Internat. J. Math. & Math. Sci.
VOL. 11 NO. 2 (1988) 355-364

ON RATIONAL SOLUTION OF THE STATE EQUATION OF A FINITE AUTOMATON

R. CHAUDHURI and H. HÖFT

Department of Computer Science
Eastern Michigan University
Ypsilanti, MI 48197

(Received January 21, 1987 and in revised form June 25, 1987)

ABSTRACT. We prove that the necessary and sufficient condition for the state equation of a finite automaton M to have a rational solution is that the lexicographical Gödel numbers of the strings belonging to each of the end-sets of M form an ultimately periodic set. A method of determining the existence of a rational solution of the state equation is also given.

KEY WORDS AND PHRASES. Automata, state equation, GF(2), rational solutions.
1980 AMS SUBJECT CLASSIFICATION CODE. 03D05.

1. INTRODUCTION.

In this paper we contribute some interesting results on the state space approach to finite automata following the work of Lee [2], Yang and Huang [1].

A state space approach was proposed by Lee [2] as an alternative way to analyze finite automata. The approach is based on the transformation of a set of words into a formal power series over the field of integers modulo 2 and also on obtaining a state equation in some linear space associated with an automation. Some useful algorithms associated with the state space approach were discussed by Yang and Huang [1] along with a condition for the state equation to have a rational solution when the automaton has 2^k states (k = 2,3).

The question of existence of a rational solution of the state equation is certainly an interesting one and it is not difficult to see that the condition given by Yang and Huang [1] is by no means necessary even for automata with 4 states only.

One of the main objectives of our present work is to give the necessary and sufficient condition for the state equation of an automaton to have a rational solution and thus providing a complete answer to the question left open by Yang and Huang [1]. We also show that the condition obtained in [1] is a special case of our theorem.

Furthermore, we discuss a practical method for determining whether the state equation of an automaton has a rational solution in case it exists. Since there is no known algebraic method for solving state equations in general, our method is useful for obtaining the closed form solution (i.e. rational solution) whenever it exists.

2. PRELIMINARIES.

Some basic definitions and results necessary for our work are treated very concisely in the following. The reader may refer to our references for a detailed discussion.

DEFINITION 1. A finite automaton (deterministic) is a 4-tuple $M = (Q,\Sigma,\delta,q_1)$, where

i) Q is a finite non-empty set of states,

ii) Σ is a finite non-empty set of inputs,

iii) δ is a function from $Q\times\Sigma$ to Q, called the transition function and

iv) q_1 is the initial state.

Let Σ^* denote the set of all possible strings consisting of symbols from Σ alongwith the empty string Λ. It is well-known that the transition function δ can be extended from $Q \times \Sigma$ to $Q \times \Sigma^*$ as

$$\delta(q_i,\Lambda) = q_i$$

and $$\delta(Q_i,w\sigma) = \delta(\delta(q_i,w),\sigma)$$

where $q_i \in Q$ and $\Lambda,w,\sigma \in \Sigma^*$.

DEFINITION 2. The end-set $E(q)$ of a state $q \in Q$ is defined as

$$E(q) = \{w \in \Sigma^* \mid \delta(q_1,w) = q \} .$$

Note that $\Lambda \in E(q_1)$ and $\bigcup_{q\in Q} E(q) = \Sigma^*$. Also, for $q_i,q_j \in Q$ we have $E(q_i) \cap E(q_j) = \emptyset$ iff $i \neq j$. In the following, without any loss of generality, we restrict ourselves to the binary alphabet $\Sigma = \{0,1\}$. Also, N denotes the set of non-negative integers. Throughout the paper we will use a specific enumeration $\mu : \Sigma^* \to N$ of the strings over $\{0,1\}$ which is based on the lexicographic ordering of Σ^*. We define $\mu(\Lambda) = 0$ and for $w \in \Sigma^*$ with $\mu(w) = n$, $\mu(w.0) = 2n+1$ and $\mu(w.1) = 2n+2$. The function μ is called a lexicographic Gödel numbering of Σ^*. Furthermore, let F denote the field of integers modulo 2, also denoted by $GF(2)$.

