Theoretical Informatics and Applications Will be set by the publisher
Informatique Théorique et Applications

e-mail: `holub@karlin.mff.cuni.cz`

ON MULTIPERIODIC WORDS *

Štěpán Holub[1]

Abstract. In this note we consider the longest word, which has periods $p_1, \ldots, p_n$, and does not have the period $\gcd(p_1, \ldots, p_n)$. The length of such a word can be established by a simple algorithm. We give a short and natural way to prove that the algorithm is correct. We also give a new proof that the maximal word is a palindrome.

1991 Mathematics Subject Classification. 68R15.

Introduction

The study of periodicity is one of the most important parts of combinatorics on words. The Periodicity Lemma, which is the discrete case of results obtained by Fine and Wilf in [**?**], has become a part of the folklore. It states that the longest word, which has period p and q, and has not the period $\gcd(p, g)$, has length $p + q - \gcd(p, q) - 1$. There were several attempts to generalize the result for more than two periods, namely [**?**] for three periods and [**?**] for arbitrarily many of them. It is easy to see that enough long word with periods $p_1, \ldots, p_n$ has also a period $\gcd(p_1, \ldots, p_n)$. Such a word contains all required periods in a trivial way. The above mentioned generalizations give valid upper bounds for the maximal length of a nontrivial word with several periods. The bounds, however, are not always optimal. The complete solution was recently given in [**?**] and [**?**].

We believe that the most appropriate way of looking not only at periodicity, but at word equations in general, are of equivalences on letters. The method dates back to Lentin's book [**?**]. For an application of this approach see also [**?**]. In this note we use this approach to give a short and hopefully clear account on the problem of multiperiodic words.

The bound we obtain is of course the same as the one given in [?] and [?]. Moreover, our algorithm computing the bound is almost identical to the one in

Keywords and phrases: periodicity, combinatorics on words

* *The work is a part of the research project MSM 0021620839 financed by MSMT.*

[1] Charles University, Faculty of Mathematics and Physics, Department of Algebra, , Sokolovská 83, 175 86 Praha, Czech Republic

[?]. The differences between [?] and the present paper are considered in the final section.

The research was done independently of the results published so far.

1. Preliminaries

Given a finite set of symbols A, called the *alphabet*, a *word* is a finite sequence of symbols from A. The length of u is denoted by $|u|$, the set of all letters, which are actually used in u, is called the *alphabet of* u and denoted by $\mathrm{alph}(u)$. The i-th letter of u is denoted by $u[i]$.

We say that a positive integer p is *a period* of a word u if $u[i] = u[i+p]$ for all $1 \leq i \leq |u| - i$. Note that any $p \geq |u|$ is a period of u.

If P is a set of positive integers, such that each $p \in P$ is a period of u, we say that u has periods P. The word is called *trivial* (when P is clear from the context) if $\gcd(P)$ is a period of u.

2. Classes of Equivalence

Let $w = a_0 \dots a_{k-1}$ be a word. (Note that $a_i = w[i+1]$. This indexing of letters is adopted because we will count modulo positive integers on indices.)

If w has periods $P \subset \mathbb{N}_+$ then obviously $a_i = a_j$ as soon as $|i - j| \in P$. This basic observation induces a relation $\sim_{P,k}$ on integers $\{0, \dots, k-1\}$ defined by

$$i \sim_{P,k} j \quad \text{iff} \quad |i - j| \in P.$$

Let $\approx_{P,k}$ be the smallest equivalence relation containing $\sim_{P,k}$. Then

$$a_i = a_j \quad \text{if} \quad i \approx_{P,k} j.$$

Clearly, if $\approx_{P,k}$ contains just one class, the word w is a power of a single letter. More generally, the number of classes is an upper bound for the cardinality of $\mathrm{alph}(w)$. We denote the number of classes of the equivalence relation $\approx_{P,k}$ by $[P, k]$. The class of $\approx_{P,k}$ containing i will be denoted by $[i]_{P,k}$.

If the set C of classes of $\approx_{P,k}$ is understood as an alphabet, we can define a word of length k, which has periods P, and maximal possible cardinality of its alphabet. It is enough to put

$$w(P, k) := [0]_{P,k} \dots [k-1]_{P,k}. \tag{1}$$

The construction yields immediately a slight generalization of Theorem 5 from [?].

