International Journal of Algebra, Vol. 4, 2010, no. 15, 693 - 707

On Primitive Words

Salwa Bouallègue

University Tunis-El Manar, Faculty of Sciences of Tunis
Department of Mathematics
"Campus Universitaire" 2092 El Manar, Tunis, Tunisia
salwa.bouallegue@gmail.com

Mongi Naimi

University Tunis-El Manar, Faculty of Sciences of Tunis
Department of Mathematics
"Campus Universitaire" 2092 El Manar, Tunis, Tunisia

Abstract

Let A be a finite alphabet, A^* be the set of all finite words. Let $c : A^* \to A^*$ be the circular shift defined by $c_{_A}(\varepsilon) = \varepsilon$, and $c_{_A}(at) = ta$, for each $a \in A$ and $t \in A^*$). Then the additive group $(\mathbb{Z}, +)$ acts on A^* by the action $\mathbb{Z} \times A^* \longrightarrow A^*$, which sends the pair (k, u) to the word $c_{_A}^k(u)$. In this paper, we prove that the stabilizer of a nonempty word u of length n is exactly $\mathcal{S}_u = \lambda\mathbb{Z} := \{k\lambda \mid k \in \mathbb{Z}\}$, where λ is the length of the primitive root of u.

Using Burnside's counting orbit theorem, we give an alternative proof of the total number of necklaces of length n on k symbols:

$$N(n,k) = \frac{1}{n}\sum_{d|n} k^d \phi(\frac{n}{d}),$$

where ϕ is the Euler totient function.

Particular bijections from A^* to itself are also introduced and studied.

Mathematics Subject Classification: 05A19, 68R05, 68R15

Keywords: Burnside's counting theorem, Combinatorics on words, Euler totient function, Primitive words, Möbius function

1 Introduction and Notations

By an *alphabet* we mean a finite nonempty set A. The elements of A are called letters of A. A *finite word* over an alphabet A is a finite sequence of elements

of A. The set of all finite words is denoted by A^*. The sequence of zero letter is called the *empty word* and denoted by ε. We will denote by A^+ the set of all finite nonempty words. If $u := u_1 \cdots u_n$ is a finite sequence of n letters, then n is called *the length* of the word u and we denote it by $|u|$. Let us denote by A^n the set of all finite words over A of length n. The *concatenation* of two words $u := u_1 \cdots u_n$ and $v := v_1 \cdots v_m$ of lengths respectively n and m is the word $uv := u_1 \cdots u_n v_1 \cdots v_m$ of length $n + m$. The set A^* equipped with the concatenation operation is a monoid with ε as a unit element. A *power* of a word u is a word of the form u^k for some $k \in \mathbb{N}$. It is convenient to set $u^0 = \varepsilon$, for each word u. When $k \in \mathbb{N} \setminus \{0, 1\}$, we say that u^k is a *proper power* of u.

A word u is said to be a *prefix* (resp. *suffix*, resp. *factor*) of a word v if there exists a word t (resp. t, resp t and s) such that $ut = v$ (resp. $tu = v$, resp. $tus = v$). If $u = vt$, then we set $ut^{-1} := v$ or $v^{-1}u := t$. The prefix of length k of a word u will be denoted by $\mathbf{pref}_k(u)$.

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 [14] and combinatorial theory of words (see [7] and [6]).

Two words x and y are said to be *conjugate* if there exists $k \in \mathbb{Z}$ such that $x = c_A^k(y)$; where $c : A^* \to A^*$ is the circular shift defined by $c_A(\varepsilon) = \varepsilon$, and $c_A(at) = ta$, for each $a \in A$ and $t \in A^*$). The bijection c may, also, be defined as follows: $c_A(\varepsilon) = \varepsilon$, and $c_A(u) = (\mathbf{pref}_1(u))^{-1} u . \mathbf{pref}_1(u)$, for each $u \in A^+$.

The relation "being conjugate", which we denote by $\sim$, is clearly an equivalence relation. The equivalence class of a word u is called *the conjugacy class* of u and denoted by $\mathcal{C}_u$. A conjugacy class of a word of length n is often called a *circular word*, or *necklace* of length n. The conjugacy class of a primitive word will be called a *primitive necklace*.

It is worth noting that necklaces occur in periodic discrete phenomenons; such as music or astronomy. The enumeration of necklaces (resp. primitive necklaces) of length n on k symbols has appeared explicitly in MacMahon's paper (1892) [10]:

$$M(n,k) = \frac{1}{n} \sum_{d|n} k^d \mu(\frac{n}{d}),$$

for the number $M(n,k)$ of primitive necklaces, where μ is the Möbius function. This formula is often called Witt's formula [11]. In connection with the Poincaré-Birkhoff-Witt theorem (a theorem on free Lie algebras) [16], Ernst Witt has proved this formula in 1937.

