กลุ่มย่อยของโมนอยด์วากยสัมพันธ์ของรหัสไบพรีฟิกผกผันจำกัด

นางสาวขจี จันทรขจร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2543

ISBN 974-13-0924-4

SUBGROUPS OF SYNTACTIC MONOIDS

OF FINITE INVERSE BIPREFIX CODES

Miss Khajee Jantarakhajorn

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2000

ISBN 974-13-0924-4

Thesis Title : Subgroups of syntactic monoids of finite inverse biprefix codes

By : Miss Khajee Jantarakhajorn

Field of Study : Mathematics

Thesis Advisor : Assistant Professor Patanee Udomkavanich, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

……………………………………………. Dean of Faculty of Science
(Associate Professor Wanchai Phothiphichitr, Ph.D.)

THESIS COMMITTEE

…………………………………………………Chairman
(Assistant Professor Ajchara Harnchoowong, Ph.D.)

……………………………………………..Thesis Advisor
(Assistant Professor Patanee Udomkavanich, Ph.D.)

……………………………………………..Member
(Assistant Professor Penpan Yongkhong)

ขจี จันทรขจร : กลุ่มย่อยของโมนอยด์วากยสัมพันธ์ของรหัสไบพรีฟิกผกผันจำกัด
(SUBGROUPS OF SYNTACTIC MONOIDS OF FINITE INVERSE
BIPREFIX CODES) อ.ที่ปรึกษา : ผศ.ดร. พัฒนี อุดมกะวานิช, 42 หน้า
ISBN 974-13-0924-4

ชูทเซนต์เบอร์กได้ศึกษารหัสไบพรีฟิกจำกัดซึ่งโมนอยด์วากยสัมพันธ์เป็นกลุ่ม ต่อมา พัฒนี อุดมกะวานิช ได้ให้ลักษณะเฉพาะของรหัสไบพรีฟิกผกผันจำกัด (ซึ่งเป็นรหัสที่โมนอยด์วากยสัมพันธ์เป็นกึ่งกลุ่มผกผันจำกัด) และให้ตัวอย่างของรหัสไบพรีฟิกผกผันจำกัดซึ่งโมนอยด์วากยสัมพันธ์บรรจุกลุ่มไม่สลับที่ S_3 ในงานวิจัยนี้ เราจะศึกษากลุ่มย่อยของโมนอยด์วากยสัมพันธ์ของรหัสไบพรีฟิกผกผันจำกัด

ภาควิชา **คณิตศาสตร์** ลายมือชื่อนิสิต..
สาขาวิชา **คณิตศาสตร์** ลายมือชื่ออาจารย์ที่ปรึกษา..............................
ปีการศึกษา **2543** ลายมือชื่ออาจารย์ที่ปรึกษาร่วม -

4172232323 MAJOR : MATHEMATICS
KEYWORD : INVERSE BIPREFIX CODES

KHAJEE JANTARAKHAJORN: SUBGROUPS OF SYNTACTIC MONOIDS OF FINITE INVERSE BIPREFIX CODES. THESIS ADVISOR : ASSISTANT PROFESSOR PATANEE UDOMKAVANICH, Ph.D. 42 pp. ISBN 974-13-0924-4

Finite biprefix codes whose syntactic monoids are groups were studied by M.P. Schützenberger. P. Udomkavanich gave a characterization of finite inverse biprefix codes (codes admitting finite inverse semigroups as their syntactic monoids). An example of finite inverse biprefix code whose syntactic monoid contains a nonabelian group, S_3 , was given. In this research, we will investigate subgroups of syntactic monoids of finite inverse biprefix codes.

Department **Mathematics** Student's signature……………………………..

Field of Study **Mathematics** Advisor's signature…………………………….

Academic year **2000** Co-advisor's signature -

ACKNOWLEDGEMENTS

I am greatly indebted to Assistant Professor Patanee Udomkavanich, Ph.D., my thesis advisor, for her untired offering me some thoughtful and helpful advice in preparing and writing my thesis. I would like to thank Assistant Professor Ajchara Harnchoowong, Ph.D., and Assistant Professor Penpan Yongkhong, my thesis committee, for their suggestions to make my perfect thesis.

In particular, "Khob khun" or "Thank you" is not enough to express my gratitude for my lovely friends, who supported me but I did not refer to above mentioned.

CONTENTS

Chapter I

Introduction

In case $C \subseteq A^*$ is a finite prefix code the syntactic monoid $M(C^*)$ has nontrivial subgroups. Since the minimal automaton recognizing C^* is easily obtained from C, prefix codes are the natural candidates to explore. It can be shown that every group is the syntactic monoid of C^* where C is a prefix code. It is important to point out that the finiteness of C is a key restriction. M.P. Schützenberger in [4] showed that if $C \subseteq A^*$ is a finite prefix code such that $M(C^*)$ is a group G, then G is a cyclic group of order n and $C = A^n$. A natural question arises whether any other kinds of groups can appear as subgroups of $M(C^*)$. In [5] P. Udomkavanich gave an example of a finite inverse biprefix code containing S_3 as a subgroup. The characterization of finite inverse biprefix codes was also given. The purpose of this thesis is to investigate more on subgroups of syntactic monoids of finite inverse biprefix codes.

The thesis is organized as follows:

Chapter II contains basic definitions on theorems relating to prefix codes and their syntactic monoids.

Chapter III, due to P. Udomkavanich [5], deals with a characterization of finite inverse biprefix codes. All results are given with proof. This is indeed done throughout the thesis so as to make the exposition a self-contained as possible.

In the last chapter, we show the existence of finite inverse biprefix codes whose syntactic monoids contain two of the most importance groups, namely the symmetric groups S_n and the dihedral groups D_n.

CHAPTER II

PRELIMINARIES

Let A be a nonempty set called an *alphabet*, whose elements are called *letters*. Define a *word* on A as a nonempty finite sequence $a_1a_2\ldots a_n$ of elements of A. Thus two words $a_1a_2\ldots a_m$ and $b_1b_2\ldots b_n$ are equal if and only if they coincide as sequences, that is if $m = n$ and $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. The number of occurrences of a letter $a \in A$ in a word w is denoted $d_a(w)$ and the length of $w, l(w)$ is defined by $l(w) = \Sigma_{a\in A} d_a(w)$. For each n, let A^n be the set of all words on A of length n, that is $A^n = \{a_1a_2\ldots a_n \mid a_1, a_2, \ldots, a_n \in A\}$. Denote $A^+ = \cup_{n=1}^{\infty} A^n$ and $A^* = A^+ \cup \{\epsilon\}$ when ϵ denotes the empty sequence, and define an operation (concatenation) on A^* by

$$(a_1a_2\ldots a_m)(b_1b_2\ldots b_n) = a_1a_2\ldots a_mb_1b_2\ldots b_n$$

for all $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n \in A$. Then A^* is a free monoid on the set A. A subset of A^* is called a *language*. Let $u, v \in A^+$, u is called a *left* (resp.*right*) *factor* of word w in A^+ if $w = uv$ (resp. $w = vu$).

An A^*- *automaton* $\mathfrak{A} = (S, f)$ is a set S together with a mapping $f : S \times A^* \to S$ satisfying :

(a) $f(s, \epsilon) = s$ for all $s \in S$

(b) $f[f(s, u), v] = f(s, uv)$ for all $s \in S, u, v \in A^*$.

The set S is called the set of *states* of $\mathfrak{A}$ and f is called the *transition function* of $\mathfrak{A}$. We usually denote $f(s, u)$ by su.

Let S be a semigroup. An equivalent relation ρ on S is called a *congruence* on S if for every $x, y, z \in S$, $x\rho y$ implies $zx\rho zy$ and $xz\rho yz$.

If ρ is a congruence on a semigroup S, then the set

$$S/\rho = \{x\rho \mid x \in S\}$$

with the operation defined by $(x\rho)(y\rho) = (xy)\rho$ for every $x, y \in S$ is a semigroup.

Let $\mathfrak{A} =(S, f)$ be an A^*-automaton. The mapping $\tau_{\mathfrak{A}} : A^* \rightarrow \mathcal{T}_r(S)$ from A^* into the monoid of all transformations on S, defined by $s\tau_{\mathfrak{A}}(u) = f(s, u)$ for all $s \in S, u \in A^*$ is a monoid homomorphism. We denote $\tau_{\mathfrak{A}}$ by τ when there is no chance of ambiguity. $A^*/Ker\tau$ is a monoid, called the *transition monoid* of $\mathfrak{A}$ where

$$Ker\tau = \{(x, y) \in A^* \times A^* \mid s\tau(x) = s\tau(y) \text{ for all } s \in S\}.$$

We denote $A^*/Ker\tau$ by $T(\mathfrak{A})$. Note that $T(\mathfrak{A})$ is also isomorphic to $\tau(A^*)$.

An A^*-automaton $\mathfrak{A} = (S, f)$ is called *monogenic* if there exists $s_0 \in S$ such that $f(s_0, A^*) = S$ (s_0 is called a *generator* of $\mathfrak{A}$).

Monogenic A^*-automata are directly related to right congruence on A^*. If $\mathfrak{A} = (S, f)$ is an A^*-automaton generated by $s_0 \in S$, we define $\gamma(\mathfrak{A})$ as follows :

$$\gamma(\mathfrak{A}) = \{ \ (u, v) \in A^* \times A^* \mid f(s_0, u) = f(s_0, v) \ \}.$$

It is clear that $\gamma(\mathfrak{A})$ is a right congruence on A^*. Conversely if ρ is a right congruence on A^*, denoting by $\overline{w}$ the class of w modulo ρ, we define $\alpha(\rho)$, the automaton of ρ, by :

$$\alpha(\rho) = (A^*/\rho, f) \qquad\qquad \text{with } \ f(\overline{w}, a) = \overline{wa} \ \text{ for all } \ w, a \in A^*.$$

A language $L \subseteq A^*$ is called *recognizable* if there exist an A^*-automaton $\mathfrak{A} = (S, f)$, with S finite, a state $s_0 \in S$ and a subset T of S such that

$$L = \{w \in A^* \mid f(s_0, w) \in T\}.$$

We also say that the finite A^*-automaton $\mathfrak{A}$ recognize L, or that L is recognized by $\mathfrak{A}$. We can show that L is recognizable if and only if L is a union of classes of a right congruence on A^* of finite index.

Given any subset L of A^*, there is a largest right congruence $P_L^{(r)}$ for which L is a union of classes. It is defined by

$$P_L^{(r)} = \{\ (u,v) \in A^* \times A^* \mid uw \in L \Leftrightarrow vw \in L \ \text{ for every } w \in A^*\}.$$

Thus the A^*−automaton $\alpha(P_L^{(r)}) = \mathfrak{A}(L)$ is a minimal automaton recognizing L. It is called the *minimal automaton* of L.

It can be shown that a relation on A^* defined by

$$P_L = \{\ (u,v) \in A^* \times A^* \mid xuy \in L \Leftrightarrow xvy \in L \ \text{ for every } x,y \in A^*\}$$

is a congruence on A^*. It is called the *syntactic congruence* of L. Hence the monoid A^*/P_L, denoted by $M(L)$, is called *the syntactic monoid* of L.

