Доклады Национальной академии наук Беларуси

2015 **ноябрь–декабрь** **Том 59 № 6**

ИНФОРМАТИКА

УДК 004.9, 004.94

Академик А. Ф. ЧЕРНЯВСКИЙ, А. А. КОЛЯДА

ВЫЧИСЛЕНИЕ ИНТЕГРАЛЬНЫХ ХАРАКТЕРИСТИК МИНИМАЛЬНО ИЗБЫТОЧНОГО МОДУЛЯРНОГО КОДА

Институт прикладных физических проблем имени А. Н. Севченко Белорусского государственного университета, Минск, Беларусь,
shabinskaya@rambler.ru; razan@tut.by

Сообщение посвящено проблематике оптимизации интегрально-характеристической базы модулярной арифметики (МА). Показано, что при минимальной кодовой избыточности данная задача успешно решается для класса немодульных операций, которые реализуются с помощью интервально-индексных характеристик и интервально-модулярной формы целых чисел. Предложен новый расширенный алгоритм расчета интегральных характеристик минимально избыточного модулярного кода, позволяющий строить конфигурации МА как на диапазонах неотрицательных чисел, так и на симметричных диапазонах. При длине минимально избыточного модулярного кода от 8 до 64 цифр синтезированный алгоритм превосходит известные аналоги для вычислений, связанных с интервально-индексными характеристиками в 6–34,4 раз по временным затратам и в 3,5–31,5 раз по затратам табличной памяти.

Ключевые слова: модулярная арифметика, минимально избыточный модулярный код, интегральные характеристики модулярного кода.

A. F. CHERNYAVSKY, A. A. KOLYADA

CALCULATION OF THE INTEGRAL CHARACTERISTICS OF MINIMALLY REDUNDANT MODULAR CODE

A. N. Sevchenko Institute of Applied Physics Problems of the Belarusian State University, Minsk, Belarus
shabinskaya@rambler.ru; razan@tut.by

The article is devoted to a perspective of optimization of the integrated and characteristic base of modular arithmetics (MA). It is shown that at the minimum code redundancy, this problem is successfully solved for a class of non-modular operations which are realized by means of interval and index characteristics and the interval and modular form of integers. Proposed is a new expanded algorithm of calculation of integrated characteristics of the minimally reductant modular code allowing one to build MA configurations both over the ranges of non-negative numbers and over the symmetric ranges. With a length of the minimally redundant modular code from 8 to 64 figures, the synthesized algorithm is superior to the known analogs for calculations connected with interval and index characteristics in time-consuming by a factor of 6–34.4 and in table memory-consuming by a factor 3.5–31.5.

Keywords: modular arithmetics, minimally redundant modular code, integral characteristics of minimally redundant modular code.

Введение. В настоящее время арифметика модулярных систем счисления (МСС) активно применяется в таких областях, как цифровая обработка сигналов, обработка изображений, защита информации, распределенные инфокоммуникационные технологии, связь, облачные вычисления в ряде других современных приложений [1–7]. Это обусловлено тем, что, благодаря кодовому параллелизму, МСС имеют ряд фундаментальных преимуществ над позиционными системами счисления. К таким преимуществам, в частности, относятся:

независимость длительности модульных (кольцевых) операций от количества оснований, а значит и от длины кода МСС;

высокая скорость вычислений в диапазонах больших чисел;

эффективность модулярных кодовых конструкций с контролем ошибок и сбойных ситуаций;

уникальность адаптационных свойств модулярной арифметики (МА) к технологиям электроники, табличным реализациям, реализациям на программируемых логических интегральных схемах, а также к передовым параллельным вычислительным технологиям, например, к технологиям на основе искусственных нейронных сетей;

гибкость базовых механизмов реконфигурирования МА-структур.

Известные разработки по теории и приложениям модулярной вычислительной технологии ориентированы на реализацию как перечисленных, так и других ключевых достоинств МСС в максимальной мере. Центральное место в рамках сформулированной стратегии отводится исследованиям по оптимизации методов и алгоритмов выполнения в МСС немодульных операций. Эффективную компьютерно-арифметическую базу для решения оптимизационных проблем МА составляет арифметика минимально избыточных МСС (МИМСС) [8].

