THE \(p\)-ADIC METHOD IN THE THEORY OF SEQUENCES

1962

SovietRxiv

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

A. G. LUNTS

THE p-ADIC METHOD IN THE THEORY OF SEQUENCES

(Presented by Academician A. N. Kolmogorov on February 7, 1962)

In the present communication, p-adic numbers are interpreted as p-ary sequences (in particular, for $p = 2$, as binary sequences), addition—as a functional element with inputs the addends and output the sum, and multiplication by the number p—as a delay element. Such an interpretation makes it possible to apply the algebra of p-adic numbers and p-adic analysis to the investigation of circuits transforming p-ary sequences. Because of lack of space, and in view of the analogy that exists between the proposed method and that of D. A. Huffman ([2]), especially in the form in which it is set forth in the article by I. A. Nazarov ([2]), we shall not dwell in sufficient detail on questions of synthesis, analysis, and graphical representation of circuits. Our aim is only to present the basic ideas of the proposed method. However, we consider it necessary, at least briefly and in simplified form, to recall the basic concepts concerning p-adic numbers.

Let p be a fixed prime number. p-adic numbers are the formal series

$$a = \sum_{k=-\infty}^{\infty} a_k p^k \tag{1}$$

(the canonical form of a p-adic number), where the a_k are integers, $0 \leq a_k \leq p-1$, and the series is infinite only to the right, i.e., for every p-adic number a there exists a number N such that $a_k = 0$ for all $k < N$. If a_N is the first nonzero coefficient in the expansion (1), then p^{-N} is called the norm of the number a: $\|a\| = p^{-N}$. If all coefficients $a_k = 0$, then $a = 0$ and $\|a\| = 0$. The limit of a sequence of p-adic numbers $\lim_{n\to\infty} a^{(n)} = a$ means that $\lim_{n\to\infty} \|a^{(n)} - a\| = 0$ in the ordinary sense. By virtue of this definition of limit, infinite series with p-adic terms converge, even converge unconditionally, if the general term of the series tends to zero. Therefore convergent series, in particular series of the form (1), may be added and multiplied term by term. With respect to addition and multiplication, the set of all p-adic numbers forms a field Δ_p, which contains as a subfield the field Δ of all rational numbers. In the canonical form of a rational number the coefficients, beginning from some point, repeat periodically. One should distinguish between rational integers and integral p-adic numbers. A p-adic number a is called integral if $\|a\| \leq 1$, i.e., in the canonical form there are no terms with negative powers of the number p.

The p-adic number (1) can be interpreted as a sequence of p-ary signals: $(\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots)$, where a_0, if desired, may be regarded either as the signal at the "initial" instant or as the signal at the "present" instant. Multiplication of a p-adic number by the number p can

interpret as a delay element, i.e. as a functional element $y = px$, whose output is the same sequence as at the input, but shifted to the right by one clock tick. We shall not dwell on the implementation of so-called one-cycle (i.e. memoryless) functional elements; this is a purely technical question and is solved with the help of various technical means, depending on how the signals are technically implemented. In particular, we shall assume that we have at our disposal functional elements that perform addition of p-ary sequences modulo p:

$$\sum_{k=-\infty}^{\infty} x_k p^k \circ \sum_{k=-\infty}^{\infty} y_k p^k = \sum_{k=-\infty}^{\infty} (x_k \circ y_k) p^k,$$

where one must take $0 \le x_k \circ y_k \le p-1$. Next we shall need a one-cycle element

$$\varphi(x, y, \dots, z) = \sum_{k=-\infty}^{\infty} \left[\frac{x_k + y_k + \dots + z_k}{p} \right] p^k$$

with a number of inputs (arguments) not exceeding $p+1$. For the case $p = 2$, this element can be implemented by means of logical multiplication

$$\sum_{k=-\infty}^{\infty} x_k p^k \cap \sum_{k=-\infty}^{\infty} y_k p^k = \sum_{k=-\infty}^{\infty} (x_k \cap y_k) p^k$$

and logical addition

$$\sum_{k=-\infty}^{\infty} x_k p^k \cup \sum_{k=-\infty}^{\infty} y_k p^k = \sum_{k=-\infty}^{\infty} (x_k \cup y_k) p^k$$

