CYBERNETICS AND CONTROL THEORY

==================================

1963

SovietRxiv

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

A. G. LUNTS

FINITE p-ADIC AUTOMATA

(Presented by Academician P. S. Novikov on 2 I 1963)

1. In the present note it is proposed, as a mathematical apparatus for the theory of finite automata, to use analysis in the space of p-adic numbers. p-Adic numbers are interpreted as sequences of states (of an automaton, of the automaton input, of the automaton output) ([7]). Under this interpretation the outputs of an automaton are p-adic functions of the inputs of the automaton, while the variables characterizing the state of the automaton play the role of intermediate parameters used to specify the automaton. The space of p-adic numbers may be regarded as a field with respect to two pairs of operations (the field of p-adic numbers and the field with respect to polynomial multiplication and addition mod p) ([5−7]). This opens broad possibilities for applying algebraic methods in the theory of finite automata (see ([5,7])). For algebraic methods it is essential that the field of p-adic numbers contains a subfield isomorphic to the field of rational numbers, and that in considering periodic sequences (and this is apparently the most important case in the theory of finite automata) we do not go beyond the limits of this field.
2. Let p be a fixed prime number. A system of m p-adic functions $y^1, \dots, y^m$ of n p-adic arguments $x^1, \dots, x^n$,

$$y^j = F^j(x^1, \dots, x^n), \qquad j = 1, \dots, m, \tag{1}$$

is conveniently regarded as a p-adic vector function $y = (y^1, \dots, y^m)$ of a p-adic vector argument $x = (x^1, \dots, x^n)$ and written in the form

$$y = F(x). \tag{2}$$

Multiplication of a p-adic vector by a p-adic quantity (scalar) is defined as multiplication of each component of the vector by this quantity. Addition of p-adic vectors of the same dimension is defined as a componentwise operation (the corresponding components are added).

If

$$x^i = \sum_{k=-\infty}^{\infty} x_k^i p^k$$

is the canonical representation of the p-adic quantity x^i $(i = 1, \dots, n)$, then

$$x = \sum_{k=-\infty}^{\infty} x_k p^k,$$

where $x_k = (x_k^1, \dots, x_k^n)$, will be the canonical representation of the p-adic vector quantity x. The p-adic order of the quantity x is defined as the number of the first nonzero vector x_k in the canonical representation of the quantity x; in other words, $\operatorname{ord} x = \min_i \operatorname{ord} x^i$.

The p-adic norm is defined in the usual way: $\|x\| = e^{-\operatorname{ord} x}$, where e is any fixed real number greater than one. Convergence is considered with respect to this norm.

Let $f^0(x_0^1, \dots, x_0^n)$ be a function of p-valued logic (the arguments and the function take the values $0, 1, \dots, p-1$), preserving zero, i.e. $f^0(0, \dots, 0) = 0$. Define the p-adic logical func-

the function f^0 from the p-adic arguments $x^1, \dots, x^n$ in the following way:

$$f^0(x^1, \dots, x^n) = \sum_{k=-\infty}^{\infty} f^0(x_k^1, \dots, x_k^n) p^k. \tag{3}$$

A vector function $y = f(x)$, where $y = (y^1, \dots, y^m)$, $x = (x^1, \dots, x^n)$, $y^j = f^j(x^1, \dots, x^n)$ $(j = 1, \dots, m)$, will be called a **vector p-adic logical function** if all the f^j are p-adic logical functions. The adjective **vector** will, as a rule, be omitted below.

3. A vector p-adic function $F(x)$ satisfying two conditions: a) $F(px) = pF(x)$, b) $\operatorname{ord} \Delta F(x) \geqslant 0$ when $\operatorname{ord} \Delta x = 0$, where $\Delta F(x) = F(x + \Delta x) - F(x)$, will be called an **automaton function**. If the argument x is interpreted as the sequence of signals at the input of the automaton, and $F(x)$ as the sequence of signals at the output, then the two conditions formulated mean that, first, a shift by several cycles of the sequence at the input causes the same shift of the sequence at the output, and, second, $F_k(x)$ (the signal at the output in the k-th cycle) depends only on the signals at the input in the k-th and preceding cycles. An automaton function is continuous: $\lim_{\Delta x \to 0} \Delta F(x) = 0$.

