International Journal of Computer and Information Sciences, Vol. 12, No. 5, 1983

A State Space Approach to the Finite Automata[1]

Tony T. Lee[2]

Received November 1982; revised August 1983

This paper proposes a state space approach for analyzing the finite automata. A Ψ-representation transforms a set of words into a formal power series for establishing the state equation of a finite automaton. We investigate the structure of the automaton via its corresponding state equation. It is shown that the solution of the state equation always exists and is unique. Furthermore, we prove that the solution field is a separable algebraic extension of the coefficient field. Finally, the concept of the substitution property of a partition is shown to be equivalent to that of invariant subspaces of the associated state space.

KEY WORDS: Finite automata; state equation; fixed point theorem; valuation; substitution property; invariant subspace; projection.

1. INTRODUCTION

Progress has often been made by transforming one system into another, such that the essential attributes of the transformed system are preserved. A familiar example is the Laplace or Fourier transform that maps a linear system from the time domain into the frequency domain.

The approach of the present work is based upon the transformation of a set of words into a formal power series over the field of integers modulo 2, which is called the Ψ-representation of the set of words. Thus a state equation in some linear space associated with a given automaton can be obtained. A fixed-point theorem of the state equation is then derived. The solution field is shown to be a separable algebraic extension of the coefficient field. The concept of a partition with the substitution property is proved to

[1] This work was performed in Polytechnic Institute of New York.

[2] Present address: Bell Laboratories, Holmdel, New Jersey 07733.

0091-7036/83/1000-0317$03.00/0

828/12/5-1

be equivalent to that of invariant subspaces and projections of the associated state space.

The formal power series over the Boolean ring $\{0, 1\}$ has been used previously by Schützenberger to study automata and formal languages,[5] where the variables in the formal power series are noncommutative. As such, it fails to describe the state space of the finite automata as a vector space over the field, which forms the basic framework of the present approach.

A finite set of symbols $\Sigma = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ is called an alphabet. By a word we mean any finite string of symbols from Σ. The set of all words is denoted by Σ^*, including the empty word (with no symbols) denoted by Λ. If ω_1 and ω_2 are words in Σ^*, then $\omega_1\omega_2$ denotes the words obtained by concatenating the two strings. Therefore, Σ^* together with the binary operation of concatenation forms the free semigroup (with unit Λ) generated by Σ.[9]

A finite automaton is a system defined by the 4-tuple $M = (\Sigma, S, \delta, s_1)$, where S is a finite nonempty set (the internal states of M); δ: $S \times \Sigma \to S$ is a single-valued function, which maps all pairs of states and symbols into the set of states and is called the next-state function; s_1 is a distinguished element of S (the initial state of M).

Let M be an automaton; the function δ can be extended from $S \times \Sigma$ to $S \times \Sigma^*$ in a natural way, as follows:

$$\delta(s, \Lambda) = s, \qquad \text{for} \quad s \in S$$

$$\delta(s, \omega\sigma) = \delta[\delta(s, \omega), \sigma], \qquad \text{for } s \in S, \qquad \omega \in \Sigma^*, \qquad \text{and} \quad \sigma \in \Sigma$$

Let $S = \{s_1, s_2, ..., s_n\}$ be the set of states of an automaton M; the word $\omega \in \Sigma^*$ is said to be accepted by the state $s_i \in S$ if and only if $\delta(s_1, \omega) = s_i$. For an automaton M, an equivalent relation E on the set of words Σ^* is defined as follows[9]:

$$\omega_1 E \omega_2 \quad \text{if and only if} \quad \delta(s_1, \omega_1) = \delta(s_1, \omega_2)$$

This implies that the words ω_1 and ω_2 are in the same equivalence class of E on Σ^* if and only if they are accepted by the same state of M. The collection of all distinct equivalence classes of E in the set Σ^* shall be denoted by $\Pi = \Sigma^*/E$. The quotient set $\Pi = \{\Omega_1, \Omega_2, ..., \Omega_n\}$ is a partition on Σ^*, where $\Omega_i = \{\omega \mid \delta(s_1, \omega) = s_i, \ \omega \in \Sigma^*\}$ is the set of words accepted by the state $s_i \in S$.

Let Σ be an alphabet. By the Gödel numbering of Σ^* we simply mean any one-to-one function μ from Σ^* onto the set N of nonnegative integers.[11] To simplify the discussion, we assume that Σ consists of two symbols 0 and 1 (binary alphabet). Suppose Σ is an arbitrary alphabet; then Σ can be

uniformly encoded by binary words. By a change of notation, if necessary, the theorems remain valid.

DEFINITION 1. Let $\Sigma = \{0, 1\}$. A lexicographical Gödel numbering of Σ is a bijective mapping $\mu\colon \Sigma^* \to N$, defined recursively by

$$\mu(\Lambda) = 0 \tag{1}$$

$$\text{If} \quad \mu(\omega) = n, \quad \text{then} \quad \mu(\omega 0) = 2n + 1, \quad \text{and} \quad \mu(\omega 1) = 2n + 2$$

Let F be the field of integers modulo 2. We employ the following notations.[6]

1. Let $F[x]$ denote the set of all polynomials in the indeterminate x of the form

$$f(x) = \sum_{k=0}^{n} a_k x^k, \qquad \forall a_k \in F$$

It may be verified that $F[x]$ is a ring, which is called the ring of polynomials in the indeterminate x over F.

