ISSN 1561-8323 (Print)
ISSN 2524-2431 (Online)

ИНФОРМАТИКА

INFORMATICS

УДК 004.9, 004.94, 004.56
https://doi.org/10.29235/1561-8323-2018-62-6-652-660

Поступило в редакцию 25.04.2018
Received 25.04.2018

Академик А. Ф. Чернявский, А. А. Коляда, С. Ю. Протасеня

Институт прикладных физических проблем имени А. Н. Севченко
Белорусского государственного университета, Минск, Республика Беларусь

ПРИМЕНЕНИЕ НЕЙРОСЕТЕВОЙ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНОЛОГИИ ДЛЯ РАСЧЕТА ИНТЕРВАЛЬНО-ИНДЕКСНОЙ ХАРАКТЕРИСТИКИ МИНИМАЛЬНО ИЗБЫТОЧНОГО МОДУЛЯРНОГО КОДА

Аннотация. Сообщение посвящено проблеме создания высокоскоростных нейронных сетей (НС) для расчета интервально-индексных характеристик минимально избыточного модулярного кода. Функциональную базу предлагаемого решения составляет расширенный класс НС конечного кольца, осуществляющих позиционно-модулярные кодовые преобразования масштабируемых чисел с применением модифицированной редукционной технологии. Разработанная НС для вычисления интервально-индексных характеристик имеет однородную параллельную структуру, проста в реализации и требует близких к теоретической нижней оценке временных затрат порядка $(3\lceil \log_2 b \rceil + 2\lceil \log_2 k \rceil + 6)t_{\text{сл}}$, где b и k – соответственно средняя разрядность и количество модулей; $t_{\text{сл}}$ – длительность двухместной операции сложения целых чисел. Отказ от нормировки цифр модулярного кода приводит к сокращению необходимого набора НС конечного кольца на $(k – 1)$ компонент. Вместе с тем ненормированная конфигурация минимально избыточного модулярного кодирования требует в среднем k-кратного увеличения модуля интервального индекса (по отношению к остальным основаниям модулярной системы счисления), что ведет к адекватному повышению аппаратурных затрат по данному модулю. Кроме того, переход от нормированного к ненормированному кодированию снижает уровень однородности структуры НС для расчета интервально-индексных характеристик. Исследована возможность снижения структурной сложности предложенной НС за счет использования ненормированных интервально-индексных характеристик.

Ключевые слова: нейронная сеть, нейронная сеть конечного кольца, синаптические веса, модулярная система счисления, интервально-индексные характеристики, редукционный метод

Для цитирования. Чернявский, А. Ф. Применение нейросетевой вычислительной технологии для расчета интервально-индексной характеристики минимально избыточного модулярного кода / А. Ф. Чернявский, А. А. Коляда, С. Ю. Протасеня // Докл. Нац. акад. наук Беларуси. – 2018. – Т. 62, № 6. – С. 652–660. https://doi.org/10.29235/1561-8323-2018-62-6-652-660

Academician Alexander F. Chernyavskiy, Andrey A. Kolyada, Stella Yu. Protasenia

Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University,
Minsk, Republic of Belarus

APPLICATION OF THE NEURAL NETWORK COMPUTING TECHNOLOGY FOR CALCULATING THE INTERVAL-INDEX CHARACTERISTICS OF A MINIMALLY REDUNDANT MODULAR CODE

Abstract. The article is devoted to the problem of creation of high-speed neural networks (NN) for calculation of interval-index characteristics of a minimally redundant modular code. The functional base of the proposed solution is an advanced class of neural networks of a final ring. These neural networks perform position-modular code transformations of scalable numbers using a modified reduction technology. A developed neural network has a uniform parallel structure, easy to implement and requires the time expenditures of the order $(3\lceil \log_2 b \rceil + 2\lceil \log_2 k \rceil + 6)t_{\text{sum}}$ close to the lower theoretical estimate. Here b and k is the average bit capacity and the number of modules respectively; t_{sum} is the duration of the two-place operation of adding integers. The refusal from a normalization of the numbers of the modular code leads to a reduction of the

required set of NN of the finite ring on the (k – 1) component. At the same time, the abnormal configuration of minimally redundant modular coding requires an average k-fold increase in the interval index module (relative to the rest of the bases of the modular number system). It leads to an adequate increase in hardware expenses on this module. Besides, the transition from normalized to unregulated coding reduces the level of homogeneity of the structure of the NN for calculating interval-index characteristics. The possibility of reducing the structural complexity of the proposed NN by using abnormal interval-index characteristics is investigated.

Keywords: neural network, neural network of finite ring, synaptic weights, modular number system, interval-index characteristics, reduction method

For citation: Chernyavskiy A. F., Kolyada A. A., Protasenia S. Yu. Application of the neural network computing technology for calculating the interval-index characteristics of a minimally redundant modular code. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2018, vol. 62, no. 6, pp. 652–660 (in Russian). https://doi.org/10.29235/1561-8323-2018-62-6-652-660

Введение. В современном процессе развития высокопроизводительных вычислительных технологий, и в частности технологий быстрых вычислений на диапазонах больших чисел (ДБЧ), особая роль отводится модулярным системам счисления (МСС) [1–8], которые обладают параллельной кодовой структурой. Отмеченное свойство МСС позволяет использовать их как эффективный инструментарий для решения задачи перевода трудоемких вычислений из ДБЧ в компьютерные диапазоны целых чисел (ЦЧ) стандартной разрядности. Важнейшим фактором, способствующим неуклонному повышению уровня востребованности модулярных вычислительных структур (МВС), является их идеальная приспособленность к нейросетевым реализациям [1; 3]. Разработка нейросетевых МВС на основе оптимально согласованных свойств параллелизма искусственных нейронных сетей (НС) и модулярной арифметики (МА) – арифметики МСС составляет активно развиваемое в настоящее время новое перспективное направление в области параллельных вычислений.