The formula for the total number of necklaces of length n on k symbols is

$$N(n,k) = \frac{1}{n} \sum_{d|n} k^d \phi(\frac{n}{d}),$$

where ϕ is the Euler totient function. This formula is called MacMahon's formula (in the book by Graham et al. [3]). In Lucas's book [8, page 503], it is credited to Moreau.

The aim of this paper is to give several new properties shedding light on primitive words. We, also, give an alternative proof of the MacMahon's formula, using Burnside's orbit counting theorem.

2 Primitive Words

We begin by recalling some preliminary results.

Lemma 2.1 (Lyndon-Schutzenberger [9]) *The words $u, v \in A^*$ are conjugate if and only if there exist two words $p, q \in A^*$ with $u = pq$ and $v = qp$.*

Lemma 2.2 (Lyndon-Schutzenberger [9]) *Let $u, v \in A^*$ with $uv = vu$. Then there exists a word t such that $u, v \in t^* := \{t^n \mid n \in \mathbb{N}\}$.*

Lemma 2.3 (Lyndon-Schutzenberger [9]) *Let $u \in A^+$. Then there exist a unique primitive word z and a unique integer $k \geq 1$ such that $u = z^k$.*

Notations 2.4 *Let $u \in A^+$. By Lemma 2.3, there exist a unique primitive word z and a unique integer $k \geq 1$ such that $u = z^k$.*

- *The word z is called* the primitive root *of u; we denote by $z = p_{_A}(u)$.*
- *The integer k is called* the exponent *of u; we denote by $k =_{_A} (u)$.*

Now, let us state some straightforward remarks about the circular shift $c_{_A} : A^* \to A^*$ defined by $c_{_A}(\varepsilon) = \varepsilon$, and $c_{_A}(at) = ta$, for each $a \in A$ and $t \in A^*$.

Remarks 2.5 *Let $c_{_A} : A^* \to A^*$ be the previously defined bijection. Then the following properties hold.*

(1) *For each$(w, n) \in A^* \times \mathbb{N}$ and each $k \in \mathbb{Z}$, we have $c_{_A}^k(w^n) = [c_{_A}^k(w)]^n$.*

Clearly, on may suppose that $k \geq 1$; and thus the equality may be established using induction on k. It is sufficient to prove that $c_{_A}(w^n) = [c_{_A}(w)]^n$. This is an easy task, it suffices to write the concatenation product

$$[c_{_A}(w)]^n = [(\mathbf{pref}_1(w))^{-1} w.\mathbf{pref}_1(w)]^n.$$

But, since the concatenation is associative and

$$\mathbf{pref}_1(w).[(\mathbf{pref}_1(w))^{-1} w] = w,$$

we get $[c_{_A}(w)]^n = [(\mathbf{pref}_1(w))^{-1}w]w^{n-1}\mathbf{pref}_1(w)$. *On the other hand,* $\mathbf{pref}_1(w) = \mathbf{pref}_1(w^n)$, *and by definition of quotient word, we have* $[(\mathbf{pref}_1(w))^{-1}w]w^{n-1} = (\mathbf{pref}_1(w^n))^{-1}w^n$ *(do not think to the associativity rule). Therefore,*

$$[c_{_A}(w)]^n = (\mathbf{pref}_1(w^n))^{-1}w^n\mathbf{pref}_1(w^n) = c_{_A}(w^n).$$

(2) *For each* $w \in A^*$ *and each integer* $0 \leq r \leq |w|$, *we have*

$$c^r_{_A}(w) = (\mathbf{pref}_r(w))^{-1}w(\mathbf{pref}_r(w)).$$

In particular, $c^{|w|}_{_A}(w) = w$.

In the following, we generalize the concept of conjugate words.

Definitions 2.6 *Let* A *be an alphabet and* $\sigma : A^* \longrightarrow A^*$ *be a bijection. We say that two words* u, v *are* σ-conjugate *if there exists an integer* $k \in \mathbb{Z}$ *such that* $u = \sigma^k(v)$.

Definitions 2.7 *Let* A *be an alphabet and* $\sigma : A^* \longrightarrow A^*$ *be a bijection. We say that* σ *is* power preserving *if for each word* $u \in A^*$, *each* $k \in \mathbb{Z}$ *and each* $n \in \mathbb{N}$, *we have*

$$\sigma^k(u^n) = (\sigma^k(u))^n.$$

For a bijection $\sigma : A^* \longrightarrow A^*$, the relation "being σ-conjugate", which we denote by $\sim_\sigma$, is clearly an equivalence relation. The equivalence class of a word u will be called the *σ-conjugacy class* (or *σ-circular word*, or *σ-necklace* of u and denoted by $\mathcal{C}_\sigma(u)$.

Proposition 2.8 *Let* A *be an alphabet and* $\sigma : A^* \longrightarrow A^*$ *be a power preserving bijection. Let* $u, v \in A^+$ *be two* σ*-conjugate words. Then* u *is primitive if and only if so is* v.

