УДК 681.04

**С.А. КОШМАН[1], Н.С. ДЕРЕНЬКО[2]**

[1]*Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Украина*
[2]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*

# МЕТОД РЕАЛИЗАЦИИ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ В МОДУЛЯРНОЙ АРИФМЕТИКЕ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МАЛОРАЗРЯДНЫХ ДВОИЧНЫХ СУММАТОРОВ

В данной статье рассмотрен метод реализации арифметических операций в модулярной арифметике на основе использования малоразрядных двоичных сумматоров. Представлен вариант технической реализации сумматора по произвольному основанию на основе рассмотренного метода.

**модулярная арифметика, система счисления в остаточных классах, двоичный сумматор**

В позиционной системе счисления выполнение арифметических операций предполагает последовательную обработку разрядов операндов по правилам, определяемым содержанием данной операции, и не может быть закончено до тех пор, пока не будут определены последовательно значения всех разрядов результата с учётом всех связей между разрядами. Отметим основные свойства модулярной арифметики (МА): малоразрядность остатков; независимость остатков; равноправность остатков.

В МА каждый из разрядов числа обрабатывается независимо, и время выполнения всей операции определяется временем, необходимым для получения результата по наибольшему основанию, что вытекает из свойств МА. Существует четыре основных принципа реализации арифметических операций в МА.

1. **Сумматорный –** на базе малоразрядных двоичных сумматоров.

2. **Принцип кольцевого сдвига** – на базе кольцевых регистров сдвига.

3. **Прямой логический принцип –** с использованием логических переменных.

4. **Табличный принцип** – на базе матричных схем (постоянных запоминающих устройств).

Если табличные методы реализации арифметических операций довольно широко рассмотрены в известной литературе, то метод реализации модульных операций в МА требует дополнительных и глубоких исследований. В данной статье предлагается рассмотреть сумматорный принцип реализации арифметической операции сложения.

**Целью статьи** является разработка метода реализации арифметических операций в модулярной арифметике на основе использования малоразрядных двоичных сумматоров.

**Анализ последних исследований**. В литературных источниках [1, 2] рассмотрена общая методика построения сумматоров работающих по произвольному основанию системы остаточных классов (СОК), однако не рассматривается техническая реализация таких устройств. В этом случае важны и актуальны исследования, посвящённые разработке технических устройств для реализации операций модульного сложения на основе использования малоразрядных двоичных сумматоров.

**Основные материалы исследований.** Рассмотрим методику построения сумматоров, работающих по произвольно заданному основанию $m_i$. Известно, что модуль двоичного сумматора – это минимальное отличное от нуля число $M$ прибавление (или вычитание) которого к содержимому сумматора не меняет его величины, т.е.

$$G_L \pm M = G_L,$$

где $G_L$ – содержимое сумматора.

В общем случае содержимое двоичного сумматора имеет вид

$$G_L = 2^{n-1} l_n + 2^{n-2} l_{n-1} + \ldots + 2l_2 + l_1,$$

где $l_n = 0, 1$ – значения разрядов двоичного сумматора; $n$ – количество разрядов двоичного сумматора.

При этом модуль двоичного сумматора определяется как $M = 2^n - 1$.

Если модуль двоичного сумматора обратного кода *M* равен основанию системы остаточных классов *m*, т.е. $M = m_i$, то коррекция результата арифметической операции не требуется, так как основанию системы *m* реализуется без избыточности. При отличии модуля сумматора *M* от основания системы $m_i$ требуется производить коррекцию результата арифметической операции, используя методы построения суммирующих устройств, которые предполагают введение дополнительных межразрядных связей.

