A Combinatorial Problem in the Theory of Free Monoids[1]

A. LENTIN and M. P. SCHÜTZENBERGER,
Faculté des Sciences, Paris, France

1. INTRODUCTION

The combinatorial properties of free monoids play a role in several lemmas which are used in the theory of free groups (or free Lie algebras), formal languages, automata, variable length codes, and elsewhere.

The purpose of the present article is to determine a property of this type (Theorem 5 below).

2. SUMMARY OF PREVIOUS WORK

2.1. Freedom ; Primitiveness

We take a set $X = \{x, y, \dots\}$, which generates the *free monoid* X^* whose elements are called *words*. The *length* of a word f is designated by $|f|$, the word of length zero by e. Every subset A of X^* generates a sub-monoid, written A^*, for which it forms a *system of generators*.

[1] This work has been supported by contract AF61(052)945 with the United States Air Force.

Example. Let $X = \{x, y\}$ and let

$$A_1 = \{xyx, x\},$$

$$A_2 = \{xy, yx, x\},$$

$$A_3 = \{x, y, xy\}.$$

It is seen that A_1^*, $A_2^* \subset X^*$ (strict inclusion),

whereas $$A_3^* = X^*.$$

Definition 1. *$B \subset X^*$ is called a base of A (or a code) if there exists a set X' and a surjection φ of X' on B which can be extended to a monomorphism of X'^* in X^*.*

More intuitively, this is equivalent to saying that B is a base iff every word of A^* has a unique factorization in terms of the words of B.

Example. A_1 is a base for A_1^*. A_2 is not a base for A_2^* since xyx is capable of two factorizations, namely, $(xy)x$ and $x(yx)$. A_3 is not a base for A_3^*; but $\{x, y\}$ is.

Definition 2. *The submonoid A^*, generated by the system of generators A, is called free if it has a base.*

Example. A_1^* is free and has the base A_1. A_3^* is free and has the base X. A_2^* is not free: in effect, if it had a base the latter would contain x, but not y, and would therefore necessarily contain xy and yx.

Remark. We have $A_2^* \subset X^*$, and **card** $(X) <$ **card** (A_2); note that this can be generalized. In what follows, whenever A^* is a free submonoid, A will always be its base.

Theorem 1. *A necessary and sufficient condition for A^* to be free and of base A is the following (condition L):*

$$(L): \quad \textit{For all} \quad h \in X^* \setminus A^*, \qquad hA^* \cap A^* \cap A^*h = \phi$$

Proof. We will prove the equivalent proposition

$$(A \text{ is not a base}) \Longleftrightarrow (\bar{L}).$$

We have

$$(\bar{L}):\quad \exists\, h \in X^* \setminus A^* \quad \text{such that} \quad hA^* \cap A^* \cap A^*h \neq \phi\,.$$

$$(A \text{ is not a base}) \Longrightarrow (\bar{L})\,.$$

Since A is not a base, A^* contains a set of words which are capable of at least two distinct factorizations, and in that set there is a subset consisting of minimal length words. Let

$$(1) \qquad m = a_{i_1} \ldots a_{i_n} = a_{j_1} \ldots a_{j_p}$$

be such a word. The minimality of m implies that $a_{i_1} \neq a_{j_1}$. We can then take $|a_{i_1}| < |a_{j_1}|$; whence

$$(2) \qquad a_{j_1} = a_{i_1}h\,, \qquad h \in X^*\,, \qquad |h| \neq 0\,.$$

Then

$$(3) \qquad a_{i_2} \ldots a_{i_n} = ha_{j_2} \ldots a_{j_p}\,.$$

But

$$(2) \Longrightarrow A^* \cap A^*h \neq \phi\,,$$

$$(3) \Longrightarrow hA^* \cap A^* \neq \phi\,,$$

whereas

$$\text{minimality and } (3) \Longrightarrow h \in X^* \setminus A^*\,;$$

whence follows $(\bar{L})$.

$$(\bar{L}) \Longrightarrow (A \text{ is not a base})$$

$$(\bar{L}) \Longrightarrow \exists\, h \in X^* \setminus A^* \quad \text{and} \quad g, m, g' \in A^* \quad \text{such that}$$
$$hg = m = g'h\,.$$

By virtue of its belonging to $X^* \setminus A^*$, h is not empty, and so neither is m. By simplifying on the left in A (if necessary) we can arrange for m and g' not to have the same initial letter in A^*.

