**УДК 651.3**

# ПРИНЦИП КОЛЬЦЕВОГО СДВИГА В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

**Загуменная Е. В.[1], Староверов Р. Н.[2]**

*Харьковский Национальный технический университет сельского хозяйства имени Петра Василенка, ООО "Вектор-21" (Республика Союз Мьянма)*

*Проанализирован принцип кольцевого сдвига в системе остаточных классов, а также представлен метод его реализации.*

**Постановка проблемы.** Существует несколько принципов реализации арифметических операций в системе остаточных классов. Такие как сумматорный принцип реализации арифметических операций, который основан на базе малоразрядных двоичных сумматоров, табличный принцип реализации, а так же прямой логический принцип (с использование логических переменных).

**Анализ последних исследований и публикаций.** Свойства системы остаточных классов позволяет нам реализовать данные принципы, такое свойство, как малоразрядность остатков $a_i$ позволяет нам реализовать арифметические операции либо в табличном варианте, либо в сумматорном варианте. Но все выше упомянутые принципы имеют свои недостатки. При сумматорном варианте точность реализации арифметических операций уменьшается, так как присутствует тот же недостаток, что и в позиционной системе счисления наличие межразрядных связей, что обусловливает разложения ошибок в пределах данного основания. При матричном (табличном) варианте отсутствуют межразрядные связи между обрабатывающими операндами вообще, но количество оборудования резко возрастает при большой разрядной сетки обрабатываемых чисел [3].

**Цель статьи.** Рассмотреть и проанализировать принцип кольцевого сдвига, а так же метод его реализации в системе остаточных классов (СОК).

**Основные материалы исследований.** Поэтому рационально рассмотреть промежуточный вариант реализации арифметических операций в СОК, который основан на применении принципа кольцевого сдвига, путем применения сдвигающих регистров. Суть данного принципа состоит в том, что результат арифметической операции $(a_i \pm b_i) \bmod m_i$ по произвольному модулю $M$, заданной совокупностью оснований $\{m_j\}$, $j = \overline{1,n}$, будет осуществляться за счет циклических сдвигов заданной цифровой структуры. Используя изоморфизм между элементами конечной абелевой группы и элементами группы перестановок известной теоремы Кэли. Матрица сложения для произвольного модуля $m_i$ СОК будет иметь вид табл. 1.

Гомоморфизм между всеми элементами абелевой группы на группу всех целых чисел позволяет определить результат арифметических операций в СОК посредством использования кольцевых сдвигающих регистров.

Таблица 1 – Матрица сложения для произвольного модуля $m_i$

| $b_i$ | $a_i$ | | | | |
|---|---|---|---|---|---|
| | 0 | 1 | 2 | … | $m_i - 1$ |
| 0 | 0 | 1 | 2 | … | $m_i - 1$ |
| 1 | 1 | 2 | 3 | … | 0 |
| 2 | 2 | 3 | 4 | … | 1 |
| ⋮ | … | … | … | … | … |
| $m_i - 1$ | $m_i - 1$ | 0 | 1 | … | $m_i - 2$ |

Операнд А в СОК представляется набором остатков от деления его на набор простых чисел $\{m_i\}, i = \overline{1,n}$, то набор остатков можно отожествлять с суммой полей Галуа $\sum_{i=1}^{n} GF(m_i)$. Для изучения метода реализации арифметических операций в СОК рассмотрим варианты для конкретной приведенной системы вычетов по модулю $m_i$.

Для заданной операции модульного сложения $(a_i + \beta_i) \bmod m_i$ в поле Галуа $GF(m_i)$ составлена матрица (таблица Кэли) (табл.1). Из существование нейтральных элементов в поле $GF(m_i)$ сделаем вывод, что строка (столбец), в которой элементы данного поля стоят в порядке возрастания. А так как в поле вычетов $GF(m_i)$ элементы различны (порядок группы равен $m_i$), следует, что в каждой строке (столбце) (табл.1) содержатся все элементы поля ровно по одному разу.

Используя свойства содержимого таблицы Кэли можно реализовать операцию модульного сложения и вычитания в СОК путем применения ПКС посредством $n$ кольцевых $M = m_i\left(\left[\log_2(m_i - 1)\right] + 1\right)$ сдвигающих регистров [3].

Представим произвольную алгебраическую систему в виде $Q = \langle G, \otimes \rangle$, где $G$ - непустое множество;

$\otimes$ - тип операции, определенной для любых двух элементов $\alpha_i$, $\beta_i \in G$.

