УДК 681.3

МОДЕЛЬ И СТРУКТУРА НЕЙРОННОЙ СЕТИ ДЛЯ РЕАЛИЗАЦИИ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ В РАСШИРЕННЫХ ПОЛЯХ ГАЛУА

к.т.н. И.А. Калмыков, Ю.О. Щелкунова, В.Р. Гахов,
Д.В. Горденко, к.т.н. В.И. Новиков
(представил д.т.н., проф. В.Д. Дмитриенко)

Исследован вопрос реализации цифровой обработки сигналов (ЦОС) в расширенных полях Галуа GF(p^v). Показано, что применение полиноминальной системы класса вычетов позволит повысить не только точность, но и скорость обработки данных. Представлена структура нейронной сети, реализующая ЦОС в полях Галуа.

Постановка задачи. Дискретное преобразование Фурье (ДПФ) является в настоящее время базовой основой большинства методов цифровой обработки сигналов (ЦОС). Одним из основных недостатков ДПФ является значительная аддитивная погрешность, определяемая иррациональностью значений поворачивающих коэффициентов. Реализация ЦОС в расширенных полях Галуа GF(p^v) на основе полиномиальной системы класса вычетов (ПСКВ) позволяет обеспечить не только высокую точность обработки сигналов, но и высокое быстродействие спецпроцессора ЦОС.

Анализ исследований в данной области. При решении многих практических задач цифровой обработки сигналов необходимо осуществлять ортогональные преобразования над входной последовательностью дискретных отсчетов GF(p^v). Такие преобразования, как правило, определены над полем комплексных чисел и называются дискретным преобразованием Фурье, которое определяется выражениями:

$$X(\kappa)=\sum_{n=0}^{N-1} x(n)\cdot W^{\kappa n}\,; \tag{1}$$

$$x(n)=\frac{1}{N}\cdot\sum_{\kappa=0}^{N-1} X(\kappa)\cdot W^{-\kappa n}\,, \tag{2}$$

где $W=\exp\left(-2\,\pi\, j\,/\,N\right)$ – поворачивающий коэффициент; $x(n)$ – количество отсчетов; κ = 0, … , N–1; n = 0, 1, … , N–1.

Известно, что реализация прямого и обратного ДПФ предопределяет значительные погрешности при вычислении значений спектральных коэффициентов в поле комплексных чисел. Это, прежде всего, обусловлено тем, что поворачивающие коэффициенты $W^{\kappa n}$ представляют собой иррациональные числа, а это при значительных значениях N приводит к существенной аддитивной арифметической погрешности. Поэтому для уменьшения среднеквадратической погрешности необходимо определить алгоритм ортогонального преобразования входного вектора $x(n)$, в котором бы не использовались операции поля комплексных чисел.

С этой точки зрения наиболее привлекательными являются преобразования, определенные над расширенным полем Галуа $GF\left(p^{\nu}\right)$, где p – простое, а ν – положительное целое число. Известно [1], что данное поле содержит $p^{\nu}-1$ ненулевых элементов, которые образуют циклическую мультипликативную группу. Следовательно, в этой группе должен существовать хотя бы один элемент d, который являлся бы делителем. Если $p^{\nu}-1$ представляет собой простое число, то значение $d=p^{\nu}-1$.

Пусть β является элементом порядка k в мультипликативной группе ненулевых элементов $GF\left(p^{\nu}\right)$. Тогда (1) можно преобразовать к виду

$$X(k)=\sum_{n=0}^{d-1} x(n)\cdot\beta^{\kappa n}\ ,\ k=0,1,\ldots,d-1\ . \tag{3}$$

Выражение (3) описывает преобразование входной последовательности отсчетов $x(n)$, являющихся элементами расширенного поля Галуа $GF\left(p^{\nu}\right)$ в последовательность «частотных» составляющих $X(\kappa)$, определенных над этим же полем.

