GIAN-CARLO ROTA, *Editor*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume 17

Section: Algebra

P. M. Cohn and Roger Lyndon, *Section Editors*

Combinatorics on Words

M. Lothaire

Foreword by

Roger Lyndon

University of Michigan

1983

Addison-Wesley Publishing Company

Advanced Book Program/World Science Division

Reading, Massachusetts

London • Amsterdam • Don Mills, Ontario • Sydney • Tokyo

CHAPTER 8

The Critical Factorization Theorem

8.1. Preliminaries

Periodicity is an important property of words that is often used in applications of combinatorics on words. The main results concerning it are the theorem of Fine and Wilf already given in Chapter 1 and the Critical Factorization theorem that is the object of this chapter. Both admit generalization to functions of real variables, a topic that will not be touched here.

In all that follows, we shall be considering a fixed word $w = a_1 a_2 \cdots a_n$ of positive length n, where $a_1, a_2, \ldots, a_n \in A$. The *period* $p = \pi(w)$ of w is the minimum length of the words admitting w as a factor of some of their powers; these words of minimal length p are the *cyclic roots* of w. Furthermore, w is *primitive* if it is not a *proper* power of one of its cyclic roots, *primary* iff it is a cyclic root of itself, and *periodic* iff $n \geq 2p$.

For instance $w = aaabaa$ of length 6 has period 4; its cyclic roots are *aaab*, *aaba*, *abaa*, *baaa*. It is not primary or periodic; its cyclic roots are all primitive, but only *aaab* and *baaa* are primary. The word *aaabaaabaa* is periodic; it is also primitive, and its cyclic roots are the same as for w.

It is clear that the set (denoted $\sqrt{w}$) of the cyclic roots of w is a conjugacy class including all the factors $a_i a_{i+1} \cdots a_{i+p-1}$ of length p of w. It contains p distinct primitive words and, accordingly, some of them are not factors of w when w is not periodic. We leave it to the reader to check the following statement:

PROPOSITION 8.1.1. *Equivalent definitions of the period p of w are*

(i) $p = n - |v|$, *where v is the longest word* $\neq w$ *that is a left and a right factor of w*;

(ii) $p = n$ *iff w is primary*; *otherwise it is the least positive integer such that one has identically* $a_i = a_{i+p}$. $(1 \leq i < i + p \leq n.)$

For the sake of completeness the theorem of Fine and Wilf will be reformulated in the present notation. An algebraic proof was given in Chapter 1.

THEOREM 8.1.2. *Let* $w = w'uw''$ *(with* $w', w'' \in A^*$, $u \in A^*$*),* $p' = \pi(w'u)$, $p'' = \pi(uw'')$*, and d be the greatest common divisor of* p' *and* p''.

$$\text{If } |u| \geq p' + p'' - d \text{ one has } p' = p'' = \pi(w).$$

8.2. The Critical Factorization Theorem

Let us consider a given factorization of the fixed word $w = a_1 \cdots a_n$ into two factors $w' = a_1 \cdots a_i$ and $w'' = a_{i+1} \cdots a_n$. We always assume that it is *proper*; that is, $w', w'' \neq 1$.

The set of the *cross factors* of (w', w'') is by definition

$$C(w', w'') = \{u \in A^+ \mid \quad A^*u \cap A^*w' \neq \varnothing \quad \text{and} \quad uA^* \cap w''A^* \neq \varnothing\}$$

The minimum of the length of the cross factors of (w', w'') is the *virtual period* $p(w', w'')$ of the factorization.

The factorization (w', w'') is *critical* iff $p(w', w'')$ is equal to the period p of w.