In addition, $M(L)$ is isomorphic to the transition monoid of the minimal automaton $\alpha(P_L^{(r)})$ of L. Thus we can consider $M(L)$ as the transition monoid of the minimal automaton of L.

Throughout this thesis, we are interested in a special type of language, a prefix code.

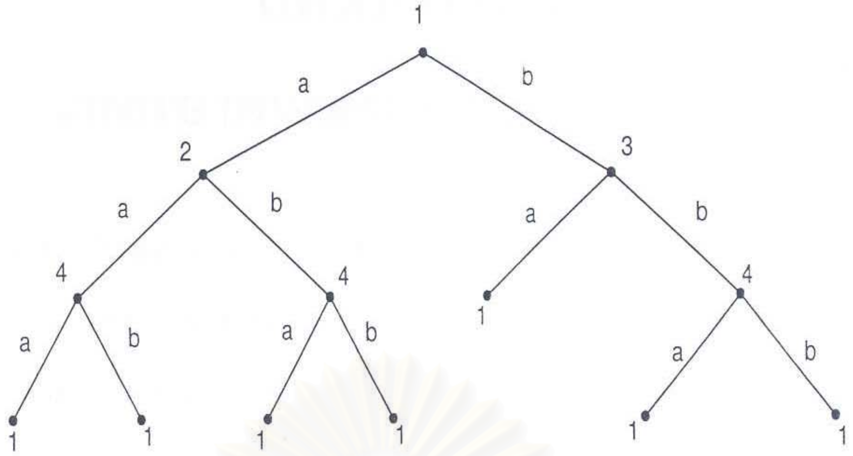
$C \subseteq A^+$ is called a *prefix code* on A if for all $u,v \in A^*, u \in C$ and $uv \in C$ implies $v = \epsilon$. A *suffix code* is defined dually. C is called a *biprefix code* if it is a prefix and a suffix code.

Defining the relation $\leq_l$ in A^* by $u \leq_l v$ if v is a left factor of u, we see that $\leq_l$ is a partial ordering of A^*. A subset C is a prefix code if and only if for every $c \in C, w \in A^*, w \leq_l c$ and $w \neq c$ implies $w \notin C$. Thus to obtain a prefix code, it suffices to select a subset C of A^* that will be end points for $\leq_l$. For example the falling tree below

gives the prefix code $C = \{a^2, aba, ab^2, b\}$ over $\{a, b\}$.

Let C be a prefix code over an alphabet A. To construct $P^{(r)}_{C^*}$, we denote by s the class of $P^{(r)}_{C^*}$ consisting of all words $u \in A^*$ such that $uA^* \cap C^* = \emptyset$. If $uA^* \cap C^* \neq \emptyset$, there exists a unique $c \in C^*$ and $z \in A^*$ such that $u = cz$ and z is a proper left factor of a word in C (eventually $z = \epsilon$). The prefix property of C implies $(u, z) \in P^{(r)}_{C^*}$ and for any two proper left factors z_1, z_2 of words in C we have $(z_1, z_2) \in P^{(r)}_{C^*}$ if and only if $(z_1, z_2) \in P^{(r)}_{C}$. Finally, for every $c \in C, (c, \epsilon) \in P^{(r)}_{C^*}$. It follows that the minimal automaton of C^* is obtained by drawing the tree representing words in C. Label the top and the end points of the tree with "1", and intermediate points using the same name, if they have identical subtree.

Example 2.1. Let $A = \{a, b\}$ and $C = \{a^3, a^2b, ab^2, aba, ba, b^3, b^2a\}$ be a prefix code. The tree representing C is shown



The minimal automaton of C^* has four states, denoted by 1, 2, 3 and 4. The transition function f is defined by

$$f(1,a)=2 \quad f(1,b)=3 \quad f(2,a)=4 \quad f(2,b)=4$$

$$f(3,a)=1 \quad f(3,b)=4 \quad f(4,a)=1 \quad f(4,b)=1$$

The corresponding syntactic monoid $M(C^*)$ is generated by

$$\tau(a)=\begin{pmatrix}1&2&3&4\\2&4&1&1\end{pmatrix} \text{ and } \tau(b)=\begin{pmatrix}1&2&3&4\\3&4&4&1\end{pmatrix}$$

In the tree representation of C^*, a node labelled s is called the *node associated with* a left factor x of a word in C, if x is a path joining the top of the tree and the nodes s. Thus the nodes associated with x and x' are labelled with the same name if $x^{-1}C=(x')^{-1}C$, where $u^{-1}C=\{w\in A^* \mid uw\in C\}$.

CHAPTER III

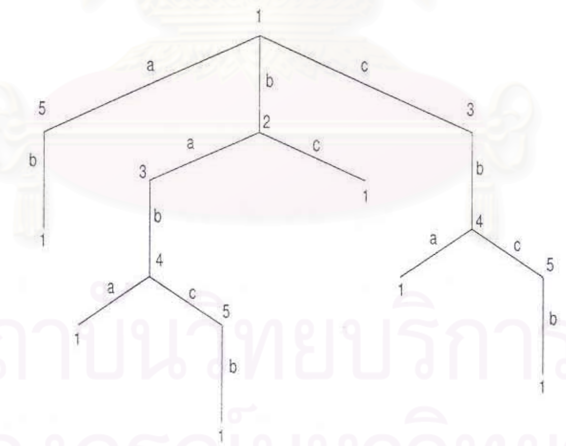
FINITE INVERSE BIPREFIX CODES

We first recall that a semigroup S is called an *inverse semigroup* if each element a of S has a unique x in S such that $axa = a$ and $xax = x$. We can see that every group is an inverse semigroup.

In 1956, M.P. Schützenberger [4] has studied a prefix code whose syntactic monoid is a group. One generalization of a group is an inverse semigroup, a prefix code whose syntactic monoid is an inverse semigroup was studied by P.Udomkavanich [5]. Such a code was proved to be biprefix, it is then called an inverse biprefix code.

Example 3.1. Let $A = \{a, b, c\}$ and $C = \{ab, baba, babcb, cba, bc, cbcb\}$.

The tree representing C is shown below



The syntactic monoid $M(C^*)$ is generated by

$$\tau(a) = \begin{pmatrix} 1 & 2 & 4 \\ 5 & 3 & 1 \end{pmatrix}, \quad \tau(b) = \begin{pmatrix} 5 & 3 & 1 \\ 1 & 4 & 2 \end{pmatrix} \quad \text{and} \quad \tau(c) = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 1 & 5 \end{pmatrix}.$$

We obtain that

$$\tau(a)\tau(bab)\tau(a) = \begin{pmatrix} 1 & 2 & 4 \\ 5 & 3 & 1 \end{pmatrix} = \tau(a) \text{ and } \tau(bab)\tau(a)\tau(bab) = \begin{pmatrix} 5 & 3 & 1 \\ 1 & 2 & 4 \end{pmatrix} = \tau(bab),$$

$$\tau(b)\tau(aba)\tau(b) = \begin{pmatrix} 5 & 3 & 1 \\ 1 & 4 & 2 \end{pmatrix} = \tau(b) \text{ and } \tau(aba)\tau(b)\tau(aba) = \begin{pmatrix} 1 & 2 & 4 \\ 5 & 1 & 3 \end{pmatrix} = \tau(aba)$$

$$\tau(c)\tau(bcb)\tau(c) = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 1 & 5 \end{pmatrix} = \tau(c) \text{ and } \tau(bcb)\tau(c)\tau(bcb) = \begin{pmatrix} 5 & 3 & 1 \\ 4 & 1 & 2 \end{pmatrix} = \tau(bcb).$$

This implies that $M(C^*)$ is an inverse semigroup.

In this chapter we give a characterization of inverse biprefix codes studied by P.Udomkavanich [5].

A few definitions are needed to characterized inverse biprefix codes.

Definition 3.2. Let $C \subseteq A^+$ be a prefix code, $a \in A$. A sequence $A_a = \{a = a_1, a_2, \ldots, a_n\}$ of letters in A satisfying :

(I.1) For every $u, v \in A^*$, $uav \in C \Rightarrow ua_1a_2 \ldots a_nav \in C^+$

is called an *inverse sequence* for a in C.

Examples 3.3. (1) Let $C = \{abab, ba, bcb, cbab, bc, cbc\}$ be a prefix code on $A = \{a, b, c\}$. An inverse sequence of a is $\{a, b, a, b\}$ but both b and c have no inverse sequences.

(2) Let $A = \{a, b, c\}$ and $C = \{ab, baba, babcb, cba, bc, cbcb\}$ be a prefix code. Inverse sequences for a, b and c are as follows:

For $a : \{a, b, a, b\}$

For $b : \{b, a, b, a\}$ and $\{b, c, b, c\}$

For $c : \{c, b, c, b\}$

In general, a prefix code on alphabet A need not have an inverse sequence for every $a \in A$ but we shall show that this is a necessary conditions for inverse biprefix codes.

A transformation α in $\mathcal{T}(S)$ has a unique inverse if α is one-to-one. Thus we may view the syntactic monoid of an inverse prefix code as a submonoid of $\mathcal{I}(S)$, the monoid of all one-to-one partial transformations on the set of states S of the minimal automaton of the code.

We first introduce a lemma which is an importance tool to obtain the characterization.

Lemma 3.4. Let $C \subseteq A^+$ be a prefix code with minimal automaton $\mathfrak{A}(C^*) = (S, f)$. Then $M(C^*)$ is a submonoid of $\mathcal{I}(S)$ if and only if C is biprefix, and C satisfies

(I.2) For $u \neq \epsilon$, $u^{-1}C \cap v^{-1}C \cap A^+ \neq \phi \Rightarrow u^{-1}C = v^{-1}C$.

Proof. Assume that $M(C^*)$ is a submonoid of $\mathcal{I}(S)$. Suppose that C is not suffix. Then there are words wx and x in C with $w \neq \epsilon$. Thus $(1\tau(w))\tau(x) = 1 = 1\tau(x)$. Since C is prefix, $w \neq \epsilon$ and $wx \in C$, it follows that $w \notin C$. Hence $1\tau(w) \neq 1$. This implies that $\tau(x)$ is not one-to-one, which contradicts the assumption. Thus C is biprefix.

Next, assume that $u \neq \epsilon, ux \in C$ and $vx \in C$ for some $x \in A^+$. Write

$$x = b_0 b_1 b_2 \dots b_n,$$

where $b_0 = \epsilon,\ b_i \in A$ for all $i = \{1, 2, \dots, n\}$. Suppose that $u^{-1}C \neq v^{-1}C$. Then there is an index $m, 1 \leq m \leq n$, such that

$$(ub_0 b_1 b_2 \dots b_{m-1})^{-1}C \neq (vb_0 b_1 b_2 \dots b_{m-1})^{-1}C$$

but

$$(ub_0b_1b_2\ldots b_m)^{-1}C = (vb_0b_1b_2\ldots b_m)^{-1}C.$$

Let s and t be the labels of the nodes associated with $ub_0b_1b_2\ldots b_{m-1}$ and $vb_0b_1b_2\ldots b_{m-1}$, respectively. Then $s \neq t$ but $s\tau(b_m) = t\tau(b_m)$. Thus $\tau(b_m)$ is not one-to-one. This again contradicts the assumption.

