УДК 004.9, 519.6

ОСОБЕННОСТИ МАШИННОЙ АРИФМЕТИКИ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ МОДУЛЯРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР

А. Ф. ЧЕРНЯВСКИЙ[1)]***, Е. И. КОЗЛОВА***[1)]***, А. А. КОЛЯДА***[1)]

[1)]*Институт прикладных физических проблем им. А. Н. Севченко БГУ,*
ул. Академика Курчатова, 7, 220045, г. Минск, Беларусь

Рассмотрены процедуры формирования модулярного кода для различных вариантов модулярных систем счисления. Определены особенности машинной арифметики базовых интегральных характеристик модулярного кода. Предложено доказательство теоремы о минимально избыточном модулярном кодировании как эффективном способе снижения времени вычисления интегральных характеристик модулярного кода. Показано, что введение в модулярный код минимальной избыточности существенно упрощает расчет интервально-индексных характеристик и связанных с ними форм представления целых чисел при реализации ряда немодульных операций. Отмечено некоторое уменьшение эффективности минимально избыточных модулярных систем счисления по мере увеличения в используемых приложениях количества интегральных характеристик модулярного кода, а также при изменении знака числа или цифр полиадического кода. Это обстоятельство не снижает целесообразности применения минимально избыточных модулярных систем счисления в широкой сфере приложений минимально избыточной модулярной арифметики, включая системы цифровой обработки сигналов, защиты информации, информационные технологии и др.

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

Благодарность. Работа выполнена в рамках государственной программы научных исследований «Цифровые и космические технологии, безопасность общества и государства» (подпрограмма «Цифровые технологии и космическая информатика», задание 5.1.6.3).

Образец цитирования:
Чернявский АФ, Козлова ЕИ, Коляда АА. Особенности машинной арифметики высокопроизводительных модулярных вычислительных структур. *Журнал Белорусского государственного университета. Математика. Информатика.* 2023; 2:94–101.
https://doi.org/10.33581/2520-6508-2023-2-94-101
EDN: EQLSUS

For citation:
Chernyavsky AF, Kozlova EI, Kolyada AA. Features of machine arithmetics of high-performance modular computing structures. *Journal of the Belarusian State University. Mathematics and Informatics.* 2023;2:94–101. Russian.
https://doi.org/10.33581/2520-6508-2023-2-94-101
EDN: EQLSUS

Авторы:
Александр Федорович Чернявский – доктор технических наук, академик НАН Беларуси, профессор; заведующий лабораторией специализированных вычислительных систем.
Елена Ивановна Козлова – кандидат физико-математических наук, доцент; научный сотрудник лаборатории специализированных вычислительных систем.
Андрей Алексеевич Коляда – доктор физико-математических наук; главный научный сотрудник лаборатории специализированных вычислительных систем.

Authors:
Alexander F. Chernyavsky, doctor of science (engineering), academician of the National Academy of Sciences of Belarus, full professor; head of the laboratory of specialised computer systems.
Elena I. Kozlova, PhD (physics and mathematics), docent; researcher at the laboratory of specialised computer systems.
kozlova@bsu.by
https://orcid.org/0000-0003-0317-7429
Andrey A. Kolyada, doctor of science (physics and mathematics); chief researcher at the laboratory of specialised computer systems.

FEATURES OF MACHINE ARITHMETICS OF HIGH-PERFORMANCE MODULAR COMPUTING STRUCTURES

A. F. CHERNYAVSKY[a], *E. I. KOZLOVA*[a], *A. A. KOLYADA*[a]

[a]*A. N. Sevchenko Institute of Applied Physical Problems,*
Belarusian State University, 7 Akademika Kurchatava Street, Minsk 220045, Belarus
Corresponding author: E. I. Kozlova (kozlova@bsu.by)

The procedures for generating a modular code for various variants of modular number systems are herein considered. The features of machine arithmetic of the basic integral characteristics of the modular code are noted. Proof of the theorem on minimally redundant modular coding is proposed as an effective way to reduce the time of computing the integral characteristics of a modular code. It is shown that the introduction of minimal redundancy into a modular code greatly simplifies the calculation of interval-index characteristics and related forms of representing integers when implementing a number of non-modular operations. We noted a certain decrease in the efficiency of minimally redundant modular number systems if the number of integral characteristics of the modular code, the sign of the number or digits of the polyadic code increases in the used applications. This circumstance does not reduce the expediency of using minimally redundant modular number systems in a wide range of applications of minimally redundant modular arithmetics, including digital signal processing, information security, information technology, etc.