DEFINITION 3. The field of extended formal power series over F, denoted by $F\langle x\rangle$, is the set of all expression of the form

$$f(x) = \sum_{k=1}^{\infty} a_k x^k \ , \ a_k \in F \quad \text{and} \quad i \in N \ \text{ or } \ -N$$

containing at most a finite number of non-zero coefficients a_k such that k is negative.

DEFINITION 4. Let $M = (Q,\Sigma,\delta,q_1)$ be a finite automaton. For $q \in Q$, the representation

$$\Psi(E(q)) = \sum_{w\in E(q)} x^{\mu(w)}$$

is called the Ψ-representation of the end-set $E(q)$.

It was noted in [1,2] that the mapping $D : F\langle x\rangle \to F\langle x\rangle$ defined by $Dz = z^2$, for $z \in F\langle x\rangle$, is a homomorphism of $F\langle x\rangle$. Also, if $z = (z_1,z_2,\ldots,z_n)'$ is an element of $(F\langle x\rangle)^n$, then the mapping D can naturally be extended as

$$Dz = (Dz_1, Dz_2, \ldots, Dz_n)'$$

where "'" denotes transposition.

Let $Q = \{q_1, q_2, \ldots, q_n\}$ be the states of a finite automaton. Let $E_i = E(q_i)$ and $z_i = \Psi(E_i)$. Then it is known that [1,2]

$$z_1 = \sum_{\delta(q_j,\sigma_k)=q_1} x^{\mu(\sigma_k)} Dz_j + 1$$

and

$$z_i = \sum_{\delta(q_j,\sigma_k)=q_i} x^{\mu(\sigma_k)} Dz_j \quad , \; i = 2,3,\ldots,n.$$

where $\sigma_k \in \Sigma$. The above equations can be written in the matrix form as

$$Z = ADZ + b$$

where $Z = (z_1, z_2, \ldots, z_n)'$ and $b = (1,0,\ldots,0)'$.

DEFINITION 5. The matrix A is called the transition matrix of the automaton and the equation $Z = ADZ + b$ is called the state equation of the automaton.

Note that the matrix A is a square matrix of size n, where $n = |Q|$ = the cardinality of the set Q. The possible non-zero elements of A are x, x^2 and $x+x^2$ and it is easy to see that

$$A_{ij} = x \quad , \text{ if } \quad \delta(q_j,0) = q_i$$

$$= x^2 \quad , \text{ if } \quad \delta(q_j,1) = q_i$$

$$= x+x^2 \quad , \text{ if } \quad \delta(q_j,0) = \delta(q_j,1) = q_i$$

$$= 0 \quad , \text{ if there is not transition from } q_j \text{ to } q_i \text{ on either input.}$$

By virtue of the deterministic nature of M, the sum of the non-zero elements in each column of A is $x+x^2$.

Lee [2] showed that the solution of a state equation always exists and is unique. In particular, the solution is $Z = (z_1, z_2, \ldots, z_n)'$ where $z_i = \Psi(E_i)$, $E_i = E(q_i)$ being the end-set of the state q_i. For details regarding the existence of the solution, which happens to be the fixed point of the equation $f(Z) = ADZ + b$, the reader is referred to [2]. We note that for each i, z_i is a formal power series and that

$$\sum_{i=1}^{n} z_i = \frac{1}{(1+x)} \quad \text{and} \quad \sum_{i=1}^{n} z_i^2 = \frac{1}{(1+x^2)} \quad .$$

It is interesting to note that sometimes the formal power series representation for each z_i can be expressed in the form of a rational function. In such a case, we say that the state equation has a rational solution.

