JOURNAL OF COMBINATORIAL THEORY, Series A 59, 285–308 (1992)

Combinatorics of Hall Trees and Hall Words

GUY MELANÇON

Département de Mathématiques et d'Informatique, Université du Québec à Montréal, C.P. 8888 succ. A, Montréal, Québec, Canada H3C 3P8

Communicated by Gian-Carlo Rota

Received May 30, 1990

We present combinatorial properties of Hall trees and Hall words. We give new proofs of the unique factorisation of words into decreasing products of Hall words. An order $<_H$ on the free monoid is then constructed upon the unique factorisation of words. When the Hall set is the set of Lyndon words, the order $<_H$ coincides with the lexicographical order (with which Lyndon words are defined). Motivated by this fact, we give combinatorial properties of Hall words, related to the order $<_H$, which generalize known properties of Lyndon words to Hall words.

INTRODUCTION

Bases of the free Lie algebra appeared for the first time in an article by M. Hall [4], although they were implicit in the work of P. Hall [6] and Magnus [9] on the commutator calculus in free groups. Known as "Hall bases," they inspired many authors and led to many generalizations: Meier-Wunderli [10], Schützenberger [12], Shirshov [14], Gorchakov [3], and Ward [16]. Lyndon [8] introduced bases which were originally thought to be different.

Viennot gave a generalization of all these constructions and showed that, in a sense, it was optimal [15, Theorem 1.2]. He also showed that this generalization was equivalent to Lazard's elimination process. It is the bases considered by Viennot that we call "Hall bases."

The construction of these bases relies on the construction of trees and words. We call these trees and words, Hall trees and Hall words. They are defined using certain inequalities. The set of Hall words form a factorisation of the free monoid, as defined by Schützenberger [13]. The major part of Viennot's work [15] is the study of the relation between bases of the free Lie algebra and factorisations of the free monoid.

Our objective is twofold. On the one hand, we give new combinatorial proofs of the unique factorisation of words in Hall words, different from

0097-3165/92 $3.00

Viennot's [15]. Our approach is nearer to Schützenberger [12], in that we use a rewriting system and its properties: convergence, confluence, and inversibility. The algorithm provided by the rewriting system is similar to the collecting process of P. Hall, although it is more general and generalizes the algorithm presented in [1] on Lyndon words. Unicity of the factorisation also results from a subtle property of the factorisation of Hall trees into their subtrees, which generalizes the "*décomposition normale gauche*" of [12].

On the other hand, once we define an adequate order on the free monoid, we show that properties of Lyndon words generalize to Hall words. Lyndon bases are defined directly from Lyndon words, which are obtained by considering some inequalities relative to the lexicographical order (see [2, 7] for a presentation). It is this order we generalize: given a set H of Hall words, we define a total order $<_H$ on the free monoid. This order coincides with the lexicographical order when H is the set of Lyndon words. We show that Hall words satisfy the same properties as Lyndon words. They are caracterised, relatively to this order, by the equivalent conditions:

(i) they are minimal in their conjugacy class,

(ii) they are strictly smaller than any of their proper right factors.

Furthermore, as is the case with Lyndon words, the standard factorisation of a Hall word, and the factorisation of a word into Hall words are obtained by choosing the minimal right factor.

Section 1 contains basic definitions and notations and the set H of Hall trees is defined. Hall words are obtained from Hall trees by ignoring their tree structure. Lemma 2.1 is the focal point of Section 2. We deduce from it that Hall trees and Hall words are in bijection. We are then free to work with trees or words as we please. A rewriting system working on standard sequences of Hall words is defined in Section 3. It provides us with an algorithm to calculate the factorisation of a word into a decreasing product of Hall words. It may be used to recover the tree structure when applied to a Hall word. Convergence, confluency and inversibility of the rewriting system are proved and used to obtain the unicity of factorisation of words. Lemma 2.1 also provides a second proof of the unicity. Section 4 and Section 5 are entitled 'Properties à la Lyndon for Hall words'. In Section 4, we introduce an order $<_H$, on the free monoid using the unique factorisation of words into decreasing products of Hall words. Further properties of the rewriting system along with a circular version of it opens the way to our first characterisation of Hall words. They are the minimal representatives of primitive conjugacy classes (relative to the order $<_H$). In Section 5, Lemma 2.1 is again used to compare Hall words with their right factors. A second characterisation of Hall words is given: a word is a Hall word if and only if it is strictly smaller than any of its proper right factors. The other results in Section 5 may be used to formulate alternative algorithms to calculate the unique factorisation of words into Hall words, as well as to recover the tree structure of Hall words.

1. Definitions and Notations

Let A be a set; we call the elements of A *letters* and A itself an *alphabet*. Let $M(A)$ denote the *free magma* over the alphabet A, that is, the set of all binary *trees* whose leaves are labelled with letters of A. The degree of a tree t is the number of its leaves; we denote it by $|t|$. The trees of degree one are identified with the letters of the alphabet A. Each tree of degree at least two may be written as $t = [t', t'']$, where t'' (resp. t') is its *immediate right subtree* (resp. *immediate left subtree*). A *right subtree* of t is defined to be either t'' itself or a right subtree of t' or of t''; an *extreme right subtree* of t is defined to be either t'' itself or, recursively, an extreme right subtree of t''. *Left* and *extreme left subtrees* of t are defined in a similar manner. A *subtree* of t is a *right or left* subtree of t, or t itself. For example, let $A = \{a, b\}$; consider the tree representation of the element $[[a\,b][[a\,b]b]]$ of $M(A)$ shown in Fig. 1.1. For this element, $[a\,b]$ is seen to be both its immediate left subtree and a left subtree; its immediate right subtree is $[[a\,b]b]$.

The immediate left and right subtrees of a tree will be denoted using the $'$ and $''$ notations, respectively. For instance, if $t = [t', t'']$ is a tree then $(t')''$ and $(t'')''$ are the immediate right subtrees of t' and t'', respectively.

We also need to consider the free monoid A^* over A; the elements of A^* we call *words*. The product on A^* is the concatenation product. That is, if $u = a_1 \cdots a_n$ and $v = b_1 \cdots b_m$ then their product is the word $uv = a_1 \cdots a_n b_1 \cdots b_m$. There is a canonical mapping from $M(A)$ onto A^* defined by $f(a) = a$ if $a \in A$ and $f(t) = f(t')\,f(t'')$ if $t = [t', t'']$ is of degree at least 2. We call $f(t)$ the *foliage* of t. For example, the foliage of the tree in Fig. 1.1 is $f([[a\,b][[a\,b]b]]) = ababb$. As the length of the word $w = f(t)$ is equal to the degree of the tree t, we denote it, too, by $|w|$.

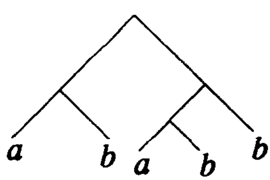

Figure 1.1

Let H be a subset of $M(A)$ supplied with a total order $\leqslant$ satisfying:

$$t < t'', \qquad \text{for every tree } t = [t', t''] \text{ of degree} \geqslant 2. \tag{1.1}$$

This subset H is called a *Hall set* if, in addition, it contains the alphabet A and is such that any tree of degree $\geqslant 2$, $h = [h', h'']$, is a *Hall tree* (i.e., $h \in H$) if and only if the two following conditions are satisfied:

$$h' \text{ and } h'' \text{ are Hall trees and } h' < h'', \tag{1.2}$$

$$\text{either } h' \text{ is a letter or } h' = [k', k''] \text{ and then } k'' \geqslant h''. \tag{1.3}$$

The second case of (1.3) may be expressed by saying that if $h = [h', h'']$ then $(h')'' \geqslant h''$.