The double equality $g'hg = mg = g'm$ (or the one which is left after simplifying) proves that A is not a base.

Definition 3. *If A^* is a free submonoid of base A, we define the set $\pi(A^*)$ of A-primitive elements by the equivalence:*

$$f \in \pi(A^*) \Longleftrightarrow f \in A^* \quad \textit{and} \quad f \neq g^p \quad \textit{for any}$$
$$g \in A^* \quad \textit{and any} \quad p \neq 0, 1 .$$

Instead of *X-primitive* we shall simply say *primitive.*

Remark. It is clear that A-imprimitiveness implies imprimitiveness, but the converse is not true. For instance:

$$A = \{xyx, y\} . \qquad f = xyxy , \qquad f \in \pi(A^*) , \qquad f \notin \pi(X^*) .$$

Every element of a submonoid A^* having the base A can be represented uniquely as the power of an A-primitive element.

Proof. Clearly, there exists such a representation. Suppose then that we have

$$f \in A^* \,;\; f = g^p = h^q \,;\; p, q \geqslant 1 \,;\; g, h \in \pi(A^*) .$$

According to the hypothesis, f, g, and h each have a unique factorization. Proceeding by identification, one shows that $g = h$, whence $p = q$.

The following theorem, as well as its corollaries, are related to the concept of primitiveness (cf. [1]).

Theorem 2. *A necessary and sufficient condition for two words a, $b \in X^*$ to be two powers of the same word (which one can always suppose to be primitive) is that a power a^p of a and a power b^q of b contain a common left (right) factor of length*

$$|a| + |b| - (|a| \cap |b|) ,$$

where $|a| \cap |b|$ stands for the greatest common divisor.

Proof. Set $|a| = \alpha$, $|b| = \beta$. We first treat the case where $\alpha \cap \beta = 1$. Let $a = x_1 \dots x_\alpha$ and $b = y_1 \dots y_\beta$; we can take $\beta < \alpha$.

Sufficiency. We have the relations:

$$1 : x_1 = y_1 ,$$

$$2 : x_2 = y_2 ,$$

$$\alpha + \beta - 1 : x_\lambda = y_\mu .$$

Let us scan this set of relations in the following way:

i) If possible, add β to the number of the line one has just read;

ii) otherwise add $-\alpha + \beta$.

This scan is possible, for it is equivalent to uniting the vertices of a polygon in steps of β. Since β and α are relative primes, we exhaust the vertices. We have therefore $a = x_1^\alpha$, $b = x_1^\beta$.

Necessity. We have above a system of $\alpha + \beta - 1$ homogeneous equations in $(\alpha + \beta)$ unknowns. Let us add the relation:

$$\sum_i \lambda_i x_i + \sum_{j'} \mu_{j'} y_j = k$$

where $k \neq 0$ and the coefficients are not all zero. The system is then determined.

It is easily seen that one can form a determined system of the same rank by replacing the last relation with

$$x_\lambda = k_1 , \qquad y_\mu = k_2 .$$

The words a and b can be written with two types of letters, and since $\alpha \cap \beta = 1$, they are not powers of a same third word.

For $\alpha \cap \beta = \delta$, we take sections of length δ and apply the previous result.

Corollary 1. *A necessary and sufficient condition for $a, b \in X^*$ to be powers of the same word is that ab and ba contain a common left factor of length*

$$|a| \pm |b| - (|a| \cap |b|) .$$

Proof. (same notations). The theorem is trivially true for $\alpha = \beta$. Let us suppose $\beta < \alpha$. The hypothesis implies that ab is a left factor a^2, ba a word of the form $b^\lambda b_1$, hence a left factor of $b^{\lambda+1}$. We apply the theorem.