Преобразование обратное (3), т.е. эквивалентное множество уравнений, позволяющих определить входной вектор $x(n)$ через совокупность спектральных составляющих $X(\kappa)$, определяется выражением

$$x(n)=-d^{*}\cdot\sum_{\kappa=0}^{d-1} X(\kappa)\cdot\beta^{-\kappa n}\ ,\ n=0,1,\ldots,d-1\ , \tag{4}$$

где d^{*} – целое число, удовлетворяющее условию

$$d^{*}\cdot d=p^{\nu}-1\ . \tag{5}$$

Анализ выражений (3) и (4) показывает, что полученное преобразование аналогично ДПФ комплексной области и действует в пространстве циклической группы порядка d, определенной полем $GF\left(p^{\nu}\right)$. Так как $\beta^{\kappa n}$ и $x(n)$ представляют собой целочисленные элементы расширенного поля Галуа, то при реализации выражений (3) и (4) будут полностью отсутствовать шумы округления. В результате этого оценка спектральных составляющих с помощью ортогональных преобразований (3) и (4) будет более точной по сравнению с ДПФ.

Итак, ***целью настоящей статьи*** *является доказательство того, что применение полиноминальной системы класса вычетов позволит не только повысить точность, но и скорость обработки данных, а также представить структуру нейронной сети, реализующей ортогональные преобразования сигналов в расширенных полях Галуа* $GF(p^{\nu})$.

Рассмотрим реализацию ортогональных преобразований в расширенном поле Галуа $GF(2^3)$. Данное поле задается порождающим полиномом $f(x)=x^3+x+1$, а его элементы имеют следующий вид:

$$0 = 000 = 0;\ \beta^0 = 001 = 1;\ \beta^1 = 010 = x;\ \beta^2 = 100 = x^2;$$
$$\beta^3 = 011 = x+1;\ \beta^4 = 110 = x^2+x;\ \beta^5 = 111 = x^2+x = 1;\ \beta^6 = 101 = x^2+1.$$

Так как $p^{\nu}-1=2^3-1=7$ является простым числом, то для него существует единственное число $d=7$, определяющее длину входной последовательности.

Пусть дана последовательность $x(n)=\{0,1,2,0,1,0,0\}$. Представим ее в двоичном виде $x(n)=\{000, 001, 010, 000, 001, 000, 000\}$.

Исходя из условия возможности представления квантованных значений $x(n)$ в виде элементов расширенного поля Галуа β, получаем входной вектор $x(n)=\left\{0, \beta^0, \beta, 0, \beta^0, 0, 0\right\}$.

Преобразуем выражение (3) к матричному виду. Тогда значения спектральных составляющих можно представить

$$X(\kappa)=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta & \beta^4 \\ 1 & \beta^4 & \beta & \beta^5 & \beta^2 & \beta^6 & \beta^3 \\ 1 & \beta^5 & \beta^3 & \beta & \beta^6 & \beta^4 & \beta^2 \\ 1 & \beta^6 & \beta^5 & \beta^4 & \beta^3 & \beta^2 & \beta \end{bmatrix} \times \begin{bmatrix} 0 \\ \beta^5 \\ \beta \\ 0 \\ \beta^0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \beta \\ \beta^5 \\ \beta^0 \\ \beta^6 \\ \beta^4 \\ \beta^2 \\ \beta^3 \end{bmatrix}. \qquad (6)$$

Следует отметить, что операции сложения при вычислении выходного вектора $X(\kappa)=\begin{bmatrix}\beta & \beta^5 & \beta^0 & \beta^6 & \beta^4 & \beta^2 & \beta^3\end{bmatrix}^T$ выполнялись по модулю 2 простого поля Галуа $GF(2)$, а операции умножения – по модулю порождающего полинома $f(x)=x^3+x+1$. Получение частного спектра входной последовательности $x(n)$ в расширенном поле β, как наглядно видно из выражения (6), потребовало 36 операций умножения и 42 операции сложения по модулю 2.