It is important to note that any subtree of a Hall tree is also a Hall tree. Hall trees of degree one are the letters, and by (1.2) Hall trees of degree two are of the form $[a\,b]$ with a, $b \in A$ and $a < b$. Here is a list, in ascending order, of Hall trees of degree $\leqslant 5$ of a potential Hall set on $A = \{a, b\}$ with $a < b$:

$$[[[[a\,b]a]a]a],\ [[[a\,b]a][a\,b]],\ [[a\,b]a],$$
$$[[[a\,b]a]a],\ [a\,b],\ [[a\,b][[a\,b]b]],\ [[[a\,b]b]a],$$
$$[[a\,b]b],\ [[[[a\,b]b]a]a],\ a,\ [a[[[a\,b]b]b]],$$
$$[[[a\,b]b]b],\ [[[[a\,b]b]b]b],\ b, \dots .$$

1.4. LEMMA. *Let $h = [h', h'']$ be a Hall tree. If h''_1 is a right subtree of h, then $h''_1 \geqslant h''$.*

Proof. We proceed by induction on the degree of h. By definition, h''_1 is either h'' itself, or a right subtree of h' or a right subtree of h''. In the first case, we have $h''_1 \geqslant h''$. In the second case we obtain by induction $h''_1 \geqslant (h')''$; and in the third case we obtain $h''_1 \geqslant (h'')''$. Since by (1.1) we have $(h'')'' \geqslant h''$ and by (1.3) we have $(h')'' \geqslant h''$, in all cases we obtain $h''_1 \geqslant h''$. ∎

2. FACTORISATIONS OF RIGHT AND LEFT FACTORS OF HALL WORDS

We now focus on right and left factors of Hall words. We will show that the mapping f is injective, and this will eventually lead us to the unicity of factorisation of words over the set of Hall words. The following lemma is crucial.

2.1. LEMMA. *Let h be a Hall tree and $w = f(h)$ be its foliage. Suppose we* *have a factorisation of* w *into non-empty words,* $w = uv$. *Then there exist Hall trees* $k_1, \ldots, k_m, h_1, \ldots, h_n$ *such that*

$$u = f(k_1) \cdots f(k_m), \qquad v = f(h_1) \cdots f(h_n),$$

and $k_1, \ldots, k_m < h_1$, $h_1 \geqslant \cdots \geqslant h_n \geqslant h''$.

Proof. We prove the lemma, along with the supplementary condition that $h_1, \ldots, h_n$ be right subtrees of h. Let $h = [h', h'']$; by definition, we have $f(h) = f(h')\, f(h'')$. By hypothesis, we also have $f(h) = uv$. It may happen that $u = f(h')$ and $v = f(h'')$, in which case we take $m = n = 1$, $k_1 = h'$, and $h_1 = h''$. Then (1.2) gives us $k_1 < h_1$ and we are done, since h'' is the immediate right subtree of h. Otherwise, we consider two cases and argue by induction on the degree of h.

Case 1. $f(h') = ux$, $v = xf(h'')$, with x non-empty (see Fig. 2.1). By induction, applied to h', there exist Hall trees $k_1, \ldots, k_m, h_1, \ldots, h_{n-1}$ such that

$$u = f(k_1) \cdots f(k_m), \qquad x = f(h_1) \cdots f(h_{n-1}),$$

and $k_1, \ldots, k_m < h_1$, $h_1 \geqslant \cdots \geqslant h_{n-1} \geqslant (h')''$, where $h_1, \ldots, h_{n-1}$ are right subtrees of h'. As h' is the immediate left subtree of h, $h_1, \ldots, h_{n-1}$ are right subtrees of h. We have $(h')'' \geqslant h''$, by virtue of (1.3). If we now take $h_n = h''$, we obtain $v = xf(h'') = f(h_1) \cdots f(h_{n-1})\, f(h_n)$ and we are done.

Case 2. $u = f(h')x$, $f(h'') = xv$, with x non-empty (see Fig. 2.2). By induction, applied to h'', there exist Hall trees $k_2, \ldots, k_m, h_1, \ldots, h_n$ such that

$$x = f(k_2) \cdots f(k_m), \qquad v = f(h_1) \cdots f(h_n),$$

and $k_2, \ldots, k_m < h_1$, $h_1 \geqslant \cdots \geqslant h_n \geqslant (h'')''$, where $h_1, \ldots, h_n$ are right subtrees of h''. As h'' is the immediate right subtree of h, $h_1, \ldots, h_n$ are right subtrees of h. Now, by (1.1) we have that $(h'')'' > h''$ and by virtue of (1.2), $h' < h''$; combining these inequalities we find $h' < h'' < (h'')'' \leqslant h_1$. So in this case we take $k_1 = h'$ and obtain everything as desired with $u = f(h')x = f(k_1)\, f(k_2) \cdots f(k_m)$ and $v = f(h_1) \cdots f(h_n)$. ∎

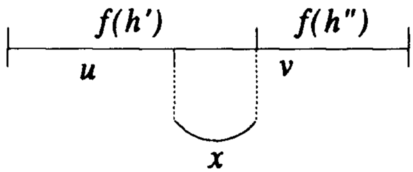

FIGURE 2.1

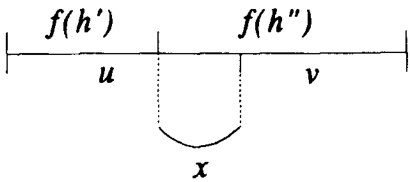

FIGURE 2.2

2.2. *Remark.* This factorization of the right factor v may be calculated by following each step of the induction. In particular, if Case 1 is encountered at least once then $v = f(h_1) \cdots f(h_n)$ with $n \geqslant 2$, and $h_1 \geqslant (h')''$. Note that Case 1 is encountered at the first step if $|v| > |h''|$. If Case 2 is encountered at the first step, then $v = f(h_1) \cdots f(h_n)$ with $h_1 \geqslant \cdots \geqslant h_n \geqslant (h'')''$, since, in this case, v is a right factor of h''. Note also that if at each step we only encounter Case 2, then we are sure that v reduces to the foliage of an extreme right subtree of h. In other words, if v does not reduce to the foliage of an extreme right subtree of h, then at least two factors occur in this factorisation of v. These observations will be needed in Section 5.

Lemma 2.1 has an interesting geometric interpretation shown on Fig. 2.3. The factorisation of the left factor u and the right factor v may be found by cutting the tree at each of its nodes (including the root) encountered along the unique path from the root to the leaft which is the first letter of the right factor v. All subtrees falling to the right of this leaf (including the one it is attached to) form the factorisation of v into a decreasing product of foliage of Hall trees. All subtrees falling to the left of this leaf form the factorisation of u as a product of foliage of Hall trees satisfying the indicated condition.

From now on, we call a *Hall word* a word that is obtained from a Hall

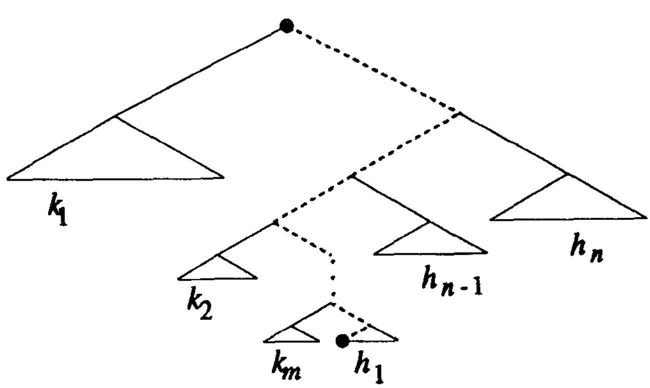

FIGURE 2.3

tree along the mapping f. We show in the next lemma that the mapping f is injective. Let H_d denote the set of Hall trees having degree at most d. Note that if $h \in H_{d+1}$ then $h', h'' \in H_d$.

2.3. THEOREM. *Each Hall word is the image of a unique Hall tree. If a Hall word, $w = f(h)$, may be written as a product of Hall words*:

$$w = f(h_1) \cdots f(h_n) \qquad \textit{with } h_1 \geqslant \cdots \geqslant h_n,$$

then we have $n = 1$.

