CHAPTER 4

Sesquipowers

4.0. Introduction

In this chapter we shall be concerned with *sesquipowers*. Any nonempty word is a sesquipower of *order* 1. A word w is a sesquipower of order n if $w = uvu$, where u is a sesquipower of order $n-1$. Sesquipowers have many interesting combinatorial properties which have applications in various domains. They can be defined by using *bi-ideal sequences*.

A finite or infinite sequence of words $f_1, \ldots, f_n, \ldots$ is called a bi-ideal sequence if for all $i > 0$, f_i is both a prefix and a suffix of f_{i+1} and, moreover, $2|f_i| \leq |f_{i+1}|$. A sesquipower of order n is then the nth term of a bi-ideal sequence. Bi-ideal sequences have been considered, with different names, by several authors in algebra and combinatorics (see Notes).

In Sections 4.2 and 4.3 we analyze some interesting combinatorial properties of bi-ideal sequences and the links existing between bi-ideal sequences, recurrence and n-divisions. From these results we will obtain in Section 4.4 an improvement (Theorem 4.4.5) of an important combinatorial theorem of Shirshov. We recall (see Lothaire 1983) that Shirshov's theorem states that for all positive integers p and n any sufficiently large word over a finite totally ordered alphabet will have a factor f which is a pth power or is n-*divided*, i.e., f can be factorized in nonempty blocks as $f = x_1 \cdots x_n$ with the property that all the words that one obtains by a nontrivial rearrangement of the blocks are lexicographically less than f.

In Theorem 4.4.5, we link bi-ideal sequences and the Shirshov property. Indeed, in this case the n-divided factor f is the nth term of a bi-ideal sequence whose canonical factorization $(x_1, \ldots, x_n)$ is an n-division of f. Moreover, $x_1, \ldots, x_n$ are Lyndon words such that $x_1 > x_2 > \cdots > x_n$.

In Section 4.5 some applications of bi-ideal sequences to finiteness conditions for finitely generated semigroups will be given. These conditions are based on different concepts such as permutation properties, iteration conditions, and minimal conditions on principal bi-ideals.

4.1. Bi-ideal sequences

A sequence $f_1, \ldots, f_n, \ldots$ of words of A^* is called a *bi-ideal sequence* if $f_1 \in A^+$ and for all $i > 0$

$$f_{i+1} \in f_i A^* f_i.$$

If the sequence is of finite length n, then $(f_1, \ldots, f_n)$ is called a bi-ideal sequence of *order* n. If $f_1, \ldots, f_n, \ldots$ is a bi-ideal sequence, then there exists a unique sequence of words $g_1, g_2, \ldots, g_n, \ldots$ such that for all $i > 0$

$$f_{i+1} = f_i g_i f_i.$$

Thus a bi-ideal sequence is any sequence of words $f_1, \ldots, f_n, \ldots$ satisfying the following requirements: for all $i > 0$

(i) f_i is both a prefix and a suffix of f_{i+1},

(ii) $2|f_i| \leq |f_{i+1}|$.

If $(f_1, \ldots, f_n)$ is a bi-ideal sequence of order n, then the last term $f = f_n$ will be called a *sesquipower of order* n. Obviously, any sesquipower of order n is also a sesquipower of order k for all $k = 1, \ldots, n-1$. Thus with any word $f \in A^+$ one can associate a positive integer, called *degree* of f, defined as the maximal order of any bi-ideal sequence having f as last term. However, in general, for a given word $f \in A^+$ there can exist different bi-ideal sequences of order equal to the degree of f and having f as last term. For instance, the word $f = abababababa$ of degree 3 is the last term of the two bi-ideal sequences (a, aba, f) and $(a, ababa, f)$.

Example 4.1.1. Recall that the *Fibonacci word* (see Chapter 1 and Chapter 8)

$$f = abaababaabaababaababaabaababaabaab \cdots$$

is the limit of the sequence of words $(f_n)_{n \geq 0}$, inductively defined by $f_0 = b$, $f_1 = a$, $f_{n+1} = f_n f_{n-1}$, for all $n > 0$. The sequences $(f_{2k})_{k \geq 1}$ and $(f_{2k+1})_{k \geq 0}$ of the terms of even and odd index, respectively, are infinite bi-ideal sequences (converging to f). Indeed, one has

$$f_2 = ab \text{ and } f_{2k} = f_{2k-2} f_{2k-3} f_{2k-2}, \; k > 1,$$

and

$$f_1 = a \text{ and } f_{2k+1} = f_{2k-1} f_{2k-2} f_{2k-1}, \; k \geq 1.$$

Bi-ideal sequences are closely related to Zimin's words, as defined in Chapter 3. Let $X = \{x_1, \ldots, x_n, \ldots\}$ be a possibly infinite alphabet, called *pattern alphabet* and Z_n, $n > 0$, be the sequence of words, inductively defined as:

$$Z_1 = x_1, \; Z_{n+1} = Z_n x_{n+1} Z_n \text{ for } n > 0.$$

Thus one has

$$Z_2 = x_1 x_2 x_1, \; Z_3 = x_1 x_2 x_1 x_3 x_1 x_2 x_1, \; \ldots.$$

Let $\phi : X^* \to A^*$ be any nonerasing morphism from X^* to A^*. One easily verifies that the sequence $(\phi(Z_n))_{n>0}$ is a bi-ideal sequence. Conversely, if $f_1, \ldots, f_n, \ldots$ is a bi-ideal sequence with $f_{n+1} = f_n g_n f_n$, and $\phi : X^* \to A^*$ is the morphism defined as:

$$\phi(x_1) = f_1,\ \phi(x_{n+1}) = g_n, \quad \text{for } n > 0,$$

then

$$f_n = \phi(Z_n)$$

for all $n > 0$. The following theorem, which shows that for all $n > 0$ the pattern Z_n is unavoidable is Proposition 3.1.4.

THEOREM 4.1.2. *Let A be a k-letter alphabet. For any $n > 0$, there exists a positive integer $M(k, n)$, such that any word of A^* of length at least $M(k, n)$ contains as a factor a sesquipower of order n.* ∎

4.2. Canonical factorizations

In this section we investigate some interesting combinatorial properties of bi-ideal sequences which will be useful later in order to prove some extensions of a theorem of Shirshov.

Let n be a positive integer and $(w_1, \ldots, w_n)$ be a sequence of n words of A^+. The sequence $(w_1, \ldots, w_n)$ is called an *n-sequence* if for any $i = 1, \ldots, n-1$

$$w_i \in w_{i+1} \cdots w_n A^*.$$

The sequence $(w_1, \ldots, w_n)$ is called *inverse n-sequence* if

$$w_{i+1} \in A^* w_1 \cdots w_i,$$

for any $i = 1, \ldots, n-1$.

We analyze now an important relationship between bi-ideal sequences of order n and n-sequences (inverse n-sequences). From this one derives two canonical factorizations of the last term of any bi-ideal sequence of order n.

Let $(f_i)_{i=1,\ldots,n}$ be a bi-ideal sequence of order n with $f_1 \in A^+$ and set $f_{i+1} = f_i g_i f_i$, with $g_i \in A^*$ for $i = 1, \ldots, n-1$. Let $w_n = f_1$ and

$$w_{n-i} = f_i g_i, \quad 1 \le i \le n-1.$$

One has $f_{i+1} = f_i g_i f_i = w_{n-i} f_i$ for $1 \le i \le n-1$, so that, by iteration, one has

$$f_{i+1} = w_{n-i} \cdots w_n, \quad 0 \le i \le n-1. \tag{4.2.1}$$

Moreover, since $w_i = f_{n-i} g_{n-i}$ for $1 \le i \le n-1$, Eq.(4.2.1) implies

$$w_i = w_{i+1} \cdots w_n g_{n-i} \in w_{i+1} \cdots w_n A^*. \tag{4.2.2}$$

It follows from Eq.(4.2.1) that $f_n = w_1 w_2 \cdots w_n$. The n-tuple $(w_1, w_2, \ldots, w_n)$ is called the *canonical factorization* of f_n.

One can also introduce the inverse canonical factorization of f_n by setting $w'_1 = f_1$ and

$$w'_{i+1} = g_i f_i, \quad 1 \leq i \leq n-1.$$

One easily derives that for all $i = 1, \ldots, n$

$$w'_1 \cdots w'_i = f_i, \tag{4.2.3}$$

where

$$w'_{i+1} = g_i w'_1 \cdots w'_i \in A^* w'_1 \cdots w'_i, \quad 1 \leq i \leq n-1. \tag{4.2.4}$$

It follows from Eq.(4.2.3) that $f_n = w'_1 \cdots w'_n$. The n-tuple $(w'_1, \ldots, w'_n)$ is called the *inverse canonical factorization* of f_n.

By Eqs (4.2.2) and (4.2.4), the canonical (inverse canonical) factorization of the last term of a bi-ideal sequence of order n is an n-sequence (inverse n-sequence).

Conversely, one easily verifies that if $(w_1, w_2, \ldots, w_n)$ is an n-sequence (inverse n-sequence), then the sequence of words $f_i = w_{n-i+1} \cdots w_n$ ($f_i = w_1 \cdots w_i$), $1 \leq i \leq n$, is a bi-ideal sequence of order n whose last term has a canonical (inverse canonical) factorization given by $(w_1, w_2, \ldots, w_n)$.

