ISSN 1561-8323 (print)

ИНФОРМАТИКА

INFORMATICS

УДК 004.9, 004.94

Поступило в редакцию 13.03.2017
Received 13.03.2017

Академик А. Ф. Чернявский, А. А. Коляда

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

ПРЕОБРАЗОВАНИЕ КОДА МОДУЛЯРНОЙ СИСТЕМЫ СЧИСЛЕНИЯ В ОБОБЩЕННЫЙ ПОЗИЦИОННЫЙ КОД

Аннотация. Сообщение посвящено проблеме построения полиадической интегрально-характеристической базы модулярной арифметики. В частности, получены расчетные соотношения для преобразования модулярного кода (МК) в код обобщенной позиционной системы счисления (ОПСС) и на их основе синтезированы последовательная и параллельная конфигурации соответствующей процедуры. Обладая модульной структурой, разработанные алгоритмы просты в реализации. Они включают лишь операции вычитания с умножением на константы по модулям применяемого базиса. Вычислительная сложность последовательной и параллельной реализаций преобразования МК в код ОПСС по предложенным алгоритмам составляет соответственно $O(k^2)$ и $O(k)$ модульных операций (k – мощность базиса систем счисления).

Ключевые слова: модулярная система счисления, модулярный код, обобщенная позиционная система счисления, полиадическая система счисления, полиадический код, интегральные характеристики модулярного кода

Для цитирования: Чернявский, А. Ф. Преобразование кода модулярной системы счисления в обобщенный позиционный код / А. Ф. Чернявский, А. А. Коляда // Докл. Нац. акад. наук Беларуси. – 2017. – Т. 61, № 4. – С. 26–30.

Academician Aleksandr F. Chernyavsky, Andrei A. Kolyada

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

CONVERSION OF A MODULAR NUMBER SYSTEM CODE INTO A GENERALIZED POSITION CODE

Abstract. The article is devoted to the problem of constructing an integrated and characteristic base of modular arithmetic. In particular, calculation estimates are obtained for conversion of a modular code (MC) into a code of a generalized positional number system (GPNS) and based on them the sequential and parallel configurations of the appropriate procedure are synthesized. With its modular structure, the developed algorithms are easy to implement. They include subtraction with multiplication by constants used by the modules of the basis. Computational complexity of sequential and parallel implementations of conversion of MC into the GPNS code according to the proposed algorithms is $O(k^2)$ and $O(k)$ of modular operations (k is the power of the basis of the number system) respectively.

Keywords: modular number system, modular code, generalized positional number system, polyadic number system, polyadic code, integral characteristics of modular code

For citation: Chernyavsky A. F., Kolyada A. A. Conversion of a modular number system code into a generalized position code. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2017, vol. 61, no. 4, pp. 26–30 (in Russian).

Ключевым компонентом процесса компиляции оптимальной конфигурации модулярной арифметики (МА) для того или иного приложения является формирование требуемой интегрально-характеристической базы. Решение данной задачи предполагает исследование особенностей и проведение структурно-операционного анализа целевых функций МА-приложения и синтез на этой основе подходящего адаптированного набора интегральных характеристик модулярного кода (МК), а также связанной с ними позиционной формы чисел для разработки ис-

комой версии МА. При решении обозначенной задачи используется ряд основополагающих критериев, нацеленных на оптимизацию наиболее важных для рассматриваемого класса МА-приложений характеристик создаваемой компьютерно-арифметической базы. Примерами таких характеристик могут служить: уровень сложности расчетных соотношений для базовых интегральных характеристик МК (ИХМК), эффективность применяемой позиционной формы модулярных чисел, затраты на реализацию синтезированных в рамках построенной интегрально-характеристической базы немодульных процедур, степень приспособленности МА к передовым параллельным вычислительным технологиям, к оперированию в диапазонах больших чисел и т. д.

Настоящее сообщение посвящено проблематике построения интегрально-характеристической базы МА на основе полиадической системы счисления, называемой также системой счисления со смешанным основанием или обобщенной позиционной системой счисления (ОПСС) [1–6].

