A Factor Theorem for Subsets of a Free Monoid*

DERICK WOOD†

Department of Applied Mathematics, McMaster University,
Hamilton, Ontario, Canada

We give a condition under which the factors of a subset of a free monoid are unique. Some related results are demonstrated and a condition is given under which a subset of a free monoid may have factors.

1. INTRODUCTION

Let $A$ be a nonempty set, an alphabet. Then $W(A)$, the set of all sequences of elements in $A$ (i.e., words over $A$), including the empty word denoted by $\epsilon$, is the free monoid generated by $A$. In this note we are interested in catenation decompositions of subsets of $W(A)$, i.e., if $X \subseteq W(A)$, $X_1 \subseteq W(A)$ and $X_2 \subseteq W(A)$ and $X = X_1X_2$ then $X$ has a catenation decomposition or a split into factors $X_1$ and $X_2$. This note gives a condition under which the split is unique.

If $W(A)$ is finitely generated, i.e., $A$ is a finite set, then the subsets of $W(A)$ are languages. In this case, the present theorem extends the work of Korenjak and Hopcroft (1966), Schorre (1965), Tixier (1967) and Wood (1971, 1971b), in a natural way. The work of Korenjak and Hopcroft (1966) on the equivalence algorithm for $s$-grammars is merged with the work of Schorre (1965), Tixier (1967) and Wood (1971) on separability. In Wood (1971b) the results reported here are applied to the equivalence algorithm for $s$-grammars and an open question raised about this algorithm is thereby solved. The main theorem in this present paper solves an open question arising from Wood (1971).

* Work carried out under National Research Council of Canada, Grant No. A-7700.
† Department of Applied Mathematics, McMaster University, Hamilton, Ontario, Canada.

Copyright © 1972 by Academic Press, Inc. All rights of reproduction in any form reserved.
2. The Factor Theorem

Before proving the main theorem of this section, some additional notation is required. It is well known that each word in $W(A)$ can be written as a unique sequence of elements in $A$; the length of $x$ in $W(A)$ is the number of elements in $A$ in this unique decomposition, denoted by $|x|$. Note that $|xy| = |x| + |y|$ for all $x$ in $W(A)$ and $y$ in $W(A)$ and that $|\epsilon| = 0$ by definition. If $X \subseteq W(A)$ then the length of a shortest word in $X$, $sh(X) = |x|$, where $x$ is in $X$ and there is no $y$ in $X$ such that $|y| < |x|$. $X$, the set of shortest words in $X$, is the set $\{x : x$ is in $X$ and $|x| = sh(X)\}$. If $X_1 \subseteq W(A)$ and $X_2 \subseteq W(A)$ then the catenation of $X_1$ with $X_2$, written $X_1X_2$ is the set $\{x_1x_2 : x_1$ is in $X_1$ and $x_2$ is in $X_2\}$.

If $X_1 \subseteq W(A)$ and $X_2 \subseteq W(A)$ then $X_1$ and $X_2$ are separable, written $\Pi(X_1, X_2)$ if for all $x$ in $X_1X_2$, if $x = x_1x_2 = y_1y_2$, where $x_1$ is in $X_1$, $y_1$ is in $X_1$, $x_2$ is in $X_2$, and $y_2$ is in $X_2$, then $x_1 = y_1$ and $x_2 = y_2$, i.e., each word in the catenation of $X_1$ with $X_2$ can be uniquely decomposed into two words, one in $X_1$ and one in $X_2$. We say $X \subseteq W(A)$ is nontrivial if $\emptyset \neq X \neq \{\epsilon\}$. If $x$ is in $W(A)$ and $y$ is in $W(A)$ then $x$ is prefix of $y$, $x \subseteq y$, if there exists $z$ in $W(A)$ such that $xz = y$. $x$ is a proper prefix of $y$, $x \subset y$, if $x \subseteq y$ and $x \neq y$. $X \subseteq W(A)$ is a prefix set if for all $x$ in $X$ there is no $y$ in $X$ such that $x \subset y$.

