

ТАБЛИЧНАЯ РЕАЛИЗАЦИЯ ОПЕРАЦИИ УМНОЖЕНИЯ НА ОСНОВЕ КЛАССОВ ВЫЧЕТОВ В ОТРИЦАТЕЛЬНОМ ЧИСЛОВОМ ДИАПАЗОНЕ

Загуменная Е. В.

Харьковский Национальный технический университет сельского хозяйства имени Петра Василенка

В данной статье рассмотрена табличная реализация операции умножения в отрицательном числовом диапазоне на основе класса вычетов.

Постановка проблемы. Результаты исследований в области создания вычислительных средств обработки информации показали, что использование класса вычетов (КВ) в качестве системы счисления компьютерных вычислительных средств, предназначенных для реализации в положительном числовом диапазоне целочисленных арифметических операций сложения, вычитания и умножения, может существенно повысить производительность решения задач определенного класса. Однако необходимо отметить, что существует многочисленный класс алгоритмов и задач (задачи маршрутизации, задачи оптимизации и пр.), где кроме выполнения целочисленных арифметических операций сложения, вычитания и умножения в положительном числовом диапазоне существуют необходимость реализации перечисленных выше арифметических операций в отрицательном числовом диапазоне.

Анализ последних исследований и публикаций. В литературе уже были описаны табличные методы и алгоритмы модульного умножения чисел в непозиционной системе счисления класса вычетов [1,4]. Поиск путей упрощения структуры табличного вычислительного средства обусловил необходимость совершенствования методов и алгоритмов реализации модульных операций, позволяющих повысить эффективность применения табличного метода в КВ. Так [4] представлен метод табличной реализации операции модульного умножения. Особенностью реализации данного метода является возможность уменьшения количества оборудования за счет сокращения на (50-70)% логических элементов "И" в узлах таблицы ПЗУ, непосредственно реализующих операцию модульного умножения по произвольному m_i модулю КВ. Это возможно за счет использования свойств симметрии таблицы реализации $a_i b_i \pmod{m_i}$ модульной операции умножения. Недостаток рассмотренного метода состоит в том, что его использование не дает возможности создать табличный метод реализации операции умножения в КВ в отрицательном числовом диапазоне.

Цель статьи. Предлагается табличная реализация операции умножения в отрицательном числовом диапазоне.

Основные материалы исследования. Для построения метода табличной реализации умножения в КВ как для положительного, так и для отрицательного числовых диапазонов представим входные числа A и B в следующем виде (искусственная форма представления чисел в КВ [1])

$$A' = A + \frac{m}{2} \text{ и } B' = B + \frac{m}{2},$$

для m – четных чисел;

$$A' = A + \frac{(m-1)}{2} \text{ и } B' = B + \frac{(m-1)}{2},$$

для m нечетных чисел.

Если, например, m – четное число, тогда выполняются следующие соотношения:

$$\begin{cases} -\frac{m}{2} \leq A(B) < \frac{m}{2}, 0 \leq A'(B') < m-1, \\ -\frac{m}{2} \leq A \cdot B < \frac{m}{2}, 0 \leq (A \cdot B)' < m-1. \end{cases}$$

Очевидно, что

$$(A \cdot B)' = A \cdot B + \frac{m}{2}. \quad (1)$$

Тогда имеем

$$\begin{aligned} (A' \cdot B') \pmod{m} &= \left[\left(A + \frac{m}{2} \right) \left(B + \frac{m}{2} \right) \right] \pmod{m} = \\ &= \left[AB \pmod{\frac{m}{2}} + \frac{m}{2} \cdot \left(A + B + \frac{m}{2} \right) \right] \pmod{m}. \end{aligned} \quad (2)$$

Из выражения (1) очевидно, что

$$A \cdot B = A' \cdot B' - \frac{m}{2} \cdot \left(A + B + \frac{m}{2} \right). \quad (3)$$

Подставим выражение (3) в формулу (1). Получим, что

$$(A \cdot B)' = A' \cdot B' - \frac{m}{2} \cdot \left(A + B + \frac{m}{2} \right) + \frac{m}{2}. \quad (4)$$