Conversely, assume that there is an $a \in A$ such that $\tau(a)$ is not one-to-one. Then there are s and t with $s \neq t$ and $s\tau(a) = t\tau(a)$. Let u and v be left factors of words in C associated with s and t, respectively. Then $(ua)^{-1}C = (va)^{-1}C$ and $u^{-1}C \neq v^{-1}C$. If $s = 1$ or $t = 1$, then $u = \epsilon$ or $v = \epsilon$ together with $(ua)^{-1}C = (va)^{-1}C$ we can conclude that C is not suffix. If $s \neq 1$ and $t \neq 1$, then $u \neq \epsilon$ and $(ua)^{-1}C = (va)^{-1}C$ implies $u^{-1}C \cap v^{-1}C \cap A^+ \neq \phi$. □

The next theorem will give us a characterization of inverse biprefix codes.

Theorem 3.5. Let $C \subseteq A^+$ be a biprefix code. Then $M(C^*)$ is an inverse semigroup if and only if C satisfies the following conditions:

(I.2) For $u \neq \epsilon, u^{-1}C \cap v^{-1}C \cap A^+ \neq \phi \Rightarrow u^{-1}C = v^{-1}C$.

(I.3) Every $a \in A$ has an inverse sequence in C. i.e., a sequence $A_a = \{a = a_1, a_2, \ldots, a_n\}$ satisfying:

(I.1) For every $u, v \in A^*$, $uav \in C \Rightarrow ua_1a_2\ldots a_nav \in C^+$.

Proof. Assume that $M(C^*)$ is an inverse semigroup. Then By Lemma 3.4, C satisfies (I.2). Let $a \in A$. Then there exist $a_2, \ldots, a_n \in A$ such that

$$\tau(a)\tau(a_2a_3\ldots a_n)\tau(a) = \tau(a).$$

Let $A_a = \{a = a_1, a_2, \ldots, a_n\}$. Suppose that $uav \in C$. Then $1\tau(uav) = 1$. Hence

$$\begin{aligned} 1\tau(ua_1a_2\ldots a_nav) &= 1\tau(u)\tau(a_1)\tau(a_2a_3\ldots a_n)\tau(a)\tau(v) \\ &= 1\tau(u)\tau(a)\tau(v) \\ &= 1\tau(uav) \\ &= 1. \end{aligned}$$

This shows that $ua_1a_2\ldots a_nav \in C^+$.

To prove the converse, assume that C satisfies (I.2) and (I.3). By Lemma 3.4, $M(C^*)$ is a submonoid of $\mathcal{I}(S)$, where S is the set of states in the minimal automaton$\mathfrak{A}(C^*)$. Let $a \in A$. Then there is a sequence

$$A_a = \{a = a_1, a_2, \ldots, a_n\}$$

satisfying (I.1). Since a regular subsemigroup of an inverse semigroup is an inverse semigroup, it is enough to show that $\tau(a)\tau(a_2a_3\ldots a_n)\tau(a) = \tau(a)$. Let s be in the domain of $\tau(a)$. Then there exist $u, v \in A^*$ such that $uav \in C$ and $1\tau(u) = s$. By (I.1), $ua_1a_2\ldots a_nav \in C^+$. Thus $ua_1a_2\ldots a_nav \in C$ or $a_ia_{i+1}\ldots a_nav \in C$ for some i. If $ua_1a_2\ldots a_nav \in C$, then $u, v \neq \epsilon$ (since C is biprefix, and $uav, uaa_2\ldots a_nav \in C$). Thus $\epsilon \neq av \in u^{-1}C \cap (ua_1a_2\ldots a_n)^{-1}C$. Hence, by (I.2), $u^{-1}C = (ua_1a_2\ldots a_n)^{-1}C$. Similarly, we can show that if $a_ia_{i+1}\ldots a_nav \in C$ for some i, then $u^{-1}C = (a_ia_{i+1}\ldots a_n)^{-1}C$. In any case, we obtain $1\tau(ua_1a_2\ldots a_n) = 1\tau(u) = s$. Hence

$$\begin{aligned} s\tau(a)\tau(a_2a_3\ldots a_n)\tau(a) &= s\tau(a_1a_2\ldots a_na) \\ &= 1\tau(u)\tau(a_1a_2\ldots a_na) \\ &= 1\tau(ua_1a_2\ldots a_n)\tau(a) \\ &= s\tau(a) \end{aligned}$$

Therefore $\tau(a)\tau(a_2a_3\ldots a_n)\tau(a) = \tau(a)$ as required. □

Given a finite biprefix code, we may show that each letter $a \in A$, $A_a = \{a = a_1, a_2, \ldots, a_n\}$ is an inverse sequence in C by using the next proposition.

We first give some definitions and remarks in order to help us to prove the proposition.

Definition 3.6. Let $C \subseteq A^+$ be a finite biprefix code, $a \in A$ and $A_a = \{a = a_1, a_2, \ldots, a_n\}$ be a sequence of letters in A. A word z in C is called an *associated word* of $w = xay$ in C *with respect to* A_a, if there are two indices $l, l', 1 \leq l, l' \leq n$, such that $z = a_l a_{l+1} \ldots a_n a_1 a_2 \ldots a_{l'}$ satisfying the following conditions:

(I.4) $l = 1$ if and only if $x = \epsilon$, and $l' = 1$ if and only if $y = \epsilon$.

(I.5) if x and y are not empty words, then $x^{-1}C \cup (a_l a_{l+1} \ldots a_n)^{-1}C$ is a biprefix code.

Examples 3.7. (1) Let $C = \{ab, baba, babcb, cba, bc, cbcb\}$ be a biprefix code on $A = \{a, b, c\}$. Let $A_a = \{a, b, a, b\} \equiv \{a_1, a_2, a_3, a_4\}$.

$\underline{a}b \equiv a_1 a_2$ is an associated word of $\underline{a}b$ (w.r.t A_a).

$bab\underline{a} \equiv a_2 a_3 a_4 a_1$ is an associated word of $bab\underline{a}$ (w.r.t A_a).

$bab\underline{a} \equiv a_2 a_3 a_4 a_1$ is an associated word of $cb\underline{a}$ (w.r.t A_a).

$b\underline{a}ba \equiv a_4 a_1 a_2$ is an associated word of $b\underline{a}ba$ (w.r.t A_a)

$b\underline{a}ba \equiv a_4 a_1 a_2$ is an associated word of $b\underline{a}bcb$ (w.r.t A_a) since $b^{-1}C = \{aba, abcb, c\}$ is a biprefix code.

(2) Let $C = \{abcdbc, bcd, dbca, dbcdbc, abca, bcab, cabc, cdb\}$ be a biprefix code on $A = \{a, b, c, d\}$. Let

$$A_b = \{b, c, a, b, c, a, b, c, a, b, c, a\} \equiv \{b_1, b_2, \ldots, b_{12}\}.$$

Observe that $b_1 = b_4 = b_7 = b_{10} = b$.

$\underline{b}cab \equiv b_1b_2b_3b_4$ is an associated word of $\underline{b}cd$ (w.r.t A_b).

$bca\underline{b} \equiv b_{10}b_{11}b_{12}b_1$ is an associated word of $cd\underline{b}$ (w.r.t A_b).

$ca\underline{b}c \equiv b_{11}b_{12}b_1b_2$ is an associated word of $dbcd\underline{b}c$, since $(ca)^{-1}C = \{bc\}$ $= (dbcd)^{-1}C$, but $ca\underline{b}c \equiv b_{11}b_{12}b_1b_2$ is not an associated word of $d\underline{b}ca$ since $d^{-1}C \cup (ca)^{-1}C = \{bca, bcdbc\} \cup \{bc\}$ is not a biprefix code.

$a\underline{b}ca \equiv b_{12}b_1b_2b_3$ is an associated word of $d\underline{b}ca$ since $a^{-1}C = \{bcdbc, bca\}$ $= d^{-1}C$ and $\{bcdbc, bca\}$ is a biprefix code.

$a\underline{b}ca$ is also associated word of $d\underline{b}cdbc$.

Remarks 3.8. (1) An associated word of a word xay in C with respect to $A_a = \{a = a_1, a_2 \ldots, a_n\}$ can be determined, according to the appearance of xay in the code word, as follows:

Case 1: $x = \epsilon$. Then we simply search for a word in C of the form $a_1a_2 \ldots a_{l'}$ for some $l' \geq 1$.

Case 2: $y = \epsilon$. Similar to Case1, we look for a code word of the form $a_la_{l+1} \ldots a_na_1$ for some $l > 1$.

Case 3: Both x and y are not the empty words.

All words $a_la_{l+1} \ldots a_na_1 \ldots a_{l'}$ for which $(a_la_{l+1} \ldots a_n)^{-1}C \cup x^{-1}C$ is biprefix are associated words of xay.

(2) Any code word z of the form $a_la_{l+1} \ldots a_na_1a_2 \ldots a_{l'}$ is its own and only associated word with respect to $A_a = \{a = a_1, a_2, \ldots, a_n\}$.

(3) Any word ay or xa in C has at most one associated word with respect to $A_a = \{a = a_1, a_2, \ldots, a_n\}$ since C is a biprefix code.

Definition 3.9. Let $C \subseteq A^+$ be a finite biprefix code, $xay \in (A^+aA^*) \cap C$, and $A_a = \{a = a_1, a_2, \ldots, a_n\}$ be a sequence of letters in A. A word

$a_l a_{l+1} \dots a_n a_1 a_2 \dots a_{l'}$ with $l \neq 1$ is called a *companion* of xay with respect to A_a if $x^{-1}C = (a_l a_{l+1} \dots a_n)^{-1}C$.

Example 3.10. Let $C = \{ae, bcfe, cab, dab, dec, fab, fec\}$ be a biprefix code on $A = \{a, b, c, d, e, f\}$. Let

$$A_a = \{a, b, c, e, f\} \equiv \{a_1, a_2, a_3, a_4, a_5\}.$$

Then $f\underline{a}b \equiv a_5 a_1 a_2$ is a companion of $d\underline{a}b$ (w.r.t A_a) since $f^{-1}C = \{ab, ec\}$ $= d^{-1}C$, but it is not a companion of $c\underline{a}b$ (w.r.t A_a) since $c^{-1}C = \{ab\} \neq f^{-1}C$.

The following example shows that a companion word need not be an associated word and an associated word need not be a companion word.

Example 3.11. Let $C = \{abab, baba, babca, cbab, cbc, daba, dabca\}$ be a biprefix code on $A = \{a, b, c, d\}$. Let $A_a = \{a, b, a, b\} \equiv \{a_1, a_2, a_3, a_4\}$.

$ab\underline{a}b \equiv a_3 a_4 a_1 a_2$ is an associated word of $cb\underline{a}b$ (w.r.t A_a) since $(ab)^{-1}C \cup (cb)^{-1}C = \{ab\} \cup \{ab, c\}$ is biprefix but it is not a companion of $cb\underline{a}b$ since $(ab)^{-1}C \neq (cb)^{-1}C$.