The fundamental definition for this section is now given: $X \subseteq W(A)$ has a split if there exist nontrivial $X_1 \subseteq W(A)$ and $X_2 \subseteq W(A)$ such that $X = X_1X_2$, in this case we say $X$ has the split $(X_1, X_2)$.

We have our first result.

**Lemma 1.** If $X \subseteq W(A)$ has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$ then

(i) $sh(X_1) + sh(X_2) = sh(Y_1) + sh(Y_2) = sh(X)$ and

(ii) $X_1X_2 = Y_1Y_2 = X$.

**Proof.** (i) Assume otherwise, then without loss of generality we can assume $sh(X_1) + sh(X_2) < sh(X)$. This implies that there is a word $x$ in $X_1X_2$, such that $|x| < sh(X)$, which in turn implies $x$ is not in $X$. However, $X = X_1X_2$, giving a contradiction.

(ii) Assume, again without loss of generality, that $X_1X_2 \neq X$. Let there be a word $x$ in $X_1X_2$, $x$ not in $X$. We obtain an immediate contradiction by part (i), $|x| = sh(X)$ and therefore $x$ not in $X$, but $X = X_1X_2$.

**Corollary 1.1.** If $X \subseteq W(A)$ has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$, such that $sh(X_1) = sh(Y_1)$ then $X_1 = Y_1$ and $X_2 = Y_2$. 

A FACTOR THEOREM FOR SUBSETS OF A FREE MONOID

Proof. It follows from Lemma 1 that $X_1X_2 = Y_1Y_2$ and that $\text{sh}(X_2) = \text{sh}(Y_2)$. Assume, without loss of generality, that $X_1 \neq Y_1$ and that there is a word $x$ in $X_1$ such that $x$ is not in $Y_1$. Immediately, it follows that $xy$ is in $Y_1Y_2$, for all $y$ in $X_2$. Because $x$ is not in $Y_1$, by the assumption, it follows that $xy = uv$ where $u$ is in $Y_1$ and $v$ is in $Y_2$, with either $|u| < \text{sh}(Y_1)$ or $|u| > \text{sh}(Y_1)$. This gives a contradiction in both cases, hence the result.

It is shown in Wood (1971) that a split of $X$ is unique under certain strong conditions given by:

**Theorem 2.** If $X \subseteq W(A)$ has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$, where $X_1$ and $Y_1$ are prefix sets and $\text{sh}(X_1) = \text{sh}(Y_1)$ then $X_1 = Y_1$ and $X_2 = Y_2$, i.e., a split $(X_1, X_2)$ is unique for a given value of $\text{sh}(X_1)$.

**Lemma 3.** If $X_1 \subseteq W(A)$ is a prefix set, then for all $X_2 \subseteq W(A)$, $\Pi(X_1, X_2)$.

Proof. Assume there is a set $X_2 \subseteq W(A)$ such that $X_1$ and $X_2$ are not separable. This implies there is a word $x$ in $X_1X_2$ such that $x = x_1x_2 = y_1y_2$, $x_1$ in $X_1$, $y_1$ in $X_1$, $x_2$ in $X_2$ and $y_2$ in $X_2$ and $x_1 \neq y_1$. Now either $x_1 \subseteq y_1$ or $y_1 \subseteq x_1$, which is contrary to $X_1$ being a prefix set. The result follows.

This result gives

**Corollary 3.1.** If $X \subseteq W(A)$ has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$, where $X_1$ and $Y_1$ are prefix sets then $H(X_1, X_2)$ and $H(Y_1, Y_2)$.

**Remark 1.** That the converse result does not hold is given by the following example:

Let $X_1 = \{a, aa\}$ and $X_2 = \{a\}$ where $a$ is in $A$, then $\Pi(X_1, X_2)$ but as $a \subseteq aa$, $X_1$ is not a prefix set. Therefore the separable condition is weaker than the prefix condition.

Following the definition of prefix, we say $x$ is a suffix of $y$, $x \subseteq y$ where $x$ is in $W(A)$ and $y$ is in $W(A)$, if there exists $z$ in $W(A)$ such that $y = zx$. If $x \neq y$, then $x$ is a proper suffix of $y$, written $x \subset y$. $X \subseteq W(A)$ is a suffix set if for all $x$ in $X$, there is no $y$ in $X$ such that $x \subset y$. We have the following remarks concerning suffix sets.

