<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>タイトル</td>
<td>初期リテラルシャフツ(代数理論のコードと関連する話題)</td>
</tr>
<tr>
<td>著者</td>
<td>伊藤 正美 田中 職次郎</td>
</tr>
<tr>
<td>雑誌名</td>
<td>数理解析研究所講究録</td>
</tr>
<tr>
<td>出版年月日</td>
<td>1989-06</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/101445">http://hdl.handle.net/2433/101445</a></td>
</tr>
<tr>
<td>タイプ</td>
<td>部門別発行集</td>
</tr>
<tr>
<td>出版者</td>
<td>京大大学出版部</td>
</tr>
</tbody>
</table>

京都大学学術情報リポジトリ
KURENAI
Kyoto University Research Information Repository
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 in-

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 $A^+ = \bigcup_{i=1}^{\infty} A^i$. 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 \( x \upharpoonright y \) of \( x \) and \( y \) is defined as follows:

1. If \( x = 1 \) or \( y = 1 \), then \( x \upharpoonright y = xy \).
2. Let \( x = a_1a_2 \ldots a_p \) and let \( y = b_1b_2 \ldots b_q \)
   where \( a_i,b_j \in X \).
   Then \( x \upharpoonright y = a_1b_1a_2b_2 \ldots a_qb_qa_{q+1}a_{q+2} \ldots a_p \) if \( p \geq q \),
   or \( = a_1b_1a_2b_2 \ldots a_pb_pb_{p+1}b_{p+2} \ldots b_q \) if \( q > p \).

Let \( A,B \subseteq X^* \). We define now the initial literal shuffle \( A \upharpoonright B \) of \( A \) and \( B \).

Definition 2.2. The initial literal shuffle \( A \upharpoonright B \) of \( A \) and \( B \) is defined as \( A \upharpoonright B = \{x \upharpoonright y \mid x \in A, y \in B \} \).

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 \( A \upharpoonright B \) to be dense.

Proposition 3.1. Let \( A,B \subseteq X^* \) be nonempty languages. Then \( A \upharpoonright B \) 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 \( w = a_1a_2 \ldots a_r \) where \( a_i \in X \) for any \( i \) (i = 1, 2, ..., r). Then
$(w \cdot w)w = a_1^2a_2 \cdots a_r^2a_1a_2 \cdots a_r$. Since $A \cdot B$ is dense, $X^*(w \cdot w)wX^* \cap (A \cdot B) \neq \emptyset$, i.e. there exist $x,y \in X^*$ such that $x(w \cdot w)wy \in A \cdot B$. Let $x(w \cdot w)wy = \alpha \cdot \beta$ 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 $xwy \cdot u = (x \cdot u)wy \in X^*wX^*$. Therefore, $X^*wX^* \cap (A \cdot B) \neq \emptyset$. 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 $A \cdot B$ is right dense.

**Proof.** Let $w \in X^*$. We show that $wX^* \cap (A \cdot B) \neq \emptyset$. 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 $(a_1a_2 \cdots a_r\alpha) \cdot (b_1b_2 \cdots b_r\beta) = (a_1b_1a_2b_2 \cdots a_rb_r)(\alpha \cdot \beta) = w(\alpha \cdot \beta) \in A \cdot B$. This means that $wX^* \cap (A \cdot B) \neq \emptyset$. Q.E.D.

The fact that $A \cdot B$ 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, $A \cdot B$ is right dense.

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

4
Unlike the case of dense languages, the statement, $A \bowtie B$: 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 $A \bowtie B = aX^+$ and thus $A \bowtie B$ is not right dense though $B$ is right dense.