2. Let $F(x)$ denote the set of all rational functions of the form

$$h(x) = \frac{f(x)}{g(x)}, \qquad f(x), \quad g(x) \in F[x], \qquad g(x) \neq 0$$

$F(x)$ is a field, which is called the field of quotients of $F[x]$.

3. Let $F[[x]]$ be the set of all expressions of the form

$$f(x) = \sum_{k=0}^{\infty} a_k x^k, \qquad \forall a_k \in F$$

$F[[x]]$ is a ring, which is called the ring of the formal power series in the indeterminate x over F.

4. Let $F\langle x\rangle$ be the set of all expressions of the form

$$f(x) = \sum_{k=n}^{\infty} a_k x^k, \qquad \forall a_k \in F$$

with the understanding that, at most, a finite number of the coefficients a_k with k a negative integer are nonzero. $F\langle x\rangle$ is a field, which is called the field of extended formal power series over F. The ring $F[[x]]$ is contained in $F\langle x\rangle$ as a subring.[6]

For any set A, let 2^A denote the collection of all subsets of A, which is called the power set of A. The set of words can be expressed by formal power series via the Ψ-representation defined as follows.

DEFINITION 2. Let $\Sigma = \{0, 1\}$. A mapping Ψ: $2^{\Sigma^*} \to F\langle x\rangle$ defined by

$$\Psi(\Omega) = \sum_{\omega \in \Omega} x^{\mu(\omega)}, \qquad \text{for} \quad \Omega \in 2^{\Sigma^*} \tag{2}$$

is called the Ψ-representation of Ω.

It is known that the range of μ is the set of all nonnegative integers N. The range of Ψ is the ring $F[[x]]$. The mapping Ψ possesses the following properties:

1. $\Psi(\varnothing) = 0$.
2. For $A, B \subseteq \Sigma^*$ and $A \cap B = \varnothing$, then $\Psi(A \cup B) = \Psi(A) + \Psi(B)$.
3. For $f, g \in F\langle x\rangle$, let $f = \sum a_k x^k$ and $g = \sum b_k x^k$. The Hadamard product of f and g is $f \odot g = \sum a_k b_k x^k$. It is easy to verify that $\Psi(A \cap B) = \Psi(A) \odot \Psi(B)$, for $A, B \subseteq \Sigma^*$.
4. Let $\Pi = \{\Omega_1, \Omega_2, \ldots, \Omega_n\}$ be a partition on Σ^*. Then,

$$\begin{aligned} \Psi(\Omega_1) + \Psi(\Omega_2) + \cdots + \Psi(\Omega_n) &= \Psi(\Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_n) \\ &= \Psi(\Sigma^*) \\ &= 1 + x + x^2 + \cdots \\ &= 1/(1 - x) \end{aligned}$$

These properties can be verified directly from the definition of Ψ. The convergence of the infinite series will be discussed in the next section.

A mapping D that maps $F\langle x\rangle$ into itself, defined by $Dz = z^2$ for $z \in F\langle x\rangle$, is an automorphism of $F\langle x\rangle$. Let $L = F\langle x\rangle$ and let L^n denote the corresponding set of n-tuple vectors. The mapping D can be extended to L^n in a natural way, as follows:

$$DZ = [Dz_1, Dz_2, \ldots, Dz_n]', \qquad \text{for} \quad Z \in L^n$$

where prime indicates transposition. Let $A = (a_{ij})$ be a linear transformation of the vector space L^n over L; then $DA = (Da_{ij})$ for $a_{ij} \in L$.

LEMMA 1. *For $\Omega \in 2^{\Sigma^*}$, $\Omega\zeta = \{\omega\zeta \mid \omega \in \Omega\}$ is the set of all words Ω concatenated with ζ. Then*

$$\Psi(\Omega 0) = xDz$$

and

$$\Psi(\Omega 1) = x^2 Dz \tag{3}$$

Proof.

$$\begin{aligned}\Psi(\Omega 0) &= \sum_{\omega \in \Omega 0} x^{\mu(\omega)} = \sum_{\omega \in \Omega} x^{\mu(\omega 0)} \\ &= \sum_{\omega \in \Omega} x^{2\mu(\omega)+1} = \sum_{\omega \in \Omega} x(x^{\mu(\omega)})^2 \\ &= x \sum_{\omega \in \Omega} Dx^{\mu(\omega)} = xD\left(\sum_{\omega \in \Omega} x^{\mu(\omega)}\right) \\ &= xD\Psi(\Omega) = xDz\end{aligned}$$

Similarly, $\Psi(\Omega 1) = x^2 Dz$. In general, we have

$$\Psi(\Omega\zeta) = x^{\mu(\zeta)} D^{l(\zeta)} z, \qquad \text{for} \quad \zeta \in \Sigma^* \tag{4}$$

where $l(\zeta)$ is the length of ζ, and (4) may be verified by mathematical induction on $l(\zeta)$. ∎

Example. For $\Omega \in 2^{\Sigma^*}$, $\zeta = 010$ and $z = \Psi(\Omega)$. Then

$$\begin{aligned}\Psi(\Omega 010) &= xD\Psi(\Omega 01) = xD(x^2 D\Psi(\Omega 0)) = x^5 D^2 \Psi(\Omega 0) \\ &= x^5 D^2 (xD\Psi(\Omega)) = x^9 D^3 \Psi(\Omega) = x^9 D^3 z\end{aligned}$$

where $\mu(010) = 9$ and $l(010) = 3$.