An explanation of this formal definition is needed. Assume for instance $i \geq p$, the period of w. Then the cyclic root $u = a_{i-p+1} \cdots a_{i-1}a_i$ is a *right* factor of the *left* term $w' = a_1 \cdots a_i$ of the factorization; that is, $w' \in A^*u$, implying $A^*u \cap A^*w' \neq \varnothing$. Let us say that it is *left internal*. When $|w''| \geq p$ the same situation is obtained symmetrically on the right (that is, for the right term $w'' = a_{i+1} \cdots a_n$) with the same word u when $|w''| \geq p$, because $a_{i-p+1} = a_{i+1}$, $a_{i-p+2} = a_{i+2}, \ldots, a_i = a_{i+p-1}$. When $|w''| < p$, the same equations show that w'' is equal to a left factor of u. Thus we have $u \in w''A^*$, implying again $uA^* \cap w''A^* \neq \varnothing$. In this case we say that u is *right external*.

The same applies with obvious modifications when $i < p$. We see that the set $C = C(w', w'')$ of the cross factors contains always at least one cyclic root of w, hence that the virtual period of a factorization never exceeds the true period of the word.

In fact it is "usually" far smaller. For example if $w = a^n b^m$ (with $n, m \geq 1$), the virtual period of any factorization is 1 (and it is internal on both sides) except for the factorization $(w' = a^n, w'' = b^m)$ where it attains its maximal value $n + m = \pi(w)$ (and it is external on both sides).

A more typical example is that of the word $w = aacabaca$ ($n = 8$, $p = 7$). The successive virtual periods ρ_i of the factorizations (w_i', w_i'') (($|w_i'| = i$, $|w_i''| = n - i$) $1 \leq i \leq 7$) are indicated below:

$$w = a_1 a_7 c_7 a_7 b_4 a_4 c_2 a$$

For instance, if $i=5$ (that is, $w_5'=aacab, w_5''=aca$), one finds $\rho_5=4$, because this is the length of the shortest corresponding cross factor $u_5=acab$ (which is left internal and right external). For $i=3$, the shortest cross factor is $u_3=abacaac$, *which* has length 7 (and is external on both sides). By our definition the factorizations for $i=2,3,4$ are critical. The main theorem of this chapter can now be stated. To give it in its most useful form let us exclude the case where the period p of w is 1. Indeed, in that case, w consists of the same letter repeated n times and every factorization is critical.

THEOREM 8.2.1 (Critical Factorization Theorem). *Let w be a word of period $p>1$. Any sequence of $p-1$ successive factorizations $\{(w_i', w_i'')|\ j<|w_i|<j+p\}$ contains at least one critical factorization. The corresponding shortest cross factor is a primary cyclic root of w.*

A corollary is the fact that any conjugacy class of primitive words contains primary words. This fact can be proved directly considering Lyndon words (Chapter 5). The same technique allows an easy proof of the theorem in the special case $n\geqslant 3p$ (see Problem 5.1.2).

The theorem as given is sharp. Indeed the word $w=a^mba^m$ $(m\geqslant 1)$ has period $p=m+1$ and exactly two critical factorizations, viz. (a^m, ba^m) and (a^mb, a^m). Only one of them is contained in the sequence of the $p-1$ first (or last) factorizations.

The proof is by induction on the length of w. It is more or less an existence proof because we do not know how to find the critical factorizations (or the primary words) other than by sifting out the other ones. Thus we proceed leisurely in order to provide the maximum information on the structure of the word.

We keep the same notations and let $C=C(w',w'')$.

PROPOSITION 8.2.2. *A cross factor $u\in C$ of minimal length is primary.*

Proof. Suppose that $u\in C$ is not primary—that is, that $u=u'g''=g'u'$ for some $u', g', g''\in A^*$. One has $u\in A^*u'$, hence $A^*u\subset A^*u'$ implying $A^*u'\cap A^*w'\neq\varnothing$. The same holds on the right showing that u' is also a cross factor. Since $|u'|<|u|$ we conclude that u has not minimal length. ■

PROPOSITION 8.2.3. *The set C contains a unique shortest cross factor u. If $|u|=p$, u is a cyclic root of w. This condition is satisfied if u is external on both sides.*

Proof. Note that any right (left) internal cross factor in C is strictly shorter than any right (left) external one. Thus a cross factor u of minimal length is internal on at least one side except if every cross factor in C is external on both sides—that is except if $C\subset A^*w'\cap w''A^*$.