Ключевую роль в технологии синтеза МВС нейросетевого типа выполняют НС, осуществляющие преобразования колец вычетов по модулям МСС. Такие НС принято называть нейронными сетями конечного кольца (НСКК) [1; 3; 9–11]. Центральное место в классе НСКК занимают сети, которые реализуют позиционно-модулярные преобразования ЦЧ в остатки по модулям базиса МСС [9–13]. Как структурно, так и на операционном уровне НСКК должны быть максимально согласованы с естественным кодовым параллелизмом МА. В полной мере данному условию удовлетворяет редукционный метод рекурсивного понижения разрядности элементов последовательности вычетов, получаемой в процессе приведения исходных ЦЧ к остаткам по модулям рабочего базиса [1]. Традиционно в качестве операционной основы НСКК используется преобразование ЦЧ из двоичной системы счисления в модулярную. Принимая, однако, во внимание то обстоятельство, что при построении различных конфигураций МА ключевую роль выполняют преобразования масштабируемых вычетов в остатки по модулям МСС, в развиваемом направлении исследований в качестве нейросетевой реализационной базы применяется расширенный класс НСКК, которые осуществляют преобразования масштабируемых ЦЧ. Фундаментальные преимущества МА наиболее полно удается реализовать в рамках так называемого минимально избыточного кодирования [1; 14], ассоциированного с интервально-модулярной формой чисел и связанными с ней интервально-индексными характеристиками кода. В соответствии с этим первостепенную важность в разработках перспективных МВС нейросетевого типа представляет проблема вычисления с применением рассматриваемого нового подхода интервально-индексных характеристик минимально избыточного модулярного кода. Решению данной задачи и посвящено настоящее сообщение.

Позиционные формы и интегральные характеристики модулярных чисел. Введем обозначения:

$\mathbf{Z}$ – множество ЦЧ;

$\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее ЦЧ соответственно не большее и не меньшее вещественной величины a;

$\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$, $\mathbf{Z}_m^- = \{-\lfloor m/2 \rfloor, -\lfloor m/2 \rfloor + 1, \ldots, \lceil m/2 \rceil - 1\}$ – множества наименьших неотрицательных и абсолютно наименьших вычетов по натуральному модулю m;

$|a|_m$ и $|a|_m^-$ – элементы множеств $\mathbf{Z}_m$ и $\mathbf{Z}_m^-$, сравнимые с a (в общем случае рациональным числом) по модулю m;

M = {m_1, m_2, …, m_k} – набор модулей базовой МСС (модулярный базис; k – мощность базиса); $X = (|X|_{m_1}, |X|_{m_2} |X|_{m_k})$ – представление ЦЧ X в МСС с базисом **M**.

Пусть в МСС с базисом **M** задано ЦЧ $X = (\chi_1, \chi_2, ..., \chi_k)(\chi_i = |X|_{m_i}\ (i = \overline{1, k}))$.

Согласно Китайской теореме об остатках [15] для X выполняется сравнение

$$X \equiv \sum_{i=1}^{k-1} M_{i,k-1}\chi_{i,k-1} (\mathrm{mod}\, M_{k-1}), \tag{1}$$

где $M_{i,k-1} = M_{k-1} / m_i$; $M_{k-1} = \prod_{j=1}^{k-1} m_j$; $\chi_{i,k-1} = |\mu_{i,k-1}\chi_i|_{m_i}$; $\mu_{i,k-1} = |M_{i,k-1}^{-1}|_{m_i}$.

Из (1) следует, что для каждого X существует единственное ЦЧ $I_k(X)$, удовлетворяющее соотношению

$$X = \sum_{i=1}^{k-1} M_{i,k-1}\chi_{i,k-1} + M_{k-1} I_k(X). \tag{2}$$

Величина $I_k(X)$ представляет собой интегральную характеристику модулярного кода $(\chi_1, \chi_2, ..., \chi_{k-1}, \chi_k)$ и называется интервальным индексом (ИИ) числа X по базису **M**, а равенство (2) называют интервально-модулярной формой (ИМФ) данного числа [1; 14].

В [1] доказано нижеследующее утверждение.

Т е о р е м а 1 (О минимально избыточном модулярном кодировании). *Для того чтобы в МСС с попарно простыми основаниями m_1, m_2, …, m_k ИИ $I_k(X)$ каждого элемента $X = (\chi_1, \chi_2, ..., \chi_k)$ диапазона* $\mathbf{Z}_{2M}^{-}$ = {–M, –M + 1, ..., M – 1} ($M = m_0 M_{k-1}$; m_0 – *вспомогательный модуль*) *полностью определялся компьютерным ИИ – вычетом* $\hat{I}_k(X) = |I_k(X)|_{m_k}$, *необходимо и достаточно, чтобы k-е основание удовлетворяло условию*

$$m_k \geq 2m_0 + k - 2\ (m_0 \geq k - 2). \tag{3}$$

При этом для $I_k(X)$ верны расчетные соотношения

$$I_k(X) = \begin{cases} \hat{I}_k(X), & \text{если } \hat{I}_k(X) < m_0, \\ \hat{I}_k(X) - m_k, & \text{если } \hat{I}_k(X) \geq m_0; \end{cases} \tag{4}$$

$$\hat{I}_k(X) = \left| \sum_{i=1}^{k} R_{i,k}(\chi_i) \right|_{m_k}; \tag{5}$$

$$R_{i,k}(\chi_i) = \left| -m_i^{-1} \left| M_{i,k-1}^{-1}\chi_i \right|_{m_i} \right|_{m_k} (i \neq k),\ R_{k,k}(\chi_k) = \left| \frac{\chi_k}{M_{k-1}} \right|_{m_k}. \tag{6}$$

