COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
20. ALGEBRAIC THEORY OF SEMIGROUPS, SZEGED (HUNGARY), 1976.

A PROPERTY OF FINITELY GENERATED SUBMONOIDS OF FREE MONOIDS

M.P. SCHÜTZENBERGER

To the memory of C. and A. Rényi

1. INTRODUCTION

Various problems in algebra lead to the study of the ways in which the words of a free monoid A^* (generated by the alphabet A) can be factorized as products of the words from a given subset X of A^*. It suffices to make reference to the works of A1.A. Markov [1], Y.I. Khmelevski [2], S.I. Adjan [3], to the recent thesis of J.C. Spehner [4], and, especially, to the book of A. Lentin on the equations in free monoids [5]. One technique to approach this question uses the syntactic monoid $S = \mathrm{Synt}(X^*)$ of the submonoid X^* generated by X. According to S. Eilenberg's theory [6], S is the least quotient of A^* such that the natural morphism σ of A^* on S *recognises* X^* (in the sense that $X^* = X^*\sigma\sigma^{-1}$). In equivalent fashion, let the X^*-*context* of a word w be the set of all pairs of words (v, v') such that vwv' is in X^*; then S is the quotient of A^* by the congruence which is defined by the equality of contextes [7]. Here we shall

be mainly concerned with the case of a finite X. Its interest, apart from the applications, is demonstrated by the researches of J.F. Perrot [8], [9] and Perrin [10] who have shown that this hypothesis implies severe conditions on S.

It is well known that the finiteness of $S = \mathrm{Synt}\,(X^*)$ for finite X is a trivial special case of Kleene's theorem (cf. [6], Chap. VII). It entails a bound on S as a function of the sum L of the lengths of the words in X. To see it directly, recall the standard notation A^+ for the free semigroup $A^* \setminus 1$ generated by the same alphabet A as A^* and assume without loss of generality that X is the minimum generating set of X^*, i.e., that X is equal to $X^+ \setminus X^+ \cdot X^+$ (where, of course, $X^+ = X^* \setminus 1$). As usual, the *prefixes* (resp. *suffixes*) of X are the proper left (resp. right) factors of its words. By definition, their set is

$$P = X(A^+)^{-1} = \{a \in A^* \colon aA^+ \cap X \neq \phi\}$$

and

$$Q = (A^+)^{-1}X = \{a \in A^* \colon A^+a \cap X \neq \phi\}.$$

Their number is at most L and it is clear that any two words have the same context when their contextes have the same restriction to $P \times Q$. Accordingly, the number of classes of the syntactic congruence is not more than 2^{L^2}.

Before examining some examples we recall that in any semigroup M the *conjugacy* relation is the least equivalence on M such that mm' and $m'm$ belong to the same class for any two elements m and m' of M. It follows that two groups in M generate the same ideal iff their idempotents are conjugate. Classical theorems by Clifford and Miller [11] show that two such maximal groups are isomorphic. One says then that thay are *conjugate*. Also, an element m is *primitive* iff the submonoid m^* contains every element m' such that m is included in m'^*. When M is a group, the conjugacy relation is the usual one (since $m' = g^{-1}mg$ is equivalent with $m' = (g^{-1})(mg)$ and $m = (mg)(g^{-1})$) and m is primitive iff it generates a maximal cyclic subgroup.

These notions are of special significance also when M is a free

monoid because, (as it is well known) every word $w \neq 1$ is in a unique manner a power $w = h^r$ of a primitive word h (often noted $\sqrt{w}$) and its conjugacy class consists of the $|h|$ words $(h'h'')^r$ where $|h|$ is the length of h and h' and h'' satisfy $h = h''h'$. Thus, here, primitive elements correspond to maximal commutative subsemigroups because, in a free monoid, two words commute iff they are both powers of the same word (cf. [5]).

We let X have k elements and we say for short that a parameter of $S = \mathrm{Synt}\,(X^*)$ is *absolutely finite* if it can be bounded as a function of k only. Suppose first $k = 1$ and $X = \{h^P\}$ where h is a primitive word of length $|h|$ and p a positive integer. Then S contains $|h|$ conjugate cyclic groups of order p. Therefore neither the number of elements or groups in S nor the order of these groups is absolutely finite. The same is true for the number of principal ideals in S as it is shown by the example of $X = \{h^P, a\}$ with h^P as above and $a \neq h$ any letter in A, where S has certainly more than $|h|$ such ideals. More generally, if $X = \{h_1^P, h_2^P, \ldots, h_k^P\}$ where $p \geqslant 2$ and where the h_i's are non conjugate words, S contains k classes of conjugate cyclic groups of order p, and the number of its principal quasi ideals (12) not meeting the images of these cyclic groups grows linearly as a function of p for each fixed $k \geqslant 2$.

Our main result, to be proved in Section 4, is that nonetheless some of the parameters of S are absolutely finite. It can be summarized by the following assertions:

(1) The number of conjugate classes of groups in S, i.e. the number of principal idempotent ideals, is absolutely finite.

(2) Apart from at most k conjugate classes of special cyclic groups of arbitrary orders, any group in S is (isomorphic to) a subgroup of the symmetric group of order $(2k)!$.

(3) The inverse images of A^* of the special groups are themselves cyclic subsemigroups of A^*.

(4) Each bi-ideal uSv where u and v are non special idempotents is absolutely finite.

The proof is an application of the theory developed by Fine and Wilf in [13]. The corollaries required for the present study are established in Section 2. To make the connection with syntactic monoids we introduce in Section 3 a somewhat larger monoid M, the *monoid of interpretations* of X^*.

The bound $(2k)!$ in (2) seems quite extravagant since the largest value known is $(k-1)!$ corresponding to X made up of the words:

$$a^{k-1}; a^{k-2}ba; a^{k-3}b; a^{k-4-j}ba^{2+j} \qquad (0 \leqslant j \leqslant k-4)$$

for any $k \geqslant 4$. One computes that the syntactic images of the words ba^{k-1} and ba^{k-2} (for instance) are a cyclic permutation and a transposition generating a symmetric group of the desired order, respectively (cf. [10]).

This result (or more accurately, the bound $k!$) would be achieved if one was able to obtain the "first periodicity lemma" of the Fine – Wilf theory under a weaker hypothesis of "twice covering".*

To end this introduction let us briefly indicate how similar observations can be applied to a special family of equidivisible monoids in the sense of McKnight and Storey [14]. Let F' be the family of all the functions f from the reals into themselves whose domain is a finite semi-open initial interval which is noted $]0, |f|]$ for each function f. The product of f with another function g is obtained by concatenating g with a translate of g. Explicitely, it is the function h of domain $]0, |h|]$ where $|h| = |f| + |g|$ and the value of h at any point r of its domain is defined as follows:

$$h(r) = \begin{cases} f(r) & \text{if} \quad r \leqslant |f|; \\ f(|f|) + g(r - |f|) & \text{otherwise.} \end{cases}$$

Thus, h is continuous when f and g are so. It has been demonstrated by Fine and Wilf (in a slightly different language) that their theory holds for submonoids of F' containing all "smooth" enough functions. In this

*Note (added in proof): This property has been proved since by Y. Césari (C.R. Acad. Sci. Paris, t. 286, 1175-1177) and further important results have been obtained by J-P. Duval (Theoretical Computer Science, to appear).

case, a maximal commutative subsemigroup of F' consists of all functions which are the restrictions to finite initial intervals of a given (ordinary) linear function.

The two "periodicity lemmas" require more stringent restrictions and one is led to consider the submonoid F of F' that is generated by all monotonic (increasing or decreasing) functions. In fact F is almost a free monoid and there is no difficulty in defining the monoid of interpretations (and the syntactic monoid) of an arbitrary submonoid X^* of F. Assuming now that X^* is finitely generated, one can apply the same proof techniques with the obvious modifications imposed by the nature of the maximal commutative subsemigroups, and one verifies that the assertions (1)-(4) above remain true in this more general set-up. This explains our introduction of the notion of "absolute finiteness" since in this case the number of principal ideals (for instance) of the syntactic monoid of X^* is in general not even enumerable.

