ПРИМЕНЕНИЕ СИСТЕМНОГО АНАЛИЗА ДЛЯ ПРЯМОЙ ПРОЦЕДУРЫ ПРЕОБРАЗОВАНИЯ ИЗ ПОЗИЦИОННОЙ СИСТЕМЫ СЧИСЛЕНИЯ В ПОЛИНОМИАЛЬНУЮ СИСТЕМУ КЛАССОВ ВЫЧЕТОВ

Калмыков И.А., Кихтенко О.А., Барильская А.В.

ГОУ ВПО

«Северо-Кавказский Государственный технический университет»

Г. Ставрополь, Россия

koa87@list.ru

Одной из первых немодульных процедур, необходимой для функционирования спецпроцессора класса вычетов, является реализация прямого преобразования позиционных кодов в код полиномиальной системы классов вычетов расширенного поля Галуа $GF(p^n)$ [1,2].

Все множество методов перевода из позиционной системы счисления в систему классов вычетов можно свести к трем основным группам.

В основу методов, образующих первую группу, положен метод понижения разрядности числа [3,4], не содержащий операцию деления. Значения C_i можно знать заранее и они являются константами для выбранной системы счисления. Цифры исходного числа умножаются на соответствующие числа C_i, полученная сумма определяется

$$A_1 = A_k \cdot C_k + ... + A_1 \cdot C_1 + A_0 \cdot C_0 < A_k \cdot S^k + ... + A_1 \cdot S^1 + A_0 . \quad (1)$$

По значению A_1 можно узнать каков остаток от деления числа A на p_j. Если A_1 имеет количество разрядов больше, чем p_j, то вновь цифры числа A_1 необходимо умножить на числа C_i, причем полученная сумма будет $A_2 < A_1$.

По значению A_2 можно узнать каков остаток от деления числа A на p_j. Этот процесс продолжается до тех пор, пока не получится число A_l, разрядностью равной или меньшей разрядности p_j. По данному числу и

определяется остаток от деления A на p_j.

Для получения требуемого вычета $a_i = |A|_{p_i}^{+}$ предлагается использовать повторение вычислительной модели

$$|A|_{p_i}^{+} = \sum_{i=0}^{k} |2^i|_{p_i}^{+} \cdot \{a(j)\}^{[i]}, \qquad (2)$$

где $j = 0,1,2,....$

Несмотря на простоту реализации, данный метод преобразования чисел по модулю, построенных по принципу рекуррентной редукции, значительно сужают область применения модулярной арифметики.

Основу второй группы составляют методы, обеспечивающие пространственное распределение вычислительного процесса перевода из ПСС в ПСКВ. Отказ от обратных связей в нейронных сетях реализует обработку исходных данных на сети прямого распространения. Число слоев в такой сети определяется количеством итераций l, необходимых для преобразования входных данных, а количество нейронов в каждом слое – разрядностью обрабатываемых данных на каждой из итераций.

Замена обратных связей в нейронных сетях на прямые позволяет повысить скорость обработки данных, так как в такой сети одновременно обрабатывается несколько отсчетов и в каждом такте работы сети на входе формируются преобразованные данные. Максимальное значение числа на первой итерации $max\{A(1)\}$ можно определить в предположении, что число A состоит из одних единиц. Принцип работы устройства, реализующего данный алгоритм перевода чисел из ПСС в ПСКВ, приведен в работе [2].

Вычислительные процессы третьей группы методов перевода чисел из ПСС в непозиционную систему реализуют различные варианты метода непосредственного суммирования [1,3,4]. Преобразование исходного $A(z)$, заданного в расширенном поле $GF(p^n)$, в полиномиальную систему классов вычетов осуществляется с помощью набора констант, являющихся эквивалентами степеней оснований 2^i и коэффициентов при

соответствующих степенях оснований a_i, представленных в системе классов вычетов.

Перевод из позиционного двоичного кода в полиномиальную систему классов вычетов осуществляется в соответствии с выражением

$$a_i(z) \equiv A(z) \bmod p_i(z) = \sum_{l=0}^{k} a_l(z) \cdot z^l \bmod p_i(z), \qquad (3)$$

где $i = 1,2,3,..,n$.

Для получения $A(z)$ в системе классов вычетов с основаниями $p_1(z), p_2(z),..., p_n(z)$ необходимо получить в этой системе значения $a_l(z) \cdot z^l \bmod p_i(z)$. В этом случае остаток по модулю $p_i(z)$ определяется

$$a_i(z) = \left| \sum_{l=0}^{k} (a_l^i \cdot z^l) \bmod p_i(z) \right|_2^+, \qquad (4)$$

где $a_l^i = a_l \bmod p_i(z)$, $i = 1,2,3,..,n$.

В соответствии с выражением (4), перевод $A(z)$ из позиционной системы счисления в непозиционную можно свести к суммированию по модулю два величин $(a_l^i \cdot z^l) \bmod p_i(z)$ в соответствии с заданным полиномом $A(z)$.

Таким образом, очевидно, что модификация и реализация метода непосредственного суммирования для полиномиальной системы классов вычетов позволяет разрабатывать высокоскоростные преобразователи кодов для вычислительных структур реального масштаба времени.

Список литературы:

1. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронных сетей для исследования ортогональных преобразований в расширенных полях Галуа/Нейрокомпьютеры: разработка, применение. №6, 2003.

2. Элементы применения компьютерной математики и нейроинформатики/Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ,

2003.

3. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: ФИЗМАТЛИТ, 2003.

4. Червяков Н.И., Шапошников А.В., Сахнюк П.А., Макоха А.Н. Нейрокомпьютеры в остаточных классах. – М.: Радиотехника, 2003.