Example 4.2.1. Consider the bi-ideal sequence of order 3, $f_1 = a$, $f_2 = aba$ and $f_3 = ababaaba$. In this case $g_1 = b$ and $g_2 = ba$. The canonical factorization of f_3 is the 3-sequence $(ababa, ab, a)$. The inverse canonical factorization is the inverse 3-sequence $(a, ba, baaba)$.

Let us remark that although a sesquipower f of order n may have several canonical factorizations, these are uniquely determined by the bi-ideal sequences of order n having f as last term. As an example, the word $f = abababababa$ is the last term of the two bi-ideal sequences of order 3

$$(a, aba, f) \text{ and } (a, ababa, f).$$

Thus f has the two canonical factorizations

$$(abababab, ab, a) \text{ and } (ababab, abab, a)$$

which uniquely correspond to the preceding bi-ideal sequences.

The following proposition, called *reciprocity law*, summarizes the links existing between the two canonical factorizations of the last term of a bi-ideal sequence of order n, expressed by Eqs (4.2.1) and (4.2.3).

Proposition 4.2.2. *Let $(w_1, \ldots, w_n)$ and $(w'_1, \ldots, w'_n)$ be the canonical factorizations of the nth term f_n of a bi-ideal sequence. For any $i = 0 \ldots, n-1$ one has*

$$w'_1 \cdots w'_{i+1} = f_{i+1} = w_{n-i} \cdots w_n \,. \qquad \blacksquare$$

We denote by $\mathcal{S}_n$ the symmetric group on $\{1,\ldots,n\}$. Let $<$ be a total order in A^*. A sequence $(u_1, u_2, \ldots, u_n)$ of n words of A^+ is called an *n-division* (with respect to the order $<$) if for any nontrivial permutation σ of $\mathcal{S}_n$ one has

$$u_{\sigma(1)} u_{\sigma(2)} \cdots u_{\sigma(n)} < u_1 u_2 \cdots u_n.$$

A word u is called *n-divided* (with respect to the order $<$) if there exists an n-division $(u_1, u_2, \ldots, u_n)$ such that $u = u_1 u_2 \cdots u_n$.

An n-division $(u_1, u_2, \ldots, u_n)$ with respect to the relation $>$, which is the inverse of $<$, is also called *inverse n-division* with respect to the order $<$. A word which is n-divided with respect to $>$ is also called *inversely n-divided* with respect to $<$.

In the following we shall consider n-divisions (inverse n-divisions) and n-divided (inversely n-divided) words only with respect to the lexicographic order, so that the above terms will be used without specifying the total order. We shall denote, when there are no ambiguities, the lexicographic order on A^* simply by $<_A$ or $<$.

EXAMPLE 4.2.3. Let the alphabet $A = \{a, b\}$ be ordered by $a < b$. The word $w = ababbaba$ is 3-divided by the sequence $(ababb, ab, a)$ and inversely 3-divided by $(a, ba, bbaba)$. Moreover, one can easily verify that $(ababb, ab, a)$ is the only 3-division of w and that w does not admits 4-divisions.

We recall the two following basic properties of the lexicographic order (Lothaire 1983).

PROPOSITION 4.2.4. *For all u, v, w, w' in A^**

1. $u < v \iff wu < wv$,
2. *if $v \notin uA^*$, then $u < v \Rightarrow uw < vw'$.* ∎

The following proposition characterizes n-divisions.

PROPOSITION 4.2.5. *An n-sequence $(w_1, \ldots, w_n)$ is an n-division (inverse n-division) if and only if for all $i = 1, \ldots, n-1$, one has $w_{i+1} w_i < w_i w_{i+1}$ ($w_{i+1} w_i > w_i w_{i+1}$).*

Proof. ($\Rightarrow$) Suppose that the n-sequence $(w_1, \ldots, w_n)$ is an n-division and let us prove that $w_{i+1} w_i < w_i w_{i+1}$ for $1 \le i \le n-1$. Assume, by contradiction, that $w_{i+1} w_i \ge w_i w_{i+1}$ for some integer i, $1 \le i \le n-1$. This implies, by Proposition 4.2.4(1), that $w_1 \cdots w_{i-1} w_i w_{i+1} \le w_1 \cdots w_{i-1} w_{i+1} w_i$. If $w_i w_{i+1} = w_{i+1} w_i$, then

$$w_1 \cdots w_{i-1} w_i w_{i+1} w_{i+2} \cdots w_n = w_1 \cdots w_{i-1} w_{i+1} w_i w_{i+2} \cdots w_n,$$

which is a contradiction. Let us then suppose $w_i w_{i+1} < w_{i+1} w_i$. Since $|w_i w_{i+1}| = |w_{i+1} w_i|$, it follows by property 4.2.4(2) of the lexicographic order that

$$w_1 \cdots w_{i-1} w_i w_{i+1} w_{i+2} \cdots w_n < w_1 \cdots w_{i-1} w_{i+1} w_i w_{i+2} \cdots w_n$$

which is again a contradiction.

($\Leftarrow$) We begin by proving that $w_j w_i < w_i w_j$ for any i, j with $1 \leq i < j \leq n$. If $i = j - 1$ the result follows from the hypotheses. Then let us suppose that $i < j - 1$. We can write

$$w_i \in w_{j-1} w_j \cdots w_n A^*$$

and

$$w_i w_j = w_{j-1} w_j \mu, \text{ for some } \mu \in A^*.$$

By assumption, one has

$$w_j w_{j-1} < w_{j-1} w_j .$$

Since $i \leq j - 2$, we can write

$$w_i = w_{j-1} \lambda, \text{ for some } \lambda \in A^*.$$

Since $|w_j w_{j-1}| = |w_{j-1} w_j|$ and $w_j w_{j-1} < w_{j-1} w_j$, in view of the property 4.2.4(2) of the lexicographic ordering, one has

$$w_j w_i = w_j w_{j-1} \lambda < w_{j-1} w_j \mu = w_i w_j.$$

Any permutation can be obtained by a sequence of exchanges of adjacent elements. Thus, the above property shows that for any nontrivial permutation $\sigma \in \mathcal{S}_n$ one has $w_{\sigma(1)} w_{\sigma(2)} \cdots w_{\sigma(n)} < w_1 w_2 \cdots w_n$. The proof in the case of the inverse n-division is perfectly symmetric. ■

By an argument similar to that of the preceding proposition, one can prove the following

Proposition 4.2.6. *An inverse n-sequence $(w_1, \ldots, w_n)$ is an n-division (inverse n-division) if and only if for all i, $1 \leq i \leq n - 1$, $w_{i+1} w_i < w_i w_{i+1}$ $(w_{i+1} w_i > w_i w_{i+1})$.*

4.3. Sesquipowers and recurrence

Let $f_1, \ldots, f_n, \ldots$ be an infinite bi-ideal sequence, where $f_{i+1} = f_i g_i f_i$ for all $i > 0$. Since for all $i > 0$, f_i is prefix of the next term f_{i+1} the sequence (f_n) converges to the infinite word

$$x = f_1 (g_1 f_1)(g_2 f_2) \cdots (g_n f_n) \cdots .$$

Let us observe that one can rewrite x as

$$x = w_1 w_2 \cdots w_n \cdots ,$$

where $w_1 = f_1$, $w_{i+1} = g_i f_i$, $i > 0$. For all $n > 0$, $(w_1, \ldots, w_n)$ is the inverse canonical factorization of f_n.

A word $x \in A^\omega$ is a *sesquipower* if it is the limit of a bi-ideal sequence.

PROPOSITION 4.3.1. *A word $x \in A^\omega$ is recurrent if and only if it is a sesquipower.*

Proof. Let $x \in A^\omega$ be recurrent. We construct, inductively, a bi-ideal sequence $(f_n)_{n>0}$ such that f_n is a prefix of x, for any $n > 0$. We set $f_1 = x_1$. Suppose, by induction, that we have constructed the bi-ideal sequence up to the ith element f_i, with $i > 0$. Since f_i is a prefix of x and x is recurrent, f_i will occur in x infinitely many times, so that there will exist a word $g \in A^*$ such that $f_{i+1} = f_i g f_i$ is still a prefix of x. Thus there exists a bi-ideal sequence $(f_n)_{n>0}$ whose elements are prefixes of x. This implies that $x = \lim_{n\to\infty} f_n$, i.e., x is a sesquipower.

Conversely, let $x \in A^\omega$ be a sesquipower, i.e., $x = \lim_{n\to\infty} f_n$, where (f_n) is a bi-ideal sequence. Let $w \in F(x)$. There exists $\lambda \in A^*$ such that λw is a prefix of x. Thus $w \in F(f_k)$ for a suitable positive integer k. Now for any $p > 0$, f_k will occur at least 2^p times in f_{k+p}. This shows that the number of occurrences of w in x has not an upper bound. ∎

Recall from Chapter 1, that a word $w \in A^\omega$ is eventually periodic if there exist words $u \in A^*$ and $v \in A^+$ such that $w = uv^\omega$. The following proposition is straightforward and is left as an exercise (see Problem 4.3.1).

PROPOSITION 4.3.2. *Let $w \in A^\omega$ be an eventually periodic word. If w is recurrent, then w is periodic.*

Uniformly recurrent words are sesquipowers which have a special interest since any factor of them occurs an infinite number of times but with bounded gaps (cf. Section 1.5.2). Moreover, as shown in Proposition 1.5.12, for any infinite set $L \subseteq A^*$ there exists a uniformly recurrent word $x \in A^\zeta$ such that $F(x) \subseteq F(L)$.