However, we can set up some relationship between $A \bowtie B$ and $B$ when $A$ is a prefix code. A nonempty language $A \subseteq X^+$ is called a code over $X$ if for $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m \in A$ the equality $x_1x_2 \cdots x_n = y_1y_2 \cdots y_m$ implies that $n = m$ and $x_i = y_i$ for $i (i = 1, 2, \ldots, n)$ (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 $AX^+ \cap A = \emptyset$. 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 $u \bowtie v = u' \bowtie v'$, 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 $u \bowtie v = a_{1}b_{1}a_{2}b_{2} \cdots a_{p}b_{p}b_{p+1} \cdots b_{q} = u' \bowtie v' = a_{1}'b_{1}'a_{2}'b_{2}' \cdots a_{p}'b_{p}'[(a_{p+1}'a_{p+2}' \cdots a_{r}') \bowtie (b_{p+1}'b_{p+2}' \cdots b_{r}')]$. Therefore, we have $a_{i} = a_{i}'$ for $i (i = 1, 2, \ldots, p)$. 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 $u \bowtie v = a_{1}b_{1}a_{2}b_{2} \cdots a_{p}b_{q}a_{q+1} \cdots a_{p} = u' \bowtie v' = a_{1}'b_{1}'a_{2}'b_{2}' \cdots a_{q}'b_{q}'[(a_{q+1}'a_{q+2}' \cdots a_{r}') \bowtie (b_{q+1}'b_{q+2}' \cdots b_{s}')]$. This implies that $v \leq v'$.

Case 3. $\|u'\| = \min\{\|u\|, \|v\|, \|u'\|, \|v'\|\}$. In parallel to Case 1, we have $u'$.
\textbf{Case 4.} \( |v'| = \min \{ |u|, |vl|, |lu'|, |lv'| \}. \) By the same reason as above, we have \( v' \leq v. \) Q.E.D.

\textbf{Lemma 3.2.} \( \text{Let } u, u', v, v' \in X^+ \text{ and let } u \circ v = u' \circ v'. \) If \( |lu| = |lu'|, \) then \( u = u' \) and \( v = v'. \)

\textbf{Proof.} \textbf{Case 1.} \( |lu| \leq |vl|. \) Note that \( |lu \circ vl| = |lu'| \circ v'| = |lu| + |vl| = |lu'| + |lv'|. \) Hence \( |lu| = |lu'| \leq |vl| = |lv'|. \) Let \( u = a_1 a_2 \ldots a_r, u' = a_1' a_2' \ldots a_r', v = b_1 b_2 \ldots b_s \) and let \( v' = b_1' b_2' \ldots b_s' \) where \( a_i, a_j', a_k, b_t \in X \) and \( s \geq r. \) Therefore, \( a_1 b_1 a_2 b_2 \ldots a_r b_r b_{r+1} \ldots b_s = a_1' b_1' a_2' b_2' \ldots a_r' b_r' b_{r+1}' \ldots b_s'. \) Obviously, \( a_i = a_i' \) for \( i \) (\( i = 1, 2, \ldots, r \)) and \( b_j = b_j' \) for \( j \) (\( j = 1, 2, \ldots, s \)). Thus \( u = u' \) and \( v = v'. \) Q.E.D.

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

\textbf{Lemma 3.3.} \( \text{Let } u, u', v \in X^+. \) If \( u \circ v \leq u' \circ v \) and \( |lu|, |lu'| \geq |vl|, \) then \( u \leq u'. \)

\textbf{Proof.} \text{Note that } |lu| \leq |lu'|. \text{ Let } (u \circ v) \alpha = u' \circ v \text{ where } \alpha \in X^*. \text{ Since } |lu| \geq |vl|, (u \circ v) \alpha = u \alpha \circ v. \text{ Therefore, } u \alpha \circ v = u' \circ v. \text{ By Lemma 3.2, } u \alpha = u', \text{ i.e. } u \leq u'. \text{ Q.E.D.}

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

\textbf{Proof.} \(( \Leftarrow ) \) \text{Obvious.} \(( \Rightarrow ) \) \text{To prove this part, it is enough to show that } A \circ (B \setminus u) \text{ is right dense for any } u \in X^*. \text{ Suppose that } A \circ (B \setminus u) \text{ is not right dense for some } u \in X^*. \text{ Then there exists } v \in X^+ \text{ such that } vX^*
\( \cap [A \bullet (B \setminus u)] = \emptyset \). We can assume that \(|v| > 2|u|\) without loss of generality. Since \( A \bullet B \) is right dense, there exists \( \alpha_1 \in X^+ \) such that \( v\alpha_1 \in A \bullet B \). Therefore, \( v\alpha_1 = \alpha \bullet \beta \) for some \( \alpha \in A \) and \( \beta \in B \). From the fact that \( v\alpha_1 \in A \bullet (B \setminus u) \), we have \( v\alpha_1 = \alpha \bullet u \). By the same reason, there exists \( \alpha_2 \in X^+ \) such that \( v\alpha_1\alpha_2 = \alpha' \bullet u \) where \( \alpha' \in A \). Consequently, \( \alpha \bullet u \leq \alpha' \bullet u \).

