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 $A(z) \hat{I} GF(p^v)$ 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 $A(z) \hat{I} GF(p^n)$ 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

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

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

В общем виде любой базис можно представить в непозиционном виде как

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

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 $A(z) \hat{I} P(Z)$ можно представить как сумму ортогональных полиномов $A_1(z),A_2(z),...,A_n(z)$, т.е.

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

Под ортогональным полиномом понимается элемент расширенного поля $GF(p^n)$ 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 $GF(p^n)$ можно представить в следующем виде

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

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

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

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

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

9. 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.

10.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.

11.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.

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

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

14.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.

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