Corollary 2. *A necessary and sufficient conditon for $a, b \in X^*$ to be powers of the same word is that there exist in $\{a, b\}^*$ two distinct elements having no common factor in $\{a, b\}^*$ and having in X^* a common left factor of degree $|a| + |b| - (|a| \cap |b|)$.*

The proof is by case, in a way analagous to the preceding proof.

Corollary 3. *a, b is a base of $\{a,b\}^*$, and $\{a,b\}^*$ is free iff a and b are not powers of the same word.*

In later applications, we shall frequently use the following corollary.

Corollary 4. *For f, $g \in \pi(X^*)$, $h \in X^*$, $p, q > 1$, the hypothesis $f^p = g^q h$ implies that either $g = f$ and $h = f^{p-q}$, or else $(q-1) \cdot |g| < |f|$.*

To state the last corollary, we must give finally the definition of a fundamental concept.

Definition. *We shall call sesquipower on X^* a word f of the form :*

$$f = (uv)^k u\,, \quad k > 0\,, \qquad uv \in \pi(X^*)\,, \quad v \neq e\,.$$

A sesquipower such that $k \geqslant 2$ will be called a strong sesquipower.

Corollary 5. *For $k \geqslant 2$, a strong sesquipower $(uv)^k u$ has a unique representation as a strong sesquipower.*

Proof. Let $(uv)^k u = (wz)^j w$; then $(uv)^{k+1}$ and $(wz)^{j+1}$ are two powers of primitive words and have a common left factor of length $k|uv| + |u| = j|wz| + |w|$. If we subtract from the length of this common factor the sum of the lengths, we obtain :

$$k|uv| + |u| - |uv| - |wz| = (k-1)|uv| + |u| - \frac{k|uv| + |u|}{j + \theta}\,,$$
$$0 < \theta < 1\,.$$

This difference has the sign of :

$$[(k-1)(j+\theta) - k]|uv| + (j + \theta - 1)|u|\,.$$

The coefficient of $|uv|$ is :

$$k(j + \theta - 1) - (j + \theta)\,.$$

For $k = 2$ it becomes $j - 2 + \theta$, which is positive. Theorem 2 is now applicable.

2.1. Conjugacy

Definition. *If A^* is a free submonoid of base A, we define the relation of A-conjugacy by the equivalence*

$$f \ A\text{-conj. } g \Longleftrightarrow \exists\, h, h' \in A^* \ \text{ such that}$$
$$f = hh' \ \text{ and } \ g = h'h\,.$$

Instead of *X-conjugacy* we shall simply speak of *conjugacy.*

Remark. It is clear that A-conjugacy implies conjugacy, but the converse is not true. For instance:

$A = \{xy, yx\}$; then xy and yx are conjugate, but not A-conjugate. It follows immediately from this definition that

1. f A-conjugate $g \Longrightarrow f, g \in A^*$.
2. i) A-conjugacy is *reflexive* (take $e = h'$).
   ii) A-conjugacy is *symmetric* (evident).
   iii) A-conjugacy is *transitive.*

Take

$$f = hh'\,, \qquad g = h'h\,; \qquad g = kk'\,, \qquad m = k'k\,.$$

Then we have in A^*

$$g = h'h = kk'\,.$$

Utilizing the uniqueness of the factorization in A^* (where A^* is free), we obtain, for example,

$$h' = k_1\,, \qquad h = k_2k'\,,$$

where $k = k_1k_2$: whence

$$f = k_2(k'k_1)\,, \qquad m = (k'k_1)k_2\,.$$

The relation of A-conjugacy is an equivalence.