$bab\underline{a} \equiv a_2 a_3 a_4 a_1$ is a companion of $dab\underline{a}$ since $(bab)^{-1}C = \{a, ca\} = (dab)^{-1}C$. Since $\{a, ca\}$ is not suffix, it is not an associated word (w.r.t A_a) of $dab\underline{a}$.

The existence of an associated word which is also a companion word of xay in C is one of the sufficient conditions for A_a to be an inverse sequence as shown in the following proposition.

Proposition 3.12. Let $C \subseteq A^+$ be a finite biprefix code. Let $a \in A$. Assume that $A_a = \{a = a_1, a_2, \dots, a_n\}$ is a sequence of letters satisfying :

(i) If $a_1 a_2 \dots a_{j_1 - 1} \in C$, then there is a (unique) partition

$$(1\ 2\ \dots\ j_1 - 1 \mid j_1\ \ j_1 + 1\ \dots\ j_2 - 1 \mid \dots \mid j_k\ \ j_k + 1\ \dots\ n)$$

of the cyclic permutation $(1\ 2\ \dots\ n)$ on $\{1, 2, \dots, n\}$ such that C contains $\{a_1a_2 \dots a_{j_1-1}, a_{j_1}a_{j_1+1} \dots a_{j_2-1}, \dots, a_{j_k}a_{j_k+1} \dots a_n\}$.

(ii) If $a_ja_{j+1} \dots a_na_1 \dots a_{j_1-1} \in C$, then there is a (unique) partition

$$(j\ \ j+1\ \dots\ j_1-1 \mid j_1\ \ j_1+1\ \dots\ j_2-1 \mid \dots \mid j_k\ \ j_k+1\ \dots\ j-1)$$

of the cyclic permutation $(j\ \ j+1\ \dots\ n\ 1\ 2\ \dots\ j-1)$ on $\{1, 2, \dots, n\}$ such that C contains $\{a_ja_{j+1} \dots a_{j_1-1}, a_{j_1}a_{j_1+1} \dots a_{j_2-1}, \dots, a_{j_k}a_{j_k+1} \dots a_{j-1}\}$.

(iii) Every xay in C has an associated word (with respect to A_a), which is also its companion in case $x \neq \epsilon$.

Then A_a is an inverse sequence for a.

Proof. Assume that $av \in C$. By(iii), there is $l', 1 \leq l' \leq n$, such that $a_1a_2 \dots a_{l'}$ is an associated word of av. By (i), $a_1a_2 \dots a_{l'}a_{l'+1} \dots a_n \in C^+$ so $(a_1a_2 \dots a_n)av \in C^+$. Similarly, we can show that if $ua \in C$, then $ua_1a_2 \dots a_na = (ua)(a_2a_3 \dots a_{l-1})(a_la_{l+1} \dots a_na_1) \in C^+$.

Let $uav \in C$ with $u, v \neq \epsilon$. By (iii) there are $l, l', 1 < l, l' \leq n$ such that $a_la_{l+1} \dots a_na_1 \dots a_{l'}$ is a companion of uav with respect to A_a, so $u^{-1}C = (a_la_{l+1} \dots a_n)^{-1}C$. Hence $ua_1a_2 \dots a_{l'}$ and $a_la_{l+1} \dots a_nav$ are in C. Since $a_la_{l+1} \dots a_na_1a_2 \dots a_{l'} \in C$ it follows by (ii) that $a_{l'+1}a_{l'+2} \dots a_{l-1} \in C^-$. Thus $ua_1a_2 \dots a_nav = (ua_1a_2 \dots a_{l'})(a_{l'+1}a_{l'+2} \dots a_na_1a_2 \dots a_{l-1})(a_la_{l+1} \dots a_nav) \in C^+$. Therefore A_a is an inverse sequence for a. □

CHAPTER IV

SUBGROUPS OF SYNTACTIC MONOIDS OF FINITE INVERSE BIPREFIX CODES

Given any prefix code $C \subseteq A^*$, it is known that every group is the syntactic monoid of a language C^* with a prefix code C. M.P.Schützenberger has shown the followings in [4].

Proposition 4.1. Let C be a finite prefix code. The group of units of $M(C^*)$ is always a cyclic group.

Proof. Assume that the group of units U of $M(C^*)$ is nontrivial. Then there exists $a \in A$ acting as a nontrivial permutation $\tau(a)$ on the set S of states of $\mathfrak{A}(C^*)$. As a permutation on S, $\tau(a)$ is a product of disjoint cycles, say $\tau(a) = \gamma_1\gamma_2 \ldots \gamma_k$ with, for example, s_0 in the cycle γ_1. In case $\gamma_i (i \neq 1)$ is the cycle $(s_{i_1}, s_{i_2}, \ldots, s_{i_k})$ with $i_1, i_2, \ldots, i_k \neq 0$, then the tree representing C has an infinite repetition

$$\frac{a}{i_1} \cdot \frac{a}{i_2} \cdots \frac{a}{i_k} \cdot \frac{a}{i_1\ \ i_2} \cdots$$

contradicting the finiteness of C. Consequently $\tau(a) = (s_0, s_1, \ldots, s_{n-1})$, assuming that the indexation of the states has been done to fit. Let $b \in A$, also acting as a nontrivial permutation $\tau(b)$ on S. Then as above $\tau(b)$ is a cycle of length n on $s_0, s_1, \ldots, s_{n-1}$. Assume that $s_{n-1}\tau(b) = s_i$ with $i \neq 0$. Then $s_i\tau(a)^{n-i-1}\tau(b) = s_{n-1}\tau(b) = s_i$ yields an infinite repetition in the tree of C, again contradicting finiteness of C. Hence $s_{n-1}\tau(b) = s_0$. Inductively, if we suppose that $s_{n-i}\tau(b) = s_{n-i+1}$ for $i = 2, 3, \ldots, k$, we cannot have $s_{n-k-1}\tau(b) = s_i$ with $i > n-k$ or $i = 0$, since $\tau(b)$ is a permutation. We cannot have $s_{n-k-1}\tau(b) = s_i$ with $i < n-k$ either, otherwise $s_i\tau(a)^{n-k-i-1}\tau(b) = s_i$ yields an infinite repetition as above.

Thus $s_{n-k-1}\tau(b) = s_{n-k}$ for all $k, 0 < k < n$, showing $\tau(b) = (s_0, s_1, \ldots, s_{n-1})$. Since any word w acting on s as a nontrivial permutation is a product of letters a with the same property, U is the cyclic group of order n, generated by the n-cycle $(s_0, s_1, \ldots, s_{n-1})$. □

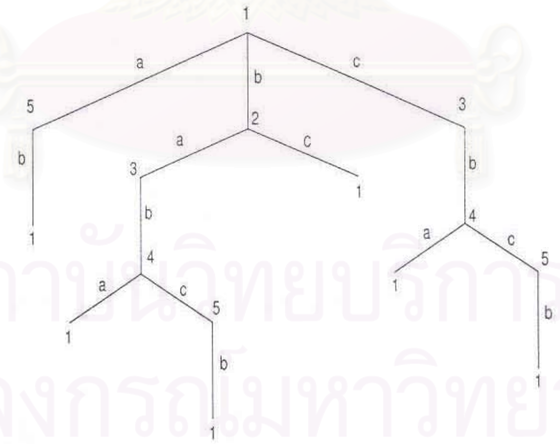
Corollary 4.2. If $C \subseteq A^*$ is a finite prefix code such that $M(C^*)$ is a group G, then G is a cyclic group of order n, and $C = A^n$ for some integer n.

Next example, given by P.Udomkavanich in [5], shows the existence of a finite inverse biprefix code whose syntactic monoid contains a nonabelian group such as S_3.

Example 4.3. Refer to the inverse biprefix code

$$C = \{ab, baba, babcb, cba, bc, cbcb\}$$

in Example 3.4. The tree representing C is shown below



The syntactic monoid $M(C^*)$ is generated by

$$\tau(a) = \begin{pmatrix} 1 & 2 & 4 \\ 5 & 3 & 1 \end{pmatrix}, \quad \tau(b) = \begin{pmatrix} 5 & 3 & 1 \\ 1 & 4 & 2 \end{pmatrix} \quad \text{and} \quad \tau(c) = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 1 & 5 \end{pmatrix}.$$

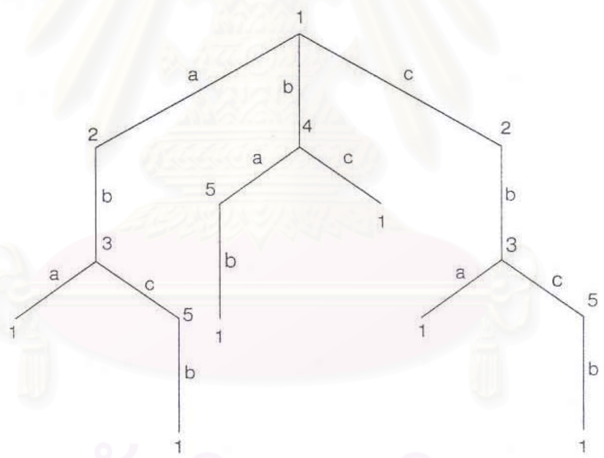
We have

$$\tau(cbab) = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \quad \text{and} \quad \tau(cbabcb) = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 1 & 4 \end{pmatrix}.$$

Thus $\tau(cbab)$ and $\tau(cbabcb)$ generate S_3. Hence $M(C^*)$ contains S_3 as a subgroup.

We tried to, based on the above code, construct a finite inverse biprefix code C whose $M(C^*)$ contains S_n for any $n \geq 3$. But this code cannot be used to generalized even for the case $n = 4$. We found the code in the next example which the generalization succeeded.

Example 4.4. Let $A = \{a, b, c\}$ and $C = \{aba, bab, abcb, cbcb, cbca. bc\}$. The tree representing C is shown below



The syntactic monoid $M(C^*)$ is generated by

$$\tau(a) = \begin{pmatrix} 1 & 3 & 4 \\ 2 & 1 & 5 \end{pmatrix}, \quad \tau(b) = \begin{pmatrix} 1 & 2 & 5 \\ 4 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \tau(c) = \begin{pmatrix} 1 & 3 & 4 \\ 2 & 5 & 1 \end{pmatrix}.$$

Thus

$$\tau(ab) = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \quad \text{and} \quad \tau(b) = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 1 & 4 \end{pmatrix}$$

generate S_3. Therefore $M(C^*)$ contains S_3.

Next, we shall show that given any positive integer n. we can construct an inverse biprefix code C whose syntactic monoid $M(C^*)$ contains the symmetric group S_n. Moreover later on we shall prove the similar result for the dihedral group D_n.

Before proving the main theorem on the existence of finite inverse biprefix codes whose syntactic monoids containing S_n. it will be convenient to prove the following propositions.

