数理解析研究所講究録
第697巻 1989年 1-15

Initial Literal Shuffles

M.Ito[1] and G.Tanaka[2]

伊藤 正美（京都産業大・理） 田中 源次郎（広島修道大・商）

Abstract : In this paper, we will study several properties of initial literal shuffles which B. Berard introduced as a more constrained form of the well-known shuffle operation. Especially, we are interested in the denseness of initial literal shuffles and principal congruences determined by initial literal shuffles.

Introduction.

In [1], B. Berard introduced the literal shuffle and initial literal shuffle of two languages as more constrained forms of the well-known shuffle operation and investigated several properties of these operations. For instance, she proved that the families of regular languages, of context-sensitive languages and of recursively enumerable sets are closed under literal shuffle operation and initial literal shuffle operation. On the other hand, in [7] G. Tanaka called the initial literal shuffle of two languages the *alternating product* of two languages without knowing the existence of the paper of B. Berard and proved that the ini-

1) Faculty of Science, Kyoto Sangyo University, Kyoto 603, Japan
2) Department of Management Science, Hiroshima Shudo University, Hiroshima 731-31, Japan

tial literal shuffle of two prefix codes becomes a prefix code and the initial literal shuffle of two prefix codes is maximal if and only if each prefix code is maximal. In the present paper, we will study further properties on initial literal shuffles of languages which have not been treated in [1]. Namely, we are interested in the denseness of initial literal shuffles and principal congruences determined by initial literal shuffles.

1. Preliminaries.

Let X be a nonempty finite set, called an *alphabet*, and let X^* be the free monoid generated by X. By 1 we denote the identity of X^*. Any element of X^* is called a *word* over X and 1 is often called the *empty word*. The length of a word x is expressed as $|x|$. Moreover, by X^+ we denote $X^* \setminus \{1\}$. In what follows, we do not distinguish the element of a singleton set from a singleton set itself. Therefore, for instance, X^+ can be expressed as $X^* \setminus 1$. Any subset of X^* is called a *language* over X. Let A, B be languages over X, i.e. $A, B \subseteq X^*$. Then AB means the language $\{xy \mid x \in A, y \in B\}$ and A^i means AA^{i-1} for any integer $i > 1$. Moreover, $A^0 = 1$, i.e. $A^0 = \{1\}$, and $A^+ = \cup_{i=1}^{\infty} A^i$. A word x over X is called *primitive* if $x = y^n$ $(y \in X^*)$ implies $n = 1$. The set of all primitive words over X is denoted by Q.

2. Initial Literal Shuffles.

In this section, we define initial literal shuffles of two words and of two languages.

Definition 2.1. Let $x,y \in X^*$. Then the *initial literal shuffle* $x \blacklozenge y$ of x and y is defined as follows :

(1) If $x = 1$ or $y = 1$, then $x \blacklozenge y = xy$.

(2) Let $x = a_1 a_2 \cdots a_p$ and let $y = b_1 b_2 \cdots b_q$ where $a_i, b_j \in X$.

Then $x \blacklozenge y = a_1 b_1 a_2 b_2 \cdots a_q b_q a_{q+1} a_{q+2} \cdots a_p$ if $p \geq q$,

$= a_1 b_1 a_2 b_2 \cdots a_p b_p b_{p+1} b_{p+2} \cdots b_q$ if $q > p$.

Let $A, B \subseteq X^*$. We define now the *initial literal shuffle* $A \blacklozenge B$ of A and B.

Definition 2.2. The *initial literal shuffle* $A \blacklozenge B$ of A and B is defined as $A \blacklozenge B = \{x \blacklozenge y \mid x \in A, y \in B\}$.

3. Denseness of Initial Literal Shuffles.

A language $A \subseteq X^*$ is called *dense* if $X^*uX^* \cap A \neq \emptyset$ for any $u \in X^*$. On the other hand, a language which is not dense is called *thin*. A language $A \subseteq X^*$ is called *right dense* if $uX^* \cap A \neq \emptyset$ for any $u \in X^*$. Moreover, a language $A \subseteq X^*$ is called *left dense* if $X^*u \cap A \neq \emptyset$ for any $u \in X^*$. In this section, we investigate relationships between these concepts and initial literal shuffles. First, we provide a necessary and sufficient condition for $A \blacklozenge B$ to be dense.

Proposition 3.1. *Let $A, B \subseteq X^*$ be nonempty languages. Then $A \blacklozenge B$ is dense if and only if at least one of A and B is dense.*

Proof. ($\Rightarrow$) Suppose that neither A nor B is dense. Then there exist $u,v \in X^+$ such that $X^*uX^* \cap A = \emptyset$ and $X^*vX^* \cap B = \emptyset$. Let $w = uv$. Obviously, $X^*wX^* \cap A = \emptyset$ and $X^*wX^* \cap B = \emptyset$. We can assume that $|w| > 0$. Let $w = a_1 a_2 \ldots a_r$ where $a_i \in X$ for any i ($i = 1, 2, \cdots, r$). Then

$(w \diamond w)w = a_1{}^2 a_2{}^2 \cdots a_r{}^2 a_1 a_2 \cdots a_r$. Since $A \diamond B$ is dense, $X^*(w \diamond w)wX^* \cap (A \diamond B) \neq \emptyset$, i.e. there exist $x,y \in X^*$ such that $x(w \diamond w)wy \in A \diamond B$. Let $x(w \diamond w)wy = \alpha \diamond \beta$ where $\alpha \in A$ and $\beta \in B$. It is easy to see that $\alpha \in X^*wX^*$ if $|\alpha| \geq |\beta|$ and $\beta \in X^*wX^*$ if $|\beta| > |\alpha|$. This means that $X^*wX^* \cap A \neq \emptyset$ or $X^*wX^* \cap B \neq \emptyset$, a contradiction. Therefore, one of A and B must be dense.

