Обробка інформації в складних технічних системах

УДК 681.3

В.И. Барсов[1], В.А. Краснобаев[2], В.О. Жадан[2], Е.А. Сотник[1]

[1] *Украинская инженерно-педагогическая академия, Харьков*
[2] *Полтавский национальный технический университет им. Юрия Кондратюка, Полтава*

ПРИМЕНЕНИЕ МЕТОДА ДВОИЧНОГО КОДИРОВАНИЯ ДЛЯ РЕАЛИЗАЦИИ МОДУЛЬНЫХ ОПЕРАЦИЙ В СИСТЕМЕ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ РЕАЛЬНОГО ВРЕМЕНИ

Рассмотрена возможность применения метода двоичного кодирования, основанного на использовании принципа кольцевого сдвига, при реализации модульных операций в системе обработки информации и управления.

Ключевые слова: *модулярная система счисления, кольцевой сдвигающий регистр, принцип кольцевого сдвига, система обработки информации и управления.*

Введение

Постановка задачи. Известно, что малоразрядность остатков a_i дает возможность реализовать арифметические операции в классе вычетов либо на базе малоразрядных двоичных сумматоров, либо в табличном варианте[1, 2].

При первом методе реализации арифметических операций проявляется (хотя и в значительно меньшей степени) тот же недостаток, что и в позиционных системах счисления (ПСС): наличие межразрядных связей в пределах данного основания m_i. При табличном варианте реализации арифметических операций отсутствуют межразрядные связи между обрабатываемыми операндами вообще, однако для достаточно большой разрядной сетки (для больших по величине модулей модулярной системы счисления (МСС)) резко увеличивается количество оборудования системы обработки информации и управления (СОИУ). Поэтому видится целесообразным рассмотреть промежуточный вариант реализации арифметических операций в МСС, основанный на применении принципа кольцевого сдвига (ПКС) путем использования кольцевых сдвигающих регистров (КСР) или как их еще называют – кольцевые регистры сдвига (КРС).

Особенность принципа кольцевого сдвига заключается в том, что результат арифметической операции $(a_i \pm \beta_i) \bmod m_i$ по произвольному модулю МСС, заданной совокупностью $\{m_j\}, j = \overline{1,n}$ оснований, определяется только за счет последовательных циклических сдвигов заданной цифровой структуры.

Цель данной статьи. Целью статьи является разработка и дальнейшее совершенствование методов эффективной реализации арифметических операций в МСС на основе применения принципа кольцевого сдвига.

Основная часть

Известная теорема Кэли [1] устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. В этом случает матрица сложения для произвольного модуля m_i МСС будет задана табл. 1 (для $m_i = 5$ – табл. 2).

Таблица 1

Таблица Кэли

β_i	a_i				
	0	1	2	…	$m_i - 1$
0	0	1	2	…	$m_i - 1$
1	1	2	3	…	0
…	…	…	…	…	…
$m_i - 1$	$m_i - 1$	0	1	…	$m_i - 2$

Таблица 2

Матрица сложения для $m_i = 5$

β_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Одним из следствий теоремы Кэли является вывод о том, что отображение элементов абелевой группы на группы всех целых чисел является гомоморфным. Это обстоятельство позволяет определить результат арифметических операций в МСС посредством использования ПКС. Так как операнд А в МСС представляется набором остатков от деления его на набор n простых (в общем случае взаимно попарно простых) чисел $\{m_j\}, i = \overline{1,n}$, то этот набор остатков можно отождествить непосредственно с суммой n полей Галуа $\sum_{i=1}^{n} GF(m_i)$. Для изучения метода реализации арифметических операций в МСС достаточно

рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i = const, т.е. для конкретной проведенной системы вычетов по модулю m_i.

Пусть для заданной операции модульного сложения $(a_i + \beta_i) \bmod m_i$ в поле $GF(n_i)$ составлена таблица Кэли (табл. 1). Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в табл. 1 есть строка (столбец) в которой элементы данного поля стоят в порядке возрастания, а из того факта, что в поле вычетов $GF(m_i)$ эти элементы различны (порядок группы равен m_i), следует, что в каждой строке (столбце) табл. 1 содержатся все элементы поля ровно по одному разу. Использование перечисленных свойств содержимого таблицы Кэли позволяет реализовать операции модульного сложения и вычитания в МСС путем применения ПКС посредством n кольцевых $M = m_i\left(\left[\log_2(m_i - 1)\right] + 1\right)$ – разрядных КСР.

