RAIRO-Theor. Inf. Appl. 51 (2017) 135–139
DOI: 10.1051/ita/2017012

Available online at:
www.rairo-ita.org

NON-PRIMITIVE WORDS OF THE FORM pq^m

Othman Echi[1,2]

Abstract. Let p, q be two distinct primitive words. According to Lentin−Schützenberger [9], the language p^+q^+ contains at most one non-primitive word and if pq^m is not primitive, then $m \leq \frac{2\mid p\mid}{\mid q\mid}+3$. In this paper we give a sharper upper bound, namely, $m \leq \lfloor \frac{\mid p\mid -2}{\mid q\mid} + 2\rfloor$, where $\lfloor x\rfloor$ stands for the floor of x.

Mathematics Subject Classification. 68R15.

1. Introduction

An alphabet is a nonempty finite set Σ. Its elements are called symbols (or letters). A (finite) word is a (finite) sequence of symbols from Σ. The length of a word $u = a_1 \dots a_n$, denoted by $\mid u\mid$ is the number n of its letters.

Two words $w_1 = a_1 \dots a_n$ and $w_2 = b_1 \dots b_m$ are equal if $n = m$ and $a_i = b_i$, for every i.

We denote by Σ^*, Σ^+ the sets of all finite, finite nonempty words, respectively. The concatenation or product of words is defined as follows

$$\text{If } w_1 = a_1 \dots a_n \text{ and } w_2 = b_1 \dots b_m, \text{ then } w_1w_2 = a_1 \dots a_nb_1 \dots b_m.$$

Clearly, this operation is associative and the empty word is the unit element.

Consequently, $\Sigma^* = (\Sigma^*, .)$ is a free monoid and $\Sigma^+ = (\Sigma^+, .)$ is a free semigroup.

When $k \in \mathbb{N} \setminus \{0, 1\}$, we say that u^k is a *proper power* of u.

A word is called *primitive* if it is not empty and not a proper power of another word. The concept of primitive words plays a crucial role in algebraic coding theory and combinatorial theory of words (see [10, 11]).

It is also worth noting that primitive words can be linked with the prime spectra of rings; endowed with the Zariski topology (see [7]).

Let $u \in \Sigma^+$; then there exist a unique primitive word $\sqrt{u}$ (called *the primitive root* of u) and a unique integer $\mathfrak{e} \geq 1$ (called *the exponent* of u) such that $u = \sqrt{u}^{\,\mathfrak{e}}$ (see [12]).

Keywords and phrases. Combinatorics on words, primitive word, primitive root.

[1] King Fahd University of Petroleum and Minerals, Department of Mathematics and Statistics PO Box 5046, Dhahran 31261, Saudi Arabia.

[2] University Tunis-El Manar. Faculty of Sciences of Tunis, Department of Mathematics, 2092 Tunis, Tunisia. othechi@yahoo.com

Let $p \neq q$ be two distinct primitive words; then following a result due to Lyndon-Schützenberger [12], the words $p^n q^m$ are primitive for all integers $m, n \geq 2$. If $m = 1$ or $n = 1$, then $p^n q^m$ is not necessarily primitive; for example if $p = a, q = bab$, then $pq = (ab)^2$ is not primitive. According to Lentin−Schützenberger [9] the language p^+q^+ contains at most one non-primitive word; which is of the form pq^m or $p^n q$. Twenty five years later, Shyr–Yu rediscovered the same result in [13].

Moreover, if pq^m is not primitive, then $m \leq \dfrac{2 \mid p \mid}{\mid q \mid} + 3$ [9]. In this paper we give a sharper upper bound, namely, $m \leq \lfloor \dfrac{\mid p \mid -2}{\mid q \mid} + 2 \rfloor$, where $\lfloor x \rfloor$ stands for the floor of x.

2. Preliminaries

In this section we will review some well known results from literature.

If Σ is an alphabet, then we denote by $\mathbf{Q}(\Sigma)$ the set of all primitive words. The symbol $\mathbf{Q}^{(k)}(\Sigma)$ stands for the set of all elements of Σ^+ with exponent k.