Theorem 1. *Let u be a word which has periods P with alphabet of maximal possible cardinality. Then u is equal to $w(P, k)$, with $k = |u|$, up to renaming of letters.*

Proof. Let $\varphi : C \to \mathrm{alph}(u)$ be the mapping, which maps $[i]_{P,k}$, $i \in \{0, \ldots, k-1\}$, to $u[i+1]$. The mapping is well defined, because $[i]_{P,k} = [j]_{P,k}$ implies $u[i+1] = u[j+1]$, by the construction of $\approx_{P,k}$. Since the alphabet of u is maximal, φ is injective. Therefore φ is a bijection renaming letters. □

We shall list three observations, which will be used in the sequel:

Lemma 1. *Let P be a set of positive integers and $m = \min(P)$. Then*

(1) $[P, k] \leq m$.
(2) *Each class of $\approx_{P,k}$ contains some $i \in \{0, \ldots, m-1\}$.*
(3) *If $k \geq m$ then $[P, k+1] \leq [P, k]$.*

Proof. (1) and (2) follow immediately from the fact that m is a period of the word $w(P, k)$.

(3) For $0 \leq i, j \leq k-1$, $i \sim_{P,k} j$ iff $i \sim_{P,k+1} j$. The number k is related to $k-m$, therefore it does not increase the number of classes. □

Remark 2.1. The described theory can be also interpreted in terms of graphs. The reader preferring the graph terminology is invited to imagine an undirected graph defined on vertices $\{0, \ldots, k-1\}$. The relation $i \sim_{P,k} j$ means that there is an edge between i and j. The notation $i \approx_{P,k} j$ corresponds to the fact that there is a path from i to j. Finally, $[i]_{P,k}$ denotes the set of vertices in the connected component containing i.

3. Coprime periods

It is natural to study first the case, in which the periods are coprime, i.e., $\gcd(P) = 1$. Whole algorithm is based on the following crucial lemma.

Lemma 2. *Let $P \subset \mathbb{N}_+$ and $m = \min(P)$. Define the set*

$$Q = \{p - m \mid p \in P, p \neq m\} \cup \{m\}. \tag{2}$$

Then

$$[Q, k] = [P, k+m],$$

for all $k \geq m$.

Proof. Note that $\min(Q) \leq \min(P) = m$. By Lemma 1(2) it is enough to study classes $[i]_{P,k+m}$ and $[j]_{Q,k}$ with $i, j \in \{0, \ldots, m-1\}$.

For each $i, j \in \{0, \ldots, m-1\}$ we want to show that

$$[i]_{P,k+m} = [j]_{P,k+m} \quad \text{if and only if} \quad [i]_{Q,k} = [j]_{Q,k}.$$

If $[i]_{P,k+m} = [j]_{P,k+m}$, then there is a sequence $i = i_0, \ldots, i_\ell = j$, of numbers from $\{0, \ldots, k+m-1\}$ such that

$$i_s \sim_{P,k+m} i_{s+1}$$

for each $s = 0, \ldots, \ell - 1$.

We shall construct a new sequence of elements from $\{0, \dots, k-1\}$ related by $\sim_{Q,k}$, and connecting i and j. The construction is quite intuitive: compare each pair of neighbours in the original sequence and decrease the greater one by m. More formally, it can be described in two steps:

a) For each $s = 0, \dots, \ell$ define numbers j_{2s} and j_{2s+1} by $i_s = j_{2s} = j_{2s+1}$.

b) For each $s = 0, \dots, \ell - 1$ replace j_{2s+1}, j_{2s+2} with $j_{2s+1} - m, j_{2s+2}$, if $j_{2s+1} > j_{2s+2}$, and with $j_{2s+1}, j_{2s+2} - m$ otherwise.

It is easy to see that the new sequence $j_0, \dots, j_{2\ell+1}$ consists of elements from $\{0, \dots, k-1\}$, and for each $t = 0, \dots, 2\ell$ either $j_t = j_{t+1}$ or $j_t \sim_{Q,k} j_{t+1}$. Moreover, $i = j_0$ and $j_{2\ell+1} = j$. It is now enough to cancel repetitions in order to get the desired sequence.

We have therefore proved that

$$[i]_{P,k+m} = [j]_{P,k+m} \quad \text{implies} \quad [i]_{Q,k} = [j]_{Q,k}.$$

The proof of the opposite implication is analogous. The only difference is that in the step b) of the construction the greater number is increased by m, instead of decreased. $\square$

We single out one more simple fact.