Let $\mathrm{M} = (\Sigma, S, \delta, s_1)$ be an automaton, where $S = \{s_1, s_2, \ldots, s_n\}$ is the set of states. Then the following identities hold:

$$\Omega_1 = \bigcup_{\delta(s_j, \sigma_k) = s_1} \Omega_j \sigma_k \cup \{\Lambda\}$$

and

$$\Omega_i = \bigcup_{\delta(s_j, \sigma_k) = s_i} \Omega_j \sigma^k, \qquad \text{for} \quad i = 2, 3, \ldots, n \tag{5}$$

It is known that the Ω_i's are mutually disjoint. By property (2) of the Ψ-representation, we have

$$z_1 = \sum_{\delta(s_j, \sigma_k) = s_1} x^{\mu(\sigma_k)} Dz_j + 1$$

and

$$z_i = \sum_{\delta(s_j, \sigma_k) = s_i} x^{\mu(\sigma_k)} Dz_j, \qquad \text{for} \quad i = 2, 3, \ldots, n \tag{6}$$

where $z_i = \Psi = (\Omega_i)$. We shall call Eq. (6) the state equation of the automaton M, which can be written in matrix form, $Z = ADZ + b$, such that $Z = [z_1, \ldots, z_n]'$, $b = [1, 0, \ldots, 0]'$. The matrix A is called the transition matrix.

Example. Let $\mathrm{M1} = (\Sigma, S, \delta, s_1)$, where $S = \{s_1, s_2, s_3, s_4\}$. The state table of M1 is given in Table I.

Let Ω_i be the set of words accepted by the state s_i, as shown in Eq. (5). We have

$$\Omega_1 = \Omega_1 0 \cup \Omega_3 0 \cup \{A\}$$
$$\Omega_2 = \Omega_1 1 \cup \Omega_3 1$$
$$\Omega_3 = \Omega_2 0 \cup \Omega_4 0$$
$$\Omega_4 = \Omega_2 1 \cup \Omega_4 1$$

It follows that

$$z_1 = xDz_1 + xDz_3 + 1$$
$$z_2 = x^2 Dz_1 + x^2 Dz_3$$
$$z_3 = xDz_2 + xDz_4$$
$$z_4 = x^2 Dz_2 + x^2 Dz_4$$

where $z_i = \Psi(\Omega_i)$.

We can write the above equations in the matrix form:

$$\begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} x & 0 & x & 0 \\ x^2 & 0 & x^2 & 0 \\ 0 & x & 0 & x \\ 0 & x^2 & 0 & x^2 \end{bmatrix} \begin{bmatrix} Zz_1 \\ Dz_2 \\ Dz_3 \\ Dz_4 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Table I. State Table of Automaton M1

	0	1
s_1	s_1	s_2
s_2	s_3	s_4
s_3	s_1	s_2
s_4	s_3	s_4

It is easy to verify that

$$z_1 = 1 + x + x^3/(1-x^4), \qquad z_2 = x^2 + x^4/(1-x^4)$$
$$z_3 = x^5/(1-x^4), \qquad z_4 = x^6/(1-x^4)$$

is the solution of the state equation.

This example illustrates the procedures for obtaining the state equation by Ψ-representation. It will be shown in the next section that the solution of the state equation always exists and is unique.

2. SOLUTION OF THE STATE EQUATION

The existence and uniqueness of the solution of the state equation are proved in this section. We begin by introducing the concept of valuation and then by means of conventional methods of functional analysis derive a fixed-point theorem, which establishes the proof and also provides the formula for the solution.

A valuation (absolute value) on a field K is a real-valued function $a \to |a|$ defined on K that satisfies the following conditions:

1. $|a| \geqslant 0$ for all $a \in K$ and $|a| = 0$ if and only if $a = 0$.
2. $|ab| = |a|\,|b|$ for all $a, b \in K$.
3. $|a + b| \leqslant |a| + |b|$ for all $a, b \in K$.

A valuation $|\,|$ on K is called non-Archimedean if

$$|a + b| \leqslant \max(|a|, |b|) \qquad \text{for all} \quad a, b \in K$$

Otherwise it is call Archimedean.[1,8] If $a = f(x)/g(x)$ is an arbitrary nonzero element of $F(x)$, we can write

$$a = \frac{f(x)}{g(x)} = x^n \frac{u(x)}{v(x)}$$

where $u(x)$ and $v(x)$ are relatively prime elements of $F[x]$, neither of which is divisible by x. If we set

$$|a|_x = \left|\frac{f(x)}{g(x)}\right|_x = e^n, \qquad |0|_x = 0 \tag{7}$$

where e is a fixed real number and $0 < e < 1$, it is easy to show that $|\,|_x$ is a non-Archimedean valuation on $F(x)$.[8] The valuation $|\,|_x$ can be extended to any $a \in F\langle x\rangle$. Suppose $a = \sum_{k=n}^{\infty} a_k x^k$, $a_n \neq 0$. The extended valuation is defined as $|a|_x = e^n$. A field K is said to be complete with respect to the

valuation $||$ if every Cauchy sequence converges to a limit in K. It can be shown that $F\langle x\rangle$ is the completion (unique up to an isomorphism) of $F(x)$ with respect to the valuation $|\,|_x$.[8]