2. THE THEORY OF FINE AND WILF

In all this section we consider a fixed word w in A^+ of positive length $m = |w|$. In order to deal with the various occurrences of the same word as a factor of w and with their mutual relationships, we shall view w as a sequence of letters and, more accurately, as a map into the alphabet A of a basic sequence C of m consecutive indices. For convenience we shall always take for C the basic chain (i.e. totally ordered set) $C = (1, 2, \ldots, m)$. If $I = (i, i+1, \ldots, i+k)$ is a subinterval of positive length $k+1$ of C, we let Iw be the word $(i)w \cdot (i+1)w \cdot \ldots \cdot (i+k)w$ obtained when restricting w to I. The pair (I, w) is a *segment* of w; I is its *support* and Iw is a factor of w. Of course, $Cw = w$ and, in the opposite direction, Iw is the neutral element of the monoid A^* iff I is the empty interval.

Suppose that, for instance w is the word *baabaababaab* of length 12 where a and b are two letters. The word $f = baaba$ occurs twice as a factor of w in the segments (I', f) and (I'', f) with $I' = (1, 5)$ and $I'' = (4, 8)$; in the same manner the word aba occurs three times, the corresponding supports being respectively $(3, 5), (6, 8)$ and $(8, 10)$.

The reader will notice that the intervals I' and I'' overlap and that their union $I = (1, 8)$ is the support of the word $Iw = baabaaba$ which exhibits an obvious periodicity. The theorem of Fine and Wilf gives a complete (and optimal) analysis of this phenomenon.

The theory is based upon the notions of *translation* and of *periodicity*. We say that a subinterval I of C admits the translation p iff p is a positive integer strictly less than the length $|I|$ of I and if one has $iw = (i + p)w$ for the indices i in I such that $i + p$ is also in I.

This condition is equivalent with $I'w = I''w$ where I' (resp. I'') is the initial (resp. final) interval of length $|I| - p$ of I. Therefore it is equivalent to the existence of words f, g, g' such that $Iw = fg = g'f$ where g and g' both have length p.

Returning to the same example as above, we see that $I = (1, 8)$ admits the translation 3 and that the word $f = I'w = I''w$ satisfies the equation $fg = g'f$ with $g = (6, 8)w = aba$ and $g' = (1, 3)w = baa$; it also admits the translation 6. In similar fashion the interval $(8, 12)$ which is the support of the word $abaab$ admits exactly one translation, viz. 3, and the interval $(7, 11)$ admits no translation whatsoever.

It is clear that when I admits the translation p it also admits any translation $kp \leqslant |I|$ for k a positive integer. We shall call *step of* I the least translation which it admits and denote it by $\|I\|$ (with the convention that the step is infinite when I admits no translation). Algebraic reasons lead to reserve the term "period" to the ratio $|I| : \|I\|$ when it is an integer.

All these notions would easily carry over to the case of the monoids of functions presented at the end of the introduction. Then the basic structure would be a fixed real valued function w of a fixed interval $C =]0, |w|]$, the only difference being that the indices would vary continuously in C instead of being the successive integers $1, 2, \ldots, m$ and that the translations could be any positive real. We refer once more to (13) for this deeper case which will not be touched here.

Since the word w and the basic interval C are fixed it is understood

in what follows that any interval mentioned is a subinterval of C. We begin by a remark.

2.1. *Let K be an interval of length n admitting the translations p and q where $q < p < n$. Its initial (or final) interval of length $n - q$ admits the translation $p - q$.*

Proof. Let $K = (k, k')$ where $k' = k + n - 1$. If i belongs to the initial interval K' of length $n - p$ of K, one has $i + p \in K$. Thus $iw = (i + p)w$ since K admits the translation p. Because of $p > q$, one has $i + p - q > i$, hence $i + p - q \in K$ and $(i + p - q)w = (i + p)w$ since K admits the translation q. Therefore $(i + p - q)w$ is equal to iw for each i in K' which shows that the initial interval of length $n - q = |K'| + p - q$ admits the translation $p - q$ The same argument applies to the final interval of K. Q.E.D.

2.2. **Theorem** (Fine and Wilf). *Let I and J be two intervals admitting the translations p and q, respectively, and having an intersection K of length at least $p + q - r$ where r is the greatest common divisor of p and q. Their union L admits the translation r.*

Proof. We may assume $p \geqslant q$, hence $|K| \geqslant p$ with equality iff $q = r$, i.e. iff p is a multiple of q.

The hypothesis that I admits the translation p implies that we can take in K an interval K' of length p such that for any index i in I there is an index i' in K' differing of i by an integral multiple of p. Thus $iw = i'w$. Accordingly, if p is a multiple of q $(= r)$ and if $x, y \in L$ differ by a multiple of r, we can find x', y' in K' such that $xw = x'w$ and $yw = y'w$ by using the hypothesis that J admits the translation q when any of these indices is in J. Since K' is included in J, the same hypothesis shows that $x'w = y'w$ from which we conclude that $xw = yw$ in this case. This proves the result when q is equal to r and we can assume hence forth that q is strictly greater than r.

We proceed by induction on the integer $(p + q): r$, the case when it is equal to 2 being already covered. From 2.1 we know that K contains an interval K' of length at least $(p + q - r) - q = p - r$ that

admits the translation $p' = p - q$. One has $p' \geqslant r$. If $p' = r$, q is a multiple of r and the same reasoning as above shows successively that J, hence K, hence I, hence L admits the translation r. If $p' \neq r$, K' admits the translations p' and q. Since r is again the greatest common divisor of p' and q and since the length of K' is at least $p' + q - r = p - r$, the induction hypothesis shows that K' admits the translation r. It follows as above that J, K, I and L have the same property. Q.E.D.

2.3. Corollary. *If the interval I has step q, each translation $p \leqslant \frac{1}{2}|I|$ of I is a multiple of q.*

Proof. Suppose indeed that I admits the translation p where $2q \leqslant 2p \leqslant |I|$. By the theorem above, I admits the translation r where r is the greatest common divisor of p and q, since its length is at least $p + q$. Since q is the step, one must have $q \leqslant r$, hence $q = r$ showing that p is a multiple of q. Q.E.D.

We spell out a (well known, cf. [15]) equivalent formulation in terms of words.

2.3 bis. *Assume that the word $a \neq 1$ satisfies an equation $ba = ab'$ where $b \neq 1$ and $|a| \geqslant 2|b| - 1$. There is a unique primitive word h such that $a = h^r h'$ with h' a prefixe of h and either $r \geqslant 2$ or $r = 1$ and $|h'| = |h| - 1$. Then b is a power of h.*

Proof. Let $a = Iw$ and apply 2.3. Q.E.D.

There is no confusion in writing $h = \sqrt{a}$ with the convention that $\sqrt{a} = a$ when the hypothesis of 2.3 bis are not satisfied. In the rest of this paper we shall say that an interval I is *periodic* iff, in equivalent fashion, $a \neq \sqrt{a}$ where $a = Iw$, or iff $|I| \geqslant 2\|I\| - 1$. It will be said to be *r-periodic* iff it satisfies the stronger condition $|I| \geqslant r\|I\| + 1$ and *long* iff it is 4-periodic. The same terminology will be applied to the words and, accordingly, a is a long periodic word iff $a = h^r h'$ with $r = 4$ and $h' \neq 1$ a prefix of h or $a = h^r$ with $r \geqslant 5$.

Let $I = (i, i')$ be a long periodic interval and p its step. Its *"internal*

zone" is the interval $(i + p - 1, i' - p + 1) = I^\circ$. Within it we distinguish the *"body"* $(i + 2p, i' - 2p)$, the *"left margin"* $I^g = (i + p, i + 2p - 1)$ and the *"right margin"* $I^d = (i' - 2p + 1, i' - p)$.