Lemma 3. *Let $m = \min(P) > 1$. Then*

$$[P, 2m - 1] > 1.$$

Proof. The inequality $(m-1)+p > 2m-2$ holds for any $p \in P$. That implies that $m - 1$ is not related to any other number in $\{0, \dots, 2m - 2\}$, and the equivalence class $[m - 1]_{P,2m-1}$ contains the single element $m - 1$. Therefore $[0]_{P,2m-1} \neq [m - 1]_{P,2m-1}$, which completes the proof. $\square$

Definition (2) of Q in Lemma 2 is the well known reduction step, which is used also by [?] and [?]. The algorithm leading to the length of the longest nontrivial word with periods P can be described as follows: given a set P, such that $\gcd(P) = 1$, apply the reduction (2) until number 1 appears. This is a kind of generalized Euclid's algorithm.

We formulate it more precisely in the following theorem.

Theorem 2. *Let $P \subset \mathbb{N}_+$ be a set of positive integers, such that $\gcd(P) = 1$, and $1 \notin P$. Let $P = Q_0, Q_1, \dots, Q_n$ be the sequence of sets defined by*

$$Q_{i+1} = \{q - m_i \mid q \in Q_i, q \neq m_i\} \cup \{m_i\}, \tag{3}$$

where $m_i = \min(Q_i)$, $m_i \neq 1$ for $i = 0, \dots, n-1$, and $m_n = 1$. Then the maximal length of a nontrivial word with periods P is

$$\mathcal{L}_P = m_{n-1} - 1 + \sum_{i=0}^{n-1} m_i.$$

Proof. We first verify that for any P (even infinite) the sequence $Q_0, \ldots, Q_n$ is well defined, namely that it is finite. For any i it is easy to see that $\gcd(Q_i) = 1$ and $m_{i+1} \le m_i$. Choose arbitrary i, for which $m_i > 1$. Since $\gcd(Q_i) = 1$, the set Q_i contains an element $t \cdot m_i + r$, with $1 \le r < m_i$. Therefore $m_{i+t} < m_i$. This shows that indeed $m_n = 1$ for some n.

Repeated application of Lemma 2, and with $\mathcal{L}_P$ as above, now yields

$$[P, \mathcal{L}_P] = [Q_j, m_{n-1} - 1 + \sum_{i=j}^{n-1} m_i]$$

for all $j = 0, \ldots, n-1$. In particular

$$[P, \mathcal{L}_P] = [Q_{n-1}, 2m_{n-1} - 1],$$

and thus $[P, \mathcal{L}_P] > 1$, by Lemma 3. This proves that the word $w(P, \mathcal{L}_P)$ is not trivial.

Note that the condition $k \ge m$ of Lemma 2 do not allow to make one more reduction from $[Q_{n-1}, 2m_{n-1} - 1]$ to $[Q_n, m_{n-1} - 1]$.

On the other hand, for $\mathcal{L}_P + 1$ we have

$$[P, \mathcal{L}_P + 1] = [Q_{n-1}, 2m_{n-1}],$$

which does allow to use Lemma 2 once more to obtain

$$[P, \mathcal{L}_P + 1] = [Q_n, m_{n-1}].$$

Since $1 \in Q_n$, the word $w(P, \mathcal{L}_P + 1)$ is trivial, which proves the maximality of $\mathcal{L}_P$. □

Note that in the case $1 \in P$ excluded in the theorem, any word with periods P is trivial.

4. General Case

The result of Theorem 2 can be used to establish the general case in the following way, which is used also in [?].

Theorem 3. *Let $P \subset \mathbb{N}_+$ and $d = \gcd(P)$. Denote*

$$\overline{P} = \{\frac{p}{d} \mid p \in P\}.$$

Then the maximal length of a word with periods P, which has not the period d is

$$\mathcal{L}_P = (\mathcal{L}_{\overline{P}} + 1) \cdot d - 1.$$

Proof. Clearly, $\gcd(\overline{P}) = 1$.

Since the claim trivially holds for $d = 1$, suppose $d > 1$. Then $[P, k] \geq d$ for each $k \geq d$, because $i \approx_{P,k} j$ may hold only if $i \equiv j \bmod d$. Consequently, the set $\{0, \dots, k\}$ splits into subsets $P_0, \dots, P_{d-1}$, where

$$P_r = \{j \mid 0 \leq j \leq k-1, j \equiv r \bmod d\}.$$

The word $w(P, k)$ is trivial iff classes of $\approx_{P,k}$ are precisely sets P_r. Therefore it is enough to study the sets P_r separately.