Proof. Suppose that u is a primitive word. Since u and v are σ-conjugate, there exists $k \in \mathbb{Z}$ such that $u = \sigma^k(v)$. Now, if v is not primitive, then there exist a word v_1 and an integer $n \geq 1$ such that $v = v_1^n$. Hence $u = \sigma^k(v) = \sigma^k(v_1^n) = (\sigma^k(v_1))^n$. It follows that $u = (\sigma^k(v_1))^n$, contradicting the primitivity of u.

Proposition 2.9 *Let* A *be an alphabet,* $\sigma : A^* \longrightarrow A^*$ *be a power preserving bijection and* $u, v \in A^+$. *Then the following statements are equivalent:*

(*i*) u *and* v *are* σ*-conjugate;*

(ii) $p_A(u)$ and $p_A(v)$ are σ-conjugate and u and v have the same exponent.

Proof.

$(i) \Longrightarrow (ii)$. Let $k \in \mathbb{Z}$ such that $u = \sigma^k(v)$. We denote by n the exponent of v; then $v = p_A(v)^n$. Hence, $u = \sigma^k(v) = [\sigma^k(p_A(v))]^n$. But, as $p_A(v)$ is primitive and $p_A(v)$, $\sigma^k(p_A(v))$ are σ-conjugate, then applying Proposition 2.8, we conclude that $\sigma^k(p_A(v))$ is a primitive word. Now, according to Lemma 2.3, $p_A(u) = \sigma^k(p_A(v))$ and $e_A(u) = e_A(v) = n$, as desired.

$(ii) \Longrightarrow (i)$. Suppose that $p_A(u)$ and $p_A(v)$ are σ-conjugate and $e_A(u) = e_A(v) := n$. Then there exists $k \in \mathbb{Z}$ such that $p_A(u) = \sigma^k(p_A(v))$. Thus,

$$\sigma^k(v) = \sigma^k((p_A(v))^n) = [\sigma^k(p_A(v))]^n = (p_A(u))^n = u.$$

Therefore, u and v are σ-conjugate.

Let us agree to say that a word v is a *central factor* of u if there are two nonempty words t, s such that $u = tvs$.

The following clarifies a result of Choffrut-Karhumäki in [2].

Theorem 2.10 *Let $u \in A^+$. Then the following statements are equivalent:*

(i) u is a primitive word;

(ii) u is not a central factor of u^2;

(iii) for each integer $n \geq 2$, u^{n-1} is not a central factor of u^n;

(iv) there exists an integer $n \geq 2$ such that u^{n-1} is not a central factor of u^n.

Proof.

$(i) \Longrightarrow (ii)$. Assume that u is a central factor of u^2. Then there exist two nonempty words t, s such that $u^2 = tus$. Hence, $|u| = |t| + |s|$; and then t (resp., s) is a prefix (resp., suffix) of u. Thus, there exist two words l and r such that

$$u = tl = rs. \quad (1)$$

This yields $u^2 = tus = tlrs$; and consequently, we get

$$u = lr. \quad (2)$$

Thus, we have

$$|u| = |l| + |r| = |t| + |l| = |r| + |s|.$$

This implies that $|r| = |t|$ and $|l| = |s|$. But, since in addition, we have $tl = rs$, we conclude that $r = t$ and $l = s$; so that combining equalities (1) and (2), we get

$$u = lr = sr = rs.$$

It follows that r and s are powers of the same word z, by Lemma 2.2. Note that $r \neq \varepsilon$, since $u \neq s$. Therefore, $u = z^n$, with $n \geq 2$, contradicting the fact that u is a primitive word.

$(ii) \Longrightarrow (iii)$. We use induction on $n \geq 2$. Suppose that for each integer $2 \leq k \leq n-1$, u^k is not a central factor of u^{k+1}. Let us prove that u^n is not a central factor of u^{n+1}. Assume the contrary, then there exist two nonempty words t and s such that $u^{n+1} = tu^n s$. Hence, $|u| = |t| + |s|$; and then t (resp., s) is a proper prefix (resp., suffix) of u. Thus, there exist two nonempty words l and r such that $u = tl = rs$. This implies that $tu^n s = u^{n+1} = uu^{n-1}u = tlu^{n-1}rs$; and consequently, we get $u^n = lu^{n-1}r$. This contradicts the induction hypothesis.

$(iii) \Longrightarrow (iv)$. Straightforward.

$(iv) \Longrightarrow (i)$. Suppose that u is not primitive; then there exist a nonempty word z and an integer $k \geq 2$ such that $u = z^k$. Accordingly, $u^n = z^{nk} = zz^{k(n-1)}z^{k-1} = zu^{n-1}z^{k-1}$; and then u^{n-1} is a central factor of u^n, a contradiction.

3 Particular Bijections on A^*

The properties of the circular shift $c_{_A} : A^* \to A^*$ incite us to introduce the following concept.

Definition 3.1 *Let A be an alphabet. A bijection $\sigma : A^* \to A^*$ is said to be a* $\mathcal{T}$-bijection *if it satisfies the following properties:*

(*i*) $\sigma^{|u|}(u) = u$, *for each word* $u \in A^*$.