3. A-conjugacy is compatible with the power mapping:

$$f \to f^p$$

In effect,

$$f = hh'\,, \qquad\qquad g = h'h\,,$$

$$f^p = h[(h'h)^{p-1}h'] , \qquad g = [(h'h)^{p-1}h']h .$$

These different results can be synthesized in the following theorem :

Theorem 3. *For $f, g \in AA^*$, set*

$$C_A(f, g) = \{h \in A^* : fh = hg\} .$$

Then f A-conjugate $g \Longleftrightarrow C_A(f, g) \neq \phi$. Furthermore, for two different A-conjugate words there exists a unique positive integer p and a unique ordered pair $u, v \in A^*$ such that :

$$v \neq e ; \qquad uv, vu \in \pi(A^*) ; \qquad f = (uv)^p ; \qquad g = (vu)^p .$$

$$C_A(f, g) = u(vu)^* ; \qquad C_A(g, f) = v(uv)^*$$

Proof. *Necessity.*

$$f \text{ A-conjugate } g \Longrightarrow f = hh' , \qquad g = h'h ; \qquad h, h' \in A^*$$

$$fh = hg = hh'h ; \qquad h \in C_A(f, g) ;$$

$$C_A(f, g) \neq \phi .$$

Sufficiency. Let us suppose that $C_A(f, g)$ contains at least one word h ; then we have

$$fh = hg ,$$

$$fhg = hgg ,$$

$$ffh = hgg .$$

More generally, for all $m \geqslant 1$,

$$f^m h = hg^m .$$

However, there exists a unique integer n such that

$$n|f| \leqslant h < (n + 1)|f| .$$

We have then :

$$f = f_1 f_2 , \qquad h = f^n f_1 ;$$

$$f^{n+1}f_1 = f^n f_1 g\,;$$

$$f_2 f_1 = g\,.$$

It can be immediately verified that this solution, obtained from necessary conditions, verifies

$$fh = hg$$

Representation. We know that every word of A^* is a power of an A-primitive word, so that we have

$$f = f_1 f_2 = f_0^p\,; \qquad p \geqslant 1\,;$$

$$f_0 = uv\,, \qquad f_1 = (uv)^i u\,, \qquad f_2 = v(uv)^j$$

$$i + j + 1 = p\,,$$

and this uniquely. It follows that

$$f = f_1 f_2 = (uv)^p\,; \qquad uv \in \pi(A^*)\,,$$

$$g = f_2 f_1 = (vu)^p\,; \qquad vu \in \pi(A^*)\,.$$

For $f \neq g$, we have $uv \neq vu$; hence $v \neq e$. The rest of the conclusion is evident.

Corollary 1. *For every $f \in AA^*$, the following properties are equivalent :*

(1) *f is A-primitive ;*

(2) *The class of A-conjugates of f containts an A-primitive word ;*

(3) *$C_A(f, f) = f^*$ and any relation*

$$f'f^p f'' = f^q \quad \textit{implies that} \quad f',\ f'' \in f^*\,.$$

(4) *If $f \in A^k$, the class of A-conjugates of A contains exactly k words.*

The proof presents no difficulties.

Finally, Theorem 2 yields the following theorem immediately by a " shift " :

Theorem 4. *A necessary and sufficient condition for the words f and g to be conjugate is that two powers f^p and g^q of these words contain a common factor of length $|f| + |g| - (|f| \cap |g|)$.*

2.3 Relation to other theories

To begin with, it is clear that, for $A = X$, the concepts of primitiveness and conjugacy originate, by restriction to the monoid X^*, in analogous concepts relative to the *free group* generated by X. They can be extended immediately to a base A with the help of the monoid X'^* and the monomorphism which were defined at the beginning. Furthermore, some concepts and results can be extended to other monoids. In order to better visualize these extensions, we give first a " geometrical " interpretation.

