онную систему реализуют различные варианты метода непосредственного суммирования [4,6,7].

Преобразование исходного A(z), заданного в расширенном поле $GF(p^v)$, 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

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

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

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

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 системы 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.- 440 с.

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. Преобразование цифровых позиционных и непозиционных кодов в системах управления и связи.- Ставрополь, СВВИУС, 1985.- 63 с.

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.А. Шилов; 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.

ИТЕРАТИВНЫЙ АЛГОРИТМ ПЕРЕВОДА ИЗ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ В ПОЗИЦИОННУЮ СИСТЕМУ СЧИСЛЕНИЯ

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

Наряду с прямым преобразованием из позиционного кода в модулярный существует и обратный перевод, позволяющий по величине n-мерного вектора A(z)=($a_1(z)$, $a_2(z)$,…, $a_n(z)$) получить двоичное представление полинома.

В настоящее время известны два основных способа перевода непозиционного кода классов вычетов в позиционную систему счисления (ПСС) [1,2,3,6].

Задачей этих методов является восстановление заданного полинома $A(z) \in GF(p^v)$ по совокупности его остатков ($a_1(z)$, $a_2(z)$,…, $a_n(z)$).

Один из методов основывается на китайской теореме об остатках (КТО). Применение КТО обеспечивает однозначное отображение одномерных величин в многомерные и позволяет осуществлять восстановление полученного результата из непозиционной системы счисления к двоичному позиционному виду[1,4,5,8].

Задача перевода n–мерного представления полинома $A(z) \in GF(p^v)$ представляется следующим образом: для заданного набора модулей $p_i(Z)$, i=1,2...,n, необходимо осуществить преобразование n–мерного образа $A(z)=(a_1(z),a_2(z),...,a_n(z))$ в систему с основанием $P(z) = \prod_{i=1}^{n} p_i(z)$ так, чтобы выполнилось условие

$$A(z)= a_1(z) \cdot B_1(z)+ a_2(z) \cdot B_2(z) +...+ a_n(z) \cdot B_n(z) \quad (1)$$

где $B_i(Z)$ – базисы системы; i=1,2...,n.

В общем виде любой базис можно представить в непозиционном виде как

$$B_i(z) = (B_1^i(z), B_2^i(z),..., B_n^i(z)), \quad (2)$$

где $B_j^i(z) \equiv B_i(z) \bmod p_j(z)$; i, j=1,2…,n

С другой стороны известно, что любой элемент A(z)∈ P(Z) можно представить как сумму ортогональных полиномов $A_1(z),A_2(z),...,A_n(z)$, т.е.

$$A(z)=(a_1(z),a_2(z),...,a_n(z)) =A_1(z)+A_2(z)+... \\ \ldots+A_n(z)=(a_1(z),0,..,0)+(0, a_2(z),0,..,0)+\ldots \\ \ldots+(0,0,\ldots a_n(z)) \quad (3)$$

Под ортогональным полиномом понимается элемент расширенного поля $GF(p^v)$ заданного основаниями $p_1(z),...,p_n(z)$ таких, что $P(z)=\prod_{i=1}^{n} p_i(z)$, у которого все остатки равны нулю, за исключением цифры по модулю $p_i(z)$

$A_i(z)=(0,0,\ldots,0, a_i(z),0,\ldots 0)$, где i=1,2...,n.

Приравнивая выражения (1) и (3) и учитывая независимость выполнения арифметических операций по модулям полиномиальной системы классов вычетов (ПСКВ), получаем, что

$$a_i(z) \cdot B_i(z) =(0,0,\ldots,0, a_i(z),0,\ldots 0). \quad (4)$$

Исходя из условия представления базисов системы согласно (2)

$$(a_i(z) \cdot b_1^i(z),..., a_i(z) \cdot b_i^i(z),..., a_i(z) \cdot b_n^i(z)) = \\ = (0,0,..., a_i(z),...,0) \quad (5)$$

Следовательно, ортогональные базисы $B_i(z)$, i=1,2...,n системы ПСКВ расширенного поля Галуа $GF(p^v)$ можно представить в следующем виде

$$\begin{aligned} B_1(z) &= (1,0,...,0,...,0); \\ &\vdots \\ B_i(z) &= (0,0,...,1,...,0); \quad (6) \\ &\vdots \\ B_n(z) &= (0,0,...,0,...,1); \end{aligned}$$

Таким образом, выражение (1) можно записать как:

$$A(z)=\sum_{i=1}^{n} a_i(z)B_i(z) \bmod P(z) \quad (7)$$

Для получения значений ортогональных базисов ПСКВ воспользуемся КТО и равенствами (6), согласно которым

$$B_i(z)=\begin{cases} 0 \bmod p_n(z), u \neq i \\ 1 \bmod p_n(z), u = i \end{cases} \quad (8)$$

где

$$B_i(z)=m_i(z)\prod_{\substack{u=1 \\ u\neq i}}^{n} p_u(z); m_i(z)\prod_{\substack{u=1 \\ u\neq i}}^{n} p_u(z) \equiv 1 \bmod p_i(z),$$

Преобразуя выражение (8), получаем формулу для вычисления ортогонального базиса по i–ому основанию

$$B_i(z) = m_i(z)\cdot P(z)/ p_i(z), \quad (9)$$

где – $m_i(z)$ - вес ортогонального базиса.

Вес ортогонального базиса выбирается из условия $B_i(z) \bmod p_i(z) \equiv 1$.