Let $R=\{X, d\}$ be an arbitrary metric space. A mapping H of the space R into itself is said to be a contraction if there exists a positive real number $\rho<1$ such that $d(Ha, Hb)\leqslant \rho d(a, b)$ for any points $a, b\in X$. Every contraction mapping is continuous. It is known that every contraction mapping defined in a complete metric space R has one and only one fixed point, i.e., the equation $Hy=y$ has only one solution.[2]

Let $L=F\langle x\rangle$ with the valuation $|\,|_x$ and $X=L^n$ be a linear space over L. The mapping $\|\ \|\colon X\to R$ defined by $\|Z\|=\max_i |z_i|_x$ is a norm of the linear space X. Since L is complete with respect to $|\,|_x$, and $X=L^n$ is a finite-dimensional linear space over L with the norm $\|\ \|$, then X is also complete, i.e., X is a Banach space.[2,10] For $Z_1, Z_2\in X$, define

$$d(Z_1, Z_2)=\|Z_1-Z_2\|$$

Clearly, $R=\{X, d\}$ is a complete metrix space.

A closed sphere $S[Z_0, r]$ in the metric space R is the set of all points $Z\in R$ such that $d(Z, Z_0)\leqslant r$. Let $U=\{a\,|\,|a|_x\leqslant 1,\ a\in L\}$. Then for any $Z\in U^n$ we have $d(Z, 0)=\|Z\|=\max_i |z_i|_x\leqslant 1$. Thus, $U^n\subset X$ is closed sphere $S[0, 1]$ in R. It follows that the closed subspace (U^n, d) is also complete.[10]

Let $A\colon X\to X$ be a linear transformation. A norm $\|\ \|$ of A is defined by $\|A\|=\max_{i,j}|a_{ij}|_x$. It is known that for any $Z\in X$, $\|AZ\|\leqslant\|A\|\,\|Z\|$. Suppose $Z=ADZ+b$ is the state equation of an automaton M and $A=(a_{ij})$ is the transition matrix; from the previous section we know that a_{ij} are elements of the maximal ideal of $F[x]$ generated by x.

Therefore

$$\|A\|=\max_{i,j}|a_{ij}|_x\leqslant |x|_x=e<1$$

Theorem 1. Let H be a mapping from U^n into itself defined by $HZ=ADZ+b$. Then H is a contraction mapping. The unique solution of $HZ=ADZ+b=Z$ is given by $Z=[\sum_{i=0}^{\infty}(AD)^i]b$.

Proof. For any $Z, W\in U^n$, we have

$$\begin{aligned} d(HZ, HW)&=\|HZ-HW\|=\|ADZ-ADW\|\\ &\leqslant\|A\|\,\|DZ-DW\|\leqslant e\max_i|z_i^2-w_i^2|_x\\ &=e\max_i|z_i-w_i|_x|z_i+w_i|_x\leqslant e\max_i|z_i-w_i|_x\\ &=ed(Z, W)\end{aligned}$$

Therefore H is a contraction mapping and there is one and only one fixed point in the complete subspace (U^n, d).

Let $Z_0 = 0$. Then

$$Z_1 = HZ_0 = b$$
$$Z_2 = HZ_1 = ADb + b = (I + AD)b$$
$$\cdots$$

and

$$Z_n = HZ_{n-1} = (I + AD + (AD)^2 + \cdots + (AD)^{n-1})b, \qquad \text{for} \quad n \geqslant 1$$

Hence,

$$Z = \lim_{n \to \infty} Z_n = \left(\sum_{i=0}^{\infty} (AD)^i \right) b$$

is the unique fixed point, where $(AD)^0 = I$ and $(AD)^n = AD(AD)^{n-1}$ for $n \geqslant 1$. ∎

Example. Consider the automaton M2 with the state table given in Table II. The state equation of M2 is

$$\begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix} = \begin{bmatrix} 0 & x & 0 & 0 & 0 \\ x & x_2 & 0 & x^2 & 0 \\ 0 & 0 & x & 0 & x^2 \\ 0 & 0 & x^2 & 0 & x \\ x^2 & 0 & 0 & x & 0 \end{bmatrix} \begin{bmatrix} Dz_1 \\ Dz_2 \\ Dz_3 \\ Dz_4 \\ Dz_5 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Table II. State Table of Automaton M2

	0	1
s_1	s_2	s_5
s_2	s_1	s_2
s_3	s_3	s_4
s_4	s_5	s_2
s_5	s_4	s_4

Then,

$$
\begin{aligned}
Z_0 &= (0, 0, \ldots, 0)' \\
Z_1 &= (1, 0, \ldots, 0)' \\
Z_2 &= (1, x, 0, 0, x^2)' \\
Z_3 &= (1 + x^3, x + x^4, x^6, x^5, x^2)' \\
Z_4 &= (1 + x^3 + x^9, x + x^4 + x^7 + x^7 + x^{10} + x^{12}, \\
&\quad x^6 + x^{13}, x^5 + x^{14}, x^2 + x^8 + x^{11})' \\
&\ldots
\end{aligned}
$$

A field L is said to be an extension of field K if L contains K. We may view L as a vector space over K, and say that L is a finite of infinite extension of K accordingly as the dimension of this vector space is finite or infinite. An element ξ of L is said to be algebraic over K if there exists a polynomial $f(x)$ over K such that $f(\xi) = 0$.