Proof. We prove the theorem by induction on d, the degree of trees. The case $d = 1$ is trivial. Suppose it true for d and let $t = [t', t'']$ be a Hall tree of degree $d + 1$ such that

$$f(t) = f(t')\, f(t'') = f(h_1) \cdots f(h_n), \qquad \text{with } h_1 \geqslant \cdots \geqslant h_n. \tag{2.4}$$

We now show that $n = 1$ and distinguish three cases according to the relative lengths of t'' and h_n.

Case 1. $|t''| = |h_n|$. As f preserves length, we have by (2.4), $f(h_1) \cdots f(h_{n-1}) = f(t')$ and $f(h_n) = f(t'')$. Induction applied to the first equality forces $h_1 = t'$ and $n - 1 = 1$, hence $n = 2$; induction applied to the second equality gives $h_n = t''$. But since $t' < t''$ by (1.2) and $h_1 \geqslant h_2$ by hypothesis, we have a contradiction. So Case 1 must be excluded.

Case 2. $|t''| > |h_n|$. Again by (2.4) we have $f(t'') = vf(h_{i+1}) \cdots f(h_n)$, where v is a right factor of $f(h_i)$ for some $i < n$. Observe that the word v is nonempty: suppose on the contrary that we have $f(t'') = f(h_{i+1}) \cdots f(h_n)$; then by induction, this factorisation of $f(t'')$ contains only one factor so that $i + 1 = n$, which contradicts the strict inequality $|t''| > |h_n|$. As v is a proper right factor of $f(h_i)$, we deduce from Lemma 2.1 that $v = f(k_1) \cdots f(k_m)$ for some Hall trees $k_1, ..., k_m$ with $k_1 \geqslant \cdots \geqslant k_m \geqslant h''_i$. Using (1.1) and the fact that $h_i \geqslant h_{i+1}$ we obtain $k_1 \geqslant \cdots \geqslant k_m > h_{i+1} \geqslant \cdots \geqslant h_n$; hence we have

$$f(t'') = f(k_1) \cdots f(k_m)\, f(h_{i+1}) \cdots f(h_n).$$

This product contains at least two factors since $i < n$ and $m \geqslant 1$. But this factorisation of t'' results in a contradiction with the induction hypothesis made on t''. So Case 2 is also impossible.

Case 3. $|t''| < |h_n|$. Again by (2.4) we have $f(h_n) = vf(t'')$, where v is a right factor of t'. The strict inequality $|t''| < |h_n|$ forces v to be non-empty.

Now, if $n>1$ then v must be a proper right factor of t' and Lemma 2.1 provides us with Hall trees $k_1, ..., k_m$ such that

$$v=f(k_1)\cdots f(k_m), \qquad \text{with } k_1 \geqslant \cdots \geqslant k_m \geqslant (t')''.$$

Since by (1.3) we have $(t')'' \geqslant t''$, $f(h_n'')$ factorises into

$$f(h_n)=f(k_1)\cdots f(k_m)\, f(t''), \qquad \text{with } k_1 \geqslant \cdots \geqslant k_m \geqslant t''. \tag{2.5}$$

Note also that $n>1$ implies $h_n \in H_d$; so the induction hypothesis applies to h_n. But, as in Case 2, the result is a contradiction, since at least two factors figure in the factorisation (2.5).

So the only possibility we are left with is that $n=1$.

We still have to show that if h and k are Hall trees of degree $d+1$ with $f(h)=f(k)$ then $h=k$. Write $h=[h'\,h'']$, $k=[k'\,k'']$ so that $f(h)=f(h')\,f(h'')=f(k')\,f(k'')=f(k)$. We may suppose that $|h''| \geqslant |k''|$. If $|h''|=|k''|$ then we have $f(h')=f(k')$ and $f(h'')=f(k'')$, so by induction $h'= \geqslant 2$ and $h''=k''$ and, finally, $h=k$. If $|h''|>|k''|$ then $f(h'')=vf(k'')$, where v is a proper right factor of k'. By Lemma 2.1, v factorises into

$$v=f(r_1)\cdots f(r_m),$$

where $r_1, ..., r_m$ are Hall trees satisfying $r_1 \geqslant \cdots \geqslant r_m \geqslant (k')''$. By (1.3), $(k')'' \geqslant k''$, so we have

$$f(h'')=f(r_1)\cdots f(r_m)\, f(k''), \qquad \text{with } r_1 \geqslant \cdots \geqslant r_m \geqslant k''.$$

At least two factors figure in this factorisation. We reach a contradiction, since by induction $f(h'')$ may not be written as a decreasing product of foliage of two or more Hall trees. ▮

Theorem 2.3 permits us to identify a Hall word with the unique Hall tree whose foliage is this word. So we denote also by H the set of Hall words in A^*. This set is therefore totally ordered by the order $\leqslant$ on the Hall set in $M(A)$.

3. A Rewriting System on Sequences of Hall Words

Conditions (1.1), (1.2), and (1.3) migrate to the set H of Hall words. Let h be a Hall word and t be the unique Hall tree such that $f(t)=h$. If h is not a letter then $t=[t', t'']$; let $h'=f(t')$ and $f(t'')=h''$. Thus $h=h'h''$; we call this factorisation of h its *standard factorisation*. Standard factorisations of Hall words will be denoted using the $'$ and $''$ notation. We note several inequalities on Hall words which are immediate consequences of (1.1), (1.2), and (1.3).

Let h be a Hall word with standard factorisation $h = h'h''$. Then

$$h \leqslant h'', \tag{3.1}$$

$$h' < h''. \tag{3.2}$$

Let k be another Hall word with $h < k$. Then hk is a Hall word with standard factorisation $(hk)' = h$ and $(hk)'' = k$ if and only if

$$\text{either } h \text{ is a letter} \quad \text{or} \quad h'' \geqslant k. \tag{3.3}$$

We now consider sequences of Hall words:

$$s = (h_1, ..., h_n), \qquad h_1, ..., h_n \in H.$$

Such a sequence will be termed a *standard sequence* if for all $i = 1, ..., n$:

$$\text{either } h_i \text{ is a letter or } h_i = h'_i h''_i \quad \text{and then } h''_i \geqslant h_{i+1}, ..., h_n. \tag{3.4}$$

Note that a sequence of letters is standard, as is a decreasing sequence of Hall words; that is, $s = (h_1, ..., h_n)$ with $h_1 \geqslant \cdots \geqslant h_n$. Indeed if $h_i = h'_i h''_i$, then by (3.1) $h''_i > h_i$; hence $h''_i > h_{i+1}, ..., h_n$.

A *rise* of the sequence $s = (h_1, ..., h_n)$ is a couple of two consecutive words (h_i, h_{i+1}) such that $h_i < h_{i+1}$. Let s be a standard sequence which is not decreasing; a *legal rise* of the sequence s is a rise (h_i, h_{i+1}) such that

$$h_{i+1} \geqslant h_{i+2}, ..., h_n. \tag{3.5}$$

Then we define two sequences of Hall words s' and s'':

$$s' = (h_1, ..., h_{i-1}, h_i h_{i+1}, h_{i+2}, ..., h_n), \tag{3.6}$$

$$s'' = (h_1, ..., h_{i-1}, h_{i+1}, h_i, h_{i+2}, ..., h_n). \tag{3.7}$$

In other words, s' is obtained by concatenating the words h_i and h_{i+1} and s'' is obtained by exchanging h_i and h_{i+1}. If $s = (h_1, ..., h_n)$ is a standard sequence the word obtained from s by concatenating its factors, giving $h_1 \cdots h_n$, will be called the word associated with s. So we see that the words associated with s and s' are equal.

Remarks. We thus "rewrite" the sequence s into two sequences s' and s''. In [11], a similar rewriting system has been defined on standard sequences of Lyndon words, with one exception, however, that we look for the rightmost rise of the sequence. As in this case we have $h_{i+1} \geqslant h_{i+2} \geqslant \cdots \geqslant h_n$, we need not verify (3.5).

