РАЗРАБОТКА ПРЕОБРАЗОВАТЕЛЯ МОДУЛЯРНОГО КОДА ПСКВ В ПОЗИЦИОННЫЙ КОД

Калмыков И.А., Петлеваный С.В., Тимошенко Л.И., Лисицын А.В.
Ставропольский военный институт связи Ракетных войск,
г. Ставрополь, Россия
kia762@yandex.ru, foxne@mail.ru

Качественно новые требования, предъявляемые к цифровой обработке сигналов (ЦОС) обусловили повышенный интерес к применению вычислительных систем, построенных на основе алгебраических систем, обладающим свойством конечного кольца или поля. Особое место среди них занимает полиномиальная система классов вычетов (ПСКВ), определяемых в расширенных полях Галуа $GF(2^v)$. Малоразрядность остатков и независимость их обработки служит идеальной основой для построения высокоскоростных специализированных процессоров (СП) ПСКВ [1,2]. В данной системе полином $A(z)$ представляется в виде

$$A(z) = (a_1(z), a_2(z), \mathbf{K}, a_n(z)), \qquad (1)$$

где $a_i(z) \equiv A(z) \bmod p_i(z)$, $p_i(z)$ – минимальный многочлен поля Галуа; $i = 1,2,...,n$.

Так как сравнения по одному и тому же модулю можно почленно складывать, вычитать и умножать [1], то выполнение операций над операндами в расширенном поле Галуа $GF(p^n)$ производятся независимо по каждому из модулей $p_i(z)$. Данные операции являются модульными.

Наряду с модульными операциями в ПСКВ выполняются и немодульные операции. Одной из таких операций является операция обратного преобразования из кода ПСКВ в код позиционной системы счисления (ПСС).

Как правило, данная операция базируется на китайской теореме об остатках (КТО). Преобразование $A(z) = (a_1(z), a_2(z), ..., a_n(z))$ в позиционный код осуществляется согласно условия

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

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

При этом любой элемент $A(z) \in P(z) = \prod_{i=1}^{n} p_i(z)$ можно представить как сумму ортогональных полиномов $A_1(z), A_2(z), ...A_n(z)$, т.е.

$$A(z) = (a_1(z), a_2(z), ..., a_n(z)) =$$

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

Под ортогональным полиномом понимается элемент поля $GF(p^v)$, у которого все остатки равны нулю, за исключением цифры по модулю $p_i(z)$

$$A_i(z) = (0, 0, ..., 0, a_i(z), 0, ...0), \quad (4)$$

где $i = 1,2,...,n$.

Приравнивая выражения (1) и (3), получаем, что

$$a_i(z) \cdot B_i(z) = (0, 0, ..., 0, a_i(z), 0, ...0). \quad (5)$$

Исходя из условия (2) имеем

$$(a_i(z) \cdot b_1^i(z), ..., a_i(z) \cdot b_i^i(z), ..., a_i(z) \cdot b_n^i(z)) = (0, 0, ..., a_i(z), ..., 0). \quad (6)$$

Тогда ортогональные базисы $B_i(z)$, $i = 1,2,...,n$ определяются как

$$\begin{aligned} &B_1(z) = (1, 0, ..., 0, ..., 0); \\ &\vdots \\ &B_i(z) = (0, 0, ..., 1, ..., 0); \\ &\vdots \\ &B_n(z) = (0, 0, ..., 0, ..., 1). \end{aligned} \quad (7)$$

Таким образом, выражение (1) можно записать как

$$A(z) = a_1(z)B_1(z) + ... + a_n(z)B_n(z) \bmod P(z) = \sum_{i=1}^{n} a_i(z)B_i(z) \bmod P(z). \quad (8)$$

Для получения значений ортогональных базисов ПСКВ должно выполняться условие

$$B_i(z)=\begin{cases}0 \bmod p_4(z), u \neq i \\ 1 \bmod p_4(z), u = i\end{cases}, \quad (9)$$

где $B_i(z)=m_i(z)\prod\limits_{\substack{u=1\\u\neq i}}^{n} p_u(z)$; $m_i(z)\cdot\prod\limits_{\substack{u=1\\u\neq i}}^{n} p_u(z)\equiv 1 \bmod p_i(z)$.

Преобразуя выражение (9), получаем

$$B_i(z)=m_i(z)\cdot P(z)/\ p_i(z), \quad (10)$$

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

Вес ортогонального базиса выбирается из условия

$$B_i(z) \bmod p_i(z)\equiv 1$$

Для определения значений ортогональных базисов $B_i(z)\ \ i=1,2,...,n$ для системы ПСКВ воспользуемся следующим алгоритмом:

1. На первом этапе осуществляется вычисления значения

$$P_i^*(z)=\frac{P(z)}{p_i(z)}=\prod_{\substack{u=1\\u\neq i}}^{n} p_u(z)$$

2. Так величина $P_i^*(z)$ составлена из множителей, взаимно простых с $p_i(z)$, то определяется значение остатка

$$d_i(z)=rest(P_i^*/\ p_i(z)). \quad (11)$$

3. В соответствии с условием (17) выбирается значение $m_i(z)$, такое что выполняется условие

$$m_i(z)d_i(z) \bmod p_i(z)\equiv 1. \quad (12)$$

4. Вычисляется значение ортогонального базиса

$$B_i(z)=m_i(z)P_i^*(z). \quad (13)$$

Рассмотрим структуру НС, осуществляющей перевод кода ПСКВ в двоичный позиционный код на основе китайской теоремы об остатках.

