Comm. Korean Math. Soc. **11** (1996), No. 1, pp. 191–199

CONJUGATION AND STRONG SHIFT EQUIVALENCE

YOUNG-HWA HA

ABSTRACT. The strong shift equivalence of nonnegative integral square matrices is a necessary and sufficient condition for the topological conjugacy of topological Markov chains. In this paper we study the relation between strong shift equivalence and matrix conjugation.

I. Introduction

Two nonegative integral square matrices A and B are elementary equivalent, denoted by $A \approx_1 B$, if there are nonnegative integral matrices R and S such that $A = RS$ and $B = SR$. The strong shift equivalence is the transitive closure of $\approx_1$, and we denote it by $\approx$. It is well known as Williams' theorem [W][LM] that two subshifts of finite type (two topological Markov chains) are topologically conjugate if and only if their representing transition matrices are strong shift equivalent. There is, however, no simple algorithm to decide strong shift equivalence. Some sufficient conditions for strong shift equivalence of 2×2 matrices have been known [Ba1][Ba2]. In this paper we show certain connection between strong shift equivalence and matrix conjugation with a hope to derive later some other sufficient conditions.

THEOREM. *Let A and B be nonnegative integral square matrices. Then A and B are strong shift equivalent if and only if there exist nonnegative integral square matrices $\bar{A}, \bar{B}, Q_1, Q_2, \cdots, Q_k$ of the same size such that the following properties are satisfied:*

i) *$\bar{A}$ and $\bar{B}$ are extensions of A and B, respectively.*

Received October 18, 1995. Revised November 26, 1995.

1991 AMS Subject Classification: 58F03.

Key words: subshift, topological Markov chain, SFT, strong shift equivalence, topological conjugacy.

Research was partially supported by a grant from Ajou University(1994), GARC-KOSEF, and KOSEF Grant 95-0701-02-01-3.

ii) Q_i *are invertible over* $\mathbb{Z}$ *for* $i = 1, 2, \cdots, k$.
iii) $[(Q_1 \cdots Q_i)^{-1}\bar{A}(Q_1 \cdots Q_i)]Q_i^{-1}$ *is nonnegative for* $i = 1, 2, \cdots, k$.
iv) $(Q_1 \cdots Q_k)^{-1}\bar{A}(Q_1 \cdots Q_k) = \bar{B}$.

This is our main theorem. As a corollary we give a nice necessary condition for strong shift equivalence.

COROLLARY. *If A and B are strong shift equivalent nonnegative integral square matrices, then there exist nonnegative integral square matrices* $\bar{A}, \bar{B}$ *and Q of the same size such that the following properties are satisfied:*

i) $\bar{A}$ *and* $\bar{B}$ *are extensions of A and B, respectively.*
ii) Q *is invertible over* $\mathbb{Z}$.
iii) $Q^{-1}\bar{A}Q = \bar{B}$.

II. Proof of the sufficiency

We first need to define the notion of extensions of a square matrix.

DEFINITION. Let A be a square matrix.

(1) The k-th state of A is *trimmable* if either the k-th row or the k-th column contains only zero entries.
(2) Trimming A at the k-th state means obtaining the submatrix of A by deleting the k-th row and column.
(3) A trimmed submatrix of A is a submatrix of A obtained by trimming A at some trimmable states.
(4) A square matrix B is an *extension* of A if there is a finite sequence $\{C_i\}_{0 \le i \le k}$ of square matrices such that $A = C_0$, $B = C_k$, and C_{i-1} is a trimmed submatrix of C_i for $i = 1, \cdots, k$.

Let A and B be nonnegative integral square matrices. Suppose that B is an extension of A and K is the graph with B as its transition matrix. Then we can find a subgraph H of K with A as its transition matrix. It is now easy to see that the two topological Markov chains X_K and X_H are identical.