Для осуществления обратного преобразования необходимо воспользоваться выражением (4), предварительно определив значение обратного элемента d*. Согласно равенству (5) он равен единице, т.е. $d^*=1$. Тогда выражение (4) в матричной форме примет следующий вид:

$$x(n)=1\cdot\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & \beta^6 & \beta^5 & \beta^4 & \beta^3 & \beta^2 & \beta^1\\ 1 & \beta^5 & \beta^3 & \beta & \beta^6 & \beta^4 & \beta^2\\ 1 & \beta^4 & \beta & \beta^5 & \beta^2 & \beta^6 & \beta^3\\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta & \beta^4\\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5\\ 1 & \beta^1 & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6\end{bmatrix}\times\begin{bmatrix}\beta\\ \beta^5\\ \beta^0\\ \beta^6\\ \beta^4\\ \beta^2\\ \beta^3\end{bmatrix}=\begin{bmatrix}0\\ \beta^0\\ \beta\\ 0\\ \beta^0\\ 0\\ 0\end{bmatrix}. \qquad (7)$$

Полученный результат свидетельствует о том, что ортогональное преобразование в расширенном поле Галуа обладает свойством обратимости. Можно доказать, что данное преобразование, как и ДПФ, характеризуется свойством линейности и цикличности свертки. Следовательно, ортогональное преобразование в $GF(p^v)$ можно применять для реализации задач ЦОС, обеспечивая при этом высокую точность результата за счет обработки целочисленных значений.

В подавляющем большинстве приложений задача ЦОС сводится к нахождению значений ортогонального преобразования конечной реализации сигнала для большого числа точек [2]. Известно, что для вычисления спектрального образа входной последовательности требуется выполнение N^2 операций умножения, где N – длина входной последовательности $x(n)$.

Лучшие скоростные показатели получаются при использовании так называемых быстрых алгоритмов, которые существуют для многих частных случаев ортогональных преобразований. Однако, для ортогональных преобразований в расширенных полях Галуа $GF\left(p^{\nu}\right)$ такие алгоритмы не были разработаны [3]. Для повышения эффективности реализации задач ЦОС целесообразно обработку одномерных сигналов свести к обработке многомерных сигналов [1, 3].

Отправной точкой при решении данной проблемы является изоморфизм, порожденный теоремой теории чисел, называемой китайской теоремой об остатках (КТО). Согласно данной теореме, если $P = p_1 \cdot p_2 \cdot \ldots \cdot p_n = \prod_{i=1}^{n} p_i$ и p_i – простые числа, то кольцо Z_P класса вычетов по модулю P изоморфно прямой сумме $GF(p_1) + GF(p_2) + \ldots + GF(p_s)$ конечных полей $GF(p_i)$:

$$Z_P \sim GF(p_1) + GF(p_2) + \ldots + GF(p_s) \ . \tag{8}$$

Основным преимуществом $GF(p_1) + GF(p_2) + \ldots + GF(p_s)$ – арифметики является возможность организации параллельных вычислений и, следовательно, значительное повышение быстродействия арифметических устройств.

Дальнейшим обобщением ортогональных преобразований над прямой суммой полей $GF(p_i)$ являются преобразования (3) и (4), определенные над расширенным полем Галуа $GF\left(p^{\nu}\right)$. Если в качестве оснований новой алгебраической системы выбрать минимальные многочлены $p_i(z)$ поля $GF\left(p^{\nu}\right)$, то любой полином $A(z)$, удовлетворяющий условию

$$A(z) \in P_{пол},$$

где

$$P_{пол} = \prod_{i=1}^{n} p_i(z) = z^{p^{\nu}-1} - 1 , \tag{9}$$

можно представить в виде n-мерного вектора

$$A(z) = \left(\alpha_1(z), \alpha_2(z), \ldots, \alpha_n(z)\right), \tag{10}$$

где $\alpha_i(z) = \mathrm{rest}\left(A(z)/p_i(z)\right)$, $i = 1, 2, \ldots, n$.

Так как сравнения по одному и тому же модулю можно почленно складывать, вычитать и умножать [4], то для суммы, разности и произведения двух полиномов $A(z)$ и $B(z)$, имеющих соответственно модулярные коды $\left(\alpha_1(z), \alpha_2(z), \ldots, \alpha_n(z)\right)$ и $\left(\beta_1(z), \beta_2(z), \ldots, \beta_n(z)\right)$ справедливы соотношения по операциям сложения, вычитания и умножения по модулю.

Таким образом, выполнение операций над операндами в расширенном поле Галуа $GF\left(p^{\nu}\right)$ производится независимо по каждому из модулей $p_i(z)$, что указывает на параллелизм данной алгебраической системы.