Note that \( |\alpha| |\alpha'| \geq 1_{\mathcal{U}} \). By Lemma 3.3, \( \alpha \leq \alpha' \). Since \( A \) is a prefix code, \( \alpha = \alpha' \) and \( \alpha_2 = 1 \), a contradiction. Therefore, \( A \bullet (B \setminus K) \) must be right dense. Q.E.D.

Lemma 3.5. Let \( u, u', v, v' \in X^+ \) and let \( u \bullet v = u' \bullet v' \). 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 \( u = a_1a_2 \cdots a_r, v = b_1b_2 \cdots b_r\alpha, \ u' = a_1'a_2' \cdots a_r\beta \) 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 \( u \bullet v = u' \bullet v' \), we have \( a_1b_1a_2b_2 \cdots a_r b_r\alpha = a_1'b_1'a_2'b_2' \cdots a_r b_r'(\beta \bullet \gamma) \). Therefore, \( a_i = a_i' \) for any \( i (i = 1, 2, \ldots, r) \). 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 \( uX^* \cap AX^* \neq \emptyset \) 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 \( A \bullet B \) 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, \( A \bullet (B \setminus K) \) is right dense. We show that \( B \setminus K \) is right dense. Suppose that \( B \setminus K \) is not right dense. Then there exists \( v \in X^* \) such that \( vX^* \cap (B \setminus K) = \emptyset \). We can assume that \(|v| > |u|\) without loss of generality. Since \( A \bullet (B \setminus K) \) is right dense, there exists \( w \in X^* \) such that \((u \bullet v)w \in A \bullet (B \setminus K) \). Let \((u \bullet v)w = u'z\) where \( u' \in A \) and
$z \in (B \setminus K)$. By Lemma 3.1, we have at least one of the following:

(i) $u \leq u'$, (ii) $u' \leq u$, (iii) $vw \leq z$, (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 $wX^* \cap (A \setminus B) \neq \emptyset$. We can assume that $|w| > 0$ and $|w|$ is even without loss of generality. Let $w = a_1b_1a_2b_2 \ldots a_rb_r$ 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) $\exists \alpha \in X^*, a_1a_2 \ldots a_r\alpha \in A$, (2) $\exists t (1 \leq t \leq r), a_1a_2 \ldots a_t \in A$.

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

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

In any case, we have $wX^* \cap (A \setminus B) \neq \emptyset$, 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 $A \setminus B = aX^+$ 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 \(A \bullet B\) is left dense.

Proof. We consider only the case where \(A\) is left dense. Let \(u \in X^*\). We show that \(X^*u \cap (A \bullet B) \neq \emptyset\). 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 \(wu \bullet v \in A \bullet B\). Then \(wu \bullet v = (w \bullet v)u \in X^*u\). Therefore, \(X^*u \cap (A \bullet B) \neq \emptyset\). 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, \(A \bullet B\) is left dense. The reason is the following:

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

Unlike the case of right dense languages, the statement, \(A \bullet B\) is left dense \(\iff\) \(B\) 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 \(A = \bigcup_{i=0}^{\infty}a^ibX^{i+1}\). Obviously, \(A\) is a maximal prefix code which is left dense. Therefore, \(A \bullet B\) 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:

\[ u \equiv v \ (P_A) \iff (xuy \in A \iff xvy \in A) \] 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:

If \( |P_A|, |P_B| < +\infty \), then \( |P_{A \cdot B}| < +\infty \).