Главным фактором, оказывающим наибольшее влияние на качественные показатели алгоритмов немодульных операций, является уровень вычислительной сложности расчетных соотношений для базовых интегральных характеристик модулярного кода (МК) и связанных с ними форм целых чисел (ЦЧ) [9; 10]. Приоритетные позиции в этом отношении принадлежат интервально-индексным характеристикам и интервально-модулярной форме (ИМФ) ЦЧ. При минимально избыточном модулярном кодировании указанная интегрально-характеристическая база позволяет синтезировать немодульные процедуры, которые в сравнении с неизбыточными аналогами обеспечивают значительное упрощение операций, требующих детектирования местоположения ЦЧ в диапазонах МСС, ряда других операций. К таким операциям относятся масштабирование, деление (общий случай), определение знака числа, контроль переполнения, обнаружение и исправление ошибок с помощью корректирующих МК.

В настоящем сообщении представлен новый алгоритм расчета интегральных характеристик минимально избыточного МК (МИМК), который является эффективной основой для построения конфигураций арифметики МСС, охватывающих практически весь спектр современных МА-приложений.

Итегрально-характеристическая база МСС с диапазонами неотрицательных целых чисел. Введем обозначения:

$\lfloor a \rfloor$ 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.

$|A|_m$ – элемент кольца $\mathbf{Z}_m$, сравнимый с A (в общем случае рациональным числом) по модулю m.

$\mathrm{sn}(a)$ – знаковая функция вида $\mathrm{sn}(a) = \begin{cases} 0, \text{ если } & a \geq 0, \\ 1, \text{ если } & a < 0. \end{cases}$

$\mathbf{M}\_l = \{m_1, m_2, \ldots, m_l\}$ – базис МСС, состоящий из $l > 1$ попарно простых модулей (оснований).

$M_j = \prod_{s=1}^{j} m_s$, $M_{i,j} = M_j / m_i$ $(i = \overline{1, j})$ – константы МСС с базисом $\mathbf{M}\_j$ $(1 < j \leq l)$.

В МСС с базисом $\mathbf{M}\_l$ ЦЧ X представляется кодом $(\chi_1, \chi_2, \ldots, \chi_l)(\chi_i = |X|_{m_i};\ i = \overline{1, l})$. Максимальная мощность множества $\mathbf{D}\_l$ чисел, на котором отображение $X \to (\chi_1, \chi_2, \ldots, \chi_l)$ взаимно однозначно составляет M_l элементов. В этом случае $\mathbf{D}\_l$ выполняет роль диапазона МСС с базисом $\mathbf{M}\_l$. Обычно в качестве диапазонов используют $\mathbf{Z}_{M_l}$ или $\mathbf{Z}_{M_l}^-$.

Из Китайской теоремы об остатках следует, что ЦЧ $X \in \mathbf{D}\_l$ может быть получено по своему МК $(\chi_1, \chi_2, \ldots, \chi_l)$ с помощью равенства

$$X = \sum_{i=1}^{l-1} M_{i,l-1} \left| M_{i,l-1}^{-1} \chi_i \right|_{m_l} + M_{l-1} I_l(X), \tag{1}$$

где $I_l(X)$ – интервальный индекс (ИИ) числа X относительно базиса $\mathbf{M}\_l$ [8; 9].

Выражение (1) называется интервально-модулярной формой ЦЧ X.

Компоненты $\hat{I}_l(X)=|I_l(X)|_{m_l}$ и $J_1(X)=\lfloor I_l(X)\,/\,m_l\rfloor$ представления ИИ $I_l(X)$ вида

$$I_l(X)=\hat{I}_l(X)+m_lJ_l(X) \tag{2}$$

называется компьютерным и главным ИИ ЦЧ X относительно базиса $\mathbf{M}\_l$.

Справедливо следующее утверждение

Т е о р е м а 1. *Для ИИ $I_l(X)$ произвольного элемента $X=(\chi_1,\chi_2,...,\chi_l)$ диапазона $\mathbf{Z}_{M_l}$ МСС с основаниями $m_1, m_2, ..., m_{l-1}, m_l \geq l-2$ верна формула*

$$I_1(X)=\hat{I}_l(X)-m_1\Theta_1(X), \tag{3}$$

где

$$\hat{I}_l(X)=\left|\sum_{i=1}^{l}R_{i,l}(\chi_i)\right|_{m_l}; \tag{4}$$

$$R_{i,l}(\chi_i)=|-m_i^{-1}\,|M_{i,\,l-1}^{-1}\chi_i\,|_{m_i}|_{m_l}\ \ (i=\overline{1,\,l-1}),\ \ R_{l,\,l}(\chi_l)=\left|\frac{\chi_l}{M_{l-1}}\right|_{m_l}; \tag{5}$$

$\Theta_l(X)$ − *минимальная интегральная характеристика МК (ИХМК) l-го порядка вида* $(\Theta_l(X)\in\{0,1\})$.

