数理解析研究所講究録
1503 巻 2006 年 148-155

A note on d-primitive words, cyclic-square-free words, and disjunctive languages

Tetsuo MORIYA

Department of Electrical Engineering, Faculty of Engineering
Kokushikan University
Setagaya 4-28-1, Setagaya-ku, Tokyo 154-8515, Japan
Electric Mail: moriya@kokushikan.ac.jp

Summary

In this paper, we give some resuts on d-primitive words, square-free words and disjunctive languages. We show that for a word $u \in \Sigma^{+}$, every element of $\lambda(cp(u))$ is d-primitive iff it is square-free, and also we give a condition of disjunctiveness for a language, which strengthens the result in [5].

Keywords: d-primitive word, square-free word, principal congruence, disjunctive language

1 Introduction

A lot of studies have been done for primitive words and square-free words, which concern the decomposition and combination of word. (See for example [6], [7].) On the other hand, various research have been done about properties of a disjunctive langauge. [5], [4].

In this paper, we give some resuts on d-primitive words, square-free words and disjunctive languages. In section 2, we show that for a word $u \in \Sigma^+$, every element of $\lambda(cp(u))$ is d-primitive iff it is square-free. In section 3, we study some properties of disjunctive languages. First we show that $p^m q^n$ is a primitive word for every $n, m \geq 1$ and primitive words p, q, under the condition that $|p| = |q|$ and $(m, n) \neq (1, 1)$. Next we give the rearranged proof for Proposition 4.17 [5] by using the above result. Moreover we investigate a condition of disjunctiveness for a language and give the result which strengthens this proposition.

2 Preliminaries

Let Σ be an alphabet consisting of at least two letters. Σ^* denotes the free moniod generated by Σ, that is, the set of all finite words over Σ, including the empty word 1, and $\Sigma^+ = \Sigma^* - 1$. For w in Σ^* $|w|$ denotes the length of w. A *language* over Σ is a set $L \subseteq \Sigma^*$.

For a word $u \in \Sigma^+$, if $u = vw$ for some $v, w \in \Sigma^*$, then $v(w)$ is called a *prefix(suffix)* of u, denoted by $v \leq_p u$ $(w \leq_u)$.

For a language $L \subseteq \Sigma^*$, we define $L^{(i)} = \{w^i | w \in L\}$ for $i \geq 1$. A nonempty word u is called a *primitive word* if $u = f^n$, $f \in \Sigma^+$, $n \geq 1$ always implies that $n = 1$. Let Q be the set of all primitive words over Q. For $u = p^i$, $p \in Q$, $i \geq 1$, let $\lambda(u) = p$, and call p the *primitive root of* u. For a language $L \subseteq \Sigma^+$, let $\lambda(L) = \{\lambda(u) | u \in L\}$. A nonempty word u is a *non-overlapping word* if $u = vx = yv$ for $x, y \in \Sigma^+$ always implies that $v = 1$. Let $D(1)$ be the set of all non-overlapping words over Σ. A words in $D(1)$ is also called a *d-primitive word.* Let $D = D(1) \cup [D(1)]^{(2)} \cup [D(1)]^{(3)} \cup \cdots$. By definition, it is immediate that $\lambda(D) = D(1)$ and that $Q \cap D = D(1)$. A word $x \in \Sigma^+$ is a *cyclic square free word* if $u = v_1 w^2 v_2$ for any $v_1, w, v_2 \in \Sigma^*$ always implies $w = 1$. For a word $u \in \Sigma^+$, $u = xy, x, y \in \Sigma^*$, yx is called a *cyclic permutation* of the word u. Let $cp(u)$ be the set of all cyclic permutations of the word u. That is, $cp(u) = \{yx | u = xy, x, y \in \Sigma^*\}$.

A word $u \in \Sigma^+$ is *λ-cyclic-squre-free word* if $\lambda(cp(u))$ is square-free. $\lambda(u)$ is called a *cyclic-square-free word* if a word u is λ-cyclic-squre-free. Let SF be the set of all square-free words and CSF be the set of all cyclic-squre-free words, and $\lambda - CSF$ be the set of all λ-cyclic-squre-free words.