Let L be an extension field of K. If $\xi \in L$ is algebraic over K, and $f(z)$ is the irreducible polynomial of ξ such that $f(\xi) = 0 \in K[z]$, then ξ is called inseparable over K if $f'(\xi) = 0$; otherwise, ξ is called separable over K. An algebraic extension field L of K is called separate if every $\xi \in L$ is separable over K; otherwise, L is an inseparable extension of.[6]

It is know that $L = K(\xi_1, \ldots, \xi_n)$ is a separable algebraic extension of the field K if and only if there exist n polynomials $f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n)$ in $K[z_1, \ldots, z_n]$ such that $f_i(\xi_1, \ldots, \xi_n) = 0$ for $i = 1, \ldots, n$, and the Jacobian[6,12]

$$
\det \left[\left(\frac{\partial f_i}{\partial z_j} \right)_{z_k = \xi_k} \right] \neq 0
$$

Let

$$
\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} a_{1,1} \cdots a_{1,n} \\ a_{2,1} \cdots a_{2,n} \\ \cdots \\ a_{n,1} \cdots a_{n,n} \end{bmatrix} \begin{bmatrix} z_1^2 \\ z_2^2 \\ \vdots \\ z_n^2 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{8}
$$

be the state equation of an arbitrary n-state automaton M and let $K = F(x)$; it follows that Eq. (8) is a set of n polynomials $f_i(z_i, \ldots, z_n)$ in $K[z_1, \ldots, z_n]$. It is shown that there is a unique solution $z_1 = \xi_1, \ldots, z_n = \xi_n$ in some extension field of K such that $f_i(\xi_1, \ldots, \xi_n) = 0$ and the Jacobian

$$\operatorname{der}\left[\left(\frac{\partial f_i}{\partial z_j}\right)_{z_k=\xi_k}\right]=1$$

Collecting the above results, we have the following theorem.

Theorem 2. Let $K=F(x)$, and let $Z=(\xi_1,\ldots,\xi_n)'$ be the unique solution of the state equation $Z=ADZ+b$ of an arbitrary n-state automaton M. Then the field $K(\xi_1,\ldots,\xi_n)$ is a separable algebraic extension of K.

3. PROPERTIES OF THE STATE SPACE

In this section we establish the connection between the invariant subspaces of the state space and the substitution property of the partition on the set of states.

A subspace W of a vector space V is invariant under a transformation T if T takes each vector of W into a vector of W; that is, $WT\subset W$. If V is the direct sum of W and Y, so that every z in V may be written uniquely in the form $z=w+y$, with w in W and y in Y, then the projection on W along Y is the transformation E defined by $zE=w$: A linear transformation E is a projection on some subspace if and only if it is idempotent, i.e., $E^2=E$.[3] If a subspace W is invariant under the linear transformation T, then $ETE=ET$ for every projection E on W. Conversely, if $ETE=ET$ for some projection E on W, then W is invariant under T.[3]

A partition π on the set of states of the automaton $M=\{S,\Sigma,\delta,s_1\}$ is said to have the substitution property (S.P. partition) if and only if $s_i\equiv s_j(\pi)$ implies $\delta(s_i,\sigma)\equiv\delta(s_j,\sigma)(\pi)$ for all $\sigma\in\Sigma$.[4] It follows that for each $\sigma\in\Sigma$ and $B\in\pi$, there exists a unique $B'\in\pi$ such that $\delta(B,\sigma)\subseteq B'$, where δ is extended from $S\times\Sigma$ to $\pi\times\Sigma$ such that $\delta(B,\sigma)=\bigcup_{s_i\in B}\delta(S_i,\sigma)$. We can

Table III. State Table of Automaton G

	0	1
1	2	3
2	1	3
3	4	5
4	3	2
5	1	6
6	1	5

Table IV. State Tables of the Image Automaton G_π

	0	1
q_1	q_1	q_2
q_2	q_3	q_4
q_3	q_2	q_1
q_4	q_1	q_4

$q_1 = \{1, 2\}$, $q_2 = \{3\}$
$q_3 = \{4\}$, $q_4 = \{5, 6\}$

think of these blocks as the states of a new M_π automaton defined by π and M, which is called the π-image of M. That is, $M_\pi = \{\pi, \Sigma, \delta_\pi, B_1\}$ with $\delta_\pi(B, \sigma) = B'$ if $\delta(B, \sigma) \subseteq B'$, and $s_1 \in B_1$.[4]

Consider automaton G of Table III. It is easily seen that the partition $\pi = \{\overline{1, 2}; \overline{3}; \overline{4}; \overline{5, 6}\}$ has the substitution property on G. The corresponding automaton G_π is shown in Table IV.