Наряду с интервально-индексными характеристиками $I_l(x)$, $\hat{I}_l(x)$, $J_l(x)$ и минимальными ИХМК $\Theta_l(X)$ при разработке методов выполнения немодульных операций используются и другие характеристики. В частности, интервальный номер $N_l(X)=\lfloor X\,/\,M_l\rfloor$ ЦЧ X относительно базиса $\mathbf{M}\_l$ $(l\geq 1)$ и цифры полиадического кода $\langle x_l\,x_{l-1}\ldots x_1\rangle$ числа $|X|_{M_l}$, которые определяются его полиадической формой

$$|X|_{M_l}=\sum_{i=1}^{l}M_{i-1}\,x_i\ \ (M_0=1;\ x_i\in\mathbf{Z}_{m_i}). \tag{6}$$

Для данных ИХМК верны нижеследующие утверждения.

Т е о р е м а 2. *Для интервального номера $N_l(X)$ произвольного неотрицательного ЦЧ X относительно модулей $m_1, m_2, ..., m_{l-1}, m_l \geq l-2$ имеет место равенство $N_l(X)=J_l(X)+\Theta_l(X)$, где $J_l(X)$ – главный ИИ числа X, а $\Theta_l(X)$ – отвечающая ему минимальная ИХМК l-го порядка $(\Theta_l(X)\in\{0,1\})$.*

Т е о р е м а 3. *Пусть в МСС с базисом $M\_k=\{m_1, m_2, ..., m_k\}$ задан произвольный элемент $X=(\chi_1,\chi_2,...,\chi_k)$ диапазона $\mathbf{Z}_{M_k}$ и пусть*

$$L_l(X)\ =\sum_{i=1}^{l-1}M_{i,l-1}\left|M_{i,l-1}^{-1}\chi_i\right|_{m_i}+M_{i,l-1}\hat{I}_l(X)\ \ (2\leq l\leq k), \tag{7}$$

$\hat{I}_l(X)$ определяется согласно (4), (5). Тогда для коэффициентов полиадической формы числа X (см. (6))

$$X=\sum_{i=1}^{k}M_{i-1}x_i\ \ (\ x_i\in\mathbf{Z}_{m_i}), \tag{8}$$

верны формулы

$$x_1=\chi_1,\ x_2=\hat{I}_2(X),\ x_3=\hat{x}_3,\ \hat{x}_l=|\hat{x}_l+\Theta_{l-1}(X)|_{m_l}\ \ (l=\overline{4,k}),$$

где $\hat{x}_l=\left|J_{l-1}(L_l(X))\right|_{m_l}$ $(l=\overline{3,k})$; $J_{l-1}(L_l(X))$ − *главный ИИ ЦЧ (7) $L_1(X)$ в МСС с базисом M_l, вычисляемый по правилу* $J_{l-1}(L_l(X))=\hat{\rho}_{l-1}(X)+\hat{I}_l(X)$; $\hat{\rho}_{l-1}(X)=\left\lfloor m_{l-1}^{-1}\sum_{i=1}^{l-1}R_{i,l-1}(\chi_i)\right\rfloor$; *вычеты $R_{i,l-1}(\chi_i)$ определяются по формулам (5) заменой l на $(l-1)$; $\Theta_{l-1}(X)$ − минимальная ИХМК $(l-1)$-го порядка, которая при $m_{l-1}\geq l-3$ принимает значения 0 или 1.*

Основой для расчета минимальных ИХМК по разработанной интервально-индексной технологии служат приводимые ниже теоремы, а также операция сужения ИМФ ЦЧ [8–10].