($\Leftarrow$) We consider only the case where A is dense. Let $w \in X^*$ and let $u \in B$. Since A is dense, there exist $x,y \in X^*$ such that $xwy \in A$. We can assume that $|x| \geq |u|$ without loss of generality. Consider $xwy \diamond u = (x \diamond u)wy \in X^*wX^*$. Therefore, $X^*wX^* \cap (A \diamond B) \neq \emptyset$. Q.E.D.

Now we consider right dense languages.

Proposition 3.2. *Let $A, B \subseteq X^*$. If both A and B are right dense, then $A \diamond B$ is right dense.*

Proof. Let $w \in X^*$. We show that $wX^* \cap (A \diamond B) \neq \emptyset$. We can assume that $|w|$ is even without loss of generality. Let $w = a_1b_1a_2b_2 \cdots a_rb_r$ where $a_i, b_j \in X$ $(i, j = 1, 2, \cdots, r)$. Since A and B are right dense, there exist $\alpha, \beta \in X^+$ such that $a_1a_2 \cdots a_r\alpha \in A$ and $b_1b_2 \cdots b_r\beta \in B$. Hence $(a_1a_2 \cdots a_r\alpha) \diamond (b_1b_2 \cdots b_r\beta) = (a_1b_1a_2b_2 \cdots a_rb_r)(\alpha \diamond \beta) = w(\alpha \diamond \beta) \in A \diamond B$. This means that $wX^* \cap (A \diamond B) \neq \emptyset$. Q.E.D.

The fact that $A \diamond B$ is right dense gives no information on A and B.

Example 3.1. Let $A = X^*$ and let $B = X$. Then A is right dense and B is not so. On the other hand, $A \diamond B$ is right dense.

Example 3.2. Let $X = \{a, b\}$, let $A = (X^+ \setminus abX^+) \cup a \cup ab$ and let $B = bX^* \cup abX^* \cup a \cup b$. Then neither A nor B is right dense. However, $A \diamond B$ is right dense, because $A \diamond B \supseteq abX^* \cup a^3X^* \cup a^2bX^* \cup ba^2X^* \cup babX^* \cup b^2aX^* \cup b^3X^*$.

Unlike the case of dense languages, the statement, $A \blacklozenge B$*: right dense* $\Leftrightarrow$ A*: right dense or* B*: right dense*, is not true.

Example 3.3. Let $X = \{a, b\}$, let $A = \{a\}$ and let $B = X^+$. Then $A \blacklozenge B = aX^+$ and thus $A \blacklozenge B$ is not right dense though B is right dense.

However, we can set up some relationship between $A \blacklozenge B$ and B when A is a prefix code. A nonempty language $A \subseteq X^+$ is called a *code* over X if for $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m \in A$ the equality $x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m$ implies that $n = m$ and $x_i = y_i$ for i $(i = 1, 2, \cdots, n)$ (for details, see [2] and [3]). One of the typical codes is a prefix code. A nonempty language $A \subseteq X^+$ is called a *prefix code* over X if $AX^+ \cap A = \varnothing$. Let $v = ux$ where $u,v,x \in X^*$. Then u is called a *left factor* of v. By $u \leq v$ we mean that u is a left factor of v.

Lemma 3.1. *Let* $u,u',v,v' \in X^+$. *If* $u \blacklozenge v = u' \blacklozenge v'$, *then we have at least one of the following :*

(i) $u \leq u'$, *(ii)* $u' \leq u$, *(iii)* $v \leq v'$, *(iv)* $v' \leq v$.

Proof. *Case* 1. $|u| = min\{|u|, |v|, |u'|, |v'|\}$. Let $u = a_1 a_2 \cdots a_p$ where $a_i \in X$. Moreover, let $v = b_1 b_2 \cdots b_q$, $u' = a_1' a_2' \cdots a_r'$ and let $v' = b_1' b_2' \cdots b_s'$ where $b_j', a_k', b_t' \in X$ and $p \leq q,r,s$. Then $u \blacklozenge v = a_1 b_1 a_2 b_2 \cdots a_p b_p b_{p+1} \cdots b_q = u' \blacklozenge v' = a_1' b_1' a_2' b_2' \cdots a_p' b_p' [(a_{p+1}' a_{p+2}' \cdots a_r') \blacklozenge (b_{p+1}' b_{p+2}' \cdots b_s')]$. Therefore, we have $a_i = a_i'$ for i $(i = 1, 2, \cdots, p)$. This implies that $u \leq u'$.