Благодаря условию (3) мощность $|\mathbf{Z}_{2M}^{-}| = 2M$ диапазона $|\mathbf{Z}_{2M}^{-}|$ превышает мощность $|\mathbf{Z}_{M_k}^{-}| = M_k = \prod_{i=1}^{k} m_i$ множества $|\mathbf{Z}_{M_k}^{-}|$ всех абсолютно наименьших вычетов по модулю M_k. Это означает, что МСС с базисом **M** и диапазоном $|\mathbf{Z}_{2M}^{-}|$ в отличие от МСС с тем же базисом **M** и диапазоном $|\mathbf{Z}_{M_k}^{-}|$ является избыточной. Несмотря на то что вводимая избыточность весьма мала, она обеспечивает значительное упрощение процедуры вычисления ИИ $I_k(X)$, описываемой расчетными соотношениями (4)–(6). Это приводит к адекватному уменьшению сложности алгоритмов немодульных операций в минимально-избыточной МСС [1; 14]. Отмеченное преимущество минимально избыточной МА (МИМА) дает ей приоритетные позиции при решении проблемы оптимизации МВС, в том числе МВС нейросетевого типа.

В немодульных процедурах МИМА фундаментальную роль выполняет интервально-индексная характеристика $I_k(X)$. Поэтому в настоящем сообщении главное внимание уделяется нейросетевой реализации расчетных соотношений для ИИ.

Редукционный метод позиционно-модулярного линейного преобразования целых чисел. Эффективную основу для создания нейрокомпьютерного обеспечения современных МА-приложений составляет класс нейронных сетей конечного кольца, осуществляющих преобразования

$$\chi = \left|CX\right|_m, \tag{7}$$

где χ – результирующий остаток от деления произведения CX на заданный модуль m; C – целочисленная константа (масштабирующий множитель); X – входное неотрицательное ЦЧ, представленное b-разрядным двоичным кодом $(x_{b-1}x_{b-2}\ldots x_0)_2$ $(x_j \in \{0,1\}\ \ (j=\overline{0,b-1}))$.

Вполне понятно, что НСКК как структурно, так и на операционном уровне должны быть максимально согласованы с естественным кодовым параллелизмом МА. По критерию простоты нейросетевой реализации наиболее приемлемым методом выполнения операции (7) является метод модулярной редукции суммы взвешенных операндов по рекурсивной схеме понижения разрядности элементов получаемой последовательности вычетов [1; 3; 10].

Положим

$$X^{(0)} = (x^{(0)}_{b_0-1}\ \ x^{(0)}_{b_0-2}\ldots x^{(0)}_0)_2 = \sum_{j=0}^{b_0-1} 2^j x_j^0\ \ (b_0 = b,\ \ x_j^{(0)} = x_j) \tag{8}$$

и пусть

$$W_j(C) = \left|C2^j\right|^{-}_{m_0} = \begin{cases} \left|C2^j\right|_m, & \text{если } \left|C2^j\right|_m < \left\lceil \dfrac{m}{2} \right\rceil, \\ \left|C2^j\right|_m - m, & \text{если } \left|C2^j\right|_m \geq \left\lceil \dfrac{m}{2} \right\rceil, \end{cases} \quad (j=\overline{0,b-1}). \tag{9}$$

В случае $C = 1$ далее употребляется также обозначение $W_j = W_j(1)$.

При необходимости конкретизации модуля МСС в (9): $m = m_i$, вместо $W_j(C)$ и W_j будем использовать $W_{j,i}(C)$ и $W_{j,i}$ $(i=\overline{1,k})$. Для наборов констант, определяемых выражением (9), в дальнейшем применяются обозначения типа $\mathbf{W}(C,\ b,\ m)$, $\mathbf{W}(C)$, $\mathbf{W} = W(1)$, $\mathbf{W}_i(C,\ b) = \mathbf{W}(C,\ b,\ m_i)$, $\mathbf{W}_i(C) = \mathbf{W}_i(C, b)$, $\mathbf{W}_i = \mathbf{W}_i(1)$.

Применяемая редукционная схема описывается операционной последовательностью

$$\left\langle \begin{gathered} X^{(1)} = \sum_{j=0}^{b_0-1} W_j(C)x_j^{(0)} = (x^{(1)}_{b_1-1}\ x^{(1)}_{b_1-2}\ldots x^{(1)}_0)_2 - 2^{b_1}x^{(1)}_{b_1-1} = \sum_{j=0}^{b_1-2} 2^j x_j^{(1)} - 2^{b_1-1}x^{(1)}_{b_1-1}, \\ X^{(s)} = \sum_{j=0}^{b_{s-1}-2} W_j x_j^{(s-1)} - W_{b_{s-1}-1}x^{(s-1)}_{b_{s-1}-1} = (x^{(s)}_{b_s-1}\ x^{(s)}_{b_s-2}\ldots x^{(s)}_0)_2 - 2^{b_s}x^{(s)}_{b_s-1} = \\ = \sum_{j=0}^{b_s-2} 2^j x_j^{(s)} - 2^{b_s-1}x^{(s)}_{b_s-1} \quad (s=\overline{2,S});\ \ \chi = \left|X^{(S)}\right|_m \end{gathered} \right\rangle, \tag{10}$$

где b_1 и b_s – длины дополнительных двоичных кодов $(x^{(1)}_{b_1-1}\ x^{(1)}_{b_1-2}\ldots x^{(1)}_0)_2$ и $(x^{(s)}_{b_s-1}\ x^{(s)}_{b_s-2}\ldots x^{(s)}_0)_2$, соответственно ЦЧ $X^{(1)}$ и $X^{(s)}$, которые, как следует из (9), могут быть как отрицательными, так и неотрицательными; S – количество итераций схемы.