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

Acknowledgements. This work was supported by the state programme of scientific research «Digital and space technologies, security of society and the state» (subprogramme «Digital technologies and space informatics», assignment 5.1.6.3).

Введение

Существующие формы параллельной обработки информации реализуются различными числовыми системами с параллельной структурой. В последние годы наблюдается рост внимания к исследованиям в области теории и приложений модулярных систем счисления (МСС), которые характеризуются максимальным уровнем внутреннего параллелизма. С точки зрения принципов высокоскоростных вариантов построения машинной арифметики наиболее существенными достоинствами МСС являются табличная структура алгоритмов, параллелизм базовых немодульных процедур, их модульность и простота конвейеризации на уровне операций над малоразрядными вычетами, высокая эффективность корректирующих кодовых конструкций.

В работе рассматриваются процедуры формирования модулярного кода для различных вариантов МСС [1–9]. Отмечаются особенности машинной арифметики базовых интегральных характеристик модулярного кода (ИХМК). Намеренно редко используется специальная математическая терминология, характерная для большинства публикаций выбранной тематики. По мнению авторов, это обеспечит положительную заинтересованность в прочтении статьи широким кругом специалистов радиофизического и инженерно-технического профиля.

Формирование модулярного кода

Устройства модулярного типа реализуют вычислительные процессы в виде последовательностей модульных операций сложения, вычитания и умножения целых чисел без анализа на переполнение. Арифметические процедуры над элементами диапазона **M** в МСС производятся независимыми друг от друга операциями по ее основаниям (каждому из модулей), что и определяет параллелизм таких систем. Обычно эти процессы сопровождаются операциями деления на константу (масштабирования), одиночными немодульными операциями и др.

Фундаментальную значимость в модулярной арифметике имеет процедура формирования модулярного кода $(x_1, x_2, \ldots, x_k)$, отвечающего множеству целых чисел **X** и удовлетворяющего системе сравнений

$$\begin{aligned} X &\equiv x_1 (\mathrm{mod}\, m_1), \\ X &\equiv x_2 (\mathrm{mod}\, m_2), \\ &\cdots\cdots\cdots\cdots \\ X &\equiv x_k (\mathrm{mod}\, m_k). \end{aligned} \qquad (1)$$

Если натуральные числа $m_1, m_2, \ldots, m_k$ попарно просты (каждый модуль m_i имеет по крайней мере два положительных делителя – m_i и 1), то решением этой системы является класс вычетов по модулю $M_k = \prod_{i=1}^{k} m_i$, который задается сравнением

$$X_{i=1}^{k} \equiv \sum_{i=1}^{k} M_{i,k}\mu_{i,k}x_i \pmod{M_k}, \tag{2}$$

где главные компоненты

$$M_{i,k} = \frac{M_k}{m_i},\ \mu_{i,k} = \left|M_{i,k}^{-1}\right|_{m_i},\ x_i = [X]_{m_i},\ i = \overline{1,\ k}.$$

Параметр $\left|M_{i,k}^{-1}\right|_{m_i} = x$, являющийся мультипликативной инверсией, т. е. обратным элементом по модулю m_i величины $M_{i,l}(i,\ l) = X$, определяется по стандартной формуле:

$$x_i = |X|_{m_i},$$

где

$$|X|_m = 1,\ m \in m_i. \tag{3}$$

В неизбыточных МСС каждому модулярному коду $(x_1, x_2, \ldots, x_k)$ отвечает целое число, а не класс вычетов, при этом взаимная однозначность обеспечивается выбором рабочего диапазона **D** на основе различных множеств вычетов. Эту роль, как правило, выполняют множества

$$Z_{M_k} = \{0, 1, \ldots, M_{k-1}\}$$

или

$$Z_{M_k}^{-} = \left\{-\left|\frac{M_k}{2}\right|, -\left|\frac{M_k}{2}\right| + 1, \ldots, \left|\frac{M_k}{2}\right| - 1\right\}.$$

При модулярном кодировании каждому $X \in \mathbf{D}$ ставится в соответствие код, представляющий собой набор $(x_1, x_2, \ldots, x_k)$ остатков $x_i = |X|_{m_i}$ от деления X на m_i, где $i = \overline{1,\ k}$. Используется запись $X = (x_1, x_2, \ldots, x_k)$.

