УДК 621.391

И. Д. ГОРБЕНКО, д-р техн. наук, *В. И. БАРСОВ*

ПРИМЕНЕНИЕ *p*-АДИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ДЛЯ ВЫЧИСЛЕНИЯ ЦИФРОВОЙ СВЕРТКИ

Развитие быстрых алгоритмов цифровой обработки сигналов (ЦОС) привело к созданию модульной *p*-адической арифметической системы, которая основывается на преобразованиях, подобных теоретико-числовым преобразованиям (ТЧП) в конечно-сегментированном *p*-адическом поле Q_p [1].

Преобразования в *p*-адическом поле имеют бо́льшую динамическую область, чем ТЧП при фиксированном значении модуля *p*, а арифметические операции над эквивалентами рациональных чисел выполняются без округлений [1].

Впервые понятие арифметики *p*-адических чисел было введено Хенселем [2]. Однако только с развитием вычислительной техники и повышением требований к точности результатов на него обратили внимание многие исследователи [1—8]. В то же время, *p*-адические преобразования имеют ряд недостатков, к которым относятся: сложность преобразования кодов Хенкеля в обратно-рациональный ряд; жесткая связь между длиной преобразования и длиной слова; трудности в определении базиса преобразования (определение корня степени *N* из единицы) и его длины [3].

Сущность *p*-адических преобразований. Любое не нулевое рациональное число α может быть представлено последовательностью цифр a_n, a^{n+1}, a_{n+2}, ..., удовлетворяющих условию $0 \leqslant a_i < p$ для $i = n+1, n+2, \ldots$, таких что

$$\alpha = \sum_{i=n}^{\infty} a_i p^i, \tag{1}$$

где p — заданное простое число, называемое модулем преобразования.

Выражение (1) называется p-адическим представлением не нулевого рационального числа α, а значение a_i называется p-адическими цифрами [6].

При практической реализации p-адического преобразования и проведении расчетов использование ряда (1) с бесконечным числом членов весьма затруднительно, поэтому предпочтительнее операции выполнять с фиксированной длиной p-адических чисел, представленных в виде кода Хенселя.

Определение 1. *Пусть α рациональное число и a_{-n}, a_{-n+1}, a_{-n+2}, ..., a_{-1}, a_0, a_1, ..., a_k — p-адические цифры его разложения. Тогда конечный сегмент a_{-n}, ..., a_k называется кодом Хенселя числа α и обозначается $H(p, r, \alpha)$, где p — заданный простой модуль; $r = n + 1 + k$ — число членов ряда.*

Согласно определению 1 вместо бесконечного ряда, получаемого с помощью выражения (1), берется конечная сумма первых r членов

$$\alpha = \sum_{i=n}^{k} a_i p^i. \tag{2}$$

Здесь α принадлежит конечно-сегментированному p-адическому полю $\bar{Q}_p$, получаемому сегментированием поля p-адических чисел Q_p по r, и является кодом Хенселя рационального числа α.

Любое рациональное число $\alpha = (a/b)$ единственным образом представимо в $\bar{Q}_p$ через $H(p, r, \alpha)$, если

$$-\sqrt{\frac{p^r-1}{2}} \leqslant a,\ b < \sqrt{\frac{p^r-1}{2}}. \tag{3}$$

Неравенство (3) называют динамической областью представления рациональных чисел кодами Хенкеля из $\bar{Q}_p$ [1].

Аналогично Z преобразованию, обладающему структурой ДПФ, в поле $\bar{Q}_p$ можно определить сходное по структуре и свойствам быстрое преобразование.

Определение 2. *Прямым p-адическим преобразованием последовательности $H(p, r, x_n)$, где $n = 0, 1, 2, \ldots, N-1$, в конечно-сегментированном p-адическом поле $\bar{Q}_p$ называется преобразование вида*

$$H(p, r, X_k) = \sum_{n=0}^{N-1} H(p, r, x_n)\,[H(p, r, \alpha)]^{nk}, \tag{4}$$

где $H(p, r, \alpha)$ — примитивный корень N-й степени из единицы в поле $\bar{Q}_p$. Обратным p-адическим преобразованием называется преобразование вида

$$H(p, r, x_l) = H(p, r, N^{-1}) \sum_{k=0}^{N-1} H(p, r, X_k) [H(p, r, \alpha)]^{-lk}. \quad [5]$$

Необходимыми и достаточными условиями существования p-адического преобразования являются следующие условия.