Основополагающая идея редукционного метода, реализуемая в рамках вычислительной схемы (10) в целях приведения ЦЧ CX к остатку по модулю m состоит в замене коэффициентов $C2^j$ правой части равенства

$$CX = CX^{(0)} = \sum_{j=0}^{b_0-1} (C2^j)x_j^{(0)}$$

на вычеты $W_j(C)$, определяемые по правилу (9), а коэффициенты 2^j, $2^{b_{s-1}-1}$ выражения

$$X^{(s)} = \sum_{j=0}^{b_{s-1}-2} 2^j x_j^{(s-1)} - 2^{b_{s-1}-1}x^{(s-1)}_{b_{s-1}-1}$$

на вычеты $W_j, W_{b_{s-1}-1}$ при $s=\overline{2,S}$. В виду (9) все получаемые после указанных замен ЦЧ $X^{(s)}$ $(s=\overline{1,S})$ равноостаточны по модулю m. Они являются элементами одного и того же класса вычетов по данному модулю: $\mathbf{R}_m(CX) = \{R \in \mathbf{Z} \mid R \equiv CX (\mathbf{mod}\ m)\}$ ($\mathbf{Z}$ – множество ЦЧ).

Проведенная оценка мощности диапазона изменения и разрядности b_s ЦЧ $X^{(s)}$ $(s=\overline{1,S})$ позволяет сформулировать следующее утверждение.

Т е о р е м а 2. *Пусть модуль m имеет разрядность* $b\_\mathrm{mod} = \lceil \log_2 m \rceil$ *бит. Тогда для длины* b_s *дополнительного двоичного кода* $(x_{b_s-1}^{(s)} x_{b_s-2}^{(s)} \ldots x_0^{(s)})_2$ *вычета* $X^{(s)}$, *определяемого по редукционной схеме (10) для входного ЦЧ (8) с использованием синаптических весов (9), верна оценка* $b_s < b\_\mathrm{mod} + \log_2 b_{s-1}$ (b_{s-1} – *разрядность ЦЧ* $X^{(s-1)}$ $(s = \overline{1, S})$).

При этом для произвольного целочисленного масштабирующего множителя C существует $S \geq 1$, при котором последовательность $b_1, b_2, \ldots, b_s$ длин дополнительных двоичных кодов вычетов $X^{(1)}, X^{(2)}, \ldots, X^{(S)}$, получаемых по рекурсивной редукционной схеме (10), является строго убывающей.

Для функции, описывающей преобразование $X \to |CX|_m$, которое осуществляется по редукционной схеме (10) введем обозначение

$$\chi = PM\_\mathrm{Reduc}(X; C, b, m), \tag{11}$$

где χ – результирующий остаток; X – аргумент (входное ЦЧ); C – масштабирующий множитель; $b = b\_X$ – разрядность аргумента X; m – заданный модуль.

Далее для b-входовой НСКК, реализующей функцию (11), употребляется условное графическое обозначение, приведенное на рис. 1.

Структура нейронной сети для расчета интервально-индексной характеристики минимально избыточного модулярного кода. Операционный анализ базовых расчетных соотношений для синтеза немодульных процедур позволяет заключить, что основу их реализации с применением нейросетевой вычислительной технологии составляют представленные на рис. 1 НСКК, которые выполняют преобразования вида $X \to |CX|_m$, где X – некоторое ЦЧ; C – масштабирующий множитель; m – модуль используемого модулярного базиса. Поскольку при построении МА ключевую роль играют интегральные характеристики модулярного кода (ИХМК), то в процессе разработки требуемых конфигураций немодульных процедур для МА-приложений исследуемого класса в первую очередь необходимо решить задачу синтеза НС для расчета применяемых ИХМК. В нашем случае такой характеристикой является интервальный индекс числа, определяемый по расчетным соотношениям (3)–(6).

Отметим, что аналитическим аналогом НСКК, осуществляющей позиционно-модулярное преобразование $X \to |CX|_m$, служит функция вида (11). На языке аппарата данной функции – функции $PM_$Reduc формула (5) для вычисления компьютерного интервального индекса $\hat{I}_k(X)$ ЦЧ $X = (\chi_1, \chi_2, \ldots, \chi_k)$ в МСС с базисом $\mathbf{M} = \{m_1, m_2, \ldots, m_k\}$ с учетом обозначений: $m_{i,k} = \left|-m_i^{-1}\right|_{m_k}$, $\mu_{i,k-1} = \left|M_{i,k-1}^{-1}\right|_{m_i}$, $\chi_{i,k-1} = \left|\mu_{i,k-1}\chi_i\right|_{m_i}$ $(i = \overline{1, k-1})$, $\mu_{k,k} = \left|M_{k-1}^{-1}\right|_{m_k}$, $\chi_{k,k} = \left|\mu_{k,k}\chi_k\right|_{m_k}$, представляется операционной последовательностью

$$\begin{aligned}\Big\langle s_k = \sum_{i=1}^{k-1} \left|m_{i,k}\chi_{i,k-1}\right|_{m_k} + \chi_{k,k} = \sum_{i=1}^{k-1} PM\_\mathrm{Reduc}\,(PM\_\mathrm{Reduc}(\chi_i; \mu_{i,k-1}, b\_\mathrm{mod}\_i, m_i);\\ m_{i,k}, b\_\mathrm{mod}\_i, m_k) + PM\_\mathrm{Reduc}(\chi_k; \mu_{k,k}, b\_\mathrm{mod}\_k, m_k);\\ \hat{I}_k(X) = PM\_\mathrm{Reduc}(s_k; 1, b\_s_k, m_k)\Big\rangle,\end{aligned} \tag{12}$$