To each $f \in X^*$, let us associate the mapping $\hat{f}$ of the segment $[1, \ldots, |f|]$ in X which sends i onto the ith letter of f. Then with the product $h = fg$ (in the monoid) there is associated the mapping $\hat{h} = \widehat{fg} = \hat{f} \cdot \hat{g}$.

$$\hat{h}(i) = \begin{cases} \hat{f}(i)\,, & \text{for} \quad i \in [1, \ldots, |f|]\,; \\ \hat{h}(i - |f|)\,, & \text{for} \quad i \in [|f|, \ldots, |f| + |g|]\,. \end{cases}$$

In this construction, f and g are conjugate iff $\hat{g}$ can be deduced from $\hat{f}$ by a cyclic shift. In other words, there exists a fixed j such that:

$$\hat{f}(i) = \begin{cases} \hat{g}(i + j)\,, & \text{for} \quad i \in [1, \ldots, |g| - j]\,; \\ \hat{g}(i + j - |g|)\,, & \text{for} \quad i \in [|g| - j + 1, \ldots, |g|]\,. \end{cases}$$

In the same way, f is the pth power of g iff

$$|f| = p|g| \ \text{and} \ \hat{f}(i + k|g|) = \hat{g}(i) \ \text{for}$$
$$i \in [1, \ldots, |g|] \ \text{and} \ k \in [0, 1, \ldots, p - 1]\,.$$

Thus, the *primitiveness* of a word is equivalent to the *aperiodicity* of the associated mapping onto its interval of definition.

Fine and Wilf have shown that most of these results can be extended to more general monoids consisting of continuous mappings in a topological set X of intervals of the real line, when these mappings are compounded by the product "." This is true in particular of Theorem 4: its extension shows that two periodic mappings are equal on the necessary and sufficient condition that they coincide on an interval whose length is equal to the sum of the lengths of their respective periods.

3. MAIN RESULTS

3.1. Statement

Theorem 5. *Let $A = \{a, b\}$ be a base such that each word of $a^*b \cap ab^*$ is primitive; then each A-primitive word of A^* is primitive.*

Actually, as we shall see, it suffices that each word of $a^*b \cap ab^*$ of length less than $3|ab|$ be primitive in order to guarantee the conclusion of the property. Also, at most one word of $a^*ab \cap abb^*$ can be imprimitive.

3.2. Terminology

We consider $A = \{a, b\} \subset X^*$, $a \neq b$. In view of the hypotheses, we have that a and b, elements of $a^*b \cup ab^*$ are primitive. For the sake of definiteness, we take $|b| \leqslant |a|$.

We introduce the following terminology :

$$\text{For} \quad d = d_1d_2 \dots d_k \in A^k \ (\text{i.e. } d_1, d_2, \dots, d_k \in A)\,,$$

we call an *A-factor of d* any product $d_id_{i+1} \dots d_j$ $(1 \leqslant i \leqslant j \leqslant k)$ occurring in d. Furthermore, we say that $d' = d'_1d'_2 \dots d'_{k'} \in A^{k'}$ is a *principal segment of d* iff there exists f, $f' \in X^*$ such that $fd'\ f' = d$ with $|f| < |d_1|$; $|f'| < |d_k|$.

Further we say that c is *disjoint from d* iff

$$f, f' \neq e \quad \text{and for all} \quad j, j', \qquad fd'_1 \dots d_{j'} \neq d_{1'} \dots d_j\,.$$

Thus, if d' is a principal disjoint segment of d, any A-factor of d' (or of d, with the exception of $d_1, d_2, \dots, d_k$, or $d_1d_2 \dots d_{k-1}$) is again a principal disjoint segment of a well defined A-factor of d (or of d').

3.3. Preliminary results

(1) *Let c, $d \in A^*$ be conjugate but not A-conjugate. Any A-factor of $c^n(n < 1)$ is a principal disjoint factor of an A-factor of d^n.*

Proof. We have $hc = dh$; hence for all positive integers n, $hc^n = d^nh$ with $h \in X^* \setminus A^*$. The hypothesis that an A-factor of c^n is not disjoint from d would imply that

$$c^n = c_1c_2\,, \qquad d^n = d_1d_2\,; \qquad c_1, c_2, d_1, d_2 \in A^*\,, \qquad hc_1 = d_1\,;$$

$$c_2 = d_2 h .$$

Thus we would have

$$hc_1c_2 = d_1c_2 = d_1d_2h \quad \text{with} \quad c_1c_2,\ d_1c_2,\ d_1d_2 \in A^* ;$$

hence $h\ A^* \cap A^*\ h \cap A^* \neq 0$ in contradiction to $h \notin A^*$ and, according to Theorem 1, the hypothesis that A^* is free.