These notions are motivated by the next statements which allow to relate the geometry of the intervals with the study of syntactic monoids. For short we say that an index n is *covered three times by the word* y iff n is contained in three *distinct* intervals I, J and K such that $y = Iw = Jw = Kw$.

2.4. *A necessary and sufficient condition that an index* t *belongs to the body of some long interval* L *is that it be covered three times by a word* y. *If this condition is satisfied,* y *is 3-periodic and its step is the same as that of* L.

Proof. Assume that $L = (i, k')$ is a long interval whose body contains t. There exist a primitive word h of length $P = \| L \|$, a prefix h' of h and an integer $k \geqslant 4$ such that $Lw = h^k h'$. One verifies immediately that the conditions are satisfied by the intervals $I = (i, k' - 2p)$, $J = (i + p, k' - p)$, $K = (i + 2p, k')$ since their intersection is the body $(i + 2p, k' - 2p)$ of L and since the words Iw, Jw and Kw are all equal to $h^{k-2}h'$.

In the opposite direction assume that t is covered three times by y, the corresponding supports being $I = (i, i')$, $J = (j, j')$, $K = (k, k')$. We can assume that $i < j < k$ and we have then $k \leqslant t \leqslant i'$ since t must be contained in the intersection (k, i') of the three intervals. By construction J is contained in the union of I and K. Thus, by reason of symmetry, we can suppose that its intersection with I is at least as long as that with K, i.e. that the difference $q = j - i$ is at most equal to half the common length $|y|$ of I, J and K.

Let $L' = (i, j')$ be the union of I and J. The hypothesis $Iw = Jw$ entails that L' admits the translation q, which is strictly less than half the length of L'. Applying the theorem of Fine and Wilf and its corollary we conclude that L' is periodic and that its step p divides q. Since $2q$ is at most equal to $|y|$, the same is true of p and we have proved that y, hence I, J and K, are periodic with step p.

The intersection (k, j') of K with L' contains (i', j') since $k \leqslant t \leqslant i'$ and this last mentioned interval has length $q \geqslant p$. Using again the same theorem, we see that the union L of L' and K admits the translation p. In fact p is its step because p is the step of J. The relation $Jw = Kw$ implies that p divides the difference $k' - j'$, hence that $p \geqslant k' - j'$. This last inequality entails that the length of L is at least $4p$, i.e. that L is long and one checks easily that t is contained in the body of L. Q.E.D.

We introduce the term "complete" to express that a periodic interval $I = (i, i')$ is maximal among the sub-intervals of C containing it and having the same step p. This is equivalent to the hypothesis that $(i-1)w \neq (i-1+p)w$ and $(i'+1)w \neq (i'+1-p)w$. It is clear that any periodic interval I is contained in a complete interval I' (having the same step) and that I' contains any interval having the properties to admit a translation $p' \leqslant p$ and to contain I. I' is the *completion* of I; its body contains the body of I when I is long.

2.5. *Let I and $J \neq I$ be two complete long periodic intervals such that $\|J\| (= q) \leqslant \|I\| (= p)$ and that the body J° of J meets one of the margins I^x of I. Then $3q < p$ and I^x contains one of the margins of J.*

Proof. Let K be the intersection of I and J. Its length is at most $p + q - 2$. Indeed, otherwise, the union L of I and J would admit the translation $r \leqslant p, q$ by the theorem of Fine and Wilf, where $r = p$ and $r = q$ according to the definitions of q and p as the steps of J and of I. Therefore, one would have $p = q$, hence $L = I = J$ since I and J are supposed to be complete, in contradiction with our initial hypothesis that $I \neq J$.

This remark shows that I is not contained in J, since, otherwise, one would have $K = I$ where I has length at least $4p + 1$ (because it is long) giving the inequality $1 + 4p \leqslant p + q - 2$ which contradicts the hypothesis $q \leqslant p$. In similar fashion, one verifies that if J is contained in I one has $1 + 4q \leqslant p + q - 2$, hence $3q < p$.

Assume now that for instance the body $J^\circ = (j + 2q, j' - 2q)$ of

J meets the left margin $I^g = (i+p, i+2p-1)$ of I. Suppose also that the left margin $J^g = (j+q, j+2q-1)$ is not included in I^g. We have the inequalities $j+q \leqslant i+p \leqslant j+2q-1$ where $j+2q-1 \leqslant$ $\leqslant i+2p-1$ in view of $q \leqslant p$. It follows that the intersection K contains the interval $(j+2q, j+3q-1)$ which has length q. Also $i<j$ since, otherwise, K would contain the interval $(i, i+p-1)$ disjoint from the previous one, in contradiction to $|K| \leqslant p+q-2$. Accordingly, K contains the initial interval of length q, $(j, j+q-1)$ of J. Since $j+q<i+p$, the same inequality on the length of K entails that J does not contain the left margin I^g, i.e. that $J'<i+2p-1$ and this shows that I^g contains the right margin of J. Q.E.D.

Recall that the internal zone of a long interval is the union of its body with the two margins.

2.6. Periodicity lemma. *Let L' $(\neq \phi)$ be an interval such that any of its indices is covered three times by a word and assume that L' is maximal among the intervals having the same property. There exists a long periodic interval L whose body is contained in L' and whose internal zone strictly contains L'. The step of L is equal to the maximum of the steps of the intervals used to cover L'.*

Proof. According to 2.4, any index t of L' is contained in the body of a long interval L_t having step p_t. Choose t such that p_t be maximum and let L be the completion of L_t. By the same remark all the indices of L° are covered three times. Thus L° is contained in L' in view of the extremal character of L'. To conclude the proof it suffices to show that at least one index belonging to a margin of L is not in L'. We do this by showing that the opposite hypothesis on (say) L^g leads to the construction of an infinite nested family of periodic intervals, which is impossible.

Let t' be an index of L^g which belongs to L'. It can be choosen so that the corresponding step $p' = p_{t'}$ is maximum. By our initial hypothesis p' is not greater than p_t and the long interval $L_{t'}$ has a body meeting the margin L^g. The same is true of its completion L_1 and we have $L_1 \neq L$ since L is complete. Thus, by 2.5, one of the margins of

L_1 is contained in L^g and p' is strictly smaller than P_t. Again, if this margin of L_1 was to contain an index belonging to L', we could repeat the same construction obtaining a new long complete interval L_2 of step $p'' < p'$ which would have a margin contained in that of L_1, etc. Q.E.D.

The reader will notice that in the case of the monoid of functions alluded to in the introduction, the above proof does not go through without some supplementary assumption of "smoothness" forcing the conclusion at the end of the argument. The same remark applies to the second periodicity lemma.

In the next statements we say that an index n of the basic interval $C = (1, m)$ is *covered three times by the suffixes* of a word iff there exist three intervals $K = (1, k)$, $J = (j', j)$, $I = (i', i)$ such that $1 \leqslant j' \leqslant i' \leqslant$ $\leqslant n \leqslant k < j < i$ and that on the one hand the word Kw is a suffix of the word Iw and, on the other hand, either $Jw = Iw$ (in which case, of course, $i' - j' = i - j$) or Jw is a suffix of Iw and then $j' = 1$.

In similar fashion, we shall use the phrase *"covered three times by the prefixes"* to express the symmetric notion obtained when exchanging the indices 1 and m, the direction of the inequalities and the terms prefix and suffix.

2.7. *Let n be an index of C which is covered three times by the suffixes of a word. Then*

(1) *The initial interval $(1, i)$ admits the translation $d = i - j$.*

(2) *If there is a long periodic interval $H = (h', h)$ with $j \leqslant h$ such that its left margin contains n, the completion of H is an initial interval of C.*

Proof. The hypothesis that Jw is equal to Iw or to one of its suffixes implies that the interval (j', i) admits the translation $d\ (= i - j)$. Thus, (1) is proved when $j' = 1$. If it is not so, we must have $Jw = Iw$ hence $i' - j' = d$. Since Kw is a suffix of Jw, the interval $(1, j)$ admits the translation $d' = j - k$. The length of its intersection with J is at least $d + d'$ (because $i' \leqslant n < i$). According to the Fine – Wilf

theorem, J, hence the union $(1, i)$ of K, J and I are periodic with a step p dividing d and d'. This concludes the proof of (1).

