On the Semigroup of a Linear Nonsingular Automaton

by

KLAUS H. ECKER

Mathematisches Institut der Universität
Düsseldorf, Germany

ABSTRACT

This paper is concerned with the structure of the semigroup of a linear nonsingular automaton and gives necessary and sufficient conditions for any semigroup to be isomorphic with the semigroup of a linear non-singular subautomaton.

Introduction. Let \( M = (X, S, Y, \delta, \lambda) \) be a finite automaton with the states \( S \), inputs \( X \), outputs \( Y \), and, as usual, the next state function \( \delta: S \times X \rightarrow S \), and the output function \( \lambda: S \times X \rightarrow Y \). By \( X^* \) we mean the set containing all finite sequences of input symbols and the empty word \( \Lambda \). Every element \( x \in X^* \) defines a mapping of \( S \) into \( S \); the monoid generated by these mappings and by the identity mapping is called the semigroup (monoid) of the automaton [2].

A automaton \( M' = (X', S', Y', \delta', \lambda') \) is called subautomaton of the automaton \( M \) if \( S' \subseteq S, X' \subseteq X, Y' \subseteq Y, \) and if \( \delta' \) and \( \lambda' \) are the restrictions of \( \delta \) and \( \lambda \) on \( S' \times X' \).

We consider here linear automata. In this case \( S, X, \) and \( Y \) are vector spaces \( V_n, V_k, V_m \) over a finite field \( GF(p) \) of characteristic \( p \) (\( p \) is a prime number). For each \( (s, x) \in S \times X \), the functions \( \delta \) and \( \lambda \) are given by \( \delta(s, x) = As + Bx, \) and \( \lambda(s, x) = Cs + Dx \); \( A \) is an \( n \times n \) matrix, \( B \) is an \( n \times k \) matrix, \( C \) is an \( m \times n \) matrix, and \( D \) is an \( m \times k \) matrix, with elements from \( GF(p) \). Let \( M = [A, B, C, D] \) be this linear automaton. According to the properties of the characteristic matrix \( A \) we distinguish nonsingular and singular linear automata. In this paper we consider only nonsingular automata; therefore the determinant \( \det A \) of \( A \) is not zero. In this case, as is easily shown, there are powers of \( A \) equal to the unit matrix \( I \). Let \( e \) be the smallest natural number with \( A^e = I \).

If we suppose \( X = \{x_0, \ldots, x_{v-1}\} \) to be a proper subset of \( V_k \), then \( M \) is called a linear subautomaton.

Each input \( x_i \in X \) causes a permutation \( \varphi_i \) on \( S \), \( \varphi_i s = \delta(s, x_i) \). The permutations \( \varphi_0, \ldots, \varphi_{v-1} \) generate a group \( G_1 \), the monoid of \( M \).

In the case \( v = 1 \) (only one input, \( M \) is autonomous) we get a very simple statement ([3]): \( G_1 \) is isomorphic to the cyclic group \( Z_e \) of order \( e \) (\( A^e = I \)) if and only if \( M \) is autonomous, linear, and nonsingular.

In Section 1 we give a few properties of \( G_1 \) (Theorems 1 and 2). In Section
2 we start from a finite group $N_1$ satisfying the hypotheses (P 1–3) (this is essentially the same as Theorems 1 and 2). Then, as will be shown, Theorem 3 holds, and there is always a linear subautomaton with a monoid isomorphic to $N_1$. In Section 3 we give an example and take the dihedral group $D_4$ for $N_1$. A linear subautomaton is constructed, according to the description in Section 2.

By $|T|$ we denote the cardinality of the set $T$.

1. Properties of the Monoid of a Linear Nonsingular Subautomaton. We need the following sets.

**Definition 1.** We define the sets $C_l, C_{-l},$ and $F$ as follows:

$$C_l = \{ \varphi_l \cdots \varphi_i l_1, \cdots, l_i \in \{0, \cdots, v-1\} \},$$

$$C_{-l} = \{ \omega^{-1} \mid \omega \in C_l \}, \quad (i \in \mathbb{N}),$$

and

$$F = \bigcup_l C_l C_{-l},$$

where $C_l C_{-l} = \{ \omega \rho \mid \omega \in C_l, \rho \in C_{-l} \}$. Then we have the following result.

**Lemma 1.** $F$ is an abelian subgroup of $G_1$.

**Proof.** First of all we see that $F \subseteq G_1$. Then we show that $F$ is a group. For each $\mu \in C_l C_{-l}$ there exists an $i'$ with $\mu \in C_{i'}$, because each $\varphi_l^{-1}$ can be written as $\varphi_l$ with a positive exponent. $C_{i'}$ contains the identity $e$, because of

$$\mu = \varphi_l \cdots \varphi_i \varphi_{i'}^{-1} \cdots \varphi_{i-1}^{-1} \in C_{i'} \Rightarrow e = \varphi_{i'} \cdots \varphi_{i} \varphi_{i-1}^{-1} \cdots \varphi_l^{-1} \in C_{i'}.$$ 

Analogously, to $v \in C_j C_{-j}$ there exists an $j'$ with $v \in C_{j'}$. Then we have $\mu v \in C_{i'+j'}$, $e \in C_{i'+}j'$ and $e \in C_{-(i'+j')}$; therefore we get

$$\mu v \in C_{i'+j'} C_{-(i'+j')} \subseteq F.$$ 

As is easily seen, the axioms necessary for $F$ to be a group hold. From

$$\mu s = s - \sum_{i=1}^{v-1} A_{i+1}^{-1} B(x_{k_{i-1}}, x_{k_i}),$$

$\nu$ analogous, we see that $\mu \nu = \nu \mu$, i.e., $F$ is abelian.

**Lemma 2.** $F$ is a normal subgroup of $G_1$.

**Proof.** Let $\varphi \in G_1$. If $\varphi \in F$ we get $\varphi F \varphi^{-1} = F$. If $\varphi \notin F$, $\varphi \in C_l$, $\varphi^{-1} \in C_j$, $\psi \in C_l \cap F$, we have $\epsilon \in C_l$ and $\varphi \psi \varphi^{-1} \in C_{i+j+1}$. Because $\epsilon \in C_{i+j+1}$ and $\epsilon \in C_{-(i+j+1)}$ it follows that

$$\varphi \psi \varphi^{-1} \in C_{i+j+1} C_{-(i+j+1)} \subseteq F.$$ 

Therefore we get $\varphi F \varphi^{-1} = F$ for all $\varphi \in G_1$.

We can get $F$ by an approach different from the above definition. For this purpose we take the permutations

$$\psi_i : = \varphi \varphi_0^{-1} \quad (i = 0, \cdots, v-1).$$

$\psi_0' = e$ is valid for each $\psi_i$; this is easily seen from $\psi \varphi s = s + Bx_{i} - Bx_{0}$. Let

$$G = \langle \psi \mid \psi = \varphi \psi \varphi^{-1}, \varphi \in G_1, i = 1, \cdots, v-1 \rangle.$$