We now introduce some notations:

(1) Let A and B be $l \times m$ and $l \times n$ matrices, respectively. Then $[A, B]$ denotes the $l \times (m+n)$ matrix obtained by appending B to the right of A.
(2) Let A and B be $m \times p$ and $n \times p$ matrices, respectively. Then $[A/B]$ denotes the $(m+n) \times p$ matrix obtained by appending B to the bottom of A.
(3) For every matrix A, we denote the number of rows of A and the number of columns of A by $\mathrm{r}(A)$ and $\mathrm{c}(A)$, respectively.

LEMMA 1. *Let A be a nonnegative integral square matrix with a trimmable state. If B is a trimmed submatrix of A trimmed at a single state, then $A \approx_1 B$.*

PROOF. Let A be of $m \times m$, and suppose first that the m-th row of A is zero. Then $A = \big[[B, *]/O\big]$ with O the $1 \times m$ zero matrix. Let $R = [B, *]$ and $S = [I/O]$, where I is the $(m-1) \times (m-1)$ identity matrix. Then $RS = B$ and $SR = A$, and so A and B are elementary equivalent.

If the m-th column of A is zero, then consider the transposes A^t and B^t to find nonnegative integral matrices R_0 and S_0 so that $A^t = S_0 R_0$ and $B^t = R_0 S_0$. Hence $A = RS$ and $B = SR$ with $R = R_0^t, S = S_0^t$.

Now suppose the k-th state of A is trimmable. Let E be the $m \times m$ matrix obtained from the $m \times m$ identity matrix by moving the k-th,$(k+1)$-th,$\cdots$,m-th rows to the m-th,k-th,$(k+1)$-th,$\cdots$,$(m-1)$-th rows, respectively. Then $E^t = E^{-1}$. Observe that the m-th state of EAE^t is trimmable, and B is obtained by trimming EAE^t at the m-th state. Hence there are nonnegative integral matrices S_0 and R_0 such that $EAE^t = R_0 S_0$ and $B = S_0 R_0$. Now, if we put $R = E^t R_0, S = S_0 E$, then we have $A = RS$ and $B = SR$. □

LEMMA 2. *Let A and B be nonnegative integral square matrices. If B is an extension of A, then $A \approx B$.*

PROOF. Choose a finite sequence $\{C_i\}_{0 \le i \le k}$ of nonnegative integral square matrices such that $A = C_0, B = C_k$, and C_{i-1} is obtained by trimming C_i at a single state for $i = 1, \cdots, k$. Then by Lemma 1, $A = C_0 \approx_1 C_1 \approx_1 \cdots \approx_1 C_k = B$. □

We now show the sufficiency of the main theorem. Suppose that A, B, $\bar{A}$, $\bar{B}$, Q_1, Q_2, Q_3, $\cdots$, Q_k satisfy the properties i),ii),iii), and iv) in the main theorem. Then, by Lemma 2, $A \approx \bar{A}$ and $B \approx \bar{B}$. Let $R_i = [(Q_1 \cdots Q_i)^{-1}\bar{A}(Q_1 \cdots Q_i)]Q_i^{-1}, i = 1, \cdots, k$. Then R_i is nonnegative and

$$\begin{aligned}\bar{A} = Q_1R_1 \approx_1 R_1Q_1 = Q_2R_2 \approx_1 \cdots \approx_1 R_{k-1}Q_{k-1} \\ = Q_kR_k \approx_1 R_kQ_k = \bar{B}.\end{aligned}$$

It now follows that $\bar{A} \approx \bar{B}$. Since the strong shift equivalence is transitive, we can conclude $A \approx B$.