(2) *For* $p > 0$ *and* $q > 2$, $c = a^q$ *cannot be a disjoint principal segment of* $d = ab^pa$.

Proof. Let $ab^pa = fa^qf'$ where $|f|$, $|f'| < |a|$. Since $q > 2$, at least one A-factor a of a^q is a principal disjoint segment of b^p, hence $p \geqslant 2$.

Now either b^p and a^q have a common segment of length $\geqslant |a| + |b|$ or they do not. In the first case, by Theorem 3, a and b are conjugate; then we have

$$a = uv , \qquad b = vu ; \qquad uv(vu)^puv = f(uv)^qf' ,$$

where the segments uv of $(vu)^p$ and of $(uv)^q$ must coincide because $p \geqslant 2$ and, by the hypothesis, a, $b \in \pi(X^*)$. Thus

$$uvvu = fuv ; \qquad (vu)^{p-2} = (vu)^{q-2} ; \qquad vuuv = uvf' .$$

The first (or the third) relation shows that $vu = uv$, i.e., $a = b$ in contradiction to the hypothesis $a \neq b$.

In the second case $|b^p| < |a| + |b|$. Because $|a| \geqslant |b|$ this implies $q = 3$ and we can write

$$a = fg = gh = h'g' = g'f' ,$$

so that

$$a^q = ghah'g' ; \qquad b^p = hah' \quad \text{with} \quad |h| + |h'| < b .$$

Thus at least one of h or h' (say h) has length $< |b|/2$; hence $1 < |a|/2$. By Theorem 3, the relation $a = fg = gh$ implies

$$f = u'v' ; \qquad h = v'u' , \qquad a = (u'v)^{r'}u' ,$$

where $r' \geqslant 2$ since $|h| < 1/2|a|$.

Thus a is a strong sesquipower and by Corollary 5, we can write in a unique manner

$$h = (vu)^s\,; \qquad a = (uv)^r u \qquad (s > 0,\ r \geqslant r')$$
$$\text{with} \quad vu \in \pi(X^*)\,.$$

Then

$$b^p = (vu)^s(uv)^r u(uv)^{s'}g'\,; \qquad (uv)^{s'}g' = h'\,; \qquad |g'| < |uv|\,.$$

Again since $vu \in \pi(X^*)$, any segment of b^p equal to vu or to uv is in fact a $\{u, v\}$-factor. The inequality $|h| < |b|/2$ shows that $(vu)^s uv$ is a left factor of b. However, b^p has no other segment $vuuv$ except at its end, where it occurs in $uv(uv)^{s'}g'$. Now this last word is strictly shorter than b and the hypothesis $a \neq b$ implies that $vu \neq uv$. Thus there is a contradiction because $p \geqslant 2$ (as has been shown above).

(3) *For $p > 1$ the word ab^pa cannot be a principal disjoint segment of $b^ra^2b^s$. For $p = 1$, it is so only if a^2b is imprimitive.*

Proof. The hypothesis implies

$$b^r = b_1b_2\,; \qquad b^s = b_3b_4\,; \qquad ab^pa = b_2a^2b_3 \quad \text{with} \quad b_3b_2 = b^p\,.$$

Thus we have $ab_3b_2a = b_2aab_3$, showing that ab^pa, hence a^2b^p, is imprimitive. For $p = 1$, the proposition is proved. For $p > 1$, the proposition will be proved by showing that $a^2b^p = c^q$, $q > 1$, is incompatible with the hypothesis that a and b are not powers of the same word (Theorem 2).

According to Corollary 4 of Theorem 2, the conclusion is established for

$$|a| \geqslant |c| \quad \text{or} \quad (p-1)|b| \geqslant c\,.$$

Let us suppose that $|a| < |c|$ and $(p-1)|b| < |c|$. Then, in view of the equality

$$2|a| + p|b| = q|c|\,,$$

these inequalities require that

$$2 + \frac{p}{p-1} > q\,;$$

hence, $q = 2$ or 3. Let $q = 2$. For even p, the conclusion follows at once. For odd p, $|b|$ is necessarily even. We have $b = b_1b_2$ with $|b_1| = |b_2|$, which allows us to segment the equation and arrive at the conclusion. For $q = 3$, the calculation offers no difficulties in principle, but it is very long. For brevity we shall not give it here.

