数理解析研究所講究録 1366 巻 2004 年 202-204

A condition for two words being powers of the same word

天理大学総合教育センター
辻　佳代子
Kayoko Tsuji
Tenri University
tsuji@sta.tenri-u.ac.jp

The theorem Fine and Wilf is well known ([1]). They gave a condition for two word being powers of the same word. A condition which is weaker than the condition is given in this paper.

Let Σ be a finite set usually called *alphabet* and Σ^* be the free monoid generated by Σ. We use the notation $\Sigma^+ = \Sigma^* - 1$, where 1 is the empty word.

The *length* of a word $x = a_1a_2 \cdots a_n, (a_1, a_2, \cdots, a_n \in \Sigma)$ is the number n and is denoted by $|x|$. A word u is said to be a *prefix* of a word x if there exists a word v such that $x = uv$. We denote the prefix of length n of x by $\mathrm{pref}_n(x)$. A word v is said to be a *suffix* of a word x if there exists a word u such that $x = uv$.

Let x be a word of length $n > 0$. For any positive integer i, there exists an integer i_0 such that $i = qn + i_0$ $(1 \le i_0 \le n)$. We denote by $\mathrm{P}_i(x)$ the i_0-th letter of x.

We define a mapping Shift: $\Sigma^* \to \Sigma^*$, inductively as follows:

$$\mathrm{Shift}^{i+1}(x) = \mathrm{Shift}(\mathrm{Shift}^i(x))$$
$$\mathrm{Shift}^1(x) = \mathrm{Shift}(x) = a_2 \cdots a_n a_1.$$

It is clear that $(\mathrm{Shift}^i(x))^j = \mathrm{Shift}^i(x^j)$ for all positive integers i, j.

By the proof of Proposition 1.3.5 of [2], we have the following proposition 1.

Proposition 1. Let $p, s \in \Sigma^+$, $|p| + |s| = n$, $\gcd(|p|, |s|) = 1$. If $\mathrm{Pref}_{n-1}(sp) = \mathrm{Pref}_{n-1}(ps)$, then there exists a letter a such that $ps = sp = a^n$.

Although the following proposition is obtained immediately by Proposition 1, the result is essential.

Proposition 2. Let $p, s \in \Sigma^+$, $|p| + |s| = n$, $\gcd(|p|, |s|) = 1$. If there exists $j \in \{1, 2, \cdots, n\}$ such that $P_i(ps) = P_i(sp)$ for $i \neq j$ $(1 \leq i \leq n)$, then there exists a letter a such that $ps = sp = a^n$.

Proof. Let $ps = a_1a_2 \cdots a_n$, $sp = b_1 \cdots b_n$, $\text{Shift}^j(ps) = a'_1a'_2 \cdots a'_n$, $\text{Shift}^j(sp) = b'_1b'_2 \cdots b'_n$. We have $a'_i = P_i(\text{Shift}^j(ps)) = P_{i+j}(ps)$ for $i \in \{1, 2, \cdots, n-1\}$. Since $i + j \not\equiv j \pmod n$, we have $a'_i = P_i(\text{Shift}^j(ps)) = P_{i+j}(ps) = P_{i+j}(sp) = P_i(\text{Shift}^j(sp)) = b'_i$ for every $i \in \{1, 2, \cdots, n-1\}$. On the other hand, let $|p| = m$, $a'_1 \cdots a'_m = p'$, $a'_{m+1} \cdots a'_n = s'$, then $b'_1 \cdots b'_n = \text{Shift}^j(sp) = \text{Shift}^j(a_{m+1} \cdots a_n a_1 \cdots a_m) = \text{Shift}^j(\text{Shift}^m(ps)) = \text{Shift}^m(\text{Shift}^j(ps)) = \text{Shift}^m(a'_1 \cdots a'_n) = a'_{m+1} \cdots a'_n a'_1 \cdots a'_m = s'p'$. Therefore, we have $\text{Pref}_{n-1}(s'p') = \text{Pref}_{n-1}(p's')$. It is obvious that $\gcd(|p'|, |s'|) = \gcd(|p|, |s|) = 1$. By Proposition 1, there exists a letter a such that p' and s' are powers of a. This shows that $ps = sp = a^n$.

Proposition 3. Let $p, s \in \Sigma^+$, $|p| + |s| = n$, $\gcd(|p|, |s|) = d$. If there exist $j, k \in \{1, 2, \cdots, n\}$ such that $P_j(ps) \neq P_k(ps)$ and that $j - k$ is divisible by d, then there are no word x such that p, s are powers of the word x.

Proof. Suppose that p, s are powers of the same x and $ps = x^r$. Since $|x|$ is divisor of d, for every integers $j, k \in \{1, 2, \cdots, n\}$ such that $j - k$ is divisible by d, $P_j(ps) = P_j(x^r) = P_k(x^r) = P_i(sp)$.

Theorem 4. Let $p, s \in \Sigma^+$, $|p| + |s| = n$, $\gcd(|p|, |s|) = d$. Words p, s are powers of the same word if and only if there exists a subset $J = \{j_1, j_2, \cdots, j_k\} \subset I = \{1, 2, \cdots, n\}$ such that (1) for $i \in I - J$, we have $P_i(ps) = P_i(sp)$, (2) for $j, j' \in I - J$, $j - j'$ is not divisible by d. Then we have $p = x^{|p|/d}$ and $s = x^{|s|/d}$ where $x = \text{Pref}_d(ps)$.