Proposition 4.5. Let $A = \{a_1, a_2, \ldots, a_n\}, n \geq 3$ be an alphabet.
Then $C = C_1 \cup C_2 \cup C_3$, where

$$C_1 = \{\ a_i a_{i+1} \ldots a_{n-1} a_1 a_2 \ldots a_i \mid i = 1, 2, \ldots, n-1\}$$

$$C_2 = \{\ a_i a_{i+1} \ldots a_n a_2 a_3 \ldots a_{i-1} \mid i = 3, 4, \ldots, n-1\}$$

$$C_3 = \{a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1}, a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}, a_n a_2 a_3 \ldots a_{n-1} a_1, a_2 a_3 \ldots a_n\}$$

is a finite inverse biprefix code.

Proof. First, note that any word in C has length $2(n-1)$, n, or $n-1$. To be more precised, we have

$$l(a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1}) = 2(n-1) = l(a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1})$$

$$l(w) = n = l(a_n a_2 a_3 \ldots a_{n-1} a_1) \quad \text{for all } w \in C_1 \text{ and}$$

$$l(w) = n - 1 = l(a_2 a_3 \ldots a_n) \quad \text{for all } w \in C_2.$$

We shall prove this proposition in two steps.

Step 1 We shall show that C is a finite biprefix code.

It is obvious that C is a finite prefix code. We shall show that C is suffix by considering the length of words in C. Since the maximal length of words in C is $2(n-1)$, it suffices to verify that any word of length n or $n-1$ is not a right factor of any other words in C.

Let $w \in C$. There are two cases to be considered.

Case 1: $l(w) = n$.

Then $w = a_n a_2 a_3 \ldots a_{n-1} a_1$ or $w \in C_1$. It suffices to show that w is not a right factor of $a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1}$ or $a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}$.

Case 1.1: $w = a_n a_2 a_3 \ldots a_{n-1} a_1$.

Since $a_{n-1} a_1$ is a right factor of w but it is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1},$$

we have that w is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Case 1.2: $w \in C_1$.

Then $w = a_i a_{i+1} \ldots a_{n-1} a_1 a_2 \ldots a_i$ for some $i \in \{1, 2, \ldots, n-1\}$. Thus $a_1 a_2 \ldots a_i$ is a right factor of w but it is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Hence w is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Case 2: $l(w) = n-1$.

Then $w = a_2a_3 \ldots a_n$ or $w \in C_2$. We need only to show that w is not a right factor of any word in C of length $2(n-1)$ or n.

Case 2.1: $w = a_2a_3 \ldots a_n$.

Since a_n is a right factor of w but it is not a right factor of any word in C of length $2(n-1)$ or n, w is not a right factor of any word in C of length $2(n-1)$ or n.

Case 2.2: $w \in C_2$.

Then $w = a_ia_{i+1} \ldots a_na_2a_3 \ldots a_{i-1}$ for some $i \in \{3, 4, \ldots, n-1\}$. Since a_{i-1} is a right factor of w but it is not a right factor of

$$a_1a_2 \ldots a_na_2a_3 \ldots a_{n-1}, \quad a_na_2a_3 \ldots a_na_2a_3 \ldots a_{n-1} \quad \text{or} \quad a_na_2a_3 \ldots a_{n-1}a_1,$$

it follows that w is not a right factor of

$$a_1a_2 \ldots a_na_2a_3 \ldots a_{n-1}, \quad a_na_2a_3 \ldots a_na_2a_3 \ldots a_{n-1} \quad \text{or} \quad a_na_2a_3 \ldots a_{n-1}a_1.$$

Next, we shall show that w is not a right factor of any word in C_1. Since $a_na_2a_3 \ldots a_{i-1}$ is a right factor of w but it is not a right factor of $a_ja_{j+1} \ldots a_{n-1}a_1a_2 \ldots a_j$ for all $j \in \{1, 2, \ldots, n-1\}$, w is not a right factor of any word in C_1

From two cases, C is suffix. Therefore C is a finite biprefix code.

Step 2 We shall show that $M(C^*)$ is an inverse semigroup by using Theorem 3.5.

First, we shall show that C satisfies (I.2)

Assume that $u^{-1}C \cap v^{-1}C \cap A^+ \neq \emptyset$ with $u \neq \epsilon$.

Case 1: $u^{-1}C \cap v^{-1}C \cap A^+ = \{a_2\}$. There are only two words in C ending with a_2, namely

$$a_2a_3 \ldots a_{n-1}a_1a_2 \quad \text{and} \quad a_3a_4 \ldots a_{n-1}a_2.$$

Moreover

$$(a_2a_3\dots a_{n-1}a_1)^{-1}C = \{a_2\} = (a_3a_4\dots a_{n-1})^{-1}C.$$

Case 2: $u^{-1}C \cap v^{-1}C \cap A^+ = \{a_2a_3\dots a_{n-1}\}$. There are only three words in C ending with $a_2a_3\dots a_{n-1}$, namely

$$a_1a_2a_3\dots a_na_2a_3\dots a_{n-1},\ a_na_2a_3\dots a_na_2a_3\dots a_{n-1} \text{ and } a_{n-1}a_1a_2\dots a_{n-1}.$$

Moreover

$$(a_1a_2\dots a_n)^{-1}C = \{a_2a_3\dots a_{n-1}\} = (a_na_2a_3\dots a_n)^{-1}C = (a_{n-1}a_1)^{-1}C.$$

Case 3: $u^{-1}C \cap v^{-1}C \cap A^+ = (a_1w)^{-1}C$ for some $w \in A^*$.

Since

$$(a_1)^{-1}C = \{a_2a_3\dots a_na_2a_3\dots a_{n-1}, a_2a_3\dots a_{n-1}a_1\} = (a_n)^{-1}C,$$

$(a_1w)^{-1}C = (a_nw)^{-1}C$ for all $w \in A^*$.

In all cases, we can conclude that $u^{-1}C = v^{-1}C$.

To finish the proof of the proposition, we need to find an inverse sequence for each $a \in A$.

For each $i \in \{1, 2, \dots, n-1\}$, let

$$\begin{aligned} A_{a_i} &= \{a_i, a_{i+1}, \dots, a_{n-1}, a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}, a_1, a_2, \dots, a_{i-1} \\ &\quad, \dots, a_i, a_{i+1}, \dots, a_{n-1}, a_1, a_2, \dots, a_{i-1}\} \\ &\equiv \{b_1, b_2, \dots, b_{(n-1)n}\} \end{aligned}$$

Note that a_{i-1} means a_{n-1} in case $i = 1$.

To show that for each A_{a_i} is an inverse sequence for a_i, we shall apply Proposition 3.12 as follows:

(i) For $b_1b_2\dots b_n \equiv a_ia_{i+1}\dots a_{n-1}a_1a_2\dots a_i \in C$, since

$$\{b_1b_2\ldots b_n, b_{n+1}b_{n+2}\ldots b_{2n},\ldots, b_{(n-2)n+1}b_{(n-2)n+2}\ldots b_{(n-1)n}\}$$

$$\equiv \{a_ia_{i+1}\ldots a_{n-1}a_1a_2\ldots a_i, a_{i+1}a_{i+2}\ldots a_{n-1}a_1a_2\ldots a_{i+1},$$
$$\ldots, a_{i-1}a_i\ldots a_{n-1}a_1a_2\ldots a_{i-1}\}$$

$$= C_1 \subseteq C,$$

it follows that

$$(1\ \ 2\ldots n \mid n+1\ \ n+2\ \ldots\ 2n \mid \ldots \mid (n-2)+1\ \ (n-2)+2\ \ldots\ (n-1)n)$$

is the required partition.

(ii) For each j such that $b_jb_{j+1}\ldots b_{(n-1)n}b_1b_2\ldots b_{(2-n)n+j-1} \equiv a_ka_{k+1}\ldots a_{n-1}a_1a_2\ldots a_k \in C$ for some $k \in \{1,2,\ldots,n-1\}$, we have that

$$(j\ \ j+1\ \ldots\ (n-1)n\ \ 1\ \ 2\ \ldots\ (2-n)n+j-1 \mid (2-n)n+j\quad (2-n)n+j+1$$
$$\ldots\ (3-n)n+j-1 \mid \ldots \mid -n+j\quad -n+j+1\ \ldots\ j-1)$$

is a partition of cyclic permutation $(j\ \ j+1\ \ldots\ (n-1)n\ \ 1\ \ 2\ \ldots\ j-1)$ on $\{1,2,\ldots,(n-1)n\}$ such that

$$\{b_jb_{j+1}\ldots b_{(n-1)n}b_1b_2\ldots b_{(2-n)n+j-1}, b_{(2-n)n+j}b_{(2-n)n+j+1}\ldots b_{(3-n)n+j-1},$$
$$\ldots, b_{-n+j}b_{n+j+1}\ldots b_{j-1}\}$$

$$\equiv \{a_ka_{k+1}\ldots a_{n-1}a_1a_2\ldots a_k, a_{k+1}a_{k+2}\ldots a_{n-1}a_1a_2\ldots a_{k+1},$$
$$\ldots, a_{k-1}a_{k-2}\ldots a_{n-1}a_1a_2\ldots a_{k-1}\}$$

$$= C_1 \subseteq C.$$

(iii) Finding an associated word (w.r.t A_{a_i}) of xa_iy depends strongly on the appearance of a_i in the code words.

Case 1: $x = \epsilon$. By Remarks 3.8 ,$a_ia_{i+1}\ldots a_{n-1}a_1a_2\ldots a_i$ is an associated word (w.r.t A_{a_i}) of xa_iy.

Case 2: $xa_iy \in C_1$. Clearly xa_iy is both an associated word (w.r.t A_{a_i}) and a companion of itself.

Case 3: $xa_iy = ba_{j_1}a_{j_1+1}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k$ for some $b \in \{\epsilon, a_n\}$ $j_1, k \in \{1,2,\ldots,n-1\}$ and $j_2 \in \{1,2\}$. Then

$$x = ba_{j_1}a_{j_1+1}\ldots a_{i-1} \text{ and } y = a_{i+1}a_{i+2}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k,$$

or

$$x = ba_{j_1}a_{j_1+1}\ldots a_na_{j_2}a_{j_2+1}\ldots a_{i-1} \text{ and } y = a_{i+1}a_{i+2}\ldots a_k$$

Case 3.1: $x = ba_{j_1}a_{j_1+1}\ldots a_{i-1}$ and $y = a_{i+1}a_{i+2}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k$

If $b = \epsilon$, then

$$x^{-1}C = \{a_ia_{i+1}a_{i+2}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k, a_ia_{i+1}\ldots a_{n-1}a_1a_2\ldots a_{j_1}\}$$

$$= (a_{j_1}a_{j_1+1}\ldots a_{i-1})^{-1}C.$$

Thus $a_{j_1}a_{j_1+1}\ldots a_{n-1}a_1a_2\ldots a_{j_1}$ is both an associated word (w.r.t A_{a_i}) and a companion of xa_iy.

If $b = a_n$, then

$$x^{-1}C = \{a_ia_{i+1}a_{i+2}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k, a_ia_{i+1}\ldots a_{n-1}a_1\} = (a_1a_2\ldots a_{i-1})^{-1}C.$$

Thus $a_1a_2\ldots a_{n-1}a_1$ is both an associated word (w.r.t A_{a_i}) and a companion of xa_iy.