(4) *For* $p > 0$, ab^pa *cannot be a principal disjoint segment of* aad', *nor of* $d'aa$ $(d' \in A^*)$, *or of* $ab^{p'}a$ *or* $b^{p'}$.

Proof. Suppose $fab^paf' = aad'$. The hypothesis of disjointness implies that a is a principal disjoint segment of aa; hence by Corollary 1, $a \notin \pi(X^*)$, which is a contradiction. The same applies to $d'aa$.

In the two other cases, the same argument applies for b and bb.

(5) *Let* $c = ab^pa$ $(p > 0)$ *be a principal disjoint segment of* $d \in A^*$ *and suppose that* d *has no A-factor* $ab^{p'}a$ *with* $p' < p$. *Then either* d *has an A-factor of the form* b^rab^s $(r + s = p)$ *which is a principal disjoint segment of* c *or else* $p = 1$ *and* $d = ba^2b$.

Proof. Assume $d \neq ba^2b$. The case of $d \in b^*a^2ab^*$ is excluded by (2) and (3) above.

For $d = b^{r'}ab^{s'}$ the hypothesis of disjointness implies $r', s' > 1$; we must have

$$|b^{r'-1}ab^{s'-1}| < |ab^pa| < |b^{r'}ab^{s'}|;$$

hence $r' + s' > p + 1$, and $r' - 1 + s' - 1 \geqslant p$: The result is verified.

If $d \notin b^*aa^*b^*$, the case of $d \in b^*$ is excluded by (4) and d must have an A-factor of the form $ab^{p'}a$ where $p' \geqslant p$ by hypothesis. Again by (4). $d \neq ab^{p'}a$ so that either $d = ab^{p'}ad'$ or $d = d'ab^{p'}a$ with $d' \neq e$. The result is verified by taking b^pa or ab^p.

3.4. Conclusion of the proof

We consider $g, g' \in A^*$, conjugate but not A-conjugate, such that $rg^n = g'^nr$, $r \notin A^*$, for all n. Such a situation necessarily obtains when $g \in A^*$ is A-primitive without being primitive; $g = f^m$ $(f \in X^* \setminus A^*,\ m > 1)$ since $f^{m+1} = fg = gf$. According to (1), every A-factor of $g^n(g'^n)$ is a principal disjoint segment of some A-factor of $g'^n(g^n)$. Since a and b are primitive, we cannot have either $g, g' \in a^*$ or $g, g' \in b^*$. If $g \in a^*$ ($g \in b^*$), (5) shows that the only remaining possibility is $g' \in b^*$ ($g' \in a^*$). Thus we can assume now $g, g' \notin a^* \cup b^*$, and suppose that g^2 has an A-factor ab^pa with p positive such that g'^2 has no A-factor $ab^{p'}a$ with $p' < p$.

We shall show that under these conditions at least one word of $a^*ab \cup abb^*$ is imprimitive.

By (5) the principal disjoint segment d of g' that covers ab^pa has an A-segment ab^p or b^pa (unless $p = 1$ and $d = bab$ in which case we know already by (3) that a^2b is imprimitive). Then ab^p (or b^pa) is a proper principal segment of ab^pa; hence of ab^pab^p (b^pab^pa). Thus it is imprimitive.

3.5. Additions

From our proof it now follows that if the set $\{a, b, a^2b\} \cup abb^*$ consists only of primitive words, the only word pairs (if there are any) which are conjugate without being A-conjugates are of the form (a^n, b^n). We can establish the following more accurate result: if a and b are conjugate, $a^*b \cup ab^* \subset \pi(X^*)$; otherwise $a^*b \cup ab^*$ contains at most one imprimitive word.