Since internal cross factors are true factors of w, this proves the unicity of the minimal $u \in C$ and the fact that it is a cyclic root of w except in the completely external case which we consider now.

Let $v \in A^*$ (that is, possibly $v = 1$) be the longest word that is a *right* factor of the *right* term w'' ($w'' \in A^*v$) and a *left* factor of the left term w' ($w' \in vA^*$). We have $w' = vy', w'' = y''v$, where $y', y'' \in A^+$, because otherwise w' or w'' would itself be a cross factor, contradicting the hypothesis that every cross factor is external.

Set $u = y''vy' = y''w' = w''y'$. By construction $u \in C$ and by our choice of v it is the (unique!) shortest word in $A^+w' \cap w''A^+$. Since C is contained in this last set by hypothesis, u is indeed the desired shortest cross factor.

We verify that u is a cyclic root of w. Observe first that no word of length $k \geq |w'|$ or $k \geq |w''|$ is a left and a right factor of w, because otherwise we would have $w' \in C$ or $w'' \in C$. In view of $y', y'' \neq 1$, this shows that v is the longest left and right factor of w—that is, that $w = vy'y''v$ has period $|vy'y''| = |u|$. ■

The next result is the key to the proof.

LEMMA 8.2.4. *Let $y \in A^*$ be a right (left) factor of the left (right) term w' (w'') of the factorization and let $q = \pi(y)$ be its period. If u is the shortest cross factor of (w', w'') one has $|u| \leq q$ or $|y| < |u|$.*

Proof. Since u must be primary it suffices to take a cross factor u' satisfying the opposite inequalities $q < |u'| \leq |y|$ and to verify that u' is not primary.

In view of $u' \in C$, $w' \in A^*y$, and $|u'| \leq |y|$, we have $y = y'u'$. Because of $q < |u'|$ we can write $u' = u''z$ with $|z| = q, u'' \in A^+$. However, since q is the period of y its left factor $y'u''$ is also a right factor—that is, $u' \in A^+u''$—showing that u' is not primary. ■

PROPOSITION 8.2.5. *Let $b \in A$ be a letter and assume that (w', w'') is a critical factorization of w.*

If w and wb have the same period, $(w', w''b)$ is a critical factorization of wb. In the opposite case, $(w', w''b)$ is critical iff (w', w'') is right external and, then $(w', w''b)$ is external on both sides.

Proof. Let u as before and v be the shortest cross factor of $(w', w''b)$.

In view of the minimum character of u and v one has $|u| \leq |v|$ with equality iff $u = v$.

Suppose first that u is right internal; that is, $w'' \in uA^*$. It is also a cross factor of $(w', w''b)$; hence $v = u$ and the factorization $(w', w''b)$ of wb is critical iff $\pi(wb) = p$.

Suppose on the contrary that $u = w''cx$ for some letter $c \in A$ and word $x \in A^*$. Because of $|v| \geq |u|$, v is not a left factor of w'' and accordingly it has the form $v = w''bx'$ for some $x' \in A^*$. The hypothesis that (w', w'') is critical is equivalent with $u \in (\sqrt{w})$ (the set of cyclic roots of w), that is with $c = a_{n-p+1}$. Thus when wb has the same period p as w—that is, when $b = a_{n-p+1}$—we have $b = c$; hence, as in the first case, $v = u$ and $(w', w''b)$ is critical.

Therefore we can assume $\pi(wb) \neq p, c \neq b$ and consequently $|v| > |u|$. Note first that v is right external because $|u| > |w''|$ and $|w''b| = |w''| + 1$.

To complete the proof it suffices by Proposition 8.2.3 to show that v is left external; that is, that $|v| > |w'|$. However, this follows from Lemma 8.2.4. with w' instead of y and $w''b$ and v instead of w'' and u, since we have $|v| > |u| = \pi(w) \geq \pi(w')$. ■

COROLLARY 8.2.6. *Under the assumption that* $\pi(a_2 \cdots a_n b) \leq p$, *every critical factorization* (w', w'') *of* $w = a_1 \cdots a_n$ *gives a critical factorization* $(w', w''b)$ *of* wb.