The transition matrix of automaton G is

$$A = \begin{bmatrix} 0 & x & 0 & 0 & x & x \\ x & 0 & 0 & x^2 & 0 & 0 \\ x^2 & x^2 & 0 & x & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & x^2 & 0 & 0 & x_2 \\ 0 & 0 & 0 & 0 & x^2 & 0 \end{bmatrix}$$

Let $\varepsilon_1, \ldots, \varepsilon_6$ be a coordinate system of the vector space $V = L^6$, where $L = F\langle x \rangle$. Then A is a linear transformation on V and we have

$$\varepsilon_1 A = x\varepsilon_2 + x\varepsilon_5 + x\varepsilon_6$$
$$\varepsilon_2 A = x\varepsilon_1 + x^2\varepsilon_4$$
$$\varepsilon_3 A = x^2\varepsilon_1 + x^2\varepsilon_2 + x\varepsilon_4$$
$$\varepsilon_4 A = x\varepsilon_3$$
$$\varepsilon_5 A = x^3\varepsilon_3 + x^2\varepsilon_6$$
$$\varepsilon_6 A = x_2\varepsilon_5$$

Consider the subspace W generated by $\{\varepsilon_1 + \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 + \varepsilon_6\}$; it can be verified that W is an invariant subspace of V, since

$$(\varepsilon_1 + \varepsilon_2)A = x(\varepsilon_1 + \varepsilon_2) + x^2\varepsilon_4 + x(\varepsilon_5 + \varepsilon_6) \in W$$
$$\varepsilon_3 A = x^2(\varepsilon_1 + \varepsilon_2) + x\varepsilon_4 \in W$$
$$\varepsilon_4 A = x\varepsilon_3 \in W$$
$$(\varepsilon_5 + \varepsilon_6)A = x^2\varepsilon_3 + x^2(\varepsilon_5 + \varepsilon_6) \in W$$

Therefore $WA \subset W$, and A restricted on W is given by

$$A \mid W = \begin{bmatrix} x & 0 & x^2 & x \\ x^2 & 0 & x & 0 \\ 0 & x & 0 & 0 \\ 0 & x^2 & 0 & x^2 \end{bmatrix}$$

This is the transition matrix of the π-image automaton G_π of G. Later we will show that this relationship between the partition with the substitution property and the invariant subspace always exists.

Let the set of states S be the set of integers $\{1, 2,..., n\}$ and the set of all partitions of S be $\Pi(S)$. The representation of a partition $\pi = \{B_1, B_2,..., B_m\}$ on the set S is an n-tuple integer array $(a_1, a_2,..., a_n)$ such that for $i \in B_k$, $a_i = \min B_k$, where $\min B_k$ is the smallest element in B_k. Thus the partition $\pi = \{\overline{1, 3, 6}; \overline{2, 5}; \overline{4, 7}\}$ is represented by (1, 2, 1, 4, 2, 1, 4). We may consider the n-tuple $(a_1, a_2,..., a_n)$ as an ordered set of images of a mapping f: $S \to S$ such that $(a_1, a_2,..., a_n) = (f(1), f(2),..., f(n))$. It is easy to verify that a mapping f that represents a partition on S should satisfy the following criteria:

1. Contraction: $f(i) \leqslant i$ for $1 \leqslant i \leqslant n$.
2. Idempotent: $f^2(i) = f(i)$ for $1 \leqslant i \leqslant n$.

The set of all mappings from S into itself that satisfy the criteria 1 and 2 will be denoted by $R(S)$, and there is a one-to-one and onto correspondence between $\Pi(S)$ and $R(S)$.[7]

Let V be an arbitrary n-dimensional vector space. We will show that for every partition π on the set S of n elements, there is a projection E on V induced by π.

Lemma 2. Let π be a partition on $S = \{1, 2,..., n\}$, and let f be the representation function of π. The $n \times n$ matrix $E = (e_{ij})$, such that

$$e_{ij} = \begin{cases} 1, & \text{if } f(j) \neq i \\ 0, & \text{if } f(j) \neq i \end{cases}$$

is a projection on any n-dimensional vector space V.

Proof. We want to prove $E^2 = E$. Letting $E^2 = (m_{ij}) = (\sum_{k=1}^{n} e_{ik} e_{kj})$, we have to show that $m_{ij} = \sum_{k=1}^{n} e_{ik} e_{kj} = e_{ij}$. For each column of E, there is one and only one element equal to 1; all other elements are equal to 0. Therefore, if $m_{ij} = 1$, there is some p, $1 \leqslant p \leqslant n$, such that $e_{ip} = e_{pj} = 1$. Then $f(p) = i$ and $f(j) = p$, which implies $f^2(j) = f(p) = i$. By the idempotent property of f, we have $f(j) = i$, and $e_{ij} = 1$. Conversely, if $e_{ij} = 1$, then $f(j) = i$. Hence, $f(i) = f^2(j) = f(j) = i$, and therefore $e_{ii} = 1$. It follows that $m_{ij} = \sum_{k=1}^{n} e_{ik} e_{kj} = e_{ii} e_{ij} = e_{ij} = 1$. Therefore $E^2 = E$. ∎

Theorem 3. Let $\mathrm{M} = \{S, \Sigma, \delta, s_1\}$ be a given automaton and A be the transition matrix of M. Let π be a S.P. partition of M, and E the projection induced by π. Then $EAE = EA$.