Рассмотрим пример. Пусть задано расширенное поле Галуа $GF\left(2^3\right)$. Для данного поля определены минимальные многочлены $p_1(z) = z + 1$; $p_2(z) = z^3 + z^2 + 1$; $p_3(z) = z^3 + z + 1$. Найдем сумму и произведение двух полиномов $A(z) = z^4 + z^3 + z$ и $B(z) = z^2 + z + 1$. Данные полиномы принадлежит диапазону $P(z)$, который определяется следующим выражением:

$$P(z) = \prod_{i=1}^{3} p_i(z) = (z+1) \cdot (z^3 + z^2 + 1) \cdot (z^3 + z + 1) = z^7 + 1 .$$

Представим полиномы в виде модулярного кода по основаниям $p_1(z)$, $p_2(z)$, $p_3(z)$. Тогда $A(z) = (1, 0, z^2 + z + 1)$, а $B(z) = (1, z^2 + z + 1, z^2 + z + 1)$.

Сумма двух полиномов в $GF\left(2^3\right)$:

$$C(z) = A(z) + B(z) = (z^4 + z^3 + z) + (z^2 + z + 1) = z^4 + z^3 + z^2 + 1 = (0, z^2 + z + 1, 0) .$$

Реализуем данную операцию, используя модулярное представление операндов:

$$\begin{array}{cl} & A(z) = (1, 0, z^2 + z + 1) \\ + & \underline{B(z) = (1, z^2 + z + 1, z^2 + z + 1)} \\ & C(z) = (0, z^2 + z + 1, 0) \end{array}$$

Следует отметить, что операции сложения и вычитания в расширенных полях Галуа $GF\left(p^{\nu}\right)$ выполняются по модулю p, то есть в рассмотренном примере по модулю 2.

Выполним операцию умножения данных полиномов

$$C(z) = \left|A(z) \cdot B(z)\right|_{p(z)}^{+} = (z^4 + z^3 + z) \cdot (z^2 + z + 1) = z^6 + z^2 + z = (1, 0, z + 1) .$$

Реализуем данную операцию, воспользовавшись китайской теоремой об остатках. Тогда

$$\times \begin{array}{l} A(z) = (1, 0, z^2 + z + 1) \\ \underline{B(z) = (1, z^2 + z + 1, z^2 + z + 1)} \\ C(z) = (1, 0, z + 1) \end{array},$$

где $\left|(z^2 + z + 1) \cdot (z^2 + z + 1)\right|^+_{p_3(z)} = \left|z^4 + z^2 + 1\right|^+_{p_3(z)} = z + 1$.

Из приведенного примера видно, что выполнение операции сложения и умножения в полиномиальном виде и в виде кода ПСКВ дает один и тот же результат. При этом порядок операндов $A(z)$ и $B(z)$ был уменьшен более чем в 2 раза, что является базовой предпосылкой для построения высокоскоростных вычислительных устройств ЦОС.

Одной из основных операций вычислений с использованием кодов ПСКВ в расширенных полях Галуа $GF\left(p^{\nu}\right)$ является приведение исходного полинома $X(z)$ по модулю $p_i(z)$, $i = 1, 2, ..., n$, т.е. нахождение остатка от деления $X(z)$ на $p_i(z)$. В работе [5] представлен итеративный алгоритм получения остатка числа по модулю p, который задается выражением

$$X(j+1) = \sum_{i=0}^{[\log_2 x(j)]} \left|2^i\right|_p \left\{x_{ij}\right\}^i \quad , \tag{11}$$

где $j = 0, 1, 2, ...$ – значение номера итерации. При многократном применении (11) алгоритм сойдется в конечную форму, которая будет сравнима с начальным значением X по модулю p.

Основным недостатком данного алгоритма является низкое быстродействие системы из-за необходимости выполнения операции сложения на каждой итерации. Кроме того, существует необходимость проверки условий окончания процесса по контролю знака полученной разницы в операции, что также значительно снижает производительность системы.