(*ii*) σ *is power preserving.*

(*iii*) *If* $u \in A^+$ *is a primitive word and* $0 \leq r < |u|$ *is an integer such that* $\sigma^r(u) = u$, *then* $r = 0$.

The following result provides few information about $\mathcal{T}$-bijections

Proposition 3.2 *Let A be an alphabet. Then the following properties hold.*

(1) *The circular shift $c_{_A}$ defined on A^* is a $\mathcal{T}$-bijection.*

(2) *Let $p_{_A} : A^* \to A^*$ be the mapping which sends ε to ε and each nonempty word to its primitive root. Let σ be a $\mathcal{T}$-bijection. Then $\sigma \circ p_{_A} = p_{_A} \circ \sigma$ (that is, σ preserves primitive words).*

(3) *If σ is a $\mathcal{T}$-bijection on A^*, then so is σ^{-1}.*

Proof. Property (3) is straightforward.

– Let us prove (1). According to Remarks 2.5, it is enough to show that if u is a primitive word and $0 \leq r < |u|$ is an integer such that $c_{A}^{r}(u) = u$, then $r = 0$. Indeed, in this case, $u = (\mathbf{pref}_r(u))^{-1}u(\mathbf{pref}_r(u))$. Thus,

$$\begin{aligned} u^2 &= uu \\ &= (\mathbf{pref}_r(u))[(\mathbf{pref}_r(u))^{-1}u](\mathbf{pref}_r(u))[(\mathbf{pref}_r(u))^{-1}u] \\ &= (\mathbf{pref}_r(u))[(\mathbf{pref}_r(u))^{-1}u(\mathbf{pref}_r(u))][(\mathbf{pref}_r(u))^{-1}u] \\ &= (\mathbf{pref}_r(u))u[(\mathbf{pref}_r(w))^{-1}u]. \end{aligned}$$

But, since in addition u is primitive, then applying Theorem 2.10, we see that u is not a central factor of u^2. We deduce that $\mathbf{pref}_r(u) = \varepsilon$ or $(\mathbf{pref}_r(u))^{-1}u = \varepsilon$. It follows that $r = 0$ or $r = |u|$. But, as $r < |u|$, we get $r = 0$, as desired.

– Now, let us show (2). From Definition 3.1 (ii), we see that $\sigma(\varepsilon) = \varepsilon$. Then $\sigma(p_{A}(\varepsilon)) = p_{A}(\sigma(\varepsilon))$. Let $u \in A^+$. Then $u = (p_{A}(u))^e$, with e the exponent of u. Hence $\sigma(u) = \sigma((p_{A}(u))^e) = (\sigma(p_{A}(u)))^e$. By Proposition 2.8, $\sigma(p_{A}(u))$ is a primitive word. Thus, according to Lemma 2.3, we have $p_{A}(\sigma(u)) = \sigma(p_{A}(u))$.

Remark 3.3 *The composition of two $\mathcal{T}$-bijections is not necessarily a $\mathcal{T}$-bijection.*

- *If $\sigma : A^* \to A^*$ is a $\mathcal{T}$-bijection, then so is σ^{-1}. But, clearly, $\sigma \circ \sigma^{-1}$ is not a $\mathcal{T}$-bijection.*
- *Also, σ^2 is not a $\mathcal{T}$-bijection. It suffices to consider a primitive word u of a nonzero even length $|u| = 2i$. Then $(\sigma^2)^i(u) = u$. However, $i \neq 0$.*

Proposition 3.4 *Let A be an alphabet and $\sigma : A^* \to A^*$ be a $\mathcal{T}$-bijection. Let k be a nonzero integer. Then the following statements are equivalent:*

(i) *σ^k is a $\mathcal{T}$-bijection;*

(ii) *$k = \pm 1$.*

Proof. Let $n \in \mathbb{N} \setminus \{0\}$ and u be a primitive word of length n. Let $d := \gcd(n, |k|)$. If we suppose that $d \neq 1$, then $0 < \dfrac{n}{d} < n$. But since $n|k| = dm$ (where m is the *lcm* of n and $|k|$), we deduce that $(\sigma^k)^{\frac{n}{d}}(u) = u$, this contradicts the fact that σ^k is a $\mathcal{T}$-bijection.

It follows that $\gcd(n, |k|) = 1$, for each $n \in \mathbb{N} \setminus \{0\}$. Consequently, $k = \pm 1$.

Conversely, if $k = \pm 1$, then σ^k is a $\mathcal{T}$-bijection, by Proposition 3.2.

Now, we are aiming to characterize primitive words by means of "group actions" concept. For convenience, let us recall this notion.

Let X be a non-empty set and G a group. Then *an action* of G on X is a mapping $G \times X \longrightarrow X$ which sends (g, x) to gx and satisfying the following properties:

(1) $1x = x$, for each $x \in X$ (where 1 is the unit of G).

(2) $g_1(g_2x) = (g_1g_2)x$, for each $g_1, g_2 \in G$ and $x \in X$.