Proof. Let $p' = \pi(wb)$, $\bar{w} = a_2 \cdots a_n$, and $\bar{p} = \pi(\bar{w}b)$. By the last result it suffices to show that when $p \neq p'$ the hypothesis $\bar{p} \leq p$ implies that every critical factorization of w is right external. This condition is certainly satisfied when $p = n$ since then the shortest cross factor has length $n = |w|$. Thus we have only to consider the case when $\bar{p} \leq p < n$ and $p < p'$.

We cannot have $\bar{p} = p$ because this would entail $b = a_{n-1+p}$; that is, $p = p'$. Thus $\bar{p} < p$. Consider any critical factorization (w', w'') of w. The word w'' is a factor of $\bar{w}$, hence of $\bar{w}b$ and, consequently its period q is at most $\bar{p} < p$. Applying Lemma 8.2.4 with $y = w''$, we conclude that the length $|u|$ of the shortest cross factor satisfies $|u| > |w''|$—that is, that this factorization is right external. ■

Proof of Theorem 8.2.1. The theorem is easily verified for words of short length. Thus, in order to keep the same notation, we shall assume that the theorem is already established for words of length n, $n \geq 2$, and, letting $w = a_1 \cdots a_n$ as before, it will suffice to verify its truth for wb ($b \in A$). We set $\bar{w} = a_2 \cdots a_n$, $\bar{p} = \pi(\bar{w}b)$, $p^* = \pi(wb)$.

By symmetry we can suppose $\bar{p} \leq p$ ($= \pi(w)$) and we distinguish three cases:

(i) $\bar{p} = p = n < p^*$ ($= n + 1$)
(ii) $\bar{p} = p = p^*$
(iii) $\bar{p} < p$

There is no further case. Indeed under the assumption $\bar{p} = p < n$, one has $b = a_{n-p+1}$ (since $n - p + 1 \geq 2$) and $a_1 = a_{1+p}$ (since $1 + p \leq n$) implying that wb has the same period p as w and $\bar{w}b$.

In each of the three cases, Proposition 8.2.5 and Corollary 8.2.6 show that every critical factorization (w', w'') of w gives a critical factorization $(w', w''b)$

of wb. It remains to verify that any sequence of p^*-1 factorizations of wb contains a critical one. Since $p^* \geqslant p$ this follows instantly from the induction hypothesis on w provided that $p^* > p$, or more generally, provided that one has ascertained the existence of a critical factorization of wb that is right external.

Case 1. By the induction hypothesis w has a critical factorization. It is right external since $p=n$. Thus it gives a critical factorization of wb, and the full result follows since $\pi(wb)=n+1$.

Case 2. Since $\pi(w)=\pi(wb)$ every critical factorization of w gives one of wb. By symmetry the same holds for $\overline{w}b$. Thus by the induction hypothesis on $\overline{w}b$ we conclude that wb has a critical factorization $(w', w''b)$ with $|w''b| < p$, and the result is entirely proved. An example of this case is

$$w = a^{p-1}ba^{p-1}, \ (p \geqslant 2).$$

Case 3. Consider a critical factorization (w', w'') of w. Since $w' \neq 1$, w'' is a factor of $\overline{w}$, hence of $\overline{w}b$ and accordingly its period q is at most $\bar{p} < p$. Applying Lemma 8.2.4 with $y = w''$, we see that the shortest cross factor u must satisfy $|u| > |w''|$. Thus it is right external and, accordingly, by Proposition 8.2.5, $(w', w''b)$ is a critical factorization of wb. Now the same lemma with $y = w''b$ shows that the corresponding cross factor is strictly longer than $w''b$, proving that $(w', w''b)$ is also external and concluding the proof. ■

Consider the set J of the factorizations of w that are not internal on both sides. They belong to three types: left external and right internal, left and right external, and left internal and right external.

The next property shows that the factorizations appear in this order when w is read from left to right. Also, the sequence $(p_j \colon j \in J)$ of the virtual periods corresponding to the factorizations in J is unimodal in the sense that if $j < j' < j''$ one cannot have $p_j > p_{j'} < p_{j''}$. For simplicity the property is stated on one side only.