Для устранения указанных недостатков в [6] был предложен алгоритм, реализующий обработку данных по модулю p на основе нейронной сети (НС) прямого распространения. Отказ от обратных связей предопределил переход от двухслойной структуры НС к многослойной. Причем число слоев нейронной сети прямого распространения определяется количеством необходимых итераций, а количество нейронов в каждом слое – разрядностью обрабатываемых данных на итерации, соответствующих номеру слоя.

Замена обратных связей на прямые позволила повысить скорость обработки данных за счет возможности организации конвейерных вычислений, но, с другой стороны, значительно увеличила аппаратурные затраты.

Одним из важнейших свойств кодов ПСКВ, определенных в расширенных полях Галуа $GF(p^{\nu})$, является отсутствие межразрядных переносов при вычислении результата по модулю $p(z)$. Это позволяет свести операцию итеративного получения остатка к однотактовой процедуре, преобразовав выражение (11) к виду

$$\alpha_i(z) = \left| \sum_{j=0}^{p^{\nu}-1} \left| \left|2^j\right|^{+}_{p_i(z)} \cdot x(j) \right|^{+}_{p_i(z)} \right|^{+}_{p}, \qquad (12)$$

где $i = 0, 1, 2, \ldots, s$ – количество оснований кода ПСКВ, j – разряд исходного числа.

При этом нейронная сеть будет содержать только два слоя. Нейроны входного слоя не выполняют вычислительных функций, а служат лишь для разветвления входов. Нейроны второго слоя осуществляют процедуру вычисления остатка по модулю $p_i(z)$. Разрядность входных данных определяется расширением поля $GF(p^{\nu})$ и составляет m разрядов, где $m = p^{\nu} - 1$. Таким образом, в состав первого слоя входит m нейронов. Второй слой нейронной сети содержит l сумматоров по модулю два, где l – порядок полинома $p_i(z)$. Данный элемент довольно легко реализуется на основе l-входового персептрона, структура которого представлена в работе [7]. На рис. 1 представлена структура НС для модуля $p(z) = z^3 + z + 1$ расширенного поля Галуа. Ее анализ позволяет сделать вывод о том, что выходы j-го нейрона первого слоя являются пространственным представлением β^j-го элемента расширенного поля $GF(2^3)$.

Таким образом, преобразование исходного полинома по модулю $p_i(z)$ сводится к сумме элементов поля $GF(p^{\nu})$ соответствующих ненулевым разрядам полинома. Другими словами, справедливо выражение

$$\alpha_i(z) = \left| \sum_{j=0}^{p^{\nu}-1} x(j) \cdot \beta^j \right|^{+}_{p_i(z)}, \qquad (13)$$

где $x(j) = \{0, 1\}$ – разряды полинома $X(z)$.

Восстановление полученного результата из непозиционной ПСКВ к двоичному позиционному виду производится на основе КТО согласно

$$x(z) = \sum_{i=1}^{s} B_i(z) \cdot \alpha_i(z) \bmod p(z), \qquad (14)$$

где s – количество оснований ПСКВ; $p(z)$ – диапазон; $B_i(z)$ – ортогональный базис по i-му основанию. При этом

$$B_u(z) \equiv \begin{cases} 0 \bmod p_i(z), \\ 1 \bmod p_i(z) \end{cases} i \neq u\ ; \tag{15}$$