If G acts on X and $Aut(X)$ denotes the set of bijections on X, then there is a homomorphism $\varphi : G \longrightarrow Aut(X)$ of groups induced by the action. Conversely, any homomorphism of groups $\varphi : G \longrightarrow Aut(X)$ induces an action of G over X. Recall that the *orbit* (resp., *stabilizer*) of an $x \in X$ under the action of G is $Gx := \{gx \mid g \in G\}$(resp., $G_x := \{g \in G \mid g.x = x\}$. It is well-known that if X is finite, then $|Gx|$ is equal to the index $[G : G_x]$ of G_x on the group G. In particular, if G is finite, then $|Gx| = [G : Gx] = \dfrac{|G|}{|G_x|}$ is a divisor of $|G|$.

Theorem 3.5 *Let A be an alphabet and $\sigma : A^* \to A^*$ be a $\mathcal{T}$-bijection. The group $(\mathbb{Z}, +)$ acts on the set of words A^* by the action $\mathbb{Z} \times A^* \longrightarrow A^*$, which sends the pair (k, u) to the word $\sigma^k(u)$. Let $u \in A^+$; we denote by $\mathcal{S}_u := \{k \in \mathbb{Z} \mid \sigma^k(u) = u\}$ the stabilizer of u under the previous action. Then the following properties hold.*

(1) *u is a primitive word if and only if $\mathcal{S}_u = |u|\mathbb{Z} := \{k|u| \mid k \in \mathbb{Z}\}$.*

(2) *$\mathcal{S}_u = \mathcal{S}_{p_A(u)} = |p_A(u)|\mathbb{Z}$.*

Proof.

(1) For the "if part", suppose that u is a primitive word and let $k \in \mathcal{S}_u$. We write the Euclidian division of k by $|u|$: there exist two integers p, r such that $k = p|u| + r$ with $0 \leq r < |u|$. Hence, $u = \sigma^k(u) = \sigma^r((\sigma^{|u|})^p(u) = \sigma^r(u)$, since $\sigma^{|u|}(u) = u$. This implies that $r = 0$, since σ is a $\mathcal{T}$-bijection. Thus, k is a multiple of $|u|$.

Now, let $k \in \mathbb{Z}$ be a multiple of $|u|$. Let us show that $\sigma^k(u) = u$. Without loss of generality, one may suppose that k is nonnegative. Hence there exists $n \in \mathbb{N}$ such that $k = n|u|$. Thus, $\sigma^k(u) = (\sigma^{|u|})^n(u)$. But, we have $\sigma^{|u|}(u) = u$. Therefore, $\sigma^k(u) = u$. It follows that $\mathcal{S}_u = |u|\mathbb{Z}$.

For the "only if part", suppose that $\mathcal{S}_u = |u|\mathbb{Z}$ and u is not a primitive word. Then, there exist $z \in A^+$ and $n \geq 2$ such that $u = z^n$. By the properties of σ, we have $\sigma^{|z|}(u) = \sigma^{|z|}(z^n) = (\sigma^{|z|}(z))^n = z^n = u$. But, $|z|$ is not a multiple of $|u|$, against our hypothesis. We conclude that u is a primitive word.

(2) According to (1), it suffices to show that $\mathcal{S}_u = \mathcal{S}_{p_A(u)}$.

Indeed, let $k \in \mathcal{S}_u$ and e be the exponent of u. Then $u = (p_{_A}(u))^e$. As $\sigma^k(u) = u$, then we get $(\sigma^k(p_{_A}(u)))^e = (p_{_A}(u))^e$. But, $c_{_A}^k(p_{_A}(u))$ is primitive as a conjugate of a primitive word (see Proposition 2.8). Now, applying Lemma 2.3 to the word $u = (\sigma^k(p_{_A}(u)))^e = (p_{_A}(u))^e$, we deduce that $\sigma^k(p_{_A}(u)) = p_{_A}(u)$. This shows that $k \in \mathcal{S}_{p_{_A}(u)}$.

Conversely, it is clear that $\mathcal{S}_v \subseteq \mathcal{S}_{v^n}$, for each integer n and each word v.

We have, thus, checked the equality $\mathcal{S}_u = \mathcal{S}_{p_{_A}(u)}$.

As a direct consequence of Theorem 3.5, one may calculate the cardinality of the the σ-necklace of a word.