Декодирующее отображение выполняется по правилам

$$X = \left|\sum_{i=1}^{k} M_{i,k}\mu_{i,k}x_i\right|_{M_k} \text{ при } X \in Z_{M_k},$$

$$X = \left|\sum_{i=1}^{k} M_{i,k}\mu_{i,k}x_i\right|_{M_k^{-}} \text{ при } X \in Z_{M_k}^{-}.$$

Пример 1. Решение системы сравнений (1) на основании класса вычетов по модулю M_k.
Представим целое число $X = 18$ модулярным кодом простых чисел ($m_1 = 2$, $m_2 = 3$, $m_3 = 11$, $m_4 = 13$).
Соответствующая система сравнений имеет вид

$$\begin{aligned} 18 &\equiv 0 \pmod{m_1 = 2}, \\ 18 &\equiv 0 \pmod{m_2 = 3}, \\ 18 &\equiv 7 \pmod{m_3 = 11}, \\ 18 &\equiv 5 \pmod{m_4 = 13}. \end{aligned} \tag{4}$$

На основании сравнения (2) для главных компонент системы сравнений (4) получаем

$$M_4 = 858,\ M_{1,4} = 429,\ M_{2,4} = 286,\ M_{3,4} = 78,\ M_{4,4} = 66,$$

$$x_1 = 0,\ x_2 = 0,\ x_3 = 7,\ x_4 = 5,$$

$$\mu_{3,4} = 1,\ \mu_{4,4} = 1.$$

Главные компоненты $\mu_{1,4}$ и $\mu_{2,4}$ не имеют значений.

Проверка: $X \equiv \sum_{i=1}^{4} M_{i,4}\mu_{i,4}x_i \pmod{858} = (78 \cdot 7 + 66 \cdot 5) \pmod{858} = 876 \pmod{858} = 18.$

Когда целое число $X \in Z_{M_k}^{-}$ представляется модулярным кодом элемента $|X|_{M_k}$ диапазона Z_{M_k}, соответствие между ними описывается выражением

$$X = |X|_{M_k} - \mathrm{sn}(X) M_k, \tag{5}$$

где $\mathrm{sn}(X)$ – знак данного числа.

Наряду с другими версиями модулярной арифметики на практике часто применяется версия, использующая полиадическую форму целого числа, которая имеет вид

$$|X|_{M_k} = \sum_{i=1}^{k} M_{i-1} x_i,\ X \in Z,\ M_0 = 1,\ x_i \in Z_{m_i}.$$

С учетом выражения (5) получаем равенство

$$\mathrm{sn}(X) = \left\lfloor \frac{2[X]_{M_k}}{M_k} \right\rfloor = \left\lfloor \frac{2x_k}{m_k} \right\rfloor,$$

где x_k – старший коэффициент полиадической формы целого числа $|X|_{M_k}$.

Алгоритм расчета ИХМК (ранга $\rho_k(X)$ интервального индекса $I_k(X)$ и полиадического кода $(x_k, \ldots, x_2, x_1)$ числа X) позволяет также определять знак числа из симметричного диапазона $Z_{M_k}^{-}$.

Модулярный код $(x_1, x_2, \ldots, x_k)$ в явном виде не содержит информацию о величине элементов его рабочего диапазона **D**. Для выполнения операций, каким-либо образом зависящих от местоположения элементов во множестве или за пределом диапазона **D**, в МСС используются определенные формы и операции представления целого числа через цифры модулярного кода. Базовые формы целого числа для немодульных операций включают одну или несколько ИХМК.