где $b\_\mathrm{mod}\_i = \lceil \log_2 m_i \rceil$ – разрядность модуля m_i; $b\_s_k = \lceil \log_2 (k(m_k - 1)) \rceil$ – разрядность суммы s_k. Принятое для суммы s_k значение b_s_k разрядности согласовано с оценкой

$$b_{s_k} = \lceil \log_2 s_k \rceil \leq \left\lceil \log_2 \textstyle\sum_{i=1}^{k} (m_k - 1) \right\rceil = \lceil \log_2 (k(m_k - 1)) \rceil.$$

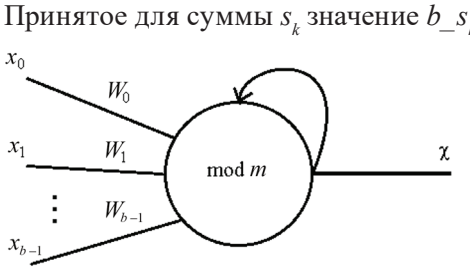

Рис. 1. Условное графическое обозначение НСКК по модулю m

Fig. 1. Conditional graphic designation of NNFR on the module m

Вычислительной схеме (12) отвечает НС, которая имеет структуру, показанную на рис. 2. Базовыми элементами данной НС служат типовые НСКК (рис. 1), реализующие используемые в (12) функции $PM_$Reduc по редукционной схеме (10). Представленная на рис. 2 НС для расчета интервально-индексной характеристики $\hat{I}_k(X)$ числа X в МСС с базисом $\mathbf{M}$ состоит из входного слоя, выполняющего роль регистра для фиксации модулярного кода $(\chi_1, \chi_2, \ldots, \chi_k)$

входного ЦЧ X, первого и второго скрытых слоев НСКК, блока SMR суммирования вычетов, объединяющего скрытые слои с третьего по $(\lceil \log_2 k \rceil + 2)$-й, и выходной слой из одиночной НСКК. Блок суммирования вычетов – SMR построен на основе двоичных сумматоров SM и имеет $\lceil \log_2 k \rceil$-каскадную «пирамидальную» архитектуру, обеспечивающую суммирование k-компонентных наборов вычетов за время порядка $\lceil \log_2 k \rceil t_{\text{сл}}$ ($t_{\text{сл}}$ – длительность двухместной операции сложения).

Вычисление интервально-индексной характеристики $\hat{I}_k(X)$ нейронной сетью, представленной на рис. 2, осуществляется следующим образом. НСКК первого скрытого слоя по цифрам модулярного кода $(\chi_1, \chi_2, \ldots, \chi_{k-1}, \chi_k)$, зарегистрированного во входном слое, и весовым коэффициентам $\mu_{1,k-1}, \mu_{2,k-1}, \ldots, \mu_{k-1,k-1}, \mu_{k,k}$ получают нормированные остатки $\chi_{1,k-1}, \chi_{2,k-1}, \ldots, \chi_{k-1,k-1}, \chi_{k,k}$ ЦЧ X по модулям $m_1, m_2, \ldots, m_{k-1}, m_k$ базовой МСС. Затем НСКК второго скрытого слоя по остаткам $\chi_{1,k-1}, \chi_{2,k-1}, \ldots, \chi_{k-1,k-1}$ и масштабирующим коэффициентам $m_{i,k}$ определяют вычеты $R_i = \left| m_{i,k} \chi_{i,k-1} \right|_{m_k}$ для всех $i = \overline{1, k-1}$. Сформированный набор вычетов: $\{R_1, R_2, \ldots, R_{k-1}, R_k = \chi_{k,k}\}$, поступают в БСВ SMR, который, реализуя $\lceil \log_2 k \rceil$-каскадную процедуру суммирования с максимальным распараллеливанием на уровне двухместных операций сложения в скрытых слоях с третьего по $(\lceil \log_2 k \rceil + 2)$-й, находит сумму $s_k = \sum_{i=1}^{k} R_i$. С приведением s_k к остатку $I = \hat{I}_k(X) = \left| s_k \right|_{m_k}$ по модулю m_k, осуществляемым НСКК выходного слоя, процесс расчета интервально-индексной характеристики $\hat{I}_k(X)$ завершается.

Нейросетевая реализация редукционного метода позиционно-модулярного кодового преобразования масштабируемых ЦЧ в структурном отношении становится более простой при ис-