Пусть произвольная алгебраическая система представлена в виде $S = \langle G, * \rangle$, где G – непустое множество; * – тип операции, определенной для любых двух элементов $a_i, \beta_i \in G$.

Операция сложения в множестве классов вычетов R, порожденных идеалом J, образует новое кольцо, называемое кольцом классов вычетов R/J. Его можно представить в виде $z/(m_i)$, где z – множество целых чисел 0, ±1, ±2, …; m_i – основание МСС (если основание МСС m_i – простое число, то $z/(m_i)$ – поле). Данное обстоятельство, как указывалось, и обуславливает возможность реализации арифметической операции сложения в МСС без межразрядных переносов путем кольцевого сдвига посредством применения группы КСР.

Суть предлагаемого метода двоичного кодирования состоит в том, что исходная цифровая структура для каждого из модулей (оснований) МСС представляется в виде содержимого первой строки (столбца) таблицы модульного сложения (вычитания) $(a_i \pm \beta_i) \bmod m_i$ вида

$$P_{\text{исх}}^{(m_i)} = \left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right], \quad (1)$$

где $\|$ – операция конкатенации; $P_V(\alpha_V)$ – k-разрядный двоичный код, соответствующий значению α_V-го остатка $\alpha_V = \overline{0, m_i - 1}$ числа по модулю m_i.

Для заданного модуля $m_i = 5$ цифровая структура представится в виде

$$P_{\text{исх}}^{(5)} = \left[000 \| 001 \| 010 \| 011 \| 100 \right].$$

Таким образом, с помощью широко используемых в ПСС кольцевых регистров сдвига легко реализовать арифметические операции в МСС, причем, исходя из выражения (1), степени циклических перестановок определяются следующими выражениями:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right]^{+Z} = \left[P_z(\alpha_z) \| P_{z+1}(\alpha_{z+1}) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \| P_0(\alpha_0) \| \ldots \| P_{z-1}(\alpha_{z-1}) \right]; \quad (2)$$

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right]^{-Z} = \left[P_{m_i-1-z}(\alpha_{m_i-1-z}) \| P_{m_i-z}(\alpha_{m_i-z}) \| \ldots \| P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-z-2}(\alpha_{m_i-z-2}) \right]. \quad (3)$$

Отметим, что

$$\left[P_0(\alpha_0) \| P(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right]^{m_i} = \varepsilon,$$

т.е. при $z = m_i$ все элементы упорядоченного множества $\left\{ P_j(\alpha_j) \right\} \left(j = \overline{0, m_i - 1} \right)$ остаются на исходном месте. При технической реализации данного метода [5] первый операнд a_i указывает на номер α_{a_i} разряда $P_{a_i}(\alpha_{a_i})$ КРС, определяющего результат модульной операции по модулю m_i, а второй операнд β_i определяет количество разрядов КРС ($\beta_i \cdot k$ – двоичных разрядов), на которые необходимо произвести сдвиг исходного (1) содержимого КРС в соответствии с алгоритмами (2), (3). Пусть $m_i = 5$ ($S = \langle \{0, 1, 2, 3, 4\}, \oplus \rangle$). Тогда таблица значений модульной суммы $(a_i \oplus \beta_i) \bmod m_i$ для кольца класса вычетов z/(5) представится в виде матрицы (табл. 2). Содержимое разрядов КСР представится в виде числовых данных, например первой строки (столбца) табл. 2 (рис. 1, а). На рисунке знаком $\oplus$ обозначено положительное (против часовой стрелки) направление сдвига содержимого разрядов КСР. При этом первый операнд a_i указывает номер разряда КСР, содержимое которого определяет результат данной операции, а второй операнд β_i указывает число сдвигов содержимого разрядов КСР (рис. 1, а, б, в).

