УДК 681.3

Анализ основных методов прямого преобразования из позиционной системы счисления в модулярный полиномиальный код.

В современных условиях цифровая обработка сигналов (ЦОС) занимает основное положение в системах передачи и обработки информации. Эффективность ЦОС полностью зависит от объема вычислений, который определяется математической моделью цифровой обработки сигналов.

Для реализации вычислительного процесса с использованием полиномиальной системы классов вычетов (ПСКВ) необходимо осуществить преобразование из позиционного кода в модулярный. 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 (СП) класса вычетов, является реализация прямого преобразования позиционных кодов в код ПСКВ расширенного поля Галуа $GF(p^{v})$.

Представление операнда в позиционном счислении определяется следующим образом: $\mathrm{A}(z) = a_r z^r + a_{r-1} z^{r-1} + \ldots + a_i z + a^0$,

где a_i – элементы поля $GF(2)$, $i = 0,\ldots r$

Для перевода из позиционной системы счисления (ПСС) в непозиционную необходимо выполнить операции деления на модули $p_i(z)$, $i = 1,2\ldots n$.. Образование остатка $a_1(\mathrm{Z})$ в этом случае осуществляется следующим образом:

$a_1(\mathrm{Z}) = \mathrm{A}(\mathrm{Z}) - \left[\mathrm{A}(\mathrm{Z}) \big/ p_i(\mathrm{Z})\right] p_i(\mathrm{Z})$, где $\left[\mathrm{A}(\mathrm{Z}) \big/ p_i(\mathrm{Z})\right]$ - наименьшее целое от деления $A(z)$ на основание $p_i(z)$, $i = 1,2\ldots n$.

Все множество методов перевода из ПСС в систему классов вычетов можно свести к трем основным группам. В основу методов образующих первую группу положен метод понижения разрядности числа. Согласно этого [1] вычисление остатка осуществляется с помощью итерационного алгоритма. Для этого необходимо определить остатки от деления на p_i степеней основания, которые дадут набор чисел C_i, $i = 1,2\ldots r$. Несмотря на простоту реализации, данный метод имеет ряд недостатков[2], основными из которых являются:

1. Наличие обратных связей, применение которых в значительной степени снижают производительность системы.
2. Необходимость проверки условий окончания процесса итерации по контролю знака полученной разницы в операции вычитания, что значительно снижает быстродействие системы.
3. Коэффициент использования оборудования на каждой последующей итерации снижается.

Во вторую группу входят методы, обеспечивающие пространственное распределение вычислительного процесса перевода из ПСС в ПСКВ. В [2] предложена математическая модель нейронной сети, реализующей прямое преобразование позиционного двоичного кода в код классов вычетов, на основе сети прямого распространения. Принцип работы устройства , реализующего данный алгоритм перевода чисел из ПСС в ПСКВ приведен в работе [3].

Вычислительные процессы третьей группы реализуют различные варианты метода непосредственного суммирования. Перевод из позиционного двоичного кода в ПСКВ осуществляется в соответствии с выражением:

$$a_i(z) \equiv \mathrm{A}(z) \bmod p_i(z) = \sum_{l=0}^{k} a_i(z) \cdot z^i \bmod p_i(z)\text{, где } i = 1,2,3,\ldots n.$$

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

$$a_i(z) = \left| \sum_{l=0}^{л} (a_l^i \cdot z^l) \bmod p_i(z) \right|_2^+\text{, где } a_i(z) \cdot z^i \bmod p_i(z),\ i = 1,2,3,\ldots n.$$

В соответствии с этим выражением перевод $A(z)$ из ПСС 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 $A(z)$. Математическая модель нейронной сети, реализующей перевод из ПСС в ПСКВ по модулю поля $GF(2^4)$ на основе метода непосредственного суммирования представлена в [3]. Очевидно, что модификация и реализация метода непосредственного суммирования для ПСКВ позволяет разрабатывать высокоскоростные преобразователи кодов для вычислительных структур в реальном масштабе времени [4].

Таким образом очевидно, что основным достоинством полиномиальной системы классов вычетов является сравнительная простота выполнения модульных операций. Рассмотренные формальные правила выполнения операций в ПСКВ позволяют существенно повысить скорость вычислительных устройств ЦОС. Так как основания системы представляют собой полиномы с небольшими степенями, то это позволяет арифметические действия описать в виде таблиц. В этом случае выполнение операций сводится к выборке результатов по заданным остаткам операндов.

Литература

1. *Червяков Н.И.* Преобразователи цифровых позиционных и непозиционных кодов в истемах управления и связи.- Ставрополь, СВВИУС. 1985.-63с.
2. *Червяков Н.И., Шапошников А.В., Сахнюк П.А.* Оптимизация структуры нейронных сетей конечного кольца/ Нейрокомпьютеры: разработка,применеие. № 10, 2001, с.13-18.
3. Элементы применения компьютерной математики и нейроинфроматики /*Червяков Н.И., Калмыков И.А., Галкина В.А., Щелкунова Ю.О., Шилов А.А.; Под ред. Н.И. Червякова.* – М.: Физматлит, 2003. – 216 с.
4. *Калмыков И.А.* Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова – М: Физматлит, 2005.-276с.