Для выполнения сложных немодульных операций (контроль переполнения, сравнение чисел, определение знака числа, округление, деление и др.) в МСС используются базовые ИХМК – ранг, ядро, минимальный след, коэффициенты полиадического представления чисел. Выбор ИХМК и методов их формирования определяет сложность соответствующих алгоритмов реализации немодульных процедур. Различные ИХМК позволяют в рамках определенного базового представления чисел выделять из модулярного кода числа искомую информацию о его величине.

Базовые интегральные характеристики МСС

Ранговая форма целого числа $|X|_{M_l}$ l-го порядка в МСС с основаниями $m_1, m_2, \ldots, m_l$ и диапазоном $Z_{M_l} = \{0, 1, \ldots, M_l - 1\}$ описывается выражениями [2]

$$|X|_{M_l} = \sum_{i=1}^{l} M \left| M_{i,l}^{-1} x_i \right|_{m_i} - M_l \rho_l(X) \sum_{i=1}^{l} M_{i,l} x_{i,l} - M_l \rho_l(X),\ x_{i,l} = \left| M_{i,l}^{-1} x_i \right|_{m_i}. \tag{6}$$

Следует отметить, что для каждого числа $|X|_{M_l} \in Z_{M_l}$ существует единственное значение рангового числа $\rho_l(X) = \rho(x_1, x_2, \ldots, x_l)$. Поскольку вычисления по выражению (6) легко распараллеливаются, оно широко используется для выполнения немодульных операций модулярными конвейерными структурами, при этом основной операцией является определение рангового числа $\rho(x)$.

Учитывая широкое распространение системного формирования базовых ИХМК на основе последовательностей значений $M_{i,l}^{-1}$, рассмотрим процедуру вычисления структуры и элементов одной из таких последовательностей.

Пример 2. Формирование последовательности структурных значений $\left| M_{i,k}^{-1} \right|_{m_i}$, являющихся мультипликативной инверсией по модулям m_i соответствующих элементов исходной последовательности модулей $M_{i,k}$.

Для МСС с основаниями $m_1 = 11$, $m_2 = 13$, $m_3 = 15$, $m_4 = 16$ получены следующие значения модулей $M_{i,k}$:

$$M_k = M_4 = m_1 m_2 m_3 m_4 = 34\ 320,$$

$$M_{1,k} = M_{1,4} = \frac{M_k}{m_1} = 3120,\ M_{2,4} = \frac{M_k}{m_2} = 2640,\ M_{3,4} = \frac{M_k}{m_3} = 2288,$$

$$M_{4,4} = \frac{M_k}{m_4} = 2145,\ M_{1,3} = \frac{M_3}{m_1} = \frac{m_1 m_2 m_3}{m_1} = 195,$$

$$M_{2,3} = \frac{M_3}{m_2} = 165,\ M_{3,3} = \frac{M_3}{m_3} = 143,$$

$$M_{1,2} = \frac{m_1 m_2}{m_1} = 13,\ M_{2,2} = \frac{m_1 m_2}{m_2} = 11.$$

Используем выражение (3) для определения последовательности значений $\left|M_{i,l}^{-1}\right|$, являющихся обратными элементами по модулю m_i значений $M_{i,l}$, i, $l = \overline{1, k}$, исходной последовательности, в результате получаем

$$\left|M_{1,4}^{-1}\right|_{1,1} = 8,\ \left|M_{2,4}^{-1}\right|_{1,3} = 1,\ \left|M_{3,4}^{-1}\right|_{1,5} = 2,\ \left|M_{4,4}^{-1}\right|_{1,6} = 1,\ \left|M_{2,2}^{-1}\right|_{1,3} = 6,$$

$$\left|M_{1,3}^{-1}\right|_{1,1} = 7,\ \left|M_{2,3}^{-1}\right|_{1,3} = 3,\ \left|M_{3,3}^{-1}\right|_{1,5} = 2,\ \left|M_{1,2}^{-1}\right|_{1,1} = 6.$$

Величина $N_l(X) = \left\lfloor \frac{X}{M_l} \right\rfloor$ является интервальным номером целого числа X относительно модулей $m_1, m_2, m_3, \ldots, m_l$, $l \geq 1$.