Т е о р е м а 4. *Для минимальной ИХМК* $\Theta_l(X)$*, отвечающей числу* X *в МСС с основаниями* $m_1, m_2, ..., m_{l-1}, m_l \geq l-2$ $(l > 1)$*, справедлива формула* $\Theta_l(X) = 1 - \mathrm{sn}(Z_l(X))$*, где* $Z_l(X) = L_l(X) - M_l$*; ЦЧ* $L_l(X)$ *определяется соотношением (7).*

Т е о р е м а 5. *Пусть числу* X *по базису* $\mathbf{M}\_k$ *отвечает МК* $(\chi_1, \chi_2, ..., \chi_k)$ *и пусть* $J_l(X)$ *– главный ИИ ЦЧ* X *относительно* $m_1, m_2, ..., m_{l-1}, m_l \geq l-2$ $(2 \leq l \leq k)$*. Знаки чисел* X *и* $J_l(X)$ *совпадают при* $l = 2$*, а также при* $l > 2$*, если* $J_l(X) \neq -1$.

Интегрально-характеристическая база МИМСС. Как известно [8; 11], использование в числовых системах кодовой избыточности, как правило, позволяет улучшить их арифметические и иные свойства. Так называемое минимально избыточное модулярное кодирование, определяемое базисом $\mathbf{M}\_k$, предусматривает применение диапазонов, мощность которых меньше мощности соответствующих диапазонов неизбыточной (классической) МСС с тем же базисом $\mathbf{M}\_k$. Сущность реализуемого принципа раскрывает нижеследующее утверждение.

Т е о р е м а 6. Для того, чтобы в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_k$ ИИ $I_k(X)$ каждого элемента $X = (\chi_1, \chi_2, ..., \chi_k)$ диапазонов $\mathbf{D} = \mathbf{Z}_{2M}^{-} = \{-M, -M+1, ..., M-1\}$ и $\mathbf{Z}_M = \{0, 1, \ldots, M-1\}$ ($M = m_0 M_{k-1}$; m_0 – вспомогательный модуль) полностью определялся компьютерным ИИ – вычетом $\hat{I}_k(X) = \left|I(X)\right|_{m_k}$ (см. (2)) необходимо и достаточно, чтобы k-е основание удовлетворяло условиям $m_k \geq 2m_0 + k - 2$ и $m_k \geq m_0 + k - 2$ ($m_0 \geq k-2$), при этом для $I_k(X)$, справедливо расчетное соотношение

$$I_k(X) = \hat{I}_k(X) - m_k\ \mathrm{sn}(m_0 - 1 - \hat{I}_k(X)) = \begin{cases} \hat{I}_k(X), & \text{если } \hat{I}_k(X) < m_0, \\ \hat{I}_k(X) - m_k, & \text{если } \hat{I}_k(X) \geq m_0, \end{cases} \tag{9}$$

где $\hat{I}_k(X)$ вычисляется согласно (4), (5) при $l = k$.

Главное преимущество МИМСС над неизбыточными аналогами заключается в значительном упрощении вычисления интервально-индексной характеристики $I_k(X)$. Сравнение формул (3) и (9) показывает, что переход от неизбыточного к минимально избыточному кодированию позволяет заменить в расчетном соотношении для ИИ $I_k(X)$ минимальную ИХМК $\Theta_k(X)$, определяемую по общей схеме в рамках трудоемкой процедуры сужения ИМФ ЦЧ (см. теоремы 4, 5) [8–10], на характеристику $\mathrm{sn}(m_0 - 1 - \hat{I}_k(X))$, которая имеет тривиальную вычислительную структуру. При табличной реализации (9) расчет ИИ $I_k(X)$ осуществляется за одну модульную операцию.

Другим важным достоинством МИМСС является простота оперирования в симметричных диапазонах. В отличие от неизбыточных МСС [10] идентификация отрицательной и неотрицательной компонент рабочего диапазона $\mathbf{Z}_{2M}^{-}$ МИМСС выполняется с помощью интервального номера $N(X) = \lfloor X / M \rfloor$, формируемого в соответствии с теоремой 2 по главному ИИ $J(x) = \lfloor I_k(X) / m_0 \rfloor$ и минимальной ИХМК $\Theta(X)$, отвечающих числу $X \in \mathbf{Z}_{2M}^{-}$ в МСС с базисом $\{m_1, m_2, \ldots, m_k - 1, m_0\}$ и диапазоном $\mathbf{Z}_M$ без использования четного модуля m_k. Необходимость в данном ограничении отпадает.