Consider a system of two equations with respect to the functions y and z:

$$y = f(x, z), \qquad z = p\varphi(x, z), \tag{4}$$

where f and φ are vector p-adic logical functions. This system has a unique solution $y = F(x)$, $z = p\Phi(x)$, since from (4) we have

$$y_k = f(x_k, z_k), \qquad z_{k+1} = \varphi(x_k, z_k). \tag{5}$$

The functions $F(x)$ and $\Phi(x)$ (and consequently also the function $p\Phi(x)$) are automaton functions. In view of equalities (5), we shall call the system (4) a **finite p-adic automaton** (Mealy) and say that the function $y = F(x)$ is **realized by this automaton**. The argument x is interpreted as the sequence of signals $\dots, x_{-1}, x_0, x_1, \dots$ at the input of the automaton, the function y as the sequence of signals $\dots, y_{-1}, y_0, y_1, \dots$ at the output, and the variable z as the sequence $\dots, z_{-1}, z_0, z_1, \dots$ of states of the automaton. The signals x_0, y_0 and the state z_0 refer to the zero cycle, which may be interpreted either as the **initial** moment or as the **present** moment. The function $\varphi(x, z)$ is called the **transition function**, and the function $f(x, z)$ the **output function**. Similarly, a finite p-adic Moore automaton can be defined as a system of equations:

$$y = p^{-1}\psi(z), \qquad z = p\varphi(x, z), \tag{6}$$

where ψ and φ are p-adic logical functions. Since system (6) is equivalent to the system

$$y = \psi(\varphi(x, z)), \qquad z = p\varphi(x, z), \tag{7}$$

a Moore automaton may be regarded as a special case of a Mealy automaton. Two automata realizing one and the same function $y = F(x)$ are called **equivalent**.

Theorem 1. *Every finite p-adic Mealy automaton is equivalent to some finite p-adic Moore automaton.*

Theorem 2. *If $y = F(x)$ and $z = \Phi(x)$ are functions realizable (by finite p-adic automata), then the function $(y, z) = (F(x), \Phi(x))$ is also realizable. Here (y, z) denotes the vector obtained by concatenating the vectors y and z, so that the dimension of the vector (y, z) is equal to the sum of the dimensions of the vectors y and z.*

Theorem 3. If $y = F(x)$ and $z = \Phi(x, y)$ are realizable, then their superposition $z = \Phi(x, F(x))$ is also realizable.

Theorem 4. The system of equations

$$y = F(x, z), \quad z = p\Phi(x, z), \tag{8}$$

$$y = F(x, z), \quad z = p\Phi(x, z),$$

where $F(x,z)$ and $\Phi(x,z)$ are realizable functions, has a unique solution $y = \widetilde{F}(x)$, $z = p\widetilde{\Phi}(x)$; moreover, the functions $\widetilde{F}(x)$ and $\widetilde{\Phi}(x)$ are also realizable.

Theorem 5. The equation

$$y = F(x, px, \dots, p^r x, py, p^2 y, \dots, p^r y), \tag{9}$$

where F is a realizable function of its arguments, has as its unique solution a realizable function $y = \Phi(x)$.

This theorem may be regarded as a generalization of Theorem 2 from (4). It should be noted that not every realizable function $y = \Phi(x)$ satisfies an equation of the form

$$y = f(x, px, \dots, p^r x, py, p^2 x, \dots, p^r y), \tag{10}$$

where r is some nonnegative integer, and f is a logical p-adic function. For example, the function $y = x - 2^{\operatorname{ord} x}$ ($p = 2$, see the example) is realizable, but it satisfies no equation of the form (10).

4. A finite p-adic Mealy (Moore) automaton is an ordinary finite initial Mealy (Moore) automaton with initial state z_0 (one may restrict oneself only to p-adic integral inputs $x : \operatorname{ord} x \geqslant 0$). Conversely, any finite initial automaton (Mealy or Moore) can be written in p-adic form, i.e., one can associate with it some finite p-adic automaton.

For this it is necessary to renumber the states of the automaton by vectors of the corresponding dimension with components $0, 1, \dots, p-1$, assigning the zero vector to the initial state; to renumber the outputs by vectors and to renumber the inputs of the automaton by nonzero vectors. Then one should adjoin also the zero vector to the set of inputs, putting $\varphi(0,0) = 0$, $f(0,0) = 0$ (if the automaton is a Mealy automaton, $y_k = f(x_k, z_k)$, $z_{k+1} = \varphi(x_k, z_k)$), and arbitrarily extend these functions to those vectors on which they are not defined by the automaton (or consider a "partial"p-adic automaton, which will be isomorphic to the original finite automaton). Moreover, by choosing a sufficiently large prime number p, one can restrict oneself to one-dimensional vectors (scalars).