For a language L, the equivalence relation P_L on Σ^*, called the *principal congruence* by L is defined as $u \equiv v \quad (P_L)$ if and only if ($xuy \in L \Longleftrightarrow xvy \in L$ for any $x, y \in \Sigma^*$).

If P_L is the equality, then we call L a *disjunctive* language.

3 premitive words and cyclic-square-free words

In this section, we show that for a word $u \in \Sigma^+$, every element of $\lambda(cp(u))$ is d-primitive iff it is square-free.

Lemma 1 *$cp(cp(u)) = cp(u)$ for every $u \in \Sigma^+$.*

Proof. Since $u \in cp(u)$, it is obvious that $cp(u) \subseteq cp(cp(u))$. Suppose that $w \in cp(cp(u))$. We can write $u = yx$, and $w \in cp(xy)$ for $x, y \in \Sigma^*$. Let $u = a_1 ... a_i a_{i+1} ... a_n$; $x = a_{i+1} ... a_n, y = a_1 ... a_i$. Since $xy = a_{i+1} ... a_n a_1 ... a_i$, we can write $w = a_k ... a_i a_{i+1} ... a_n a_1 ... a_{k-1}$, with $k < i$, or $w = a_k ... a_n a_1 ... a_n a_1 ... a_i a_{i+1} ... a_{k-1}$, with $i < k$. In either case, $w \in cp(u)$. □

Lemma 2 *For $u \in \Sigma^+$, $i \geq 1$, $cp(u^i) = (cp(u))^{(i)}$.*

Proof. Let $xy = u^i$ for $x, y \in \Sigma^*$. For $yz \in cp(u^i)$, and $u = u_1 u_2$ with $u_1, \in \Sigma^+; u_2 \in \Sigma^*$, we can write as $yx = u_2 u ... u u_1 = (u_2 u_1)^i \in (cp(u))^{(i)}$. Thus $cp(u^i) \subseteq (cp(u))^{(i)}$. Conversely, suppose that $u = vw$ for $v \in \Sigma^+, w \in \Sigma^*$. We have that $(wv)^i = w(vw)^{i-1} v \in cp((vw)^i) = cp(u^i)$. Hence $(cp(u))^{(i)} \subseteq cp(u^i)$. □

Lemma 3 *[3] Let $u \in \Sigma^+$. Then $u \notin D(1)$ if and only if there exists a unique word $v \in D(1)$ with $|v| \leq (1/2)|u|$ such that $u = vwv$ for some $w \in \Sigma^*$.*

Proposition 4 *For $u \in \Sigma^+$, the following two statements are equivalent.*
(1) $cp(u) \subseteq D(1)$.
(2) $cp(u) \subseteq SF$.

Proof. [(1) $\Rightarrow$ (2)] Suppose that $cp(u) \not\subseteq SF$. There exist x and y such that $xy = u$ and $yx \notin SF$. We can write $yx = z_1 w^2 z_2$ for $z_1, z_2 \in \Sigma^*$, and $w \in \Sigma^+$. Hence $wz_1z_2w \in cp(yx) \subseteq cp(cp(u)) = cp(u)$ by Lemma 1. Thus $cp(u) \not\subseteq D(1)$.
[(2) $\Rightarrow$(1)] Suppose that $cp(u) \not\subseteq D(1)$. There exist x and y such that $xy = u$ and $yx \notin D(1)$. We can write $yx = wvw$ for $v \in \Sigma^*$, and $w \in \Sigma^+$ by Lemma 3. Hence $vw^2 \in cp(yx) \subseteq cp(cp(u)) = cp(u)$. Thus $cp(u) \not\subseteq SF$. □

Lemma 5 *For $u \in \Sigma^+$, $\lambda(cp(u)) = cp(\lambda(u))$.*

Proof. Let $u = f^i$ for $f \in Q$. By Lemma 2, it follows that $\lambda(cp(u)) = \lambda(cp(f^i)) = \lambda((cp(f))^{(i)})$. Since $cp(f) \subseteq Q$, we have that $\lambda((cp(f))^{(i)}) = cp(f) = cp(\lambda(u))$. Thus the result holds. □

Corollary 6 *The following two statements are equivalent for $u \in \Sigma^+$.*
(1) $\lambda(cp(u)) \subseteq D(1)$.
(2) $\lambda(cp(u)) \subseteq SF$.

