УДК 681.3

НЕЙРОСЕТЕВАЯ РЕАЛИЗАЦИЯ ОПЕРАЦИЙ МОДУЛЯРНОГО ПОЛИНОМИАЛЬНОГО КОДА

Шилов А.А., Юртаев М.В., Калмыков М.И.

ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Использование непозиционных систем счисления позволяет повысить скорость выполнения арифметических операций. В качестве оснований таких систем счисления могут выступать неприводимые полиномы. В работе рассмотрены вопросы реализации модульных операций в модулярном полиномиальном коде (МПК). Представлена нейросетевая реализация этих модульных операций. Применение нейронных сетей позволяет обеспечить параллельную обработку данных. Разработана схема многовходового сумматора по модулю два, построенного на основе нейронных сетей. Показано, что полученный сумматор характеризуется минимальными аппаратурными и временными затратами.

Ключевые слова: остатки, модулярный полиномиальный код, модульные операции, нейронные сети, многовходовые сумматоры по модулю два

NEURAL NETWORK SALES OPERATIONS MODULAR POLYNOMIAL CODE

Shilov A.A., Yurtaev M.V., Kalmykov M.I.

North-Caucasian federal university, Stavropol, e-mail: kia762@yandex.ru

Using nonpositional value systems can improve the speed of an arithmetic operation. As the base value of such systems can act irreducible polynomials . The paper discusses the issues of implementation of modular operations in the modular polynomial code (MPC) . Presented neural network implementation of these modular operations. The use of neural networks enables parallel processing . A scheme for multi-input adder modulo two constructed based on neural networks . It is shown that the resulting adder is characterized by minimal governmental instrumental and time-consuming .

Keywords: residues modular polynomial code, modular operations, neural networks, multi-input adders modulo two

Использование параллельных модулярных кодов позволяет повысить скорость обработки данных. Применение арифметики над малоразрядными остатками обеспечивает обработку информации в реальном масштабе времени. Дальнейшее повышение скорости цифровой обработки сигналов возможно за счет использования параллельной элементной базы, которая по своему характеру и организации вычислений совпадала с модулярными полиномиальными кодами

Среди непозиционных модулярных кодов особое место занимают модулярные полиномиальные коды (МПК). В данных кодах в качестве оснований системы используют неприводимые полиномы [1-5]. Обладая высокой скоростью обработки информации, такие коды нашли широкое применение в различных областях. Так в работах [1-3] показана реализация методов цифровой обработки сигналов (ЦОС) с использованием модулярного полиномиального кода. Малоразрядность остатков, выполнение вычислений по параллельным каналам, определяемых основаниями МПК, позволяют обеспечить цифровую обработку сигналов в реальном масштабе времени. Применения МПК в области защиты данных от несанкционированного доступа приведены в работах [4-6]. Использование кодов МПК позволяет повысить степень защиты данных от НСД за счет использования нелинейных алгоритмов зашифрования, которые базируются на операциях умножения и возведении в степень по модулю. Использование модулярных полиномиальных кодов для построения отказоустойчивых вычислительных систем ЦОС показано в работах [7-10]. Использование контрольных оснований позволяет разрабатывать эффективные алгоритмы поиска и коррекции ошибок, которые возникают в процессе функционирования специализированных процессоров из-за отказов и сбоев оборудования.

В основу всех данных реализаций положены математические основы построения полиномиальных непозиционных кодов. Если в качестве модулей алгебраической системы, на основе которой базируются модулярные полиномиальные коды, выбрать минимальные многочлены $p_i(z)$ поля $GF(p^{\nu})$, то любой полином $A(z)$, удовлетворяющий условию $A(z) \in P_{\text{пол}}$, где

$$P_{\text{пол}} = \prod_{i=1}^{n} p_i(z), \qquad (1)$$

можно представить в виде n-мерного вектора

$$A(z) = \left(\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)\right), \quad (2)$$

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

Рассмотрим выполнение арифметических операций в модулярном полиномиальном коде. Представим значения остатков операндов в виде полиномиальной записи.