В ОПСС с базисом $\mathbf{M} = \{m_1, m_2, \ldots, m_k\}$, состоящим из $k > 1$ модулей $m_1, m_2, \ldots, m_k$ неотрицательное целое число (ЦЧ) X представляется в виде

$$X = \sum_{i=1}^{k} M_{i-1} x_i, \tag{1}$$

где $X \in \mathbf{Z}_{M_k}$; через $\mathbf{Z}_m$ обозначается множество $\{0, 1, \ldots, m-1\}$ (m – натуральное число); $X = \sum_{i=1}^{k} M_{i-1} x_i \quad (M_0 = 1, M_{i-1} = \prod_{j=1}^{i-1} m_j \ (i \neq 1); x_i \in \mathrm{Z}_{m_i})$. В исследованиях по проблематике немодульных операций цифры полиадического кода $\langle x_k \ x_{k-1} \ldots x_1 \rangle$, определяемого соотношением (1), выполняют роль ИХМК. Главными достоинствами полиадических версий МА являются:

полнота информации о числе X, включая его величину и знак, содержащейся в обобщенном позиционном коде $\langle x_k \ x_{k-1} \ldots x_1 \rangle$;

простота и высокий уровень модульности последовательных реализаций преобразования МК в код ОПСС, а также полиадической формы (1) ЦЧ;

минимизация количества используемых констант.

Обозначим через $|x|_m$ элемент $\mathbf{Z}_m$, сравнимый с x (в общем случае рациональным числом), и пусть ЦЧ $X \in \mathbf{Z}_{M_k}$ задано кодом $(\chi_1, \chi_2, \ldots, \chi_k)$ модулярной системы счисления с базисом $(\chi_i = |X|_{m_i} \ (i = \overline{1, k}))$, тогда коэффициенты полиадической формы (1) числа $X = (\chi_1, \chi_2, \ldots, \chi_k)$ могут быть получены по следующей рекурсивной схеме:

$$\Big\langle X^{(1)} = X, x_1 = \left|X^{(1)}\right|_{m_1}; X^{(2)} = m_1^{-1}(X^{(1)} - x_1), x_2 = \left|X^{(2)}\right|_{m_2}; \ X^{(3)} = m_2^{-1}(X^{(2)} - x_2), \ x_3 = \left|X^{(3)}\right|_{m_3}; \ldots;$$

$$X^{(k)} = m_{k-1}^{-1}(X^{(k-1)} - x_{k-1}), \ x_k = \left|X^{(k)}\right|_{m_k} \Big\rangle. \tag{2}$$

Развернутый (нерекурсивный) эквивалент записи чисел $X^{(i)}$ из (2) имеет вид

$$X^{(1)} = X, X^{(i)} = m_{i-1}^{-1}(m_{i-2}^{-1}(\ldots m_2^{-1}(m_1^{-1}(X - x_1) - x_2)\ldots - x_{i-2}) - x_{i-1}) \ (i = \overline{2, k}). \tag{3}$$

Переход в (3) к остаткам по модулям базиса $\mathbf{M}$ дает (см. (2)) результирующее правило расчета цифр полиадического кода $\langle x_k \ x_{k-1} \ldots x_1 \rangle_{\mathbf{M}}$ ЦЧ X по его МК $(\chi_1, \chi_2, \ldots, \chi_k)$:

$$\begin{gathered} x_1 = \chi_1, \ x_i = |\,|\, m_{i-1}^{-1} \,|_{m_i} |\,|\, m_{i-2}^{-1} \,|_{m_i} |\,|\, m_{i-3}^{-1} \,|_{m_i} | \ldots |\,|\, m_2^{-1} \,|_{m_i} |\,|\, m_1^{-1} \,|_{m_i} |\, \chi_i - \chi_1 \,|_{m_i} |_{m_i} - x_2 \,|_{m_i} |_{m_i} - \ldots \\ \ldots - x_{i-3} \,|_{m_i} |_{m_i} - x_{i-2i-3} \,|_{m_i} |_{m_i} - x_{i-1i-3} \,|_{m_i} |_{m_i} \quad (i = \overline{2, k}). \end{gathered} \tag{4}$$