III. Proof of the necessity

Suppose that A and D are square matrices, and B and C are rectangular matrices such that $\mathrm{r}(A) = \mathrm{r}(B)$, $\mathrm{c}(B) = \mathrm{c}(D)$, $\mathrm{r}(C) = \mathrm{r}(D)$, and $\mathrm{c}(A) = \mathrm{c}(C)$. We define a square matrix $[A, B; C, D]$ by $[A, B; C, D] = \big[[A, B]/[C, D]\big]$. We say that square matrices $[A_1, A_2; A_3, A_4]$ and $[B_1, B_2; B_3, B_4]$ are *compatible* if each pair of A_k and B_k, $1 \le k \le 4$, have the same size. One can easily see that if two square matrices $[A, B; C, D]$ and $[P, Q; R, S]$ are compatible, then

$$[A, B; C, D][P, Q; R, S] = [AP + BR, AQ + BS; CP + DR, CQ + DS].$$

DEFINITION. Suppose that the matrices I and O in the following statements are the identity and the zero matrices of appropriate size. Let A be a square matrix and S a rectangular matrix.

(1) If $\mathrm{c}(S) \le \mathrm{c}(A)$, then we define square matrices $\alpha(A, S)$ and $\delta(A, S)$ by

$$\alpha(A, S) = [A, O; S_{\mathrm{h}}, O],$$

and

$$\delta(A, S) = [I, S_{\mathrm{h}}; O, A],$$

where $S_{\mathrm{h}} = [O, S]$ such that $\mathrm{c}(S_{\mathrm{h}}) = \mathrm{c}(A)$.

(2) If $\mathrm{r}(S) \le \mathrm{r}(A)$, then we define a square matrix $\beta(A, S)$ and $\gamma(A, S)$ by

$$\beta(A, S) = [O, O; S_{\mathrm{v}}, A],$$

and

$$\gamma(A,S) = [A, S_{\mathrm{v}}; O, I],$$

where $S_{\mathrm{v}} = [S/O]$ such that $\mathrm{r}(S_{\mathrm{v}}) = \mathrm{r}(A)$.

If A is a square matrix and $\mathrm{c}(S) \le \mathrm{c}(A)$ and $\mathrm{r}(T) \le \mathrm{r}(A)$, then $\alpha(A,S)$ and $\beta(A,T)$ are extensions of A. If I and O are the identity and the zero matrices, then $\gamma(I,O)$ and $\delta(I,O)$ are the identity matrices.

Direct computation gives the following results.

LEMMMA 3. *Suppose that A and B are square matrices of the same size, and C and D are rectangular matrices.*

(1) *If $\mathrm{r}(A) = \mathrm{r}(C) = \mathrm{r}(D)$ and $\mathrm{c}(C) = \mathrm{c}(D)$, then*

$$\gamma(A,C)\gamma(B,D) = \gamma(AB, AD + C).$$

(2) *If $\mathrm{r}(A) = \mathrm{r}(C)$, $\mathrm{c}(B) = \mathrm{c}(D)$, and $\mathrm{c}(C) = \mathrm{r}(D)$, then*

$$\gamma(A,C)\alpha(B,D) = \alpha(AB{+}CD, D), \text{ and } \alpha(B,D)\gamma(A,O) = \alpha(BA, DA).$$

(3) *If $\mathrm{c}(A) = \mathrm{c}(C) = \mathrm{c}(D)$ and $\mathrm{r}(C) = \mathrm{r}(D)$, then*

$$\delta(A,C)\delta(B,D) = \delta(AB, CB + D).$$

(4) *If $\mathrm{c}(A) = \mathrm{c}(C)$, $\mathrm{r}(B) = \mathrm{r}(D)$, and $\mathrm{r}(C) = \mathrm{c}(D)$, then*

$$\beta(B,D)\delta(A,C) = \beta(BA{+}DC, D), \text{ and } \delta(A,O)\beta(B,D) = \beta(AB, AD).$$

COROLLARY 4. *Suppose that Q is an invertible matrix and R is a rectangular matrix. Then*

(1) $\gamma(Q,O)^{-1} = \gamma(Q^{-1},O)$, *and* $\gamma(I,R)^{-1} = \gamma(I,-R)$.
(2) $\delta(Q,O)^{-1} = \delta(Q^{-1},O)$, *and* $\delta(I,R)^{-1} = \delta(I,-R)$.