Case 2. $|v| = min\{|u|, |v|, |u'|, |v'|\}$. Let $v = b_1 b_2 \cdots b_q$ where $b_i \in X$. Moreover, let $u = a_1 a_2 \cdots a_p$, $u' = a_1' a_2' \cdots a_r'$ and let $v' = b_1' b_2' \cdots b_s'$ where $a_j', a_k', b_t' \in X$ and $q \leq p,r,s$. Then $u \blacklozenge v = a_1 b_1 a_2 b_2 \cdots a_q b_q a_{q+1} \cdots a_p = u' \blacklozenge v' = a_1' b_1' a_2' b_2' \cdots a_q' b_q' [(a_{q+1}' a_{q+2}' \cdots a_r') \blacklozenge (b_{q+1}' b_{q+2}' \cdots b_s')]$. This implies that $v \leq v'$.

Case 3. $|u'| = min\{|u|, |v|, |u'|, |v'|\}$. In parallel to Case 1, we have u'

$\leq u$.

Case 4. $|v'| = min\{|u|, |v|, |u'|, |v'|\}$. By the same reason as above, we have $v' \leq v$. Q.E.D.

Lemma 3.2. *Let $u,u',v,v' \in X^+$ and let $u \blacklozenge v = u' \blacklozenge v'$. If $|u| = |u'|$, then $u = u'$ and $v = v'$.*

Proof. *Case* 1. $|u| \leq |v|$. Note that $|u \blacklozenge v| = |u' \blacklozenge v'| = |u| + |v| = |u'| + |v'|$. Hence $|u| = |u'| \leq |v| = |v'|$. Let $u = a_1a_2 \cdots a_r$, $u' = a_1'a_2' \cdots a_r'$, $v = b_1b_2 \cdots b_s$ and let $v' = b_1'b_2' \cdots b_s'$ where $a_i,a_j',a_k,b_t' \in X$ and $s \geq r$. Therefore, $a_1b_1a_2b_2 \cdots a_rb_rb_{r+1} \cdots b_s = a_1'b_1'a_2'b_2' \cdots a_r'b_r'b_{r+1}' \cdots b_s'$. Obviously, $a_i = a_i'$ for i ($i = 1, 2, \cdots ,r$) and $b_j = b_j'$ for j ($j = 1, 2, \cdots , s$). Thus $u = u'$ and $v = v'$.

Case 2. $|u| > |v|$. Let $u = a_1a_2 \cdots a_r$, $u' = a_1'a_2' \cdots a_r'$, $v = b_1b_2 \cdots b_s$ and let $v' = b_1'b_2' \cdots b_s'$ where $a_i,a_j',a_k,b_t' \in X$ and $r > s$. Therefore, $a_1b_1a_2b_2 \cdots a_s b_sa_{s+1} \cdots a_r = a_1'b_1'a_2'b_2' \cdots a_s'b_s'a_{s+1}' \cdots a_r'$ and $a_i = a_i'$ for i ($i = 1, 2, \cdots , r$) and $b_j = b_j'$ for j ($j = 1, 2, \cdots , s$). Thus $u = u'$ and $v = v'$. Q.E.D.

Lemma 3.3. *Let $u,u',v \in X^+$. If $u \blacklozenge v \leq u' \blacklozenge v$ and $|u|,|u'| \geq |v|$, then $u \leq u'$.*

Proof. Note that $|u| \leq |u'|$. Let $(u \blacklozenge v)\alpha = u' \blacklozenge v$ where $\alpha \in X^*$. Since $|u| \geq |v|$, $(u \blacklozenge v)\alpha = u\alpha \blacklozenge v$. Therefore, $u\alpha \blacklozenge v = u' \blacklozenge v$. By Lemma 3.2, $u\alpha = u'$, i.e. $u \leq u'$. Q.E.D.

Lemma 3.4. *Let $A, B, K \subseteq X^*$ where K is a finite language and A is a prefix code. Then $A \blacklozenge B$ is right dense if and only if $A \blacklozenge (B \setminus K)$ is right dense.*

Proof. ($\Leftarrow$) Obvious. ($\Rightarrow$) To prove this part, it is enough to show that $A \blacklozenge (B \setminus u)$ is right dense for any $u \in X^*$. Suppose that $A \blacklozenge (B \setminus u)$ is not right dense for some $u \in X^*$. Then there exists $v \in X^+$ such that vX^*

$\cap$ $[A \blacklozenge (B \setminus u)] = \varnothing$. We can assume that $|v| > 2|u|$ without loss of generality. Since $A \blacklozenge B$ is right dense, there exists $\alpha_1 \in X^+$ such that $v\alpha_1 \in A \blacklozenge B$. Therefore, $v\alpha_1 = \alpha \blacklozenge \beta$ for some $\alpha \in A$ and $\beta \in B$. From the fact that $v\alpha_1 \notin A \blacklozenge (B \setminus u)$, we have $v\alpha_1 = \alpha \blacklozenge u$. By the same reason, there exists $\alpha_2 \in X^+$ such that $v\alpha_1\alpha_2 = \alpha' \blacklozenge u$ where $\alpha' \in A$. Consequently, $\alpha \blacklozenge u \leq \alpha' \blacklozenge u$. Note that $|\alpha|, |\alpha'| \geq |u|$. By Lemma 3.3, $\alpha \leq \alpha'$. Since A is a prefix code, $\alpha = \alpha'$ and $\alpha_2 = 1$, a contradiction. Therefore, $A \blacklozenge (B \setminus K)$ must be right dense. Q.E.D.