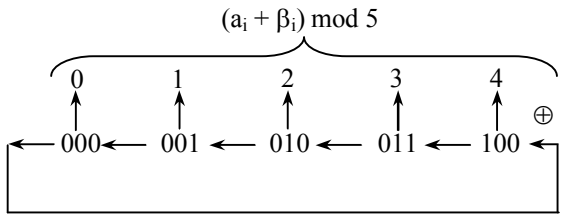
Введем понятие оператора кольцевого сдвига (ОКС). ОКС – это оператор, определяющий величину (выраженную в количестве сдвигаемых разрядов КСР) и направление сдвига разрядов КСР, и обозначается $k^{(z)}$, где

$$z = \begin{cases} +z - \text{при положительном направлении} \\ \quad \text{сдвига содержимого разрядов КСР;} \\ -z - \text{при отрицательном (по часовой стрелке)} \\ \quad \text{направлении сдвига содержимого разрядов КСР;} \end{cases}$$

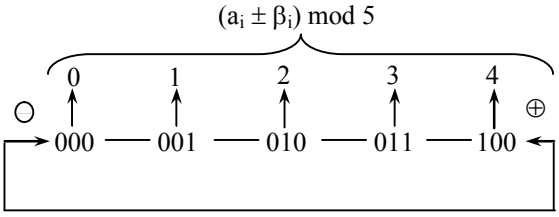
(z – показатель оператора кольцевого сдвига (ПОКС)).

Так, для операции модульного сложения ОКС представится в виде $k^{(+\beta i)}$, при этом время сдвига t_c (составляющее в основном время t выполнения операции) содержимого разрядов КСР определяется выражением

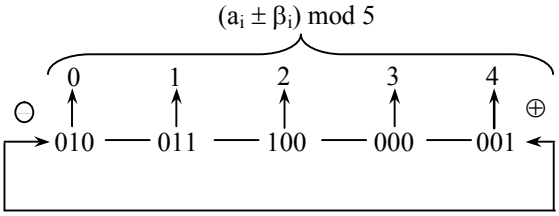
$$t_c = k \cdot \tau \cdot z, \quad (4)$$



а



б



в

Рис. 1. Варианты структуры кольцевого регистра сдвига для $m_i = 5$: а – 1-й вариант; б – 2-й вариант; в – 3-й вариант

(в дальнейшем будем считать, что $t \approx t_c$), где $k = [\log_2 (m_n - 1)] + 1$ (m_n – модуль, по которому работает схема модульного сложения); τ – время сдвига одного двоичного разряда (время срабатывания одного триггера).

На основании ПКС, используя следующее тождество

$$(a_i - \beta_i) \equiv \left[a_i + (m_n - \beta_i)\right] \bmod m_n, \quad (5)$$

можно реализовать операцию модульного вычитания $(a_i - \beta_i) \bmod m_n$. В этом случае ОКС имеет вид $k^{(+(m_n - \beta_i))}$.

Как видно, преимущество ПКС по сравнению с методами, основанными на применении двоичных сумматоров, состоит в отсутствии межразрядных переносов, что существенно повышает достоверность реализации модульных операций. Однако, время выполнения модульных операций (см. выражение 4) сравнительно велико, что снижает общую эффективность применения СОИУ в классе вычетов.

Данное обстоятельство и обусловливает необходимость разработки алгоритмов повышения быстродействия выполнения данных операций в СОИУ.

Рассмотрим пример конкретного выполнения операции модульного сложения $(a_i + \beta_i) \bmod m_n$ на основе применения ПКС (табл. 2; рис. 1, а) для m_n=5. Пусть $a_i = 001$; $\beta_i = 100$. В этом случае исходное содержимое разрядов КСР представлено на рис. 1, а. Первый операнд a_i определяет местоположение разряда КСР, содержимое которого будет определять результат операции (для $a_i = 001$ – первый разряд), а второй операнд β_i определяет количество сдвигов содержимого КСР, т.е. для $\beta_i = 100$ ПОКС имеет вид $z = +4$, а ОКС представится в виде $k^{(+4)}$. Для данных значений входных операндов после четырех сдвигов в положительном направлении во втором разряде КСР будет находиться значение 000, что соответствует правильному результату операции $1 + 4 = 0 (\text{mod} 5)$ (рис. 1, а). Устройство для реализации рассмотренного алгоритма представлено на рис. 2.