In [12], the condition $h < h'$ is added to condition (3.1) for a word h to be a Hall word. There also, a rewriting system that works on "legal sequences" is defined. A sequence $s = (h_1, ..., h_n)$ is termed *legal* if for all pairs of consecutive words (h_i, h_{i+1}), either $h_i \geqslant h_{i+1}$ or $h_i h_{i+1}$ is a Hall word. The supplementary condition $h < h'$ is used to prove that working on the rightmost rise of a legal sequence produces a legal sequence.

In [5], sequences of Hall words (with their bracketings) considered as commutators in the free group are rewritten using the "collecting process." There we look for a rise $h_i < h_{i+1}$ with h_{i+1} maximal amongst the terms of the sequence. So (3.5) is verified, since we have $h_{i+1} \geqslant h_j$ for all j.

3.8. PROPOSITION. *Let $s = h_1, ..., h_n$ be a standard sequence of Hall words. If (h_i, h_{i+1}) is a legal rise of s then both s' and s'' are standard sequences. Moreover, the standard factorisation of the product $h_i h_{i+1}$ is $(h_i h_{i+1})' = h_i$ and $(h_i h_{i+1})'' = h_{i+1}$.*

Proof. (1) We have $h_i < h_{i+1}$ and either h_i is a letter or $h_i = h'_i h''_i$ and then $h''_i \geqslant h_{i+1}$, by (3.4). Hence, by (3.3), $h_i h_{i+1}$ is a Hall word written in standard form.

To show that s' is standard we need to verify that (i) $h''_j \geqslant h_i h_{i+1}$ for $j = 1, ..., i-1$ and (ii) $h_{i+1} \geqslant h_{i+2}, ..., h_n$. Since (h_i, h_{i+1}) is a legal rise of s, (ii) is immediate. Now, let $h_j = h'_j h''_j$ be the standard factorisation of h_j. Then, by (3.4) we have $h''_j \geqslant h_{i+1}$ for $j < i$ and by (3.1) we have $h_{i+1} > h_i h_{i+1}$. Hence, $h''_j > h_i h_{i+1}$ and s' is standard.

(2) To show that s'' is standard we need only verify that $h''_{i+1} \geqslant h_i$. But we have $h_i < h_{i+1}$, since (h_i, h_{i+1}) is a rise of the sequence and $h_{i+1} < h''_{i+1}$ by (3.1). So $h''_{i+1} > h_i$ and s'' is standard. ∎

Remark. In [11] the rewriting system was used to calculate polynomials over the Poincaré–Birkhoff–Witt basis obtained from the Lyndon words. The rewriting system presented here allows for similar calculations on the Poincaré–Birkhoff–Witt basis obtained from Hall words. These calculations may be performed by using the rewriting system, since we have $s = s' + s''$, when sequences are considered as products of Lie polynomials associated with Hall words. We shall not consider this aspect here, but we will only consider factorisation of words. Consequently, our attention will mainly be focused on the sequence s'.

The next result was found by many authors with varying degrees of generality (relatively to the order on H). See [7, 15]. We give it a new proof.

3.9. FACTORISATION THEOREM. *Every word, $w \in A^*$, may be written in a unique way as a decreasing product of Hall words*:

$$w = h_1 \cdots h_n \qquad \text{with } h_1 \geqslant \cdots \geqslant h_n.$$

First we give a lemma needed in the proof of Theorem 3.9 and in subsequent proofs.

3.10. LEMMA. *Let $w = h_1 \cdots h_n$, $h_1 \geqslant \cdots \geqslant h_n$, be a decreasing product of foliages of Hall trees and let v be a proper right factor of h_i. If $v = r_1 \cdots r_m$ is a factorisation of v given by Lemma 2.1, then $r_m > h_{i+1}$ and the word $vh_{i+1} \cdots h_n$ may be written as a decreasing product of Hall words*: $vh_{i+1} \cdots h_n = r_1 \cdots r_m h_{i+1} \cdots h_n$.

Proof. If v is empty there is nothing to prove. If v is non-empty then let $v = r_1 \cdots r_m$ be its factorisation as given by Lemma 2.1. That is, $r_1, ..., r_m \in H$ and $r_1 \geqslant \cdots \geqslant r_m \geqslant h''_i$. Then, $h''_i > h_i$ by condition (1.1) and $h_i \geqslant h_{i+1}$ by hypothesis, so $r_m > h_{i+1}$ and we may write $vh_{i+1} \cdots h_n$ as a decreasing product of Hall words:

$$vh_{i+1} \cdots h_n = r_1 \cdots r_m h_{i+1} \cdots h_n. \quad ∎$$

Proof of Theorem 3.9. Existence. The rewriting system provides us with an algorithm to calculate a factorisation of a word w into a decreasing product of Hall words. That is, we may calculate successive standard sequences s_0, $s_1 = s'_0$, $s_2 = s'_1, ..., s_p = s'_{p-1}$ with $s_p = (h_1, ..., h_n)$, $h_1 \geqslant \cdots \geqslant h_n$, and $w = h_1 \cdots h_n$.

If $w = a_1 \cdots a_m$ with $a_i \in A$ then $s = (a_1, ..., a_m)$ is a standard sequence. So we take $s_0 = (a_1, ..., a_m)$ and calculate $s_1 = s'_0$, $s_2 = s'_1$, and so on. We ultimately reach a decreasing sequence $s_p = (h_1, ..., h_n)$. By (3.6), w is equal to the product of the words appearing in s_i, for each $i = 1, 2, ..., p$. So, in particular, $w = h_1 \cdots h_n$, and the existence of the factorisation is proved.

Unicity. Suppose that the word w has more than one factorisation:

$$w = k_1 \cdots k_m = h_1 \cdots h_n,$$

where the k_i's and h_j's are Hall words with $k_1 \geqslant \cdots \geqslant k_m$ and $h_1 \geqslant \cdots \geqslant h_n$. We argue by contradiction. By virtue of Theorem 2.3, we may assume that $n > 1$ and $m > 1$. Moreover, we may suppose that $|k_m| > |h_n|$ (since $|k_m| = |h_n|$ implies $k_m = h_n$ and induction on the length of w gives $m = n$ and $k_i = h_i$).

We have $k_m = vh_{i+1} \cdots h_n$, where $i < n$ and v is a non-empty right factor of h_i. Again, by Theorem 2.3, the case $v = h_i$ is impossible. So v is a proper left factor if h_i and by Lemma 3.10, k_m factorises into

$$k_m = vh_{i+1} \cdots h_n = r_1 \cdots r_p h_{i+1} \cdots h_n$$

with $r_1, ..., r_p \in H$ and $r_1 \geqslant \cdots \geqslant r_p \geqslant h_{i+1} \geqslant \cdots \geqslant h_n$. This contradicts Theorem 2.3 and ends the proof. ∎

We will prove unicity of factorisation a second time (see Corollary 3.14) by using a property of the rewriting system. We define a binary relation, denoted $\rightarrow$, on the set of standard sequences of Hall words by defining; $s \rightarrow t$ if and only if $t = s'$, where s' is given by (3.6). In other words, $s \rightarrow t$ if and only if t is obtained from s by concatenating two consecutive words of a legal rise of s. If $s \rightarrow t$ then we say that t is *derived from* s.

3.11. PROPOSITION. *The relation $\rightarrow$ is confluent. That is, if s_1 and s_2 are two standard sequences derived from s then there exists a standard sequence t such that $s_1 \rightarrow t$ and $s_2 \rightarrow t$.*

Proof. Let

$$s = (h_1, ..., h_n)$$

and let s_1 and s_2 be obtained from s by working on legal rises (h_i, h_{i+1}) and (h_j, h_{j+1}), respectively:

$$s_1 = (h_1, ..., h_{i-1}, h_i h_{i+1}, h_{i+2}, ..., h_n),$$
$$s_2 = (h_1, ..., h_{j-1}, h_j h_{j+1}, h_{j+2}, ..., h_n).$$

We may assume $i < j$. In fact, we have $i + 1 < j$. If on the contrary we suppose that $j = i + 1$, we obtain a contradiction: $h_{i+1} < h_{i+2}$, since (h_j, h_{j+1}) is a rise and $h_{i+1} \geqslant h_{i+2}$, since (h_i, h_{i+1}) is a legal rise. Hence $i + 1 < j$.

