod \ p$, enough to prove, that u period condition holds for $w[|w| - |y|, |w|$. As we know, that $y \sqsubset uv$, the proof is done. $\square$

4

5

6

7

$$
\begin{aligned}
\sum_{k=1}^{n} a_i r^{n-k} \ mod \ q &= (\ldots((ra_1 + a_2)r + a_3)r \ldots)r + a_n \ mod \ q \\
&= (\ldots((ra_1 \ mod \ q \ + a_2)r \ mod \ q \ + a_3)r \ mod \ q \ \ldots)r \ mod \ q \ + a_n \ mod \ q
\end{aligned} \tag{11}
$$

n multiplications, n modulos, n - 1 additions gives us O(n) time. The second transformation is unnecessary. However, enables us to computing values less than q^2. If our $\Sigma \ll |S|$, then calculation all the $ra \ mod \ q$ in preprocessing might be better than doing it ad hoc.

8

Given $\phi_r(x)$ and $\phi_r(y)$:

$$
\begin{aligned}
\phi_r(xy) &= \sum_{k=1}^{|xy|} S[k] r^{|xy|-k} \ mod \ q \\
&= (\sum_{k=1}^{|x|} S[k] r^{|xy|-k} + \sum_{k=|x|+1}^{|xy|} S[k] r^{|xy|-k}) \ mod \ q \\
&= (r^{|}y| \sum_{k=1}^{|x|} x[k] r^{|x|-k} \ mod \ q \ + \sum_{k=|x|+1}^{|xy|} S[k] r^{|xy|-k} \ mod \ q \ ) \ mod \ q \\
&= (r^{|y|}\phi_r(x) + \phi_r(y)) \ mod \ q
\end{aligned}
\tag{12}
$$

Given $\phi_r(xy)$ and $\phi_r(y)$ and referencing 12:

$$
\begin{aligned}
\phi_r(xy) &\equiv r^{|y|}\phi_r(x) + \phi_r(y) \ (mod \ q) \\
\phi_r(xy) - \phi_r(y) &\equiv r^{|y|}\phi(x) \ (mod \ q)
\end{aligned}
\tag{13}
$$

As we know, $q \in \mathbb{P}$ and $r \in \{1, 2, \ldots, q-1\}$. Hence, $gcd(r, q) = 1$. Considering, that we are in $\mathbb{Z}_p^*$, the inverse element of $r^{|y|}$, basing on Fermat's little theorem, is $r^{q-|y|-1}$. Therefore

$$\phi_r(x) \equiv r^{q-|y|-1}(\phi_r(xy) - \phi_r(y)) \ (mod \ q)$$

As $\phi_r(x) < q$:

$$\phi_r(x) = r^{q-|y|-1}(\phi_r(xy) - \phi_r(y)) \ mod \ q$$