Lemma 3.5. *Let $u,u',v,v' \in X^+$ and let $u \blacklozenge v = u' \blacklozenge v'$. If $|u| \leq |u'|$ and u is not a left factor of u', then $|v'| < |u|$.*

Proof. Suppose $|v'| \geq |u|$. Since $|u| \leq |u'|$, $|v| \geq |v'|$ and $|v| \geq |u|$. Let $u = a_1a_2 \cdots a_r$, $v = b_1b_2 \ldots b_r\alpha$, $u' = a_1'a_2' \cdots a_r\beta$ and $v' = b_1'b_2' \cdots b_r\gamma$ where $a_i,a_j',b_k,b_t' \in X$ and $\alpha,\beta,\gamma \in X^*$. Since $u \blacklozenge v = u' \blacklozenge v'$, we have $a_1b_1a_2b_2 \cdots a_rb_r\alpha = a_1'b_1'a_2'b_2' \cdots a_r'b_r'(\beta \blacklozenge \gamma)$. Therefore, $a_i = a_i'$ for any i $(i = 1, 2, \cdots, r)$. This means that $u \leq u'$, i.e. u is a left factor of u', a contradiction. Hence $|v'| < |u|$. Q.E.D.

A prefix code $A \subseteq X^+$ is called *maximal* if for any prefix code $B \subseteq X^+$ with $A \subseteq B$ we have $A = B$. It is well known that $A \subseteq X^+$ is maximal if and only if $uX^* \cap AX^* \neq \varnothing$ for any $u \in X^*$.

Proposition 3.3. *Let $A \subseteq X^+$ be a maximal prefix code over X and let $B \subseteq X^*$. Then $A \blacklozenge B$ is right dense if and only if B is right dense.*

Proof. ($\Rightarrow$) Let $u \in A$ with $|u| = min\{|x| \mid x \in A\}$ and let $K = \bigcup_{i<|u|} X^i$. By Lemma 3.4, $A \blacklozenge (B \setminus K)$ is right dense. We show that $B \setminus K$ is right dense. Suppose that $B \setminus K$ is not right sense. Then there exists $v \in X^*$ such that $vX^* \cap (B \setminus K) = \varnothing$. We can assume that $|v| > |u|$ without loss of generality. Since $A \blacklozenge (B \setminus K)$ is right dense, there exists $w \in X^*$ such that $(u \blacklozenge v)w \in A \blacklozenge (B \setminus K)$. Let $(u \blacklozenge v)w = u \blacklozenge (vw) = u' \blacklozenge z$ where $u' \in A$ and

$z \in (B \setminus K)$. By Lemma 3.1, we have at least one of the following :

$$(i)\ \ u \leq u', \quad (ii)\ \ u' \leq u, \quad (iii)\ \ vw \leq z, \quad (iv)\ \ z \leq vw.$$

The case (i) or (ii) implies that $u = u'$. In this case, by Lemma 3.2, $vw = z$. This contradicts the fact that $vX^* \cap (B \setminus K) = \emptyset$. Consider the case (iii). Obviously, we have $z \in vX^*$, a contradiction. Now consider the case (iv). In this case, $|u| \leq |u'|$. If $u \leq u'$, then $u = u'$ and hence $vw = z$, a contradiction. Therefore, u is not a left factor of u'. Then, by Lemma 3.5, $|z| < |u|$. This contradicts the fact that $z \in (B \setminus K)$. Consequently, $B \setminus K$ is right dense and thus B is right dense.

($\Leftarrow$) Let $w \in X^*$. We prove that $wX^* \cap (A \blacklozenge B) \neq \emptyset$. We can assume that $|w| > 0$ and $|w|$ is even without loss of generality. Let $w = a_1b_1a_2b_2 \cdots a_rb_r$ where $a_i, b_j \in X$ $(i, j = 1, 2, \ldots, r)$. Since A is a maximal prefix code, we have the following two cases :

(1) $\exists \alpha \in X^+, a_1a_2 \cdots a_r\alpha \in A$, (2) $\exists t\ (1 \leq t \leq r),\ a_1a_2 \cdots a_t \in A$.

Case 1. Since B is right dense, there exists $\beta \in X^*$ such that $b_1b_2 \cdots b_r\beta \in B$. Therefore, $(a_1a_2 \cdots a_r\alpha) \blacklozenge (b_1b_2 \cdots b_r\beta) = a_1b_1a_2b_2 \cdots a_rb_r(\alpha \blacklozenge \beta) \in wX^* \cap (A \blacklozenge B)$. Hence $wX^* \cap (A \blacklozenge B) \neq \emptyset$.