For a uniformly recurrent word w, we denote by r_w the *recurrence index* of w. We recall that for any $n > 0$ each factor u of w of length n will occur in any factor of w of length $r_w(n)$.

When a word is uniformly recurrent one can 'localize' in any sufficiently large factor of it (whose length depends on the recurrence index) the occurrence of a sesquipower of any order.

PROPOSITION 4.3.3. *Let $t \in A^\omega$ be a uniformly recurrent word. For any $n > 0$ there exists a positive integer $D(n)$ such that for any $w \in A^*$, $a \in A$, with $wa \in F(t)$ and $|w| \geq D(n)$ one has that*

$$w = \lambda f_n,$$

where $\lambda \in A^*$, and f_n is the nth term of a bi-ideal sequence $f_{i+1} = f_i g_i f_i$, with $g_i \in aA^*$, $i = 1, \ldots, n-1$, $f_1 \in aA^*$ and $|f_i| \leq D(i)$ for $i = 1, \ldots, n$.

Proof. The proof is by induction on n. For $n = 1$ we set $D(1) = r_t(1)$, where r_t is the recurrence index of the word t. Let $w \in A^*$, $|w| \geq D(1)$ and $wa \in F(t)$. Then in w the letter a has to occur, so that we can factorize w as $w = xay$

with $x, y \in A^*$ and $|ay| \leq D(1)$. The statement follows if we set $f_1 = ay$. Now let $n > 1$. By induction we may suppose that there exists an integer $D(n-1)$ satisfying the statement for $n-1$. Then we set

$$D(n) = r_t(D(n-1)+1) + D(n-1).$$

Let $w \in A^*$, $a \in A$ such that $|w| \geq D(n)$ and $wa \in F(t)$. We can write $w = xv$, with $|x| \geq r_t(D(n-1)+1)$ and $|v| = D(n-1)$. Since $va \in F(t)$, by the induction hypothesis one has

$$v = \lambda' f_{n-1},$$

with $\lambda' \in A^*$, and f_{n-1} is the $(n-1)$th term of a bi-ideal sequence $f_{i+1} = f_i g_i f_i$, with $f_1 \in aA^*$, $g_i \in aA^*$, $i \in \{1, \ldots, n-2\}$ and $|f_i| \leq D(i)$ for $i \in \{1, \ldots, n-1\}$. By the properties of the recurrence index r_t, one has that x contains va as a factor and then also $f_{n-1}a$. Hence one can write $x = \lambda f_{n-1} a \mu$, with $\lambda, \mu \in A^*$, so that

$$w = \lambda f_{n-1} a \mu \lambda' f_{n-1} .$$

Therefore, if we set $g_{n-1} = a\mu\lambda'$, one has $f_n = f_{n-1} g_{n-1} f_{n-1}$ with $g_{n-1} \in aA^*$. Since $|f_{n-1} a \mu| \leq r_t(D(n-1)+1)$ and $|\lambda' f_{n-1}| = D(n-1)$ it follows that $|f_n| \leq D(n)$. ∎

Let p be a positive integer. A finite or infinite word w is called *p-power-free* if it does not have a factor of the form u^p with $u \neq \varepsilon$. An infinite word w is called *ω-power-free* if for any $u \in F(w)$, $u \neq \epsilon$, there exists an integer p such that $u^p \notin F(w)$.

It is clear that a finite word which is 2-power-free (i.e., square-free) is primitive, whereas the converse is not, generally, true. If a word is p-power-free, then it is also ω-power-free. However, there exist infinite words which are ω-power-free even though for any $p > 1$ they have a factor which is a p-power (see Problem 4.3.2). The following lemma shows that a uniformly recurrent word $w \in A^\omega$ is ω-power-free if and only if it is not periodic.

LEMMA 4.3.4. *A uniformly recurrent word $w \in A^\omega$ is either periodic or ω-power-free.*

Proof. Suppose by contradiction that $w \in A^\omega$ is a uniformly recurrent word which is neither periodic nor ω-power-free. Hence, there exists a word $u \in A^+$, that one can always take to be primitive, such that for all $n > 0$, $u^n \in F(w)$. Let us now consider an occurrence of u in w. This is determined by a word $\lambda \in A^*$ such that λu is a prefix of w. Since, by Proposition 4.3.2, w is not eventually periodic, there exists $n > 0$ and $v \in A^+$ such that $|v| = |u|$, $v \neq u$ and $\lambda u^n v$ is still a prefix of w. Let $m > 0$ be such that $|u^m| > r_w((n+1)|u|)$, where r_w is the recurrence index of w. Hence, u^m has as a factor the word $u^n v$. Since u is primitive and $|u| = |v|$, one easily derives $u = v$ which is a contradiction. ∎

4.4. Extensions of a theorem of Shirshov

In this section we prove (Theorem 4.4.4) that an ω-power-free one-sided infinite word has a factor which is the last term of a bi-ideal sequence of any order n whose canonical factorization is an n-division. We need to recall some properties and prove some lemmas on Lyndon words.

The set of all Lyndon words on the alphabet A will be denoted by $\mathcal{L}_A$, or simply $\mathcal{L}$ when there is no confusion. For $A = \{a, b\}$ and $a < b$, a list of Lyndon words of increasing length is

$$a, b, ab, aab, abb, aaab, aabb, abbb, aaaab, aaabb, aabab, \ldots.$$

The following proposition (Lothaire 1983) gives an equivalent definition of Lyndon words.

PROPOSITION 4.4.1. *A nonempty word w is a Lyndon word if and only if it is strictly less than any of its proper nonempty suffixes.*

Let A be a finite totally ordered alphabet, let $a = \min(A)$ and denote by $<_A$ the lexicographic order on A^*. The set

$$Y = a^+(A \setminus \{a\})^+$$

is a code on the alphabet A (see Chapter 1). Let X be a finite subset of Y and B be an alphabet such that $\mathrm{Card}(B) = \mathrm{Card}(X)$. If δ is a bijection of B and X, then it can be extended to a injective morphism $\delta : B^* \to Y^*$. We can then totally order B by setting for $x, y \in B$

$$x <_B y \Longleftrightarrow \delta(x) <_A \delta(y). \tag{4.4.1}$$

The total order of B can be extended to the lexicographic order $<_B$ of B^*.

LEMMA 4.4.2. *For $u, v \in B^*$, one has $u <_B v \Rightarrow \delta(u) <_A \delta(v)$.*

Proof. Suppose first that u is a left factor of v, i.e., $v = u\xi$ with $\xi \in B^*$. One has then $\delta(v) = \delta(u)\delta(\xi)$, i.e., $\delta(u)$ is a prefix of $\delta(v)$, so that $\delta(u) <_A \delta(v)$. Let us then suppose that

$$u = hx\xi, \; v = hy\eta,$$

with $h, \xi, \eta \in B^*$, $x, y \in B$ and $x <_B y$. From Eq.(4.4.1), $x <_B y \Rightarrow \delta(x) <_A \delta(y)$. We have to consider two cases:

Case 1. $\delta(x) = rbs$, $\delta(y) = rct$ with $r, s, t \in A^*$, $b, c \in A$ and $b < c$. One has then $\delta(u) = \delta(h)rbs\delta(\xi)$, $\delta(v) = \delta(h)rct\delta(\eta)$ and $\delta(u) <_A \delta(v)$.

Case 2. $\delta(x)$ is a proper prefix of $\delta(y)$, i.e., $\delta(y) = \delta(x)\zeta$ with $\zeta \in A^+$. Since $\delta(x), \delta(y) \in X$, one has $\delta(x) = a^h f$, $\delta(y) = a^k g$ with $h, k > 0$ and $f, g \in (A \setminus \{a\})^+$. It follows that ζ begins with a letter $b > a$. Hence, we can write $\zeta = b\zeta'$. One has then $\delta(u) = \delta(h)\delta(x)\delta(\xi)$ and $\delta(v) = \delta(h)\delta(x)b\zeta'\delta(\eta)$. Hence, if $\delta(\xi) = \epsilon$ then $\delta(u)$ is a prefix of $\delta(v)$ so that $\delta(u) <_A \delta(v)$. If, on the contrary, $\delta(\xi) \neq \epsilon$ then $\delta(\xi) \in aA^*$ and again $\delta(u) <_A \delta(v)$. ■

LEMMA 4.4.3. *If $w \in \mathcal{L}_B$, then $\delta(w) \in \mathcal{L}_A$.*

Proof. Let $w = x_1 \cdots x_n \in \mathcal{L}_B$ with $x_i \in B$ $(i = 1, \ldots, n)$. From Proposition 4.4.1 one has:

$$x_1 \cdots x_n <_B x_i \cdots x_n$$

for all $i \geq 2$. This implies by Lemma 4.4.2

$$\delta(x_1) \cdots \delta(x_n) <_A \delta(x_i) \cdots \delta(x_n). \tag{4.4.2}$$

To prove that $\delta(w) \in \mathcal{L}_B$ we have to show that for any factorization $\delta(w) = uv$ with $u \neq \epsilon$, $v \in A^+$ one has $\delta(w) <_A v$. This is the case by Eq.(4.4.2) when $v = \delta(x_i) \cdots \delta(x_n)$ for a suitable $i \geq 2$. Let us then suppose that there exist an integer i and words $\delta' \in A^+$, $\delta'' \in A^*$ such that $0 < i \leq n$ and

$$\delta(x_i) = \delta'\delta'', \ v = \delta''\delta(x_{i+1}) \cdots \delta(x_n),$$