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, \( Q \cdot Q \) 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 $P_{A \cdot B} \leq P_B$, i.e. $x \equiv y (P_{A \cdot B})$ 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 $x \equiv y (P_{A \cdot B})$. We prove that $x \equiv y (P_B)$. Let $az(z \cdot z)zx\beta \in B$ where $\alpha, \beta \in X^*$. Consider $u \cdot [az(z \cdot z)zx\beta] \in A \cdot B$. Note that $u \cdot [az(z \cdot z)zx\beta] = (u \cdot az)(z \cdot z)zx\beta \in A \cdot B$. Since $x \equiv y (P_{A \cdot B})$, $u \cdot [az(z \cdot z)zy\beta] = (u \cdot az)(z \cdot z)zy\beta \in A \cdot B$. Let $u \cdot [az(z \cdot z)zy\beta] = v \cdot w$ where $v \in A$ and $w \in B$. Suppose $|w| \leq |v|$. Then it is easy to see that $v \in X^+zxX^*$. 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, $w = az(z \cdot z)zy\beta \in B$. This means that $az(z \cdot z)zx\beta \in B$ implies $az(z \cdot z)zy\beta \in B$. By the same reason, $az(z \cdot z)zy\beta \in B$ implies $az(z \cdot z)zx\beta \in B$. Therefore, we have $z(z \cdot z)zx \equiv z(z \cdot z)zy (P_B)$. 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 $A \cdot B$ 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 $A \cdot B$ is a disjunctive language.

There is a case where $P_{A \cdot B} \leq P_B$ 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 $P_{A \cdot B} \leq P_B$. 

11
Proof. Let $u \in A$ be a left singular word such that $|u| \leq \#B$. In the proof of Proposition 4.1, we replace $z(z \star z)$ 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 $x \equiv y (P_{A \star B})$. Q.E.D.

Let $X = \{a, b\}$ and let $A = (\bigcup_{i=1}^{\infty} a^i b X^i) \cup (\bigcup_{j=1}^{\infty} \overline{a}^j a X^j)$. 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 $P_{A \star B} \leq P_B$.

Proof. Let $x \equiv y (P_{A \star B})$ and $z \in X^+$ with $|z| > 3$. Moreover, let $\alpha z x \beta \in B$. Consider $aba \star \alpha z x \beta = (aba \star \alpha z) x \beta \in A \star B$. Since $x \equiv y (P_{A \star B})$, $aba \star \alpha z y \beta = (aba \star \alpha z) y \beta \in A \star B$. Let $(aba \star \alpha z) y \beta = u \star v$ 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 $(aba \star \alpha z) y \beta = (a^{l|w|} b w) \star v$ for some $w \in X^+$. Note that $|w| \geq 2$. Let $\alpha z \in c X^*$ and $v \in d X^*$ where $c, d \in X$. Then we have $a c b \ldots = a d a \ldots$, a contradiction. Therefore, $u = aba$. By Lemma 3.2, $v = \alpha z y \beta \in B$. That is, $\alpha z x \beta \in B$ implies $\alpha z y \beta \in B$. By the same way, we see that $\alpha z y \beta \in B$ implies $\alpha z x \beta \in B$. This show that $z x \equiv z y (P_B)$. Since $B$ is cancellative, $x \equiv y (P_B)$. Hence $P_{A \star B} \leq P_B$. 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 $P_{A \star B} \leq P_B$.

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

Proposition 4.4. Let $A \subseteq X^*$ be a language satisfying the following condition:
$aX^+ \cap A$ is thin for any $a \in I_\alpha(A)$.

Then $P_B \leq P_{A\vdash B}$ if $A \vdash B$ is left cancellative.

Proof. Let $I_\alpha(A) = \{a_1, a_2, \ldots, a_r\}$. By definition, there exists $z_i \in X^+$ such that $(X^*z_iX^+) \cap (a_iX^+ \cap A) = \emptyset$ for any $i (i = 1, 2, \ldots, r)$. Let $z = z_1z_2 \cdots z_r$. Assume that $x \equiv y (P_B)$. Let $\alpha a(z \vdash z)zx\beta \in A \vdash B$ where $a \in X$ and $\alpha, \beta \in X^*$. Then $\alpha a(z \vdash z)zx\beta = u \vdash v$ for some $u \in A$ and $v \in B$. By the definition of $I_\alpha(A)$, $|u| < |\alpha a(z \vdash z)|/2$ and $u \vdash v = (u \vdash v')v''x\beta$ where $|v'| = |u|$ and $v''x\beta = v$. Hence $v''y\beta \in B$ and $u \vdash (v''y\beta) = (u \vdash v')v''y\beta = \alpha a(z \vdash z)zy\beta \in A \vdash B$. This means that $\alpha a(z \vdash z)zx\beta \in A \vdash B$ implies $\alpha a(z \vdash z)zy\beta \in A \vdash B$. By the same reason, $\alpha a(z \vdash z)zy\beta \in A \vdash B$ implies $\alpha a(z \vdash z)zx\beta \in A \vdash B$. Therefore, $a(z \vdash z)zx \equiv a(z \vdash z)zy (P_{A \vdash B})$. Since $A \vdash B$ is left cancellative, $x \equiv y (P_{A \vdash B})$. 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 $A \vdash B$ is left cancellative, then $P_B \leq P_{A \vdash B}$.