The crucial observation is that for $i, j \in P_r$

$$i \approx_{P,k} j \quad \text{iff} \quad \frac{i-r}{d} \approx_{\overline{P},|P_r|} \frac{j-r}{d}.$$

Informally, the restriction of $\approx_{P,k}$ on P_r behaves like the equivalence induced by $\overline{P}$ on the set $\{0, \dots, |P_r|\}$.This is justified by the simple fact that $|i - j| \in P$ if and only if $i \equiv j \bmod d$ and $|\frac{i-j}{d}| \in \overline{P}$.

We now show that the bound given in the theorem is correct.

If $k = (\mathcal{L}_{\overline{P}} + 1) \cdot d$ then each set P_r has cardinality exactly $\mathcal{L}_{\overline{P}} + 1$, which is just enough to unify all of its elements, by Theorem 2.

If, on the other hand, $k = (\mathcal{L}_{\overline{P}} + 1) \cdot d - 1$ then the set P_{d-1} has cardinality just $\mathcal{L}_{\overline{P}}$. Theorem 2 implies that P_{d-1} is divided in at least two classes, and consequently the period of $w(P, k)$ is not d. $\square$

Example 4.1. Let $P = \{6, 10, 16\}$. Then $\gcd(P) = 2$, which means that periods "act" independently on even and odd numbers.

$\overline{P} = \{3, 5, 8\}$ and the sequence of sets is

$$\begin{aligned} \overline{P} = Q_0 &= \{3, 5, 8\} & m_0 &= 3 \\ Q_1 &= \{2, 3, 5\} & m_1 &= 2 \\ Q_2 &= \{1, 2, 3\}. \end{aligned}$$

We count $\mathcal{L}_{\overline{P}} = m_0 + m_1 + m_1 - 1 = 6$ and $\mathcal{L}_P = 2 \cdot 7 - 1 = 13$.

A word isomorphic to $w(P, 13)$ is

$$a\ b\ a\ c\ a\ b\ a\ b\ a\ c\ a\ b\ a.$$

Note that all letters on odd positions are the same, because there are 7 of them. Letters on even positions divide in two classes. The word corresponding to $w(\overline{P}, 6)$ is

$$b\ c\ b\ b\ c\ b,$$

which gives the letters on even positions.

5. Palindromes

It is an interesting property of the maximal nontrivial words with a given set of periods that they are palindromes. This property was proved in [?] for coprime periods considering the behaviour of a special algorithm constructing the word. In this section we show that the property follows directly from the definition (1) of $w(P, \mathcal{L}_P)$. To simplify the notation we shall write $\mathcal{L}$ instead of $\mathcal{L}_P$.

The core of the proof is the following lemma.

Lemma 4. *Let* $\mathfrak{c}$ *be a class of* $\approx_{P,\mathcal{L}}$. *Then* $\min \mathfrak{c} + \max \mathfrak{c} = \mathcal{L} - 1$.

Proof. Proceed by contradiction. We may suppose

$$\min \mathfrak{c} + \max \mathfrak{c} > \mathcal{L} - 1, \tag{4}$$

since the two possible cases are mirror images of each other.

The definition of $\mathcal{L}$ implies that

$$\min \mathfrak{c} \sim_{P,\mathcal{L}+1} \mathcal{L}.$$

Therefore there is a sequence

$$\min \mathfrak{c} = i_0 \sim_{P,\mathcal{L}+1} i_1 \sim_{P,\mathcal{L}+1} \dots \sim_{P,\mathcal{L}+1} i_\ell = \mathcal{L},$$

such that

$$i_s < \mathcal{L} \qquad \text{for all} \qquad s = 0, \dots, \ell - 1. \tag{5}$$

Then also

$$i_0 \sim_{P,\mathcal{L}} i_1 \sim_{P,\mathcal{L}} \dots \sim_{P,\mathcal{L}} i_{\ell-1},$$

and the minimality of $\min \mathfrak{c}$ implies that we may suppose

$$i_s > \min \mathfrak{c} \qquad \text{for all} \qquad s = 1, \dots, \ell. \tag{6}$$

Consider now the sequence $j_0, \dots, j_\ell$ defined by

$$j_s = i_s + \max \mathfrak{c} - \mathcal{L}.$$

Clearly, $j_s < i_s$ for all s, in particular $j_0 < \min \mathfrak{c}$. From (4), (5) and (6) we deduce that

$$0 \le j_s \le \max \mathfrak{c}$$

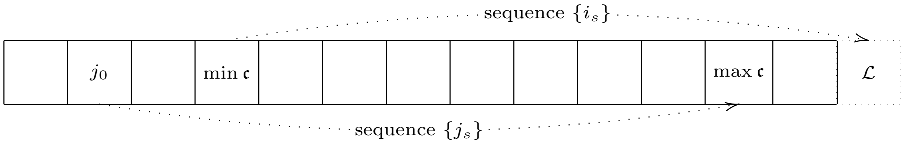
for all $s = 0, \dots, \ell$.