The question of existence of a rational solution of a state equation was originally raised by Yang and Huang [1]. A condition for the existence was obtained for automata with 4 or 8 states (more generally, for automata with $n=2^k$ states). The

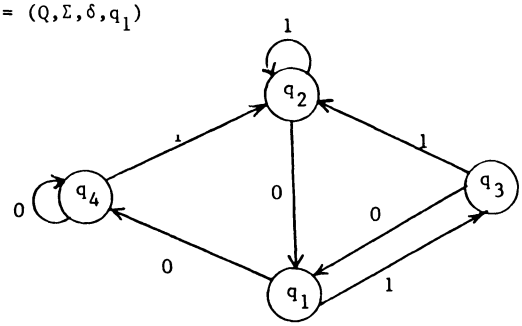
condition imposes a particular block structure on the transition matrix A of the automaton. In the following, we obtain a necessary and sufficient condition for the state equation of a finite automaton to have a rational solution. We also show that the sufficient condition obtained in [1] is only a particular situation of our theorem. We also discuss, given an arbitrary finite automaton how to determine whether the corresponding state equation has a rational solution or not.

3. MAIN RESULTS.

We begin this section with examples of finite automata whose state equations have rational solutions but the sufficient conditions given in [1] do not hold.

EXAMPLE 1. Consider the automaton $M = (Q,\Sigma,\delta,q_1)$

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



whose transition matrix is

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

Obviously, the matrix A violates part 1 and consequently violates part 2 of the sufficient condition in Theorem 2 of [1]. Let $Z = (z_1,z_2,z_3,z_4)$ be the unique solution of the state equation. The solution satisfies the state equation (written explicitly)

$$z_1 = x(z_2^2+z_3^2) + 1$$
$$z_2 = x^2(z_2^2+z_3^2+z_4^2)$$
$$z_3 = x^2 z_1^2$$
$$z_4 = x(z_1^2+z_4^2)$$

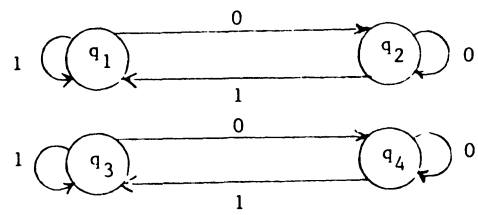
and is rational in nature and has the following form viz.

$$z_1 = 1 + x + \frac{x}{(1+x^4)} \quad , \qquad z_2 = 1 + x^2 + x^4 + \frac{1+x^2+x^6}{(1+x^8)}$$

$$z_3 = x^2 + x^4 + \frac{x^4}{(1+x^8)} \quad , \qquad z_4 = x + \frac{x^3}{(1+x^4)}$$

EXAMPLE 2. Consider the automaton $M = (Q, \Sigma, \delta, q_1)$

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



whose transition matrix is

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

Thus the matrix A satisfies part 1 but violates part 2 of the sufficient conditions given in [1]. The state equation is given by the system

$$z_1 = x^2(z_1^2+z_2^2) + 1$$

$$z_2 = x\,(z_1^2+z_2^2)$$

$$z_3 = x^2(z_3^2+z_4^2)$$

$$z_4 = z\,(z_3^2+z_4^2)$$

This system splits into the homogeneous part of z_3 and z_4 whose associated states q_3 and q_4 are unreachable and which has trivial solution $z_3 = z_4 = 0$, and into the non-homogeneous part of z_1 and z_2 whose solutions have the rational values

$$z_1 = \frac{1}{1 + x^2}$$

$$z_2 = \frac{x}{1 + x^2} \quad .$$

In the following, we will see that the reason why the state equation of the above automaton has a rational solution is that the Gödel numbers of the strings belonging to each of the end-sets of the four states form an ultimately periodic set. First, we have the definition of an ultimately periodic set.

DEFINITION 6. A set X of natural numbers is said to be ultimately periodic if X is finite or if there exist two integers $k_0 \geq 0$ and $p > 0$ such that if $x \geq k_0$ then $x \in X$ if and only if $x + p \in X$.

We say that p is a period of the (infinite) set X. Note that a set X of period p has also period k.p, for any $k \in N^+$. However, in the following we only consider the smallest p for any set X.

In order to prove our main theorem, we need the following Lemma.

LEMMA. Let f(x) be a polynomial with coefficients in GF(2) such that x does not divide f(x). Then there exists an integer k such that f(x) divides $(1 + X^k)$.

For a proof of the above lemma, we refer the reader to Van der Waerden [4]. Some applications of the above lemma in the theory of linear sequential machines can be found in Harrison [3]. We are now ready to prove our main result.