В МСС с основаниями $m_1, m_2, m_3, \ldots, m_l > l-2$, $l > 1$, и диапазоном Z_{M_l} ранг $\rho_l\left(\left|X\right|_{M_l}\right)$ числа $\left|X\right|_{M_l} = \left(x_1, x_2, \ldots, x_l\right)$, $X \in Z$, представляется в виде

$$\rho_l(X) = \hat{\rho}(X) + \Theta_l(X), \tag{7}$$

где

$$\hat{\rho}_l(X) = \left\lfloor m_l^{-1} \sum_{i=1}^{l} R_{i,l}(x_i) \right\rfloor,$$

$$R_{i,l}(x_i) = \left\lfloor \frac{m_l}{m_i} \left|M_{i,l}^{-1} x_i\right|_{m_i} \right\rfloor = \left| -m_i^{-1} \left| M_{i,l-1}^{-1} x_i \right|_{m_i} \right|_{m_l},\ i = \overline{1, l-1}, \tag{8}$$

$$R_{l,l}\left(x_{l,l}\right) = \left| \frac{x_l}{M_{l-1}} \right|_{m_l}. \tag{9}$$

В МСС с основаниями $m_1, m_2, \ldots, m_l$ для числа $\left|X\right|_{M_l} = \left(x_1, x_2, \ldots, x_l\right)$, $X \in Z$, $l > 1$, максимальное значение ранга $\rho_l(X) = \rho_l\left(\left|X\right|_{M_l}\right)$ удовлетворяет условию

$$\rho_l(X) \leq \rho_{l,\max} = \max\left\{\rho_l(A) \middle| A \in Z_{M_l}\right\} \leq l-1,\ l > 1.$$

Величина $\Theta_l(X)$ является минимальной ИХМК для целого числа X в МСС с основаниями $m_1, m_2, \ldots, m_{l-1}$, $m_l \geq l-2$, $l > 1$, и принимает значение 0 или 1.

Интервальный индекс $I_l(X)$ произвольного элемента $X = \left(x_1, x_2, \ldots, x_l\right)$ диапазона Z_{M_l} МСС с основаниями $m_1, m_2, \ldots, m_l > l-2$, $l > 1$, описывается формулой

$$I_l(X) = \hat{I}_l(X) + m_l \Theta_l(X),$$

$$\hat{I}_l(X) = \left| \sum_{i=1}^{l} R_{i,l}(x_i) \right|_{m_l}.$$

Для интервального индекса $I(X)$ и его эвклидовых составляющих – компьютерного интервального индекса $\hat{I}(X)$ и главного интервального индекса $J(X)$ произвольного элемента $X = \left(x_1, x_2, \ldots, x_k\right)$ симметричного диапазона Z_{2M}^{-} МСС с основаниями $m_1, m_2, \ldots, m_{k-1}, m_k = 2m_0$, $m_k \geq k-2$, – действительны следующие соотношения [5; 6; 9]:

$$I(X) = \left\lfloor \frac{X}{M_{k-1}} \right\rfloor - \rho_{k-1}(X), \tag{10}$$

$$I(X) = \hat{I}(X) - m_k\left(Q_k(X) + \mathrm{sn}(X)\right),$$

$$\hat{I}(X) = \left|I(X)\right|_{m_0} = \left|\hat{I}_k(X)\right|_{m_0},$$

$$J(X) = \left\lfloor \frac{I(X)}{m_0} \right\rfloor = \left\lfloor \frac{\hat{I}_k(X)}{m_0} \right\rfloor - 2\left(Q_k(X) + \mathrm{sn}(X)\right),$$

$$\hat{I}_k(X) = I\left(\left|X\right|_{2M}\right)_{m_k} = \left|\sum_{i=1}^{k} R_{i,k}(x_i)\right|_{m_k}.$$

Вычеты $R_{i,k}$ рассчитываются по формулам (8) и (9).

Алгоритм вычисления ИХМК с применением интервально-индексного метода четного модуля рассмотрен в работе [9].

Для улучшения арифметических и иных свойств числовых систем часто используется кодовая избыточность. Применение избыточности кодирования элементов рабочего диапазона в модулярных структурах существенно упрощает выполнение немодульных операций. Однако это обеспечивается только при введении относительно большой избыточности и, как следствие, требует значительных аппаратурных затрат. Отмеченный недостаток в значительной мере устраняется при использовании специфического способа введения избыточности, положенного в основу минимально избыточной МСС [1; 3; 4; 7].