as follows: $\varphi(x, y, z) = x \cap y \cup (x \cup y) \cap z$, or with the help of a threshold element ([3]). We shall call a summator a functional element that transforms several (not more than p) p-ary sequences $x, y, \dots, z$ into the sequence $v = x + y + \dots + z$. A summator can be implemented, for example, by the functional circuit $v = x \circ y \circ \dots \circ z \circ u$, $u = p\varphi(x, y, \dots, z, u)$, which for the case $p = 3$ is shown in Fig. 1a. The signal u at the output of the intermediate element may be regarded as the "state" of the summator automaton. Let us consider several simple examples of constructing correct circuits from delay elements and summators. By correct we mean circuits that contain no "anticipation" elements p^{-1} and contain no closed loop without delay elements.

Example 1. Let us find a circuit implementing the function $y = -x$, i.e. transforming every sequence x into the sequence $-x$. We seek the equation of the

Figure 1 and Figure 2 diagrams

Figure 1: Figure 1 and Figure 2 diagrams

circuit in the form $y = ax + pby$. The coefficient of y on the right-hand side is taken to be a multiple of p so that the circuit is correct. Substituting $y = -x$ into the last equation, we obtain $-x = ax - pbx$, whence $pb = a + 1$. Taking $a = p-1,\ b = 1$, we arrive at the circuit $y = (p-1)x+py$, containing one delay element and one summator (Fig. 1b, case $p = 3$).

Example 2. Let us find a circuit implementing the function $y = rx$, where r is a given rational, integral p-adic number, i.e. $r = d/e$, where d and e are rational integers and e is not divisible by p. We note that for non-integral p-adic r there is no correct implementation, while for irrational r there is no finite implementation. We again seek the solution in the form $y = ax + pby$. After substituting $y = \dfrac{d}{e}x$, we arrive at the equation $d = ea + pdb$, which has an integral rational solution (a, b). For example, in the case $p = 2$ one may take $a = d,\ b = \dfrac{1-e}{2}$. Let $r = -63/125,\ p = 2$; then the equation of the desired circuit has the form $y = 63x + 126y$. To obtain an economical

(containing few elements) realization, we transform the right-hand side of this equation: $63x+126y = 63(x+2y) = 7\cdot 9(x+2y) = (1+2+2^2)\times(1+2^3)(x+2y)$. Thus, $y = (1 + 2 + 2^2)(1 + 2^3)(x + 2y)$. This circuit (Fig. 2a) contains 6 delay elements (or delays by 1, 2, and 3 cycles) and 4 adders (the adder in the middle of the circuit, having three inputs, should be regarded as a composition of two adders, if one has in mind the realization of an adder indicated above).

Fig. 1. $p = 3$–delay element,
1–adder, 2–adder modulo 3

Fig. 2. $p = 2$–delay element

Example 3. Let us find a circuit transforming the binary sequence

$$x = 2^{-3}(1 + 2 + 2^3 + 2^5 + 2^7 + \cdots) = 2^{-3}\left(1 + \frac{2}{1-2^2}\right) = \frac{1}{24}$$

into the sequence

$$y = 2^{-1}(1 + 2 + 2^3 + 2^4 + 2^6 + 2^7 + 2^9 + 2^{10} + \cdots) = 2^{-1}\frac{1+2}{1-2^3} = -\frac{3}{14}.$$

As in the preceding examples, we seek the solution in the form $y = ax + 2by$. Substituting $x = \frac{1}{24}$, $y = -\frac{3}{14}$, we arrive at the equation $72b - 7a = 36$. Taking $a = 36$, $b = 4$, we shall have $y = 36x + 8y$. However, to solve this problem one could have used the result of the preceding example. Let us write the equation

obtained in the form $y = 2^2(2(2^2x + y) + x)$. The corresponding realization is shown in Fig. 2b.

