planetmath.org

Math for the people, by the people.

Fine and Wilf's theorem on words

Canonical name	FineAndWilfsTheoremOnWords
Date of creation	2013-03-22 18:00:39
Last modified on	2013-03-22 18:00:39
Owner	Ziosilvio (18733)
Last modified by	Ziosilvio (18733)
Numerical id	18
Author	Ziosilvio (18733)
Entry type	Theorem
Classification	msc 68Q70
Classification	msc 68Q45
Classification	msc 68R15

Let w be a word on an alphabet A and let $|w|$ be its length. A period of w is a value $p > 0$ such that $w_{i+p} = w_i$ for every $i \in \{1, 2, \ldots, |w| - p\}$. This is the same as saying that $w = u^k r$ for some $u, r \in A^*$ and $k \in \mathbb{N}$ such that $|u| = p$ and r is a prefix of u.

Fine and Wilf's theorem gives a condition on the length of the periods a word can have.

Theorem 1 *Let w be a word on an alphabet A having periods p and q. If $|w| \geq p+q-\gcd(p, q)$, then w has period $\gcd(p, q)$. The value $p+q-\gcd(p, q)$ is the smallest one that makes the theorem true.*

As a counterexample showing that the condition on $|w|$ is necessary, the word *aaabaaa* has periods 4 and 6, but not $2 = \gcd(4, 6)$. This can happen because its length is $7 < 4 + 6 - 2 = 8$.

Observe that Theorem **??** can be restated as follows (cf. [**?**]).

Theorem 2 *Let u and w be words over an alphabet A. Suppose u^h and w^k, for some h and k, have a common prefix of length $|u| + |w| - \gcd(|u|, |w|)$. Then there exists $z \in A^*$ of length $\gcd(|u|, |w|)$ such that $u, w \in z^*$. The value $|u| + |w| - \gcd(|u|, |w|)$ is also the smallest one that makes the theorem true.*

In fact, Theorem **??** clearly implies Theorem **??**. Now, suppose Theorem **??** is true. Suppose w has periods p and q and length at least $p + q - \gcd(p, q)$: write $w = u^k r = v^h s$ with $|u| = p$, $|v| = q$, r prefix of u, s prefix of v. Let M be a common multiple of p and q greater than p, q, and $|w|$: then $u^{M/p}$ and $v^{M/q}$ have the common prefix w, so they also have a common prefix of length $p + q - \gcd(u, v)$. Then u and v are powers of a word z of length $\gcd(p, q)$, and it is easy to see that $w = z^m t$ for some $m > 0$ and some prefix t of z.

References

[1] M. Lothaire. *Combinatorics on words.* Cambridge University Press 1997.