Proposition 3.6 *Let A be an alphabet and $\sigma : A^* \to A^*$ be a $\mathcal{T}$-bijection. Let u be a word of length n over A and e be the exponent of u. Then the cardinality of the σ-necklace of u is equal to $\dfrac{n}{e}$.*

Proof. Let us consider the action $\mathbb{Z} \times A^* \longrightarrow A^*$, which sends the pair (k, u) to the word $\sigma^k(u)$. Then $\mathcal{C}_\sigma(u)$ is the orbit of u under the above action. Let $\mathcal{S}_u$ be stabilizer of u. Then , $|\mathcal{C}_\sigma(u)|$ is the index of the subgroup $\mathcal{S}_u$ of $\mathbb{Z}$. Now, applying Theorem 3.5, $\mathcal{S}_u = |p_{_A}(u)|\mathbb{Z} = \dfrac{n}{e}\mathbb{Z}$; and thus

$$|\mathcal{C}_\sigma(u)| = [\mathbb{Z} : \frac{n}{e}\mathbb{Z}] = \frac{n}{e}.$$

Remark 3.7 *Let $\sigma : A^* \to A^*$ be a degree preserving bijection (a bijection such that $\sigma(A^n) = A^n$). Then σ is a $\mathcal{T}$-bijection if and only if it satisfies the following properties:*

(*a*) *For each $n \in \mathbb{N} \setminus \{0\}$, the restriction of σ to the set of primitive words of size n is a bijection from the set to itself.*

(*b*) *The σ-conjugacy class of a primitive word of size n contains exactly n words.*

(*c*) *σ is power preserving.*

In Proposition 3.2, we have mentioned that the right circular shift $c_{_A}$ and the left circular shift $c_{_A}^{-1}$ are $\mathcal{T}$-bijections. The above remark allows us to construct $\mathcal{T}$-bijections distinct from $c_{_A}$ and $c_{_A}^{-1}$.

Example 3.8 *It suffices to construct bijections from the set of primitive words to itself verifying Condition (b) of Remark 3.7 and to extend the construction using the property of power preserving. For example, if $A = \{a, b\}$, then one constructs σ as follows:*

$$\begin{array}{r}
\varepsilon \longrightarrow \varepsilon \\
\hline
a \longrightarrow a \\
b \longrightarrow b \\
\hline
ab \longrightarrow ba \longrightarrow ab \\
\hline
aab \longrightarrow abb \longrightarrow aba \longrightarrow aab \\
bba \longrightarrow baa \longrightarrow bab \longrightarrow bba \\
\hline
aaab \longrightarrow abaa \longrightarrow aaba \longrightarrow baaa \longrightarrow aaab \\
aabb \longrightarrow baab \longrightarrow bbaa \longrightarrow abba \longrightarrow aabb \\
abbb \longrightarrow bbab \longrightarrow babb \longrightarrow bbba \longrightarrow abbb \\
\hline
\vdots \\
\hline
\end{array}$$

The following result gives a condition under which a $\mathcal{T}$-bijection is exactly the circular shift.

Proposition 3.9 *Let A be an alphabet and $\sigma : A^* \to A^*$ be a $\mathcal{T}$-bijection. If for each $u \in A^*$, the words $c_{_A}(u)$ and $\sigma(u)$ commute, then σ coincides with the circular shift $c_{_A}$.*

Proof. Let $u \in A^*$. If $u = \varepsilon$, then $\sigma(u) = c_{_A}(u) = \varepsilon$. We may, thus, suppose that $u \neq \varepsilon$.

Since $c_{_A}(u)\sigma(u) = \sigma(u)c_{_A}(u)$, we get, combining Lemmas 2.2 and 2.3, $p_{_A}(c_{_A}(u)) = p_{_A}(\sigma(u))$.

We denote by e the exponent of u; then $u = (p_{_A}(u))^e$.

Thus, we have

$$\begin{aligned}
\sigma(u) &= \sigma((p_{_A}(u))^e) \\
&= (\sigma(p_{_A}(u)))^e.
\end{aligned}$$

But, by Proposition 3.2, $\sigma(p_{_A}(u)) = p_{_A}(\sigma(u))$; implying that

$$\begin{aligned}
\sigma(u) &= (p_{_A}(\sigma(u)))^e \\
&= (p_{_A}(c_{_A}(u)))^e.
\end{aligned}$$

Applying again Proposition 3.2, we have $p_{_A}(c_{_A}(u)) = c_{_A}(p_{_A}(u))$. Therefore,

$$\begin{aligned}
\sigma(u) &= (c_{_A}(p_{_A}(u)))^e \\
&= c_{_A}((p_{_A}(u))^e) \\
&= c_{_A}(u).
\end{aligned}$$

It follows that σ coincides with the circular shift $c_{_A}$.

4 Burnside's Orbit Counting Theorem

This section is devoted to enumerating the number $N_\sigma(n,k)$ of σ-conjugacy classes of words of length n over an alphabet A of size k.

Let us, first, recall Burnside's Theorem.

Burnside's counting theorem, has various eponyms including William Burnside, George Pólya, Augustin Louis Cauchy, and Ferdinand Georg Frobenius. It seems that this theorem is not due to Burnside himself (it has been quoted by Burnside in his book "On the Theory of Groups of Finite Order").

Burnside's orbit counting theorem states that if G is a finite group acting on a finite set X and r denotes the number of distinct orbits, then

$$r = \frac{1}{|G|}\sum_{g\in G}|X_g|,$$

where $X_g := \{x \in X \mid gx = x\}$.