Алгоритм повышения быстродействия выполнения операции модульного сложения (вычитания) состоит в использовании тождества (5), а также следующих соотношений:

$$a_i + \beta_i = \beta_i + a_i,$$
$$a_i + (m_n - \beta_i) = (m_n - \beta_i) + a_i.$$

В этом случае для операции модульного сложения $(a_i + \beta_i) \bmod m_n$ ПОКС представляется в виде

$$z = \begin{cases} +a_i, & \text{если } a_i \le \beta_i, \\ +\beta_i, & \text{если } a_i > \beta_i, \end{cases}$$

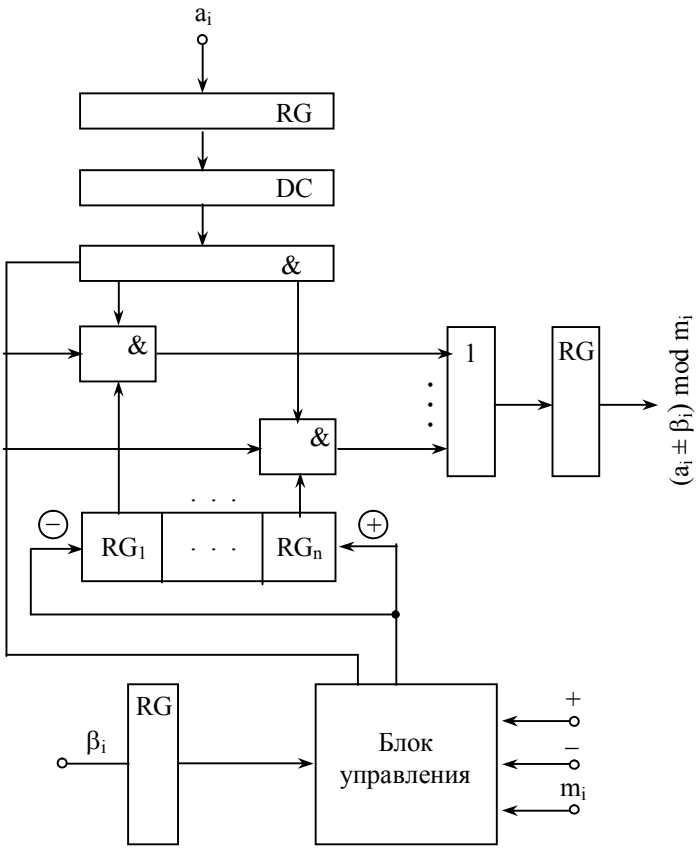


Рис. 2. Устройство для сложения и вычитания чисел по модулю МСС

т.е. при $a_i \le \beta_i$ операнд a_i определяет количество z сдвигов содержимого КСР, а операнд β_i – номер разряда КСР, определяющий результат операции; при $a_i > \beta_i$ операнд β_i определяет количество z сдвигов содержимого КСР, а операнд a_i – номер разряда КСР, определяющий результат операции.

Для операции модульного вычитания $(a_i - \beta_i) \bmod m_n$ ПОКС представляется в виде

$$z = \begin{cases} +a_i, & \text{если } a_i \le (m_n - \beta_i), \\ +(m_n - \beta_i), & \text{если } a_i > (m_n - \beta_i). \end{cases}$$

Данный алгоритм реализации модульных операций позволяет существенно уменьшить время t выполнения операции модульного сложения и вычитания [3].

Одним из алгоритмов повышения быстродействия выполнения операции модульного сложения (вычитания) является алгоритм, основанный на свойстве тождества (5) и свойстве следующего тождества:

$$(a_i + \beta_i) \equiv [a_i - (m_n - \beta_i)] \bmod m_n, \qquad (6)$$

т.е. сдвиг содержимого КСР можно осуществить как в положительном, так и в отрицательном направлениях (для $m_n = 5$, рис. 1, б), где для операции модульного сложения ПОКС представляется в виде

$$z = \begin{cases} +\beta_i, \text{ если } 0 \le \beta_i \le (m_n - 1)/2, \\ -(m_n - \beta_n), \text{ если } (m_n + 1)/2 \le \beta_i \le m_n - 1. \end{cases}$$

В дальнейшем, не теряя общности рассуждений, и для удобства расчетов будем считать, что m_n – нечетное число. Для операции модульного вычитания ПОКС представится в виде (табл. 3). Применение данного алгоритма позволяет (в зависимости от величины модуля m_n) до 90% сократить значение величины z, что значительно уменьшает время t выполнения модульных операций (рис. 3, а, б).

Рассмотрим методы и алгоритмы реализации ПКС, позволяющие вдвое сократить максимальное значение ПОКС (максимальное число сдвигов содержимого разрядов КСР).