Proof. By Proposition 3, the condition is necessary. We prove that the condition is sufficient. Let $ps = a_1a_2 \cdots a_n$, $|p| = m$. For $k \in \{1, 2, \cdots, d\}$, we denote $a_ka_{k+d} \cdots a_{k+(m-d)}$ and $a_{k+m} \cdots a_{k+(q-1)d}$, by p_k and s_k, respectively. Since $k \equiv k + d \equiv \cdots \equiv k + (q-1)d \pmod d$ and the condition of

J, the set $\{k, k+d, \cdots, k+(q-1)d\} \cap J$ contains only one element, say j_k. We then have $P_i(p_k s_k) = P_i(s_k p_k)$ for $i \in \{k, k+d, \cdots, k+(q-1)d\} - \{j_k\}$. It is easy to see that gcd($|p_k|$, $|s_k|$) = 1. By Proposition 2, there exists a letter c_k such that $p_k s_k = s_k p_k = c_k^q$ for $k \in \{1, 2, \cdots, d\}$. Therefore, we have $p = x^{|p|/d}$ and $s = x^{|s|/d}$ where $x = (c_1 c_2 \cdots c_d)^q = \mathrm{Pref}_d(ps)$..

Example 1. Let $ps = c_1c_2c_3?c_5c_6c_7c_8?c_{10}c_{11}c_{12}c_{13}?c_{15}$, $sp = c_1c_2c_3?c_5c_6c_7c_8?c_{10}c_{11}c_{12}c_{13}?c_{15}$, and $|p| = 9$. The set $J = \{1, 2, \cdots, 16\} - \{4, 9, 14\}$ satisfies the conditions of the theorem. Therefore, we have $p = (c_1c_2c_3)^3$ and $s = (c_1c_2c_3)^2$.

Corollary 5. Let $p, s \in \Sigma^+$, $|p| + |s| = n$, gcd($|p|$, $|s|$) = d. If there exists integer k such that $\mathrm{Pref}_{n-d}(\mathrm{Shift}^k(ps)) = \mathrm{Pref}_{n-d}(\mathrm{Shift}^k(sp))$, then we have $p = x^{|p|/d}$ and $s = x^{|s|/d}$ where $x = \mathrm{Shift}^{n-k}(\mathrm{Pref}_d(\mathrm{Shift}^k(ps)))$.

Proof. Let $ps = a_1a_2 \cdots a_n$, then there is an integer $t \in \{1, 2, \cdots, n\}$ such that $a_t = P_{n-d}(\mathrm{Shift}^k(ps))$. Since set $J = I - \{t+1, t+2, \cdots, t+d\}$ satisfies the conditions of Theorem 4, we have $ps = sp = x^{n/d}$ where $x = a_1a_2 \cdots a_d$. On the other hand, we have $a_1a_2 \cdots a_d = \mathrm{Pref}_d(ps) = \mathrm{Pref}_d(\mathrm{Shift}^{n-k}(\mathrm{Shift}^k(ps))) = \mathrm{Pref}_d(\mathrm{Shift}^{n-k}(\mathrm{Shift}^k((a_1a_2 \cdots a_d)^{n/d}))) = \mathrm{Pref}_d(\mathrm{Shift}^{n-k}(\mathrm{Shift}^k(a_1a_2 \cdots a_d)))$ $= \mathrm{Shift}^{n-k}(\mathrm{Pref}_d(\mathrm{Shift}^k(a_1a_2 \cdots a_d))) = \mathrm{Shift}^{n-k}(\mathrm{Pref}_d((\mathrm{Shift}^k(a_1a_2 \cdots a_d))^{n/d})) = \mathrm{Shift}^{n-k}(\mathrm{Pref}_d(\mathrm{Shift}^k((a_1a_2 \cdots a_d)^{n/d}))) = \mathrm{Shift}^{n-k}(\mathrm{Pref}_d(\mathrm{Shift}^k(ps)))$

Example 2. Let $p, s, x, y, u, v \in \Sigma^+$, $ps = vxu$, $sp = vyu$, $|p| = 9$, $|x| = 3$, $|u| = 5$, $\mathrm{Pref}_3(u) = abc$. Since $\mathrm{Pref}_{12}(\mathrm{Shift}^{10}(ps)) = uv = \mathrm{Pref}_{12}(\mathrm{Shift}^{10}(sp))$. On the other hand, $\mathrm{Shift}^{15-10}(\mathrm{Pref}_3(\mathrm{Shift}^{10}(ps))) = \mathrm{Shift}^5(\mathrm{Pref}_3(uv)) = \mathrm{Shift}^{10}(\mathrm{Pref}_3(uv)) = \mathrm{Shift}^{10}(abc) = \mathrm{Shift}(abc) = bca$. Hence, Corollary 5 shows that $p = x^3$ and $s = x^2$ where $x = \mathrm{Shift}^{15-10}(\mathrm{Pref}_3(\mathrm{Shift}^{10}(ps))) = bca$. Therefore, we have $p = (bca)^3$ and $s = (bca)^2$.

References

[1] N. J. Fine and H.S. Wilf, Uniqueness theorem for periodic functions, Proc. Am. Math Soc., (1965), 109-114.
[2] M. Lothair, Combinatrics on Words, Cambridge Univ. Press, 1983.