THEOREM 1. Let $M = (Q,\Sigma,\delta,q_1)$ be a finite automaton. A necessary and sufficient condition for the state equation of M to have a rational solution is that the Gödel numbers of the strings in each of the end-sets of the states of M form an ultimately periodic set.

PROOF. Fix $q_i \in Q$ and consider the Gödel numbers of the strings in the end-set $E_i = E(q_i)$. Let $M_i = \{n_1,n_2,\ldots\}$ be the set consisting of the Gödel numbers of the strings in $E_i = \{x_1,x_2,\ldots\}$. Hence, $n_k = \mu(x_k)$ and without any loss of generality we may assume that $n_k < n_{k+1}$ for each k. If M_i is finite, then $Z_i = \Psi(E_i)$ is a rational solution. If M_i is infinite and ultimately periodic with period $p > 0$, then there exists an integer k_0 such that for all $k \geq k_0$, $n_k+p \in M_i$ exactly when $n_k \in M_i$. Let $\{n_{k_0},n_{k_1},\ldots,n_{k_r}\}$ be the set of consecutive integers belonging to M_i such that $n_{k_0} < n_{k_1} < \ldots < n_{k_r} < n_{k_0} + p$. Then it follows that

$$z_i = \Psi(E_i) = x^{n_1} + x^{n_2} + \ldots + x^{n_{k_0-1}} + \frac{x^{n_{k_0}} + x^{n_{k_1}} + \ldots + x^{n_{k_r}}}{1 + x^p}$$

observing that the formal power series $1 + x^p + x^{2p} + \ldots$ is represented by $\frac{1}{1+x^p}$. Clearly, each z_i has a rational function representation.

Conversely, assume that $Z = (z_1,z_2,\ldots,z_n)'$ is a rational solution of the state equation of a finite automaton. Then we can write each z_i as

$$z_i = e_i(x) \qquad \text{or} \qquad z_i = e_i(x) + \frac{f_i(x)}{g_i(x)}$$

where $e_i(x)$, $f_i(x)$ and $g_i(x)$ are formal polynomials with coefficients in GF(2), $0 \leq \deg(f_i(x)) < \deg(g_i(x))$ and the rational function $f_1(x)/g_i(x)$ is in its lowest terms.

In the first case, the end-set $E(q_i)$ is finite so that its associated set of Gödel numbers is periodic. For the second case, we claim that $g_i(x)$ must be of the form $1 + h_i(x)$, where $h_i(x)$ is divisible by x.

To see this, assume on the contrary that $g_i(x) = x^m(1 + h_i(x))$, $m > 0$. Since $f_i(x)$ and $g_i(x)$ are relatively prime, we can write $f_i(x) = 1 + r_i(x)$ where $r_i(x)$ is divisible by x. Let k be the smallest integer such that $1 + h_i(x)$ divides $1 + x^k$ as given by the lemma. Then we can write

$$z_i = e_i(x) + \frac{(1+r_i(x))(1+s_i(x))}{x^m(1+x^k)}$$

where $1+x^k = (1+s_i(x))(1+h_i(x))$. This implies that the formal power series representation of z_i contains the term $1/x^m$, which is a contradiction for $m > 0$. Hence $m = 0$ and therefore

$$z_i = e_i(x) + \frac{f_i(x)}{1+h_i(x)} = e_i(x) + \frac{t_i(x)}{1+x^k}$$

and $\deg(t_i(x)) < k$. Since $t_i(x)$ is a polynomial over GF(2), it follows that the Gödel numbers of the strings belonging to the end-set of the state q_i form a periodic (ultimately) set with period k. This completes our proof.

Next, we proceed to show that the sufficient conditions of [1] imply that Gödel numbers of the strings belonging to each of the end-sets form a periodic set. As before, we let $\Sigma = \{0,1\}$.

Let $M = (Q,\Sigma,\delta,q_1)$ be a finite automaton. Define

$$C_o = \{q \in Q \mid \delta(q',0) = q \text{ for some } q' \in Q\}$$

and

$$C_1 = \{q \in Q \mid \delta(q',1) = q \text{ for some } q' \in Q\}.$$

Note that, in general C_0 and C_1 need not be disjoint. The following theorem generalizes the sufficient conditions of [1] in the case when the automaton has 4 states.