Case 3.2: $x = ba_{j_1}a_{j_1+1}\ldots a_na_{j_2}a_{j_2+1}\ldots a_{i-1}$ and $y = a_{i+1}a_{i+2}\ldots a_k$

Since

$$x^{-1}C = \{a_ia_{i+1}\ldots a_k\} = (a_ka_{k+1}\ldots a_{n-1}a_1a_2\ldots a_{i-1})^{-1}C,$$

$a_ka_{k+1}\ldots a_{n-1}a_1a_2\ldots a_k$ is both an associated word (w.r.t A_{a_i}) and a companion of xa_iy.

It remains to find an inverse for a_n. Again, we shall use Proposition 3.12 to show that

$$A_{a_n} = \{a_n, a_2, a_3, \ldots, a_n, a_2, a_3, \ldots, a_{n-1}\} \equiv \{b_1, b_2, \ldots b_{2(n-1)}\}$$

is an inverse sequence for a_n.

(i) For $b_1 b_2 \dots b_{2(n-1)} \equiv a_n a_2 a_3 \dots a_n a_2 a_3 \dots a_{n-1} \in C$, $(1 \ \ 2 \ \dots 2(n-1))$ is a partition of cyclic permutation $(1\ 2 \dots\ 2(n-1))$ on $\{1, 2, \dots, 2(n-1)\}$ such that

$$\{b_1 b_2 \dots b_{2(n-1)}\} \equiv \{a_n a_2 a_3 \dots a_n a_2 a_3 \dots a_{n-1}\} \subseteq C.$$

(ii) We shall find the required partition for $b_j b_{j+1} \dots b_{2(n-1)} b_1 b_2 \dots b_{j-1} \in C$, in three cases as follows:

Case 1: For $b_{n+1} b_{n+2} \dots b_{2(n-1)} b_1 \equiv a_2 a_3 \dots a_n \in C$, we have that

$$(n+1 \ \ n+2 \ \dots 2(n-1) \ \ 1 \mid 2\ 3 \ \dots \ n)$$

is a partition of cyclic permutation $(n+1 \ \ n+2 \ \dots 2(n-1) \ \ 1\ 2 \ \dots \ n)$ such that

$$\{b_{n+1} b_{n+2} \dots b_{2(n-1)} b_1, b_2 b_3 \dots b_n\} \equiv \{a_2 a_3 \dots a_n\} \subseteq C.$$

Case 2: For $b_n b_{n+1} \dots b_{2(n-1)} b_1 b_2 \dots b_{n-1} \equiv a_n a_2 a_3 \dots a_n a_2 a_3 \dots a_{n-1} \in C$, we have that

$$(n \ \ n+1 \ \ n+2 \ \dots 2(n-1) \ \ 1\ 2 \ \dots \ n-1)$$

is a partition of cyclic permutation $(n \ \ n+1 \ \ n+2 \ \dots 2(n-1) \ \ 1\ 2 \ \dots \ n-1)$ such that

$$\{b_n b_{n+1} b_{n+2} \dots b_{2(n-1)} b_1 b_2 b \dots b_{n-1}\} \equiv \{a_n a_2 a_3 \dots a_n a_2 a_3 \dots a_{n-1}\} \subseteq C$$

.

Case 3: For $b_{n+k-1} b_{n+k} \dots b_{2(n-1)} b_1 b_2 \dots b_{n+k-2} \equiv a_k a_{k+1} \dots a_n a_2 a_3 \dots a_{k-1} \in C$ for some $k \in \{3, 4, \dots, n-1\}$, we have that

$$(n+k-1 \ \ n+k \ \dots 2(n-1) \ \ 1\ 2 \ \dots k-1 \mid k \ \ k+1 \dots \ n+k-2)$$

is a partition of cyclic permutation

$$(n+k-1 \ \ n+k \ \dots 2(n-1) \ \ 1\ 2 \ \dots \ n+k-2)$$

such that

$\{b_{n+k-1}b_{n+k}\dots b_{2(n-1)}b_1b_2\dots b_{k-1}, b_kb_{k+1}\dots b_{n+k-2}\}$

$\equiv \{a_ka_{k+1}\dots a_na_2a_3\dots a_{k-1}\} \subseteq C_2 \subseteq C$.

(iii) We shall find an associated word (w.r.t A_{a_n}) and a companion word for any xa_ny in C as follows :

Case 1: $xa_ny = a_2a_3\dots a_n$ or $xa_ny \in C_2$ or $xa_ny = a_na_2a_3\dots a_na_2a_3\dots a_{n-1}$.

By Remarks 3.8 , xa_ny is both an associated word (w.r.t A_{a_n}) and a companion of itself.

Case 2: $xa_ny = a_1a_2a_3\dots a_na_2a_3\dots a_{n-1}$

Then $(a_1a_2\dots a_{n-1})^{-1}C = \{a_na_2a_3\dots a_{n-1}, a_1\} = (a_na_2a_3\dots a_{n-1})^{-1}C$. Thus $a_na_2a_3\dots a_na_2a_3\dots a_{n-1}$ is both an associated word (w.r.t A_{a_n}) and a companion of xa_ny.

Therefore C is a finite inverse biprefix code. □

Proposition 4.6. The syntactic monoid $M(C^*)$ of the code C defined in Proposition 4.5 contains the symmetric group S_n.

Proof. Note that the nodes associated with a_1 and a_n are labelled with the same name since $a_1^{-1}C = a_n^{-1}C$. It suffices to label only the nodes associated with a_iw where $i \in \{1, 2, \dots, n-1\}, w \in A^*$.

We label the tree representation of C^* as follows :

The top and the end points of the tree are labelled 1.

For each $i \in \{1, 2, \dots, n-1\}$,

the node associated with a_i is labelled

$$(n+1) + (i-2)(n-1),$$

the node associated with $a_i a_{i+1}$ is labelled

$$(n+1)+(i-2)(n-1)+1,$$

the node associated with $a_i a_{i+1} a_{i+2}$ is labelled

$$(n+1)+(i-2)(n-1)+2,$$

$$\vdots$$

the node associated with $a_i a_{i+1} \dots a_{n-1}$ is labelled

$$(n+1)+(i-2)(n-1)+(n-1-i),$$

the node associated with $a_i a_{i+1} \dots a_{n-1} a_1$ is labelled

$$(n+1)+(i-2)(n-1)+(n-i),$$

$$\vdots$$

and the node associated with $a_i a_{i+1} \dots a_{n-1} a_1 a_2 \dots a_{i-1} (a_1 a_2 \dots a_{n-1} a_1$ in case $i = 1)$ is labelled

$$(n+1)+(i-2)(n-1)+(n-2).$$

Since each of the remaining unlabelled nodes has the same subtree as one of the above labelled nodes. they must have the same name. Hence $P_{C^*}^{(r)}$ has been constructed.

The corresponding syntactic monoid $M(C^*)$ is generated by $\{\tau(a_i) \mid i = 1, 2, \dots, n\}$ where $\tau(a_i)$'s are defined as follows :

$$\tau(a_1) = \begin{pmatrix} 1 & n & 2n-2 & 3n-4 & \cdots & (n-1)n-2(n-2) \\ 2 & 1 & 2n-1 & 3n-3 & \cdots & (n-1)n-2(n-2)+1 \end{pmatrix}$$

$$\tau(a_2) = \begin{pmatrix} 1 & 2 & 2n-1 & 3n-3 & \cdots & (n-1)n-2(n-2)+1 \\ n+1 & 3 & 1 & 3n-2 & \cdots & (n-1)n-2(n-2)+2 \end{pmatrix}$$

$$\tau(a_3) = \begin{pmatrix} 1 & 3 & n+1 & 3n-2 & \cdots & (n-1)n-2(n-2)+2 \\ (n+1)+(n-1) & 4 & n+2 & 1 & \cdots & (n-1)n-2(n-2)+3 \end{pmatrix}$$

$$\vdots$$

$$\tau(a_{n-1}) = \begin{pmatrix} 1 & n-1 & 2n-3 & 3n-5 & \cdots & nn-(n-2) \\ (n+1)+(n-3)(n-1) & n & 2n-2 & 3n-4 & \cdots & 1 \end{pmatrix}$$

$$\tau(a_n)$$

$$= \begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-1)n-2(n-2) \\ 2 & (n+1)+(n-3)(n-1)+1 & 1 & \cdots & (n-1)n-2(n-2)-(n-3) \end{pmatrix}.$$

To be precised for each $i \in \{2, 3, \ldots, n-1\}$, $\tau(a_i)$ is defined as follows:

$$1\tau(a_i) = (n+1) + (i-2)(n-1)$$

$$i\tau(a_i) = i + 1$$

for each $k \in \{2, 3, \ldots, i-1\}$,

$$((n+1) + (k-2)(n-1) + (i-k-1))\tau(a_i) = (n+1) + (k-2)(n-1) + i - k$$

and

for each $k \in \{i, i+1, \ldots, n-1\}$.

$$(kn-2(k-1)+(i-1))\tau(a_i) = \begin{cases} 1 & \text{if} \quad k = i \\ kn-2(k-1)+i & \text{if} \quad k \in \{i+1, i+2, \ldots, n-1\}. \end{cases}$$

Then we obtain that

$$\tau(a_1a_2\ldots a_{n-1})$$
$$= \begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-2)n-2(n-3) & (n-1)n-2(n-2) \\ n & 2n-2 & 3n-4 & \cdots & (n-1)n-2(n-2) & 1 \end{pmatrix}$$

and

$$\tau(a_na_2\ldots a_{n-1})$$
$$= \begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-2)n-2(n-3) & (n-1)n-2(n-2) \\ n & 1 & 2n-2 & \cdots & (n-2)n-2(n-3) & (n-1)n-2(n-2) \end{pmatrix}.$$

Then $\tau(a_1a_2\ldots a_{n-1})$ and $\tau(a_na_2\ldots a_{n-1})$ generate S_n. Therefore S_n is a subgroup of the syntactic monoid $M(C^*)$. □

Theorem 4.7. For each n, there is a finite inverse biprefix code C whose syntactic monoid of C^* contains S_n as a subgroup.

Proof. If $n = 1$ or $n = 2$, S_n must be cyclic group. By Corollary4.2, $C = A^n$. If $n \geq 3$, then the theorem is obtained directly from Proposition 4.5 and Proposition 4.6. □

Before showing the existence of finite inverse biprefix codes whose syntactic monoids containing D_n, it will be convenient to prove the following propositions.

Proposition 4.8. Let $A = \{a_1, a_2, \ldots, a_n\}, n \geq 3$ be an alphabet.

Then $C = C_1 \cup C_2 \cup C_3$, where

$$C_1 = \{ \ a_i a_{i+1} \ldots a_{n-1} a_1 a_2 \ldots a_i \mid i = 1, 2, \ldots, n-1\}$$

$$C_2 = \{ \ a_i a_{i+1} \ldots a_n a_2 a_3 \ldots a_{n-i} \mid i = 2, 3, \ldots, n-2\}$$

$$C_3 = \{a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1}, a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}, a_n a_2 a_3 \ldots a_{n-1} a_1, a_{n-1} a_n\}$$

is a finite inverse biprefix code.