Для расчета интегральных характеристик МИМК целиком применимы несколько модифицированные методологические и алгоритмические средства, разработанные для неизбыточных МСС [9; 10]. Требуемые изменения связаны с упрощением вычисления в МИМСС интервально-индексной характеристики $I_k(X)$. Наряду с теоремой 6 основой минимально избыточной версии процедуры расчета ИХМК – РИХ_1–РИХ_7, синтезированной в [10], служат ИМФ (1), евклидовы составляющие $\hat{I}(X) = \left|I_k(X)\right|_{m_0}$ и $J(X) = \lfloor I_k(X) / m_0 \rfloor$ ИИ $I_k(X)$ относительно вспомогательного модуля m_0 (см. (2)), а также интервальный номер $N(X)$ и минимальная ИХМК $\Theta(X)$, которые с учетом теорем 1, 2, 4, 5 дают следующие базовые соотношения:

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_k} + M_{k-1} \hat{I}(X) + M \cdot J(X) \quad (X \in \mathbf{Z}_{2M}^{-});$$

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_k} + M_{k-1} I_k(X) \left(\left|X\right|_M + M(J(X) + \Theta(X) \right) =$$

$$\left|X\right|_M + M \cdot N(X) \quad (I_k(\left|X\right|_M) = \hat{I}(X) - m_0 \Theta(X);$$

$$N(X) = \lfloor X / M \rfloor = J(X) + \Theta(X));$$

$$\mathrm{sn}(X) = \mathrm{sn}(N(X)) = \mathrm{sn}(J(X) + \Theta(X)).$$

Алгоритм расчета интегральных характеристик минимально избыточного модулярного кода. На основании изложенных теоретических положений технологии вычисления ИХМК для расчета характеристик кода МИМСС синтезирован новый расширенный алгоритм, который заключается в нижеследующем.

Параметры алгоритма: попарно простые модули $m_1, m_2, \ldots, m_k$ базовой МИМСС с диапазоном $\mathbf{Z}_{2M}^{-} = \{-M+1, ..., M-1\}$ ($M = m_0\ M_{k-1}$), удовлетворяющие условиям $m_l \ge l-1$ ($l = \overline{2, k-1}$), $m_k \ge 2m_0 + k - 2$, $m_0 \ge k - 2$.

Входные данные: МИМК $(\chi_1, \chi_2, ..., \chi_k)$ произвольного элемента X диапазона $\mathbf{Z}_{2M}^{-}$ по базису $\{m_1, m_2, \ldots, m_k\}$.

Выходные данные:

минимальные ИХМК $\Theta_l(X)$ $(l = \overline{3, k})$ и $\Theta(X)$, отвечающие числу X в МСС с базисами $\{m_1, m_2, \ldots, m_l\}$ и $\{m_1, m_2, \ldots, m_{k-1}, m_0\}$ соответственно;

ИИ $I_k(X)$ и знак $\mathrm{sn}(X)$ элемента X диапазона $\mathbf{Z}_{2M}^{-}$;

ИИ $I_k(|X|_{M_k})$ и полиадический код $\langle x_k x_{k-1} \ldots x_1 \rangle$ ЦЧ $|X|_{M_k} \in \mathbf{Z}_{M_k}$;

ИИ $I_k(|X|_M)$ и полиадический код $\langle x\, x_{k-1} \ldots x_1 \rangle$ ЦЧ $|X|_M$, рассчитанные по базису $\{m_1, m_2, \ldots, m_{k-1}, m_0\}$.

Предварительно получаемые данные:

таблицы ТИi интервального индекса, которые в соответствии с (5) генерируются по правилам: $\text{ТИ}i[c] = R_{i,k}(\chi) = |-m_i^{-1}\, |M_{i,\,k-1}^{-1}\chi|_{m_i}|_{m_k}$ $(\chi = \overline{0, m_i - 1},\ i = \overline{1, k-1})$, $\text{ТИ}k[c] = R_{k,\,k}(\chi) = \left|\dfrac{\chi}{M_{k-1}}\right|_{m_k}$ $(\chi = \overline{0, m_k - 1})$;

коэффициенты нормировки цифр МК

$$C_{i,l-1} = \left|M_{i,l-1}^{-1}\right|_{m_i},\ C_{l,l} = \left|M_{l-1}^{-1}\right|_{m_l} \quad (i = \overline{1, l-1};\ l = \overline{2, k-1}).$$