Example 4. Let us find a circuit which, in contrast to the preceding example, transforms the binary sequence $y = -3/14$ into the sequence $x = 1/24$. If, as in the preceding example, we seek the solution in the form $x = ay + 2bx$, then for determining the coefficients a and b we obtain the equation $14b - 36a = 7$, which has not only no integral rational solutions (this is not serious), but also no integral 2-adic solutions. A nonintegral 2-adic solution will not suit us, since it leads to an incorrect circuit. This is explained by the fact that the first one at the output x must appear earlier than the one appears at the input y. Consequently, without a "generator" the problem cannot be solved. Therefore, in the case under consideration, the solution must be sought in the more general form:

$$x = ay + 2bx + c,$$

where c will play the role of a constant sequence supplied to the circuit from outside. Substituting into the last equation $x = 1/24$, $y = -3/14$, we arrive at the equation $14b - 36a + 168c = 7$. We shall be satisfied only by a solution of this equation in which a and b are integral 2-adic numbers. In addition, it is desirable that a and b be nonnegative integral rational numbers; otherwise one would have to construct additionally realizations of the functions ay and $2bx$. If the condition of the problem does not restrict the choice of the sequence c, then we have the trivial solution $a = b = 0$, $c = 1/24$. Less trivial

we obtain a solution if we take $c = 2^{-3}$ (a one-cycle signal), $a = 0$, $b = -1$ (or $a = 7$, $b = 17$) or $c = -2^{-3} = 2^{-3}(1 + 2 + 2^2 + \cdots)$ ("generator of ones"), $a = 0$, $b = 2$. In the last case $x = 2^2x - 2^{-3}$ (Fig. 2c).

The analysis of any circuit by our method is reduced to solving, in a p-adic field, a system of equations specifying the circuit in terms of the output sequences.

A circuit that transforms each pair of sequences x, y into their product xy must possess infinite memory. Fig. 3 shows a circuit transforming any two binary sequences

$$x = \sum_{k=-\infty}^{\infty} x_k 2^k \quad \text{and} \quad y = \sum_{k=-\infty}^{\infty} y_k 2^k$$

into the product

$$\sum_{k=0}^{\infty} x_k 2^k \cdot \sum_{k=0}^{n} y_k 2^k \quad (n = 4).$$

In particular, this circuit can be used to multiply ordinary positive integers x (arbitrary) and y ($y \leq 2^{n+1} - 1$), encoded by signals in the binary system.

Fig. 3. 1–element of logical multiplication, 2–sequence converter z into $-z$

Fig. 3

Figure 2: Fig. 3

If "polynomial multiplication modulo p" is introduced, as is done in paper ([1]) and more explicitly in paper ([2]),

$$\sum_{k=-\infty}^{\infty} x_{kp}^{k} \times \sum_{k=-\infty}^{\infty} y_{kp}^{k} = \sum_{k=-\infty}^{\infty} z_{kp}^{k}, \quad \text{where} \quad z_k = \sum_{i=-\infty}^{\infty} x_i y_{k-i} \quad (\text{sum modulo } p),$$

then, with respect to the operations $\circ$ and $\times$, the set Δ_p' will be a normed field Δ_p' with characteristic equal to p. Here the norm will still remain non-Archimedean, i.e.

$$\|x \times y\| = \|x\| \cdot \|y\| \quad \text{and} \quad \|x \circ y\| \leq \max\{\|x\|, \|y\|\}.$$

For the canonical notation of a sequence we shall have

$$\sum_{k=-\infty}^{\infty} x_{kp}^{k} = \sum_{k=-\infty}^{\infty} x_k \times p^k.$$

The method of analysis and synthesis of linear circuits in the field Δ_p' will coincide with Huffman' s method ([1]) (see also ([2])).

Let us note that our interpretation of sequences as p-adic numbers makes it possible to use simultaneously the operations both of the field Δ_p and of the field Δ_p'. True, these operations are only weakly connected with one another. We shall point out only the obvious relation

$$x \circ y \circ \cdots \circ z = x + y + \cdots + z - p\varphi(x, y, \ldots, z)$$

(where there are no more than $p + 1$ terms), or, for the case $p = 2$,

$$x \circ y \circ z = x + y + z - 2(x \cap y \cup (x \cup y) \cap z).$$

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

Received
25 XI 1961

CITED LITERATURE

1. D. A. Huffman, *The Theory of Message Transmission*, IL, 1957, p. 52.

2. I. A. Nazarov, *Proceedings of the Leningrad Electrotechnical Institute*, issue 39, 153 (1959).

3. V. I. Varshavsky, DAN, 139, No. 5 (1961).

4. B. L. van der Waerden, *Modern Algebra*, part 1, 1947.

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