PROPOSITION 8.2.7. *Let u and v be the shortest cross factors of the factorizations (w', xw''') and $(w'x, w''')$ $(x \in A^*)$ of w and assume that u is left internal and right external. Then v is left internal. Further, $|u| \geqslant |v|$ with equality only if v is right external and a conjugate of u.*

Proof. Let $w'' = xw'''$. The hypothesis means that there is a word $y \in A^*$ such that $w''y$ is a right factor of the left term w' and that no strictly shorter right factor of w' is a left factor of a word in $w''A^*$.

Thus the left term $w'x$ of the factorization $(w'x, w''')$ has at least one right factor, viz. $w'''yx$, which belongs to $w'''A^*$. This shows that the minimal cross factor v is left internal. We have the inequalities

$$|v| \leqslant |w'''yx| = |xw'''y| = |u|,$$

which prove that the virtual period $|v|$ is at most equal to the virtual period $|u|$ with equality iff $v = w'''yx$. Since $w'''yx$ is a conjugate of $u = xw'''y$, the equality $|v| = |u|$ entails that v be right external as u. ∎

8.3. An Application

This section gives an application of the critical factorization theorem to a problem arising in the study of free submonoids and free groups.

Let $w = a_1 \cdots a_n$ be a fixed word, as before, and let X be a given finite set of words of positive length. In the case of interest the words of X are short with respect to w and we assume $|x| \leqslant n$ for all $x \in X$.

The problem is to find upper bounds to the number of different ways w can appear as factor in a word of the submonoid X^* generated by X or, in equivalent manner, to bound the number of factorizations of w of the form $w = x'yx''$ with $y \in X^*$ and x'' (resp. x') a *prefix* (resp. *suffix*) of X—that is, a proper *left* (resp. right) factor of a word of X that is not itself a word of X.

For instance, let $w = bababbaba$, $X = \{a, bb, bab\}$. Two such factorizations can be found: $w = [(bab)(a)(bb)(a)]ba$ and $w = b[(a)(bab)(bab)(a)]$, where the term y is between square brackets and the pair x'', x' is respectively $(1, ba)$ and $(b, 1)$.

A *X-interpretation* of w is a factorization $w = x_0 x_1 \cdots x_r x_{r+1}$ where $0 \leqslant r$, $x_i \in X$ for $1 \leqslant i \leqslant r$, x_{r+1} (resp. x_0) is a prefix (resp. suffix of X). It is *disjoint* from another X-interpretation $y_0 y_1 \cdots y_s y_{s+1}$ iff $x_0 x_1 \cdots x_i \neq y_0 y_1 \cdots y_j$ for any $i \leqslant r$, $j \leqslant s$. The *X-degree* of w is the maximum number of elements in a system of pairwise disjoint X-interpretations of w.

The main result of this section may be stated as follows:

THEOREM 8.3.1. *If the period of w is strictly greater than the periods of the words of X, the X-degree of w is at most Card(X).*

The restriction upon the periodicity of w is clearly necessary to obtain such a bound. The word $w = a^n$ has $p+1$ X-interpretation when X consists of a^p only. The notion of disjointedness has algebraic motivations that have no place here. It suffices to note that without this restriction the number of X-interpretations of w could grow exponentially with its length when there are words that admit several factorizations as product of words of X (that is, when X is not a code).

The bound given by the theorem is not far from being sharp, and it is even conjectured that the exact value is $-1 + \text{Card}(X)$. Indeed if X is the biprefix code made up of a^p and of p words of the form $a^i b a^j$ where i and j

take each of the values $0,1,\ldots,p-1$ exactly once, it is easily verified that any word w admits exactly p pairwise disjoint X-factorizations provided that two successive bs are separated by more than $2p-2$ a's (that is, $w\in(a^*a^{2p-2}b)^*a^*$).

The proof of the theorem uses a lemma of independent interest. To handle conveniently the various occurrences of the same word as a factor of w, we need one more definition: a *covering*.

