$R_a R_b$ Transformation of Compound Finite Automata over Commutative Rings

Wang Hao (王 浩)

Institute of Software, The Chinese Academy of Sciences, Beijing 100080

Received February 8, 1996; revised September 4, 1996.

Abstract

Some results on $R_a R_b$ transformation of compound finite automata over finite field are generalized to the case of commutative rings. Properties of $R_a R_b$ transformation are discussed and applied to the inversion problem for compound finite automata.

Keywords: Finite commutative ring with identity, finite automaton, compound finite automaton, $R_a R_b$ transformation method.

1 Introduction

The invertibility theory of finite automata has received continuous attention and found its own wide applications in cryptology, especially in public key cryptosystem. For the linear case over finite fields, the fundamental problem of the theory has been throughoutly solved. The need in cryptography motivates us to generalize the invertibility theory of finite automata over finite fields to the case over finite rings.

Tao Renji[1] and Lu Shuzhi[2] discussed the linear finite automata over finite commutative rings. In this paper, some properties of $R_a R_b$ transformation are described and applied to the invertibility theory for compound finite automata. For notations and terminologies, please refer to [3,4].

Let $R$ be a finite commutative ring with identity. Assume $X$ and $Y$ are free modules over $R$ with dimension $l$ and $m$ respectively. For $c \geq 0$, denote an equation $eq_c(i)$:

$$
\phi_c(y_{i+c}, \ldots, y_{i-k}) + \sum_{j=0}^{h} C_{jc} \psi(x_{i-j}, \ldots, x_{i-j-h'}) = 0 \quad (1)
$$

and an equation $eq'_c(i)$:

$$
\phi'_c(y_{i+c}, \ldots, y_{i-k}) + \sum_{j=0}^{h} C'_{jc} \psi(x_{i-j}, \ldots, x_{i-j-h'}) = 0 \quad (2)
$$

Supported by The National Natural Science Foundation of China.
where $x_j \in X$, $y_j \in Y$ for any integer $j$. Both $\phi_c(y_{i+1}, \ldots, y_{i-k})$ and $\phi'_c(y_{i+c}, \ldots, y_{i-k})$ are vector functions with $m$ components. $\psi(x_{i-j}, \ldots, x_{i-j-h'})$ is a vector function with $L$ components. Both $C'_{jc}$ and $C''_{jc}$ are $m \times L$ matrices over $R$.

If $eq'_c(i)$ is the left multiplication of $eq_c(i)$ in two sides by a nonsingular matrix $P_c$ over $R$, such an $eq'_c(i)$ is called to be obtained from $eq_c(i)$ by using generalized linear $R_a$ transformation, denoted by $eq_c(i) \xrightarrow{R_a[P_c]} eq'_c(i)$. Further, if the last $m - r_c$ rows of $C'_{0c}$ are 0, let $eq_{c+1}(i)$ be the equation \[
\begin{cases}
E'_c eq'_c(i) \\
E''_c eq'_c(i+1)
\end{cases},
\]
where $E'_c$ and $E''_c$ are submatrices of the first $r_c$ rows and of the last $m - r_c$ rows of the $m \times m$ identity matrix $E_m$ respectively, then $eq_{c+1}(i)$ is said to be obtained from $eq'_c(i)$ by using generalized linear $R_b$ transformation, denoted by $eq'_c(i) \xrightarrow{R_b[R_c]} eq_{c+1}(i)$.

Suppose $F$ is a free module over $R$. We will say that vectors $\{v_1, \ldots, v_s\}$ of $F$ are linearly independent\cite{5}, if $\sum_{i=1}^s \lambda_i v_i = 0$ for $\lambda_i \in R$, implying $\lambda_i = 0$ for $i = 1, \ldots, s$.

Let $eq_c(i) \xrightarrow{R_a[P_c]} eq'_c(i) \xrightarrow{R_b[R_c]} eq_{c+1}(i)$ be a generalized linear $R_aR_b$ transformation. If the first $r_c$ rows of $C'_{0c}$ are linearly independent, and the last $m - r_c$ rows are 0, such $R_aR_b$ transformation is called a linear $R_aR_b$ transformation, denoted by $eq_c(i) \xrightarrow{R_a[P_c]} eq'_c(i) \xrightarrow{R_b[R_c]} eq_{c+1}(i)$.

We use $M_{m,n}(R)$ to denote the set of all $m \times n$ matrices over $R$. The maximum number of linearly independent rows of $A \in M_{m,n}(R)$ is called row rank\cite{4} of $A$, denoted by $rr(A)$. Column rank of $A$ can be defined in a similar way, denoted by $cr(A)$.

**Lemma 1.** Let $R$ be a finite commutative ring with identity.

(a) If row rank of $A \in M_{m,n}(R)$ is $m$, we have $m \leq n$.

(b) Suppose $A \in M_{m,n}(R)$, $B \in M_{n,k}(R)$, and $rr(B) = n$, then $rr(AB) = m$ if and only if $rr(A) = m$.

**Proof.** (a) From the definition, we know $rr(A) = m$ if and only if the transposed matrix $A^t$ of $A$ being regarded as a map from $R^m$ to $R^n$, the image of any $v \in R^m$ given by $A^t v$, is injective. Since $R$ is finite, so $m \leq n$.

(b) When $B^t$ regarding as a map is injective, $B^t A^t$ is injective if and only if $A^t$ is injective. So we have the conclusion of (b).

**Lemma 2.** Assume a matrix $A \in M_{m,n}(R)$ can be written as $A = \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix}$.

(a) If the rows of $A_{11}$ are linearly independent, then $rr(A_{22}) = rr(A) - rr(A_{11})$;

(b) If the columns of $A_{22}$ are linearly independent, then $cr(A_{11}) = cr(A) - cr(A_{22})$.

## 2 $R_aR_b$ Transformation over Rings

Throughout this section, $R$ is a finite commutative ring with identity.