**Remark 2.** (a) If $X_2 \subseteq W(A)$ is a suffix set, then for all $X_1 \subseteq W(A)$, $\Pi(X_1, X_2)$, (cf. Lemma 3).

(b) There exist two sets $X_1 \subseteq W(A)$ and $X_2 \subseteq W(A)$ such that $\Pi(X_1, X_2)$ but $X_2$ is not a suffix set.

(c) There exist two sets $X_1 \subseteq W(A)$ and $X_2 \subseteq W(A)$ such that $\Pi(X_1, X_2)$ but $X_1$ is not a prefix set and $X_2$ is not a suffix set. Let
$X_1 = \{a, aa\}, X_2 = \{a, aaa\}$, where $a$ is in $A$, then $\Pi(X_1, X_2)$ but as $a \not\subset aa$ and $a \subset \cdot aaa$, then $X_1$ is not prefix and $X_2$ is not suffix.

(d) There exists a set $X \subseteq W(A)$ that has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$, where $\Pi(X_1, X_2), \Pi(Y_1, Y_2)$ and $\text{sh}(X_1) = \text{sh}(Y_1)$ but $X_1 \neq Y_1$.

Let $X_1 = \{a, aa\} = Y_2$ and $X_2 = \{a, aaa\} = Y_1$, then $\Pi(X_1, X_2), \Pi(Y_1, Y_2)$, $\text{sh}(X_1) = \text{sh}(Y_1)$ but $X_1 \neq Y_1$.

**Corollary 3.2.** If $X \subseteq W(A)$ has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$, where $X_1$ and $Y_1$ are prefix sets then $\Pi(X_1, X_2), \Pi(Y_1, Y_2), \Pi(X_1, Y_2)$ and $\Pi(Y_1, X_2)$.

Corollary 3.2 together with the example in Remark 2(d) gives rise to the conjecture that Theorem 2 can be generalized by replacing the two prefix set conditions by the four separability conditions. This conjecture is now proved.

**Theorem 4 (The Factor Theorem).** If $X \subseteq W(A)$ has two splits $(X_1, X_2)$ and $(Y_1, Y_2)$, where $\Pi(X_1, X_2), \Pi(Y_1, Y_2), \Pi(X_1, Y_2)$ and $\Pi(Y_1, X_2)$ and $\text{sh}(X_1) = \text{sh}(Y_1)$ then $X_1 = Y_1$ and $X_2 = Y_2$, i.e., the split is unique for a given value of $\text{sh}(X_1)$.

**Proof.** Denote elements of $X$ by $\hat{x}$. We argue by contradiction. Assume $X_1 \neq Y_1$, then there exists at least one word $x$ in $X$ such that $x = x_1x_2 = y_1y_2$, $x_1 \neq y_1$, where $x_1$ is in $X_1$, $x_2$ is in $X_2$, $y_1$ is in $Y_1$ and $y_2$ is in $Y_2$. Choose a smallest such $x$, denoted by $\hat{x}$ and let the decompositions be $\hat{x}_1\hat{x}_2 = y_1y_2 = \hat{x}$. We show that $\hat{x}_1$ is in $Y_1$ and $\hat{x}_2$ is in $Y_2$.

Now $X_1 = \bar{Y}_2$ and $X_2 = \bar{Y}_1$ by Corollary 1.1. Consider any word $\hat{x}_1\bar{x}_2$ in $X_1X_2$. $\hat{x}_1\bar{x}_2$ is in $Y_1Y_2$. Further, as $|\hat{x}_1\bar{x}_2| < |\hat{x}|$, i.e., $\text{sh}(X_2) < |x_2|$, it follows that $\hat{x}_1$ is in $Y_1$, because

**Case 1.** $\text{sh}(X_2) < |\hat{x}_2|$. Assume $\hat{x}_1$ is not in $Y_1$. Let $\hat{x}_1 = z_1z_2$, $z_2 \neq \epsilon$ such that $z_1$ is in $Y_1$ and $z_2\bar{x}_2$ is in $Y_2$. Then as $|\hat{x}_1\bar{x}_2| < |\hat{x}|$ we have a contradiction that $\hat{x}$ was a shortest word with two decompositions.