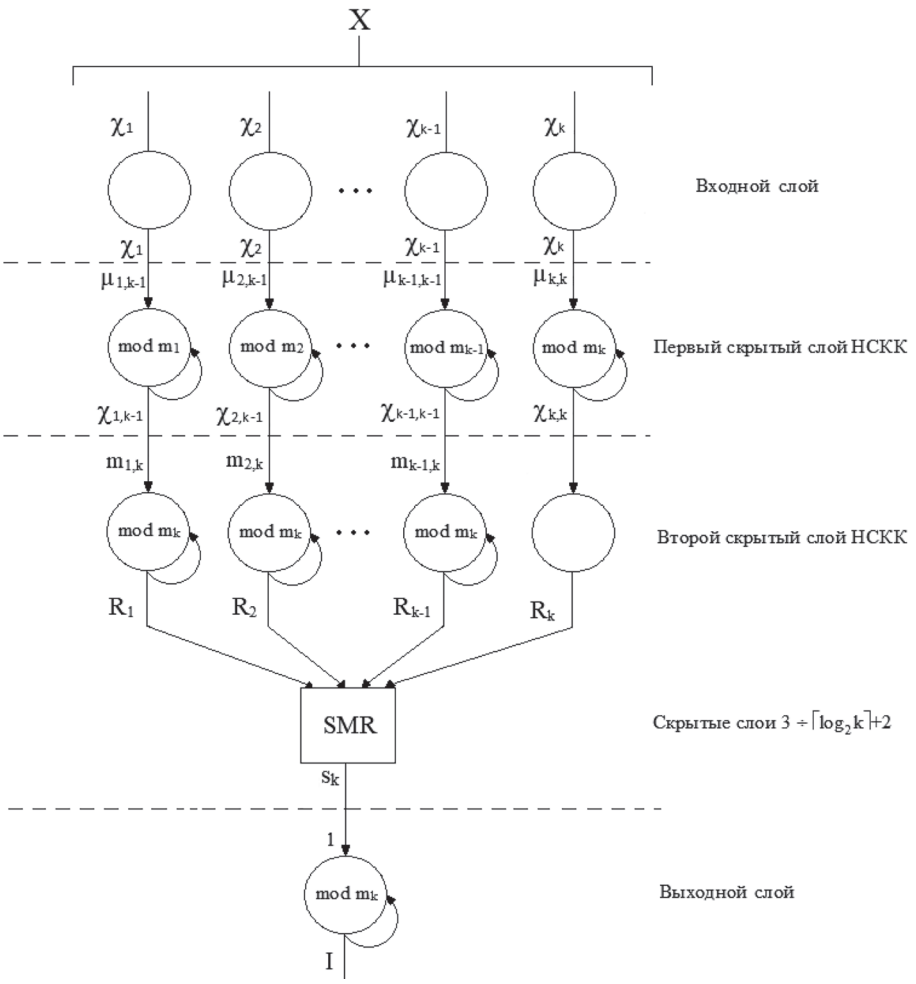

Рис. 2. Нейронная сеть для расчета нормированной интервально-индексной характеристики минимально избыточного модулярного кода

Fig. 2. Neural network for calculating the normalized interval-index characteristic of a minimally redundant modular code

пользовании МИМА, базирующейся на ненормированной ИМФ, которая вытекает из соответствующей версии китайской теоремы об остатках

$$X = \sum_{i=1}^{k-1} M_{i,k-1}\mu_{i,k-1}\chi_i \,(\mathrm{mod}\, M_{k-1}), \tag{13}$$

и имеет вид

$$X = \sum_{i=1}^{k-1} M_{i,k-1}\mu_{i,k-1}\chi_i + M_{k-1}\mathfrak{I}_k(X), \tag{14}$$

где $\mathfrak{I}_k(X)$ – ненормированный аналог интервального индекса $I_k(X)$ числа X в МСС с базисом **M** и диапазоном $\left|\mathbf{Z}_{2M}^{-}\right|$ ($M = m_0 M_{k-1}$; m_0 – вспомогательный модуль).

Из (13) следует, что для любого X существует единственная целочисленная величина $r_{k-1}(X)$, определяемая равенством

$$\left|X\right|_{M_{k-1}} = \sum_{i=1}^{k-1} M_{i,k-1}\mu_{i,k-1}\chi_i - Mr_{k-1}r_{k-1}(X), \tag{15}$$

и называемая ненормированным рангом ЦЧ X по базису $\{m_1, m_2, \ldots, m_{k-1}\}$. Из (15) для ранговой характеристики $r_{k-1}(X) = r_{k-1}(\left|X\right|_{M_{k-1}})$ вытекает равенство

$$r_{k-1}(X) = \left\lfloor \sum_{i=1}^{k-1} \frac{\mu_{i,k-1}\chi_i}{m_i} \right\rfloor. \tag{16}$$

Как видно из (16), максимуму $r\_\max$ характеристики $r_{k-1}(X)$ отвечает ЦЧ $M_{k-1} - 1$, которое в МСС с основаниями $m_1, m_2, \ldots, m_{k-1}$ имеет код $(m_1 - 1, m_2 - 1, \ldots, m_{k-1} - 1)$. Таким образом,

$$r\_\max = r_{k-1}(M_{k-1} - 1) = \left\lfloor \sum_{i=1}^{k-1} \frac{\mu_{i,k-1}(m_i - 1)}{m_i} \right\rfloor = \sum_{i=1}^{k-1} \mu_{i,k-1} - \left\lceil \sum_{i=1}^{k-1} \frac{\mu_{i,k-1}}{m_i} \right\rceil. \tag{17}$$

Сущность минимально избыточного модулярного кодирования, ассоциированного с интервально-модулярной формой (14) и интервально-индексной характеристикой $\mathfrak{I}_k(X)$, раскрывает нижеследующее утверждение.

Т е о р е м а 3 (О минимально избыточном модулярном кодировании). *Для того чтобы в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_k$ ИИ $I_k(X)$ каждого элемента $X = (\chi_1, \chi_2, \ldots, \chi_k)$ диапазона $\mathbf{Z}_{2M}^{-} = \{-M, -M + 1, \ldots, M - 1\}$ ($M = m_0 M_{k-1}$; m_0 – вспомогательный модуль) полностью определялся компьютерным ИИ-вычетом $\hat{I}_k(X) = \left|I_k(X)\right|_{m_k}$, необходимо и достаточно, чтобы k-е основание удовлетворяло условию*

$$m_k \geq 2m_0 + r\_\max, \tag{18}$$

где $r\_\max$ *вычисляется по (17).*

При этом для $\mathfrak{I}_k(X)$ верны расчетные соотношения

$$\mathfrak{I}_k(X) = \begin{cases} \hat{\mathfrak{I}}_k(X), & \text{если } \hat{\mathfrak{I}}_k(X) < m_0, \\ \hat{\mathfrak{I}}_k(X) - m_k, & \text{если } \hat{\mathfrak{I}}_k(X) \geq m_0; \end{cases} \tag{19}$$

$$\hat{\mathfrak{I}}_k(X) = \left| \sum_{i=1}^{k} \left|C_{i,k}\chi_i\right|_{m_k} \right|_{m_k}; \tag{20}$$

$$C_{i,k} = \left|-m_i^{-1}\mu_{i,k-1}\right|_{m_k} \ (i = \overline{1, k-1}), \ C_{k,k} = \mu_{k,k} = \left|M_{k-1}^{-1}\right|_{m_k}. \tag{21}$$