Proof. Let $u = f^i$ for $f \in Q$, and $i \geq 1$. By Lemma 5, it follows that $\lambda(cp(u)) = cp(f)$. Since $cp(f) \in D(1)$ if and only if $cp(f) \in SF$ by Proposition 4, the result holds. □

4 disjunctive languages

In this section, we study some properties of disjunctive languages. Next two Lemmnas are well-known results

Lemma 7 *[6] Let $uv = f^i$, $u, v \in \Sigma^+$, $f \in Q$, $i \geq 1$. Then $vu = g^i$ for some $g \in Q$.*

Lemma 8 *[8] Let $u, v \in \Sigma^+$. If $uv = vu$, then u and v are powers of a common primitive words.*

The following two lemmmas are immediate.

Lemma 9 *If $f \in Q$, then $cp(f) \subseteq Q$.*

Lemma 10 *If $pq = qp$ for $p, q \in Q$, then $p = q$.*

The following is the key lemma for results in this section.

Lemma 11 *If $y = xx' \in Q$ with $x, x' \in \Sigma^+$, then $(xx')^k x \in Q$ for $k \geq 2$.*

Proof. Suppose that $(xx')^k x \notin Q$. Let $(xx')^k x = p^j$ for $p \in Q$, and $j \geq 2$.
(Case 1)$|x| > |p|$
Then $x = p^s u_1 = u_2 p^s$ with $|u_1| = |u_2| < |p|$ for some $s \geq 1$, and $p = u_1 u_1' = u_2' u_2$ with $|u_1'| = |u_2'|$. Since $(u_1 u_1')^s u_1 = u_2(u_2' u_2)^s$, we have that $u_2' = u_1'$, and $u_1 = u_2$. Hence $x = p^s u_1 = u_1 p^s$. Both p^s and u_1 are in a^+ for some $a \in \Sigma$. Thus $p \in a^+$, and $x' \in a^+$. This contradicts to that $y \in Q$.
(Case 2) $|x| < |p|$
(2.1) $p = (xx')^s w = w'(x'x)^s$ for $s \geq 1$, and some w, $w' \in \Sigma^+$ with $|w| = |w'|$, and $w <_p x$, $w' <_s x$. Let $x = wz = z'w'$. Since $(xx')^k x = p^j$, $(wzx')^k(wz) = ((wzx')^s w)^j$. It follows that $(x'w)z = z(x'w)$. This implies that both $x'w$ and z are in a^+ for some $a \in \Sigma$. Thus both x and x' are also in a^+. Hence $y \in a^t$ for $t \geq 2$. This is a contradiction.
(2.2) $p = (xx')^s xu = u'x(x'x)^s$ for $s \geq 0$, and u, $u' \in \Sigma^+$ with $|u| = |u'|$, and $u <_p x'$, $u' <_s x'$. Let $x' = uv = v'u'$.
(2.2.1) $s \geq 1$

Since $(xx')^k x = p^j$, $(xuv)^k x = ((xuv)^s xu)^j$, $uvx = vxu$. we have that y is in a^t for $t \geq 2$. This is a contradiction.

(2.2.2) $s = 0$

If $v <_p x$, then we can write $x = vv_1$ for some $v_1 \in \Sigma^+$. Since $(xx')^k x = p^j$, $(xuv)^k x = (xu)^j$. Since $k \geq 2$, $vxu = xuv$. Thus $p = xu, v \in a^+$ for some $a \in \Sigma$. we have that $p \in a^t$ for some $a \in \Sigma$ and $t \geq 2$. This is a contradiction. If $x <_p v$, then we can write $x' = up^t w$, for $t \geq 0$, and $p = ww'$ $w' \in \Sigma^+$. Since $(xx')^k x = p^j$, $w(p^{t+1}w)^{k-1}x = p^{j-t-1}$, that is, $w((ww')^{t+1})^{k-1}x = (ww')^{j-t-1}$. By $k \geq 2$, we have that $j \geq t+3$, that is, $j-t-1 \geq 2$. Thus $www' = ww'w$. This implies that both w and w' is in a^+ for some $a \in \Sigma$. Hence $p \notin Q$. This is a contradiction. if $x = v$, then we have that $xu = ux = x'$ since $(xux)^k x = (xu)^j$ for $k \geq 2$. Thus $y = xx' \notin Q$. □