Пусть степень минимального многочлена $p_i(z), i = 1, ..., n$, равна mi. Тогда остаток можно представить

$$\alpha_i(z) = \alpha^i_{m_i-1} z^{m_{i-1}} + \alpha^i_{m_i-2} z^{m_{i-2}} + ... + \alpha^i_1 z^1 + \alpha_0 . \quad (3)$$

Соответственно для второго операнда получаем

$$i = 0, ..., n . \quad (4)$$

Так как сравнения по одному и тому же модулю можно почленно складывать, то для суммы двух полиномов $A(z)$ и $B(z)$, имеющих соответственно коды $\left(\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)\right) \rightarrow$ и $\left(\beta_1(z), \beta_2(z), ..., \beta_n(z)\right)$ справедливы соотношения:

$$\left|A(z) + B(z)\right|^+_{p(z)} = \left(\left|\alpha_1(z) + \beta_1(z)\right|^+_{p_1(z)}, ..., \left|\alpha_n(z) + \beta_n(z)\right|^+_{p_n(z)}\right) =$$

$$= \left(\alpha^1_0 \oplus \beta^1_0, \sum_i (\alpha^2_{m_2-i} \oplus \beta^2_{m_2-i}) z^i, \sum_j (\alpha^3_{m_2-j} \oplus \beta^3_{m_2-j}) z^j, ..., \sum_w (\alpha^n_{m_2-w} \oplus \beta^n_{m_2-w}) z^w\right), \quad (5)$$

где $\oplus$ – операция суммирования по модулю *p*.

Аналогично получаем для операции вычитания в МПК

$$\left|A(z) - B(z)\right|^+_{p(z)} = \left(\left|\alpha_1(z) - \beta_1(z)\right|^+_{p_1(z)}, ..., \left|\alpha_n(z) - \beta_n(z)\right|^+_{p_n(z)}\right) =$$

$$= \left(\alpha^1_0 \oplus \beta^1_0, \sum_i (\alpha^2_{m_2-i} \oplus \beta^2_{m_2-i}) z^i, \sum_j (\alpha^3_{m_2-j} \oplus \beta^3_{m_2-j}) z^j, ..., \sum_w (\alpha^n_{m_2-w} \oplus \beta^n_{m_2-w}) z^w\right), \quad (6)$$

Следует отметить, что операция вычитания по модулю два совпадает с операцией суммирования по модулю 2.

Согласно (5) и (6) полученные подмножества по основаниям $p_i(z), i = 1, ..., n$ МПК образуют циклическую группу сложения, которая содержит конечное число элементов. Операция сложения и обратная ей – вычитание производятся по модулю p, так как данные подмножества образуют аддитивную циклическую группу.

В силу дистрибутивности операции умножения операндов над кольцом на элементы этого кольца относительно операции сложения имеем

$$\left|A(z) \cdot B(z)\right|^+_{p(z)} = \left(\left|\alpha_1(z) \cdot \beta_1(z)\right|^+_{p_1(z)}, ..., \left|\alpha_n(z) \cdot \beta_n(z)\right|^+_{p_n(z)}\right) =$$

$$= (\alpha^1_0 \beta^1_0, \sum_{l=0}^{2m_2-2} q^2_{2m_2-2-l} z^{2m_2-2-l}; \ldots; \sum_{j=0}^{2m_n-2} q^n_{2m_n-2-j} z^{2m_n-2-j}), \quad (7)$$

где $q^i_s = \sum_{k=0}^{s} \alpha^i_k \beta^i_{s-k}$ – линейная свертка; $s = 0, ..., 2m_i - 2$; $i = 0, ..., n$.

Таким образом, выполнение операции умножения над операндами в расширенном поле Галуа $GF(p^v)$ согласно

$$A(z)B(z) = \left(\sum_{k,l \geq 0} a_k b_l z^{k+l}\right) \bmod P_{\text{пол}}(z), \quad (8)$$

сводится к умножению соответствующих остатков по основаниям МПК с последующих суммированием по модулю характеристики поля.

Анализ выражений (5)-(8) показывает, что основным достоинством модулярных полиномиальных кодов является сравнительная простота выполнения модульных операций (сложения, вычитания, умножения). Рассмотренные выше формальные правила выполнения операций в МПК позволяют существенно повысить скорость

вычислительных устройств. Так как основания системы представляют собой полиномы с небольшими степенями, то это позволяет использовать вычислительные устройства с заранее просчитанной детерминированной структурой.