(in the case $i = n$, $v = \delta''$). By definition $\delta(x_i) = \delta'\delta'' = a^k f$ with $k > 0$ and $f \in (A \setminus \{a\})^+$. If $|\delta'| \geq k$, then δ'' begins with a letter $b > a$, i.e., $\delta'' = b\zeta$. Thus

$$v = b\zeta\delta(x_{i+1}) \cdots \delta(x_n).$$

Since $\delta(w)$ begins with the letter a the result in this case trivially follows. Let us then suppose that $|\delta'| < k$ so that

$$v = a^{k-p} f\delta(x_{i+1}) \cdots \delta(x_n),$$

with $p > 0$. Now $a^k f <_A a^{k-p} f$, so that by $(L2)$ one derives:

$$\delta(x_i) \cdots \delta(x_n) = a^k f\delta(x_{i+1}) \cdots \delta(x_n) <_A a^{k-p} f\delta(x_{i+1}) \cdots \delta(x_n) = v.$$

Therefore,

$$\delta(x_1) \cdots \delta(x_n) <_A \delta(x_i) \cdots \delta(x_n) <_A v,$$

which concludes the proof. ∎

THEOREM 4.4.4. *Let x be an ω-power-free one-sided infinite word over a finite and totally ordered alphabet A. For any $n > 1$, x has a factor s which is the nth term of a bi-ideal sequence whose canonical factorization $(w_1, \ldots, w_n)$ is an n-division of s such that the words w_i are Lyndon words with*

$$w_1 > w_2 > \cdots > w_n.$$

Proof. We shall prove the theorem in the case of uniformly recurrent ω-power-free bi-infinite words. Indeed, by Proposition 1.5.12, one derives that for any one-sided infinite ω-power-free word x there exists a uniformly recurrent ω-power-free two-sided infinite word x' such that $F(x') \subseteq F(x)$. Thus if the assertion of the theorem holds for x', then it will hold also for x. We give now a procedure in order to find for any positive integer n a sequence of totally ordered finite alphabets Σ_i $(i = 1, \ldots, n+1)$ and a sequence of bi-infinite uniformly recurrent and ω-power-free words $x_i \in \Sigma_i^{\zeta}$, with $\Sigma_i = \mathrm{alph}\, x_i$, such that $x_1 = x$ and for any i, $2 \leq i \leq n+1$, there exists a injective morphism

$$\delta_i : \Sigma_i^* \to \Sigma_{i-1}^*,$$

with the property

$$\delta_i(x_i) = x_{i-1}.$$

The construction is given inductively. We totally order $\Sigma_1 = \mathrm{alph}\, x \subseteq A$ and extend this order to the lexicographic order of Σ_1^*. Let us suppose that we have constructed the sequence until the ith step. Then let $x_i \in \Sigma_i^{\zeta}$, where $\Sigma_i = \mathrm{alph}\, x_i$ is supposed to be totally ordered. This order can be extended to the lexicographic order $<_{\Sigma_i}$ of Σ_i^*. Let $b_i = \min(\Sigma_i)$. One can then construct the sets

$$X_i = b_i^+(\Sigma_i \setminus \{b_i\})^+$$

and

$$\Lambda_{i+1} = F(x_i) \cap X_i.$$

By induction x_i is uniformly recurrent and ω-power-free. Hence, there are not enough long subwords in x_i which are either a power of b_i or do not contain b_i as a factor, so that Λ_{i+1} is finite.

The set Λ_{i+1} is a code having a *synchronization delay* equal to 1, i.e., for any pair $(y_1, y_2) \in \Lambda_{i+1} \times \Lambda_{i+1}$ and $\alpha, \beta \in \Sigma_i^*$ one has:

$$\alpha y_1 y_2 \beta \in \Lambda_{i+1}^* \Longrightarrow \alpha y_1, \quad y_2 \beta \in \Lambda_{i+1}^*.$$

One can then consider an alphabet Σ_{i+1} with $\mathrm{Card}(\Sigma_{i+1}) = \mathrm{Card}(\Lambda_{i+1})$ and a bijection $\gamma_{i+1} : \Sigma_{i+1} \to \Lambda_{i+1}$. Let $\delta_{i+1} : \Sigma_{i+1}^* \to \Sigma_i^*$ be the morphism which extends γ_{i+1}. Since Λ_{i+1} is a code then δ_{i+1} is injective. Moreover, from the bounded synchronization delay (equal to 1) one has that x_i can be uniquely factorized in terms of the elements of Λ_{i+1}. Then there exists a bi-infinite word $x_{i+1} \in \Sigma_{i+1}^{\zeta}$ such that

$$\delta_{i+1}(x_{i+1}) = x_i.$$

Since, by the inductive hypothesis, x_i is uniformly recurrent and ω-power-free, then one derives that so will be x_{i+1}. Indeed, it is trivial that x_{i+1} is not ω-power-free. Let us prove that x_{i+1} is recurrent. In fact let $u \in F(x_{i+1})$. One has that $\delta_{i+1}(u) \in F(x_i)$. Moreover, there exists a letter $x \in \Sigma_i \setminus \{b_i\}$ such that $x\delta_{i+1}(u)b_i \in F(x_i)$. The factor $x\delta_{i+1}(u)b_i$ is recurrent in the unique factorization of x_i in terms of the elements of Λ_{i+1}. This implies that u will be recurrent in x_{i+1}. Moreover, x_{i+1} is uniformly recurrent. In fact one easily derives that for any n an upper bound to $r_{x_{i+1}}(n)$ is given by $r_{x_i}((n+2)l_M)$ where $l_M = \max\{|y| \mid y \in \Lambda_{i+1}\}$.

Now we define in Σ_{i+1} a total ordering by setting for $x, y \in \Sigma_{i+1}$:

$$x <_{\Sigma_{i+1}} y \Longleftrightarrow \delta_{i+1}(x) <_{\Sigma_i} \delta_{i+1}(y).$$

This total order of Σ_{i+1} can be extended to the lexicographic order $<_{\Sigma_{i+1}}$ of Σ_{i+1}^*. Moreover, for any $u, v \in \Sigma_{i+1}^*$ one has by Lemma 4.4.2

$$u <_{\Sigma_{i+1}} v \Longrightarrow \delta_{i+1}(u) <_{\Sigma_i} \delta_{i+1}(v).$$

Let $w_0, w_1, w_2, \ldots, w_n \in \Sigma_1^+ \subseteq A^*$ be defined as:

$$w_n = b_1 = \min(\Sigma_1),$$

and for $i = 2, \ldots, n+1$

$$w_{n-i+1} = \delta_2(\delta_3(\cdots \delta_i(b_i) \cdots))$$

with $b_i = \min(\Sigma_i)$.

We prove that $s = w_1 w_2 \cdots w_n \in F(x)$. Moreover, s is the nth term of a bi-ideal sequence whose canonical factorization is $(w_1, w_2, \ldots, w_n)$. By construction for any $i > 1$ and for any $b \in \Sigma_i$ one has

$$\delta_i(b) = b_{i-1} u_1, \quad \text{with} \quad u_1 \in \Sigma_{i-1}^+,$$

thus, applying the same relation to the first letter of u_1, we obtain

$$\delta_{i-1}(\delta_i(b)) = \delta_{i-1}(b_{i-1}) b_{i-2} u_2, \quad \text{with} \quad u_2 \in \Sigma_{i-2}^+.$$

Iterating this procedure one has

$$\delta_2(\cdots \delta_{i-1}(\delta_i(b)) \cdots) = \delta_2(\cdots \delta_{i-1}(b_{i-1}) \cdots) \cdots \delta_2(b_2) b_1 u_{i-1},$$

with $u_{i-1} \in \Sigma_1^+ \subseteq A^+$. Thus, for $b = b_i$, we obtain for any i, $2 \le i \le n+1$,

$$w_{n-i+1} = w_{n-i+2} \cdots w_n u_{i-1}. \tag{4.4.3}$$

Thus, in particular, one has:

$$w_0 = w_1 \cdots w_n u_n.$$

Since $w_0 \in F(x)$ then $s = w_1 \cdots w_n \in F(x)$. Moreover, Eq.(4.4.3) implies that $(w_1, w_2, \ldots, w_n)$ is an n-sequence, so that $s = w_1 \cdots w_n$ is the last term of a bi-ideal sequence of order n whose canonical factorization is $(w_1, \ldots, w_n)$.

Let us denote by $\mathcal{L}_i$ the set of the Lyndon words on the alphabet Σ_i. For each $i = 2, \ldots, n$ the word $b_i = \min(\Sigma_i)$ is a Lyndon word on the alphabet Σ_i. Moreover, by Lemma 4.4.3 the injective morphism δ_i preserves Lyndon words. Thus, $\delta_i(b_i) \in \mathcal{L}_{i-1}$ and

$$w_{n-i+1} = \delta_2(\delta_3(\cdots \delta_i(b_i) \cdots)) \in \mathcal{L}_1.$$

All the words w_i, $(i = 1, \ldots, n)$ are then Lyndon on the alphabet A. Moreover, since from Eq.(4.4.3) w_{n-i+2} is a proper prefix of w_{n-i+1}, one has:

$$w_1 > w_2 > \cdots > w_n.$$

From this one easily derives (see Problem 4.4.1) that $(w_1, \ldots, w_n)$ is an n-division and this concludes the proof. ∎

As a consequence of the preceding proposition we give the following theorem.