Операция "+" сложения в множестве классов вычетов $R$, порожденных идеалом $J$, образует новое кольцо

, называемое кольцом вычетов $R/J$ . Представим его в виде $Z/(m_i)$, где $Z$-множество целых чисел $0,\pm1,\pm2,..;$ $m_i$ - основание СОК. Это и дает нам возможность реализации арифметической операции сложения в СОК без межразрядных переносов путем применения кольцевого сдвига (с помощью кольцевых сдвигающих регистров). На основе данного принципа кольцевого сдвига рассмотрим метод реализации арифметических операций в классе вычетов. Данный метод состоит в том, что исходная цифровая структура для каждого основания СОК представляется в виде содержимого первой строки (столбца) таблицы модульной операции сложения (вычитания) $(\alpha_i \pm \beta_i) \bmod m_i$ вида

$$Q_{исх}^{(m_i)} = \left[ Q_0(\alpha_0) \| Q_1(\alpha_1) \| ... \| Q_{m_i-1}(\alpha_{m_i-1}) \right], \qquad (1)$$

где $\|$ - операция конкатенации;

$Q_n(a_n)$ - $k$ - разрядный двоичный код, соответствующий значению $\alpha_n$ - го остатка $\alpha_n = \overline{0, m_i - 1}$ числа по модулю $m_i$ .

Исходя из вышесказанного с помощью кольцевых регистров сдвига, которые широко используются в ПСС, легко реализовать арифметические операции в СОК. Степень циклических переносов определяется следующим выражениями:

$$\begin{aligned} &\left[ Q_0(\alpha_0) \| Q_1(\alpha_1) \| ... \| Q_{m_i-1}(\alpha_{m_i-1}) \right]^{+z} = \\ &= \left[ Q_z(\alpha_z) \| Q_{z+1}(\alpha_{z+1}) \| \right. \\ &\left. ... \| Q_{m_{i-1}}(\alpha_{m_{i-1}}) \| Q_0(\alpha_0) \| ... \| Q_{z-1}(\alpha_{z-1}) \right] \end{aligned} \qquad (2)$$

$$\begin{aligned} &\left[ Q_0(\beta_0) \| Q_1(\beta_1) \| ... \| Q_{m_i-1}(\beta_{m_i-1}) \right]^{-z} = \left[ Q_{m_i-1-z}(\beta_{m_i-1-z}) \right. \\ &\left. \| Q_{m_i-z}(\beta_{m_i-z}) \| ... \| Q_0(\beta_0) \| Q_1(\beta_1) \| ... \| Q_{m_i-z-2}(\beta_{m_i-z-2}) \right] \end{aligned} \qquad (3)$$

Отметим, что $\left[ Q_0(\alpha_0) \| Q_1(\alpha_1) \| ... \| Q_{m_i-1}(\alpha_{m_i-1}) \right]^{m_i} = \varepsilon$ , т.е при $z = m_i$ все элементы упорядочного множества остаются на исходном месте.

Рассмотрим техническую реализацию данного метода первый операнд $a_i$ указывает на номер $\alpha_{a_i}$ разряда $Q_{a_i}(\alpha_{a_i})$ КРС определяющего результат модульной операции по модулю $m_i$ , а второй $\beta_i$ определяет количество разрядов КРС ( $\beta_i \cdot k$ - двоичных разрядов), на которые необходимо повести сдвиг исходного (1) содержимого КРС в соответствии с алгоритмами (2) (3).

**Вывод.** Таким образом мы рассмотрели принцип кольцевого сдвига, который в отличии от других принципов увеличивает достоверность и точность арифметических операции, за счет отсутвия межрозрядных связей.

**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 остаточних классах / В. Я. Жихарев, Я. В. Илюшко, Л. Г. Кравец, В. А. Краснобаев. – Ж.:Волынь, 2005.-219 с.

3. Долгов А. И. Диагностика устройств, функционирующих в системе остаточніх классов / А. И. Долгов. – М.:Радио и связь, 1982.- 64с.

4. Яськова Е. В. Повышение отказоустойчивости информационно-управляющей системы АСУТП сельскохозяйственного производства на основе использование 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.

5. Яськова Е. В. Разработка и исследование метода реализации арифметических операций в модулярной арифметике / Е. В. Яськова // Проблемы информатики и моделирования: тез. докл. VII международной научно-технической конференции, Харьков, 29 ноября – 1 декабря 2007 г. – С. 38.

6. 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. – Радіоелектронні і комп'ютерні системи, 2009. – № 5 (39). 44–48 с.

7. Яськова Е. В. Методы обработки информации в модулярной арифметике / Е. В. Яськова // Радиоэлектроника и молодежь в XXI веке: тез. докл. XIII международного молодежного форума, Харьков, 30 марта – 1 апреля 2009 г. – С. 187.

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


**Анотація**

**ПРИНЦИП КОЛЬЦЕВОГО ЗСУВУ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ**


Загуменна К. В., Старовєров Р. М.



*Проаналізований принцип кільцевого зсуву у системі залишкових класів, а також запропонований метод його реалізації.*


**Abstract**

**THE PRINCIPLE OF CIRCULAR SHIFT IN RESIDUAL CLASSES SYSTEM**


K. Zagymennaya, R. Staroverov



*Analyzed the principle of circular shift in residual classes system, and also provides a method of its implementation.*