Assume now that the hypothesis of (2) are fulfilled. We have just seen that $(1, j)$ admits the translation d'. The length of its intersection with H is at least $d + r$ where r is the step of H. Accordingly, as above, $(1, h)$ is periodic with a step r' dividing r and d'. Since r is the step of H, we must have $r \leqslant r'$. Thus $r = r'$, concluding the proof. Q.E.D.

2.8. **Second periodicity lemma.** *The basic interval $C = (1, m)$ is 3-periodic iff each of its indices is covered three times by a word or by the suffixes or by the prefixes of a word.*

Proof. The proof that this condition is sufficient proceeds in the same manner as above and it can be omitted.

Reciprocally, assume that the covering condition is fulfilled.

There is a largest index $k \geqslant 1$ that is covered three times by the suffixes of a word, the corresponding intervals being K, J, I as above. Symmetrically, there is a least index f that is covered three times by the prefixes of a word the corresponding intervals being $F = (f, m)$, $G = (g, g')$, $Q = (q, q')$ with $q < g < f \leqslant q' \leqslant g' \leqslant m$ (= the last index of C).

Suppose first that $g \leqslant j$. The intersection (q, i) of $(1, i)$ and (q, m) has length greater or equal $d + e$ where $d = i - j$ and $e = g - q$. Using the last result and the Fine – Wilf theorem, one concludes that their union (which is C) is periodic with a step r dividing d and e and one checks easily that in fact C is 3-periodic.

We can therefore suppose that $j < q$, an assumption which entails that no index in the non-empty interval (k, f) is covered three times by the prefixes or the suffixes of a word. Since each of them must be covered three times anyway, we can use the first periodicity lemma to establish the existence of a long periodic interval H whose internal zone strictly contains (k, f). If r is its step, this quantity is also the length of its margins. It follows that H has an intersection of length at least $r + d$

(resp. $r+e$) with the interval $(1,i)$ (resp. with (q,m)) and the desired conclusion is obtained as above. Q.E.D.

Taking a 5 letters alphabet $A=\{a,b,c,d,e\}$ and letting $x=abc$; $u=xdxdx$; $v=dxexd$, the example of the word $w=c(vu)^3va$ $(=Cw)$ shows that the hypothesis of the lemma do not imply that w is long.

Various other applications of the theory of Fine and Wilf can be found in the literature (cf. [13], [15] and [5]). We record here two simple observations for later reference.

2.9. *Let T be a non-empty subsemigroup of A^+. Each of the following conditions implies that it is contained in a cyclic subsemigroup h^+ of A^*.*

(i) *For some $\epsilon>0$, any word w in T has a periodic factor w' of length $|w'|\geqslant\epsilon|w|$.*

(ii) *There are words f,f' such that $ft^+t'^+f'$ contains a non-primitive word for any t,t' in T.*

In (ii) *there are h',h'' satisfying $h'h''=h$ or $=1$ such that f is in $h''\cdot h^*$ and f' in $h^*\cdot h'$.*

Proof. Take in T a fixed t which can be assumed to be a power $t=h^r$ of a primitive word h.

For (i) let u be any word in T and consider the word

$$w=t^2u^2t^3u^3\ldots t^ku^k\ldots t^nu^n$$

where n is large enough for t^n and u^n to have both a length less than $\frac{1}{8}\epsilon|w|$. Then any periodic factor w' of w of length $\geqslant\epsilon|w|$ has the form $gt^ku^k\ldots t^{k'}u^{k'}g'$ with $k'\geqslant k+2$. The hypothesis that it is periodic implies that t^ku^k is (equal to) a factor of $t^{k''}u^{k''}t^{k''+1}u^{k''+1}$ where $k\leqslant k''\leqslant k'-1$. Replacing t by h^r and using the hypothesis that h is primitive shows that u must also be a power of h and it establishes the result.

For (ii) we can assume that t is longer than f and f'. Take now

any power t' of an arbitrary word of T and choose it so that its length satisfies the same condition as that of t. The existence of a non-primitive word $w = ft^k t'^{k'} f'$ implies as above that w is a power of a word conjugate with h and the result follows by identifying the initial and final factors f and f'.

3. THE MONOID OF INTERPRETATION

In this section and in the next one we consider a fixed non-empty subset X of the free semigroup $A^+ = A^* \setminus 1$ and we assume that it is the minimal generating set of X^+, i.e. that its intersection with X^+X^+ is empty. The set $X(A^+)^{-1}$ (resp. $(A^+)^{-1}X$) of its prefixes (resp. suffixes) will be denoted by P (resp. by Q). We also consider another alphabet B and a bijection α of B into X which is extended to a morphism into A^* of the free monoid B^*.

An *interpretation* of a word a in A^* is a triple $y = (q, b, p)$ in $Q \times B^* \times P$ such that $a = q \cdot b\alpha \cdot p \ (= y\alpha)$ and $a\beta$ will be the set of the interpretations of a. Thus, $(1, 1, 1)$ is the only interpretation of the neutral element 1 of A^* and no other word admits it as an interpretation.

In the following definitions, a (resp. b, p, q) denotes an arbitrary element of A^* (resp. of B^*, P, Q); c is either a letter of B or the neutral element 1.

$[p, a] = pa$ if pa is in P and $= \phi$ otherwise;

$[a, q] = aq$ if aq is in Q and $= \phi$ otherwise;

$[p, q] = c$ if either $p = q = 1$ or $p, q \neq 1$;
$pq = c\alpha$; and $[p, q] = \phi$ otherwise.

Also we use the following Boolean matrices:

C = the $P \times Q$ matrix such that its (p, q) entry is 1 iff $[p, q] \neq \phi$;

$a\pi$ = the $P \times P$ matrix such that its (p, p') entry is 1 iff $pa = p'$;

$a\chi =$ the $Q \times Q$ matrix such that its (q', q) entry is 1 iff $aq = q'$;

$a\gamma =$ the $Q \times P$ matrix such that its (q, p) entry is 1 iff a admits an interpretation of the form (q, b, p) for at least one word b.

$a\mu = C \cdot a\gamma + a\pi$.

The only reason for using Boolean matrices instead of (binary) relations is typographic convenience.

A simple remark allows connecting the product on A^* with one on the set of interpretations.

3.1. *For any two words a and a' the set of interpretations of aa' is the union over all the interpretations $y = (q, b, p)$ of a and $y' = (q', b', p')$ of a' of their product*

$$yy' = (q, b, [p, a']) + (q, b \cdot [p, q'] \cdot b', q') + ([a, p], b', p').$$

Proof. It follows immediately from the definitions that each term written is an interpretation of aa' or ϕ.

Reciprocally, consider an interpretation $y'' = (q'', b'', p'')$ of aa'. When $a' = 1$, it is also an interpretation of a and it appears in the product since $y'' = (q'', b'', [p'', a'])$. A symmetric remark applies when $a = 1$ and we assume henceforth that $a, a' = 1$.

If the word a has a length $|a|$ greater of equal that of $q'' \cdot b''\alpha$, there is a prefix p such that $y = (q'', p'', p)$ is an interpretation of a. One has $[p'', a'] = p''$ showing that $y'' = (q'', b'', [p, a'])$ is in the product. The same holds if $|a| \leqslant |q''|$ because this inequality is equivalent to $|b''\alpha \cdot p''| \leqslant |a'|$. In the remaining case there is a factorization $b'' = bcb'$ with $[p, q'] = c$ such that $a = q'' \cdot b\alpha \cdot p$. Then $y = (q'', b, p)$ and $y' = (q', b', p'')$, are interpretations of a and of a' whose product contains y''. Q.E.D.