В избыточной МСС интервально-модульная форма (ИМФ) целого числа X задается соотношением

$$X = \sum_{i=1}^{i-1} M_{i,l-1}\left[M_{i,l-1}^{-1} x_i\right]_{m_i} + M_{l-1} I_l(X) = \sum_{i=1}^{l-1} M_{i,l-1} x_{i,l-1} + M_{l-1} I(X), \tag{11}$$

$$I(X) = -\sum_{i=1}^{k-1} m_i^{-1}\left[M_{i,k-1}^{-1} x_i\right]_{m_i} + M_{k-1}^{-} X.$$

Набор величин $\left(x_{1,l-1}, x_{2,l-2}, \ldots, x_{l-1,l-1}\right)$ и интервальный индекс $I(X)$ формируют интервально-модулярный код целого числа X.

С помощью ранговой и интервально-индексной характеристик, а также связанных с ними форм целого числа можно реализовать все немодульные операции.

Минимально избыточная МСС (МИМСС)

Основой минимально избыточной конфигурации процедуры расчета ИХМК служат ИМФ (11), эвклидовы составляющие – компьютерный интервальный индекс $\hat{I}(X)$ и главный интервальный индекс $J(X)$, а также интервальный номер $N(X) = \left\lfloor \frac{X}{M} \right\rfloor$, минимальная ИХМК $\Theta_l(X)$ и вспомогательный модуль m_0.

При минимально избыточном модулярном кодировании применяется диапазон **D**, мощность которого меньше мощности диапазона $Z_{M_k}^{-}$ классической неизбыточной МСС с базисом $\{m_1, m_2, \ldots, m_k\}$.

В соответствии с китайской теоремой об остатках при любом $l > 1$ задаваемое ИМФ (11) отображение $I_l(X)$ числа X однозначно как на множестве **Z**, так и на диапазоне $Z_{M_k}^{-}$.

Теорема (о минимально избыточном модулярном кодировании как эффективном способе снижения времени вычисления ИХМК). *Чтобы в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_k$ интервальный индекс $I(X)$ каждого элемента $X = (x_1, x_2, \ldots, x_k)$, $x_i = \left|X\right|_{m_i}$, $i = \overline{1, k}$, диапазона $\mathbf{D} = Z_{2M}^{-} = (-M, -M+1, \ldots, M-1)$ ($M = m_0 M_{r-1} = m_0 m_1 \cdots m_{k-1}$; m_0 – вспомогательный модуль) полностью определялся компьютерным интервальным индексом – вычетом $\hat{I}_k(X)$, необходимо и достаточно выполнить следующее условие [9]:*

$$m_k \geq 2m + \rho,\ m_0 > \rho,\ \rho = \rho_{k-1,\max},$$

где $\rho = \rho_{k-1,\max}$ *– максимальное значение ранговой характеристики* $\rho_{k-1}(X)$ *(при* $l = k-1$ *в формуле (7)).*

Проанализируем следующие расчетные значения для интервального индекса $I(X)$ целого числа X:

$$I(X) = \hat{I}_k(X) - m_k \operatorname{sn}\left(m_0 - 1 - \hat{I}_k(X)\right) = \hat{I}_k(X), \text{ если } \hat{I}_k(X) < m_0,$$
$$I(X) = \hat{I}_k(X) - m_k, \text{ если } \hat{I}_k(X) \geq m_k. \tag{12}$$

Вычеты $R_{i,k}(x)$ и $R_{k,k}(x)$ рассчитываются по формулам (8) и (9).