Качественным скачком в обеспечении реального масштаба времени при реализации параллельных вычислений является использование нейросетевого логического базиса (НЛБ) [1-3]. Длительное время считалось, нейронные сети эффективны для решения так называемых трудноформализуемых и неформализуемых задач, связанных с необходимостью включения в алгоритм решения задач процесса обучения на реальном экспериментальном материале. В настоящее время к этому классу задач добавляется второй класс задач, не требующий обучения на экспериментальном материале, но хорошо представимый в нейросетевом логическом базисе. К ним относятся в первую очередь задачи с ярко выраженным параллелизмом – цифровая обработка сигналов и изображений в реальном масштабе времени [1-3]. Для этих задач переход к НЛБ обусловлен резким увеличением размерности пространства решения и необходимостью резкого уменьшения времени решения.

Основу нейросетевого логического базиса составляют операции типа $\left\{\sum \overline{ax}, sign\right\}$, которые максимальным образом соответствуют логическому базису основных решаемых задач. Таким образом, соответствие базиса вычислительной системы и задачи обеспечивает максимальную производительность [1]. По общему признанию многих авторов это обусловлено, прежде всего, тем, что в основу параллельной работы НЛБ заложено внутреннее свойство большего массированного параллелизма.

Как наглядно видно из выражений (5)-(8) характерной чертой всех арифметических устройств, функционирующих в МПК, является необходимость выполнения операции суммирования по модулю два. Так как операция XOR нелинейная, то для ее решения используют классическую трехслойную нейронную сеть. Первый слой – входной слой содержит два формальных нейрона, которые не участвуют в процессе вычисления, однако осуществляют процесс распределения входного вектора x. Во втором слое располагаются два нейрона, а в выходном слое – один нейрон. Данная нейронная сеть относится к нейронным сетям прямого распространения и осуществляет выполнение операции суммирования по модулю два за 2 итерации, считая перераспределение входного вектора x на нейроны второго слоя. При этом синаптические веса между слоя образуют множество {–1, 1}.

Качественным скачком в решении данной проблемы является отказ от линейного вида функции активации и переход к нелинейному виду. Применение функции активации tribas (приведенной к треугольному виду) позволяет реализовать нейроподобный двухвходовой сумматор по модулю два на основе одного формального нейрона. На рисунке 1 показана структура сумматора по модулю два, реализованного в данном НЛБ.

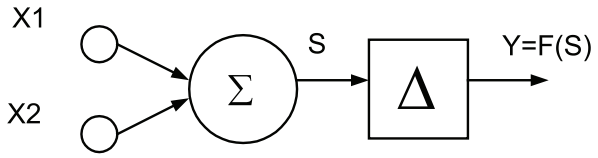

Рис. 1. Структура двухвходового сумматора по модулю два

Применение функции активации вида tribas обеспечивает значения сигналов

$$Y = F(S) = \begin{cases} 0 & \text{если} \quad S < -1; \\ 1 - |S|, & \text{если} \quad -1 \le S \le 1; \\ 0 & \text{если} \quad S > 1. \end{cases} \quad (9)$$

Графически данная функция активация представлена на рис. 2.

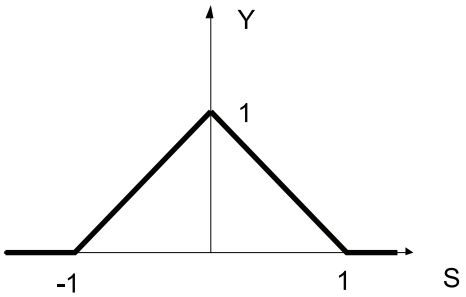

Рис. 2. Функция активации tribas

Исходные данные в двухмерном виде подаются на входы нейрона, умножаются на значения синаптических весов и поступают на сумматор, который реализует

$$S = \sum_{i=1}^{2} W_i X_i - b = \sum_{i=1}^{2} X_i - 1, \qquad (10)$$

где S – выходной сигнал сумматора; W_i – весовые коэффициенты (равны единице); X_i – входные значения нейрона $(X_i \in \{0,1\})$; $b = -1$ – смещение.

С выхода сумматора полученное значение подается на схему активации, где и осуществляется разделение гиперкуба размерности $n = 2$ на два класса. Геометрическая интерпретация преобразования вводимых образцов под действием весовых коэффициентов, смещение и функции активации показана на рис. 3

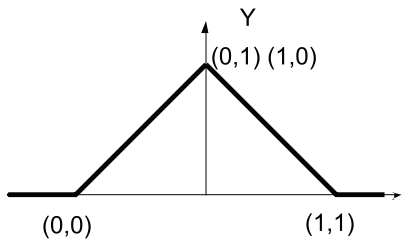

Рис. 3. Геометрическая интерпретация операции XOR с использованием функции активации tribas

Увеличение размерности входного вектора требует увеличения числа гиперплоскостей осуществляющих деление п-мерного гиперкуба на два класса. Пусть размерность гиперкуба n =3. Проблема моделирования отношения XOR для трехмерного входного вектора разделяющими плоскостями на рис. 4.

