РАЗРАБОТКА ПРЕОБРАЗОВАТЕЛЯ ПОЗИЦИОННОГО КОДА В ПОЛИНОМИАЛЬНУЮ СИСТЕМУ КЛАССА ВЫЧЕТОВ

Калмыков И.А., Тимошенко Л. И., Чипига А.А.

Ставропольский военный институт связи Ракетных войск,

г. Ставрополь, Россия

kia762@yandex.ru

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

Особое место среди таких моделей занимает полиномиальная система класса вычетов (ПСКВ), с помощью которых возможна организация ортогональных преобразований сигналов в расширенных полях Галуа $GF(p^n)$ [1,2]. Основным достоинством системы класса вычетов является сравнительная простота выполнения модульных операций (сложения, вычитания, умножения). Формальные правила выполнения таких операций в ПСКВ позволяют существенно повысить скорость вычислительных устройств ЦОС.

Одной из немодульных процедур, выполняемой спецпроцессором (СП) класса вычетов, является реализация прямого преобразования кода позиционной системы счисления (ПСС) в код ПСКВ. В настоящее время нашли широкое применение несколько методов перевода из ПСС в ПСКВ. Один из основополагающих методов перевода является метод понижения разрядности числа [1,3]

$$a_i = C_i = \left|2^i\right|_{p_i}^{+} = 2^i, \qquad \forall \ \ i \in [0, r]. \tag{1}$$

Таким образом, для получения требуемого вычета $a_i = \left|A\right|_{p_i}^{+}$ предлагается использовать повторение вычислительной модели

$$\left|A\right|_{p_i}^{+} = \sum_{i=0}^{k} \left|2^i\right|_{p_i}^{+} \cdot \{a(j)\}^{[i]}, \text{ где } j = 0,1,2,..., \tag{2}$$

При этом для реализации (2) используется позиционный сумматор.

Однако реализация выражения (2) характеризуется необходимостью проверки условий окончания процесса итераций по контролю знака полученной разницы в операции вычитания, что значительно снижает быстродействие системы. А при достаточно большой размерности входных данных количество итераций может быть достаточно большим, что снижает быстродействие системы в целом.

Устранить указанные недостатки можно отказавшись от обратных связей в нейронных сетях (НС) конечного кольца, реализовав обработку на сети прямого распространения [1]. 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. Веса, связывающие i-й нейрон с j-м нейроном следующего слоя, определяются $v_{ij} = \left\{ 2^i \Big|_p^+ \right\}^{[j]}$. Тогда итеративный алгоритм преобразования A по модулю p определяется выражением

$$A(l+1) = \sum_{i=0}^{ord\,A(l)} \left| 2^i \right|_p^+ \cdot \left| \left[\frac{A(l)}{2^i} \right] \right|_2^+, \qquad (3)$$

Замена обратных связей в НС 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.

Повысить скорость реализации прямого преобразования из кода ПСС в код ПСКВ можно за счет метода непосредственного суммирования [1,3]. Преобразование исходного $A(z)$, заданного в поле $GF(p^n)$, в полиномиальную систему класса вычетов осуществляется с помощью набора констант, являющихся эквивалентами степеней оснований 2^i и коэффициентов при соответствующих степенях оснований $a_i(z)$, представленных в ПСКВ

$$A(z) = \sum_{l=0}^{k} a_l(z) \cdot z^l \equiv a_i(z) \bmod p_i(z), \quad i = 1,2,3,..,n. \qquad (4)$$

Для получения значений $A(z)$ в системе класса 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

$$a_i(z) = \left| \sum_{l=0}^{k} (a_l^i \cdot z^l) \bmod p_i(z) \right|_2^+, \qquad (5)$$

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

В соответствии с (5), 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 $A(z)$.

Пример. Определить остаток $A(z) = z^{12} + z^7 + z^5 + z^4 + z^3 + z$ по модулю $p(z) = z^4 + z^3 + 1$.

Для перевода из ПСС в ПСКВ воспользуемся выражением (5). Тогда значения остатков степеней оснований и коэффициентов при них равны

$z^{12} \equiv z + 1 \bmod (z^4 + z^3 + 1)$ $\qquad$ $z^4 \equiv z^3 + 1 \bmod (z^4 + z^3 + 1)$

$z^7 \equiv z^2 + z + 1 \bmod (z^4 + z^3 + 1)$ $\qquad$ $z^3 \equiv z^3 \bmod (z^4 + z^3 + 1)$

$z^5 \equiv z^3 + z + 1 \bmod (z^4 + z^3 + 1)$ $\qquad$ $z \equiv z \bmod (z^4 + z^3 + 1)$

Тогда, согласно (5), получаем

$$a(z) = (z+1) \oplus (z^2 + z + 1) \oplus (z^3 + z + 1) \oplus (z^3 + 1) \oplus z^3 \oplus z = z^3 + z^2.$$

Таким образом, $z^{12} + z^7 + z^5 + z^4 + z^3 + z \equiv z^3 + z^2 \bmod (z^4 + z^3 + 1)$.

В работе [1] представлена матрица связанности, т. е. синаптические веса нейронной сети, представляются в виде матрицы, строки которой соответствуют области аксонов предыдущего слоя, а столбцы – рецепторным полям нейронов последующего слоя. Разрабатываемая НС для перевода из ПСС в ПСКВ содержит 2 слоя. Первый слой состоит из 15 нейронов, на входы которых подается исходный полином в двоичном коде. С выходов нейронов первого слоя сигналы поступают на входы нейронов 2-го слоя в соответствии с матрицей T_{12}

$$T_{12} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{vmatrix}^T$$

При этом операция перевода осуществляется всего за одну итерацию, что является существенным преимуществом по сравнению с ранее рассмотренными методами перевода. Структура НС, реализующей перевод по $p(z) = z^4 + z^3 + 1$ в ПСКВ поля $GF(2^4)$, представлена [1].

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

Литература

1. Элементы компьютерной математики и нейроноинформатики /Червяков Н.И., Калмыков И.А., Галкина В.А., Щелкунова Ю.О., Шилов А.А.. – М.: ФИЗМАТЛИТ, 2003. – 216 с.

2. Червяков Н.И., Калмыков И.А., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронных сетей для исследования ортогональных преобразований сигналов в расширенных полях Галуа. – Нейрокомпьютеры: разработка и применение. 2003, №6, с.61-68.

3. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2005. - 276 с.