$$B_i(z) \equiv T_i(z) \cdot \prod_{i=1}^{s} p_i(z)\ . \tag{16}$$

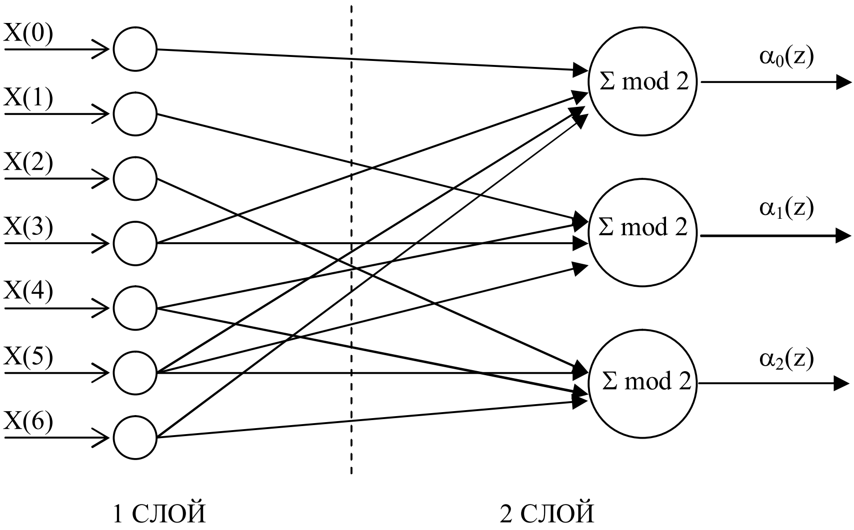

Рис. 1. Структура НС определения остатка по модулю $p(z) = z^3 + z + 1$

Так для расширенного поля Галуа $GF(2^3)$, задаваемого взаимнопростыми основаниями $p_1(z) = z+1$; $p_2(z) = z^3 + z^2 + 1$; $p_3(z) = z^3 + z + 1$, ортогональные базисы определяются соответственно:

$B_1(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$; $B_2(z) = z^6 + z^5 + z^3 + 1$; $B_3(z) = z^4 + z^2 + z + 1$.

Тогда обратное преобразование полинома $A(z) = (1, 0, z^2 + z + 1)$ согласно (14) имеет вид

$$A(z) = \sum_{i=1}^{3} B_i(z) \cdot \alpha_i(z) \bmod (z^7 + 1) = ((1 \cdot (z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) +$$

$$+ 0 \cdot (z^6 + z^5 + z^3 + 1) + (z^2 + z + 1) \cdot (z^4 + z^2 + z + 1)) \bmod (z^7 + 1) = z^4 + z^3 + z\ .$$

Отсутствие межразрядных связей при вычислении результата преобразования позволяет свести выражение (17) к виду

$$x(z) = \left| \sum_{i=1}^{s} \right| \cdot \left| 2^{j} \cdot \alpha_i^j(z) \right|_{p(z)}^{+} \Big|_{p}^{+}, \tag{17}$$

где j – разряд i-го остатка $\alpha_i(z)$ по модулю $p_i(z)$.

Структура НС, реализующей преобразование из ПСКВ в позиционную для $GF\left(2^3\right)$, представлена на рис. 2.

