IEICE TRANS. INF. & SYST., VOL.E91–D, NO.10 OCTOBER 2008

LETTER

# Some Results on Primitive Words, Square-Free Words, and Disjunctive Languages

**Tetsuo MORIYA**[†a)], ***Member***

**SUMMARY** In this paper, we give some resuts on 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, where $cp(u)$ is the set of all cyclic-permutations of $u$, and $\lambda(cp(u))$ is the set of all primitive roots of it. Next 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 $(m, n) \neq (1, 1)$. We also give a condition of disjunctiveness for a language.

***key words:*** *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 words. (See for example [4], [5].) On the other hand, various research have been done about properties of a disjunctive langauge. [2], [3].

In this paper, we give some resuts on primitive words, square-free words and disjunctive languages. In Sect. 2, some basic definitions are presented. In Sect. 3, we show that for a word $u \in \Sigma^+$, every element of $\lambda(cp(u))$ is d-primitive iff it is square-free, where $cp(u)$ is the set of all cyclic-permutations of $u$, and $\lambda(cp(u))$ is the set of all primitive roots of it. This is an arrangement of the relation between d-primitive words and squre-free words by means of a cyclic permutation. Next 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 $(m, n) \neq (1, 1)$. This strengthen the result in [6] that $q^m q^n$ is primitive for two distinct primitive words $p$, $q$, and integers $m, n \geq 2$. In Sect. 4, we study disjunctive languages. We give a condition of disjunctiveness for a language. This result is an improved one for Proposition 4.7 [4].

## 2. Preliminaries

Let $\Sigma$ be an alphabet consisting of at least two letters. $\Sigma^*$ denotes the free moniod generated by $\Sigma$, that is, the set of all finite words over $\Sigma$, including the empty word 1, and $\Sigma^+ = \Sigma^* - 1$. For $w$ in $\Sigma^*$ $|w|$ denotes the length of $w$. A *language* over $\Sigma$ is a set $L \subseteq \Sigma^*$. For a language $L \subseteq \Sigma^*$, we define $L^* = \bigcup_{i=0}^{\infty} L^i$ and $L^+ = \bigcup_{i=1}^{\infty} L^i$. For a word $u \in \Sigma^+$, by $u^+$ we mean the set $\{u\}^+$.

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 $v \leq_p u$ ($w \leq_s u$, *resp.*). If $v \leq_p u$ ($w \leq_s u$) and $u \neq v(w \neq u)$, then $v$ ($w$) is called a *proper prefix (proper suffix)* of $u$, denoted by $v <_p u$ ($w <_s u$, resp.).

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 $\Sigma$. 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 $\Sigma$. A word 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 the definition, it is immediate that $\lambda(D) = D(1)$ and that $Q \cap D = D(1)$. A word $u \in \Sigma^+$ is a *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, $cp(u) = \{yx | u = xy, x, y \in \Sigma^*\}$. For a language $L \subseteq \Sigma^+$, let $cp(L) = \{cp(u) | u \in L\}$.

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

For a language $L$, the equivalence relation $P_L$ on $\Sigma^*$, called the *principal congruence* by $L$ is defined as $u \equiv v$ $(P_L)$ if and only if ($xuy \in L \iff xvy \in L$ for any $x, y \in \Sigma^*$). If $P_L$ is the equality, then we call $L$ a *disjunctive* language.

## 3. Primitive Words and 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 $u \in \Sigma^+$. In other words, for every $u$ and $w \in \Sigma^+$, if $w \in cp(u)$, then $cp(u) = cp(w)$.

[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 $x = a_{i+1} \ldots a_n, y = a_1 \ldots a_i$. It

Manuscript received March 5, 2008.
Manuscript revised June 13, 2008.