So (h_i, h_{i+1}) is a rise of the sequence s_2, as is (h_j, h_{j+1}) for s_1. The rise (h_j, h_{j+1}) is s_1 is legal since it takes place to the right of h_{i+1}. This is also the case for (h_i, h_{i+1}) in s_2. In fact, by Proposition 3.8, the word $h_j h_{j+1}$ has its standard factorisation $(h_j h_{j+1})' = h_j$ and $(h_j h_{j+1})'' = h_{j+1}$. We had $h_{i+1} \geqslant h_{j+1}$ and, since by (3.1) $h_{j+1} > h_j h_{j+1}$, we have $h_{i+1} > h_j h_{j+1}$. So the rise (h_i, h_{i+1}) is a legal rise of s_2.

As $i + 1 < j$, the legal rises (h_j, h_{j+1}) and (h_i, h_{i+1}) do not overlap in s. So, working on the rises (h_j, h_{j+1}) and (h_i, h_{i+1}) in s_1 and s_2 respectively produces the same standard sequence t:

$$t = (h_1, ..., h_{i-1}, h_i h_{i+1}, ..., h_j h_{j+1}, h_{j+2}, ..., h_n). \quad ∎$$

We now define $\xrightarrow{*}$ to be the reflexive and transitive closure of $\rightarrow$. If $s \xrightarrow{*} t$

we still say that t is derived from s. If $s \xrightarrow{*} t$ is the chain $s = s_0 \to s_1 \to \cdots \to s_n = t$ then we say that the derivation $s \xrightarrow{*} t$ has length n. A simple induction on the length of derivations, using Proposition 3.11, gives the next result.

3.12. COROLLARY. *The relation $\xrightarrow{*}$ is confluent.*

Sequences of letters are standard sequences. So, by Proposition 3.8, any sequence derived from a sequence of letters is standard. We now show that any standard sequence is obtained in this way.

3.13. PROPOSITION. *Let $t = (h_1, ..., h_n)$ be a standard sequence. If not all words h_i are letters then there exists a standard sequence s such that $s \to t$.*

Proof. Let h_i be a word in s such that if h_j is not a letter then $h''_j \geqslant h''_i$, for all $j = 1, ..., i-1$. Such one word h_i exists since we can take h_i to be the leftmost word in s which does not reduce to a letter. We wish to prove that $s = (h_1, ..., h_{i-1}, h'_i, h''_i, h_{i+1}, ..., h_n)$ is standard and that (h'_i, h''_i) is a legal rise of s.

We have $(h''_i)'' > h''_i$ by (3.1), $(h'_i)'' \geqslant h''_i$ by (3.3), and $h''_i \geqslant h_j$ for all $j = i+1, ..., n$, since t is standard. So $(h''_i)''$, $(h'_i)'' \geqslant h_j$ for all $j = i+1, ..., n$. Since $h''_j \geqslant h''_i$ for all $j = 1, ..., i-1$, by hypothesis, and $h''_i > h'_i$ by (3.2) we have $h''_j \geqslant h''_i$, h'_i for all $j = 1, ..., i-1$. This proves that s is standard. Because t is standard, the rise (h'_i, h''_i) is legal, since $h''_i \geqslant h_{i+1}, ..., h_n$. So t may be derived from s. ▮

3.14. COROLLARY (Second proof of Theorem 3.9).

Proof. First, let $s = (h_1, ..., h_m)$ be a standard sequence and $w = h_1 \cdots h_m = a_1 \cdots a_p$ $(a_i \in A)$ be the word associated with s. Then, by applying Proposition 3.13 often enough we find a derivation $(a_1, ..., a_p) \xrightarrow{*} s$.

Now suppose that $w = a_1 \cdots a_p$ has two factorisations into decreasing products of Hall words:

$$w = h_1 \cdots h_m = k_1 \cdots k_n \qquad \text{with } h_1 \geqslant \cdots \geqslant h_m,\ k_1 \geqslant \cdots \geqslant k_n.$$

As we noted earlier, the sequences $s_1 = (h_1, ..., h_m)$ and $s_2 = (k_1, ..., k_n)$ are both standard sequences since they are decreasing. So there exist two derivations $(a_1, ..., a_p) \xrightarrow{*} s_1$ and $(a_1, ..., a_p) \xrightarrow{*} s_2$. By Corollar 3.12, there exists a standard sequence t such that $s_1 \xrightarrow{*} t$ and $s_2 \xrightarrow{*} t$. Since s_1 and s_2 are both decreasing sequences, the only sequences we may derive from them are themselves, so they must be equal, $s_1 = t = s_2$. That is, $m = n$ and $h_i = k_i$ for $i = 1, ..., n$. ▮

4. Properties "*à la Lyndon*" for Hall Words. I. Conjugacy

A word $w \in A^*$ is said to be *primitive* if it is not a power of another word; that is, w is primitive if it is not empty and if $w = z^n$ implies $n = 1$ and $w = z$. For example, the word *ababb* is primitive but *abbabb* is not since $abbabb = (abb)^2$. Hall words will be seen to be primitive.

Two words w and z of A^* are said to be conjugate if and only if there exists words u, v of A^* such that $w = uv$ and $z = vu$. For example, the words *ababb* and *abbab* are conjugates of one another; we may take, in this case, $u = ab$ and $v = abb$. This is an equivalence relation on A^*, since w is conjugate to z if and only if z can be obtained from w by a cyclic permutation of the letters of w. The *conjugacy class* of a word w may be viewed as a circular word. The members of the conjugacy class of w are then obtained by reading the circular word, starting from each of its letters. For example, the circular word associated with the conjugacy class of $w = ababb$ is shown in Fig. 4.1.

Thus, the conjugacy class of $w = ababb$ is $\{ababb, babba, abbab, bbaba, babab\}$. If w and z are conjugate, then w is primitive if and only if z is primitive. Suppose now that a word w is not primitive; that is, $w = z^n$ with z non-empty and $v \geqslant 2$. Then, if we take $u = z^i$ and $v = z^j$ with $i + j = n$, we see that not all conjugates of w are distinct from w since $vu = z^j z^i = z^n = w$. For more details the reader is referred to [7].

Let H be a fixed Hall set in A^*. We now introduce a total order $<_H$ on A^*, using the unique factorisation of words over H. Let w and z be two words in A^* and consider their factorisations as decreasing products of Hall words:

$$w = k_1 k_2 \cdots k_m, \qquad z = h_1 h_2 \cdots h_n.$$

We say that w is *smaller than* z, and we write $w <_H z$ if and only if one of the following two conditions is satisfied: either

$$m < n \text{ and } k_i = h_i \quad \text{for} \quad i = 1, ..., m,$$

or there exists a subscript i such that

$$k_1 = h_1, ..., k_{i-1} = h_{i-1} \qquad \text{and} \qquad k_i < h_i,$$

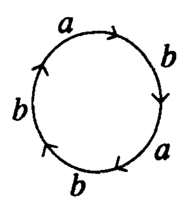

Figure 4.1

where the two Hall words k_i and h_i are compared using the order $<$ on the set of Hall words.

Remark. We now momentarily turn our attention to *Lyndon words.* They form an important example of Hall words. We will show that the order $<_L$ obtained from this particular set of Hall words coincide with the lexicographic order $<_{\text{lex}}$, upon which the Lyndon words are constructed. This fact has been the main motivation for finding the results in Section 4 and Section 5. They generalize properties known for Lyndon words to an arbitrary set of Hall words.