На основании формулы (10) получены следующие экстремальные значения интервального индекса $I(X)$:

$$I_{\min} = \left\{ \left| \frac{X}{M_{k-1}} \right| - \rho_{k-1}(X) \middle| X \in D \right\} = \left\lfloor \frac{-M + X_0}{M_{k-1}} \right\rfloor - \rho_{k-1}(-M - X_0) = -m_0 - \rho_0,$$
$$I_{\max} = \left\{ \left| \frac{X}{M_{k-1}} \right| - \rho_{k-1}(X) \middle| X \in D \right\} = \left\lfloor \frac{-M - M_{k-1}}{M_{k-1}} \right\rfloor - \rho_{k-1}(-M - M_{k-1}) = m_0 - 1. \tag{13}$$

С учетом выражений (13) расчетные значения (12) для интервального индекса $I(X)$ целого числа X можно представить в виде

$$I(X) = \hat{I}_k(X) - m_k \operatorname{sn}\left(m_0 - 1 - \hat{I}_k(X)\right) = \hat{I}_k(X), \text{ если } \hat{I}_k(X) \leq I_{\max},$$
$$I(X) = \hat{I}_k(X) - m_k, \text{ если } \hat{I}_k(X) > I_{\max}. \tag{14}$$

Теорема полностью доказана.

Сравнение формул (7) и (14) показывает, что переход к минимально избыточному кодированию позволяет при оценке интервального индекса $I_k(X)$ вместо трудоемкой процедуры сужения ИМФ целого числа X применять относительно простое выражение $\operatorname{sn}\left(m_0 - 1 - \hat{I}_k(X)\right)$.

Использование МИМСС с кодовой избыточностью значительно уменьшает вычислительную сложность определения значений интервального индекса $I(X)$ целого числа X, компьютерного интервального индекса $\hat{I}(X) = |I(X)|_{m_0}$ и главного интервального индекса $J(X) = \left\lfloor \frac{I(X)}{m_0} \right\rfloor$. Так, вычисление интервального индекса $I_k(X)$ целого числа X, заданного неизбыточным модулярным кодом $(x_1, x_2, \ldots, x_k)$, требует $0{,}5\left(k^2 + 5k - 12\right)$ модульных операций и $0{,}5k(k-1)$ таблиц для хранения вычетов (8) и (9). В МИМСС соответствующие затраты по формулам (12) составляют k модульных операций и k таблиц для хранения вычетов [9]. В случае минимальной избыточности коэффициенты информационной эффективности за счет снижения вычислительных затрат на определение интегральных характеристик оцениваются значениями

$$K_{\text{МО}} = \frac{k^2 + 5k - 12}{2k}$$

для числа модульных операций,

$$K_{\text{т}} = \frac{k-1}{2}$$

для количества необходимых таблиц.

Таким образом, с увеличением числа k оснований МИМСС коэффициенты информационной эффективности $K_{\text{МО}}$ и $K_{\text{т}}$ алгоритмических структур возрастают, асимптотически приближаясь к величине $\frac{k}{2}$.

Практическую важность имеет обеспечиваемая в МИМСС простота выполнения вычислительных процедур в симметричных диапазонах. В отличие от неизбыточных МСС идентификация отрицательных и неотрицательных компонент рабочего диапазона $\mathbf{D} = Z_{2M}^{-}$ производится с помощью интервального номера $N(X) = \left\lfloor \frac{X}{M} \right\rfloor$, формируемого по главному интервальному индексу $J(X) = \left\lfloor \frac{I(X)}{m_0} \right\rfloor$ и минимальной ИХМК $\Theta(X)$, которые отвечают числу $X \in Z_{2M}^{-}$ в МСС с базисом $\{m_1, m_2, \ldots, m_{k-1}, m_0\}$ и диапазоном Z_M, без использования четного модуля m_k.

Заключение

Введение в модулярный код минимальной избыточности существенно упрощает расчет интервально-индексных характеристик и связанных с ними форм представления целого числа при реализации ряда немодульных операций. Алгоритм расчета ИХМК можно рекомендовать в качестве эффективной основы синтеза немодульных процедур, включая расширение кода, масштабирование, деление целого числа (общий случай), преобразование модулярного кода в позиционную систему счисления, контроль ошибок и др. Однако следует отметить уменьшение эффективности МИМСС по мере увеличения в используемых приложениях количества ИХМК, а также при изменении знака числа или цифр полиадического кода. Отмеченное обстоятельство не снижает целесообразности применения МИМСС в широкой сфере приложений минимально избыточной модулярной арифметики, таких как системы цифровой обработки сигналов, защиты информации, информационные технологии и др.