We now define a relation, and derive some results about this relation.

DEFINITION. Let A and B be nonnegative integral square matrices. We write $A \approx_c B$ if there is a nonnegative integral square matrix Q which is invertible over $\mathbb{Z}$ such that i) $Q^{-1}A$ is nonnegative, and ii) $Q^{-1}AQ = B$. In this case we write $A \approx_c B$ *by* Q.

It is obvious that if $A \approx_c B$, then $A \approx_1 B$.

LEMMA 5. *Suppose that A, B, R, and S are nonnegative integral matrices. If $A = RS$ and $B = SR$, then $\alpha(A,S) \approx_c \beta(B,S)$ by $\gamma(I,R)$.*

PROOF. Observe

$$\gamma(I,R)^{-1}\alpha(A,S) = \gamma(I,-R)\alpha(A,S) = \alpha(A - RS, S) = \alpha(O,S),$$

and so

$$\gamma(I,R)^{-1}\alpha(A,S)\gamma(I,R) = \alpha(O,S)\gamma(I,R) = \beta(SR,S) = \beta(B,S).$$

Since $\alpha(O,S)$ is nonnegative, the proof completes. $\square$

LEMMA 6. *Suppose that A, B, Q, and S are nonnegative integral matrices and Q is invertible over $\mathbb{Z}$. If $A \approx_c B$ by Q and $SQ = S$, then $\alpha(A,S) \approx_c \alpha(B,S)$ by $\gamma(Q,O)$.*

PROOF. Observe

$$\gamma(Q,O)^{-1}\alpha(A,S) = \gamma(Q^{-1},O)\alpha(A,S) = \alpha(Q^{-1}A,S),$$

and so

$$\begin{aligned}\gamma(Q,O)^{-1}\alpha(A,S)\gamma(Q,O) &= \alpha(Q^{-1}A,S)\gamma(Q,O)\\ &= \alpha(Q^{-1}AQ,SQ) = \alpha(B,S).\end{aligned}$$

Since $\alpha(Q^{-1}A,S)$ is nonnegative, the proof completes. $\square$

LEMMA 7. *Suppose that A, B, Q, and S are nonnegative integral matrices and Q is invertible over $\mathbb{Z}$. If $A \approx_c B$ by Q and $Q^{-1}S = S$ (or equivalently, $QS = S$), then $\beta(A,S) \approx_c \beta(B,S)$ by $\delta(Q,O)$.*

PROOF. Observe

$$\delta(Q,O)^{-1}\beta(A,S) = \delta(Q^{-1},O)\beta(A,S) = \beta(Q^{-1}A,Q^{-1}S) = \beta(Q^{-1}A,S),$$

and so

$$\begin{aligned}\delta(Q,O)^{-1}\beta(A,S)\delta(Q,O) &= \beta(Q^{-1}A,S)\delta(Q,O)\\ &= \beta(Q^{-1}AQ,S) = \beta(B,S).\end{aligned}$$

Since $\beta(Q^{-1}A,S)$ is nonnegative, the proof completes. $\square$

We need to consider compositions of α and β and compositions of γ and δ. For the sake of simplicity we define the following compound operators.

DEFINITION. Let $\alpha^0(A) = \beta^0(A) = A$, $\alpha^1(A;S) = \alpha(A,S)$, and $\beta^1(A;S) = \beta(A,S)$. For $n > 1$ and $1 \le m < n$ we define

(1) $\alpha^n(A; S_1, \cdots, S_n) = \alpha(\alpha^{n-1}(A; S_1, \cdots, S_{n-1}), S_n)$,

(2) $\beta^n(A; S_1, \cdots, S_n) = \beta(\beta^{n-1}(A; S_1, \cdots, S_{n-1}), S_n)$,

(3) $\alpha^{n-m}\beta^m(A; S_1, \cdots, S_m, S_{m+1}, \cdots, S_n)$
$= \alpha^{n-m}(\beta^m(A; S_1, \cdots, S_m); S_{m+1}, \cdots, S_n)$,

(4) $\beta^{n-m}\alpha^m(A; S_1, \cdots, S_m, S_{m+1}, \cdots, S_n)$
$= \beta^{n-m}(\alpha^m(A; S_1, \cdots, S_m); S_{m+1}, \cdots, S_n)$.