Proof. The transition matrix A can be expressed by a matrix polynomail $A = xT_0 + x^2 T_1$, where T_0 and T_1 can be defined as follows:

$$T_0 = (\alpha_{ij}) \qquad \text{such that} \quad \alpha_{ij} = \begin{cases} 1 & \text{if } \delta(j, 0) = i \\ 0 & \text{if } \delta(j, 0) \neq i \end{cases}$$

and

$$T_1 = (\beta_{ij}) \qquad \text{such that} \quad \beta_{ij} = \begin{cases} 1 & \text{if } \delta(j, 1) = i \\ 0 & \text{if } \delta(j, 1) \neq i \end{cases}$$

In order to show that $EAE = EA$, we must prove that $ET_0E = ET_0$ and $ET_1ET = ET_1$. It should be noted that for each column of T_0 and T_1 only one element is equal to 1 and all the other elements are equal to 0. Let $ET_0E = (q_{ij})$ and $ET_0 = (p_{ij})$. Since $q_{ij} = \sum_{k=1}^{n} e_{ik} (\sum_{l=1}^{n} \alpha_{kl} e_{li})$, we assume that

$$f(j) = l \tag{10}$$

and

$$\delta(l, 0) = k \tag{11}$$

Then

$$q_{ij} = e_{ik} \tag{12}$$

where f is the representation of π defined as above.

If we assume

$$\delta(j, 0) = m \tag{13}$$

then $\alpha_{mj} = 1$ and

$$p_{ij} = \sum_{k=1}^{n} e_{ik}\alpha_{kj} = e_{im} \tag{14}$$

Since Eq. (10) implies that $j = l(\pi)$, it follows that $\delta(l, 0) = \delta(j, 0)(\pi)$. Hence, if from Eqs. (11) and (13) we know $k = m(\pi)$, then $f(k) = f(m)$, and it follows that $e_{ik} = e_{im}$. From Eqs. (12), (14), and (15), we have $q_{ij} = p_{ij}$. Therefore $ET_0E = ET_0$. Similarly, we can show that $ET_1E = ET_1$. Hence, $EAE = EA$. ∎

Example. Automaton M3 and its S.P. partition lattice are given in Tables V and VI, respectively.

The transition matrix of automaton M3 is

$$A = \begin{bmatrix} 0 & x & 0 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & x^2 & 0 \\ x_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x^2 & x & 0 \\ 0 & 0 & x^2 & x^2 & 0 & 0 & x \\ 0 & x^2 & x & x & 0 & 0 & x^2 \\ 0 & 0 & 0 & 0 & x & 0 & 0 \end{bmatrix}$$

The representations of the S.P. partitions are

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 1 & 1 & 1 & 2 & 2 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 3 & 2 & 2 & 1 \end{pmatrix} \qquad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 3 & 3 & 1 & 3 & 1 \end{pmatrix}$$

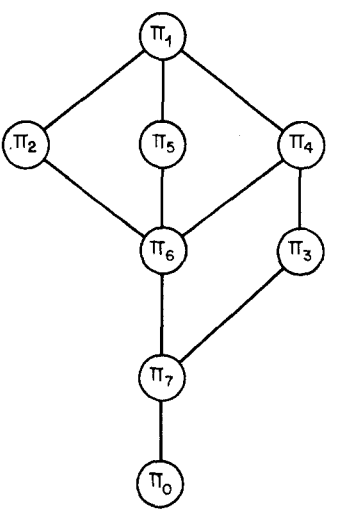
$$f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 2 & 2 & 1 & 1 & 2 \end{pmatrix} \qquad f_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 3 & 1 & 6 & 2 \end{pmatrix}$$

$$f_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 3 & 5 & 6 & 7 \end{pmatrix} \qquad f_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Table V. State Table of Automaton M3

	0	1
1	2	3
2	1	6
3	6	5
4	6	5
5	7	4
6	4	2
7	5	6

Table VI. S.P. Partitions of Automaton M3 and Its Lattice



$\pi_1 = \{\overline{1, 2, 3, 4, 5, 6, 7}\}$

$\pi_2 = \{\overline{1, 3, 4, 5}; \overline{2, 6, 7}\}$

$\pi_3 = \{\overline{1, 7}; \overline{2, 5}; \overline{3, 4, 6}\}$

$\pi_4 = \{\overline{1, 2, 5, 7}; \overline{3, 4, 6}\}$

$\pi_5 = \{\overline{1, 5, 6}; \overline{2, 3, 3, 7}\}$

$\pi_6 = \{\overline{1, 5}; \overline{2, 7}; \overline{3, 4}; \overline{6}\}$

$\pi_7 = \{\overline{1}; \overline{2}; \overline{3, 4}; \overline{5}; \overline{6}; \overline{7}\}$

$\pi_0 = \{\overline{1}; \overline{2}; \overline{3}; \overline{4}; \overline{5}; \overline{6}; \overline{7}\}$