Отсутствие межразрядных связей при вычислении результата преобразования позволяет свести выражение (16) к виду

$$x(z)=\left|\sum_{i=1}^{s}\left|2^j a_i^j(z)\right|_{p(z)}^{+}\right|_{p(z)}^{+}, \quad (24)$$

где j - разряд i-го остатка $a_i(z)$ по модулю $p_i(z)$.

Пример. Разработать структуру нейронной сети, выполняющей перевод кода ПСКВ в позиционный двоичный код для поля $GF(2^3)$.

Структура НС, реализующей преобразование из ПСКВ в позиционную для $GF(2^3)$ представлена на рисунке 1. Входной слой сети состоит из 7 нейронов, распределенных по группам соответственно структуре 1-3-3. Данные нейроны осуществляют разветвление входного вектора $(a_1(z), a_2(z), a_3(z))$, представленного в двоичной форме.

Синаптические веса связей между первым и вторым слоями равны 1. Выходной слой содержит 7 сумматоров по модулю два, реализованных на основе модели представленной в работе [1].

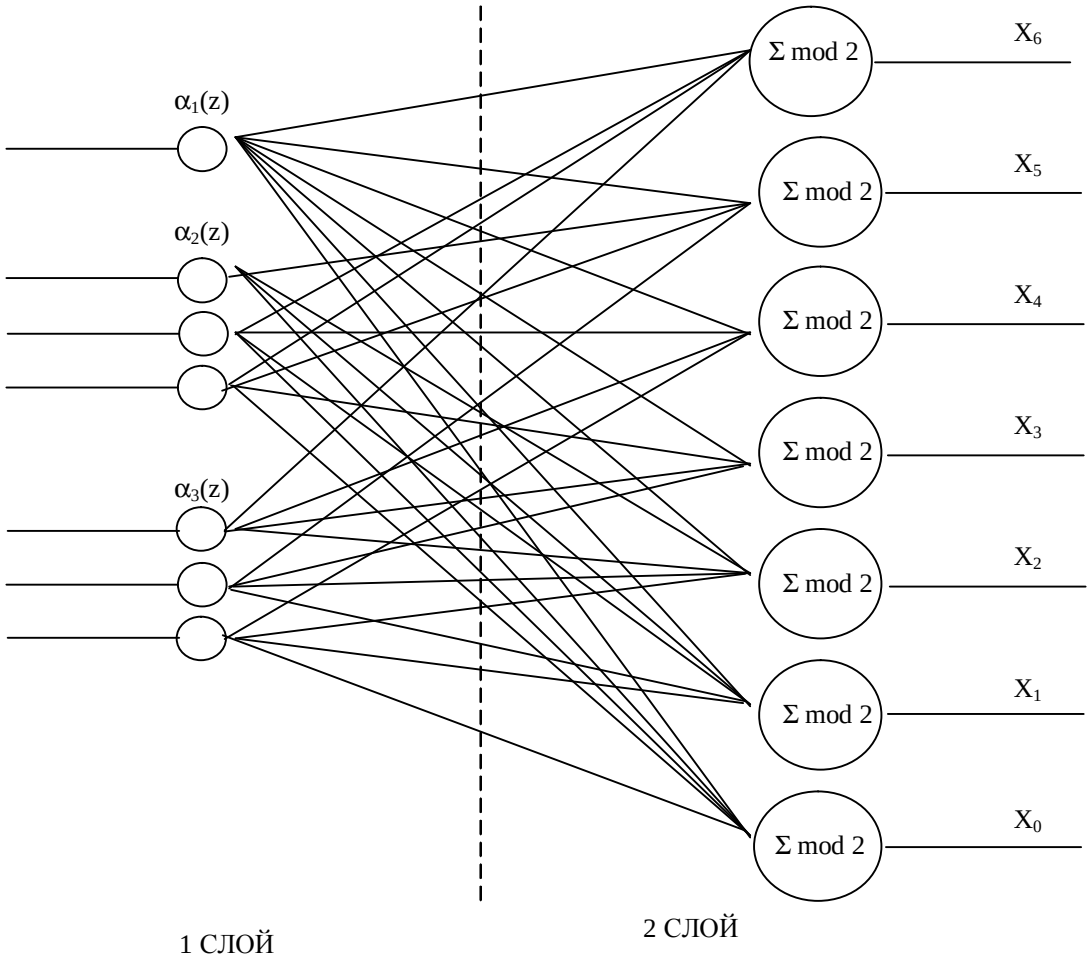

Рисунок 1– Структура преобразователя из ПСКВ в ПСС для $GF(2^3)$

Данная структура характеризуется отсутствием выходного сумматора по модулю $P(z) = \prod_{i=1}^{3} p_i(z) = z^7 + 1$, а, следовательно, и обратных связей, что

в значительной степени приведет к повышению быстродействия системы в целом. Проведенный анализ матрицы синаптических весов показал, что для реализации устройства преобразования кода ПСКВ в ПСС для поля $GF(2^3)$ потребуется:

- 3-входовых сумматоров по модулю 2 – 1;
- 4-входовых сумматоров по модулю 2 – 3;
- 5-входовых сумматоров по модулю 2 – 3;

Следует отметить, что разработанное устройство обратного преобразования из кода ПСКВ, обладает высоким быстродействием - процедура перевода осуществляется за одну итерацию на основе НС прямого распространения.

Литература

1. 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.
2. 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.
3. Элементы применения компьютерной математики и нейроинформатики/Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.