В выражении (4) есть член, который имеет численное значение $\frac{m}{2}$. Он и обуславливает ошибку в вычислении значения $A' \cdot B' \pmod{m}$. Таким образом формулы для вычисления $A \cdot B \pmod{m}$ имеют следующий вид для m – четных чисел

$$\left[(A \cdot B) \pmod{\frac{m}{2}} \right]' = (A' \cdot B') \pmod{m} + \frac{m}{2}, \quad (5)$$

или

$$\left[(A \cdot B) \bmod \frac{m}{2} \right]' = (A' \cdot B') \bmod m. \quad (6)$$

Для m нечетного имеем

$$\left[(A \cdot B) \bmod \frac{(m-1)}{2} \right]' = (A' \cdot B') \bmod m + \frac{(m-1)}{2}, \quad (7)$$

или

$$\left[(A \cdot B) \bmod \frac{(m-1)}{2} \right]' = (A' \cdot B') \bmod m. \quad (8)$$

Учитывая выражения (1) ÷ (8), выводим соотношение для реализации модульного умножения для положительного и отрицательного числовых диапазонов:

$$\begin{aligned} a'_i &= a_i + m_i / 2, & a'_i &= a'_i + (m_i - 1) / 2; & a'_i &= [\gamma'_{a'_i}, (a'_i)^*]; \\ b'_i &= b_i + m_i / 2, & b'_i &= b'_i + (m_i - 1) / 2; & b'_i &= [\gamma'_{b'_i}, (b'_i)^*]. \end{aligned} \quad (9)$$

Для m_i - четного

$$\gamma'_{a'_i}(\gamma'_{b'_i}) = \begin{cases} 0, & \text{если } 0 \leq a'_i(b'_i) \leq m_i / 2, \\ 1, & \text{если } m_i / 2 < a'_i(b'_i) \leq m_i - 1. \end{cases} \quad (10)$$

Для m_i - нечетного

$$\gamma'_{a'_i}(\gamma'_{b'_i}) = \begin{cases} 0, & \text{если } 0 \leq a'_i(b'_i) \leq (m_i - 1) / 2, \\ 1, & \text{если } (m_i - 1) / 2 < a'_i(b'_i) \leq m_i - 1. \end{cases} \quad (11)$$

Числовая часть $(a'_i)^* [(b'_i)^*]$ кода информационно-сжатия данных определяется следующим образом. Для m_i - четного

$$(a'_i)^* [(b'_i)^*] = \begin{cases} a'_i(b'_i), & \text{если } 0 \leq a'_i(b'_i) \leq m_i / 2; \\ \overline{a'_i(b'_i)} = m_i - a'_i(b'_i), & \\ \text{если } m_i / 2 < a'_i(b'_i) \leq m_i - 1. \end{cases} \quad (12)$$

при этом $0 \leq (a'_i)^* [(b'_i)^*] \leq m_i / 2$.

Для m_i - нечетного числа

$$(a'_i)^* [(b'_i)^*] = \begin{cases} a'_i(b'_i), & \text{если } 0 \leq a'_i(b'_i) \leq (m_i - 1) / 2; \\ \overline{a'_i(b'_i)} = m_i - a'_i(b'_i), & \\ \text{если } (m_i - 1) / 2 < a'_i(b'_i) \leq m_i - 1. \end{cases} \quad (13)$$

при этом $0 \leq (a'_i)^* [(b'_i)^*] \leq (m_i - 1) / 2$.

Результат $(a'_i \cdot b'_i) \bmod m_i$ операции представляется в коде информационного сжатия данных, т.е. в виде $\{\gamma'_i, [(a'_i)^* (b'_i)^*] \bmod m_i\}$, тогда

$$(a'_i \cdot b'_i) \bmod m_i = \begin{cases} [(a'_i)^* \cdot (b'_i)^*] \bmod m_i, & \\ \text{если } (\gamma'_{a'_i} + \gamma'_{b'_i}) = 0 \pmod{2}; \\ m_i - [(a'_i)^* \cdot (b'_i)^*] \bmod m_i, & \\ \text{если } (\gamma'_{a'_i} + \gamma'_{b'_i}) = 1 \pmod{2}. \end{cases} \quad (14)$$

при этом $0 \leq [(a'_i)^* \cdot (b'_i)^*] \bmod m_i \leq m_i - 1$.