Таблица 3

Операции модульного вычитания ПОКС

β_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

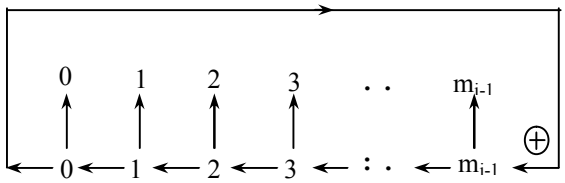
Очевидно, что $z_{max} = m_n - 1$. Рассмотрим следующее равенство:

$$a_i + \beta_i = a_i' + \beta_i' = (a_i + m_n/2) + (\beta_i - m_n/2). \qquad (7)$$

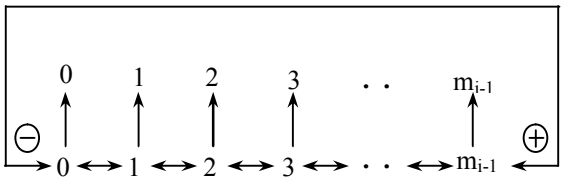
В этом случае содержимое разрядов КСР соответствует $[(m_n - 1)/2]$-й строке (столбцу) матрицы табл. 1 (см. рис. 2, в), а сдвиг содержимого разрядов КСР будет производиться относительно величины $(m_n - 1)/2$, т.е. величина максимального количества сдвигов содержимого разрядов КСР будет равна $(m_n - 1)/2$. Таким образом, максимальное значение ПОКС равно

$$z_{max} = (m_n - 1)/2. \qquad (8)$$

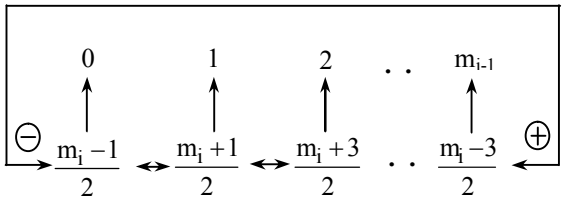
Рассмотренный алгоритм (рис. 3, в) выполнения операции модульного сложения (вычитания) позволяют существенно повысить быстродействие выполнения модульных операций в МСС.



а



б



в

Рис. 3. Варианты структуры кольцевого регистра сдвига для модуля m_i МСС: а – 1-й вариант; б – 2-й вариант; в – 3-й вариант

Современные СОИУ при решении задач значительную часть своего полезного времени затрачивают на реализацию операции умножения. СОИУ примерно половину времени своей работы «посвящает» реализации операции умножения и деления. Существует достаточно много методов обойти операцию деления (например, умножение первого операнда на обратную мультипликативную величину делителя), однако замена операции умножения совокупностью однотипных операций сложения посредством ПКС значительно снижает пользовательскую производительность СОИУ. Поэтому при создании СОИУ в МСС важно синтезировать устройство для умножения, непосредственно используя принцип кольцевого сдвига.

Один из вариантов реализации операции модульного умножения $a_i \cdot \beta_i \pmod{m_n}$ методом кольце-

вого сдвига состоит в использовании набора из двух КСР с применением известного соотношения:

$$a_i\beta_i \left(\mathrm{mod}\, m_n\right) = \left[\left\{\left(a_i + \beta_i\right) \mathrm{mod}\, m_n\right]^2 \mathrm{mod}\, m_n - \right.$$
$$\left. -\left[\left(a_i - \beta_i\right) \mathrm{mod}\, m_n\right]^2 \mathrm{mod}\, m_n\right\} \mathrm{mod}\, m_n\big) / 4\Big] \mathrm{mod}\, m_n. \quad (9)$$

ОКС для первого КСР представится в виде $K^{(+\beta_i)}$, а для второго – $K^{(-\beta_i)}$. Время t выполнения операции модульного умножения будет не намного больше того времени, что определяется выражением (4). Недостаток данного варианта реализации операции модульного умножения – сравнительно большой объем оборудования операционного устройства СОИУ [7].

Рассмотрим вариант реализации операции модульного умножения – вариант множеств контуров (ВМК). В этом случае используется один КСР, с помощью которого определяется и результат модульного сложения – вычитания, а ОКС для операции модульного умножения представляется в виде $K_{ij}^{(z_i)}$, где i – номер контура, в котором производится сдвиг содержимого разрядов КСР ($i = \overline{1,n}$); n – количество контуров, по которым работает устройство ($n = m_n - 1$); j – номер устанавливаемой строки матрицы значений $a \cdot \beta \pmod{m_n}$ (индекс i для операндов a, β опускается), $j = \overline{1,n}$; z_i – ПОКС, обозначающий количество сдвигов содержимого разрядов КСР в данном i-м контуре $\left(z_i = \overline{0, m_i - 2}\right)$.