We recall that the *residual* of a subset K of any monoid T is the set of all t in T such that K does not meet the ideal TtT. Therefore

it is always an ideal (possibly empty). It is clear that when T is the free monoid A^* and when X is finite the residual of X contains all the words longer than its longest element. We summarize the properties of μ which will be needed later.

3.2. *The mapping μ is a morphism. It recognizes X^*. Further:*

– *for any word a the (p,p) entry of the matrix $a\mu$ is 1 iff a has an interpretation of the form (q,b,p) for some suffix q such that $[p,q] \neq \phi$;*

– *if one of the words a and a' is in the residual of X, one has $(aa')\mu = a\mu \cdot a'\mu$;*

– *the residual of X^* is the inverse image of the zero $P \times P$ matrix.*

Proof. It is clear that π and χ are two morphisms and that they reduce to 0 on the residual of X. They satisfy the intertwinning identity $a\pi \cdot C = C \cdot a\chi$ because $C(pa,q) = C(p,aq)$ for any a,p,q.

The formula given for the product of interpretations translates into the identity

$$(aa')\gamma = a\gamma \cdot a'\pi + a\gamma \cdot C \cdot a'\gamma + a\chi \cdot a'\gamma.$$

Multiply it on the left by C and add $(aa')\pi = a\pi \cdot a'\pi$ to both members. Since $C \cdot a\gamma \cdot a'\gamma = a\pi \cdot C \cdot a'\gamma$, one can regroup terms and one obtains the identity $(aa')\mu = a\mu \cdot a'\mu$ which establishes that μ is a morphism.

It is clear that $1\pi = 1\mu$ is the unit $P \times P$ matrix and that every diagonal entry of $a\pi$ is 0 when $a \neq 1$. Thus, for a in A^+, the (p,p) entry of $a\mu$ is 1 iff there is a q such that $C(p,q) = a\gamma(q,p) = 1$, which is the result stated because of the definition of C and of γ. Also $(aa')\mu = C \cdot a\gamma \cdot C \cdot a'\gamma = a\mu \cdot a'\mu$ when a or a' is in the residual of X since then the matrix $a\pi$ or $a'\pi$ is 0.

Consider now the entry $(1,1)$ of $a\mu$. It is 1 when $a = 1$. When $a \neq 1$ it is 1 iff there is a suffix q such that $[1,q] = 1$ and that a has an interpretation of the form $(q,b,1)$. The first condition implies that

$q = 1$ and then, the second is equivalent with $a \in X^*$. Thus μ recognizes X^*.

Suppose that the (p, p') entry of $a\mu$ is 1. There is a suffix q' such that $p'q'$ is in X, if $p' = 1$ and that $p'q' = 1$ otherwise. In both cases paq' is in X^* as we have just seen and, consequently, a is not in the residual of X^*. In the opposite direction, if $a\mu$ is 0, no matrix $(a'aa'')\mu$ can have its $(1, 1)$ entry equal to 1 and a is in this residual. Q.E.D.

It may be mentioned that X^* is also recognized by γ since the $(1, 1)$ entry of $a\gamma$ is 1 iff a has an interpretation of the form $(1, b, 1)$, i.e. iff it is in X^*. The formula given in the preceding proof shows that the restriction of γ to the residual of X is a morphism with respect to the "sandwich" multiplication $(aa')\gamma = a\gamma \cdot C \cdot a'\gamma$. For the whole of A^*, the mapping (π, γ, χ) is a morphism (with the indicated product for γ).

We call $M = A^*\mu$ *the monoid of interpretations* of X^*. The syntactic monoid S of X^* is a quotient of M in view of the minimal character of S and of the fact that μ recognizes X^*. The reader will notice the relationship between M and the left to right non deterministic automaton realizing the relation from B^* to A^* which is the inverse of the morphism α.

When X is finite the same is true of P, hence of M. It is a known fact that under this hypothesis every group in S is a quotient of a group in M. The same holds when X is a recognizable set in the sense of S. Eilenberg but we shall not make use of this generalization.

These notions are illustrated by the following example which shows that except in a very special case the morphism μ also recognizes $\{1\}$, hence the semigroup X^+.

Example. A necessary and sufficient condition that $w\mu = 1\mu$ for some $w_1 = w \neq 1$ is the existence of $d \geqslant 1$ and a letter a such that X consists of a^d and of words of the form $a^{d'}a'$ with $d' \leqslant d - 1$ and a' a letter different from a.

Reciprocally, if X has this form, M has a subgroup of order d whose inverse image is a^* and w_1 is a power of a^d.

Proof. Assume first that X has the form indicated. The set of the prefixes P consists of the words $a^{d'}$ with $d' \leqslant d-1$. The matrix $a\pi$ has a 1-entry for the pairs $(a^{d'}, a^{d'+1})$ where $d'+1 \leqslant d-1$. One has $C(p,p')=1$ iff $p=p'=1$ or if $p,p' \neq 1$ and $pp'=a^d$. Since the only interpretations of a are $(a,1,1)$ and $(1,1,a)$ one sees that $a\mu$ is the cyclic matrix m obtained when adding the 1-entry $(a^{d-1},1)$ to $a\pi$. For any other letter a' and prefix p, the line p of a' is zero if pa' is not in X and it has a single 1-entry in the column 1 otherwise. This shows that the condition is sufficient and that the *subgroup* of M (i.e. the maximal group in M whose idempotent is 1) has the properties stated.

In the opposite direction, assume $w \neq 1$ and that the matrix $w\mu$ contains 1μ, i.e. that all its diagonal entries are 1. As we have seen it, this implies that w is in X^* and that it has an interpretation (q,b,p) for each prefix p in P. Thus, if a is the last letter of w, it is also the last letter of any prefix p and since P contains every left factor of its members we see that it consists of the powers a^k of a for $k \leqslant d-1$ where d is the length of the longest word in X.

Consider the prefix $p=a^{d-1}$. Since $w(p,p)=1$ there is a suffix q such that $[p,q] \neq \phi$ and $w=qxp$ for some x in X^*. The first relation implies $q \neq 1$ and the maximal character of d that q is the first letter of w. Since w is in X, this letter is a prefix in P, hence it is a, proving that X contains the word a^d. It follows, as above, that $a\mu$ contains the cyclic matrix m.

Assume now that $w\mu = 1\mu$. It is in the subgroup of the monoid of the $P \times P$ Boolean matrices. Thus $a'\mu$ is a permutation matrix for any letter a' which is a factor of w, hence in particular for a (since a is the first letter of w). It follows that a^d is the only power of a which is in X because a^k in X implies that the $(a^{k-1},1)$ entry of $a\mu$ be 1. This shows that X has the form indicated and computing $a'\mu$ for a letter $a' \neq a$ establishes that it is not a permutation matrix. Thus, w is a power of a^d. Q.E.D.

We recall that a $P \times P$ matrix m has finite *rank* $\leqslant r$ iff there is a subset K of at most r elements of P such that m admits a factorization $m = m'hm''$ where m' (resp. m'') is a $P \times K$ (resp. $K \times P$) matrix and h a $K \times K$ matrix. If it is so, all the matrices in the ideal MmM have the same property and, more accurately, it is isomorphic to a semigroup of $K \times K$ matrices. These notions apply as well to the case of the Boolean matrices with which we are concerned here.

3.3. *A necessary and sufficient condition for the monoid of interpretations M to have a 0-minimal ideal completely 0-simple and a finite Suschkewitsch group G is that X and X^* have different residuals.*

Proof. Since X is contained in X^*, its residual contains the residual of X. Thus, if these two residuals are not equal we can find a word w in X^* which belongs to the residual of X. Suppose it is so and consider an interpretation (q, b, p) of w. One has $b \neq 1$ or $p, q \neq 1$ and the matrix $w\pi$ is 0. It follows instantly that the matrix $a\mu = C \cdot w\gamma + w\pi$ has a rank at most equal to the length of w. Thus $M \cdot w\mu \cdot M$ is an ideal not reduced to 0 in which all the matrices have a finite rank. This shows that M has a completely 0-simple 0-minimal ideal. Taking w such that $w\mu$ has a minimal rank, the bi-ideal wMw is finite and it is isomorphic to the group G. This proves that the condition stated is sufficient. Since the syntactic monoid of X^* is a quotient of M we see that it also enjoys the same property.