The compound operators $\gamma^n, \delta^n, \gamma^{n-m}\delta^m$, and $\delta^{n-m}\gamma^m$ are defined similarly.

One can easily show that

$$\beta(\alpha(A,S),T) = \alpha(\beta(A,T),S),$$

and

$$\beta^q\alpha^p(A; S_1, \cdots, S_p, T_1, \cdots, T_q) = \alpha^p\beta^q(A; T_1, \cdots, T_q, S_1, \cdots, S_p).$$

THEOREM 8. *If* $A = C_0 = R_0S_0$, $S_0R_0 = C_1 = R_1S_1, \cdots, S_{n-1}R_{n-1} = C_n = R_nS_n$, *and* $S_nR_n = C_{n+1} = B$, *then for* $0 \le k \le n$

$$\beta^k\alpha^{n+1-k}(C_k; S_k, S_{k+1}, \cdots, S_n, S_{k-1}, S_{k-2}, \cdots, S_0) \approx_c \beta^{k+1}\alpha^{n-k}(C_{k+1}; S_{k+1}, S_{k+2}, \cdots, S_n, S_k, S_{k-1}, \cdots, S_0)$$

by $\delta^k\gamma^{n+1-k}(I; R_k, O, \cdots, O)$.

PROOF. We prove the theorem by induction on the number n. The case $n = 0$ corresponds to Lemma 5. Suppose $n > 0$ and assume that the theorem is true for $n - 1$. Then

$$\alpha^n(C_0; S_0, S_1, \cdots, S_{n-1}) \approx_c \beta^1\alpha^{n-1}(C_1; S_1, \cdots, S_{n-1}, S_0)$$

by $\gamma^n(I; R_0, O, \cdots, O)$. Since

$$[O, \cdots, O, S_n]\gamma^n(I; R_0, O, \cdots, O) = [O, \cdots, O, S_n],$$

it follows that

$$\alpha(\alpha^n(C_0; S_0, \cdots, S_{n-1}), S_n) \approx_c \alpha(\beta^1\alpha^{n-1}(C_1; S_1, \cdots, S_{n-1}, S_0), S_n)$$

by $\gamma(\gamma^n(I; R_0, O, \cdots, O), O)$. Therefore,

$$\begin{aligned}\alpha^{n+1}(C_0; S_0, \cdots, S_n) &= \alpha(\alpha^n(C_0; S_0, \cdots, S_{n-1}), S_n)\\ &\approx_c \alpha(\beta^1\alpha^{n-1}(C_1; S_1, \cdots, S_{n-1}, S_0), S_n)\\ &= \beta^1\alpha^n(C_1, S_1, \cdots, S_n, S_0)\end{aligned}$$

by $\gamma^{n+1}(I; R_0, O, \cdots, O)$, and this corresponds to the case $k = 0$ for n. Now suppose $0 < k \leq n$. Then $0 \leq k-1 \leq n-1$, and so if we apply the induction hypothesis for the case $n-1$ and $k-1$ to the chain

$$C_1 = R_1S_1, S_1R_1 = C_2 = R_2S_2, \cdots, S_nR_n = C_n$$

we obtain that

$$\begin{aligned}&\beta^{k-1}\alpha^{n-(k-1)}(C_k; S_k, \cdots, S_n, S_{k-1}, \cdots, S_1)\\ &\quad\approx_c \beta^k\alpha^{n-k}(C_{k+1}; S_{k+1}, \cdots, S_n, S_k, \cdots, S_1)\end{aligned}$$

by $\delta^{k-1}\gamma^{n-(k-1)}(I; R_k, O, \cdots, O)$.