Используя набор констант $m_{i,l} = |-m_i^{-1}|_{m_l} \ (i = \overline{1, l-1}; \ l = \overline{2, k})$ запишем (4) в следующей эквивалентной форме:

$$\begin{gathered} x_1 = \chi_1, \ x_l = |m_{l-1,\,l}\,|\, x_{l-1} - |\, m_{l-2,l}\,|\, x_{l-2} - \ldots \\ \ldots |\, m_{2,\,l}\,|\, x_2 - |\, m_{1,l}\,|\, x_1 - \chi_l\,|_{m_l} |_{m_l} |_{m_l} |_{m_l} \ldots |_{m_l} |_{m_l} |_{m_l} |_{m_l} \\ (i = \overline{2, k}). \end{gathered} \tag{5}$$

Основанная на (5) вычислительная схема расчета цифр полиадического по заданному МК в базисе $\mathbf{M}$ имеет рекурсивную организацию, в рамках которой на l-итерации $(l = \overline{2, k})$ цифра x_l

полиадического кода $\langle x_k x_{k-1} ... x_1 \rangle$ определяется по предыдущим цифрам: x_1, x_2,..., x_{l-1}, сформированным на предшествующих итерациях, а также по цифре χ_l входного МК ($\chi_1, \chi_2, ..., \chi_k$).

Синтезированный алгоритм преобразования кода МСС в обобщенный позиционный код заключается в нижеследующем.

Параметры алгоритма: основания m_1, m_2, …, m_k базовых МСС и ОПСС.

Входные данные алгоритма: МК ($\chi_1, \chi_2, ..., \chi_k$) произвольного элемента X диапазона $\mathbf{Z}_{M_k}$.

Выходные данные: полиадический код $\langle x_k x_{k-1} ... x_1 \rangle$ числа X в базисе $\mathbf{M} = \{m_1, m_2, \ldots, m_k\}$.

Предварительно получаемые данные: набор констант $m_{i,l} = |-m_i^{-1}|_{m_l}$ $(i = \overline{1, l-1};\ l = \overline{2,k})$.

Тело алгоритма преобразования модулярного кода в обобщенный позиционный код:

М_ОП.1. Положить $x_1 = \chi_1$, $l = 2$.

М_ОП.2. Переменным i и x присвоить начальные значения: $i = 1$, $x = \chi_l$.

М_ОП.3. Выполнить операцию $x = |m_{i,l}|x_i - x|_{m_l}|_{m_l}$, после чего переменную i инкрементировать ($i = i + 1$).

М_ОП.4. Если $i \neq l$, то перейти к М_ОП.3.

М_ОП.5. В качестве искомого значения l-й цифры полиадического кода зафиксировать $x_l = x$.

М_ОП.6. Если $l \neq k$, то l увеличить на 1 ($l = l + 1$) и перейти к М_ОП.2.

М_ОП.7. Завершить работу алгоритма.

Временные затраты на получение l-й цифры полиадического кода ЦЧ алгоритмом М_ОП.1–М_ОП.7 оцениваются как

$$t_{\text{М\_ОП},\,l} = (l-1)t_{\text{МВ}} + (l-1)t_{\text{МУ}} = (l-1)(t_{\text{МВ}} + t_{\text{МУ}}), \tag{6}$$

где $t_{\text{МВ}}$ – время вычитания двух остатков; $t_{\text{МУ}}$ – время умножения вычета на константу по модулю МСС.