Case 2. Since B is right dense, there exists $\beta \in X^*$ such that $b_1b_2 \cdots b_ta_{t+1}b_{t+1} \cdots a_rb_r\beta \in B$. Consider $(a_1a_2 \cdots a_t) \blacklozenge (b_1b_2 \cdots b_ta_{t+1}b_{t+1} \cdots a_rb_r\beta) \in A \blacklozenge B$. Obviously, $(a_1a_2 \cdots a_t) \blacklozenge (b_1b_2 \cdots b_ta_{t+1}b_{t+1} \cdots a_rb_r\beta) = a_1b_1a_2b_2 \cdots a_rb_r\beta \in wX^*$. Therefore, $wX^* \cap (A \blacklozenge B) \neq \emptyset$.

In any case, we have $wX^* \cap (A \blacklozenge B) \neq \emptyset$, i.e. A is right dense. Q.E.D.

Remark 3.1. The maximality of A is necessary as a condition in Proposition 3.3. For instance, let $X = \{a, b\}$, let $A = \{a\}$ and let $B = X^+$. Then $A \blacklozenge B = aX^+$ is not right dense though A is a prefix code and B is right dense.

Finally, we deal with left dense languages.

Proposition 3.4. *Let* $A, B \subseteq X^*$ *be nonempty languages. If one of* A

and B is left dense, then $A \blacklozenge B$ is left dense.

Proof. We consider only the case where A is left dense. Let $u \in X^*$. We show that $X^*u \cap (A \blacklozenge B) \neq \emptyset$. Let $v \in B$. Since A is left dense, there exists $w \in X^*$ such that $wu \in A$. We can assume that $|w| > |v|$ without loss of generality. Consider $wu \blacklozenge v \in A \blacklozenge B$. Then $wu \blacklozenge v = (w \blacklozenge v)u \in X^*u$. Therefore, $X^*u \cap (A \blacklozenge B) \neq \emptyset$. Q.E.D.

The converse of the above proposition does not hold.

Example 3.4. Let $X = \{a, b\}$, let $A = X^*a$ and let $B = X^*b$. Then neither A nor B is left dense. However, $A \blacklozenge B$ is left dense. The reason is the following :

Let $u \in X^*$. We prove that $X^*u \cap (A \blacklozenge B) \neq \emptyset$. We can assume that $|u| > 0$ without loss of generality. If $u \in X^*a$, then $abu = au \blacklozenge b \in A \blacklozenge B$. If $u \in X^*b$, then $au = a \blacklozenge u \in A \blacklozenge B$. In any case, $X^*u \cap (A \blacklozenge B) \neq \emptyset$.

Unlike the case of right dense languages, the statement, *$A \blacklozenge B$ is left dense $\Leftrightarrow$ B is left dense for any maximal prefix code $A \subseteq X^+$*, is not true though the direction $\Leftarrow$ is true

Example 3.5. Let $X = \{a, b\}$ and let $A = \bigcup_{i=0}^{\infty} a^i b X^{i+1}$. Obviously, A is a maximal prefix code which is left dense. Therefore, $A \blacklozenge B$ is left dense even for a language B which is not left dense.

4. Principal Congruences on X^* Determined by Initial Literal Shuffles.

Principal congruences play an important role to combine the combinatorics theory and the algebraic theory of languages. Let $A \subseteq X^*$. Then the *principal congruence* P_A on X^* determined by A is defined as follows :

$$u \equiv v\ (P_A) \Leftrightarrow (\ xuy \in A \Leftrightarrow xvy \in A\ ) \text{ for any } x,y \in X^*.$$

For example, let $A \subseteq X^*$. Then A is regular if and only if P_A is of finite index, i.e. the number of congruence classes of P_A is finite. By $|P_A|$ we denote the index of P_A. The fact that the family of regular languages is closed under initial literal shuffle operation can be restated as follows :

$$\textit{If } |P_A|,\ |P_B| < +\infty\ ,\ \textit{then } |P_{A \,\blacklozenge\, B}| < +\infty\ .$$

There are languages, called disjunctive, which are located on the opposite side of regular languages (see [5]). A language $A \subseteq X^*$ is called *disjunctive* if P_A is the identity, i.e. every congruence class of P_A is a singleton set. An example of a disjunctive language is Q, i.e. the set of all primitive words over X. One might expect that, like the case of regular languages, the initial literal shuffle of two disjunctive languages is disjunctive. However, this is not true. For example, $Q \blacklozenge Q$ is regular though Q is disjunctive (see Section 5). Let $A \subseteq X^*$ be a language over X. Then P_A is called *left cancellative* if $xu \equiv xv\ (P_A)$ implies $u \equiv v\ (P_A)$ for any $u,v,x \in X^*$. A language $A \subseteq X^*$ is called *left cancellative* if P_A is left cancellative. An example of left cancellative language is a disjunctive language. In this section, we deal with relationships between initial literal shuffles and left cancellative languages.