Формула для определения произведения двух чисел в КВ имеет следующий вид:

$$\begin{aligned} (A \cdot B) \bmod M &= (A' \cdot B') \bmod M = \\ &= [(a'_1, a'_2, \dots, a'_i, \dots, a'_n) \cdot (b'_1, b'_2, \dots, b'_i, \dots, \\ &\dots, b'_n)] \bmod M = [(a'_1 \cdot b'_1) \bmod m_1, \\ &(a'_2 \cdot b'_2) \bmod m_2, \dots, (a'_i \cdot b'_i) \bmod m_i, \dots \\ &\dots, (a'_n \cdot b'_n) \bmod m_n]. \end{aligned} \quad (15)$$

Так, как все модули $\{m_i\}$, $i = \overline{1, n}$ КВ, (за исключением возможно только одного основания), нечетные числа, то в дальнейшем, без потери общности рассуждений, будем считать, что основание КВ нечетные числа. Формула (15) с учетом кода информационного сжатия данных имеет следующий вид:

$$\begin{aligned} (A' \cdot B') \bmod M &= (\{[\gamma'_{a'_1}, (a'_1)^*] \cdot \\ &[\gamma'_{b'_1}, (b'_1)^*]\} \bmod m_1, \\ &\{[\gamma'_{a'_2}, (a'_2)^*] \cdot [\gamma'_{b'_2}, (b'_2)^*]\} \bmod m_2, \\ &\dots, \{[\gamma'_{a'_i}, (a'_i)^*] \cdot [\gamma'_{b'_i}, (b'_i)^*]\} \bmod m_i, \dots \\ &\dots, [\gamma'_{a'_n}, (a'_n)^*] \cdot [\gamma'_{b'_n}, (b'_n)^*]\} \bmod m_n) = \\ &= (\{\gamma'_1, [(a'_1)^* \cdot (b'_1)^*] \bmod m_1\}, \\ &\{\gamma'_2, [(a'_2)^* \cdot (b'_2)^*] \bmod m_2\}, \dots \\ &\dots, \{\gamma'_i, [(a'_i)^* \cdot (b'_i)^*] \bmod m_i\}, \dots \\ &\dots, \{\gamma'_n, [(a'_n)^* \cdot (b'_n)^*] \bmod m_n\}), \end{aligned} \quad (16)$$

где

$$\begin{aligned} (a \cdot b) \bmod m_i &= \{[\gamma'_{a'_i}, (a'_i)^*] \cdot [\gamma'_{b'_i}, (b'_i)^*]\} \bmod m_i = \\ &= \{\gamma'_i, [(a'_i)^* \cdot (b'_i)^*] \bmod m_i\}. \end{aligned} \quad (17)$$

Исходя из (16) ÷ (17) где, а также учитывая, что (9) ÷ (15), для m - нечетного получим следующие соотношение для реализации модульной операции алгебраического умножения в КВ:

$$\begin{cases}
\{(a_i \cdot b_i) \bmod [(m_i - 1) / 2]\}' = \\
= \{[(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [(m_i - 1) / 2]\}' = \\
= (a_i' \cdot b_i') \bmod m_i + (m_i - 1) / 2 = \\
= \{[\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\}' \bmod m_i + (m_i - 1) / 2 = \\
= \{\gamma_{a_i}', [(a_i')^* \cdot (b_i')^*]\}' \bmod m_i + (m_i - 1) / 2; \\
\{(a_i \cdot b_i) \bmod [(m_i - 1) / 2]\}' = \\
= \{[(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [(m_i - 1) / 2]\}' = \\
= (a_i' \cdot b_i') \bmod m_i = \{[\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\}' \bmod m_i = \\
= \{\gamma_{a_i}', [(a_i')^* \cdot (b_i')^*]\}' \bmod m_i.
\end{cases} \quad (18)$$

Для m_i – четного числа получим

$$\begin{cases}
(a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[(\gamma_{a_i}, a_i) \cdot \\
(\gamma_{b_i}, b_i)] \bmod [m_i / 2]\}' = (a_i' \cdot b_i') \bmod m_i + \\
+ m_i / 2 = \{[\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\}' \bmod m_i + \\
m_i / 2 = \{\gamma_{a_i}', [(a_i')^* \cdot (b_i')^*]\}' \bmod m_i + m_i / 2; \\
\{(a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[(\gamma_{a_i}, a_i) \cdot \\
(\gamma_{b_i}, b_i)] \bmod [m_i / 2]\}' = (a_i' \cdot b_i') \bmod m_i = \\
= \{[\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\}' \bmod m_i = \\
= \{\gamma_{a_i}', [(a_i')^* \cdot (b_i')^*]\}' \bmod m_i.
\end{cases} \quad (19)$$

Выводы. Соотношение (18)÷(19) применяется для табличной реализации операций умножения в КВ, как в положительных, так и в отрицательных числовых диапазонах обработки информации. Полученные соотношения рекомендованы к практическому применению.