Reciprocally, suppose that M has a 0-minimal completely 0-simple ideal $D' + 0$ and that the group G' is finite. This is also true of the syntactic monoid S and we denote the corresponding objects by D and G. We can assume that G meets the image of X^* in S. Since G is finite and X^* is a semigroup, the idempotent u of G belongs to the image of X^*. Since D is 0-simple, there is a subgroup H of G, a union R of $\mathscr{R}$-classes of D and a union L of $\mathscr{L}$-classes of D such that the intersection E of D with the image of X^* is the set of all the elements d belonging to R and L which satisfy $udu \in H$.

We now construct a finite sequence $(g_0 = u, g_1, \ldots, g_n)$ of ele-

ments of G having the property that for any g in G one has $u = gg_0g_1 \ldots g_i$ for at least one index i. This is possible since G is a finite group.

Also, for each g_i, we take a word $a_i \neq 1$ in its inverse image. Having selected g_n so that $g_0g_i \ldots g_n = u$, the product $w = a_0a_1 \ldots a_n$ is in X^2X and we have only to verify that it belongs to the residual of X.

Suppose to the contrary that awa' is in X for some pair of words a and a', and let, for an arbitrary i, d and d' be the images of the words $aa_0 \ldots a_i$ and $a_{i+1} \ldots a_na'$. Since D is 0-simple, d and d' belong to the intersection of R and of L and the same is true of udu and $ud'u$. Further $udd'u = uduud'u$ is in the subgroup H. Choose i in such a way that $udu = u$. We have also $ud'u$ in H and, accordingly, d and d' both belong to the image E of X^* in D. This shows that $aa_1 \ldots a_i$ and $a_{i+1} \ldots a_n$ belong to X, and, in fact, to X^+. Thus awa' is in X^+X^+, in contradiction with our initial hypothesis that X is disjoint from this set (because we assumed that X was a minimal generating set). Q.E.D.

From now on we shall let W denote the set of the words which belong to the residual of X and not to that of X^*. It is clear that if X is finite, W contains every long enough word which is not in the residual $0\mu^{-1}$ of X^*.

3.6. *Every element g in M such that the intersection W_g of its inverse image with the residual W is not empty, has a finite order (i.e. it has a positive power which is idempotent).*

Proof. Take a word w in W_g and let P' (resp. Q') be the set of the prefixes (resp. suffixes) which can appear as the prefix (suffix) component of one of its interpretations. It is a finite set since the lengths of its elements is bounded by the length of w. Further, P' and Q' contain the corresponding sets for any positive power w^n because w is in W. Therefore any non zero entry of the matrix $w^n\gamma$ is in its $Q' \times P'$-part. It follows that the number of different matrices $w^n\gamma$ is bounded in function of the number of elements of P' and Q'; the same applies

to the matrices $w^n\mu = C \cdot w^n\gamma$ etc. The rest of the argument is a classical one. Q.E.D.

If u is an idempotent, we let G_u denote the (necessarily unique) maximal group containing it. We say that u (or G_u) is *strongly cyclic* iff its inverse image does not reduces to $\{1\}$ (i.e. if it meets A^+) and it is contained in a cyclic submonoid of A^*, that is, in a submonoid generated by a single word.

3.5. *Assume that u is a strongly cyclic idempotent. Then:*

– *there is a unique primitive word h called the root of G_u, such that the inverse image of G_u is contained in h^*;*

– *G_u is a finite cyclic group and MuM is a maximal principal idempotent ideal or M itself depending upon whether $u \neq 1$ or not;*

– *the conjugacy class of G_u consists of groups having the same properties; the corresponding roots are the words conjugate with h;*

– *there is at most* Card (X) *conjugacy classes of such groups such that their root h has the following further property: there is a word x in X of length $|x| = 2|h| - 1$ or $= |h|$ which is a factor of a word in h.*

Proof. Since the inverse image of u is an infinite semigroup, we can apply 2.9 to conclude to the existence of a unique primitive word h such that it is contained in h^*. The fact that the inverse image of G_u is contained in the same cyclic submonoid follows from the observation that the inverse image of u meets a^nA^* for any n and any word a in the inverse image of G_u. It is then a classical exercise to show that G_u is a finite cyclic group. The last assertion of 2.9 shows that MuM is contained in MvM where $v = v^2 \neq 1$ iff the inverse image of v is contained in the cyclic submonoid generated by a word conjugate with h. Thus MuM is maximal (as a proper principal idempotent ideal of M) unless $u = 1$.

Suppose now that the root h and the word x satisfy the supplementary conditions stated. There is a unique word h' conjugate with h

which is a prefix of x. Returning to the notions developped as the beginning of Section 2, we see that in fact one has $h' = x$ since h' is primitive, and since either $h' = x$ of $h''h''$ with the inequality on the lengths stated. This provides an injection into X of the corresponding classes. Q.E.D.

For later reference we call *special* the strongly cyclic idempotents (or their maximal groups) satisfying the supplementary condition at the end of 3.5.

Let us recall that if u is an idempotent $P \times P$ (Boolean) matrix there exists a maximal partial equivalence relation, noted $\hat{u}$, on P whose support is contained in u (i.e. which is such that the (p, p') entry of u is 1 for every pair (p, p') in $\hat{u}$). Its proper domain will be noted P_u. One knows that a group in M having u as its idempotent is a permutation group on the $\hat{u}$-classes of P_u. Therefore its degree, $\deg(u)$, is the number of these classes. It is zero iff $u = 0$.

To do this we consider an interpretation $y = (q, b, p)$ of a word w and we say that it is *repeatable* iff $[q, p] \neq \phi$, this implies that any positive power of w has an interpretation having the same suffix and prefix components, q and p, as y. Another interpretation $y_2 = (q_2, b_2, p_2)$ of w is *linked* with y iff there are factorizations $b = b'b''$ and $b_2 = b_2' b_2''$ such that the words $q \cdot b'\alpha$ and $q_2 \cdot b_2'\alpha$ have the same length; otherwise, y and y_2 are *separated.*

The following observations supply the connection between the Fine – Wilf theory and its applications in the next section.

3.6. *Assume that the maximal group $G = G_u$ has an element g whose inverse image has a non empty intersection W_g with the residual W. Then, if G is not strongly cyclic, every W_g contains an infinity of primitive words. In any case:*

– *every word in W_u is conjugate with a word in X^*;*

– *any word w in W_u admits a system of $d = \deg(u)$ pairwise separated repeatable interpretations; further, for any two of them, say*

y_1 *and* y_2, *there is no chain* $(y_1, y_2, \ldots, y_n)$ *of interpretations of* w *such that each* y_i *is linked with* y_{i+1}.

Proof. Assume w' in W_g. The ideal $A^*w'A^*$ meets W_u since g has an inverse. Thus W_u is a non empty semigroup. Assuming for a moment that u is not strongly cyclic the assertions concerning the primitive words follow from 2.9.

Consider a word w in W_u and a prefix p such that the (p,p) entry of the matrix u is 1. Since w is in the residual of X we know that this is equivalent with the existence of an interpretation $y = (q, b, p)$ of w such that $[p, q] \neq \phi$. The word $b\alpha \cdot pq$ is conjugate with w and it is in X^* by construction, proving the second assertion.

Let $y_2 = (q_2, b_2, p_2)$ be another interpretation of w and suppose that it is linked with y. Using the same notations as above we see that w admits the interpretations $(q, b'b_2'', p_2)$ and $(q_2, b_2'b'', p)$. Therefore the entries (p, p_2) and (p_2, p) of u are 1 and the same is true of the entry (p_2, p_2) since u is idempotent. We conclude that the class of the prefix p in the equivalence $\hat{u}$ contains any prefix which is linked with it in this manner and the truth of the last assertion follows. Q.E.D.