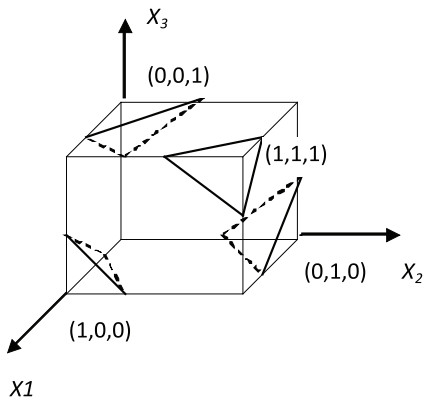

Рис. 4. Гиперплоскости, реализующие операцию XOR, для трехвходового нейроподобного сумматора

Из рис. 4 наглядно видно существование трех гиперплоскостей, осуществляющих разделение единичного гиперкуба на два класса:

– вершины у которых число единичных элементов равно единице;

– вершины у которых число единичных элементов отлично от единицы.

При этом данные гиперплоскости реализуются нейроном скрытого слоя, функционирующим согласно

$$Y_1 = F(\sum_{i=1}^{3} W_i^1 X_i - b_1) = F(\sum_{i=1}^{3} X_i - 1). \quad (11)$$

Однако выходной сигнал нейроподобного трехвходового сумматора по модулю два равен единице и в случае, когда число единичных элементов во входном векторе равно трем. Следовательно, необходим еще один нейрон, осуществляющий деление гиперкуба на два класса:

– вершины, у которых число единичных элементов равно трем;

– вершины, у которых число единичных элементов отлично от трех.

При этом данная гиперплоскость реализуется вторым нейроном скрытого слоя, функционирующим согласно

$$Y_2 = F(\sum_{i=1}^{3} W_i^1 X_i - b_2) = F(\sum_{i=1}^{3} X_i - 3). \quad (12)$$

Таким образом, количество нейронов второго (скрытого) слоя равно двум, что определяется как

$$N_2 =]3/2[=]\ /2[. \qquad (13)$$

Для объединения информации об этих гиперплоскостях в выходном слое используется один нейрон с пороговой функцией активации, который осуществляет преобразование

$$Y_{\text{сум}} = sign \sum_{i=1}^{2} Y_i. \qquad (14)$$

Обобщая сказанное, можно определить правила построения нейроподобного сумматора по модулю два:

– в качестве модели нейросетевого логического базиса выбран многослойный персептрон, семантические веса которого равны единице;

– входной слой содержит n нейронов (n – размерность входного слова), которые осуществляют приём и распределение сигналов на второй слой;

– скрытый слой содержит $V_2 =]n/2[$ нейронов с функцией активации tribas, осуществляющих разделение вершин гиперкуба гиперплоскостями на 2 класса, с чётным и нечётным числом единичных элементов, при этом смещение l-го нейрона равно $b_l = -(2l-1)$, где $l = 1,2,...,]n/2[$;

– выходной слой содержит один нейрон пороговой функцией активации, используемый для объединения информации об этих гиперплоскостях.

Структура нейроподобного n-входового сумматора по модулю два показана на рисунке 5. Входной слой в процессе вычисления значения суммы по модулю два n-разрядного вектора не участвует, а осуществляет перераспределение данных, поступивших на входы нейронной сети. Скрытый слой содержит по одному нейрону для каждого возможного нечетного значения суммы элементов вектора входа, причем смещение нейрона равно значению возможной нечетной суммы со знаком минус. Синаптические веса между нейронами входного и срытого слоя равны 1. В качестве функции активации используем треугольную функцию активации. Выходной слой состоит из одного нейрона, синаптические веса входов которого равны 1, а смещение 0. В качестве функции активации используется пороговая функция.