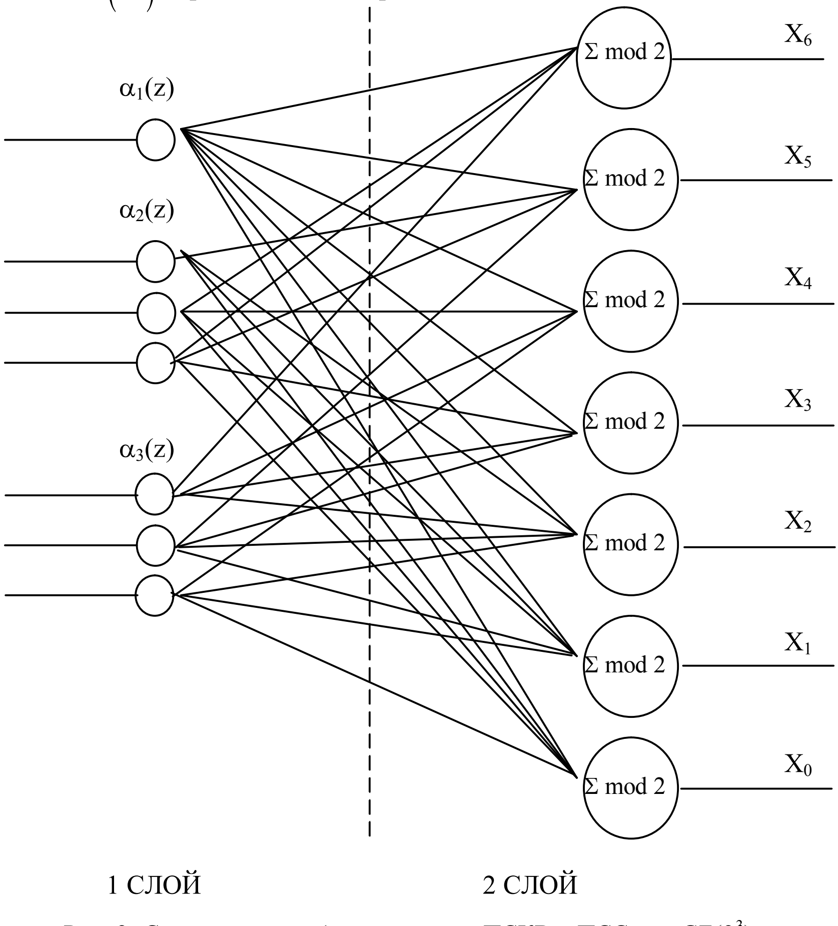

Рис. 2. Структура преобразователя из ПСКВ в ПСС для $GF(2^3)$

Входной слой сети состоит из 7 нейронов, распределенных по группам соответственно структуре 1-3-3. Данные нейроны осуществляют разветвление входного вектора $(\alpha_1(z), \alpha_2(z), \alpha_3(z))$, 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 персептрона. Для удобства определения связей слева представлены результаты умножения j-го разряда $\alpha_i(z)$ остатка на значение $B_i(z)$, выраженные в полиномиальной форме.

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.

Параллельный алгоритм вычисления ортогональных преобразований в расширенных полях Галуа $GF\left(p^{\nu}\right)$ легко реализуется на НС прямого распространения. Если число входов (синоптических весов) нейронов, используемых для организации и функционирования НС, согласовано с числом модулей ПСКВ, то нейронная сеть становится натуральным представлением ПСКВ.

В этом случае такая НС представляет собой многослойную сеть прямого распространения, состоящую из трех подсетей. Первая подсеть осуществляет преобразование p^{ν}-разрядного сигнала в s-размерный вектор $\left(\alpha_1(z),\alpha_2(z),\ldots,\alpha_s(z)\right)$, определяемый остатками от деления исходного полинома $X(z)$ на модули $p_i(z)$, $i=0,1,2,\ldots,s$. Полученные остатки подаются на нейроны второй подсети. Синаптические веса входов нейронов определяются, исходя из условия (3), и представляют собой значения $\left|\beta^j\right|^{+}_{p_i(z)}$. На выходе данной подсистемы формируются значения спектральных составляющих, которые затем подаются на входы третьей подсистемы НС. Нейроны последней подсистемы осуществляют перевод из непозиционной алгебраической системы ПСКВ в позиционную полиномиальную форму. Структура НС, реализующей ортогональные преобразования в расширенном поле Галуа, представлена на рис. 3.

Синтезированная нейронная сеть обеспечивает высокую эффективность при решении задач ЦОС повышенной размерности. Рассмотренный метод реализации ортогонального преобразования является одним из наиболее перспективных методов цифровой обработки сигнала в реальном масштабе времени. Кроме того, этот метод обеспечивает высокую точность вычислений.

Следует отметить, что в плане аппаратурной реализации предложенная математическая модель ортогонального преобразования над расширенным полем Галуа $GF(p^v)$ довольно удачно сочетается с параллельно-конвейерной структурой нейронных сетей. Для исследования процессов, ортогональных преобразований в расширенных полях Галуа $GF(p^v)$ была разработана имитационная модель. В качестве исходных данных были выбраны:

– разрядность обрабатываемых данных – 8 бит;

– расширенное поле Галуа $GF(2^3)$.

Проведенные исследования показали, что применение ортогональных преобразований в $GF(2^3)$ на основе ПСКВ позволило повысить производительность вычислительного устройства более чем на 10 %.