[†]The author is with School of Science and Engineering, Kokushikan University, Tokyo, 154–8515 Japan.
a) E-mail: moriya@kokushikan.ac.jp

DOI: 10.1093/ietisy/e91–d.10.2514

is obvious that $w \in cp(xy) \subseteq cp(u)$. ::

**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 $yx \in cp(u^i)$, and $u = u_1u_2$ with $u_1 \in \Sigma^+; u_2 \in \Sigma^*$, we can write as $yx = u_2u \ldots uu_1 = (u_2u_1)^i \in (cp(u))^{(i)}$. 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:** [1] 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 $w \in \Sigma^*$.

Next two lemmnas are well-known results.

**Lemma 4:** [4] Let $uv = f^i$, $u, v \in \Sigma^+$, $f \in Q$, $i \geq 1$. Then $vu = g^i$ for some $g \in Q$.

**Lemma 5:** [6] Let $u, v \in \Sigma^+$. If $uv = vu$, then $u$ and $v$ are powers of a common primitive word.

The following is immediate by Lemmas 4 and 5.

**Lemma 6:** If $f \in Q$, then $cp(f) \subseteq Q$.

**Proposition 7:** For $u \in \Sigma^+$, the following are equivalent.
(1) $cp(u) \subseteq D(1)$.
(2) $cp(u) \subseteq SF$.

[Proof] [(1) $\Rightarrow$ (2)] Suppose that $cp(u) \nsubseteq SF$. There exist $x$ and $y$ such that $xy = u$ and $yx \notin SF$. We can write $yx = z_1w^2z_2$ 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 $cp(u) \nsubseteq D(1)$.
[(2) $\Rightarrow$(1)] Suppose that $cp(u) \nsubseteq D(1)$. 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 $cp(u) \nsubseteq SF$. ::

**Lemma 8:** 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 $cp(f) \subseteq Q$ by Lemma 6, we have that $\lambda((cp(f))^{(i)}) = cp(f) = cp(\lambda(u))$. Thus the result holds. ::

**Corollary 9:** The following 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. ::

Now we consider a word $p^mq^n$ for $m, n \geq 1$, and $p, q \in Q$.

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

**Lemma 10:** If $y = xx' \in Q$ with $x, x' \in \Sigma^+$, then $(xx')^kx \in Q$ for every $k \geq 2$.

[Proof] Suppose that $(xx')^kx \notin Q$. Let $(xx')^kx = p^j$ for some $p \in Q$, and some $j \geq 2$.
(Case 1)$|x| > |p|$
If $x = p^t$ for some $t \geq 2$, then $x' = p^s$ for some $s \geq 1$. This contradicts that $y \in Q$.
We can write $x = p^su_1 = u_2p^s$ with $|u_1| = |u_2| < |p|$ for some $s \geq 1$, and $p = u_1u_1' = u_2'u_2$ with $|u_1'| = |u_2'|$. Since $(u_1u_1')^su_1 = u_2(u_2'u_2)^s$, we have that $u_2' = u_1'$, and $u_1 = u_2$. Hence $p = u_1u_1' = u_1'u_1$. By Lemma 5 both $u_1$ and $u_1'$ are powers of some common primitive word $q$. Thus $p = q^i$ for some $i \geq 2$. This is a contradiction.
(Case 2) $|x| < |p|$
(2.1) $p = (xx')^sw = w'(x'x)^s$ 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 $(wzx')^sw = w'(x'wz)^s$, we have that $w = w'$ and $zx'w = x'wz$. By Lemma 5 both $x'w$ and $z$ are powers of some common primitive word $q$. Let $x'w = q^i$ and $z = q^l$ for some $i, l \geq 1$. Then $x'x = x'wz = q^{i+l}$. By Lemma 9, $x'x = cp(y) \subseteq Q$. This is a contradiction.
(2.2) $p = (xx')^sxu = u'x(x'x)^s$ 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 $(xuv)^sxu = u'x(uvx)^s$, we have that $uvx = vxu$. Thus both $vx$ and $u$ are powers of some common primitive word $q$. Let $vx = q^i$ and $u = q^l$ for some $i, l \geq 1$. Hence $x'x = uvx = q^{i+l}$. This is a contradiction.
(2.2.2) $s = 0$
Since $x <_p p$ and $v <_p p$, we have that $x \leq_p v$ or $v \leq_p x$. If $v <_p x$, then we can write $x = vv_1$ for some $v_1 \in \Sigma^+$. Since $(xx')^kx = p^j$, we have that $vv_1u = v_1uv$. Thus $xx' = vv_1uv = q^i$ for some $q \in Q$ and $i \geq 2$. This is a contradicion. If $x <_p v$, then we can write $x' = up^tw$, and $p = ww'$ for some $t \geq 0$, and $w, w' \in \Sigma^+$. Since $(xx')^kx = p^j$, we have that $w(p^{t+1}w)^{k-1}x = p^{j-t-1}$, that is, $w((ww')^{t+1}w)^{k-1}x = (ww')^{j-t-1}$. Since $w(p^{t+1}w)^{k-1}x = www'\alpha$ and $p^{j-t-1} = ww'w\beta$ for some $\alpha, \beta \in \Sigma^*$, $p = ww' = w'w$. This implies that $p \notin Q$. If $x = v$, then we have that $xu = ux = x'$ since $(xux)^kx = (xu)^j$ 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 11:** For $p, q \in Q$ with $p \neq q$ and $|p| = |q|$, $pq^n \in Q$ and $p^nq \in Q$ 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 $p = y^sx$ for some $s \geq 1$ and $x \in \Sigma^+$ with $x <_p y$. Thus $x <_p p$, 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 10. This is a contradiction.
(Case 2) $|p| < |y|$