THEOREM 4.4.5. *For all k, p, n positive integers there exists a positive integer $N(k, p, n)$ such that for any totally ordered alphabet A of cardinality k any word $w \in A^*$ whose length is at least $N(k, p, n)$ is such that*
(i) *there exists $u \neq \epsilon$ such that $u^p \in F(w)$ or*
(ii) *there exists $s \in F(w)$ which is the nth term of a bi-ideal sequence whose canonical factorization $(w_1, \ldots, w_n)$ is an n-division of s. Moreover, the words w_i, $i = 1, \ldots, n$, are Lyndon words such that*

$$w_1 > w_2 > \cdots > w_n.$$

Proof. Let A be a totally ordered alphabet of cardinality k. The set of all words of A^* which satisfy either (i) or (ii) is a two-sided ideal $J_{k,n,p}$, or simply J, of A^*. Let $C = A^* \setminus J$. The set C is closed by factors, so that if we suppose that C is infinite, then by König's lemma (Proposition 1.2.3) there exists a one-sided infinite word $x \in A^\omega$ such that $F(x) \subseteq C$. Now either x has a factor which is a p-power and then $F(x) \cap J \neq \emptyset$ or x is p-power-free. In this cas,e it follows from Theorem 4.4.4 that again $F(x) \cap J \neq \emptyset$. Hence, in both the cases we reach a contradiction. Thus C is finite and this proves the assertion. ■

4.5. Finiteness conditions for semigroups

Let S be a semigroup. One can naturally embed S in a monoid S^1 as follows. If S is a monoid, then $S^1 = S$. If S has no identity, then S^1 is obtained from S by adjoining an extra element 1 satisfying the property $s1 = 1s = s$ for all $s \in S^1$.

If $s, t \in S$ we say that s is a *factor* of t if $t \in S^1 s S^1$. If $t \in sS^1$ ($t \in S^1 s$) then s is called *left factor* (*right factor*) of t. For any $t \in S$ we denote by $F(t)$ the set of the factors of t. For any subset X of S, $F(X) = \cup_{t \in X} F(t)$. One says that X is *factorial* or *closed by factors* if $F(X) = X$.

A semigroup (group) S is *finitely generated* if there exists a finite subset X of S such that the subsemigroup (subgroup) $\langle X \rangle$ generated by X is S. A semigroup (group) S is called *locally finite* if every finitely generated subsemigroup (subgroup) of S is finite.

When a semigroup S is finitely generated by a set X, one can introduce an alphabet A having the same cardinality of X. As is well known any bijection $\delta : A \to X$ can be extended in a unique surjective morphism

$$\phi : A^+ \to S.$$

When δ is the identity map, then ϕ is usually called the *canonical epimorphism.* Moreover, one has $S \cong A^+/\phi\phi^{-1}$.

Let us suppose that A is totally ordered. Recall from Chapter 1 that the *radix order* $<_a$ on A^+ is defined for u, v in A^+ by

$$u <_a v \iff (|u| < |v|) \text{ or } (|u| = |v| \text{ and } u < v),$$

where $<$ is the lexicographic order. From the definition it follows that $<_a$ is a well-order.

A word w is said *reducible* with respect to the morphism ϕ and to the order $<_a$, or simply *reducible*, if there exists $u \in A^+$ such that

$$u <_a w \quad \text{and} \quad \phi(u) = \phi(w).$$

A word which is not reducible will be called *irreducible*. Let $s \in S$. In the set $\phi^{-1}(s)$ there is a unique minimal element with respect to $<_a$ usually called the *canonical representative* of s. Hence, the set of all canonical representatives of the elements of S is the set of all irreducible elements of S. For any set $T \subseteq S$, we denote by C_T the set of the canonical representatives of the elements of T.

An infinite (bi-infinite) word x is *reducible*, relative to the morphism $\phi : A^+ \to S$ and to the order $<_a$, if there exists $w \in F(x)$ which is reducible. An infinite word x which is not reducible, i.e., any $w \in F(x)$ is irreducible, is called *irreducible*.

We recall now some lemmas and propositions on canonical representatives.

LEMMA 4.5.1. *Let S be a finitely generated semigroup and T be any subset of S closed by factors. Then the set C_T is closed by factors.*

Proof. Let $x \in C_T$ and u be a factor of x, i.e., $x = \lambda u \mu$, with $\lambda, \mu \in A^*$. Since $\phi(x) = \phi(\lambda)\phi(u)\phi(\mu)$ and T is closed by factors one has $\phi(u) \in T$ and then $u \in \phi^{-1}(T)$. Suppose now that $u' \in A^+$ exists such that $u' <_a u$ and $\phi(u') = \phi(u)$. If $|u'| < |u|$, then $x' = \lambda u' \mu$ is such that $|x'| < |x|$ and $\phi(x') = \phi(x)$ which is a contradiction. Let us then suppose $|u'| = |u|$ and $u' < u$. Thus $x' = \lambda u' \mu < \lambda u \mu$ and $\phi(x') = \phi(x)$ which is again a contradiction. Hence, $u \in C_T$ which concludes the proof. ∎

LEMMA 4.5.2. *Let S be a finitely generated semigroup. If T is an infinite subset of S closed by factors, then there exists a uniformly recurrent irreducible word x such that $F(x) \subseteq C_T$.*

Proof. Since C_T is closed by factors then by Proposition 1.5.12 there exists a uniformly recurrent word $x \in A^\omega$ such that $F(x) \subseteq C_T$, so that x is irreducible. ∎

As in the case of free monoids one can introduce for any semigroup S the notions of bi-ideal sequence and n-sequence. A sequence

$$s_1, \ldots, s_n, \ldots$$

of elements of a semigroup S is a *bi-ideal sequence* if for any $i > 0$

$$s_{i+1} \in s_i S^1 s_i.$$

When the sequence is finite and of length n, then $(s_1, \ldots, s_n)$ is called a bi-ideal sequence of *order* n.

From Lemma 4.5.2 one easily derives the following

PROPOSITION 4.5.3. *Let S be a finitely generated semigroup. If T is an infinite subset of S closed by factors, then there exists a bi-ideal sequence $(s_n)_{n>0}$ such that for all $n > 0$, $s_n \in T$ and for all positive integers i, j, $i \neq j$, $s_i \neq s_j$.*

Proof. By Lemma 4.5.2 there exists an irreducible uniformly recurrent word $x \in A^\omega$ such that $F(x) \subseteq C_T$. By Proposition 4.3.1, the word x is a sesquipower, so that there exists a bi-ideal sequence $(f_n)_{n>0}$, such that $x = \lim_{n\to\infty} f_n$. Since for every $n > 0$, $f_n \in F(x) \subseteq C_T$ then $\phi(f_n) \in T$, where ϕ is the canonical epimorphism. Moreover, since x is irreducible it follows that for all positive integers $i, j, i \neq j$, $\phi(f_i) \neq \phi(f_j)$. The image by ϕ of the bi-ideal sequence $(f_n)_{n>0}$ is then a bi-ideal sequence $(s_n)_{n>0}$, with $s_n = \phi(f_n) \in T$ for all $n > 0$, such that $s_i \neq s_j$ for $i \neq j$. ∎

A sequence $t_1, \ldots, t_n$ of n elements of a semigroup S is called *n-sequence* if for all $i = 1, \ldots, n-1$,

$$t_i \in t_{i+1} \cdots t_n S^1. \tag{4.5.1}$$

As in the case of free monoids the notions of bi-ideal sequence of order n and of n-sequence are related. In fact, let $s_1, \ldots, s_n$ be a bi-ideal sequence of S where

$$s_{i+1} = s_i g_i s_i$$

with $g_i \in S^1$, $i = 1, \ldots, n-1$. As one easily verifies setting $t_n = s_1$ and $t_{n-i} = s_i g_i$, $i = 1, \ldots, n-1$, the sequence $(t_1, \ldots, t_n)$ is an n-sequence. Conversely, if $(t_1, \ldots, t_n)$ is an n-sequence, then the sequence $s_i = t_{n-i+1} \cdots t_n$, $i = 1, \ldots, n$, is a bi-ideal sequence of order n.

Let us, finally, observe that in the case of a group G any sequence $g_1, \ldots, g_n$ of n elements of G is an n-sequence.

4.5.1. Permutation property

Let S be a finitely generated semigroup and $\phi : A^+ \to S$ be the canonical epimorphism. For any $s \in S$ the *order* of s is the order (cardinality) of the subsemigroup $\langle s \rangle$ generated by $\{s\}$. The order of s is finite if and only if there exist positive integers i and j, $i < j$, depending on the element s, such that

$$s^i = s^j. \tag{4.5.2}$$

Let j be the minimal integer for which the above relation is satisfied. The integer i, which is unique, is called the *index* and $p = j - i$ the *period* of s. The order of $\langle s \rangle$ is then given by $i+p-1$. In the case of a group, due to cancellativity, condition (4.5.2) simply becomes $s^p = 1$, where 1 denotes the identity of the group and the period p depends on the element s.

A semigroup (group) S is periodic (or torsion) if any element $s \in S$ generates a subsemigroup (subgroup) of finite order.

The problem of whether a finitely generated and periodic group is finite was posed by W. Burnside in 1902 and, subsequently, extended to the case of semigroups. However, the condition of a finite generation and the periodicity are not sufficient to assure the finiteness of a semigroup or a group (cf. Notes).