Proposition 2.1 [12]**.** *Let $u, v \in \Sigma^+$; then $uv = vu$ if and only if u, v are powers of a common word.*

Proposition 2.2 [12]**.** *Let $u \in \Sigma^+$; then there exist a unique primitive word $\sqrt{u}$ (called* the primitive root *of u) and a unique positive integer $\mathfrak{e}$ (called* the exponent *of u) such that $u = \sqrt{u}^{\,e}$.*

Proposition 2.3 [9, 13]**.** *Let p, q be distinct primitive words over Σ, then the language p^+q^+ contains at most one non-primitive word.*

Proposition 2.4 [13]**.** *Let $p \neq q \in \mathbf{Q}(\Sigma)$. If $pq^m = g^k$ for some $m, k \geq 2$ and $g \in \mathbf{Q}(\Sigma)$, then one of the following two statements hold*:

(1) $p = (xq^m)^{k-1}x$*, for some* $x \in \Sigma^+$.
(2) $p = (yx(x(yx)^{j+1})^{m-1})^{k-2} yx(x(yx)^{j+1})^{m-2}xy$ *and* $q = x(yx)^{j+1}$*, for some* $x \neq y \in \Sigma^+, j \geq 0$.

We close this section by a theorem due to Fine–Wilf [8] which is the main ingredient to solve most problems on primitivity.

Theorem 2.5 (Fine–Wilf Theorem)**.** *Let $u, v \in \Sigma^+$. Then the following statements are equivalent.*

(i) *u and v are powers of the same word.*
(ii) *there exist $i, j > 0$ so that u^i and v^j have a common prefix (suffix) of length* $\mid u \mid + \mid v \mid - \gcd(\mid u \mid, \mid v \mid)$.

3. Non-Primitive Words of the form pq^m

The following Lemma is inspired from Proposition 2.4, but here we are assuming that $m \geq 1$ instead of $m \geq 2$. Let us first recall a lemma from [9] that appeared also in [13].

Lemma 3.1 ([9], Corollary 4 and [13])**.** *If $uq^m = g^k$ for some $m, k \geq 1$, $u \in \Sigma^+$, and $g, q \in \mathbf{Q}(\Sigma)$, with $u \notin q^+$, then $g \neq q$ and $\mid g \mid > \mid q^{m-1} \mid$.*

Lemma 3.2. *Let p, q be distinct primitive words on an alphabet Σ, and $k \geq 2, m \geq 1$ be integers. Then the following statements are equivalent.*

(i) $pq^m \in \mathbf{Q}^{(k)}(\Sigma)$.
(ii) *One of the following properties hold.*
  (1) *there exists $x \in \Sigma^+$ such that $p = (xq^m)^{k-1}x$ and $xq^m \in \mathbf{Q}(\Sigma)$.*

(2) *there exist* $x, y \in \Sigma^+$ *such that* $q = yx$, $py = (x(yx)^{m-1})^{k-1}$ *and* $x(yx)^{m-1} \in \mathbf{Q}(\Sigma)$.

Proof. (i) $\Longrightarrow$ (ii). Assume $pq^m = \rho^k$, for some $\rho \in \mathbf{Q}(\Sigma)$.

We claim that $|\rho| \neq |q^m|$, otherwise $\rho = q^m$ as suffixes with the same length of the same word; so $m = 1$ and $q = \rho$. Hence $p = q^{k-1}$; thus $k = 1$. We deduce that $p = \rho$; this leads to the equality $p = q$, which is contrary to our assumption. Therefore $|\rho| \neq q^m$.

Two cases have to be considered.

Case 1. Assume $|\rho| > |q^m|$. In this case, as $pq^m = \rho^k$, we deduce that $\rho = xq^m$, for some $x \in \Sigma^+$. Hence

$$pq^m = \rho^k = \rho^{k-1}(xq^m).$$

Thus

$$p = \rho^{k-1}x = (xq^m)^{k-1}x.$$

Case 2. Assume $|\rho| < |q^m|$.