If $y = pq^s$ for $s \geq 1$, then $p \in q^+$. This contradicts to that $p, q \in Q$ and $p \neq q$. Thus $y = pq^tx$ for some $t \geq 0$

and $x \in \Sigma^+$ with $x <_p q$. Let $q = xw$ for $w \in \Sigma^+$. 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 $y = pz \in Q$ and $pq^n = y^r = (pz)^r$, it follows that $q^n = (zp)^{r-1}z \in Q$ with $r - 1 \geq 2$ by Lemmas 6 and 10. This is a contradiction::

**Corollary 12:** 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 [3]. For other cases, the result holds by Proposition 11. ::

**Remark 2:** As mentioned in [6], 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 13:** Let $p, q \in Q$ with $p \neq q$ and $|p| = |q|$. Then $pqp^n \in Q$ and $p^n qp \in Q$ 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 11. By Lemma 6, $pqp^n \in cp(qp^{n+1}) \subseteq Q$ and $p^n qp \in cp(p^{n+1}q) \subseteq Q$. ::

## 4. Disjunctive Languages

In this section, we study a condition of disjunctiveness for a language. The following proposition is an improved result for Proposition 4.7 [4].

**Proposition 14:** Let $A \subseteq \Sigma^*$. Then the following 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 [4])
[(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 $\alpha, \beta \in D(1)$. Since $|\alpha| = |\beta|$ and $\alpha \equiv \beta\ (P_A)$, we have $\alpha = \beta$, and thus $x = y$. Accordingly (2) holds. ::

### References

[1] S.C. Hsu, M. Ito, and H.J. Shyr, "Some properties of overlapping order and related languages," Soochow J. Mathematics, vol.15, pp.29–45, 1989.
[2] C.M. Reis and H.J. Shyr, "Some properties of disjunctive languages on free monoid," Information and Control, vol.37, pp.334–344, 1978.
[3] H.J. Shyr, "Disjunctive languages on a free monoid," Information and Control, vol.34, pp.123–129, 1977.
[4] H.J. Shyr, Free monoids and languages, Hon Min Book Company, Taichung, Taiwan, 2001.
[5] C.-M. Fan, H.J. Shyr, and S.S. Yu, "d-words and d-languages," Acta Informatica, vol.35, pp.709–727, 1998.
[6] R.C. Lyndon and M.P. Shützenberger, "The equation $a^M = b^N c^P$ in a free group," Michigan Math. J., vol.9, pp.289–298, 1962.