Since

$$\delta^{k-1}\gamma^{n-(k-1)}(I; R_k, O \cdots, O)\begin{bmatrix} S_0 \\ O \\ \vdots \\ O \end{bmatrix} = \begin{bmatrix} S_0 \\ O \\ \vdots \\ O \end{bmatrix},$$

it then follows that

$$\begin{aligned}&\beta(\beta^{k-1}\alpha^{n-(k-1)}(C_k; S_k, \cdots, S_n, S_{k-1}, \cdots, S_1), S_0)\\ &\qquad\approx_c \beta(\beta^k\alpha^{n-k}(C_{k+1}; S_{k+1}, \cdots, S_n, S_k, \cdots, S_1), S_0)\end{aligned}$$

by $\delta(\delta^{k-1}\gamma^{n-(k-1)}(I; R_k, O, \cdots, O), O)$. We now have

$$\begin{aligned}&\beta^k\alpha^{n+1-k}(C_k; S_k, \cdots, S_n, S_{k-1}, \cdots, S_1, S_0)\\ &\quad= \beta(\beta^{k-1}\alpha^{n-(k-1)}(C_k; S_k, \cdots, S_n, S_{k-1}, \cdots, S_1), S_0)\\ &\quad\approx_c \beta(\beta^k\alpha^{n-k}(C_{k+1}; S_{k+1}, \cdots, S_n, S_k, \cdots, S_1), S_0)\\ &\quad= \beta^{k+1}\alpha^{n-k}(C_{k+1}; S_{k+1}, \cdots, S_n, S_k, \cdots, S_0)\end{aligned}$$

by $\delta^k\gamma^{n-k}(I; R_k, O, \cdots, O)$. $\square$

We can now complete the proof of the necessity of the main theorem. Suppose $A \approx B$ and

$$\begin{aligned} A = C_0 = R_0C_0, S_0R_0 = C_1 = R_1S_1, \cdots, S_{n-1}R_{n-1} \\ = C_n = R_nS_n, S_nR_n = C_{n+1} = B. \end{aligned}$$

Let

$$\bar{C}_k = \beta^k\alpha^{n+1-k}(C_k; S_k, S_{k+1}, \cdots, S_n, S_{k-1}, S_{k-2}, \cdots, S_0)$$

for $0 \leq k \leq n+1$, and

$$Q_k = \delta^k\gamma^{n+1-k}(I; R_k, O. \cdots, O)$$

for $0 \leq k \leq n$. Then by Theorem 8, $\bar{C}_k \approx_c \bar{C}_{k+1}$ by Q_k for $0 \leq k \leq n$. Since $\bar{C}_0 = \alpha^{n+1}(A; S_0, S_1, \cdots, S_n)$ and $\bar{C}_{n+1} = \beta^{n+1}(B; S_n, S_{n-1}, \cdots, S_0)$ are extensions of A and B, respectively, the proof is now completed.

References

[Ba1] K. A. Baker, *Strong shift equivalence of 2 by 2 matrices of nonnegative integers*, Ergod. Th. Dynam. Sys. **3** (1983), 501-508.

[Ba2] ———, *Strong shift equivalence and shear adjacency of nonnegative square integer matrices*, Linear Alge. Appl. **93** (1987), 131-147.

[BM] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, Elsevier Science Publ. Co., New York, 1976.

[G] F. R. Gantmacher, *The Theory of Matrices*, Vol. II, Chelsea Publ. Co., New York, 1960.

[LM] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics*, manuscript.

[W] R. F. Williams, *Classification of subshifts of finite type*, Ann. Math. **98** (1973), 120-153; Errata, *ibid.* **99** (1974), 380-381.

Department of Mathematics
Ajou University
Suwon, 442-749, Korea