4. APPLICATIONS

We come to the proof of the main results stated in the introduction. To simplify we make the standing assumption that the generating set X of X^* has a finite number $k \geqslant 2$ of words and that it has not the very special from displayed in the example of the last section. Letting L denote the maximum of the lengths of the words of X, we have that the inverse image $u\mu^{-1}$ of any idempotent u in the monoid of interpretations M has an intersection W_u with the residual W of X that is an infinite semigroup and that W contains $A^L A^+$.

We recall the notion of a *special group* in M introduced in 3.5 and that the number of their conjugacy classes is at most k. By 3.6 and the finiteness of the complement of W every conjugate class of groups in M has a member such that its idempotent is in the image of X^*.

4.1. *Any idempotent* $u \neq 1$ *of degree* $2k+1$ *or more is special.*

Proof. Let $u = u^2 \neq 1$ have degree $d \geqslant 2k+1$ and take any primitive word h having a power h^r in its inverse image. We can choose r large enough for the length m of $w = h^r$ to satisfy the inequality $m \geqslant 2L + 4|h|$.

As explained in the beginning of Section 2 we consider w as a mapping in A of the basic interval $C = (1, m)$. Let j be any index in the sub-interval $L' = (L+1, m-L)$. By 3.4 we know that w has a system Y of d pairwise separated repeatable interpretations. If $y = (q, b, p)$ is any one of them, our choice of j implies a factorization $b = b'cb''$ where the support I_y of c contains j, i.e. where $c\alpha$ is a word x_y of X and where $|q \cdot b'\alpha| < j \leqslant |q \cdot (b'c)\alpha|$. Since $d \geqslant 2k+1$ there are three interpretation for which the word x is the same. Therefore our hypotheses imply that every index in $(L+1, m-L)$ is covered three times. Applying the First Periodicity Lemma of the Fine – Wilf theory, we conclude that it is a long periodic interval. By the same lemma its step p is the step of one of the covering words x in X. Further, L' admits the translation $|h|$ because of our choice of the exponent r. Applying once more the Fine – Wilf theory we conclude that the length of h is exactly p since it is a primitive word. The conclusion follows from 2.9 since it applies to any word h having a power in $u\mu^{-1}$. Q.E.D.

Observation. For each word x in X let $r(x)$ be 0 if x is not a factor of a word of h^*. In the opposite case, let $r(x) = 2$ if $|x| \leqslant 2|h|$ and $r(x) = p$ if $p \geqslant 3$ is the least integer such that $|x| \leqslant p|h|$. Since every index j can be covered three times by a word x only if $r(x) \geqslant 3$, one sees that the degree d is at most equal to the sum of the numbers $r(x)$.

4.2. **Corollary.** *Apart from at most* k *conjugate classes of maximum cyclic groups that generate maximal idempotent principal ideals, every group in the monoid of interpretations or in the syntactic monoid of* X^* *divides the symmetric group of order* $(2k)!$.

Proof. This is just a reformulation of the previously established result since every group in S is a quotient of a group in M. Q.E.D.

From now on, we let U denote the set of the idempotents $u \neq 0, 1$ which are not special, and we proceed with the proof of other absolute finiteness properties concerning the ideal MUM. If R is a subset of P, let e_R denote the idempotent diagonal $P \times P$ matrix such that its entry (p, p') is 1 iff $p = p'$ is an element of R. A pair (F, F') of subsets of A^+ will be said to be a *R-factorization* of the subset K of M iff:

(i) $F = A^*F$, $F' = F'A^*$ and K is contained in the image of FF' by μ;

(ii) For any f in F and f' in F', one has $(ff')\mu = f\mu \cdot e_R \cdot f'\mu$.

To motivate this notion we apply it in the following remark.

4.3. *Assume that (F, F') is a R-factorization of an ideal K. The number of idempotent principal ideals in K is at most 2^n where $n = (\text{Card } R)^2$.*

Proof. Consider an idempotent u in K and a R-factorization (f, f') of u. Since $u = u^3$, one has $u = (ff'ff'ff')\mu$. The matrix $m_u = (f'ff'f)\mu$ generates the same ideal as u since it is contained in MuM and since u is in Mm_uM.

Because of condition (ii) and of the fact that F is a left ideal and F' a right one, we have also $u = f\mu \cdot m'_u \cdot f'\mu$ where $m'_u = e_R \cdot M_u \cdot e_R$.

Let now v be another idempotent in K and m_v and m'_v the corresponding matrices. Suppose further that $m'_u = m'_v$. Again by (ii) we have $u = f\mu \cdot m'_u \cdot f'\mu = f\mu \cdot m'_v \cdot f'\mu = f\mu \cdot m_v \cdot f'\mu$ showing that u is in MvM since m_v is in MvM. By symmetry, $Mum = MvM$. The result follows since the number of classes for the equivalence defined by $m'_u = m'_v$ is certainly less than the number of Boolean $R \times R$ matrices. Q.E.D.

For each word x in X let $U(x)$ denote the set of the idempotents u in U which have the property that x has a maximum length among the words x' in X such that MuM is contained in the image of $Ax'A$, i.e. among the x' which are a factor of at least one word in the inverse

image of u. It is clear that we can find a minimal subset X_0 of X such that U is the union of the sets $U(x)$ over all x in X_0.

Let now x be any fixed element of X_0. We construct a subset $R = R(x)$ of P and a R-factorization of $MU(x)M$. Since this is slightly complicated by the possibility that x can be a 3-periodic word (in the sense given to this expression in Section 2), we break it into several steps before proving that it has the desired properties.

Construction.

(1) If x is not 3-periodic we consider it as a mapping in A of its basic interval $(1, m)$ where m is its length. In view of the Second Periodicity Lemma we can select an index j in $(1, m)$ which is not covered three times (understood, by a word, or by the suffixes or by the prefixes of a word).

In the opposite case, $x = h^r h_1$ where $r \geqslant 3$, $h = \sqrt{x}$ is a primitive word of length n equal to the step of x and h_1 is a prefix of h. Consider first $w = h^2$ as a mapping of its basic interval $(1, 2n)$. The word w is periodic but since h is primitive it is not 3-preiodic. Thus, as above, we can choose an index j' in $(1, 2n)$ which is not covered three times. Returning to x and to its basic interval $(1, m)$, we let $j = j'$ or $= j' + n$ depending upon whether $j' \geqslant n$ or not. Thus, in both cases $n < j \leqslant 2n$.

(2) An interpretation (q, b, p) of x is *acceptable* iff p is a prefix of at least one word in the subset X' of the words of X which are not strictly longer than x and the symmetric conditions hold for q. When x is 3-preiodic we impose the further restriction that q is a suffix of at least one word from the subset X'' of the words x'' of X' which have the form $x'' = p'q$ with $|p'| < n\ (= |h|)$ or $p' = p''h''$ where h'' is any word of length n different from h.

(3) Let $y = (q, b, p)$ be an acceptable interpretation of x. It can be of three types depending upon the position of j with respect of the supports of p and of q. In each case we select a subset P_y of P.

Type X. $|q| < j \leqslant |q \cdot b\alpha|$. There are factorizations $b = b'cb''$ and $c\alpha = p_y q_y = x_y$ such that x_y is a word of X and $j = |q \cdot b\alpha \cdot p_y|$. if $q_y \neq 1$ we let $p_y^X = \{p_y\}$; otherwise, $p_y = x_y$ and we let $p_y^X = \{1\}$.

Type P. $|q \cdot b\alpha| < j$. Then $P_y^p = \{p_y\}$ where this word is the left factor of p such that $|q \cdot b\alpha \cdot p_y| = j$.

Type Q. $j < |q|$. Let $q = aq_y$ where a has length j. Then P_y^Q is the set of all prefixes p' of the form $p' = p''a$ which are such that $p'q_y = x_y$ is a word of X'' or of X' depending upon x whether it is or not 3-periodic.

For $T = X$, P or Q we let P^T denote the union of the sets P_y^T over all the acceptable interpretations of x and $R = R(x)$ be the union of the P^T's.