A finitely generated, torsion and commutative semigroup is obviously finite. A. Restivo and C. Reutenauer introduced in 1984 a property of semigroups, called *permutation property*, which generalizes commutativity and is such that a finitely generated and torsion semigroup is finite if and only if it is permutable. Let us give the following:

Let S be a semigroup and n be an integer > 1. A sequence $s_1, \ldots, s_n$ of n elements of S is called *permutable* if the product $s_1 \cdots s_n$ remains invariant under some nontrivial permutation of its factors, i.e., there exists a permutation $\sigma \in \mathcal{S}_n$, different from the identity, such that

$$s_1 s_2 \cdots s_n = s_{\sigma(1)} s_{\sigma(2)} \cdots s_{\sigma(n)}.$$

We say that a semigroup S is *n-permutable* if any sequence of n elements of S is permutable. Obviously, 2-permutability is equivalent to commutativity. We say that S is *permutable* if there exists an integer $n > 1$ such that S is n-permutable.

THEOREM 4.5.4. *Let S be a finitely generated and periodic semigroup. S is finite if and only if it is permutable.*

The original proof of the theorem is based on the theorem of Shirshov. We prove here a slight more general version of Theorem 4.5.4 by considering a weak notion of permutability of a semigroup S. One requires that for some integer $n > 1$, not all the sequences of n elements are permutable, but only the n-sequences of S.

THEOREM 4.5.5. *Let S be a finitely generated and periodic semigroup. S is finite if and only if there exists an integer $n \geq 2$ such that any n-sequence of S is permutable.*

Proof. The 'only if' part is trivial, then we prove the 'if' part. Let $n \geq 2$ be an integer such that any n-sequence of S is permutable. Let $\phi : A^+ \to S$ be the canonical epimorphism and suppose by contradiction that S is infinite. By Lemma 4.5.2 there exists an irreducible and uniformly recurrent word t. Since S is periodic, t is ω-power-free. Indeed, otherwise, by Lemma 4.3.4, t is periodic so that it contains a factor u^p, such that

$$\phi(u^p) = \phi(u)^p = \phi(u)^q = \phi(u^q),$$

with $1 \leq q < p$, and this contradicts the irreducibility of t. By Theorem 4.4.4, t contains a factor x which is the nth term of a bi-ideal sequence whose canonical factorization is an n-division. We can write $x = w_1 w_2 \cdots w_n$, where $(w_1, w_2, \ldots, w_n)$ is the canonical factorization of x which is an n-sequence. Let us set $s_i = \phi(w_i)$, for $i = 1, \ldots, n$. Since $(s_1, s_2, \ldots, s_n)$ is an n-sequence of S, it is permutable. Then, for a nontrivial permutation $\sigma \in \mathcal{S}_n$ one has

$$\phi(x) = s_1 s_2 \cdots s_n = s_{\sigma(1)} s_{\sigma(2)} \cdots s_{\sigma(n)}.$$

On the other hand one has $x > w_{\sigma(1)} w_{\sigma(2)} \cdots w_{\sigma(n)}$ and this contradicts the irreducibility of t. ∎

4.5.2. Iteration property

In this section we consider some finiteness conditions for semigroups based on *iteration properties*. These properties, are very important in formal language theory, since they are related to the 'pumping properties' of regular languages.

Let S be a semigroup and m and n two integers such that $m > 0$ and $n \geq 0$. We say that the sequence $s_1, s_2, \ldots, s_m$ of m elements of S is *n-iterable* if there exist i, j such that $1 \leq i \leq j \leq m$ and

$$s_1 \cdots s_m = s_1 \cdots s_{i-1}(s_i \cdots s_j)^n s_{j+1} \cdots s_m. \tag{4.5.3}$$

We say that S is *(m,n)-iterable*, or satisfies the property $C(n,m)$ if all sequences of m elements of S are n-iterable.

Let us observe that property $C(1,m)$ is always trivially true. Moreover, property $C(0,m)$ is actually a cancellation property (*m-cancellation property*) which obviously implies the finiteness of any finitely generated semigroup satisfying it, so that a semigroup satisfies properly the iteration property $C(n,m)$ only if $n > 1$.

PROPOSITION 4.5.6. *If S is a finite semigroup, then S satisfies $C(n,m)$ with $m = \mathrm{Card}(S) + 1$ and any $n \geq 0$. If S satisfies $C(n,m)$, with $n \neq 1$, then S is periodic.*

Proof. Let $s_1, \ldots, s_m$ be a sequence of m elements of S, with $m = \mathrm{Card}(S) + 1$. We consider then the sequence

$$s_1,\ s_1 s_2, \ldots,\ s_1 s_2 \cdots s_m.$$

Since $m > \mathrm{Card}(S)$ there exist integers i, j such that $1 \leq i < j \leq m$ and

$$s_1 \cdots s_i = s_1 \cdots s_i(s_{i+1} \cdots s_j) = s_1 \cdots s_i(s_{i+1} \cdots s_j)^n,$$

for all $n \geq 0$. Thus

$$s_1 \cdots s_i s_{j+1} \cdots s_m = s_1 \cdots s_i(s_{i+1} \cdots s_j)^n s_{j+1} \cdots s_m,$$

so that $C(n,m)$ holds for all $n \geq 0$.

If S satisfies $C(n,m)$, then for any $s \in S$, consider the sequence $s_1 = s_2 = \cdots = s_m = s$. One has that there exist integers i, j such that $1 \leq i \leq j \leq m$ and

$$s^m = s^{m+(n-1)(j-i+1)},$$

so that, since $n \neq 1$, S is periodic. ∎

Let us consider in a semigroup S the following equivalence relations $\mathcal{R}$ and $\mathcal{L}$ defined, for $s, t \in S$, by

$$s \,\mathcal{R}\, t \Longleftrightarrow sS^1 = tS^1,\quad s \,\mathcal{L}\, t \Longleftrightarrow S^1 s = S^1 t.$$

Moreover we set $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$ and $\mathcal{D} = \mathcal{R} \vee \mathcal{L}$, where $\mathcal{R} \vee \mathcal{L}$ denotes the smallest equivalence relation on S containing $\mathcal{R}$ and $\mathcal{L}$. From the definition one has that $\mathcal{R}$ and $\mathcal{L}$ are left invariant and right invariant, respectively.

Lemma 4.5.7. *Let S be a finitely generated semigroup satisfying $C(n,m)$, with $n > 1$, and $\phi : A^+ \to S$ be the canonical epimorphism. For any uniformly recurrent word w there exists a positive integer M such that for any $u, v \in F(w)$ with $|u| > M$*

$$uv \in F(w) \Rightarrow \phi(u) \mathrel{\mathcal{R}} \phi(uv).$$

Proof. It is sufficient to prove that there exists a positive integer M such that for each $u \in F(w)$ and $a \in A$ if $ua \in F(w)$, then $\phi(u) \mathrel{\mathcal{R}} \phi(ua)$. By Proposition 4.3.3 there exists a positive integer $M = D(m)$ such that for any $u \in A^*$, $a \in A$, with $ua \in F(w)$ and $|u| \geq M$ one has that

$$u = \lambda f_m,$$

where $\lambda \in A^*$, and f_m is the mth term of a bi-ideal sequence $f_{i+1} = f_i g_i f_i$, with $f_1 \in aA^*$ and $g_i \in aA^*$, $i = 1, \ldots, m-1$. Let us write f_m as

$$f_m = w_1 \cdots w_m$$

where $(w_1, \ldots, w_m)$ is the canonical factorization of f_m. As S satisfies $C(n,m)$ there exist integers i, j such that $1 \leq i \leq j \leq m$ and

$$w_1 \cdots w_m \equiv w_1 \cdots w_{i-1}(w_i \cdots w_j)^n w_{j+1} \cdots w_m, \tag{4.5.4}$$

where $\equiv$ denotes the congruence relation $\phi\phi^{-1}$. One can rewrite the preceding equation as

$$w_1 \cdots w_m \equiv w_1 \cdots w_i \cdots w_j w_i v, \tag{4.5.5}$$

with $v \in A^*$. Let us first suppose $j < m$. By Eq.(4.2.2) one derives, by iteration,

$$w_i = w_{j+1} \cdots w_m g_{m-j} u,$$

with $u \in A^*$. Hence, since $g_{m-j} \in aA^*$ one has

$$w_1 \cdots w_m \equiv w_1 \cdots w_j w_{j+1} \cdots w_m g_{m-j} \zeta = w_1 \cdots w_j w_{j+1} \cdots w_m a \xi.$$

with $\zeta, \xi \in A^*$. This implies

$$\phi(f_m) \mathrel{\mathcal{R}} \phi(f_m a).$$

Since the relation $\mathcal{R}$ is left invariant it follows $\phi(u) \mathrel{\mathcal{R}} \phi(ua)$. In the case $j = m$ since $w_i \in aA^*$ for all $i = 1, \ldots, m$, from Eq.(4.5.5) one has again $\phi(f_m) \mathrel{\mathcal{R}} \phi(f_m a)$ which implies $\phi(u) \mathrel{\mathcal{R}} \phi(ua)$. ∎

Theorem 4.5.8. *Let S be a finitely generated semigroup. S is finite if and only if it satisfies $C(2,m)$ for a suitable $m > 0$.*