Consider the projection E_6 induced by π_6

$$E_6 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

It is easy to verify that $E_6^2 = E_6$ and $E_6 A E_6 = E_6 A$. Suppose $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7\}$ is a basis of the vector space $V = L^7$. The set of vectors $\{\varepsilon_1 + \varepsilon_5,\ \varepsilon_2 + \varepsilon_7,\ \varepsilon_3 + \varepsilon_4, \varepsilon_6\}$ generates the range of E_6, which is a subspace of V, denoted by W. From Theorem 3, we know that W is invariant under the transition matrix A of M, i.e., $WA \subset W$, and this is illustrated as follows:

$$\begin{aligned} (\varepsilon_1 + \varepsilon_5)A &= x(\varepsilon_2 + \varepsilon_7) + x^2(\varepsilon_3 + \varepsilon_4) \\ (\varepsilon_2 + \varepsilon_5)A &= x(\varepsilon_1 + \varepsilon_5) + x^2\varepsilon_5 \\ (\varepsilon_3 + \varepsilon_4)A &= x^2(\varepsilon_1 + \varepsilon_5) + \varepsilon_6 \\ \varepsilon_6 A &= x^2(\varepsilon_2 + \varepsilon_7) + x(\varepsilon_3 + \varepsilon_4) \end{aligned}$$

The matrix A restricted on W is

$$A \mid W = \begin{bmatrix} 0 & x & x^2 & 0 \\ x & 0 & 0 & x^2 \\ x^2 & 0 & 0 & x \\ 0 & x_2 & x & 0 \end{bmatrix}$$

The π_6-image automaton $\mathrm{M3}_{\pi_6}$ is shown in Table VII. It is easy to see that the transition matrix of $\mathrm{M3}_{\pi_6}$ is identical to $A \mid W$. Therefore, the state space of the π_6-image automaton $\mathrm{M3}_{\pi_6}$ is an invariant subspace of the state space of automaton M3 with respect to the transition matrix A of M3. We have the following theorem.

Theorem 4. Let M be a finite-state automaton, and π a S.P. partition on M. The state space W of the π-image automaton M_π is an invariant subspace of the state space V of M with respect to the transition matrix A of M restricted on W, i.e., $A_\pi = A \mid W$.

Table VII. State Table of Automaton $M3_{\pi_6}$

	0	1
B_1	B_2	B_3
B_2	B_1	B_4
B_3	B_4	B_1
B_4	B_3	B_2

$B_1 = \{1, 5\}$, $B_2 = \{2, 7\}$
$B_3 = \{3, 4\}$, $B_4 = \{6\}$

From the discussion above, we know that for each S.P. partition there is a corresponding projection and an invariant subspace of the state space, which shows that these concepts are equivalent.

4. CONCLUSION

We have investigated the structure o finite automata based on the state equation obtained via the Ψ-representation. The state space of the automaton is a finite-dimensional vector space over the field of extended formal power series with coefficients that lie in the $\{0, 1\}$ field of integers modulo 2. This is different from that the formal power series used by Schützenberger,[5] where the coefficients lie in the $\{0, 1\}$ Boolean ring and the variables are noncommutative. Because the equation is based on a commutative field, we can show that the solution is separable algebraic over the coefficient field. We have also proved that the concept of substitution property of partition is equivalent to an invariant subspace of the associated state space. This suggests that it should be possible to study the decomposition of finite automata in parallel with the decomposition of vector space and linear transformations.

ACKNOWLEDGMENTS

The author wishes to thank Prof. Edward J. Smith of Polytechnic Institute of New York, who supervised this work, for his help and guidance. Special thanks are also due to the referees for their helpful comments. The author is grateful to Dr. M. Eisenberg, Bell Laboratories, Holmdel, New Jersey, for his valuable suggestions.

REFERENCES

1. E. Artin, *Algebraic Numbers and Algebraic Functions*, New York University, New York (1951).
2. G. Bachman and L. Narici, *Functional Analysis*, Academic Press, New York (1966).
3. P. R. Halmos, *Fnite-Dimensional Vector Space*, 2nd ed., D. VanNostrand, Princeton, New Jersey (1958).
4. J. Hartmanis and R. E. Stearns, *Algebraic Structure Theory of Sequential Machines*, Prentice-Hall, Englewood Cliffs, New Jersey (1966).
5. G. Lallement, *Semigroups and Combinatorial Applications*, John Wiley & Sons, New York (1979).
6. S. Lang, *Algebra*, Addison-Wesley, Reading Massachusetts (1965).
7. T. T. Lee, Order-preserving representations of the partitions on the finite set, *J. Combinatorial Theory* **SE-A31**(2):136–145 (September 1981).
8. P. J. McCarthy, *Algebraic Extensions of Fields*, Chelsea Publishing Company, Chelsea, New York, (1976).
9. M. O. Rabin and D. Scott, *Finite automata and their decision problems*, *IBM J. Res. Dev.* **3**:114–125 (1959).
10. H. L. Royden, *Real Analysis*, Macmillan, New York (1963).
11. R. M. Smullyan, *Theory of Formal Systems*, Princeton University Press, Princeton, New Jersey (1961).
12. O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, D. VanNostrand, Princeton, New Jersey (1958).