Устройство обратного преобразования из ПСКВ, обладает высоким быстродействием – процедура перевода осуществляется за одну итерациюна основе нейронных сетей (НС) прямого распространения. Кроме того, данная структура характеризуется отсутствием выходного сумматора по модулю $P(z)=\prod_{i=1}^{n} p_i(z) = z^{p^{v}-1}+1$, а, следовательно, и обратных связей, что в значительной степени приведет к повышению быстродействия вычислительной структуры в целом [7,8].

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. Математическая модель нейронных сетей для исследования ортогональных преобразований в расширенных полях Галуа. /Нейрокомпьютеры: разработка, применение. №6, 2003, с.61-68.

3. 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.

4. Калмыков И.А. Лободин М.В., Гахов В.Р., Владимиров А.А. Высокоскоростной нейросетевой преобразователь из полиномиальной системы классов вычетов в позиционный код /Труды международного форума по проблемам науки, техники и образования. Том1. /Под ред. В.П. Савиных, В.В, Вишневского. - М.: Академия наук, 2004. - с.151-152.

5. Червяков Н.И. Преобразование цифровых позиционных и непозиционных кодов в системах управления и связи.- Ставрополь, СВВИУС, 1985. – 63 с.

6. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Рядов С.А.Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: ФИЗМАТЛИТ, 2003. – 288 с.

7. 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. - 216 с.

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

МИНИМИЗАЦИЯ АППАРАТУРНЫХ ЗАТРАТ ПРИ ВЫЧИСЛЕНИИ КОЭФФИЦИЕНТОВ ОБОБЩЕННОЙ ПОЛИАДИЧЕСКОЙ СИСТЕМЫ В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССОВ ВЫЧЕТОВ

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

Основным достоинством полиномиальной системы классов вычетов (ПСКВ) является сравнительная простота выполнения модульных операций (сложения, вычитания, умножения). Выполнение операций в ПСКВ позволяют существенно повысить скорость вычислительных устройств цифровой обработке сигналов.

Для реализации вычислительного процесса с использованием ПСКВ необходимо осуществить преобразование из позиционного кода в модулярный и обратно.

Обратное преобразование из ПСКВ в позиционную систему счисления (ПСС) базируется на применении обобщенной полиадической системы (ОПС) счисления. Введение промежуточной системы счисления [1,3,4], позволяет изображать число А в виде

$$A = a_1 + a_2 p_1 + a_3 p_1 p_2 + \ldots + a_n p_1 \ldots p_{n-1} = \\ = \sum_{k=1}^{n} a_k q_{k-1}, \quad (1)$$

где a_k - цифры в полиадической системе счисления; $q_k = p_k q_{k-1}$ - вес цифры в ОПС (смешанный базис).

Если обеспечить соответствие между основаниями ОПС и основаниями системы классов вычетов, то справедливо равенство

$$A = (a_1(z), a_2(z), \ldots, a_n(z)) = \lfloor a_1(z), a_2(z), \ldots, a_n(z) \rfloor$$

На основании этого можно сделать вывод о возможности перевода кода класса вычетов в кодовую последовательность ОПС. При этом все процедуры должны осуществляться в модулярной арифметике.

Проведенный анализ основных реализаций вычислений коэффициента обобщенной полиадической системы счисления позволил выделить три основных подхода к построению нейросетевых устройств, предназначенных для выполнения этой немодульной операции.

Основу первого подхода составляют методы, базирующиеся на рекуррентном алгоритме вычисления коэффициентов [3,6], согласно которому

$$a_k = restA_k \,(\mathrm{mod}\, p_k), \quad (2)$$

где A_k определяется по рекуррентной формуле

$$A_k = (A_{k-1} - a_{k-1}) w_{k-1} \quad (3)$$

где $A_1 = A$; $w_k = p_k^j$ - формальная обратная величина k-ого основания по j-ому основанию (j ≠ k); a_{k-1}^{*} - набор остатков по всем модулям, номера которых выше номера k-1; k=1…n.

При этом все операции по вычислению коэффициента a_k производятся в системе классов вычетов [2,6].

Наряду с достоинствами, такими как параллельно-конвейерная организация вычислений и достаточно высокое быстродействие, очевидны и недостатки данной реализации. Основной недостаток – значительные аппаратные затраты, что затрудняет широкое применение данного метода перевода из непозиционной системы классов вычетов в обобщенную полиадическую систему, определяемую в расширенных полях Галуа.

Сократить аппаратные затраты позволяют методы, обеспечивающие основу второго подхода к построению устройства для преобразования ПСКВ в ОПС [4,6]. Алгоритм вычисления коэффициента ОПС по данному методу позволяет минимизировать аппаратные затраты, необходимые для выполнения этой немодульной операции [5,6]. Последовательное получение коэффициентов ОПС для заданного полинома А (z) по составным основаниям можно осуществить согласно выражения

$$a_i(z) = \left| \frac{\left| a_i(z) - \sum_{y=1}^{i=1} a_j(z) \cdot \prod_{k=1}^{j} p_k(z) \right|_{p_i(z)}^{+}}{\prod_{j=1}^{i=1} p_i(z)} \right|_{p_i(z)}^{+} \quad (4)$$

Принимая во внимание парную простоту модулей $p_i(z)$, где $i = \overline{1-n}$, можно заключить, что схемная реализация обладает пирамидальной структурой.