Пусть сумматор состоит из *n* двоичных разрядов, обозначаемых соответственно через $r_1$, $r_2$, ..., $r_n$ по мере возрастания старшинства разрядов. Условимся, что вход каждого разряда сумматора будет обозначаться индексом *i*, а выход – индексом *j*. Обозначим через $X_{ij}$ связь между выходом $r_j$ разряда с входом $r_i$ разряда сумматора. Таким образом, наличие связи $X_{ij}$ обеспечивает связь по переносу $r_j$ разряда не только с $r_{j+1}$, но и с $r_i$ разрядом. Тогда для того чтобы *n*-разрядный двоичный сумматор обратного кода работал по основанию *m*, т.е. чтобы выполнялось условие $M = m_i$, необходимо ввести дополнительную связь $X_{ij}$ в разрядах $r_i$, которые соответствуют нулевым значениям в записи основания системы $m_i$.

Введение дополнительных связей $X_{ij}$ переводит систему счисления рассматриваемого сумматора из двоичной в полиадическую, основания которой определяются характером связей. Если основания полиадической позиционной системы $\pi_1, \pi_2, \ldots, \pi_k$ и расположены в порядке возрастания, то единица *z*-го разряда числа $L = (l_1, l_2, \ldots, l_k)$ представленного в ней имеет вес $g_z = \sum_{i=1}^{k-1} \pi_i$, т.е. $G_L = \sum_{z=1}^{k} l_m \prod_{i=1}^{z-1} \pi_i$.

Пусть имеет место одна дополнительная связь $X_{ij}$, соединяющая выход *j*-го разряда со входом *i*-го разряда, т.е, объединяющая разряды с номерами $i, i+1, \ldots, j$ в единый разряд, работающий по основанию $\pi_{ij}$. Тогда величина $G_L$ определится как

$$G_L = \sum_{z=1}^{n} l_z 2^{z-1} - \sum_{z=j+1}^{n} l_z 2^{\theta},$$

где $\theta = z + i - j - 2$.

В то же время при отсутствии дополнительной связи величина $G_L$ числа *L* равна

$$G_L = \sum_{z=1}^{n} l_z 2^{z-1},$$

т.е. при одном и том же кодировании числа *L*, его величина за счет введения одной дополнительной связи $X_i$ уменьшается на величину

$$\Delta G_L = \sum_{z=j+1}^{n} l_z 2^{\theta} = 2^{i-j-2} \sum_{z=j+1}^{n} l_z 2^{z}.$$

Действительно, наличие одной дополнительной связи $X_{ij}$ указывает на то, что группа из $(j - i + 1)$-го разрядов работает по модулю $\pi_{ij} = 2^{j-i+1} - 1$. Остальные $n - j + i - 1$ разряды равноправны между собой. При перестановке любого из этих разрядов с группой, работающей по модулю $\pi_{ij}$, модуль сумматора не меняется, так как он равен

$$M = \pi_{ij} 2^{n-j+i-1} - 1$$

и не зависит от взаимного расположения разрядов. Всего возможных положений группы, работающей по модулю $\pi_{ij}$ по отношению к другим разрядам, может быть $n - j + i - 1$. В каждой конструкции сумматора число *L*, описывающее его содержимое, будет в общем случае принимать новое числовое значение, определяемое местоположением $j$-го разряда.

Модуль сумматора при введении одной дополнительной связи $X_{ij}$, уменьшается на величину

$$\Delta M = 2^{i-j-2} \sum_{z=j+1}^{n} s_z 2^{z},$$

где $s_z$ – значение $z$-го разряда числа, описывающего значение основания.

Соответственно на ту же величину уменьшается диапазон представимых на сумматоре чисел.

Проиллюстрируем сказанное на примере. Рассмотрим четырехразрядный сумматор по модулю $M = 11$. Введем дополнительную связь $X_{34}$ между выходом четвертого и входом третьего разряда, т.е. $j = 4$, $i = 3$, $n = 4$, $\pi_{ij} = 2^2 - 1 = 3$, модуль суммато-

ра при этом равен $M = \pi_{ij} 2^2 - 1 = 11$. Пусть на сумматоре записано число $L = (1, 0, 1, 0)$, которое для рассматриваемой конструкции имеет величину $G_L = 10$ (в десятичной системе счисления), совпадающую с его величиной в двоичной системе счисления, поскольку выполнено условие $j = n$. На рис. 1 представлена структурная схема сумматора по произвольному основанию с $\Delta G_L = 0$, выполненного на базе позиционного сумматора обратного кода.