5. We describe a method for synthesizing a finite p-adic automaton realizing a given function $F(x)$ (cf. Theorem 8 from (1)). Suppose an automaton function $y = F(x)$ is given. To each p-adic vector u of the same dimension as the argument x, whose canonical expansion has the form

$$u = \sum_{k=-\infty}^{-1} u_k p^k,$$

we associate the function

$$F^u(v) = [F(u+v)] \tag{11}$$

of a p-adically integral argument v ($\operatorname{ord} v \geqslant 0$). Here $[F(x)]$ denotes the integral part of the function $F(x)$, i.e.

$$[F(x)] = \sum_{k=0}^{\infty} F_k(x) p^k.$$

The function $y = F(x)$ can be realized by a Mealy automaton whose states are all the distinct functions from (11):

$$y_k = f(x_k, z_k), \quad z_{k+1} = \varphi(x_k, z_k), \tag{12}$$

where

$$f(x_0, F^u) = F_0^u(x_0), \quad \varphi(x_0, F^u) = F^{p^{-1}(u+x_0)}. \tag{13}$$

In this case we shall have $f(0, F^0) = 0$, $\varphi(0, F^0) = F^0$, and therefore such an automaton is naturally also called (generally speaking, an infinite) p-adic automaton. If the number of distinct functions among (11) is finite, then the automaton (12) is finite, and it can be written in p-adic form. The finiteness of the number of distinct functions in (11) is not only a sufficient, but also a necessary condition for the given automaton function $F(x)$ to be realizable by a finite p-adic automaton.

Example. Let p be equal to 2. We construct a 2-adic automaton which replaces the first unit in the input sequence by zero, i.e., we find a realization of the function $y = F(x) = x - 2^{\operatorname{ord} x}$ (we regard $2^\infty = 0$). It is not hard to verify that the function $F(x)$ satisfies the conditions of automatonness. Next we find $F^0(y) = F(y)$, and for $u \neq 0$, $F^u(y) = y$. Thus we have only two distinct functions. If to the first function we assign the state $z_0 = 0$, and to the second the state $z_0 = 1$, then by formulas (13) we shall have $\varphi(x_0, 0) = x_0$, $\varphi(x_0, 1) = 1$, $f(x_0, 0) = F_0^0(x_0) = 0$, $f(x_0, 1) = x_0$, whence $\varphi(x_0, z_0) = x_0 \cup z_0$, $f(x_0, z_0) = x_0 \cap z_0$, consequently, $y_k = x_k \cap z_k$, $z_{k+1} = x_k \cup z_k$, i.e. $y = x \cap z$, $z = p(x \cup z)$.

6. The norm in a field generates a metric. Regardless of whether we start from the field of p-adic numbers or from the field with respect to polynomial multiplication and addition modulo p, we arrive at the same metric space. The presence of a metric makes it possible to apply iterative methods, as stated in the following

Theorem 6. If $\lim_{s\to\infty} x^{(s)} = x$, $y^{(s)} = F(x^{(s)}, z^{(s)})$, $z^{(s+1)} = p\Phi(x^{(s)}, z^{(s)})$, where F and Φ are automaton functions, and $z^{(0)}$ and $x^{(s)}$ $(s = 0, 1, ...)$ are arbitrary

p-adic functions of x, then the limits $\lim_{s\to\infty} y^{(s)} = y$ and $\lim_{s\to\infty} z^{(s)} = z$ exist and satisfy the equations $y = F(x, z)$, $z = p\Phi(x, z)$.

One may, for example, take $x^{(s)} = x$ or

$$x^{(s)} = \sum_{k=-\infty}^{s} x_k p^k.$$

Let us note, incidentally, that y and $p^{-1}z$ will be automaton functions of x.

Leningrad Electrotechnical Institute
named after V. I. Ulyanov (Lenin)

Received
9 VI 1962

CITED LITERATURE

1. V. M. Glushkov, UMN, **16**, No. 5, 3 (1961).
2. V. M. Glushkov, *Zhurn. vychislit. matem. i matem. fiz.*, **1**, No. 3, 371 (1961).
3. N. E. Kobrinskii, B. A. Trakhtenbrot, *Logical Investigations*, Publishing House of the Academy of Sciences of the USSR, 1959, pp. 352–378.
4. A. Sh. Blokh, *Problems of Cybernetics*, No. 3, 1960, p. 81.
5. D. A. Khaffmen, *Theory of Sequential Machines*, IL, 1957, p. 52.
6. I. A. Nazarov, *Izv. Leningrad. elektrotekhn. inst. im. V. I. Ulyanova (Lenina)*, **39**, 153 (1959).
7. A. G. Lunts, DAN, **144**, No. 6, 1241 (1962).

Note: Figure translations are in progress. See original paper for figures.