Суммирование оценок (6) по $l = \overline{2,k}$ дает общие затраты на выполнение процедуры М_ОП.1–М_ОП.7:

$$t_{\text{М\_ОП}} = 0{,}5k(k-1)(t_{\text{МВ}} + t_{\text{МУ}}). \tag{7}$$

Приведенный алгоритм преобразования модулярного кода в обобщенный позиционный код имеет строго последовательную организацию. Получая цифру за цифрой (от младшей до старшей), он предусматривает полное выполнение сегмента операций по каждому разряду – по соответствующему модулю МСС в последовательном режиме без включения в этот сегмент операций по другим модулям. Алгоритм М_ОП.1–М_ОП.7 предназначен для ПЭВМ-реализаций. Оценка (7) общих временных затрат относится именно к этому случаю. Аппаратная реализация вычислительной схемы (5), осуществляемая, например, с помощью нейросетевых модулярных вычислительных структур, предполагает проведение всех расчетов параллельно по всем модулям МСС.

Параллельная конфигурация алгоритма преобразования модулярного кода в обобщенный позиционный код по схеме (5) заключается в нижеследующем.

Параметры алгоритма: основания m_1, m_2, …, m_k базовых МСС и ОПСС.

Входные данные алгоритма: МК ($\chi_1, \chi_2, ..., \chi_k$) произвольного элемента X диапазона $\mathbf{Z}_{M_k}$.

Выходные данные: полиадический код $\langle x_k x_{k-1} ... x_1 \rangle$ числа X в базисе $\mathbf{M} = \{m_1, m_2, \ldots, m_k\}$.

Предварительно получаемые данные: набор констант

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

Тело алгоритма:

_М_ОП.1. Переменным x_1, x_2, …, x_k присвоить значения $x_1 = \chi_1$, $x_2 = \chi_2, ..., x_k = \chi_k$ и положить $l = 2$.

_М_ОП2. Для всех: $i = \overline{l, k}$ выполнить операцию $x_i = |m_{l-1,i}|x_{l-1} - x_i|_{m_i}|_{m_i}$.

_М_ОП.3. Если $l \neq k$, то переменную инкрементировать y ($l = l + 1$) и перейти к _М_ОП.2.

_М_ОП.4. Текущие значения переменных x_1, x_2, …, x_k зафиксировать в качестве искомых значений одноименных цифр полиадического кода $\langle x_k x_{k-1} ... x_1 \rangle$ числа X в базисе $\mathbf{M}$ и завершить работу алгоритма.

Временные затраты на получение l коэффициентов $x_1, x_2, \ldots, x_1$ ($l = \overline{2,k}$) полиадической формы (1) ЦЧ $X = (\chi_1, \chi_2, ..., \chi_k)$ по алгоритму _М_ОП.1–_М_ОП.4 в системе модулярной обработки информации (СМОИ), функционирующей в базисе **M**, составляют $t_{\_М\_ОП} = (l-1)(t_{МВ} + t_{МУ})$.

Отметим, что расчет цифр полиадического кода $< x_k x_{k-1} ... x_1 >$ с помощью предложенного в [7] алгоритма РИХ_МИМК.1–РИХ_МИМК.8, который по своей структуре является параллельным, может быть выполнен за время порядка $t_{РИХ\_МИМК} = \lceil \log_2 k \rceil t_{МС} + 2t_{МУ}$, где через $\lceil x \rceil$ обозначается наименьшее ЦЧ, не меньшее вещественной величины x; $t_{МС}$ – время операции модульного сложения. Реализация на ПЭВМ алгоритма РИХ_МИМК.1–РИХ_МИМК.8 занимает такое же время (7), как и алгоритм _М_ОП.1–_М_ОП.4. При этом процедура РИХ_МИМК.1–РИХ_МИМК.8 обладает гораздо большими функциональными возможностями. Вместе с тем алгоритм _М_ОП.1–_М_ОП.4 более прост в случае нейросетевых реализаций при довольно высокой производительности.

Приведем числовой пример.

Пусть в МСС с базисом **M** = {3, 7, 11, 13} задано ЦЧ $X = (\chi_1, \chi_2, \chi_3, \chi_4) = (0,\ 5,\ 1,\ 12)$, для которого требуется получить полиадический код $\langle x_4\ x_3\ x_2\ x_1 \rangle$.