Proof. First, note that any word in C has length 2, $n, 2(n-1)$, or $2(n-i)$ for all $i \in \{2, 3, \ldots, n-2\}$. To be more precised, we have that

$$l(a_{n-1}a_n) = 2$$

$$l(a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1}) = 2(n-1) = l(a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1})$$

$$l(w) = n = l(a_n a_2 a_3 \ldots a_{n-1} a_1) \text{ for all } w \in C_1 \text{ and}$$

$$l(a_i a_{i+1} \ldots a_n a_2 a_3 \ldots a_{n-i}) = 2(n-i) \text{ for all } i \in \{2, 3, \ldots, n-2\}.$$

We shall prove this proposition in two steps.

Step 1 We shall show that C is a finite biprefix code.

It is clear that C is a finite prefix code. We shall show that C is suffix by considering the length of words in C. Since the maximal length of words in C is $2(n-1)$, it suffices to verify that words of length $2, n$ or $2(n-i)$ for all $i \in \{2, 3, \ldots, n-2\}$ is not a right factor of any other words in C.

Let $w \in C$. There are three cases to be considered.

Case 1: $l(w) = 2$.

Then $w = a_{n-1}a_n$. It is easy to see that $a_{n-1}a_n$ is not a right factor of any word in C.

Case 2: $l(w) = n$.

Then $w = a_n a_2 a_3 \ldots a_{n-1} a_1$ or $w \in C_1$. It suffices to show that w is not a right factor of $a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1}$ or $a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}$.

Case 2.1: $w = a_n a_2 a_3 \ldots a_{n-1} a_1$.

Then $a_{n-1} a_1$ is a right factor of w but it is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Thus w is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Case 2.2: $w \in C_1$.

Then $w = a_i a_{i+1} \ldots a_{n-1} a_1 a_2 \ldots a_i$ for some $i \in \{1, 2, \ldots, n-1\}$. Thus $a_1 a_2 \ldots a_i$ is a right factor of w but it is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Hence w is not a right factor of

$$a_1 a_2 \ldots a_n a_2 a_3 \ldots a_{n-1} \quad \text{or} \quad a_n a_2 a_3 \ldots a_n a_2 a_3 \ldots a_{n-1}.$$

Case 3: $l(w) = 2(n-i)$ for some $i \in \{2, 3, \ldots, n-2\}$.

Then $w = a_i a_{i+1} \ldots a_n a_2 a_3 \ldots a_{n-i}$. We need only to show that w is not a right factor of words in C of length n or $2(n-1)$.

Since $a_n a_2 a_3 \ldots a_{n-i}$ is a right factor of w but it is not a right factor of any word in C of length n or $2(n-1)$, we have w is not a right factor of any word in C of length n or $2(n-1)$.

Thus C is suffix. Therefore C is a finite biprefix code.

Step 2 We shall show that $M(C^*)$ is an inverse semigroup by using Theorem 3.5.

We shall first show that C satisfies (I.2).

Assume that $u^{-1}C \cap v^{-1}C \cap A^+ \neq \emptyset$. with $u \neq \epsilon$

Case 1: $u^{-1}C \cap v^{-1}C \cap A^+ = \{a_2\}$.

There are only two words in C ending with a_2, namely

$$a_2a_3\ldots a_{n-1}a_1a_2 \text{ and } a_{n-2}a_{n-1}a_na_2.$$

Moreover

$$(a_2a_3\ldots a_{n-1}a_1)^{-1}C = \{a_2\} = (a_{n-2}a_{n-1}a_n)^{-1}C.$$

Case 2: $u^{-1}C \cap v^{-1}C \cap A^+ = \{a_2a_3\ldots a_{n-1}\}$.

There are only three words in C ending with $a_2a_3\ldots a_{n-1}$, namely

$$a_1a_2a_3\ldots a_na_2a_3\ldots a_{n-1}, a_na_2a_3\ldots a_na_2a_3\ldots a_{n-1} \text{ and } a_{n-1}a_1a_2\ldots a_{n-1}.$$

Moreover

$$(a_1a_2\ldots a_n)^{-1}C = \{a_2a_3\ldots a_{n-1}\} = (a_na_2a_3\ldots a_n)^{-1}C = (a_{n-1}a_1)^{-1}C.$$

Case 3: $u^{-1}C \cap v^{-1}C \cap A^+ = (a_1w)^{-1}C$ for some $w \in A^*$.

Since

$$(a_1)^{-1}C = \{a_2a_3\ldots a_na_2a_3\ldots a_{n-1}, a_2a_3\ldots a_{n-1}a_1\} = (a_n)^{-1}C,$$

$(a_1w)^{-1}C = (a_nw)^{-1}C$ for all $w \in A^*$.

Case 4: $u^{-1}C \cap v^{-1}C \cap A^+ = \{a_2a_3\ldots a_{n-2}\}$.

There are only two words in C ending with $a_2a_3\ldots a_{n-2}$, namely

$$a_{n-2}a_{n-1}a_na_1a_2\ldots a_{n-2} \text{ and } a_2a_3\ldots a_na_2a_3\ldots a_{n-2}.$$

Moreover

$$(a_{n-2}a_{n-1}a_1)^{-1}C = \{a_2a_3 \dots a_{n-2}\} = (a_2a_3 \dots a_n)^{-1}C.$$

In all cases, we obtain that $u^{-1}C = v^{-1}C$.

To finish the proof of the proposition, we need to find an inverse sequence for each $a \in A$.

For each $i \in \{1, 2, \dots, n-1\}$, let

$A_{a_i} = \{a_i, a_{i+1}, \dots, a_{n-1}, a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}, a_1, a_2, \dots, a_{i-1}$

$, \dots, a_i, a_{i+1}, \dots, a_{n-1}, a_1, a_2, \dots, a_{i-1}\}$

$\equiv \{b_1, b_2, \dots, b_{(n-1)n}\}$

Note that a_{i-1} means a_{n-1} in case $i = 1$.

We shall show that A_{a_i} is an inverse sequence for a_i applying Proposition 3.12 as follows:

(i) For $b_1b_2 \dots b_n \equiv a_ia_{i+1} \dots a_{n-1}a_1a_2 \dots a_i \in C$ since $\{b_1b_2 \dots b_n, b_{n+1}b_{n+2} \dots b_{2n}, \dots, b_{(n-2)+1}b_{(n-2)+2} \dots b_{(n-1)n}\}$

$\equiv \{a_ia_{i+1} \dots a_{n-1}a_1a_2 \dots a_i, a_{i+1}a_{i+2} \dots a_{n-1}a_1a_2 \dots a_{i+1}, \dots,$

$, \dots, a_{i-1}a_i \dots a_{n-1}a_1a_2 \dots a_{i-1}\}$

$= C_1 \subseteq C,$

it follows that $(1 \ 2 \dots n \mid n{+}1 \ \ n{+}2 \dots 2n \mid \dots \ (n{-}2){+}1 \ \ (n{-}2){+}2 \dots \ (n{-}1)n)$ is the required partition.

(ii) For each j, such that $b_jb_{j+1} \dots b_{(n-1)n}b_1b_2 \dots b_{(2-n)n+j-1} \equiv a_ka_{k+1} \dots a_{n-1}a_1a_2 \dots a_k \in C$ for some $k \in \{1, 2, \dots, n-1\}$, we have that

$(j \ \ j+1 \ \dots \ (n-1)n \ \ 1 \ \ 2 \ \dots \ (2-n)n-j-1 \mid (2-n)n+j$

$(2-n)n+j+1 \ \dots \ (3-n)n+j-1 \mid \dots \mid -n-j \ \ -n+j+1 \ \dots \ j-1)$ is a partition of cyclic permutation $(j \ \ j+1 \ \dots \ (n-1)n \ \ 1 \ \ 2 \ \dots \ j-1)$ on $\{1, 2, \dots, (n-1)n\}$ such that $\{b_jb_{j+1} \dots b_{(n-1)n}b_1b_2 \dots b_{(2-n)n+j-1}, b_{(2-n)n+j}b_{(2-n)n+j+1} \dots b_{(3-n)n+j-1},$

$$\ldots, b_{-n+j}b_{n+j+1}\ldots b_{j-1}\}$$

$$\equiv \{a_k a_{k+1}\ldots a_{n-1}a_1a_2\ldots a_k, a_{k+1}a_{k+2}\ldots a_{n-1}a_1a_2\ldots a_{k+1},$$

$$\ldots, a_{k-1}a_{k-2}\ldots a_{n-1}a_1a_2\ldots a_{k-1}\}$$

$$= C_1 \subseteq C.$$

(iii) Finding an associated word (w.r.t A_{a_i}) of xa_iy depends strongly on the appearance of a_i in the code word.

Case 1: $x = \epsilon$.

By Remarks 3.8, $a_ia_{i+1}\ldots a_{n-1}a_1a_2\ldots a_i$ is an associated word (w.r.t A_{a_i}) of xa_iy.

Case 2: $xa_iy \in C_1$.

By remarks 3.8. xa_iy is both an associated word (w.r.t A_{a_i}) and a companion of itself.

Case 3: $xa_iy = ba_{j_1}a_{j_1+1}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k$ for some $b \in \{\epsilon, a_n\}$ and $j_1, k \in \{1, 2, \ldots, n-1\}$.

Then

$$x = ba_{j_1}a_{j_1+1}\ldots a_{i-1} \text{ and } y = a_{i+1}a_{i+2}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k,$$

or

$$x = ba_{j_1}a_{j_1+1}\ldots a_na_{j_2}a_{j_2+1}\ldots a_{i-1} \text{ and } y = a_{i+1}a_{i+2}\ldots a_k$$

Case 3.1 : $x = ba_{j_1}a_{j_1+1}\ldots a_{i-1}$ and $y = a_{i+1}a_{i+2}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k$.

if $b = \epsilon$, then

$$x^{-1}C = \{a_ia_{i+1}\ldots a_na_{j_2}a_{j_2+1}\ldots a_k, a_ia_{i+1}\ldots a_{n-1}a_1a_2\ldots, a_{j_1}\}$$

$$= (a_{j_1}a_{j_1+1}\ldots a_{i-1})^{-1}C.$$

Thus $a_{j_1}a_{j_1+1}\ldots a_{n-1}a_1a_2\ldots a_{j_1}$ is both an associated word (w.r.t A_{a_i}) and a companion of xa_iy.

if $b = a_n$, then

$$x^{-1}C = \{a_i a_{i+1} a_{i+2} \dots a_n a_{j_2} a_{j_2+1} \dots a_k, a_i a_{i+1} \dots a_{n-1} a_1\} = (a_1 a_2 \dots a_{i-1})^{-1} C.$$

We have $a_1 a_2 \dots a_{n-1} a_1$ is both an associated word (w.r.t A_{a_i}) and a companion of $x a_i y$.

Case 3.2: $x = b a_{j_1} a_{j_1+1} \dots a_n a_{j_2} a_{j_2+1} \dots a_{i-1}$ and $y = a_{i+1} a_{i+2} \dots a_k$

Then $x^{-1}C = \{a_i a_{i+1} \dots a_k\} = (a_k a_{k+1} \dots a_{n-1} a_1 a_2 \dots a_{i-1})^{-1} C$.