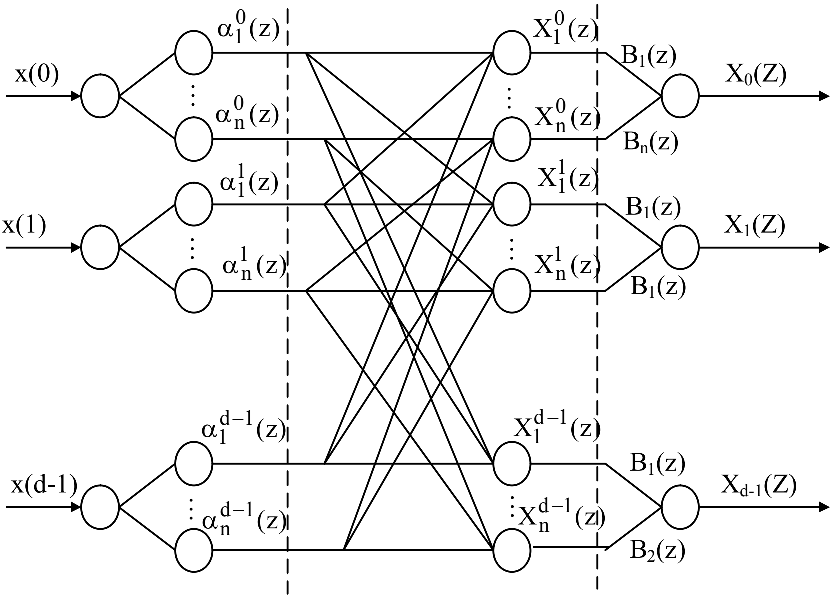

Рис. 3. Структура НС, реализующей ортогональное преобразование в $GF(p^v)$

Выводы. Показано, что реализация цифровой обработки сигналов в полях Галуа позволяет обеспечить высокую точность вычисления. Кроме того, применение ПСКВ является основой для построения высокоскоростных вычислительных систем цифровой обработки сигналов. Представлена модель и структура нейронной сети, реализующей цифровую обработку сигналов в расширенных полях Галуа. Полученные результаты имеют важное практическое значение, так как позволяют поднять аппаратные средства для цифровой обработки сигналов на качественно более высокую ступень.

ЛИТЕРАТУРА

1. *Абстрактные алгебраические системы и цифровая обработка сигналов / Вариченко Л.В., Лабунец В.Г., Раков М.А. – К.: Наук. думка, 1986. – 248 с.*
2. *Техническое обеспечение цифровой обработки сигналов. Справочник / Куприянов М.С. и др. – С.-Пб.: Форт, 2000. – 752 с.*
3. *Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов / Пер. с англ. Под ред. Ю.Н. Александрова – М.: Мир, 1978. – 848 с.*
4. *Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 440 с.*
5. *Червяков Н.И., Шапошников А.В., Сахнюк П.А. Модель и структура нейронной сети для реализации арифметики системы остаточных классов // Нейрокомпьютеры: разработка и применение. – М.: МПРЖР. – 2001. – № 10. – С. 6 – 12.*
6. *Червяков Н.И., Шапошников А.В., Сахнюк П.А. Оптимизация структуры нейронных сетей конечного кольца // Нейрокомпьютеры: разработка и применение. – М.: МПРЖР, 2001. – № 10. – С. 13 – 18.*
7. *Каллан Р. Основные концепции нейронных сетей: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 288 с.*

Поступила 22.01.2003

КАЛМЫКОВ Игорь Анатольевич *– кандидат технических наук, доцент, зам. нач. кафедры информатики и информационных технологий в системах управления филиала Ростовского военного института РВ (г. Ставрополь). Области научных интересов – нейронные сети, системы остаточных классов, параллельные вычисления в полях Галуа.*

ЩЕЛКУНОВА Юлия Олеговна *– инженер-электрик научно-вычислительной лаборатории филиала Ростовского военного института РВ (г. Ставрополь). Области научных интересов – нейронные сети, параллельные вычисления в полях Галуа.*

ГАХОВ Вячеслав Романович *– курсант ВКА им. Можайского (г. Санкт-Петербург). Область научных интересов – нейронные сети.*

ГОРДЕНКО Дмитрий Владимирович *– адъюнкт кафедры информатики и информационных технологий в системах управления филиала Ростовского военного института РВ (г. Ставрополь). Области научных интересов – нейронные сети, системы остаточных классов.*

НОВИКОВ Владимир Иванович, *кандидат технических наук, заместитель начальника кафедры ХИ ВПС. Окончил в 1983 году ХВВКИУ, в 1994 году – ВА им. Дзержинского. Область научных интересов – системы управления и связи.*