Corollary 4.4. Let $A \subseteq X^*$ be a thin language and $B \subseteq X^*$. If $A \vdash B$ 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 $A \vdash B$ is left cancellative, then $A \vdash B$ is regular.

5. Computation of $Q \vdash Q$.

To conclude this paper, we compute $Q \vdash Q$ where $Q$ is the set of all primitive words over $X$. It can be proved that $Q$ is disjunctive (see [5]). Let $i \geq 1$ 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 \( Q \cdot Q \).

Proposition 5.1. \( Q \cdot Q = X^2 X^* \setminus \bigcup_{a \in X} a^2 a^+ \).

Proof. Let \( u \in X^2 X^* \setminus \bigcup_{a \in X} a^2 a^+ \). If \( u = a^2 \) for some \( a \in X \), then \( u = a \cdot a \in Q \cdot Q \). Now assume that \( u \notin a^2 a^+ \) for any \( a \in X \). Then \( u = a^k bu' \) 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 \( u = a^k bu' = a \cdot (a^{k-1}bu') = (a'b) \cdot (a'bu') \) if \( k = 2t \) and \( u = a^k bu' = a \cdot (a^{k-1}bu') = (a'u') \cdot (a'^{t-1}b) \) 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, \( (u'a^t)a^{k-1}b \in Q^{(i)} \) and \( u'a^t \in Q^{(j)} \). If \( (i, j) \neq (2, 2) \), then we have
\[
|u'| + t - (k + |u'|)/i - (|u'| + t)/j
= (1 - 1/i - 1/j)|u'| + (1 - 1/j)t - k/i
\geq |u'|/6 + (1 - 1/j)k/2 - k/i
\geq 2k/3 - (1/2j + 1/i)k
\geq 2k/3 - (1/6 + 1/2)k
= 0.
\]

Hence, by Lemma 5.2, \( (u'a^t)a^{k-1}b \in w^+ \) and \( u'a^t \in w^+ \) for some \( w \in X^+ \). Thus \( a^{k-1}b \in w^+ \). This yields a contradiction, because \( w \in X^*a \cap X^*b \).

Therefore, \( (u'a^t)a^{k-1}b \in Q^{(2)} \) and \( u'a^t \in Q^{(2)} \). Since \( |(u'a^t)a^{k-1}b|_b > 0 \) and \( |(u'a^t)a^{k-1}b|_b \) is even, \( |u'a|_b > 0 \) where \( |v|_b \) means the number of occurrences of \( b \) in \( v \). On the other hand, \( |u'a|_b \) must be even. Hence, \( |(u'a^t)a^{k-1}b|_b \) is odd, a contradiction. Consequently, \( a^{k-1}bu' \in Q \) or \( a'u' \in Q \), and thus \( u \in Q \cdot Q \). Now consider the case \( k = 1 \). In this case, \( u = abu' \).
Let \( u = abu' = a \bullet bu' = au' \ast b \). 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

\[
|u'| - (1 + |u'|)/i - (1 + |u'|)/j = (1 - 1/i - 1/j)|u'| - (1/i + 1/j) \\
\geq |u'|/6 - 5/6 \\
\geq 0.
\]

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. \( u \in Q \ast Q \). Finally, we show that \( a^i \notin Q \ast Q \) for any \( a \in X \) and \( i \geq 3 \). Obviously, if \( a^i = u \ast v \), 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 \( a^i \notin Q \ast Q \). This completes the proof of the proposition. Q.E.D.

References