For the first part of this result, one is led to examine

$$(uv)(vu)^\lambda = c^\mu ; \qquad \lambda \geqslant 1 ; \qquad \mu \geqslant 2 .$$

The case where $\lambda = 1$, $\mu = 2$ evidently contradicts the hypothesis of primitiveness. For $(\lambda - 1)|uv| > |c|$, the hypothesis of primitiveness is contradicted by Corollary 4 of Theorem 2. There remains the case $(\lambda - 1)|uv| < |c|$. From the equality $(\lambda + 1)|uv| = \mu c$, one obtains $2 > (\mu - 1)(\lambda - 1)$ and the conclusion follows easily.

We give an outline of the proof of the second part of the result.

(i) The following lemma is useful (we have already proven particular cases of it; cf. [2] and [3]):

The condition $a^mb^m = c^q$, $m, n, q \geqslant 2$ implies that a, b and c are imprimitive and powers of the same word.

By Theorem 2, we have only to consider the case where:

$$(m - 1)\alpha < \gamma - (\alpha \cap \gamma) , \qquad (n - 1)\beta < \gamma - (\beta \cap \gamma) ,$$

with $\alpha = |a|$, $\beta = |b|$, $\gamma = |c|$. From the equality

$$m\alpha + n\beta = q\gamma ,$$

we obtain the condition

$$2 + \frac{1}{m-1} + \frac{1}{n-1} - \frac{m}{m-1}\,\frac{\alpha \cap \gamma}{\gamma} - \frac{n}{n-1}\,\frac{\beta \cap \gamma}{\gamma} > q ,$$

which characterizes the cases to be studied. We treat them directly.

(ii) We have seen that for $|a| \geqslant |b|$, the only imprimitive word of a^*a^2b is a^2b. By Corollary 4, $a^2b = f^m$ implies that $|a| > |f|$; hence $m = 2$. Solving $a^2b = f^2$ gives $a = (uv)^{k+1}u$, $b = vuuv$, and the technique of (2) above applies.

(iii) The lemma in (i) is applicable to the case $ab^m = f^p$, $ab^{m'} = g^q$ $(p, q \geqslant 2 ;\ m' > m \geqslant 1)$. We have only to consider $m' = m + 1$; then $f^pb = g^q$.

We have the equalities

$$|a| + m|b| = p|f| ;\ |a| + (m+1)|b| = q|g| ;$$

and the inequalities

$$(m-1)|b| < |f| ; \qquad m|b| < |g| ;$$

and by Corollary 4

$$(p-1)|f| < |g| .$$

This system of equalities and inequalities has only the following solutions :

$m = 1$, $p = 2$, $q = 3$;

or

$m = 2$, $p = 3$, $q = 2$;

$m = 1$, $q = 2$, p arbitary ;

or

m arbitary, $p = q = 2$.

The first two solutions contradict the hypothesis $|a| \geqslant |b|$.

There remain the following cases to consider :

$$ab = f^p ; \quad ab^2 = g^2 \ \text{ and } \ ab^m = f^2 ; \quad ab^{m+1} = g^2 .$$

The first case can be treated in the same way as the case $a^2b = f^2$ above. In the second case we can assume $m > 1$. Set $f = cb$, $g = db$, giving

$$ab^{m-1} = cbc\,, \qquad ab^m = dbd\,.$$

The relation

$$cbcb = dbd$$

cuts b into two words of equal length which we can show to be equal, and this contradicts the hypothesis of primitiveness.

References

1. Fine, N. J. and Wiff, H. S. "Uniqueness Theorems for Periodic Functions," *Proc. American Math. Soc.*, **16** (1965), 109-114.
2. Lentin, A. "Sur l'Equation $a^M = b^N c^P d^Q$ dans un Monoide Libre," *C. R. Academic Sci.*, **260** (1965), 3242-3244.
3. Lyndon, R. C. and Schützenberger, M. P. "On the Equation $a^M = b^N c^P$ in a Free Group," *Michigan Math. J.*, **9** (1962), 289-298.