Нейронная сеть для вычисления по формуле (20) с использованием синаптических весов (21) интервально-индексной характеристики $\hat{\mathfrak{I}}_k(X)$ реализует операционную последовательность

$$\left\langle R_i = PM\_\mathrm{Reduc}(\chi_i; C_{i,k}, b\_\mathrm{mod}\_i, m_k)\ \ (i=\overline{1,k});\right.$$
$$\left. s_k = \sum_{i=1}^{k} R_i;\ \ \Im_k(X) = \hat{\Im}_k(X) = PM\_\mathrm{Reduc}(s_k; 1, b\_s_k, m_k)\right\rangle. \tag{22}$$

В отличие от НС для вычисления нормированного компьютерного ИИ $\hat{I}_k(X)$ (см. рис. 2) НС для расчета $\hat{\Im}_k(X)$ согласно схеме (22) не содержит НСКК для получения нормированных остатков $\chi_{1,k-1}$, $\chi_{2,k-1}$, …, $\chi_{k-1,k-1}$. Поэтому в структурном отношении она является более простой. Вместе с тем, как видно из сравнения условий (3) и (18) с учетом (17), налагаемых на k-е основание минимально избыточной МСС теоремами 1 и 3, применение ненормированных интервально-индексных характеристик вместо нормированных требует примерно k-кратного увеличения модуля m_k по отношению к остальным модулям МСС, а следовательно и адекватного повышения аппаратурных затрат по модулю m_k. Кроме того, отмеченное обстоятельство приводит к неоднородности нейросетевых вычислительных МИМА-структур соответствующего класса.

Заключение. Основные результаты представленных в сообщении исследований по проблематике создания нейросетевых МВС для высокоскоростных МА-приложений различного назначения, включая приложения в области защиты информации, состоят в нижеследующем.

Дана математическая формализация редукционного метода позиционно-модулярного кодового преобразования больших чисел, который ориентирован на создание расширенного класса нейронных сетей конечного кольца – НСКК, осуществляющих приведение к остаткам по модулям МСС масштабируемых целых чисел. Это открывает принципиально новые возможности для построения нейросетевых конфигураций компьютерных алгоритмов МА.

Новые возможности модифицированной редукционной технологии синтеза нейросетевых МВС продемонстрированы на примере параллельной НС для расчета интегральных характеристик минимально избыточного модулярного кода. Структура предложенной НС отличается высоким уровнем однородности, а также простотой реализации.

В целях снижения сложности синтезированной НС для вычисления базовой интервально-индексной характеристики минимально избыточной МА исследован альтернативный вариант разработанной НС, осуществляющий формирование ненормированных интегральных характеристик минимально избыточного модулярного кода. Показано, что применение ненормированной интервально-индексной характеристики приводит к структурному упрощению базовой НС. При этом, однако, существенно увеличиваются (примерно в k раз) аппаратурные затраты по модулю интервального индекса – k-му модулю МСС.

Список использованных источников

1. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков [и др.]. – М., 2017. – 400 с.

2. Ananda Mohan, P. V. Residue number systems: Theory and applications / P. V. Ananda Mohan. – Basel, 2016. – 351 p. https://doi.org/10.1007/978-1-4615-0997-4

3. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М., 2012. – 280 с.

4. Инютин, С. А. Основы модулярной алгоритмики / С. А. Инютин. – Ханты-Мансийск, 2009. – 347 с.

5. Omondi, Amos. Residue number systems: Theory and implementation / Amos Omondi, Benjamin Premkumar. – Singapore, 2007. – 311 p. https://doi.org/10.1142/9781860948671

6. Оцоков, Ш. А. Способ организации высокоточных вычислений в модулярной арифметике / Ш. А. Оцоков // Первая международная конференция «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах»: сб. науч. трудов. – Ставрополь, 2014. – С. 270–277.

7. Комарова, Ю. А. Аналитический обзор методов и структур для работы с большими данными / Ю. А. Комаров, И. А. Талалаев // Первая международная конференция «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах»: сб. науч. трудов. – Ставрополь, 2014. – С. 477–485.

8. Афонин, М. С. Способ обработки больших чисел на ПЛИС с малой ресурсной мощностью / М. С. Афонин // Первая международная конференция «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах»: сб. науч. трудов. – Ставрополь, 2014. – С. 511–520.

9. Червяков, Н. И. Нейронные сети конечного кольца для реализации пороговых схем разделения секрета / Н. И. Червяков, А. А. Евдокимов // Нейрокомпьютеры: разраб., применение. – 2007. – № 2–3. – С. 45–50.

10. Нейронная сеть конечного кольца: пат. № 2279132 РФ. МКП G06N3/04. / Ю. А. Стрекалов, Н. И. Червяков, В. А. Галкина, С. В. Лавриненко. – Опубл.: 27.06.2006.

11. Червяков, Н. И. Нейронная сеть конечного кольца прямого распространения для операций на эллиптических кривых / Н. И. Червяков, А. Б. Спельников, А. Ф. Мезенцева // Нейрокомпьютеры: разраб., применение. – 2008. – № 1–2. – С. 28–34.

12. Тихонов, Э. Е. Программно-аппаратная реализация нейронных сетей / Э. Е. Тихонов, А. А. Евдокимов. – Невинномысск, 2013. – 116 с.