A language $A \subseteq X^+$ is called *left singular* if there exists $u \in A$ such that $\{u, v\}$ is a prefix code for any $v \in A$. Moreover, u is called a *left singular word* of A. Note that any prefix code is a left singular language. Let $u \in A$ be a left singular word of A and let $u = au'$ where $a \in X$ and $u' \in X^*$. If $aX^+ \cap A$ is thin, then u is called a *thin left singular word* of A.

Proposition 4.1. *Let $A \subseteq X^+$ be a left singular language and let $B \subseteq X^*$ be a left cancellative language. If A has a thin left singular word,* *then* $P_{A \blacklozenge B} \leq P_B$, *i.e.* $x \equiv y\ (P_{A \blacklozenge B})$ *implies* $x \equiv y\ (P_B)$ *for any* $x,y \in X^*$.

Proof. Let $u \in A$ be a thin left singular word and let $u = au'$ where $a \in X$ and $u' \in X^*$. Since $aX^+ \cap A$ is thin, there exists $z \in X^+$ such that $(X^*zX^*) \cap (aX^+ \cap A) = \emptyset$. We can assume that $|z| > |u|$ without loss of generality. Let $x \equiv y\ (P_{A \blacklozenge B})$. We prove that $x \equiv y\ (P_B)$. Let $\alpha z(z \blacklozenge z)zx\beta \in B$ where $\alpha,\beta \in X^*$. Consider $u \blacklozenge [\alpha z(z \blacklozenge z)zx\beta] \in A \blacklozenge B$. Note that $u \blacklozenge [\alpha z(z \blacklozenge z)zx\beta] = (u \blacklozenge \alpha z)(z \blacklozenge z)zx\beta \in A \blacklozenge B$. Since $x \equiv y\ (P_{A \blacklozenge B})$, $u \blacklozenge [\alpha z(z \blacklozenge z)zy\beta] = (u \blacklozenge \alpha z)(z \blacklozenge z)zy\beta \in A \blacklozenge B$. Let $u \blacklozenge [\alpha z(z \blacklozenge z)zy\beta] = v \blacklozenge w$ where $v \in A$ and $w \in B$. Suppose $|w| \leq |v|$. Then it is easy to see that $v \in X^*zX^*$. On the other hand, $v \in aX^+$. Therefore, $(X^*zX^*) \cap (aX^+ \cap A) \neq \emptyset$, a contradiction. Hence $|v| < |w|$. By the proof of Lemma 3.1, $u \leq v$ or $v \leq u$. Thus $u = v$. Moreover, by Lemma 3.2, $w = \alpha z(z \blacklozenge z)zy\beta \in B$. This means that $\alpha z(z \blacklozenge z)zx\beta \in B$ implies $\alpha z(z \blacklozenge z)zy\beta \in B$. By the same reason, $\alpha z(z \blacklozenge z)zy\beta \in B$ implies $\alpha z(z \blacklozenge z)zx\beta \in B$. Therefore, we have $z(z \blacklozenge z)zx \equiv z(z \blacklozenge z)zy\ (P_B)$. Since P_B is left cancellative, $x \equiv y\ (P_B)$. This completes the proof of the proposition. Q.E.D.

Corollary 4.1. *Let* $A \subseteq X^+$ *be a left singular language and let* $B \subseteq X^*$ *be a disjunctive language. If* A *has a thin left singular word, then* $A \blacklozenge B$ *is a disjunctive language.*

Corollary 4.2. *Let* $A \subseteq X^+$ *be a thin prefix code and let* $B \subseteq X^*$ *be a disjunctive language. Then* $A \blacklozenge B$ *is a disjunctive language.*

There is a case where $P_{A \blacklozenge B} \leq P_B$ even though A is a left singular language which does not contain any thin left singular word. Let $A \subseteq X^*$. By $\#A$, we denote the value $min\{|u| \mid u \in A\}$.

Proposition 4.2. *Let* $A \subseteq X^+$ *be a left singular language and let* $B \subseteq X^*$ *be a left cancellative language. If* $|u| \leq \#B$ *for some left singular word* $u \in A$, *then* $P_{A \blacklozenge B} \leq P_B$.

Proof. Let $u \in A$ be a left singular word such that $|u| \leq \#B$. In the proof of Proposition 4.1, we replace $z(z \blacklozenge z)z$ by z' where $z' \in X^+$ and $|z'| > |u|$. Then we can show that $z'x \equiv z'y\ (P_B)$ and thus $x \equiv y\ (P_B)$ if $x \equiv y\ (P_{A \blacklozenge B})$. Q.E.D.

Let $X = \{a, b\}$ and let $A = (\bigcup_{i=1}^{\infty} a^i bX^i) \cup (\bigcup_{j=1}^{\infty} b^j aX^j)$. Moreover, let $B \subseteq X^*$ be a left cancellative language over X. Then A is a left singular language which does not have any thin left singular word. However, we have the following result.

Proposition 4.3. *Let A and B be the above mentioned languages. Then* $P_{A \blacklozenge B} \leq P_B$.