THEOREM 2. Let $M = (Q,\Sigma,\delta,q_1)$ be a 4-state automaton. Let C_0 and C_1 be as defined above such that the conditions $|C_0| = |C_1| = 2$, $C_0 \cup C_1 = Q$ hold. Furthermore, assume that the state equation has the form

$$z_{i_1} = d_{1i_1} + x \sum_{q_k \in C_0} z_k^2 \quad \text{and} \quad z_{i_2} = d_{1i_2} + x \sum_{q_k \in C_1} z_k^2 \quad \text{if } C_0 = \{q_{i_1}, q_{i_2}\} \text{ and}$$

$$z_{j_1} = d_{1j_1} + x^2 \sum_{q_k \in C_0} z_k^2 \quad \text{and} \quad z_{j_2} = d_{1j_2} + x^2 \sum_{q_k \in C_1} z_k^2 \quad \text{if } C_1 = \{q_{j_1}, q_{j_2}\}$$

where d_{1i} is a constant equal to 1 iff i=1 and 0 otherwise. Then the state equation of M has a rational solution.

PROOF. Since $\sum_{i=1}^{4} z_i^2 = \frac{1}{1+x^2}$, we have

$$\sum_{q_i \in C_0} z_i = 1 + \frac{x}{1+x^2} \text{ or } \frac{x}{1+x^2} \text{ depending on whether } q_1 \in C_0 \text{ or not and}$$

$$\sum_{q_i \in C_1} z_i = 1 + \frac{x^2}{1+x^2} \text{ or } \frac{x^2}{1+x^2} \text{ depending on whether } q_1 \in C_1 \text{ or not, } q_1 \text{ being}$$

the start state of the automaton. Since D is a homomorphism of on F<x>, $\sum_{q_i \in C_0} z_i^2$ and $\sum_{q_i \in C_1} z_i^2$ are rational so that each z_i, $1 \leq i \leq 4$, has a rational expression. Note that the exponents of x in the formal power series corresponding to the rational function $\frac{1}{1+x^2}$ form a periodic set of period 2 and as a consequence the

set of Gödel numbers of the strings in each of the end-sets is periodic with period 4.

It is not difficult to see that an extension of the above theorem in the case of an automaton with $n=2^k$ states implies that the Gödel numbers of the strings in each of the end-sets is periodic with period 2^k, k=2,3,... and each component of the rational solution of the state equation is of the form $f(x)/(1+x^{2^k})$.

4. DETERMINING THE EXISTENCE OF A RATIONAL SOLUTION.

In this section we provide an answer to the following question: "Given a finite automaton $M = (Q,\Sigma,\delta,q_1)$, is it possible to determine whether the corresponding state equation has a rational solution?"

We show that the answer to the above question is 'yes'. Let $\Sigma = \{0,1\}$ and also let us assume without any loss of generality that E(q) is infinite for each $q \in Q$. The case where not all E(q)'s are infinite can be handled analogously by considering only those q's for which E(q) is infinite.

Let $\Sigma^* = L_0 \cup L_1 \cup L_2 \cup \ldots$, where L_i is the set consisting of all binary strings of length i. Note that $L_0 = \{\Lambda\}$ and $|L_i| = 2^i$. Also, it is possible to enumerate the elements of L_i as

$$L_i = \{w_{i0}, w_{i1}, \ldots, w_{i,2^i-1}\}$$

where w_{ik} is the binary encoding of the integer k ($0 \leq k \leq 2^i-1$) using i bits and consequently we have

$$2^i-1 \leq \mu(w_{ik}) \leq 2(2^i-1)$$

for each k.