Let $v=a_i\cdots a_j$ $(i\leq j)$ be a segment of w and x be a word of length at least $j+1-i$. A *covering* of v by x is a segment $v'=a_{i'}\cdots a_{j'}$ such that $i'\leq i\leq j\leq j'$ and that $v'=x$ or that $i'=1$ (resp. $j'=n$) with v' a proper right (resp. left) factor of x.

Let now $w=w'vw''$ where $v=a_i\cdots a_j$ as above and where $w',w''\in A^*$.

LEMMA 8.3.2. *If the segment v has two coverings by x, the virtual period of any factorization $(w'v',v''w'')$ $(v',v''\in A^*, v'v''=v)$ is at most equal to the period of x.*

Proof. Let $a_{i_1}\cdots a_{j_1}, a_{i_2}\cdots a_{j_2}$ be the two coverings of v by x. We can suppose $i_1\leq i_2$ and $j_1\leq j_2$, where at least one inequality is strict.

There are several cases to consider. Assume first that both words $a_{i_1}\cdots a_{j_1}$ and $a_{i_2}\cdots a_{j_2}$ are equal to x. Thus $i_2-i_1=j_2-j_1$ and the common value d of this difference is strictly less than $|x|$ because the two intervals $[i_1, j_1]$ and $[i_2, j_2]$ overlap on $[i, j]$ or on a larger interval. Also we have $a_k=a_{k+d}$ for every k satisfying $i_1\leq k<k+d\leq j_2$. It follows that for any factorization $(w'v',v''w'')$ $(v'v''=v)$, the right factor of length d of $w'v'$ is equal to the left factor of the same length of $v''w''$.

It also follows that the period p of x is at most d. Suppose $p<d$ and let q be the length of the shortest cross factor of $(w'v',v''w'')$. By Lemma 8.2.4 we have $q\leq p$ or $a\geq|w'v'|$. Since $q\leq d$ where d is at most equal to the length of $w'v'$ we conclude that $q\leq p$ and the result is proved in this case.

Assume now that $a_{i_1}\cdots a_{i_2}=x''$, a proper right factor of x, but that the same is not true for $a_{i_2}\cdots a_{j_2}$. Defining x' by $x'x''=x$ and replacing w' by $x'w'$ cannot decrease the virtual period. The same can be done for w'' if the covering $a_{i_2}\cdots a_{j_2}$ is right external, and we are back to the initial case.

It remains only to discuss the case where both $a_{i_1}\cdots a_{j_1}$ and $a_{i_2}\cdots a_{j_2}$ are external on the same side, say on the left. Then we have $j_1<j_2$ and $a_1\cdots a_{j_1}=x_1'$ equal to a right factor of the right factor $a_1\cdots a_{j_2}=x_2'$ of x. It is clear that in fact x enters in the discussion only through x_2'; replacing it by x_2' we are back to the previous case, where only one of the two coverings is not internal. The conclusion is that the virtual period is bounded by the period of x_2', which is itself at most equal to that of x, and the result is proved in all cases. ■

Proof of Theorem 8.3.1. Let (w',w'') be a critical factorization of w. We have $1\leq|w'|=i\leq|w|-1$.

For each X-interpretation $w = x_0 x_1 \cdots x_{r+1}$ $(0 \leqslant r)$, there is a smallest s such that $|x_0 x_1 \cdots x_s| \geqslant i$ and a word $x = x_j$ that produces a covering of the segment $v = a_i$ of length 1 of w. If there exists a system of $1 + \operatorname{Card} X$ pairwise disjoint X-interpretations, at least two of them lead to the same word x and the conclusion follows from the preceding lemma. ■

Notes

The critical factorization theorem and its application in Section 8.3 have been discovered by Cesari and Vincent (1978). The presentation given here follows closely Duval (1979), who contributed many crucial improvements and developed a deeper theory in his thesis (1980). Further applications also due to Duval relate the period of a word to the maximum length of its primary factors, a problem originally attacked in Ehrenfeucht and Silberger 1979 and in Assous and Pouzet 1979. See Duval 1980 for the best result known so far in this direction.