Тело алгоритма расчета интегральных характеристик МИМК

РИХ_МИМК.1. Для МИМК $(\chi_1, \chi_2, \ldots, \chi_k)$ получить наборы вычетов $R_l = \{R_{1,l}(\chi_1), R_{2,l}(\chi_2), ..., R_{l-1,l}(\chi_{l-1}), R_{l,l}(\chi_l)\}$ $(l = \overline{2, k-1})$, где

$$R_{i,l}(\chi_i) = \left|-m_i^{-1}\left|C_{i,l-1}\ \chi_i\right|_{m_i}\right|_{m_l} \quad (i = \overline{1, l-1}),\ R_{l,l}(\chi_l) = \left|C_{l,l}\ \chi_l\right|_{m_l}.$$

РИХ_МИМК.2. Рассчитать характеристики $\hat{I}_l(X)$, $\hat{\rho}_l(X)$ $(l = \overline{2, k-1})$, а также $\hat{I}_k(X)$, следуя схемам

$$\left\langle s_l = \sum_{i=1}^{l} R_{i,l}(\chi_i),\ \hat{I}_l(X) = \left|s_l\right|_{m_l},\ \hat{\rho}_l(X) = \lfloor s_l / m_l \rfloor \right\rangle;$$

$$\left\langle s_k = \sum_{i=1}^{k} \text{ТИ}i[\chi_i],\quad \hat{I}_k(X) = \left|s_k\right|_{m_k} \right\rangle.$$

РИХ_МИМК.3. С помощью (8) для X найти ИИ $I_k(X)$ и его эвклидовы составляющие $\hat{I}(X) = \left|I_k(X)\right|_{m_0}$, $J(X) = \lfloor I_k(X) / m_0 \rfloor$, реализуя действия:

РИХ_МИМК.3А. При $\hat{I}_k(X) < m_0$ положить $I_k(X) = \hat{I}_k(X)$, $\hat{I}(X) = \hat{I}_k(X)$, $J(X) = 0$ и перейти к РИХ_МИМК.4.

РИХ_МИМК.3Б. Интервально-индексным характеристикам $I_k(X)$, $\hat{I}(X)$ и $J(X)$ присвоить значения $I_k(X) = \hat{I}_k(X) - m_k$, $\hat{I}(X) = I_k(X) + m_0$, $J(X) = -1$.

РИХ_МИМК.3В. В случае $\hat{I}(X) < 0$ выполнить корректирующие операции: $\hat{I}(X) = \hat{I}(X) + m_0$, $J(X) = -2$.

РИХ_МИМК.4. Для каждого $l \in \{3, 4, ..., k\}$ выполнить:

РИХ_МИМК.4А. Найти $\hat{x}_l = \hat{\rho}_{l-1}(X) + \hat{I}_l(X)$, $J_{l-1} = \hat{x}_l - m_l$.

РИХ_МИМК.4Б. Обнулить булеву переменную S_l, а при $l \ne 3$ и переменную δ_l;

РИХ_МИМК.4В. Если $J_{l-1} \ge 0$, то положить $\hat{x}_l = J_{l-1}$, $S_l = 1$ и перейти РИХ_МИМК.5.

РИХ_МИМК.4Г. При $J_{l-1} = -1$ $(l \ne 3)$ переменной δ_l; присвоить значение $\delta = 1$.

РИХ_МИМК.5. Реализовать операционную последовательность:

РИХ_МИМК.5А. Получить $\hat{x} = \hat{\rho}_{k-1}(X) + \hat{I}(X)$, $J = \hat{x} - m_0$.

РИХ_МИМК.5Б. Обнулить булевы переменные S и δ ($S = \delta = 0$).

РИХ_МИМК.5В. Если $J \geq 0$, то положить $\hat{x} = J$, $S = 1$ и перейти к РИХ_МИМК.6.

РИХ_МИМК.5Г. В случае, когда $J = -1$, переменной δ присвоить значение $\delta = 1$.

РИХ_МИМК.6. Принимая во внимание равенство $\Theta_2(X) = 0$, сформировать минимальные ИХМК $\Theta_3(X), \Theta_4(X), ..., \Theta_{l-1}(X), \Theta_l(X), \Theta(X)$ согласно правилам $\Theta_l(X) = S_l \vee \delta_l \Theta_{l-1}(X)$ ($l = \overline{3, k}$); $\Theta(X) = S \vee \delta\Theta_{k-1}(X)$.