For details on what is discussed below, the reader is refered to [7]. Denote by $<_{\text{lex}}$ the lexicographical order on A^*. That is, a total order $<$ is given on the alphabet A and is extended to words in the following way: $w <_{\text{lex}} z$ if and only if either w is a left factor of z or there exist words s, t, $t' \in A^*$ and letters a, $b \in A$ such that

$$w = sat, \qquad z = sbt', \qquad a < b.$$

The set of Lyndon words, L, is the set of words that are strictly smaller than any of their proper right factors, for the order $<_{\text{lex}}$. One can show that, equivalently, Lyndon words are the minimum words of primitive conjugacy classes. Now, if $u \in L$ and if y is the longest proper right factor of u that is in L, then $u = xy$, x is also a Lyndon word, and $x <_{\text{lex}} xy <_{\text{lex}} y$. This factorisation of u is called its standard factorisation. We may show that if v is another Lyndon word such that $u <_{\text{lex}} v$ then uv is a Lyndon word and the factorisation uv is standard if and only if $y \geqslant_{\text{lex}} v$. So Lyndon words satisfy conditions (3.1), (3.2), and (3.3). The standard factorisation of Lyndon words is used to associate to each Lyndon word a tree in $M(A)$. One can show that the set of Lyndon trees, with the order $<_{\text{lex}}$, is a Hall set.

So, by virtue of Theorem 3.9, any word may be uniquely factorised into a decreasing product of Lyndon words and we may consider on A^* the order $<_L$.

We wish to prove that the order $<_L$ coincides with the lexicographical order on A^*. Note that $w <_{\text{lex}} z$ if and only if $uw <_{\text{lex}} uz$ for any word $u \in A^*$. We proceed by induction on $|w| + |z|$ to show that $w <_L z$ implies $w <_L z$. This will prove that the two orders are the same.

When w and z are letters the implication is clear. Suppose now that $w <_L z$. That is,

$$w = u_1 \cdots u_m, \qquad z = v_1 \cdots v_n,$$

with u_i, $v_j \in L$, $u_1 \geqslant_{\text{lex}} \cdots \geqslant_{\text{lex}} u_m$, $v_1 \geqslant_{\text{lex}} \cdots \geqslant_{\text{lex}} v_n$ and either

(i) $m < n$, $u_1 = v_1, ..., u_m = v_m$ or

(ii) $u_1 = v_1, ..., u_{k-1} = v_{k-1}$, $u_k <_{\text{lex}} v_k$.

In the first case, we obtain from the definition of $<_{\text{lex}}$ that $w <_{\text{lex}} z$. So we need only consider the second case. If u_k is not a left factor of v_k, or if u_k is a left factor of v_k and $k = m$, then we conclude easily that $w <_{\text{lex}} z$. So we are left with the case where u_k is a proper left factor of v_k and $k < m$. We have $v_k = u_k x$ with x non-empty. Let $x = h_1 \cdots h_p$ with $h_1 \geqslant_{\text{lex}} \cdots \geqslant_{\text{lex}} h_p$ be the factorisation of x into a decreasing product of Lyndon words. Since Lyndon words are strictly smaller than their proper right factors, we have $h_p >_{\text{lex}} v_k$. This provides us with the factorisation of $xv_{k+1} \cdots v_n = h_1 \cdots h_p v_{k+1} \cdots v_n$ into a decreasing product of Lyndon words. Now we use the order $<_L$ to compare the words $u_{k+1} \cdots u_m$ and $xv_{k+1} \cdots v_n$. Since $xv_{k+1} \cdots v_n = h_1 \cdots h_p v_{k+1} \cdots v_n$ and $h_1 \geqslant_{\text{lex}} h_p >_{\text{lex}} v_k >_{\text{lex}} u_k \geqslant_{\text{lex}} u_{k+1}$, we see that $u_{k+1} \cdots u_m <_L xv_{k+1} \cdots v_n$. By induction, this implies $u_{k+1} \cdots u_m <_{\text{lex}} xv_{k+1} \cdots v_n$, which in turn implies

$$u_1 \cdots u_k u_{k+1} \cdots u_m <_{\text{lex}} u_1 \cdots u_k x v_{k+1} \cdots v_n = v_1 \cdots v_k v_{k+1} \cdots v_n.$$

We are now ready to show that Hall words are representatives of primitive conjugacy classes of words, each Hall word being the minimum of its conjugacy class for the order $<_H$ we just defined. The rewriting system will be used to calculate factorisation of words. Two lemmas must first be established. The first lemma is part (i) of Lemma 2 of [11], adapted to our rewriting system on sequences of Hall words. We give the (short) proof for the sake of completeness.

4.1. LEMMA. *Let $s = (h_1, h_2, ..., h_n)$ be a standard sequence of Hall words of length at least two such that h_1 is maximal, $h_1 \geqslant h_2, ..., h_n$. Then any sequence derived from s is of length at least two and has h_1 as its first term.*

Proof. By hypothesis (h_1, h_2) is not a rise of the sequence so s' is of length at least two and is equal to

$$s' = (h_1, ..., h_{i-1}, h_i h_{i+1}, h_{i+2}, ..., h_n),$$

with $2 \leqslant i \leqslant n$. We have $h_1 \geqslant h_{i+1}$ and, by virtue of (3.1), $h_{i+1} > h_i h_{i+1}$, so s' satisfies the hypothesis of the lemma. This allows us to conclude by induction on the length of the derivations. ∎

4.2. LEMMA. *Let $s = (h_1, h_2, ..., h_n)$ be a sequence of Hall words of length* *at least two such that h_1 is maximal, $h_1 \geqslant h_2, ..., h_n$. It is possible to find a standard sequence $t = (k_1, k_2, ..., k_m)$ such that*

$$h_1 h_2 \cdots h_n = k_1 k_2 \cdots k_m, \qquad h_1 = k_1, \qquad k_1 \geqslant k_2, ..., k_m.$$

Proof. We define the *disparity* $\delta(s)$ of a sequence $s = (h_1, h_2, ..., h_n)$ to be the difference between its total degree and the number of its terms: $\delta(s) = |h_1| + \cdots + |h_n| - n$. We show the lemma by induction on the disparity of sequences. The sequences of disparity zero are sequences of letters and are surely standard. Nevertheless a sequence may be standard without having disparity zero.

Let $s = (h_1, h_2, ..., h_n)$ be a sequence satisfying the hypothesis of the lemma. If s is already standard there is nothing to do. If s is not standard then there exist i and j such that

$$i < j, \qquad h_i \text{ is not a letter and } h''_i < h_j.$$

We know $i > 1$ since $h''_1 > h_1$, by (3.1), and $h_1 \geqslant h_2, ..., h_n$, by assumption. The sequence

$$t = (h_1, ..., h_{i-1}, h'_i, h''_i, h_{i+1}, ..., h_n)$$

has a disparity equal to $\delta(t) = \delta(s) - 1$. Furthermore, t satisfies the hypothesis of the lemma. Indeed, we have $h'_i < h''_i$ by (3.2), so

$$h'_i < h''_i < h_j \leqslant h_1.$$

Since $h_1 h_2 \cdots h_i \cdots h_n = h_1 h_2 \cdots h'_i h''_i \cdots h_n$, we may conclude by induction. ▮

We can now prove one half of an important characterisation of Hall words.

4.3. THEOREM. *Let $w \in A^*$ be a word. Then w is a Hall word if and only if for any factorisation of w into non-empty words, $w = uv$, we have $w <_H vu$.*

Proof. We prove the "only if" part. The proof of the "if" part is delayed until the end of Section 4.