Proof. Let $x \equiv y\ (P_{A \blacklozenge B})$ and $z \in X^+$ with $|z| > 3$. Moreover, let $\alpha zx\beta \in B$. Consider $aba \blacklozenge \alpha zx\beta = (aba \blacklozenge \alpha z)x\beta \in A \blacklozenge B$. Since $x \equiv y\ (P_{A \blacklozenge B})$, $aba \blacklozenge \alpha zy\beta = (aba \blacklozenge \alpha z)y\beta \in A \blacklozenge B$. Let $(aba \blacklozenge \alpha z)y\beta = u \blacklozenge v$ where $u \in A$ and $v \in B$. If $aba \leq u$, then $u = aba$. If aba is not a left factor of u, then $(aba \blacklozenge \alpha z)y\beta = (a^{|w|}bw) \blacklozenge v$ for some $w \in X^+$. Note that $|w| \geq 2$. Let $\alpha z \in cX^*$ and $v \in dX^*$ where $c,d \in X$. Then we have $acb \cdots = ada \cdots$, a contradiction. Therefore, $u = aba$. By Lemma 3.2, $v = \alpha zy\beta \in B$. That is, $\alpha zx\beta \in B$ implies $\alpha zy\beta \in B$. By the same way, we see that $\alpha zy\beta \in B$ implies $\alpha zx\beta \in B$. This show that $zx \equiv zy\ (P_B)$. Since B is cancellative, $x \equiv y\ (P_B)$. Hence $P_{A \blacklozenge B} \leq P_B$. Q.E.D.

Conjecture 4.1. *Let $A \subseteq X^+$ be a left singular language and let $B \subseteq X^*$ be a left cancellative language. Then $P_{A \blacklozenge B} \leq P_B$.*

Finally, we consider the case where $P_B \leq P_{A \blacklozenge B}$ holds. Let $A \subseteq X^*$. By $\mathbf{I}_\alpha(A)$ we denote the set $\{a \in X \mid aX^* \cap A \neq \emptyset\}$.

Proposition 4.4. *Let $A \subseteq X^*$ be a language satisfying the following condition :*

$$aX^+ \cap A \text{ is thin for any } a \in \mathbf{I}_\alpha(A).$$

Then $P_B \le P_{A \diamond B}$ *if* $A \diamond B$ *is left cancellative.*

Proof. Let $\mathbf{I}_\alpha(A) = \{a_1, a_2, \cdots, a_r\}$. By definition, there exists $z_i \in X^+$ such that $(X^* z_i X^*) \cap (a_i X^+ \cap A) = \varnothing$ for any i $(i = 1, 2, \cdots, r)$. Let $z = z_1 z_2 \cdots z_r$. Assume that $x \equiv y$ (P_B). Let $\alpha a(z \diamond z)zx\beta \in A \diamond B$ where $a \in X$ and $\alpha, \beta \in X^*$. Then $\alpha a(z \diamond z)zx\beta = u \diamond v$ for some $u \in A$ and $v \in B$. By the definition of $\mathbf{I}_\alpha(A)$, $|u| < |\alpha a(z \diamond z)|/2$ and $u \diamond v = (u \diamond v')v''x\beta$ where $|v'| = |u|$ and $v'v''x\beta = v$. Hence $v'v''y\beta \in B$ and $u \diamond (v'v''y\beta) = (u \diamond v')\, v''y\beta = \alpha a(z \diamond z)zy\beta \in A \diamond B$. This means that $\alpha a(z \diamond z)zx\beta \in A \diamond B$ implies $\alpha a(z \diamond z)zy\beta \in A \diamond B$. By the same reason, $\alpha a(z \diamond z)zy\beta \in A \diamond B$ implies $\alpha a(z \diamond z)zx\beta \in A \diamond B$. Therefore, $a(z \diamond z)zx \equiv a(z \diamond z)zy$ $(P_{A \diamond B})$. Since $A \diamond B$ is left cancellative, $x \equiv y$ $(P_{A \diamond B})$. This completes the proof of the proposition. Q.E.D.

Corollary 4.3. *Let* $A \subseteq X^*$ *be a thin language and* $B \subseteq X^*$. *If* $A \diamond B$ *is left cancellative, then* $P_B \le P_{A \diamond B}$.

Corollary 4.4. *Let* $A \subseteq X^*$ *be a thin language and* $B \subseteq X^*$. *If* $A \diamond B$ *is disjunctive, then* B *is disjunctive.*

Corollary 4.5. *Let* $A \subseteq X^*$ *be a thin language and* $B \subseteq X^*$ *be a regular language. If* $A \diamond B$ *is left cancellative, then* $A \diamond B$ *is regular.*

5. Computation of $Q \diamond Q$.

To conclude this paper, we compute $Q \diamond Q$ where Q is the set of all primitive words over X. It can be proved that Q is disjunctive (see [5]). Let $i \ge 1$ be a positive integer. Then by $Q^{(i)}$ we denote the set $\{q^i \mid q \in Q\}$. The following lemmas are well known (see [4] or [5]).

Lemma 5.1. *Let* $u,v \in X^+$. *If* $uv \in Q^{(i)}$ *for some* $i \geq 1$, *then* $vu \in Q^{(i)}$.

Lemma 5.2. *Let* $u,v \in X^+$ *and let* $i, j \geq 1$. *If* u^i *and* v^j *have a common left factor of length* $|u| + |v|$, *then* u *and* v *are powers of a common word.*

Now we compute $Q \blacklozenge Q$.