(4) Let $x = zz'$ where z has length j. We let $F' = F'(x)$ be the right ideal $z'A^L A^+$ where, we recall, L is the maximum of the length of the words in X. If x is not 3-periodic, $F = F(x) = A^+ A^L z$. If it is, we replace in the definition of F the set A^L of all words of length L by $A^L \setminus A^* h$, i.e. by the set of the words of the same length such that their suffix of length n is not the word h defined in (1) above.

This concludes the construction.

4.4. *The pair* (F, F') *is a* R*-factorization of* $MU(x)M$.

Proof. Let u be any idempotent in $U(x)$. There are arbitrary long words g, g' such that $w = gxg'$ is in its inverse image. Thus we can take $z'g'$ in F' and, when x is not 3-periodic, gz in F. In the opposite case let W'' be the set of all g'' such that $g''xg'$ is in the inverse image of u. It contains a suitable g unless all its members have the form $g_1 h'^s$ with $s \geqslant 0$, $h' = \sqrt{x}$ and $|g_1| < |h| = |h'|$. However, in view of $u = u^2$, the set W'' contains wW''. Therefore such a possibility could arise only if there were a factorization $h' = h''h'''$ for which xg' were in $h'h''$ and W' a subset of $h'''h'^*$. This is excluded by the initial hypothesis that u is not special. Thus we can always take gz in F.

Let $y_1 = (q, b_1, p)$ be an interpretation of gxg'. Because of the hypothesis upon the lengths of the words in X involved, one sees that there are interpretations $y = (q, b, p')$ of gz and $y' = (q', b', p)$ of $z'g'$ such that $y_1 = yy'$, i.e. $b_1 = b \cdot [p', q'] \cdot b'$ and one checks readily that p' is in R.

It follows that all the $P \setminus R$ columns of the matrix $(gz)u$ are identically zero, i.e. that $(gz)u = (gz)\mu \cdot e_R$.

The same holds for any matrix m in MuM since it has the form $m'um''$ for suitable m', m''. Q.E.D.

4.5. *The set R has less than $6k^2$ elements.*

Proof. Consider first the case when x is not 3-periodic.

Since the index j is not covered three times by a word, each x' in X' can appear at most twice as the word x_y in an interpretation y of z of type X. Each times it supplies one prefix to P^X and, consequently, this set has at most $2k$ elements. In the same manner, since j is not covered three times by the prefix of a word, each x' can have at most two different prefixes which appear as the prefix term of an interpretation of type P. Thus, Card $(P^P) \leqslant 2k$.

If q is the suffix term of an interpretation y of type Q the corresponding set P_y^Q has at most k elements since for any two of them, p' and p'', the words $p'q$ and $p''q$ are different. Because j is not covered three times by the suffixes, the number of interpretations of type Q is $\leqslant 2k$.

Consequently, $6k^2$ is a generous bound for R.

Assume now that $x = h^r h_1$ is 3-periodic.

Since j is not covered three times as a member of the interval $(1, 2n)$, we see as above that the total contribution to R of the k' words of X of length less than $2n$ is inferior to $6k^2$. Consider now a word x' of X' of length $2n$ or more. There are three mutually exclusive possibilities:

– $x' = h'^s h'_1$ where h' is conjugate with h, h'_1 is a prefix of h' and $s \geqslant 2$;

– $x' = h'^s t$ with h' as before, $s \geqslant 0$ and $t \neq 1$ not a prefix of h';

– symmetrically, $x' = t h'^s$ with $t \neq 1$ not a prefix of h'.

The last two cannot participate in interpretations of type X. In the first one, the fact that h' is conjugate with $h = \sqrt{x}$ entails the existence of fixed words a, a' such that any factorization of x involving x' has the form $x = h^{s'} a x' a' h^{s''} h_1$ $(s', s'' \geqslant 0)$. Because of $n < j \leqslant 2n$ we see that x' can be a word x_y in a type X interpretation only if $s' = 0$ or 1. Thus, the corresponding contribution to P^X of these words x' is at most twice their number k'.

A similar argument applies for the interpretations of type P and, again, the only words involved belong to one of the first two categories. For the type Q, the word x' must belong to the first or third category. Because of our restriction to acceptable interpretations, it can supply at most one suffix term. Thus its contribution to P^Q is at most $k - k'$ by the same observation as in the initial non periodic case and we conclude that R has less than $6k'^2 + 6(k - k')^2$ elements when x is 3-periodic. Q.E.D.

4.6. *The number of conjugacy classes of maximal groups in M (or in S) is absolutely finite.*

Proof. There is at most k special classes and, for the other ones, the result follows from the last three Remarks 4.3, 4.4 and 4.5, since MuM is the union of the $k'' \leqslant k$ ideals $MU(x)M$.

4.7. *For any two elements m, m' of MUM the bi-ideal mMm' is absolutely finite.*

Proof. We have m in $MU(x)M$ and m' in $MU(x')M$ for words x, x' of X. Therefore, by the preceding remarks, there are subsets R and R' of P having less than $6k^2$ elements and matrices m_i such that $m = m_1 e_R m_2$ and $m' = m_3 e_R m_4$. Each element of the bi-ideal has the

form $mm''m'$, hence $m_1 m_5 m_4$ where $m_5 = e_R m_2 m'' m_3 e_R$, has all its non zero entries in $R \times R'$ and, accordingly, it belongs to an absolutely finite set. Q.E.D.

* * * * * * * * *

Let us thank A. Lentin, pioneer of this subject, whose friendly vigilance has preserved me from many mistakes.

REFERENCES

[1] Al.A. Markov, On finitely generated subsemigroups of a free semigroup, *Semigroup Forum,* 3 (1971), 251-258.

[2] Y.I. Khmelevski, *Equations in free semigroups,* Proc. Steklov Inst., 107 (1971) (in Russian).

[3] S.I. Adjan, *Definition relations and algorithmic problems for groups and semigroups,* Proc. Steklov Inst., 85 (1966) (in Russian).

[4] A. Spehner, Quelques problèmes d'extension de conjugaison et de présentation des sous-monoïdes d'un monoïde libre, Thèse Paris (1976).

[5] A. Lentin, *Equations dans les monoïdes libres,* Gauthier-Villars, Paris (1972).

[6] S. Eilenberg, *Automata languages and machines,* Vol. A, Academic Press, N.Y. (1975).

[7] R. Croisot, Equivalences principales bilatères définies dans un demigroupe, *J. Math. Pures Appl.,* (9) 36 (1957), 373-417.

[8] J-F. Perrot, Contribution à l'étude des monoïdes syntaxiques et de certains groupes associés aux automates finis, Thèse, Paris (1972).

[9] J-F. Perrot, Groupes de permutations associés aux codes préfixes finis, in *Permutations,* Gauthier-Villars, Paris (1972), 201-235.

[10] D. Perrin, La transitivité du groupe d'un code bipréfixe fini, *Math. Zeitschrift,* 153 (1977), 283-287.

[11] D.D. Miller – A.H. Clifford, Regular *D*-classes in semigroups, *Trans. Amer. Math. Soc.,* 82 (1956), 270-280.

[12] O. Steinfeld, Über die quasi-ideale von Halbgruppen, *Publ. Debrecen,* 4 (1956), 262-275.

[13] N.J. Fine – M.S. Wilf, Uniqueness theorem for periodic functions, *Proc. Amer. Math. Soc.,* 16 (1965), 109-114.

[14] J.D. McKnight – J.A. Storey, Equidivisible semigroups, *J. Algebra,* 12 (1969), 24-48.

[15] A. Lentin, Sur l'équation $a^m = b^n c^b d^q$ dans un monoïde libre, *C.R. Acad. Sci. Paris.,* 260 (1965), 3242-3244.

M.P. Schützenberger

Laboratoire d'Informatique Théorique et Programmation, LA 248, Université Paris VII, 2, Place Jussieu 75221 Paris Cedex 05, France.