РИХ_МИМК.7. В дополнение к вычисленным ИХМК, определить:

знак $\mathrm{sn}(X) = \mathrm{sn}(J(X) + \Theta(X))$ ЦЧ $X \in \mathbf{Z}_{2M}^{-}$;

ИИ $I_k(|X|_{M_k}) = \hat{I}_k(X) - m_k\Theta_k(X)$ и цифры $x_1 = \chi_1, x_2 = \hat{I}_2(X), x_3 = \hat{x}$, $x_l = \begin{cases} 0, & \text{если } \delta_l\Theta_{l-1}(X) = 1, \\ \hat{x}_l + \Theta_{l-1}(X), & \text{если } \delta_l\Theta_{l-1}(X) = 0, \end{cases}$ ($l = \overline{4, k}$), полиадического кода $\langle x_k\, x_{k-1} ... x_1 \rangle$ числа $|X|_{M_k} = (\chi_1, \chi_2, ..., \chi_k)$;

ИИ $I_k(|X|_M) = \hat{I}(X) - m_0\Theta(X)$ и старшую k-ю цифру $x = \begin{cases} 0, & \text{если } \delta\Theta_{k-1}(X) = 1, \\ \hat{x} + \Theta_{k-1}(X), & \text{если } \delta\Theta_{k-1}(X) = 0, \end{cases}$ полиадического кода $\langle x_k\ \ x_{k-1} ... x_1 \rangle$ элемента $|X|_M$ диапазона $\mathbf{Z}_M$.

РИХ_МИМК.8. Завершить работу алгоритма.

Реализуемый в алгоритме РИХ_МИМК.1–РИХ_МИМК.8 инструментарий вспомогательного модуля m_0, открывающий принципиально новые возможности для расширения набора базовых ИХМК при разработке немодульных процедур, может быть обобщен и на вспомогательные модули, кратные модулю m_0, в частности, на модуль вида $2m_0$. Это позволяет оперировать не только в диапазонах $\mathbf{Z}_{2M}^{-}$, $\mathbf{Z}_M^{-}$, но и в диапазоне $\mathbf{Z}_{2M}$, в том числе на его составных компонентах $\mathbf{Z}_M$ и $\mathbf{Z}_{2M} \setminus \mathbf{Z}_M$.

Из алгоритма РИХ_МИМК.1–РИХ_МИМК.8 видно, что благодаря использованию кодовой избыточности вычислительная сложность расчетных соотношений для интервально-индексных характеристик $I_k(X)$, $\hat{I}(X)$, $J(X)$, а следовательно, и интервального номера $N(X)$ ЦЧ X в сравнении с неизбыточными аналогами [9; 10] существенно уменьшается. Получение в рамках алгоритмов РИХ.1–РИХ.5 и РИХ_1–РИХ_7 ИИ $I_k(X)$ ЦЧ X, заданного неизбыточным МК $(\chi_1, \chi_2, ..., \chi_k)$ требует $0{,}5(k^2 + 5k - 12)$ модульных операций (МО) и $0{,}5k(k - 1)$ таблиц для хранения вычетов. Соответствующие затраты на вычисление ИИ в МИМСС согласно теореме 6 составляют k МО и k таблиц для вычетов. Таким образом, коэффициенты повышения эффективности за счет использования минимальной избыточности в случае расчета ИИ принимают значения: $K_{\text{МО, ИИ}} = (k^2 + 5k - 12) / (2k)$ для числа МО и $K_{\text{Т, ИИ}} = (k - 1) / 2$ для количества необходимых таблиц. Например, при k = 8; 16; 32; 64 аналитические оценки дают $K_{\text{МО, ИИ}}$ = 6; 10,125; 18,3125; 34,40625 и $K_{\text{Т, ИИ}}$ = 3,5; 7,5; 15,5; 31,5.

Из приведенных данных ясно, что указаны показатели эффективности алгоритмических структур, базирующихся на ИИ, с увеличением числа k оснований МИМСС возрастают, асимптотически приближаясь к порогу k / 2. Именно это обстоятельство и является определяющим фактором, который обеспечивает версиям МИМА с преимущественным использованием интервально-индексных характеристик, приоритетные позиции, особенно в области быстрых вычислений на диапазонах больших чисел.

Заключение. Основные результаты представленной в настоящей статье разработки по проблематике оптимизации немодульных операций в МСС состоят в нижеследующем.

1. Для МИМСС сформирована интегрально-характеристическая база, которая оптимизирована по критериям вычислительной сложности и функциональным возможностям. Ключевыми ее составляющими являются интервально-индексные характеристики (ИИ, компьютерный ИИ и главный ИИ), минимальные ИХМК, а также интервально-модулярные формы ЦЧ.