Proof. The 'only if' part follows from Proposition 4.5.6. Let us then prove the 'if' part. Let S be a finitely generated semigroup satisfying $C(2,m)$ for a suitable $m > 0$ and suppose, by contradiction, that S is infinite. From Lemma 4.5.2

there exists a uniformly recurrent word w which is irreducible with respect to the canonical epimorphism $\phi : A^+ \to S$. By Lemma 4.5.7 there exists a positive integer M such that for any $u, v \in F(w)$ with $|u| > M$, $uv \in F(w) \Rightarrow \phi(u) \mathcal{R} \phi(uv)$. Let now u be any factor of w such that $|u| > M$. Since w is uniformly recurrent we can consider $m+1$ consecutive non-overlapping occurrences of u and then the factor v of w

$$v = ux_1ux_2 \cdots ux_mu,$$

with $x_i \in A^*$ for $(i = 1, \ldots, m)$. From condition $C(2, m)$ there exist i, j such that $1 \leq i \leq j \leq m$ and:

$$v \equiv ux_1 \cdots ux_{i-1}(ux_i \cdots ux_j)^2 ux_{j+1} \cdots ux_m u. \tag{4.5.6}$$

Moreover, from Lemma 4.5.7 one has that

$$\phi(u) \mathcal{R} \phi(ux_i \cdots ux_m u),$$

for all $i = 1, \ldots, m$. This implies that for any $i = 1, \ldots, m$, there exists a word $t \in A^*$ depending on i, such that

$$u \equiv ux_i \cdots ux_m ut.$$

One has then

$$v = ux_1ux_2 \cdots ux_m u \equiv ux_1 \cdots ux_{i-1}(ux_i \cdots ux_j)^2 ux_{j+1} \cdots ux_m ut\zeta,$$

having set $\zeta = x_{j+1} \cdots ux_m u$. By Eq.(4.5.6), it follows

$$v \equiv ux_1 \cdots ux_{i-1}ux_i \cdots ux_m ut\zeta \equiv$$

$$ux_1 \cdots ux_{i-1}ux_{j+1} \cdots ux_m u.$$

Hence, v is reducible that is a contradiction. ∎

A special form of iteration property is the *iteration on the right.* A semigroup S satisfies the condition $D(n, m)$, $m > 0, n \geq 0$, if for any sequence $s_1, s_2, \ldots, s_m$ of m elements of S there exist integers i, j such that $1 \leq i \leq j \leq m$ and

$$s_1 \cdots s_j = s_1 \cdots s_{i-1}(s_i \cdots s_j)^n.$$

It is clear that if a semigroup satisfies $D(n, m)$, then it satisfies $C(n, m)$. Thus from Theorem 4.5.8, $D(2, m)$ is a finiteness condition for finitely generated semigroups. Moreover, it is straightforward to derive that any finite semigroup S satisfies $D(n, m)$ for a suitable m, depending on the cardinality of S, and for all $n \geq 0$.

Another important property, strictly related to the iteration property, is the *strong periodicity.* Let S be a semigroup. We denote by $E(S)$ the set of its idempotent elements.

Let m be a positive integer. A semigroup S is *strongly m-periodic* if for any sequence $s_1, \ldots, s_m$ of m elements of S there exist integers i and j such that $1 \leq i \leq j \leq m$ and $s_i \cdots s_j \in E(S)$.

A semigroup S is *strongly periodic* if there exists a positive integer m such that S is strongly m-periodic. The origin of the term strongly m-periodic is due to the fact that if S is strongly m-periodic, then S is certainly periodic and, moreover, the index and the period of any element are less than or equal to m. It is clear from the definition that if a semigroup S is strongly m-periodic, then S satisfies $C(2,m)$ and $D(2,m)$.

The following interesting theorem holds

THEOREM 4.5.9. *Let S be a finitely generated semigroup. The following conditions are equivalent:*
(i) *S is finite.*
(ii) *$S \setminus E(S)$ is finite.*
(iii) *S is strongly periodic.*

Proof. The implication (i)⇒(ii) is trivial. For the implication (ii)⇒(iii) one uses the theorem of Ramsey (Lothaire 1983, Chapter 4). Let $F = S \setminus E(S)$ and be $p = \mathrm{Card}(F)$. We prove that S is strongly m-periodic with $m = R(2,3,p+1)-1$ where R denotes the function of Ramsey's theorem. Let $s_1, \ldots, s_m$ be a sequence of m elements of S. We define:

$$B_0 = \{\{i,j\} \mid 1 \le i < j \le m+1 \text{ and } s_i s_{i+1} \cdots s_{j-1} \in E(S)\},$$

and for any $f \in F$,

$$B_f = \{\{i,j\} \mid 1 \le i < j \le m+1 \text{ and } s_i s_{i+1} \cdots s_{j-1} = f\}.$$

By Ramsey's theorem there exist $1 \le i_1 < i_2 < i_3 \le m+1$ such that $\{i_1,i_2\}$,$\{i_2,i_3\}$ and $\{i_1,i_3\}$ are all in the same class. This class is certainly B_0 because, otherwise, there will exist $f \in F$ such that:

$$f = s_{i_1} \cdots s_{i_3-1} = (s_{i_1} \cdots s_{i_2-1})(s_{i_2} \cdots s_{i_3-1}) = f^2$$

which is a contradiction.

(iii)⇒(i). If a semigroup S is strongly m-periodic, then it satisfies condition $C(2,m)$. Then, by Theorem 4.5.8, S is finite. ∎

4.5.3. Minimal conditions on principal bi-ideals

We recall that a *bi-ideal* B of S is a subsemigroup of S such that

$$BSB \subseteq B.$$

A bi-ideal is called *principal* if it is of the form sS^1s, where s is any element of S.

A semigroup S satisfies the *minimal condition on principal bi-ideals* if any strictly descending chain

$$s_1S^1s_1 \supset s_2S^1s_2 \supset \cdots \supset s_nS^1s_n \supset \cdots,$$

with $s_1, s_2, \ldots, s_n, \ldots \in S$, has a finite length.

THEOREM 4.5.10. *Let S be a finitely generated semigroup. If S satisfies the minimal condition on principal bi-ideals and if all subgroups of S are finite, then S is finite.*

Proof. Let S be a semigroup satisfying the hypotheses of the statement and let $\phi : A^+ \to S$ be the canonical epimorphism. Suppose by contradiction that S is infinite. Then, by Proposition 4.5.3, there exists a bi-ideal sequence $(s_n)_{n>0}$ such that for all positive integers i, j, with $i \neq j$, one has $s_i \neq s_j$. Since $s_{n+1} \in s_n S^1 s_n$, for $n \geq 1$, it follows

$$s_n S^1 s_n \supseteq s_{n+1} S^1 s_{n+1}.$$

Thus we have a descending chain

$$s_1 S^1 s_1 \supseteq s_2 S^1 s_2 \supseteq \cdots \supseteq s_n S^1 s_n \supseteq \cdots.$$

By the minimal condition on principal bi-ideals, there exists an integer k such that $s_k S^1 s_k = s_n S^1 s_n$, for any $n \geq k$. Let n be any integer $\geq k$. One has $s_n S^1 s_n = s_{n+1} S^1 s_{n+1} = s_{n+2} S^1 s_{n+2}$, and, moreover, $s_{n+1} \in s_n S^1 s_n$. Thus we have

$$s_{n+1} = s_n t s_n = s_{n+1} h s_{n+1} = s_{n+2} r s_{n+2}, \tag{4.5.7}$$

for some $t, h, r \in S^1$. Moreover, since $s_{n+2} \in s_{n+1} S^1 s_{n+1}$, one has

$$s_{n+2} = s_{n+1} z s_{n+1}, \tag{4.5.8}$$

for some $z \in S^1$. From Eq.s (4.5.7) and (4.5.8) one derives that for any $n \geq k$ $s_{n+1} \ \mathcal{R} \ s_{n+2}$, $s_{n+1} \ \mathcal{L} \ s_{n+2}$ and, therefore, $s_{n+1} \ \mathcal{H} \ s_{n+2}$. In conclusion, for any $n > k$ all the elements s_n lie in the same $\mathcal{H}$-class H. From Eq. (4.5.7) one has that s_{n+1} is a regular element (cf. Problem 4.5.5) for any $n \geq k$. The $\mathcal{H}$-class H is in a regular $\mathcal{D}$-class D, hence it is finite since it has the same cardinality of a maximal subgroup contained in D (cf. Problem 4.5.5), and, by hypothesis, all subgroups of S are finite. Then there exist two integers i, j, with $k < i < j$ such that $s_i = s_j$ which is a contradiction. ∎

Problems

Section 4.1

4.1.1 A sequence $f_1, f_2, \ldots, f_n$ of n words on the alphabet A is called a *quasi-ideal* sequence of order n if $f_1 \in A^+$ and for all $i = 1, 2, \ldots, n-1$ one has:

$$f_{i+1} \in f_i A^* \cap A^* f_i.$$

Thus a bi-ideal sequence of order n is also a quasi-ideal sequence of order n. Give an example of a quasi-ideal sequence which is not a bi-ideal sequence.

4.1.2 Any word $w \in A^+$ is a *quasi-power* of order 1. For any $n > 0$ a word w is called a *quasi-power* of order $n+1$ if there exists a quasi-power u of order n such that

$$w \in uA^+ \cap A^+u.$$

The *quasi-power degree* of w is the maximal order of w as a quasi-power. Show that if w is a quasi-power of degree n, then there exists a *unique* quasi-ideal sequence $(f_1, \ldots, f_n)$ such that $f_n = w$.