By ([13], Lem. 2.1), we have $|\rho| > |q^{m-1}|$. Now, since $pq^m = pqq^{m-1} = \rho^{k-1}\rho$, we conclude that $\rho = xq^{m-1}$, for some $x \in \Sigma^+$; so

$$pq = \rho^{k-1}x = (xq^{m-1})x.$$

Now, as $|\rho| < |q^m|$ and $pq^m = \rho^{k-1}\rho$, there exists $y \in \Sigma^+$ such that $q^m = y\rho$. We conclude that $pq^m = py\rho = \rho^k$. This yields

$$py = \rho^{k-1} = (xq^{m-1})^{k-1}.$$

Thus

$$pq = \rho^{k-1}x = pyx,$$

so $q = yx$.

We conclude that

$$q = yx, py = (x(yx)^{m-1})^{k-1} \text{ and } x(yx)^{m-1} \in \mathbf{Q}(\Sigma).$$

(ii) $\Longrightarrow$ (i).

– Suppose that $p = (xq^m)^{k-1}x$ and $xq^m \in \mathbf{Q}(\Sigma)$, for some $x \in \Sigma^+$; then

$$\begin{aligned} pq^m &= (xq^m)^{k-1}xq^m \\ &= (xq^m)^k \in \mathbf{Q}^{(k)}(\Sigma). \end{aligned}$$

Now, assume $q = yx$, $py = (x(yx)^{m-1})^{k-1}$ and $x(yx)^{m-1} \in \mathbf{Q}(\Sigma)$, for some $x, y \in \Sigma^+$; then we get

$$\begin{aligned} pq^m &= p(yx)^m \\ &(py)x(yx)^{m-1} \\ &= (x(yx)^{m-1})^{k-1}kx(yx)^{m-1} \\ &= (x(yx)^{m-1})^k \in \mathbf{Q}^{(k)}(\Sigma). \end{aligned}$$

□

From the paper of Lentin$-$Schützenberger [9], one may see that if pq^m is not a primitive word, then $m \leq \dfrac{2|p|}{|q|} + 3$. Lemma 3.2 enables us giving an upper bound shaper than that of [9].

Theorem 3.1. *Let* p, q *be distinct primitive words on an alphabet* Σ *and* m *be a positive integer. If* pq^m *is not primitive, then*

$$m \leq \left\lfloor \frac{|p| - 2}{|q|} + 2 \right\rfloor,$$

where $\lfloor x \rfloor$ *stands for the floor of* x.

Proof. By the previous theorem, we consider two cases.
Case 1. Assume $p = (xq^m)^{k-1}x$, for some $x \in \Sigma^+$ and $k \geq 2$, then

$$| p | = (k-1)(| x | + m | q |) + | x | = k | x | + (k-1)m | q | .$$

In this case, we get

$$| p | \geq 2 + m | q |,$$

consequently $m < \frac{| p | - 1}{| q |}$.
Case 2. Assume $q = yx$, $py = (x(yx)^{m-1})^{k-1}$, for some $x, y \in \Sigma^+$. Hence

$$| p | + | y | = (k-1)[| x | + (m-1) | q |].$$

So

$$| p | + | q | = k | x | + (m-1)(k-1) | q | .$$

This gives

$$\begin{aligned} | p | &= k | x | + ((m-1)(k-1) - 1) | q | \\ &= k | x | + (k(m-1) - m) | q |, \end{aligned}$$

yielding the following inequalities:

$$\begin{aligned} | p | &\geq 2 + (k(m-1) - m) | q | \\ &\geq 2 + (2m - 2 - m) | q | \\ &= 2 + (m-2) | q | . \end{aligned}$$

Therefore, $m \leq \frac{| p | - 2}{| q |} + 2$. □

Remark 3.3.

(1) Clearly, our upper bound is sharper than that provided in [9]; indeed

$$\left(\frac{2 | p |}{| q |} + 3\right) - \left(\frac{| p | - 2}{| q |} + 2\right) = \frac{| p | + 2}{| q |} + 1.$$

(2) Our upper bound may be reached: it suffices to consider $p = a$, $q = bab$; then for $m = \lfloor \frac{| p | - 2}{| q |} + 2 \rfloor = 1$; and $pq^m = (ab)^2$ is non-primitive.