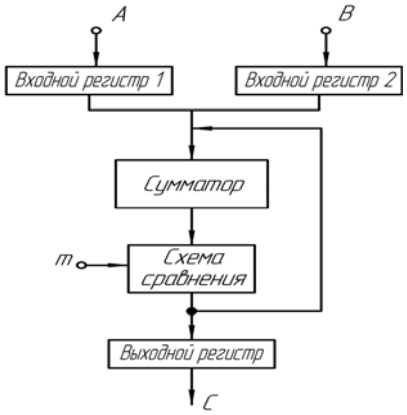


Рис. 1. Структурная схема сумматора по произвольному основанию с $\Delta G_L = 0$

Общий алгоритм выполнения арифметических операций на таком сумматоре следующий: 1) поразрядное суммирование операндов, которые поступают с входных регистров на вход позиционного сумматора обратного кода; 2) сравнение результата суммы с основанием системы $m_i$ в блоке сравнений; 3) суммирование полученного результата с переносами дополнительных цепей $X_{ij}$ и цепи обратной связи, если результат суммы больше основания системы $m_i$; 4) запись окончательного результата в выходной регистр.

Рассмотрим возможные варианты работы устройства, представленного на рис. 1, для основания одиннадцать СОК ($m = 1011$).

**Вариант 1.** Сума операндов меньше, чем значение основания, т.е. ($A + B = C < m = 11$). Пусть $A = 0011$ и $B = 0100$. Тогда при суммировании операндов $A$ и $B$ в позиционном сумматоре обратного кода получается результат $C = 0111$, который при сравнении с основанием $m$ в схеме сравнения является меньше данного основания. Поэтому результат $C$ поступает в выходной регистр.

**Вариант 2.** Сума операндов больше, чем значение основания, т.е. ($A + B = C > m = 11$). Пусть $A = 1010$ и $B = 0110$. Тогда при суммировании операндов $A$ и $B$ в позиционном сумматоре обратного кода получается результат $C = 10000$, который при сравнении с основанием $m$ в схеме сравнения является больше данного основания. Поэтому на вход сумматора обратного кода поступает сигнал коррекции результата $\overline{m} = 0101$, с учётом дополнительной цепи $X_{34}$ и цепи обратной связи сумматора. После корректировки в позиционном сумматоре обратного кода результат операции будет равен $C = 0101$, что меньше основания $m$, поэтому этот результат запишется в выходной регистр.

**Вариант 3.** Сума операндов равна значению основания, т.е. ($A + B = C = m = 11$). Результат операции, гасится и в выходной регистр записывается значение $C = 0000$, так как модуль сумматора является его вторым нулём.

**Выводы.** Таким образом, в статье предложен метод реализации арифметических операций в модулярной арифметике на основе использования малоразрядных двоичных сумматоров. Данный метод позволяет проводить модульные операции, как сложение, так и вычитание. Приведены примеры конкретной реализации данного метода, что подтверждает его научно-практическую значимость.

## Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 440 с.

2. Концепция, методы и средства моделирования на ПЛИС контроллеров и процессоров с параллельной архитектурой / И.А. Фурман, В.А. Краснобаев, М.Л. Малиновский, С.А. Кошман, С.Я. Бовчалюк // Автомобильный транспорт. – Х.: ХНАДУ, 2005. – Вып. 16. – С. 338-341.

*Поступила в редакцию 28.02.2007*

**Рецензент**: д-р техн. наук, проф. И.А. Фурман, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.