Theorem 4.1 *Let A be an alphabet with k letters and $\sigma : A^* \to A^*$ be a $\mathcal{T}$-bijection such that $\sigma(A^n) = A^n$, for each $n \in \mathbb{N}$. Then the number of σ-necklaces of words of length n over A is*

$$N_\sigma(n,k) = N(n,k) = \frac{1}{n}\sum_{d|n} k^d \phi(\frac{n}{d}),$$

where ϕ is the Euler totient function.

Proof. Let $\sigma_n : A^n \longrightarrow A^n$ be the bijection on A^n induced by σ. According to the properties of a $\mathcal{T}$-bijection, the order of σ_n is equal to n. Consider the action of the quotient group $\mathbb{Z}/n\mathbb{Z} := \{0, 1, \cdots, n-1\}$ over the set A^n of all words in A^* of length n:

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times A^n & \longrightarrow & A^n \\ (j,w) & \longmapsto & \sigma^j(w), \end{array}$$

Let us write Burnside's formula for this action:

$$r = \frac{1}{n}\sum_{j\in\mathbb{Z}/n\mathbb{Z}} |A_j^n|,$$

where $A_j^n = \{w \in A^n \mid \sigma^j(w) = w\}$, and r is the number of distinct orbits under the action. Note that $r = N_\sigma(n,k)$.

On the other hand, we have :

$$\sum_{j\in\mathbb{Z}/n\mathbb{Z}} |A_j^n| = \sum_{d|n} \Big(\sum_{\substack{j\in\mathbb{Z}/n\mathbb{Z} \\ o(j)=d}} |A_j^n| \Big),$$

where $o(j)$ denotes the order of j in the group $\mathbb{Z}/n\mathbb{Z}$.

Now, let us prove that, if $o(j) = d$, then $|A_j^n| = |A^{\frac{n}{d}}|$. Indeed, the equality holds for $j = 0$. For $j \in \mathbb{Z}/n\mathbb{Z}\setminus\{0\}$, there exists $1 \leq l \leq d-1$ such that $j = \frac{n}{d}l$ with $\gcd(l, d) = 1$. Let $w \in A_j^n$; then $\sigma^j(w) = w$. According to Theorem 3.5, there exists $k \in \mathbb{N}$ such that $j = \frac{n}{e_{_A}(w)}k$, where $e_{_A}(w)$ is the exponent of w. But, since $\gcd(l, d) = 1$, we deduce that l divides k. It follows that there is a $t_w \in \mathbb{N}$ such that $\frac{n}{d} = t_w(\frac{n}{e_{_A}(w)})$.

Consider the mapping

$$\begin{array}{rccc} \gamma: & A_j^n & \longrightarrow & A^{\frac{n}{d}} \\ & w & \longrightarrow & (p_{_A}(w))^{t_w}, \end{array}$$

where $p_{_A}(w)$ is the primitive root of w.

Let us check that γ is bijective.

– γ *is injective.* Let $u, v \in A_j^n$ such that $\gamma(u) = \gamma(v)$. Since $p_{_A}(u)$ and $p_{_A}(v)$ are primitive words, we have, by Lemma 2.3, $p_{_A}(u) = p_{_A}(v)$ and $t_u = t_v$. This implies that $e_{_A}(u) = e_{_A}(v)$; and consequently $u = v$.

– γ *is onto.* Let $v \in A^{\frac{n}{d}}$. One may write $v = (p_{_A}(v))^t$, where t is the exponent of v. Consider the word $w := v^d = (p_{_A}(v))^{td} \in A^n$. Then, $p_{_A}(w) = p_{_A}(v)$ and $e_{_A}(w) = td$. Thus we have, $\frac{n}{d} = t\frac{n}{e_{_A}(w)}$; which implies that j is a multiple of $\frac{n}{e_{_A}(w)}$. Thus $w \in A_j^n$, by Theorem 3.5. Now, clearly $\gamma(w) = v$, and we are done.

Therefore, $|A_j^n| = |A^{\frac{n}{d}}| = k^{\frac{n}{d}}$.

Accordingly, we have

$$\begin{aligned} N_\sigma(n,k) &= \frac{1}{n}\sum_{j\in\mathbb{Z}/n\mathbb{Z}}|A_j^n| \\ &= \frac{1}{n}\Big(\sum_{d|n}\Big(\sum_{\substack{j\in\mathbb{Z}/n\mathbb{Z}\\ o(j)=d}}|A_j^n|\Big)\Big) \\ &= \frac{1}{n}\Big(\sum_{d|n}k^{\frac{n}{d}}\Big(\sum_{\substack{j\in\mathbb{Z}/n\mathbb{Z}\\ o(j)=d}}1\Big)\Big) \\ &= \frac{1}{n}\sum_{d|n}k^{\frac{n}{d}}\ \varphi(d) \\ &= N(n,k). \end{aligned}$$

Let $Pr(n, k)$ be the number of primitive words of length n on k symbols and $L(n, k)$ be the number of primitive necklaces of length n. Recall that if A is a totally ordered alphabet of size k, then a word $u \in A^+$ is said to be a

Lyndon word if it is primitive and $u \leq_l v$, for each $v \in \mathcal{C}_u$, where $\leq_l$ is the lexicographic order. Thus $L(n,k)$ is the number of Lyndon words of length n. Lyndon words have been introduced and studied in [1]; they have important applications in the theory of free Lie algebras, combinatorics on words and even in Cryptology (see for example [13], [1], [15], and [4]).