Assume that the state equation corresponding to M has a rational solution. Since the set of Gödel numbers of the strings belonging to each end-set E(q) is ultimately periodic, there exists an integer

$$p = \text{l.c.m } \{p_1, p_2, \ldots, p_n\}$$

an integer $N = \max \{N_1, N_2, \ldots, N_n\}$

such that for all $k \geq N$ whenever $x \in E(q)$ with $\mu(x) = k$ then $y \in E(q)$ where $\mu(y) = k+p$. Here, p_i is the smallest non-zero period of the set consisting of the Gödel numbers of the strings in the end-set $E(q_i)$ and N_i is the lower bound of periodicity. Let m be the smallest index for which there exists an integer k, $0 < k \leq 2^m-1$ and an integer j, $1 \leq j \leq n$, such that

$$\delta(q_1, w_{m0}) = q_j$$

and $$\delta(q_1, w_{mk}) = q_j$$

and moreover, if $t < k$ with $\delta(q_1, w_{mt}) = q_j$ then the sequence

$$\delta(q_1, w_{m0}),\ \delta(q_1, w_{m1}),\ \ldots\ldots,\ \delta(q_1, w_{mt})$$

does not contain each $q \in Q$ at least once. We claim that

$$p = \mu(w_{mk}) - \mu(w_{m0}) \quad .$$

To see this, let v be a string long enough such that $\mu(v) > N$ and $\delta(q_1,v) = q_1$. Consider the set

$$v.L_m = \{v.w_{m0}, v.w_{m1}, \ldots, v.w_{m,2^m-1}\}$$

which is obtained by concatenating L_m with the string v. Note that the behavior of M over L_m is the same as its behavior over $v.L_m$ in the sense that

$$\delta(q_1,w_{ms}) = \delta(q_1,v.w_{ms})$$

for each $s = 0,1,2, \ldots, 2^m-1$.
Since, $\mu(v.w_{ms}) > N$ for each s and the Gödel numbers of the strings $v.w_{ms}$ are consecutive for $s = 0,1,2,\ldots,2^m-1$, the pattern in which final states are reached by the strings $v.w_{m0}, v.w_{m1}, v.w_{m2}, \ldots, v.w_{mk}$ (starting with the initial state q_1) is repeated forever and the same argurment applies to the sequence $w_{m0}, w_{m1}, \ldots, w_{mk}$ also. It is now clear that for each $q_i \in Q$, $\Psi(E_i)$ may be written in the form

$$a_i(x) + \frac{b_i(x)}{1+x^p}$$

where the polynomial $a_i(x)$ arises from the contribution of the strings in $E(q_i)$ before the periodic behavior starts. Note that the above expression need not be in the reduced form and $\deg(b_i(x))$ may not be less that p. However, a suitable equivalent reduced form is easily obtainable. Since the solution of a state equation is unique, substituting the $\Psi(E_i)$'s back into the state equation we can decide whether the state equation has a rational solution or not.

5. CONCLUDING REMARKS.

Since there is no analytic procedure available for solving state equations in general, the relationship between rational solutions and the periodic behavior of the Gödel numbers of strings belonging to the end-sets gives us an insight into how to obtain the closed form solution (i.e. rational solution) of a state equation whenever it exists.

Finally, we note that even if the state equation of an automaton $M = (Q,\Sigma,\delta,q_1)$ does not have a rational solution, it is quite possible for Q to have a subset Q' such that for each $q' \in Q'$ the Gödel numbers of the strings in E(q') form an ultimately periodic set. To see this, consider the 3-state automaton whose transition matrix is

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

If $Q = \{q_1,q_2,q_3\}$, then it is easy to see that only the set consisting of the Gödel numbers of strings belonging to $E(q_2)$ is periodic with period 2 since all the strings ending ina 0 belong to $E(q_2)$. The fact that the corresponding state equation does not have a rational solution follows easily by using our method discussed in section 4.

REFERENCES

1. YANG, C. and HUANG, H. Algorithms for the inverse and a generalization of the state space approach to finite automata, Int. J. of Computer and Information Sciences 13(1) (1984), 59-76).

2. LEE, T.T. A state space approach to the finite automata, Int. J. of Computer and Information Sciences 12(5) (1983), 317-335.

3. HARRISON, M.A. Lectures on Linear Sequential Machines, Academic Press, N.Y., (1969).

4. VAN DER WAERDEN, B.L. Modern Algebra, Vol. I, Frederick Ungar Publishing Co., N.Y., (1953).