13. Кондрашёв, А. В. Нейронная сеть для преобразования чисел, представленных в позиционном коде в систему остаточных классов / А. В. Кондрашёв, Д. В. Горденко, Д. Н. Павлюк // Исследования в области естественных наук. – 2015. – № 1 [Электронный ресурс]. – Режим доступа: http://science.snauka.ru/2015/01/8925. – Дата доступа: 25.04.2018.

14. Коляда, А. А. Обобщенная интегрально-характеристическая база модулярных систем счисления / А. А. Коляда // Информационные технологии. – 2017. – Т. 23, № 9. – С. 641–649.

15. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – СПб., 2009. – 176 с.

References

1. Chervjakov N. I., Koljada A. A., Ljahov P. A., Babenko M. G., Lavrinenko I. N., Lavrinenko A. V. *Modular Arithmetic and its Applications in Infocommunication Technologies*. Moscow, 2017. 400 p. (in Russian).

2. Ananda Mohan P. V. Residue number systems: Theory and applications. Basel, 2016. 351 p. https://doi.org/10.1007/978-1-4615-0997-4

3. Chervjakov N. I., Evdokimov A. A., Galushkin A. I., Lavrinenko I. N., Lavrinenko A. V. *The Use of Artificial Neural Networks and the Residual Class System in Cryptography*. Moscow, 2012. 280 p. (in Russian).

4. Injutin S. A. *Fundamentals of Modular Algorithms*. Khanty-Mansiysk, 2009. 347 p. (in Russian).

5. Omondi A., Premkumar B. Residue number systems: Theory and implementation. Singapore, 2007. 311 p. https://doi.org/10.1142/9781860948671

6. Otsokov Sh. A. The way to organize high-precision calculations in modular arithmetic. *Pervaya mezhdunarodnaya konferentsiya «Parallel'naya komp'yuternaya algebra i ee prilozheniya v novykh infokommunikatsionnykh sistemakh»: sbornik nauchnykh trudov* [*First International Conference "Parallel Computer Algebra and Its Applications in New Infocommunication Systems": collection of scientific papers*]. Stavropol, 2014, pp. 270–277 (in Russian).

7. Komarova Yu. A., Talalaev I. A. Analytical review of methods and structures for working with large data. *Pervaya mezhdunarodnaya konferentsiya «Parallel'naya komp'yuternaya algebra i ee prilozheniya v novykh infokommunikatsionnykh sistemakh»: sbornik nauchnykh trudov* [*First International Conference "Parallel Computer Algebra and Its Applications in New Infocommunication Systems": collection of scientific papers*]. Stavropol, 2014, pp. 477–485 (in Russian).

8. Afonin M. S. The way of processing large numbers on a PLIS with a small resource capacity. *Pervaya mezhdunarodnaya konferentsiya «Parallel'naya komp'yuternaya algebra i ee prilozheniya v novykh infokommunikatsionnykh sistemakh»: sbornik nauchnykh trudov* [*First International Conference "Parallel Computer Algebra and Its Applications in New Infocommunication Systems": collection of scientific papers*]. Stavropol, 2014, pp. 511–520 (in Russian).

9. Chervjakov N. I., Evdokimov A. A. Neural networks of the finite ring for the implementation of threshold separation schemes for secretion. *Nejrokomp'yutery: razrabotka, primenenie* [*Neurocomputers*], 2007, no. 2–3, pp. 45–50 (in Russian).

10. Strekalov Yu. A., Chervyakov N. I., Galkina V. A., Lavrinenko S. V. *Neural network of a finite ring*. Patent RF no 2279132 МКП G06N3/04. Publ.: 27.06.2006.

11. Chervjakov N. I., Spel'nikov A. B., Mezenceva A. F. Neural network of a finite ring of direct propagation for operations on elliptic curves. *Nejrokomp'yutery: razrabotka, primenenie* [*Neurocomputers*], 2008, no. 1–2, pp. 28–34 (in Russian).

12. Tihonov Je. E., Evdokimov A. A. *Software and Hardware Implementation of Neural Networks*. Nevinnomyssk, 2013. 116 p. (in Russian).

13. Kondrashov A. V., Gordenko D. V., Pavljuk D. N. Neural network to convert numbers presented in the position code in the residual class. *Researches in Science*, 2015. no. 1. Available at: http://science.snauka.ru/en/2015/01/8925 (accessed 25.04.2018) (in Russian).

14. Kolyada A. A. Generalized Integrated Characteristic Base of Modular Number System. *Informacionnye tehnologii* [*Information Technologies*], 2017, vol. 23, no. 9, pp. 641–649 (in Russian).

15. Vinogradov I. M. *Fundamentals of number theory*. Saint Petersburg, 2009. 176 p. (in Russian).

Информация об авторах

Чернявский Александр Федорович – академик, д-р техн. наук, профессор, заведующий лабораторией. Институт прикладных физических проблем имени А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: niipfp@bsu.by.

Коляда Андрей Алексеевич – д-р физ.-мат. наук, доцент, гл. науч. сотрудник. Институт прикладных физических проблем имени А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: razan@tut.by.

Протасеня Стелла Юрьевна – мл. науч. сотрудник. Институт прикладных физических проблем имени А. Н. Севченко БГУ (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: Estellita@mail.ru.

Information about the authors

Chernyavsky Alexander Fedorovich – Academician, D. Sc. (Engineering), Professor, Head of the Laboratory. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: niipfp@bsu.by.

Kolyada Andrey Alexeyevich – D. Sc. (Physics and Mathematics), Accociate professor, Chief researcher. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: razan@tut.by.

Protasenya Stella Yuryevna – Junior researcher. Institute of Applied Physical Problems named after A. N. Sevchenko of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: Estellita@mail.ru.