Lemma 3.4. *Let p, q be distinct primitive words on Σ such that $| q |$ divides $| p |$. Then $qp^2 \in \mathbf{Q}(\Sigma)$.*

Proof. We let $| p | = m | q |$, with $m \geq 1$. Assume $qp^2 \notin \mathbf{Q}(\Sigma)$; then $qp^2 = r^n$, for some $n \geq 2$. By 3.1, $r \neq p$ and $| r | > | p |$; this yields $n = 2$. Now, Considering the length of $qp^2 = r^2$ we have $2 | r | = (1 + 2m) | q |$. Thus $| q |$ is even and $| r | = (1 + 2m)\frac{| q |}{2}$. This implies, in particular, that $\gcd(| p |, | r |) \geq \frac{| q |}{2}$.

It follows that p^2 is a common suffix of p^2 and r^2 with length

$$| p^2 | = 2 | p | = | p | + | r | - \frac{| q |}{2} \geq | p | + | r | - \gcd(| p |, | r |).$$

Therefore, according to Theorem 2.5, p and r are powers of the same word, leading to $p = r$, a contradiction. □

Now, combining Lemma 3.2, Lemma 3.4 and Theorem 3.1, one may easily obtain the following result.

Corollary 3.5 [1]**.** *Let p, q be distinct primitive words on Σ such that $\mid q \mid$ divides $\mid p \mid$. Then for all positive integers $(m, n) \neq (1, 1)$ and $m \geq \frac{\mid p \mid}{\mid q \mid}$, the word $p^n q^m$ is primitive.*

Acknowledgements. I gratefully thank the referee for the constructive comments, suggestions and recommendations which definitely help to improve the readability and quality of this paper. A special thank to the referee for simplifying the proof of Lemma 3.4 and providing references [8,9].

References

[1] C. Chunhua, Y. Shuang and Y. Di, Some Kinds of Primitive and non-primitive Words. *Acta Inform.* **51** (2014) 339–346.

[2] P. Dömösi and G. Horváth, Alternative proof of the Lyndon−Schützenberger theorem. *Theoret. Comput. Sci.* **366** (2006) 194–198.

[3] P. Dömösi and G. Horvath, The language of primitive words is not regular: two simple proofs. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS* **87** (2005) 191–197.

[4] P. Dömösi, G. Horváth and L. Vuillon, On the Shyr−Yu theorem. *Theoret. Comput. Sci.* **410** (2009) 4874–4877.

[6] P. Dömösi and M. Ito, Context-free languages and primitive words. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ (2015).

[6] P. Dömösi, M. Ito and S. Marcus, Marcus contextual languages consisting of primitive words. *Discrete Math.* **308** (2008) 4877–4881.

[7] O. Echi and M. Naimi, Primitive words and spectral spaces. *New York J. Math.* **14** (2008) 719–731.

[8] N.J. Fine and H. S. Wilf, Uniqueness theorems for periodic functions. *Proc. Amer. Math. Soc.* **16** (1965) 109–114.

[9] A. Lentin and M. P. Schützenberger, A combinatorial problem in the theory of free monoids. 1969 Combinatorial Mathematics and its Applications. *Proc. Conf., Univ. North Carolina, Chapel Hill, N.C.* Univ. North Carolina Press, Chapel Hill, N.C. (1967) 128–144.

[10] M. Lothaire, Combinatorics on words (Corrected reprint of the 1983 original). Cambridge University Press, Cambridge (1997).

[11] M. Lothaire, Algebraic combinatorics on words. Vol. 90 of *Encyclopedia of Math. Appl.* Cambridge University Press, Cambridge (2002).

[12] R.C. Lyndon and M.P. Schützenberger, The equation $a^M = b^N c^P$ in a free group. *Michigan Math. J.* **9** (1962) 289–98.

[13] H.J. Shyr and S.S. Yu, Non-primitive words in the language p^+q^+. *Soochow J. Math.* **20** (1994) 535–546.

Received November 8, 2017. Accepted November 14, 2017.