2. Максимальный уровень уменьшения сложности времени реализации созданная интегрально-характеристическая база обеспечивает в классе немодульных процедур, которые требуют вычислений с использованием ИМФ чисел. Прежде всего, к таким процедурам относятся расширение МИМК, масштабирование, деление (общий случай), контроль ошибок и т. п.

3. Являясь симметрической ИХМК, интервальный индекс позволяет существенно упростить оперирование в симметричных диапазонах, в частности, операции детектирования знака числа и контроль переполнения. Ключевую роль при этом выполняет также и минимальная ИХМК, формируемая по базису $\{m_1, m_2, ..., m_{k-1}, m_0\}$. Таким образом, созданная интегрально-характеристическая база МИМСС может служить основой конфигураций МА, ориентированных как на диапазоны неотрицательных ЦЧ, так и на симметричные диапазоны.

4. На основе построенной интегрально-характеристической базы предложен новый высокоэффективный алгоритм расчета интегральных характеристик МИМК. В сравнении с неизбыточными аналогами [9; 10] данный алгоритм за счет использования минимальной кодовой избыточности обеспечивает сокращение временных затрат и затрат табличной памяти для вычислений, связанных с ИИ, соответственно в $K_{\text{МО, ИИ}} = (k^2 + 5k - 12) / (2k)$ и $K_{\text{Т, ИИ}} = (k - 1) / 2$ раз. При $k = 8$; 16; 32; 64 указанные аналитические оценки дают $K_{\text{МО, ИИ}} = 6$; 10,125; 18,3125; 34,40625 и $K_{\text{Т, ИИ}} = 3{,}5$; 7,5; 15,5; 31,5. С увеличением k приведенные показатели эффективности разработанного алгоритма возрастают, асимптотически приближаясь к порогу $k / 2$.

Список использованной литературы

1. *Червяков, Н. И.* Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков. – М.: Физматлит, 2012. – 280 с.

2. Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики / А. Н. Каленик [и др.] // Информационные технологии. – 2012. – № 4. – С. 37–44.

3. Применение таблично-сумматорной вычислительной технологии для позиционно-модулярного кодового преобразования по схеме Горнера / А. А. Коляда [и др.] // 1-ая Международная конференция «Параллельная компьютерная алгебра и её приложения в новых инфокоммуникационных системах»: сб. науч. тр. − Ставрополь: Издательско-информационный центр «Фабула», 2014. – С. 247–252.

4. *Schinianakis, D.* Multifunction recidue architectures for cryptography / D. Schinianakis, T. Stouraitis // IEEE Trans. Circuits and Syst. I. – 2014. – Vol. 61, N 4. – P. 1156–1169.

5. *Червяков, Н. И.* Реализация модулярного вейвлет-преобразования в нейросетевом базисе / Н. И. Червяков, П. А. Ляхов // Нейрокомпьютеры: разраб., применение. – 2011. – № 11. – С. 18–25.

6. *Червяков, Н. И.* Реализация КИХ-фильтров в системе остаточных классов / Н. И. Червяков, П. А. Ляхов // Нейрокомпьютеры: разраб., применение. – 2012. – № 5. – С. 15–24.

7. *Червяков, Н. И.* Проектирование КИХ-фильтров в системе остаточных классов с модулями специального вида / Н. И. Червяков, П. А. Ляхов // Нейрокомпьютеры: разраб., применение. – 2014. – № 9. – С. 52–60.

8. *Коляда, А. А.* Модулярные структуры конвейерной обработки цифровой информации / А. А. Коляда, И. Т. Пак. – Минск: Университетское, 1992. – 256 с.

9. *Коляда, А. А.* Интегрально-характеристическая база модулярных систем счисления / А. А. Коляда, А. Ф. Чернявский // Информатика. – 2013. – № 1. – С. 106–119.

10. *Коляда, А. А.* Интервально-индексный метод четного модуля для расчета интегральных характеристик кода неизбыточной МСС с симметричным диапазоном / А. А. Коляда, А. Ф. Чернявский // Докл. НАН Беларуси. – 2013. – Т. 57, № 1. – С. 38–45.

11. *Sengupta, Avik.* Redundant Number System Based Space-Time Block Codes / Avik Sengupta, Natarajan Balasobramariam // Phisycal communication. – 2014. – Vol. 12, N 9. – P. 1–15.

Поступило в редакцию 01.07.2015