In [5], Lijun has counted the number $Pr(n,k)$ by using an inclusion/exclusion argument. Let us note that this count is usually performed by using Möbius transformations.

The following result is well-known (see, for instance [2] and [6]).

For convenience, we will include its proof.

Proposition 4.2 *We have the following formulas.*

(1) $Pr(n,k) = nL(n,k)$.

(2) $k^n = \sum_{d|n} Pr(d,k)$.

(3) $L(n,k) = \frac{1}{n}\sum_{d|n} k^d \mu(\frac{n}{d})$.

Proof. (1) This may be proved easily. Indeed, if u is a primitive word of length n, then $|\mathcal{C}_u| = n$ (by Proposition 3.6) and the elements of $\mathcal{C}_u$ are primitive words (by Proposition 2.8). Thus, the primitive necklaces of length n constitute a partition of the set of primitive words of length n. This establishes the formula $nL(n,k) = Pr(n,k)$.

Burnside's counting orbit theorem may be also used to give an alternative proof of the above fact.

Indeed, the quotient group $\mathbb{Z}/n\mathbb{Z}$ acts on the set $X := Prim(A^n)$ of primitive words of length n over the alphabet A of size k under the action

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times X & \longrightarrow & X \\ (j,w) & \longmapsto & c_{A}^{j}(w), \end{array}$$

Let us write Burnside's formula for this action:

$$nL(n,k) = \sum_{j \in \mathbb{Z}/n\mathbb{Z}} |X_j|,$$

where $X_j = \{u \in Prim(A^n) \mid c_{A}^{j}(u) = u\}$. But, by Theorem 3.5(1), $X_j = \emptyset$ for $j \in \{1, \cdots, n-1\}$, and $X_0 = Prim(A^n)$. Thus, we have $Pr(n,k) = nL(n,k)$.

(2) The mapping $\Phi : A^n \longrightarrow \bigcup_{d|n} Prim(A^d) \times \{d\}$ defined by $\Phi(u) = (p_{A}(u), \frac{n}{e_{A}(u)})$ is clearly a bijection. Consequently, we have

$$|A^n| = \sum_{d|n} |Prim(A^d)|.$$

We deduce that

$$k^n = \sum_{d|n} Pr(d, k).$$

(3) According to (2) and applying Möbius inversion formula, we have

$$Pr(n, k) = \sum_{d|n} k^d \mu(\frac{X}{n} d).$$

References

[1] K.T. Chen, R. H. Fox, and R. C. Lyndon, Free differential calculus IV, *Ann. Math.* **68** (1958) 81–95.

[2] C. Choffrut, J. Karhumäki, *Combinatorics of words* (in Handbook of formal languages), Vol.1 329–438, Springer, Berlin, 1997.

[3] R. L. Graham, D. E. Knuth, O. Pataschnik, *Concrete Mathematics*, Addison Wesley, 1988.

[4] M. Hazewinkel, The algebra of quasi-symmetric functions is free over the integers, *Adv. Math.*, **164** (2001) 283–300.

[5] W. Lijun, Count of primitive words, *Appl. Math, J. Chinese Univ. Ser. B* **16** (2001) 339–344.

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

[7] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its Applications, 90. Cambridge University Press, Cambridge, 2002.

[8] E.Lucas, Théorie des Nombres, Gauthier-Villars, 1891, reprinted by Albert Blanchard, 1961.

[9] R. C. Lyndon, M.P. Schützenberger, The equation $a^M = b^N c^P$ in a free group, *Michigan Math. J.* **9** (1962) 289–298.

[10] P. A. MacMahon, Application of a theory of permutations in circular procession to the theory of numbers, *Proc. London Math. Soc.* **23** (1892) 305–313.

[11] W. Magnus, A. Karass, Donald Solitar, Combinatorial Group Theory: presentation of groups in terms of generators and relations, Dover, 1966.

[12] H. Petersen, On the language of primitive words, *Theoret. Comput. Sci.* **161** (1996) 141–156.

[13] C. Reutenauer, Free Lie Algebras, Oxford Univ. Press (1993).

[14] H. J. Shyr and G. Thiemin, Disjunctive languages and codes, in: Proc. FC777, Lecture Notes in Computer Science, Vol. 56, (Springer, Berlin, 1977) 171–176.

[15] R. Siromoney, L. Mathew, A public key cryptosystem based on Lyndon words, *Information Processing Letters* **35** (1990) 33–36.

[16] E. Witt, Treue Darstellung Lieschen Ringe, *J. Reine Angew. Math.* **177** (1937) 152–160.

Received: November, 2009