Let w be a Hall word. We transfer the results of Lemma 2.1 to the set of Hall words. Let $w = uv$ with u, v non-empty; we obtain

$$u = q_1 \cdots q_m, \qquad v = r_1 \cdots r_n,$$

where

$$q_i, r_j \in H,\ q_1, ..., q_m < r_1, \qquad r_1 \geqslant \cdots \geqslant r_n \geqslant w''. \tag{4.4}$$

So we have $w = uv = q_1 \cdots q_m r_1 \cdots r_n$; consequently the conjugate vu of w may be written as

$$vu = r_1 \cdots r_n q_1 \cdots q_m.$$

Now we wish to calculate the factorisation of vu into a decreasing product of Hall words in order to compare it to w. Using inequalities (4.4) we see that the sequence

$$s = (r_1, ..., r_n, q_1, ..., q_m)$$

satisfies the hypothesis of Lemma 4.2. So we find a *standard* sequence

$$t = (k_1, ..., k_p)$$

such that $vu = r_1 \cdots r_n q_1 \cdots q_m = k_1 \cdots k_p$,

$$r_1 = k_1, \qquad \text{and} \qquad k_1 \geqslant k_2, ..., k_p. \tag{4.5}$$

Now, to obtain the factorisation of vu into a decreasing product of Hall words, we may use the rewriting system on the standard sequence $t = (k_1, ..., k_p)$. By (4.5), the sequence t satisfies the hypothesis of Lemma 4.1. Consequently, any sequence we derive from t has length at least two and begins with k_1. So we know that at least two Hall words figure in the factorisation of vu and that the first one is k_1. That is,

$$vu = h_1 h_2 \cdots h_d \qquad \text{with } d \geqslant 2 \text{ and } h_1 = k_1. \tag{4.6}$$

To compare vu to w we must compare the first factor in the factorisation of vu to w. That is, we must compare h_1 to w. But, by (4.4), (4.5), and (4.6), we have that $h_1 \geqslant w''$ and (3.1) gives $h_1 > w$. By definition of $<_H$ we obtain $h_1 >_H w$ and, as a consequence, $vu >_H w$. ∎

4.7. COROLLARY. *Let $w \in A^*$ be a Hall word. Then w is primitive.*

Proof. Suppose on the contrary that w is not primitive. Then there exist words u, v such that $w = uv = vu$. Using Theorem 4.3 we obtain $w <_H vu = w$ and we reach a contradiction. So w is primitive. ∎

We will now show that every primitive word is the conjugate of a unique Hall word and establish the "if" part of Theorem 4.3. For this we need a variation of our rewriting system.

A sequence of Hall words $\sigma = (h_1, ..., h_n)$ is said to be *circularly standard* if for all $i = 1, ..., n$,

$$\text{either } h_i \text{ is a letter, or } h_i = h'_i h''_i, \text{ and then } h''_i \geqslant h_1, h_2, ..., h_n. \tag{4.8}$$

Equivalently, σ is circularly standard if every sequence

$$(h_i, ..., h_n, h_1, ..., h_{i-1}), \qquad i=1, ..., n,$$

is standard. For example, words considered as sequences of letters are circularly standard. A *rise* (h_i, h_{i+1}) of a circularly standard sequence will be termed *legal* if $h_{i+1} \geqslant h_1, ..., h_n$; that is, the factor h_{i+1} must be maximal. We will admit the rise (h_n, h_1) when $h_n < h_1$. These two cases can be summarized by saying that *subscripts are taken* mod *n*.

Let σ be a circularly standard sequence and let (h_i, h_{i+1}) be a legal rise of σ, the subscripts being taken mod n. We define a new sequence σ':

If $i<n$ then σ' is defined in the same way as s',

$$\sigma' = (h_1, ..., h_i h_{i+1}, ..., h_n).$$

If $i=n$ then we define σ' to be

$$\sigma' = (h_n h_1, h_2, ..., h_{n-1}). \tag{4.9}$$

Contrary to the previous rewriting system, the words associated with the sequences σ and σ' are no longer equal. But we see easily that the words associated with σ and σ' are conjugates of one another.

4.10. PROPOSITION. *Let $\sigma = (h_1, ..., h_n)$ be a circularly standard sequence. Then σ' is circularly standard. Moreover, the words associated with the sequences σ and σ' belong to the same conjugacy class.*

Proof. Let (h_i, h_{i+1}) be the legal rise of σ on which we operate, the subscripts being taken mod n. On the one hand, h_{i+1} is maximal among the words of the sequence and, on the other hand, we have $(h_i h_{i+1})'' = h_{i+1}$, by Proposition 3.8. So in either case we have $(h_i h_{i+1})'' \geqslant h_1, ..., h_{i-1}, h_i h_{i+1}, h_{i+2}, ..., h_n$ and σ' is circularly standard. The last part of the statement is clear. ▌

Since the set of Hall words form a factorisation of A^* (see Theorem 3.9), we know, by Schützenberger's factorisation theorem [13], that each conjugacy class is met exactly once by a power of a Hall word. We will obtain this result as a corollary of Proposition 4.10, with the aid of the "circular version" of our rewriting system.

4.11. COROLLARY. *Every primitive word is the conjugate of a unique Hall word.*

Proof. Observe that the rewriting system operates on a sequence until it is left with a sequence consisting of one word or a repetition of the same word, because only these sequences have no rise.

Now let $w \in A^*$ be primitive. We use the rewriting system we just defined to calculate successive circularly standard sequences σ_0, $\sigma_1 = \sigma'_0$, $\sigma_2 = \sigma'_1, ..., \sigma_p = \sigma'_{p+1}$ with $\sigma_p = (h_1, ..., h_n)$ such that w and $h_1 \cdots h_n$ are in the same conjugacy class.

If $w = a_1 \cdots a_m$ with $a_i \in A$ then $\sigma = (a_1, ..., a_m)$ is a circularly standard sequence. So we take $\sigma_0 = (a_1, ..., a_m)$ and calculate $\sigma_1 = \sigma'_0$, $\sigma_2 = \sigma'_1$, and so on. We ultimately reach a sequence $\sigma_p = (h_1, ..., h_n)$ with $h_1 = \cdots = h_n$. By Proposition 4.10, the words associated with σ_i and σ_{i+1} are conjugates, so w is a conjugate of $h_1 \cdots h_n$. Now, if a word is primitive, then the same is true of all its conjugates. Consequently, we must have $n = 1$. This shows that w is the conjugate of a Hall word. Since a Hall word is the minimum of its conjugacy class ("only if" part of Theorem 4.3), h_1 is unique. ∎

4.12. Corollary. *Every word is the conjugate of a power of a unique Hall word.*

We now prove the "if" part of Theorem 4.3.

4.13. Corollary. *Let $w \in A^*$ be a word such that for any factorisation of w into non-empty words, $w = uv$, we have $w <_H vu$. Then w is a Hall word.*

Proof. Observe that w is primitive. If, on the contrary, w was not primitive we could find two non-empty words u, v such that $w = uv = vu$. But this would contradict the strict inequality $w <_H vu$. So, the corollary is an immediate consequence of Corollary 4.11 and the "only if" part of Theorem 4.3. ∎

5. Properties "*à la Lyndon*" for Hall Words. II. Right Factors

We now give properties of right factors of Hall words related to the order $<_H$.

5.1. Proposition. *Let $h = h'h''$ be a Hall word of length at least two. Then*

(i) *amongst all proper rights factors of h that are Hall words, h'' is of maximal length,*

(ii) *amongst all proper right factors of h, h'' is minimal for the order $<_H$.*

Proof. (i) Let v be a right factor of h of length greater than that of h''. Let

$$v = h_1 \cdots h_n, \qquad \text{with } h_1, ..., h_n \in H,\ h_1 \geqslant \cdots \geqslant h_n,$$

be the factorisation of v as given by Lemma 2.1. Then by Remark 2.2, at least two factors occur in this factorisation. So v is not a Hall word.