1. В поле $\bar{Q}_p$ существует элемент $H(p, r, \alpha)$, являющийся примитивным корнем N-й степени из единицы, т. е.

$$[H(p, r, \alpha)]^N = H(p, r, 1).$$

2. Поле $\bar{Q}_p$ должно содержать элемент $H(p, r, N^{-1})$ [1]. В работе [1] показано, что максимальная длина для p-адических преобразований равна $N_{max} = p - 1$ (6), а $(p-1)$-й корень всегда существует и такой, что

$$[H(p, r, \alpha)]^{p-1} = H(p, r, 1).$$

Для обращения кодов Хенселя в рациональное число существует несколько методов, так в работах [4; 5] предлагается решить эту задачу для множества рациональных чисел Фарея порядка N, где N — положительное число, удовлетворяющее неравенству

$$N \leqslant \sqrt{(p-1)/2}.$$

Кроме этого, в работе [7] предложен метод просмотра таблицы для определения нужного рационального числа среди уже вычисленных значений множества чисел Фарея. Решать данную задачу можно, используя и другие методы, в частности, расширенный алгоритм Евклида [6].

Одной из возможных областей применения p-адических преобразований в ЦОС является вычисление цифровой свертки двух последовательностей X_Q и h_Q длины N с использованием параллельных матричных процессоров. Исходя из выражений (3), (6) определяем значения модуля p и длину кода Хенселя r.

Для заданных p и r определим значение примитивного корня из единицы порядка N $H(p, r, \alpha)$, которое используется для построения матриц прямого T_Q и обратного T_Q^{-1} p-адического преобразования:

$$T_Q = \begin{bmatrix} H(p, r, 1) H(p, r, 1) H(p, r, 1) \dots H(p, r, 1); \\ H(p, r, 1) H(p, r, \alpha) H(p, r, \alpha^2) \dots H(p, r, \alpha)^{N-1} \\ \dots \\ H(p, r, 1) H(p, r, \alpha^{N-1}) H(p, r, \alpha^{2(N-1)}) \dots H(p, r, \alpha^{(N-1)^2}) \end{bmatrix};$$

$$T_Q^{-1} = H(p, r, N^{-1}) \begin{Bmatrix} H(p, r, 1) H(p, r, 1) H(p, r, 1) \dots H(p, r, 1); \\ H(p, r, 1) H(p, r, \alpha^{-1}) H(p, r, \alpha^{-2}) \dots \\ \dots H(p, r, \alpha^{-(N-1)}) \\ \dots \\ H(p, r, 1) H(p, r, \alpha^{-(N-1)}) H(p, r, \alpha^{-2(N-1)}) \dots \\ \dots H(p, r, \alpha^{-(N-1)^2}) \end{Bmatrix},$$

где $H(p, r, 1) = H(p, r, \alpha^0)$.

Сворачивание последовательностей x_Q и h_Q тоже представляется в виде последовательностей кодов Хенселя. Прямое преобразование в кодах Хенселя осуществляется следующим образом: $X_Q = T_Q \cdot x_Q$; $H_Q = T_Q \cdot h_Q$ (7). Далее, используя теорему о свойстве циклической свертки, получаем значение выходной последовательности $Y_Q = X_Q \times H_Q$ (8). Обратное преобразование для Y_Q имеет вид $Y'_Q = T_Q^{-1} \cdot Y_Q$ (9). Обратная задача восстановления рациональных чисел из значений их кодов Хенселя решается одним из методов, указанных в работах [4—6].

Итак, большая часть матричных задач нуждается в разнообразном множестве вычислительных требований: увеличение скорости решения, выбор точности, алгоритма, устойчивости. Эти требования могут одновременно удовлетворяться при использовании преимуществ многокритичной модульной p-адической арифметики, осуществляемой высокопараллельной вычислительной системой.

Список литературы: 1. *Nasrabadi N. M., King R. A.* The fast digital convolution using P—ADIC transforms // Electron. Letters. 1983. N 1. P. 111—113. 2. *Hensel K.* Theori der algebrai shen zahlen. Teubner. Leipzig. 1908. P. 158. 3. *Bachman G.* Introduction to P—ADIC numbers and valuation theory. New York. 1964. P. 200. 4. *Krishnamurhy E. D.* On the conversion of hensel codes to farey rational // JEEE trans. computers. 1983. N 4. P. 130—150. 5. *Pei S.* and *Wu L.* Determination of P—ADIC transform bases and leugths. // Electron letters. 1986. N 10. P. 50—53. 6. *Miola A.* Algebraic approach to P-ADIC conversion of rational numbers // Information Processing letters. 1984. N3. P. 180—200. 7. *Manadeva Rao T.* Convertion of hensel codes to rational numbers. // Computers & matematics. 1984. N 2. P. 200—225. 8. *Боревич З. Н., Шафаревич И. Р.* Теория чисел. М., 1972. 66 с.

Поступила в редколлегию 27.07.89