Therefore, since each j_s is in $\{0, \dots, \mathcal{L} - 1\}$ and the sequence $\{j_s\}_0^\ell$ is just a linear shift of the sequence $\{i_s\}_0^\ell$, we have

$$j_0 \sim_{P,\mathcal{L}} j_1 \sim_{P,\mathcal{L}} \dots \sim_{P,\mathcal{L}} j_\ell = \max \mathfrak{c}.$$

Hence $j_0 \in \mathfrak{c}$, a contradiction with $j_0 < \min \mathfrak{c}$. ☐

The proof of the previous lemma is visualized by the following picture.



We can now give a new proof of the generalized version of Theorem 5 from [?].

Theorem 4. *Let $P \subset \mathbb{N}_+$ be an arbitrary set of periods. Then the word $w(P,\mathcal{L})$ is a palindrome.*

Proof. Clearly, the mirror image of $w(P,\mathcal{L})$ has also periods P. Hence, by Theorem 1, it can be obtained from $w(P,\mathcal{L})$ by renaming letters, where $[i]_{P,\mathcal{L}}$ is renamed to $[\mathcal{L}-1-i]_{P,\mathcal{L}}$. Considering the minimal and the maximal element of each class Lemma 4 implies that the renaming is identity. $\square$

The technique of the proof of Lemma 4 is a promising tool for gaining information about the maximal words without constructing them, in fact even without computing $\mathcal{L}$. As an example we sketch the proof of the claim that each new letter is preceded by the first one.

Lemma 5. *Let $w = w(P,\mathcal{L})$ and let $w[i+1]$, $i \geq 1$, be the first occurence of a letter in w. Then $w[i] = w[1]$.*

Proof. As in Lemma 4, let $\{i_s\}_0^\ell$ relate $[i]_{P,\mathcal{L}+1}$ to $[\mathcal{L}]_{P,\mathcal{L}+1}$ by $\sim_{P,\mathcal{L}+1}$. Then the sequence $\{i_s-1\}_0^\ell$ relates $[i-1]_{P,\mathcal{L}}$ to $[\mathcal{L}-1]_{P,\mathcal{L}}$. Therefore $[i-1]_{P,\mathcal{L}} = [\mathcal{L}-1]_{P,\mathcal{L}}$, which completes the proof, since w is a palindrome. $\square$

6. Concluding remarks

As already noted, the algorithm computing $\mathcal{L}$ is almost identical with the one presented in [?]. In fact, the only real difference in the run of the algorithm can be found in the termination condition. Our algorithm ends as soon as the first 1 is obtained, the algorithm in [?] continues until all "activated columns" have 0 or 1. Albeit the authors note that after the appearance of the first 1 the remaining part of the procedure can be "foreseen", with our approach this is the most natural end of the computation.

Our description of the algorithm, however, is much simpler, e.g. the definition of the reduction step. Another complication is the division of periods into "activated" and "not activated", which property is even used in the termination condition. The complex notation seems to be adopted in order to construct the maximal word and then to prove its properties by examination of the algorithm.

In contrast, we do not bring forward any explicit construction, since with our approach one is able to study the maximal word without even computing its length, utilising just its definition. The main theoretical reason is that the letters in the word have a precise meaning, they are equivalence classes. Theorem 1 and

Theorem 4 are then without any additional effort more general than corresponding Theorem 4 and Theorem 5 in [?], as they hold also for periods, which are not coprime.

The equality (1), moreover, defines the word up to isomorphism, and as soon as its length is known it can be obtained using any suitable algorithm computing equivalence classes of a relation (or connected components of a graph).

Note also that all our proofs work also for an infinite P.

I am grateful to an anonymous referee for comments and suggestions, which helped to improve the exposition.

Communicated by (The editor will be set by the publisher).
(The dates will be set by the publisher).