Рассчитаем константы:

$M_1 = m_1 = 3$, $M_2 = m_1 m_2 = 3 \cdot 7 = 21$, $M_3 = m_1 m_2 m_3 = 3 \cdot 7 \cdot 11 = 231$, $M_4 = m_1 m_2 m_3 m_4 = 3 \cdot 7 \cdot 11 \cdot 13 = 3003$; $m_{1,2} = \left| -\frac{1}{m_1} \right|_{m_2} = \left| -\frac{1}{3} \right|_7 = 2$, $m_{1,3} = \left| -\frac{1}{m_1} \right|_{m_3} = \left| -\frac{1}{3} \right|_{11} = 7$, $m_{1,4} = \left| -\frac{1}{m_1} \right|_{m_4} = \left| -\frac{1}{3} \right|_{13} = 4$, $m_{2,3} = \left| -\frac{1}{m_2} \right|_{m_3} = \left| -\frac{1}{7} \right|_{11} = 3$, $m_{2,4} = \left| -\frac{1}{m_2} \right|_{m_4} = \left| -\frac{1}{7} \right|_{13} = 11$, $m_{3,4} = \left| -\frac{1}{m_3} \right|_{m_4} = \left| -\frac{1}{11} \right|_{13} = 7$.

Согласно (5) цифры полиадического кода ЦЧ X принимают значения:

$$x_1 = \chi_1 = 0,$$

$$x_2 = |m_{1,2}|x_1 - \chi_2|_{m_2}|_{m_2} = |2-5|_7|_7 = 4,$$

$$x_3 = |m_{2,3}|x_2 - |m_{1,3}|x_1 - \chi_3|_{m_3}|_{m_3}|_{m_3} = |3|4-|7|0-1|_{11}|_{11}|_{11}|_{11} = 0,$$

$$x_4 = |m_{3,4}|x_3 - |m_{2,4}|x_2 - |m_{1,4}|x_1 - \chi_4|_{m_4}|_{m_4}|_{m_4}|_{m_4}|_{m_4} =$$

$$|7|0-|11|4-|4|0-12|_{13}|_{13}|_{13}|_{13}|_{13}|_{13} = 0.$$

Таким образом, искомый полиадический код имеет вид: $\langle x_4\ x_3\ x_2\ x_1 \rangle = \langle 0\ 0\ 4\ 0 \rangle$.

Согласно (1) сформированному коду отвечает

$$X = \sum_{l=1}^{4} M_{l-1} x_l = 0 + M_1 \times 4 + M_2 \times 0 + M_3 \times 0 = M_1 \times 4 = 3 \times 4 = 12.$$

Число X = 12 в заданной МСС имеет код (0, 5, 1, 12), который совпадает с исходным МК. Это подтверждает корректность выполненного преобразования.

Представленные результаты исследований по проблеме построения интегрально-характеристической базы полиадической конфигурации МА позволяют сформулировать нижеследующие основные выводы.

1. Полиадическая форма модулярных чисел содержит исчерпывающую информацию об их местоположении в рабочем диапазоне. Благодаря данному обстоятельству преобразование МК в код ОПСС является универсальным инструментарием для решения задачи синтеза алгоритмов любых немодульных операций – масштабирования, общего деления, сравнения чисел, контроля переполнения и т. д. Другие из известных позиционных форм модулярных чисел, включая ранговую и интервально-модулярную, отмеченным свойством универсальности не обладают.

2. Разработанные алгоритмы преобразования МК в обобщенный позиционный код имеют модульную структуру. Они целиком состоят из операций вычитания с умножением на константы по модулям применяемого базиса. Это дает возможность минимизировать уровень сложности неизбыточных последовательных немодульных процедур. При избыточном модулярном кодировании улучшение арифметических свойств полиадических вычислительных структур, как

это имеет место в случае ранговых и интервально-индексных аналогов, не происходит. Важной отличительной особенностью интегрально-характеристической базы МА на основе ОПСС является снижение до теоретического минимума количества необходимых констант. Данное свойство, а также модульная структура преобразования МК в обобщенный позиционный код обеспечивают полиадической конфигурации МА оптимальные условия для ее применения в активно развиваемых в настоящее время МА-приложениях нейросетевого типа.

