Анализ методов перевода из позиционной системы счисления в полиномиальную систему классов вычетов

Резеньков Д.Н.
Ставропольский военный институт связи Ракетных войск
Ставрополь, Россия

Для реализации вычислительного процесса с использованием полиномиальной системы классов вычетов необходимо осуществить преобразование из позиционного кода в модулярный и обратно [1,2,3]. Такие операции являются немодульными и относятся к классу позиционных операций, которые являются наиболее трудоемкими в непозиционной системе классов вычетов. Как правило, немодульные процедуры реализуют с помощью последовательности модульных операций.

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 $GF(p^n)$[4,5,6].

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, не содержащий операцию деления.

В основу данного метода положена теорема, согласно которой вычисление остатка осуществляется с помощью итерационного алгоритма. Для этого необходимо определить остатки от деления на p_j степеней основания, которые дадут набор чисел C_i, $i=1,2...,r$. Если остаток от деления степени основания C_i превосходит половину модуля p_j, то в качестве значения C_i необходимо взять число, дополняющее до значения p_j, со знаком минус. Значения C_i можно знать заранее и они являются константами для выбранной системы счисления. Количество разрядов C_i определяется разрядностью исходного числа A. Затем цифры исходного числа умножаются на соответствующие числа C_i, полученная сумма определяется

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

В этом методе используется два принципа. Первый заключается в преобразовании числа A большей разрядности в число малой разрядности за счет использования в качестве коэффициентов $a_i = C_i = \left|2^i\right|^+_{p_i} = 2^i$, разрядность которых не превышает разрядности модуля p_i. Вторая идея заключается в нахождении свертки исходного числа путем определения наименьшего неотрицательного вычета в результате реализации первой идеи малоразрядного числа последовательным применением разработанного метода до получения операции сокращения по модулю p_i, т.е. $\left|A\right|^+_{p_i} \le p_i$

Основу второй группы составляют методы, обеспечивающие пространственного распределение вычислительного процесса – перевода из ПСС

в ПСКВ. 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 [6]. В этом случае итеративный алгоритм преобразования *A* по модулю *p* определяется выражением

$$A(l+1)=\sum_{i=0}^{ordA(l)}\left|2^{i}\right|_{p}^{+}\cdot\left|\left[\frac{A(l)}{2^{i}}\right]\right|_{2}^{+} \qquad (2)$$

где *l=0,1,2,…* - число 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(l)}* можно определить в предположении, что число *A* состоит из одних единиц [5,6].

Вычислительные процессы третьей группы методов перевода чисел из ПСС в непозиционную систему реализуют различные варианты метода непосредственного суммирования [4,6,7].

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

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

где *i=1,2...,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...,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)* [5,6].

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

СПИСОК ЛИТЕРАТУРЫ

1. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах.-М.:Сов. Радио, 1968.-440с

2. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О.,Бережной В.В. Архитектура отказоустойчивой нейронной сети для цифровой обработки сигналов /Нейрокомпьютеры: разработка, применение.№12, 2004, с.51-60.

3. Червяков Н.И. Преобразованиецифровых позиционных и непозиционныхкодов в системах управления и связи.-Ставрополь,СВВИУС.1985.-63с.

4. 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, с.61-68.

5. Элементы применения компьютерной математики и нейроинформатики/ Н.И. Червяков, И.А. Калмыков, В.А. Галкина, Ю.О. Щелкунова, А.АШилов; под редакцией Н.И. Червякова.-М.: ФИЗМАТЛИТ, 2003.-216с.

6. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе класса вычетов.-М.: ФИЗМАТЛИТ,2005.-274с.

7. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А.Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: ФИЗМАТЛИТ,2003.-288с.