defect theorem

Canonical name	DefectTheorem
Date of creation	2013-03-22 18:21:43
Last modified on	2013-03-22 18:21:43
Owner	Ziosilvio (18733)
Last modified by	Ziosilvio (18733)
Numerical id	6
Author	Ziosilvio (18733)
Entry type	Theorem
Classification	msc 20M10
Classification	msc 20M05
Defines	$x^m = y^n$ has only trivial solutions over A^*

Let A be an arbitrary set, let A^* be the free monoid on A, and let X be a finite subset of A^* which is not a code. Then the free hull H of X is itself finite and $|H| < |X|$.

Observe how from the defect theorem follows that the equation $x^m = y^n$ over A^* has only the trivial solutions where x and y are powers of the same word: in fact, $x^m = y^n$ iff $\{x, y\}$ is not a code.

Proof. It is sufficient to prove the thesis in the case when X does not contain the empty word on A.

Define $f : X \to H$ such that $f(x)$ is the only $h \in H$ such that $x \in hH^*$: f is well defined because of the choice of X and H. Since X is finite, the thesis shall be established once we prove that f is surjective but not injective.

By hypothesis, X is not a code. Then there exists an equation $x_1 \cdots x_n = x'_1 \cdots x'_m$ over X with a nontrivial solution: it is not restrictive to suppose that $x_1 \neq x'_1$. Since however the factorization *over* H is unique, the h such that $x_1 \in hH^*$ is the same as the h' such that $x'_1 \in h'H^*$: then $f(x_1) = f(x'_1)$ with $x_1 \neq x'_1$, so f is not injective.

Now suppose, for the sake of contradiction, that $h \in H \setminus f(X)$ exists. Let $K = (H \setminus \{h\})h^*$. Then any equation

$$k_1 \cdots k_n = k'_1 \cdots k'_m \ , k_1, \cdots , k_n, k'_1, \ldots , k'_m \in K \tag{1}$$

can be rewritten as

$$h_1 h^{r_1} \cdots h_n h^{r_n} = h'_1 h^{s_1} \cdots h'_m h^{s_m} \ , h_1, \ldots , h_n, h'_1, \ldots , h'_m \in H \setminus \{h\} \ ,$$

with $k_i = h_i h^{r_i}$, $k'_i = h'_i h^{s_i}$: this is an equation over H, and as such, has only the trivial solution $n = m$, $h_i = h'_i$, $r_i = s_i$ for all i. This implies that (**??**) only has trivial solutions over K: by the characterization of free submonoids, K is a code. However, $X \subseteq K^*$ because no element of x "starts with h", and K^* is a proper subset of H^* because the former does not contain h and the latter does. Then K^* is a free submonoid of A^* which contains X and is properly contained in H^*, against the definition of H as the free hull of X.

References

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