Remark 1 *Unfortunately, the previous Lemma does not hold for $k = 1$. For example, for $\Sigma = \{a, b\}$, let $x = abba$, $x' = bbaabb$. Then $xx'x = (abbabba)^2 \notin Q$.*

Proposition 12 *For $p, q \in Q$ with $p \neq q$ and $|p| = |q|$, $pq^n \in Q$ and $p^n q \in Q$ for every $n \geq 2$.*

Proof. It suffices to show that $pq^n \in Q$. Let $p, q \in Q$ and $p \neq q$. Suppose that there exists $y \in Q$ such that $pq^n = y^r$ for some $r \geq 2$. If $|y| = |p|$, that is, $p = y$, then immediately $y = q$. This contradicts that $p \neq q$.

(Case 1) $|y| < |p|$

Let $p = y^s x$ for some $s \geq 1$ and $x \in \Sigma^+$ with $x <_p y$. Thus $x <_p$, and $x <_s p$. Let $y = xx'$ for $x' \in \Sigma^+$. By $pq^n = y^r$, $n \geq 2$, and $|p| = |q|$, we have that $q^n = (x'x)^{r-s-1}x'$ with $r \geq (n+1)s+1$. Since $r-s-1 \geq ns \geq 2$, and $x'x \in Q$, it follows that $(x'x)^{r-s-1}x'$ is in Q by the Lemma 11. This is a contradiction.

(Case 2) $|p| < |y|$

If $y = pq^s$ for $s \geq 0$, then $p \in q^+$. This contradicts to that $p, q \in Q$ and $p \neq q$. Thus $y = pq^t x$ for some $t \geq 0$ and $x \in \Sigma^+$ with $x <_p q$. Let $q = xw$ for $\in \Sigma^+$. If $r = 2$, then we have that $pq^t x = wq^{n-t-1}$ and $|x| = |w| = (1/2)|q|$. It follows that $q = xw = wx$. This implies that $q \notin Q$. Thus $r \geq 3$. Let $z = q^t x$. Since $pq^n = y^r$, $q^n = (zp)^{r-1}z$ with $r-1 \geq 2$. Since $y = pz \in Q$, and $n \geq 2$, this conradicts to the Lemma 11. □

Corollary 13 *For $p, q \in Q$ with $p \neq q$ and $|p| = |q|$, $p^n q^m \in Q$ for every $n, m \geq 1$ with $(n, m) \neq (1, 1)$.*

Proof. Let $p, q \in Q$ with $p \neq q$ and $|p| = |q|$. If $n \geq 2$ and $m \geq 2$, then $p^n q^m \in Q$ in either $|p| = |q|$ or not, by [5]. For other cases, the result holds by Proposition 10. □

Remark 2 *As mentioned in [5], the previous corollary does not hold for* $n = 1$, $m \geq 2$ *or* $n \geq 2$, $m = 1$ *without the condition* $|p| = |q|$. *On the other hand, for* $n = m = 1$, *let* $p = aba$ *and* $q = bab$. *Then* $pq = (ab)^3 \notin Q$.

Corollary 14 *Let* $p, q \in Q$ *with* $p \neq q$ *and* $|p| = |q|$. *Then* $pqp^n \in Q$ *and* $p^nqp \in Q$ *for every* $n \geq 2$.

Proof. Since $n+1 \geq 2$, $qp^{n+1} \in Q$ and $p^{n+1}q \in Q$ by Proposition 12. By Lemma 9, $pqp^n \in cp(qp^{n+1}) \subseteq Q$ and $p^nqp \in cp(p^{n+1}q) \subseteq Q$. □

Proposition 15 *[6] Let* $A \subseteq X^*$. *Then the folllowings are equivalent.*
(1) A *is a disjunctive language.*
(2) If $u, v \in X^*$, $|u| = |v|$, *and* $u \equiv v\ (P_A)$, *then* $u = v$.
(3) If $u, v \in Q$, $|u| = |v|$, *and* $u \equiv v\ (P_A)$, *then* $u = v$.