Thus $a_k a_{k+1} \dots a_{n-1} a_1 a_2 \dots a_k$ is both an associated word (w.r.t A_{a_i}) and a companion of $x a_i y$.

It remains to find an inverse sequence for a_n. Again, we shall apply Proposition 3.12

$$A_{a_n} = \{a_n, a_2, a_3, \dots, a_n, a_2, a_3, \dots, a_{n-1}\} \equiv \{b_1, b_2, \dots b_{2(n-1)}\}.$$

is an inverse sequence for a_n.

(i) For $b_1 b_2 \dots b_{2(n-1)} \equiv a_n a_2 a_3 \dots a_n a_2 a_3 \dots a_{n-1} \in C$, since

$$\{b_1 b_2 \dots b_{2(n-1)} \equiv \{a_n a_2 a_3 \dots a_n a_2 a_3 \dots a_{n-1}\} \subseteq C,$$

it follows that $(1\ 2\ \dots 2(n-1))$ is a partition of cyclic permutation $(1\ 2 \dots\ 2(n-1))$ on $\{1, 2, \dots, 2(n-1)\}$.

(ii) We shall find the required partitions for $b_j b_{j+1} \dots b_{2(n-1)} b_1 b_2 \dots b_{j_1} \in C$, in three cases as follows:

Case 1: For $b_{2(n-1)} b_1 \equiv a_{n-1} a_n \in C$, we have that $\{b_{2(n-1)} b_1, b_2 b_3 \dots b_{2(n-1)-1}\} \equiv \{a_{n-1} a_n, a_2 a_3, \dots a_n a_2 a_3 \dots a_{n-2}\} \subseteq C$. Thus

$$(2(n-1)\ 1 \mid 2\ \ 3\ \dots\ 2(n-1)-1)$$

is a required partition.

Case 2: For $b_{n+k-1}b_{n+k}\dots b_{2(n-1)}b_1b_2\dots b_k \equiv a_ka_{k+1}\dots a_na_2a_3\dots a_{n-k}$ for some $k\in\{2,3,\dots,(n-2)\}$. Thus

$$(n+k-1\ \ n+k\ \dots 2(n-1)\ \ 1\ \ 2\ \dots\ k \mid k+1\ k+2\ \dots\ n+k-2)$$

is a partition of cyclic permutation

$$(n+k-1\ n+k\ \ \dots 2(n-1)\ \ 1\ \ 2\ \dots\ n+k-2)$$

on $\{1,2,\dots.2(n-1)\}$ such that

$\{b_{n+k-1}b_{n+k}\dots b_{2(n-1)}b_1b_2\dots b_k, b_{k+1}b_{k+2}\dots b_{n+k-2}\}$

$\equiv \{a_ka_{k+1}\dots a_na_2a_3\dots a_{n-k}, a_{n-k+1}a_{n-k+2}\dots a_na_2a_3\dots a_{k-1}\}$

$\subseteq C_2 \subseteq C$.

Case 3: For $b_nb_{n+1}\dots b_{2(n-1)}b_1b_2\dots b_{n-1} \equiv a_na_2a_3\dots a_na_2a_3\dots a_{n-1}\in C$, then $(n\ \ n+1\ \dots\ 2(n-1)\ \ 1\ \ 2\ \dots\ n-1)$ is a partition of cyclic permutation $(n\ \ n+1\ \dots\ 2(n-1)\ \ 1\ \ 2\ \dots\ n-1)$ such that $\{b_nb_{n+1}\dots b_{2(n-1)}b_1b_2\dots b_{n-1}\} \equiv \{a_na_2a_3\dots a_na_2a_3\dots a_{n-1}\}\subseteq C$.

(iii) We shall find an associated word (w.r.t A_{a_n}) and a companion word for any xa_ny in C as follows :

Case 1: $xa_ny = a_{n-1}a_n$ or $xa_ny\in C_2$ or $xa_ny = a_na_2a_3\dots a_na_2a_3\dots a_{n-1}$.

By Remarks 3.8, xa_ny is its both an associated word (w.r.t A_{a_n}) and a companion word of itself in case $x\neq\epsilon$.

Case 2: $xa_ny = a_1a_2\dots a_na_2a_3\dots a_{n-1}$.

Then $(a_1a_2\dots a_{n-1})^{-1}C = \{a_na_2a_3\dots a_{n-1}, a_1\} = (a_na_2a_3\dots a_{n-1})^{-1}C$. Thus $a_na_2a_3\dots a_na_2a_3\dots a_{n-1}$ is both an associated word (w.r.t A_{a_n}) and a companion of xa_ny.

Therefore C is an inverse biprefix code. $\square$

Proposition 4.9. The syntactic monoid $M(C^*)$ of the code C defined in Proposition 4.8. contains the dihedral group D_n.

Proof. Note that the nodes associated with a_1 and a_n are labelled with the same name since $a_1^{-1}C = a_n^{-1}C$. It suffices to label only the nodes associated with a_iw where $i \in \{1, 2, \ldots, n-1\}, w \in A^*$.

We label the tree representation of C^* as follows :

The top and the end points of the tree are labelled 1.

For each $i \in \{1, 2, \ldots, n-1\}$,

the node associated with a_i is labelled

$$(n+1) + (i-2)(n-1) \quad ,$$

the node associated with a_ia_{i+1} is labelled

$$(n+1) + (i-2)(n-1) + 1 \quad ,$$

the node associated with $a_ia_{i+1}a_{i+2}$ is labelled

$$(n+1) + (i-2)(n-1) + 2 \quad ,$$

$$\vdots$$

the node associated with $a_ia_{i+1}\ldots a_{n-1}$ is labelled

$$(n+1) + (i-2)(n-1) + (n-1-i) \quad ,$$

the node associated with $a_ia_{i+1}\ldots a_{n-1}a_1$ is labelled

$$(n+1) + (i-2)(n-1) + (n-i) \quad ,$$

and the node associated with $a_ia_{i+1}\ldots a_{n-1}a_1a_2\ldots a_{i-1}(a_1a_2\ldots a_{n-1}a_1$ in case $i=1)$ is labelled

$$(n+1)+(i-2)(n-1)+(n-2)\quad .$$

Since each of the remaining unlabelled nodes has the same subtree as one of the above labelled nodes, they must have the same name. Hence $P^{(r)}_{C^*}$ has been constructed.

The corresponding syntactic monoid $M(C^*)$ is generated by $\{\tau(a_i)\mid i=1,2,\ldots,n\}$ where $\tau(a_i)$'s are defined as follows :

$$\tau(a_1)=\begin{pmatrix} 1 & n & 2n-2 & 3n-4 & \cdots & (n-1)n-2(n-2) \\ 2 & 1 & 2n-1 & 3n-3 & \cdots & (n-1)n-2(n-2)+1 \end{pmatrix}$$

$$\tau(a_2)=\begin{pmatrix} 1 & 2 & 2n-1 & 3n-3 & \cdots & (n-1)n-2(n-2)+1 \\ n+1 & 3 & 1 & 3n-2 & \cdots & (n-1)n-2(n-2)+2 \end{pmatrix}$$

$$\tau(a_3)=\begin{pmatrix} 1 & 3 & n+1 & 3n-2 & \cdots & (n-1)n-2(n-2)+2 \\ (n+1)+(n-1) & 4 & n+2 & 1 & \cdots & (n-1)n-2(n-2)+3 \end{pmatrix}$$

$$\vdots$$

$$\tau(a_{n-1})=\begin{pmatrix} 1 & n-1 & 2n-3 & 3n-5 & \cdots & nn-(n-2) \\ (n+1)+(n-3)(n-1) & n & 2n-2 & 3n-4 & \cdots & 1 \end{pmatrix}$$

$$\tau(a_n)$$
$$=\begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-1)n-2(n-2) \\ 2 & (n+1)+(n-3)(n-1)+1 & (n-1)n-2(n-2)+1 & \cdots & 1 \end{pmatrix}$$

To be precised for each $i\in\{2,3,\ldots,n-1\}$, $\tau(a_i)$ is defined as follows:

$1\tau(a_i)=(n+1)+(i-2)(n-1)$

$i\tau(a_i) = i+1$

for each $k \in \{2, 3, \ldots, i-1\}$,

$$((n+1)+(k-2)(n-1)+(i-k-1))\tau(a_i) = (n+1)+(k-2)(n-1)+i-k$$

and

for each $k \in \{i, i+1, \ldots, n-1\}$,

$$(kn-2(k-1)+(i-1))\tau(a_i) = \begin{cases} 1 & \text{if } \ k = i \\ kn-2(k-1)+i & \text{if } \ k \in \{i+1, i+2, \ldots, n-1\}. \end{cases}$$

Then we obtain that

$$\tau(a_1a_2\ldots a_{n-1})$$
$$= \begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-2)n-2(n-3) & (n-1)n-2(n-2) \\ n & 2n-2 & 3n-4 & \cdots & (n-1)n-2(n-2) & 1 \end{pmatrix}$$

and

$$\tau(a_na_2\ldots a_{n-1})$$
$$= \begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-1)n-2(n-2) \\ 2 & 1 & (n-1)n-2(n-2) & \cdots & 2n-2 \end{pmatrix}$$

We have that

$$\tau(a_1a_2\ldots a_{n-1})\tau(a_na_2a_3\ldots a_{n-1})$$
$$= \begin{pmatrix} 1 & n & 2n-2 & \cdots & (n-1)n-2(n-2) \\ 1 & (n-1)n-2(n-2) & (n-2)n-2(n-3) & \cdots & 2n-2 \end{pmatrix}$$

Thus $\tau(a_1a_2\ldots a_{n-1})$ and $\tau(a_1a_2\ldots a_{n-1}a_na_2\ldots a_{n-1})$ generate D_n. Therefore D_n is a subgroup of syntactic monoid $M(C^*)$. □

Theorem 4.10. For each $n \geq 3$, there is a finite inverse biprefix code C whose syntactic monoid of C^* contains D_n as a subgroup.

Proof. It follows from Proposition 4.8 and Proposition4.9. □

REFERENCES

[1] Hungerford, T.w.Algebra. New York: Springer-Verlag New York, 1974.

[2] Keenan. M and Lallement. G 1974, On certain code admitting inverse semigroup as syntactic monoid. Semigroup Forum 8:312-331.

[3] Lallement. Gerard. Semigroups and combinatorial application. New York: John wilely & Sons, 1979.

[4] Schützenberger, M.P., Un theorie algebrique du codage. C.R. Acad.Sci. Paris 242,862-845;Seminaire Dubreil-Pisot,1956, No.15.

[5] Udomkavanich, P. Inverse semigroup and codes. Doctoral dissertation, Department of Mathematics, Graduate School. The Pennsylvania State University.

VITA

Name : Khajee Jantarakhajorn

Degree : B.Sc.(Mathematics), 1995,

Thammasat University, Bangkok, Thailand.

Position : Instructor, Department of Mathematics and Statistics,

Faculty of Science, Thammasat University, Bangkok, Thailand.

Scholarship : Ministry of University Affairs