Proposition 5.1. $Q \blacklozenge Q = X^2X^* \setminus \bigcup_{a \in X} a^2a^+$.

Proof. Let $u \in X^2X^* \setminus \bigcup_{a \in X} a^2a^+$. If $u = a^2$ for some $a \in X$, then $u = a \blacklozenge a \in Q \blacklozenge Q$. Now assume that $u \notin a^2a^+$ for any $a \in X$. Then $u = a^kbu'$ for some $a,b \in X$, $a \neq b$, $k \geq 1$ and $u' \in X^*$. First, consider the case $k \geq 2$. Note that $u = a^kbu' = a \blacklozenge (a^{k-1}bu') = (a^tb) \blacklozenge (a^tu')$ if $k = 2t$ and $u = a^kbu' = a \blacklozenge (a^{k-1}bu') = (a^tu') \blacklozenge (a^{t-1}b)$ if $k = 2t - 1$. Obviously, $t \geq k/2$. Suppose that $a^{k-1}bu' \in Q^{(i)}$ and $a^tu' \in Q^{(j)}$ for some $i, j \geq 2$. In this case, $|u'| \geq k$. By Lemma 5.1, $(u'a^t)a^{k-t-1}b \in Q^{(i)}$ and $u'a^t \in Q^{(j)}$. If $(i, j) \neq (2, 2)$, then we have

$$
\begin{aligned}
|u'| + t - (k + |u'|)/i - (|u'| + t)/j \\
&= (1 - 1/i - 1/j)|u'| + (1 - 1/j)t - k/i \\
&\geq |u'|/6 + (1 - 1/j)k/2 - k/i \\
&\geq 2k/3 - (1/2j + 1/i)k \\
&\geq 2k/3 - (1/6 + 1/2)k \\
&= 0.
\end{aligned}
$$

Hence, by Lemma 5.2, $(u'a^t)a^{k-t-1}b \in w^+$ and $u'a^t \in w^+$ for some $w \in X^+$. Thus $a^{k-t-1}b \in w^+$. This yields a contradiction, because $w \in X^*a \cap X^*b$. Therefore, $(u'a^t)a^{k-t-1}b \in Q^{(2)}$ and $u'a^t \in Q^{(2)}$. Since $|(u'a^t)a^{k-t-1}b|_b > 0$ and $|(u'a^t)a^{k-t-1}b|_b$ is even, $|u'a^t|_b > 0$ where $|v|_b$ means the number of occurrences of b in v. On the other hand, $|u'a^t|_b$ must be even. Hence, $|(u'a^t)a^{k-t-1}b|_b$ is odd, a contradiction. Consequently, $a^{k-1}bu' \in Q$ or $a^tu' \in Q$, and thus $u \in Q \blacklozenge Q$. Now consider the case $k = 1$. In this case, $u = abu'$.

Let $u = abu' = a \blacklozenge bu' = au' \blacklozenge b$. Suppose that $au' \in Q^{(i)}$ and $bu' \in Q^{(j)}$ for some $i, j \geq 2$. Then, by Lemma 5.1, $u'a \in Q^{(i)}$ and $u'b \in Q^{(j)}$. It can easily be verified that $|u'| \geq 5$ and $(i, j) \neq (2, 2)$. Therefore, we have

$$\begin{aligned} |u'| - (1 + |u'|)/i - (1 + |u'|)/j &= (1 - 1/i - 1/j)|u'| - (1/i + 1/j) \\ &\geq |u'|/6 - 5/6 \\ &\geq 0. \end{aligned}$$

By Lemma 5.2, $u'a \in w^+$ and $u'b \in w^+$ for some $w \in X^+$, a contradiction. Therefore, $au' \in Q$ or $bu' \in Q$, i.e. $u \in Q \blacklozenge Q$. Finally, we show that $a^i \notin Q \blacklozenge Q$ for any $a \in X$ and $i \geq 3$. Obviously, if $a^i = u \blacklozenge v$, then $u = a^s$ and $v = a^t$ for some $s, t \geq 1$ with $s + t = i$. Since $i \geq 3$, $a^s \notin Q$ or $a^t \notin Q$. Hence $a^i \notin Q \blacklozenge Q$. This completes the proof of the proposition. Q.E.D.

References

[1] B. Berard, Literal shuffle, *Theoret. Compt. Sci.* **51** (1987) 281-299.

[2] J. Berstel and D. Perrin, *Theory of Codes* (Academic Press, New York, 1985).

[3] G. Lallement, *Semigroups and Combinatorial Applications* (John Wiley & Sons, New York, 1979).

[4] M. Lothaire, *Combinatrics on Words* (Addison-Wesley publ. Co., Reading, Mass., 1983).

[5] H.J. Shyr, *Free Monoids and Languages* (Lect. Notes, Dep. Math., Soochow Univ., Taipei, 1979).

[6] G. Tanaka, Alternating products of prefix codes, *Proceedings of The 2nd Conference on Automata, Formal Languages and Programming Systems*, Salgotarjan, Hungary (1988), to appear.