Proof. (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), and (3) are immediate. (3) $\Rightarrow$ (1).
Suppose that (3) holds and let x, $y \in \Sigma^*$ be such that $x \equiv y$. Take $a \in \Sigma$. Let $\alpha = axab^n$ and $\beta = ayab^n$ with $n \geq 2max\{|x|, |y|\} + 2$. Hence we have tha both α and β are primitive, and $\alpha \equiv \beta(P_A)$. Moreover, $\alpha\alpha \equiv \alpha\beta \equiv \beta\alpha(P_A)$.
(Case 1) $\alpha\beta \in Q$
By Lemma 9, $\beta\alpha \in Q$. Since $|\alpha\beta| = |\beta\alpha|$, $\alpha\beta = \beta\alpha$ by (3). By Lemma 10, we have that $\alpha = \beta$. Hence $x = y$.
(Case 2) $\alpha\beta \notin Q$.
(2.1) $\alpha = \beta$. Immediately $x = y$.
(2.2) $\alpha \neq \beta$. By Proposition 12 and Corollary 13, both $\alpha\alpha\alpha\beta$ and $\alpha\alpha\beta\alpha$ are in Q. Since $|\alpha\alpha\alpha\beta| = |\alpha\alpha\beta\alpha|$, we have that $\alpha\alpha\alpha\beta = \alpha\alpha\beta\alpha$ by (3). It follows that $\alpha\beta = \beta\alpha$. By Lemma 10, we see that $\alpha = \beta$. Thus $x = y$. □

Proposition 16 *Let* $A \subseteq X^*$. *Then the folllowings are equivalent.*
(1) A *is a disjunctive language.*
(2) If $u, v \in X^*$, $|u| = |v|$, *and* $u \equiv v\ (P_A)$, *then* $u = v$.
(3) If $u, v \in Q$, $|u| = |v|$, *and* $u \equiv v\ (P_A)$, *then* $u = v$.
(4) If $u, v \in D(1)$, $|u| = |v|$, *and* $u \equiv v\ (P_A)$, *then* $u = v$.

Proof. (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), and (3) $\Rightarrow$ (4) are immediate.

[(3) $\Rightarrow$ (1)] (See [6])

[(4) $\Rightarrow$ (2)] Suppose (4) holds, and let $x, y \in X^*$ be such that $|x| = |y|$ and $x \equiv y\ (P_A)$. Take $b \in X$. Then $bxb \equiv byb(P_A)$. For $n > |bxb| = |byb|$, consider the word $\alpha = bxba^n$ and $\beta = byba^n$ with $a \neq b$. It is easy to see that α, $\beta \in D(1)$. Since $|\alpha| = |\beta|$ and $\alpha \equiv \beta\ (P_A)$, we have that $\alpha = \beta$. Hence $x = y$. Thus (2) holds. □

References

[1] J. Berstel and D. Perrin, Theory of Codes, Academic Press, New York, 1985

[2] M.Ito, H. Jürgensen, H. J. Shyr and G. Thierrin, Outfix and infix codes and related classes of languages, Jounal of Comp. and Sys. Sci. vol 43, pp 484-508, 1991.

[3] Hsu, S.C., Ito, M., Shyr, H.J.: Some properties of overlapping order and related languages. Soochow Journal of Mathematics 15, 29-45 (1989).

[4] C.M.Reis and H.J.Shyr, Some properties of disjunctive languages on free monoid. Information and Comtrol, vol 37, pp 334-344, 1978.

[5] H.J.Shyr, Disjunctive languages on a free monoid, Information and Comtrol, vol 34, pp 123-129, 1977.

[6] H.J.Shyr, Free monoids and languages, Hon Min Book company, Taichung, Taiwan, 2001

[7] Chen-Ming Fan, H.J.Shyr, S.S.Yu, d-words and d-languages, Acta Informatica, vol 35, pp 709-727, 1998.

[8] Lyndon, R.C., Shützenberger, M.P.:The equation $a^M = b^N c^P$ in a free group. Michigan Math. J.9, pp289-298, 1962.