Библиографические ссылки

1. Чернявский АФ, Аксенов АМ, Коляда АА, Ревинский ВВ, Шабинская ЕВ. Мультипроцессорная реализация алгоритма Винограда для ДПФ на основе минимально избыточной модулярной арифметики. *Информатика.* 2005;4:78–86.

2. Коляда АА, Чернявский АФ. Общая технология вычисления интегральных характеристик модулярного кода. *Доклады Национальной академии наук Беларуси.* 2008;52(4):38–44.

3. Чернявский АФ, Коляда АА. Метод и алгоритм масштабирования в минимально избыточной модулярной системе счисления. *Доклады Национальной академии наук Беларуси.* 2009;53(3):29–37.

4. Чернявский АФ, Коляда АА. Умножение по большим простым модулям на основе минимально избыточной модулярной схемы Барретта. *Доклады Национальной академии наук Беларуси.* 2010;54(2):40–53.

5. Коляда АА, Чернявский АФ. Интегрально-характеристическая база модулярных систем счисления. *Информатика.* 2013;1:106–119.

6. Чернявский АФ, Коляда АА, Коляда НА, Шабинская ЕВ. Интервально-индексная технология расширения модулярного кода. *Электроника инфо.* 2010;6:66–71.

7. Чернявский АФ, Коляда АА, Коляда НА, Шабинская ЕВ. Умножение по большим модулям методом Монтгомери с применением минимально избыточной модулярной арифметики. *Нейрокомпьютеры: разработка, применение.* 2010;9:3–8.

8. Коляда АА, Чернявский АФ. Интервально-индексный метод четного модуля для расчета интегральных характеристик кода неизбыточной МСС с симметричным диапазоном. *Доклады Национальной академии наук Беларуси.* 2013;57(1):38–45.

9. Червяков НИ, Коляда АА, Ляхов ПА. *Модулярная арифметика и ее приложения в инфокоммуникационных технологиях.* Москва: Физматлит; 2017. 400 с.

References

1. Chernyavsky AF, Aksenov AM, Kolyada AA, Revinsky VV, Shabinskaya HV. Multiprocessor realization of Winograd's algorithm for DFT on the basis of minimally superfluous modular arithmetics. *Informatics.* 2005;4:78–86. Russian.

2. Kolyada AA, Chernyavsky AF. [The general technology of calculation of integral characteristics of a modular code]. *Doklady of the National Academy of Sciences of Belarus.* 2008;52(4):38–44. Russian.

3. Chernyavsky AF, Kolyada AA. [Scaling method and algorithm in the minimally superfluous modular number system]. *Doklady of the National Academy of Sciences of Belarus.* 2009;53(3):29–37. Russian.

4. Chernyavsky AF, Kolyada AA. Multiplication on big simple modules on the basis of Barrett's minimally superfluous modular scheme. *Doklady of the National Academy of Sciences of Belarus.* 2010;54(2):40–53. Russian.

5. Kolyada AA, Chernyavsky AF. Integrated characteristic base of modular number systems. *Informatics.* 2013;1:106–119. Russian.

6. Chernyavsky AF, Kolyada AA, Kolyada NA, Shabinskaya EV. [Interval-index technology of extension of modular code]. *Elektronika info.* 2010;6:66–71. Russian.

7. Chernyavsky AF, Kolyada AA, Kolyada NA, Shabinskaya EV. Montgomery's method for multiplication of large modules with application of the minimally redundant modular arithmetic. *Neurocomputers.* 2010;9:3–8. Russian.

8. Kolyada AA, Chernyavsky AF. Interval-index method of the even module for calculation of integrated characteristics of the code irredundant modular number system with the symmetric range. *Doklady of the National Academy of Sciences of Belarus.* 2013; 57(1):38–45. Russian.

9. Chervyakov NI, Kolyada AA, Lyakhov PA. *Modulyarnaya arifmetika i ee prilozheniya v infokommunikatsionnykh tekhnologiyakh* [Modular arithmetic and its applications in infocommunication technologies]. Moscow: Fizmatlit; 2017. 400 p. Russian.

Получена 06.04.2023 / исправлена 10.05.2023 / принята 15.05.2023.
Received 06.04.2023 / revised 10.05.2023 / accepted 15.05.2023.