(ii) Let v be a right factor of h of length greater than that of h''. Then by Remark 2.2, we have

$$v = h_1 \cdots h_n \qquad \text{with } h_1, ..., h_n \in H,\ h_1 \geqslant \cdots \geqslant h_n, \\ n \geqslant 2,\ h_1 \geqslant (h')''. \tag{5.2}$$

Comparing v to h reduces to comparing h_1 to h. Using (3.1), (3.3), and (5.2), we find

$$h < h'' \leqslant (h')'' \leqslant h_1.$$

So $h <_H v$.

Let v be a right factor of h of length less than that of h''. By Remark 2.2 again, we have

$$v = h_1 \cdots h_n \qquad \text{with } h_1, ..., h_n \in H,\ h_1 \geqslant \cdots \geqslant h_n, \\ h_1 \geqslant \cdots \geqslant h_n \geqslant (h'')''. \tag{5.3}$$

Again, comparing v to h reduces to comparing h_1 to h. Using (3.1) twice and (5.3), we find

$$h < h'' < (h'')'' \leqslant h_1.$$

So $h <_H v$. ∎

Remark. Part (i) of Proposition 5.1 is known. A quite different proof was given by Viennot [15].

5.4. THEOREM. *Let $w \in A^*$ be a word. Then w is a Hall word if and only if it is smaller than any of its proper right factors.*

Proof. Suppose first that w is a Hall word and let v be a proper right factor of w. Then by Proposition 5.1(ii), we have $w'' \leqslant_H v$. Since $w <_H w''$ we obtain $w <_H v$.

Assume now that w is smaller than any of its proper right factors. We proceed by contradiction. Suppose w is not a Hall word; then it factorises into

$$w = h_1 \cdots h_n \qquad \text{with } h_1 \geqslant \cdots \geqslant h_n,\ n \geqslant 2.$$

We claim that $h_1 > h_n$. If on the contrary, $h_1 = \cdots = h_n$, then by definition of $<_H$ we have

$$h_i \cdots h_n <_H h_1 \cdots h_n = w \qquad \text{for} \quad i = 2, ..., n.$$

This contradicts the assumption made on w. So $h_1 > h_n$. But this implies that $h_n <_H h_1 \cdots h_n = w$ which contradicts again the assumption made on w. So we must have $w \in H$. ▌

5.5. PROPOSITION. *Let $w \in A^*$ be a word and let $w = h_1 \cdots h_n$ be its non-decreasing factorisation into Hall words. Then*

(i) *amongst all right factors of w that are Hall words, h_n is of maximal length,*

(ii) *amongst all right factors of w, h_n is minimal for the order $<_H$.*

Proof. Note that when w is a Hall word, part (i) of the proposition is trivial and part (ii) is also true by Theorem 5.4. So we may assume that w is not a Hall word and that $n \geqslant 2$. Let z be a proper right factor of w:

If $|z| < |h_n|$ then, by Theorem 5.4, we have $h_n <_H z$.

If $|z| > |h_n|$ then $z = vh_{i+1} \cdots h_n$, where v is a right factor of h_i with $i < n$. Either $v = h_i$, or v is a proper right factor of h_i, in which case, by Lemma 3.10, z factorises into

$$z = vh_{i+1} \cdots h_n = k_1 \cdots k_m h_{i+1} \cdots h_n,$$
$$\text{with } k_1 \geqslant \cdots \geqslant k_m > h_{i+1} \geqslant \cdots \geqslant h_n. \qquad (5.6)$$

In both cases, we see that at least two factors figure in the factorisation of z. So z is not a Hall word and part (i) of the Proposition is proved.

To compare z to h_n we need only compare k_1 to h_n. We use (5.6) to find that $k_1 > h_n$; so in this case again we have $z >_H h_n$. ▌

Remark. Duval [1] has established Proposition 5.5 for Lyndon words. He also showed that part (i) of Proposition 5.5 holds true for left factors of Lyndon words. That is, he showed that *amongst all left factors of a word w that are Lyndon words*, h_1 (the leftmost factor in its factorisation) *is of maximal length.* This is not the case, in general. For example, we may take for H, the Hall set described in Section 1. Then $w = abbab$ factorises into $w = h_1 h_2$ with $h_1 = abb$ and $h_2 = ab$. Since *abba* is a Hall word, we see that *abb* is not the longest left factor of w to qualify as a Hall word.

The next result is from Viennot [15]. It is used to find the standard factorisation of a Hall word using the factorisation into Hall words of its longest proper right factor. It may be proved twice using parts (i) or parts (ii) of Proposition 5.1 and Proposition 5.5.

5.7. COROLLARY. *Let $w \in A^*$ be a Hall word of length at least two; that is, $w = az$ with $a \in A$ and $z \in A^*$, $|z| \geqslant 1$. Suppose the factorisation of z into Hall words is*

$$z = h_1 \cdots h_n, \qquad \text{with } h_1 \geqslant \cdots \geqslant h_n.$$

Then we have $w'' = h_n$.

Remarks. 1. The question of characterising the family of orders $<_H$ is still open. It may prove useful, in this case, to return to Lazard's elimination process, used by Viennot [15] to formulate his generalization.

2. The "collecting process" of P. Hall [6] may be generalized to work with Viennot's generalization of Hall bases. The tree structure of a Hall word is interpreted as a bracketing, in order to obtain an element of the nth term of the lower central series of the free group. We may define a rewriting system working on standard sequences of "Hall commutators." Instead of producing, at each step, the two sequences (3.6) and (3.7), we produce a single sequence that comprises both. That is, the two factors h_i and h_{i+1} of a rise are exchanged and are followed by the commutator (h_i, h_{i+1}). In doing this, the length of the sequence increases. Again, we have confluency and inversibility of the rewriting system. Convergence is assured by the fact that we work modulo the nth term of the lower central series. Results concerning this rewriting system will be presented elsewhere.

REFERENCES

1. J. P. DUVAL, Factorizing words over an ordered alphabet. *J. Algorithms* **4** (1983), 363–381.
2. A. GARSIA, Combinatorics of the free Lie algebra and the symmetric group, *in* "Analysis, et Cetera: Research Papers Published in Honor of Jürgen Moser's 60th Birthday" (Paul M. Rabinowitz and Eduard Zehnder, Eds.), pp. 309–382, Academic Press, New York, 1990.
3. Y. M. GORCHAKOV, Commutator subgroups, *Sibirsk. Mat. Zh.* **10**, No. 5 (1969), 1023–1033.
4. M. HALL, A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.* **1** (1950), 575–581.
5. M. HALL, "Theory of Groups," Macmillan Co., New York, 1959.
6. P. HALL, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc. (2)* **36** (1933), 29–95.
7. M. LOTHAIRE, "Combinatorics on Words," Addison–Wesley, Reading, MA, 1982.
8. R. C. LYNDON, On Burnside's problem, I, *Trans. Amer. Math. Soc.* **77** (1954), 202–215.
9. W. MAGNUS, Über Beziehungen zwischen höheren Kommutatoren, *J. Grelle* **177** (1937), 105–115.
10. H. MEIER-WUNDERLI, Note on a basis of P. Hall for the higher commutators in free groups, *Comm. Math. Helv.* **26** (1952), 1–5.

11. G. MELANÇON AND C. REUTENAUER, Lyndon words, free algebras and shuffles, *Canad. J. Math.* **41**, No. 4 (1989), 577–591.
12. M. P. SCHÜTZENBERGER, Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées, *in* "*Séminaire Dubreuil-Pisot*, année 58–59, Inst. Henri Poincaré, Paris."
13. M. P. SCHÜTZENBERGER, On a factorisation of free monoids, *Proc. Amer. Math. Soc.* **16**, No. 1 (1965), 21–24.
14. A. I. SHIRSHOV, On bases for a free Lie algebra, *Algebra i Logika Sém.* **1** (1962), 14–19.
15. X. G. VIENNOT, "Algèbres de Lie Libres et Monoïdes Libres," Lectures Notes in Math., Vol. 691, Springer-Verlag, Berlin, 1978.
16. M. A. WARD, Basic commutators, *Philos. Trans. Roy. Soc. London Ser. A* **264** (1969), 343–412.