Список использованных источников

1. Omondi, A. Residue number systems: theory and implementation / A. Omondi, B. Premkumar. – Singapore: Imperial College Press, 2007. – 311 p. doi.org/10.1142/9781860948671

2. Преобразователь из модулярного кода в обобщенную полиадическую систему счисления для отказоустойчивых систем управления / И. А. Калмыков [и др.] // Успехи современного естествознания. – 2009. – № 4. – С. 41–43.

3. Sousa, L. MRC – based RNS reverse converters for the four – moduli sets $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$ / L. Sousa, S. Antao // IEEE trans. circuits and syst. II: Express briefs. – 2012. – Vol. 59, issue 4. – P. 244–248. doi.org/10.1109/tcsii.2012.2188456

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

5. Построение обратных преобразователей модулярной арифметики с коррекцией ошибок на базе полиадического кода / В. М. Амербаев [и др.] // Нейрокомпьютеры: разработка, применение. – 2014. – № 9. – С. 30–35.

6. Ananda Mohan, P. V. Residue number systems: theory and applications / P. V. Ananda Mohan. – Basel: Birchauser (mathematics), 2016. – 351 p. doi.org/10.1007/978-3-319-41385-3

7. Чернявский, А. Ф. Вычисление интегральных характеристик минимально избыточного модулярного кода / А. Ф. Чернявский, А. А. Коляда // Докл. Нац. акад. наук Беларуси. – 2015. – Т. 59, № 6. – С. 40–46.

References

1. Omondi A., Premkumar B. *Residue number systems: theory and implementation*. Singapore, Imperial College Press, 2007. 311 p. doi.org/10.1142/9781860948671

2. Kalmykov I. A., Lobodin M. V., Zinov'ev A. V., Demorlukova Ia. V. Converter of the modular code into the generalized polyadic number system code in nonstop control systems. *Uspekhi sovremennogo estestvoznaniia = Advances in current natural sciences*, 2009, no. 4, pp. 41–43 (in Russian).

3. Sousa L., Antao S. MRC – based RNS reverse converters for the four – moduli sets $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2012, vol. 59, iss. 4, pp. 244–248. doi.org/10.1109/tcsii.2012.2188456

4. Kolyada A. A., Chernyavsky A. F. Integrated characteristic base of modular number systems. *Informatika = Informatics,* 2013, no. 1, pp. 106–119 (in Russian).

5. Amerbaev V. M., Soloviev R. A., Telpukhov D. V., Balaka E. S. Construction of residue number system reverse onverters with error correction, based on mixed-number system. *Neirokomp'iutery: razrabotka, primenenie = Neurocomputers*, 2014, no. 9, pp. 30–35 (in Russian).

6. Ananda Mohan P. V. *Residue number systems: theory and applications*. Basel, Birchauser (mathematics), 2016. 351 p. doi.org/10.1007/978-3-319-41385-3

7. Chernyavsky A. F., Kolyada A. A. Calculation of the integral characteristics of minimally redundant modular code. *Doklady Natsional'noi akademii nauk Belarusi = Doklady of the National Academy of Sciences of Belarus*, 2015, vol. 59, no. 6, pp. 40–46 (in Russian).

Информация об авторах

Чернявский Александр Федорович – академик, д-р техн. наук, профессор, заведующий лабораторией. Институт прикладных физических проблем имени А. Н. Севченко Белорусского государственного университета (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: shabinskaya@rambler.ru.

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

Information about the authors

Chernyavsky Aleksandr Fedorovich – Academician, D. Sc. (Engineering), Professor, Head of the Laboratory. A. N. Sevchenko Institute of Applied Physics Problems of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: shabinskaya@rambler.ru.

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