**Case 2.** $\text{sh}(X_2) = |\hat{x}_2|$. Assume $\hat{x}_1$ is not in $Y_1$. Let $\hat{x}_1 = z_1z_2$, $z_2 \neq \epsilon$ such that $z_1$ is in $Y_1$ and $z_2\bar{x}_2$ is in $Y_2$. It follows that $z_1$ is in $X_1$ since $z_1\bar{x}_2$ is in $Y_1Y_2$ and $|z_1\bar{x}_2| < |\hat{x}|$. As $z_1$ is in $X_1$, $z_1z_2$ is in $X_1$, $\bar{x}_2$ is in $Y_2$ and $z_2\bar{x}_2$ is in $Y_2$ then $X_1$ and $Y_2$ are not separable. In both cases a contradiction ensues; therefore $\hat{x}_1$ is in $Y_1$. Similarly, we can show that $\bar{x}_1\hat{x}_2$ in $X_1X_2$ implies $\hat{x}_2$ is in $Y_2$, this part of the proof uses the fact that $\Pi(Y_1, X_2)$. 
We have shown that \( \tilde{x}_1 \) is in \( Y_1 \) and \( \tilde{x}_2 \) is in \( Y_2 \). This implies that \( Y_1 \) and \( Y_2 \) are not separable, which is a contradiction.

As in Wood (1971, 1971b), we can generalize the notions of split and separability. Given an integer \( k > 1 \), \( X \subseteq W(A) \) has a \( k \)-split \((X_1, \ldots, X_k)\), if there exist nontrivial \( X_i \subseteq W(A), 1 \leq i \leq k \), such that \( X = X_1 \cdots X_k \). It follows that a split is a 2-split. Given an integer \( k > 1 \) and \( X_i \subseteq W(A), 1 \leq i \leq k \), the sets \( X_1, \ldots, X_k \) are separable, written \( \Pi(X_1, \ldots, X_k) \), if for all \( i, 1 \leq i < k \), \( \Pi(X_i, X_{i+1} \cdots X_k) \). Theorem 4 can then be generalized as follows:

**Theorem 5 (The \( k \)-Factor Theorem).** Given an integer \( k, k > 1 \) and a set \( X \subseteq W(A) \), where \( X \) has two \( k \)-splits \((X_1, \ldots, X_k) \) and \((Y_1, \ldots, Y_k)\), such that \( \Pi(X_1, \ldots, X_k), \Pi(Y_1, \ldots, Y_k) \), for all \( i, 1 \leq i < k \), \( \Pi(X_1 \cdots X_i, Y_{i+1} \cdots Y_k) \) and \( \Pi(Y_1 \cdots Y_i, X_{i+1} \cdots X_k) \) and for all \( i, 1 \leq i \leq k \), \( \text{sh}(X_i) = \text{sh}(Y_i) \) then for all \( i, 1 \leq i \leq k \), \( X_i = Y_i \), i.e., the \( k \)-split is unique for given values of \( \text{sh}(X_i), 1 \leq i \leq k \).

We terminate this paper by noting:

**Lemma 6.** If \( X \subseteq W(A) \) has a split \((X_1, X_2) \) then \( \overline{X} \) has a split \((\overline{X}_1, \overline{X}_2) \).

This gives a weak necessary condition for \( X \) to have a split. That it is not sufficient is demonstrated by the following:

**Example.** Let \( X = \{bb, ccc\} \), then \( \overline{X} = \{bb\} \) has a split \((\{b\}, \{b\}) \); however, \( X \) does not have a split.

**Acknowledgment**

The author gratefully acknowledges the help of the referee for his careful reading of this paper, which led to a considerable improvement in its style of presentation.

**Received:** May 20, 1971

**References**

2. SCHORRE, D. V. (1965), A necessary and sufficient condition for a context-free grammar to be unambiguous, SDC document SP-2153.