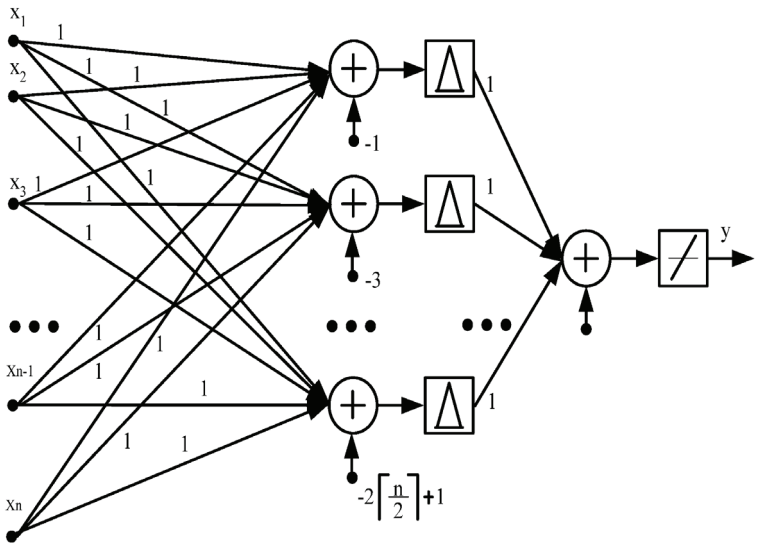

Рис. 5. Нейроподобный сумматора по модулю два

При этом число нейронов скрытого слоя составит $V_1 = \lceil n/2 \rceil$, в то время как выходной слой содержит один нейрон $V_2 = 1$. Тогда общее число нейронов равно

$$V^n = \lceil n/2 \rceil + 1. \qquad (15)$$

Применение трехслойной нейронной сети позволяет реализовать данную операцию за две итерации. Таким образом, очевидно, что достоинством данного метода построения многовходового нейросетевого сумматора по модулю два является высокое быстродействие при сравнительно небольших затратах оборудования.

В работе [1] показана возможность обучения нейронной сети с помощью генетических алгоритмов. Как показан в данной работе применение алгоритма обучения позволил обеспечить реализацию многовходового сумматора, который обладает меньшими аппаратными и временными затратами по сравнению с ранее рассмотренными.

Выводы. С целью повышения скорости обработки сигналов в современных вычис-

лительных устройствах используют параллельные вычисления. Применение модулярного полиномиального кода позволяет осуществить распараллеливание на уровне операций. Дальнейшее повышение скорости обработки данных возможно за счет использования нейросетевого логического базиса. В работе приведена разработка многовходового нейросететвого сумматора по модулю два, который обладает минимальными временными и аппаратными затратами.

Список литературы

1. Воронкин Р.А, Калмыков, И.А., Резеньков Д.Н., Емарлукова Я.В. Генетические алгоритмы в системах цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. 2011. Вып. 5. С. 20-27.

2. Калмыков И.А., Чипига А.Ф. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности // Вестник Ставропольского государственного университета. 2004. Т.38. С. 46.

3. Калмыков И.А., Зиновьев А.В., Резеньков Д.Н., Гахов В.Р. Применение систолических ортогональных преобразований в полиномиальной системе классов вычетов для повышения эффективности цифровой обработки сигналов // Инфокоммуникационные технологии. Самара. 2010. Т.8. № 3. С. 4-11

4. Калмыков И.А. Чипига А.А. Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации // Инфокоммуникационные технологии. Самара. 2007. Т.5. № 2. С. 159-162.

5. Калмыков И.А., Дагаева О.И. Разработка псевдослучайной функции повышенной эффективности // Известия Южного федерального университета. Технические науки. 2011. Т.125. № 12. С.160-169.

6. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О.А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. 2010. Т.8. № 2. С. 14-22

7. Калмыков И.А., Емарлукова Я.В., Зиновьев А.В. Высокоскоростные систолические отказоустойчивые процессоры цифровой обработки сигналов для инфотелекоммуникационных систем // Инфокоммуникационные технологии. Самара. 2009. № 2. С. 31-37

8. Калмыков И.А., Гахов В.Р., Емарлукова Я.В. Устройство обнаружения и коррекции ошибок в кодах полиномиальной системы классов вычетов // Патент России № 2300801. 30.06.2005.

9. Чипига А.А., Калмыков И.А., Лободин М.В. Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов // Патент России № 2301441. 01.08.2005.

10. Хайватов А.Б., Калмыков И.А. Математическая модель отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов // Инфокоммуникационные технологии. 2007. Т.5. № 3. С.39-42.