Список использованных источников

1. Акушский И. Я. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. – М.: Советское радио, 1968. – 440 с.
2. Жихарев В. Я. Методы и средства обработки информации в непозиционной системе счисления в остаточных классах / В. Я. Жихарев, Я. В. Илюшко, Л. Г. Кравец, В. А. Краснобаев. – Ж.: Волянь, 2005–219 с.
3. Koshman S. A. Method of bit-by-bit tabular realization of arithmetic operations in the system of residual classes / S. A. Koshman, V. I. Barsov, V. A. Krasnobayev, K. V. Yaskova, N. S. Derenko. – Радиоелектронні і комп'ютерні системи, 2009. – № 5 (39). 44–48 с.
4. Загуменна К. В. Математическая модель процесса табличной реализации операций алгебраического умножения в классе вычетов / С. О Мороз, В. О. Жадан, В. А. Краснобаев В. А. – Радиоелектронні і комп'ютерні системи, 2012. – № 1(53). 68–74 с.
5. Краснобаев В. А. Методы сравнения чисел, представленных кодом системы остаточных классов / В. А. Краснобаев. // Электронное моделирование. – 1988. – Том.10, № 2. – С. 84–87.
6. Yaskova K. V. Method of bit-by-bit tabular realization of arithmetic operations in the system of residual

classes / S. A. Koshman, V. I. Barsov, V. A. Krasnobayev, K. V. Yaskova, N. S. Derenko // Радиоелектронні і комп'ютерні системи, 2009, № 5 (39). – 44–48 с.

5. Загуменная Е. В. Метод арифметического сравнения чисел в классе вычетов / Е. В. Загуменная, С. А. Кошман, М. А. Маврина, В. А. Краснобаев. // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка, Технічні науки, - Харків: ХНТУСГ, 2012, Вип. 130. - 72-75 с.

6. Загуменная Е. В. Методы и алгоритмы сравнения чисел в классе вычетов на основе использования позиционного признака непозиционного кода / Е. В. Загуменная, В. А. Краснобаев, М. А. Маврина. // Радиоелектронні і комп'ютерні системи, 2012, № 3(55). - 111-121с.

7. Watson R.W. Residue arithmetic and Reliable Computer Design / R. W. Watson, C. W. Hastings. – Washington.: Spartan Books, 1967. – 128с.

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

9. Труды Юбилейной Международной научно-технической конференции "50 лет модулярной арифметике", Россия, Москва, Зеленоград, 23-25 ноября 2005, издательство МИЭТ. 550с.

10. Малашевич Б. М. Разработка вычислительной техники в Зеленограде. Неизвестные супер-ЭВМ / Б. М. Малашевич // Электроника, наука, технология, бизнес. – 2004. – № 2. – С. 72 – 76.

11. Яськова Е. В. Повышение отказоустойчивости информационно-управляющей системы АСУТП сельскохозяйственного производства на основе использования модулярной арифметики / Е. В. Яськова // Молодежь и сельскохозяйственная техника в XXI веке: тез. докл. III – го международного форума молодежи. - Харьков, 4 - 6 апреля 2007 г. – С. 143.

Анотація

ТАБЛИЧНА РЕАЛІЗАЦІЯ ОПЕРАЦІЙ МНОЖЕННЯ НА ОСНОВІ КЛАСІВ ЛИШКІВ У ВІД'ЄМНОМУ ЧИСЛОВОМУ ДІАПОЗОНІ

Загуменна К. В.

У даній статті розглянута таблична реалізація операції множення у від'ємному числовому діапазоні.

Abstract

TABULAR INSTRUCTION MULTIPLICATION CLASS BASED DEDUCTION NEGATIVE NUMERIC RANGE

E. Zagumennaya

This article describes the implementation of the multiplication table-negative number range based on the residue class.