4.1.3 A word w has a *bord* $u \in A^+$, if $w \in uA^+ \cap A^+u$. As is well known a word w has the proper period p $(0 < p < |w|)$ if and only if there exists a bord u such that $p = |w| - |u|$. Show that if w is a quasi-power of degree n and $(f_1, \ldots, f_n)$ is the unique quasi-ideal sequence such that $f_n = w$, then $(f_1, \ldots, f_{n-1})$ is the sequence of all the bords of w. Thus $n-1$ is the number of all proper periods of w.

Section 4.2

4.2.1 Let $(w_1, \ldots, w_n)$ and $(w'_1, \ldots, w'_n)$ be the canonical factorizations of the nth term of a bi-ideal sequence. Prove that

- for each i, $1 \le i \le n-1$, one has: $w'_i w'_{i+1} < w'_{i+1} w'_i$ if and only if $w_{n-i+1} w_{n-i} < w_{n-i} w_{n-i+1}$.
- $(w_1, \ldots, w_n)$ is an n-division (inverse n-division) if and only if $(w'_1, \ldots, w'_n)$ is an inverse n-division (n-division).

4.2.2 Let $(w_1, \ldots, w_m)$ be a sequence of words. We say that $(u_1, \ldots, u_n)$ is a *derived sequence* of $(w_1, \ldots, w_m)$ if there exist $n+1$ integers j_1, j_2, $\ldots, j_{n+1}$ such that $1 \le j_1 < j_2 < \cdots < j_{n+1} \le m+1$, and

$$u_1 = w_{j_1} \cdots w_{j_2 - 1}, \ldots, u_n = w_{j_n} \cdots w_{j_{n+1}-1}.$$

Prove that a derived sequence $(u_1, \ldots, u_n)$ of an m-sequence $(w_1, \ldots, w_m)$ (inverse m-sequence) is an n-sequence (inverse n-sequence).

Section 4.3

4.3.1 Prove that if an eventually periodic word $w \in A^\omega$ is recurrent, then w is periodic.

4.3.2 Let $A = \{a, b, c, d\}$ and m be the Thue-Morse word on the alphabet $\{a, b, c\}$ which can be generated iterating on the letter a the morphism ϕ defined by $\phi(a) = abc$, $\phi(b) = ac$, $\phi(c) = b$ (cf. Lothaire 1983). Let us denote by p_i the prefix of m of length i and construct the word:

$$w = dp_1(dp_2)^2(dp_3)^3 \cdots (dp_n)^n \cdots.$$

Show that for any $p > 1$, w has a factor which is a p-power. However, w is ω-power-free.

Section 4.4

4.4.1 Let $l_1, l_2, \ldots, l_n$ be n Lyndon words with $l_1 > l_2 > \cdots > l_n$. Let $w_i = l_i^{k_i}$, with $k_i \geq 1$, $1 \leq i \leq n$. Prove that the word $w = w_1 w_2 \cdots w_n$ is n-divided and $(w_1, w_2, \ldots, w_n)$ is an n-division. (*Hint.* Use the property, cf. Lothaire 1983, that if x and y are Lyndon words and $x < y$, then xy is a Lyndon word and $x < xy < y$).

Section 4.5

4.5.1 The notion of finite, as well as infinite, irreducible word can be given with respect to any partial order $\leq$ in A^+. A partial order in A^+ is a *well partial order*, if any subset X of A^+ has at least one and at most a finite number of minimal elements in X. In such a case if $\phi : A^+ \to S$ is a morphism of A^+ onto the semigroup S, then for any $s \in S$ the set $\phi^{-1}(s)$ of the representatives of s has a finite > 0 number of representatives. Prove that if a well partial order $\leq$ in A^+ is monotone (i.e., invariant with respect to concatenation), then the set C_T of all irreducible representatives of any factorial set $T \subseteq S$ is closed by factors.

4.5.2 Prove that if H is an abelian subgroup of a group G such that the index m of H in G is finite, then G is n-permutable with $n = 2m$.

4.5.3 A semigroup S is called *weakly permutable*, if there exists an integer $n > 1$ such that for any sequence $s_1, s_2, \ldots, s_n$ of of n elements of S there exist two permutations $\sigma, \tau \in \mathcal{S}_n$, $\sigma \neq \tau$ such that $s_{\sigma(1)} s_{\sigma(2)} \cdots s_{\sigma(n)} = s_{\tau(1)} s_{\tau(2)} \cdots s_{\tau(n)}$.
It is obvious that if a semigroup S is permutable, then it is weakly permutable. Show that the converse is not, in general, true.

4.5.4 A semigroup S is called a *band* if all its elements are idempotents, i.e., for any $s \in S$, $s = s^2$. Show that a finitely generated band is finite.

4.5.5 Let S be a semigroup. The relations $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{D}$ satisfy the following properties:

1. The relations $\mathcal{R}$ and $\mathcal{L}$ commute, and so $\mathcal{D} = \mathcal{RL} = \mathcal{LR}$.
2. Any two $\mathcal{H}$-classes in the same $\mathcal{D}$-class have the same cardinality.
3. An $\mathcal{H}$-class H_e containing an idempotent e is equal to the maximal subgroup of S having e as identity.

An element s of a semigroup S is called *regular* if there exists $x \in S$ such that $s = sxs$. A $\mathcal{D}$-class D of a semigroup is called *regular* if all its elements are regular. Let D be a $\mathcal{D}$-class of a semigroup S. The following holds:

i. D is regular if and only if contains a regular element.
ii. D is regular if and only if contains an idempotent.
iii. Any two maximal subgroups in D are isomorphic.

(cf. Clifford and Preston 1961, Chapter 2)

4.5.6 Define in a semigroup S the quasi-order relation $\leq_B$ as: for $s, t \in S$

$$s \leq_B t \Longleftrightarrow s = t \text{ or } s \in tS^1t.$$

A semigroup satisfies the condition $\min_B$ if any strictly descending chain $s_1 >_B s_2 >_B \cdots >_B s_n >_B \cdots$ of elements of S has a finite length. Prove that if a semigroup S satisfies the minimal condition on principal bi-ideals, then it satisfies $\min_B$.

4.5.7 A nonempty subset Q of a semigroup S is called a quasi-ideal of S if

$$QS \cap SQ \subseteq Q.$$

Show that

- every quasi-ideal of S is a bi-ideal of S.
- a subset of a semigroup S is a quasi-ideal if and only if it is the intersection of a right ideal of S and a left ideal of S.
- A semigroup S is a group if and only if it contains no proper quasi-ideal (bi-ideal).

Notes

The name of bi-ideal sequence appears in Coudrain and Schützenberger 1966 who introduced these sequences in the frame of semigroup theory. Actually, these sequences were considered ten years earlier by Jacobson 1964 in his book on ring theory. A bi-ideal sequence of order n was called by Jacobson *n-sequence*. Zimin's words Z_n were introduced by Zimin 1982. A word which is the nth term of a bi-ideal sequence was also called *sesquipower of order n* by Simon 1988 and *quasi-power of order n* by Berstel and Reutenauer 1988. Theorem 4.1.2 was first proved in Coudrain and Schützenberger 1966.

Shirshov's theorem appears in Shirshov 1957 (cf. also Lothaire 1983, Chapter 7). A different proof of Shirshov's theorem based on an unavoidable regularity related to Lyndon words was given by Reutenauer 1986. A proof which uses the uniform recurrence is given by Justin and Pirillo 1991. An improvement of Shirshov's theorem in which the n-divided factor is the nth term of a bi-ideal sequence was given in De Luca and Varricchio 1991a. Theorem 4.4.5, whose proof is in De Luca and Varricchio 1999, is a further generalization since the n-division is a strictly decreasing sequence of Lyndon words.

The problem of whether a finitely generated and periodic group is finite was posed by W. Burnside in 1902 and, subsequently, extended to the case of semigroups. A negative answer to the Burnside problem was given by Golod 1964. This author by means of a technique of proof discovered with I. R. Shafarevich, based on the non-finiteness of a dimension of a suitable algebra associated with a field, was able to show the existence of an infinite 3-generated p-group.

The permutation property of semigroups was introduced in Restivo and Reutenauer 1984, where the proof of Theorem 4.5.4, based on Shirshov's theorem, was given. A characterization of permutable groups is given in Curzio et al. 1985. Curzio et al. 1983 give an algebraic proof that a finitely generated and torsion group is finite if and only if it is permutable. An extension of Theorem 4.5.4 based on the weaker notion of ω-permutability appears in De Luca and Varricchio 1990.

The notion of strong periodicity and Theorem 4.5.9 are due to Simon 1980. The proof of Simon makes use of a finiteness condition due to Hotzel 1979. The proof that condition $D(n,m)$ is a finiteness condition for finitely generated semigroups appears in De Luca and Restivo 1984 for $n=2$ and in De Luca and Varricchio 1991b for $n=3$. A more constructive proof of the result in the case of $D(2,m)$, as well as an upper bound to the cardinality of the semigroup, was given by Hashiguchi 1986.

The proof that condition $C(n,m)$ is a finiteness condition for finitely generated semigroups in the cases $n = 2$ and $n = 3$ appears in De Luca and Varricchio 1991a. The proof makes use of a deep structure theorem on finitely generated semigroups (the J-depth decomposition theorem) (De Luca and Varricchio 1999).

Theorem 4.5.10 is due to Coudrain and Schützenberger 1966. An extension of this result under the weaker hypothesis that the subgroups of the given finitely generated semigroup are locally finite appears in De Luca and Varricchio 1994.