Сущность ВМК состоит в том, что по значению второго β операнда устанавливается β-я строка таблицы значений $a \cdot \beta \pmod{m_n}$ путем сдвига содержимого разрядов КСР по отдельным контурам (по отдельным модулям m_i, причем $m_i = i + 1$, так как минимальный (первый) модуль равен двум, т.е. $m_i = 2$. Поскольку нулевая строка таблицы значений $a\,\beta \pmod{m_n}$ не устанавливается ($j \neq 0$), то $j = \overline{2,n}$. Вместе с тем первый разряд КСР устанавливается одновременно со вторым и, таким образом, $i = \overline{2,n}$. Нулевой разряд КСР участия в реализации ВМК не принимает, так, как операция умножения на ноль ($a = 0$; $\beta = 0$) проще организуется по отдельному алгоритму, например, путем вывода входных нулевых шин операндов a, β непосредственно на нулевой выход устройства. Установление значения содержимого разрядов КСР производится последовательно, начиная с (m – 1)-го (старшего) разряда и до второго включительно, т.е. справа налево (рис. 4, 5, табл. 4).

Введем понятие обобщенного операнда кольцевого сдвига (ООКС) в виде матрицы $\left\{ K_{ij} \right\} = \left\{K_{ij}^{(z_{ij})}\right\}$, где показатель обобщенного операнда кольцевого сдвига (ПООКС) z_{ij} означает количество сдвигов содержимого разрядов КСР в i-м контуре при установлении j-й строки матрицы модульного произведения $a \cdot \beta \pmod{m_n}$. Таким образом, ООКС $\{K_{ij}\}$ будет состоять из набора $(m_n - 2)$-х ОКС и может быть разложен либо по строкам $K_j\left(j = \overline{2,n}\right)$, либо по контурам $K\left(i = \overline{2,n}\right)$ в виде

$$\left\{ K_{ij} \right\} = K_j = \left(K_{2j}^{(z_{2j})} K_{3j}^{(z_{3j})} \ldots K_{nj}^{(z_{nj})} \right), \quad (10)$$

$$\left\{ K_{ij} \right\} = K_i = \left(K_{i2}^{(z_{i2})} K_{i3}^{(z_{i3})} \ldots K_{in}^{(z_{in})} \right). \quad (11)$$

Исходя из записи ООКС $\{K_{ij}\}$ (10) можно определить временную матрицу $\{T_j\}$:

$$\left\{T_j\right\} = \begin{vmatrix} z_{22} & z_{32} & \ldots & z_{n2} \\ \vdots & \vdots & & \vdots \\ z_{2n} & z_{3n} & \ldots & z_{nn} \end{vmatrix}. \quad (12)$$

Время t_j установления j-й строки матрицы (время реализации операции) значений $a\,\beta \pmod{m_n}$ равно сумме ПООКС для j-й строки матрицы (12) умноженной на величину $k \cdot \tau$ (4):

$$t_j = \sum_{i=2}^{n} z_{ij} k\tau. \quad (13)$$

Очевидно, что $t \approx t_j$. Время t реализации модульной операции умножения можно так же определить, исходя из выражения (11). Действительно, в этом случае временная матрица $\{T_i\}$ по контурам будет совпадать с транспонированной матрицей $\{T_j\}$, т.е.

$$\left\{T_i\right\} = \left\{T_j\right\}^T = \begin{vmatrix} z_{22} & z_{23} & \ldots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z_{n2} & z_{n3} & \ldots & z_{nn} \end{vmatrix}, \quad (14)$$

а время установления j-й строки матрицы равно сумме ПООКС для j-го столбца матрицы (14), умноженной на величину $k\tau$. Очевидно, что в общем случае время t реализации модульной операции $a\,\beta \pmod{m_n}$ как и для операции модульного сложения и вычитания, зависит от величины операнда β (от номера j устанавливаемой строки), т.е.

$$t_{j\,min} \le t \le t_{j\,max}. \quad (15)$$

Таблица 4

Содержимое разрядов КСР

β_i	a_i				
	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

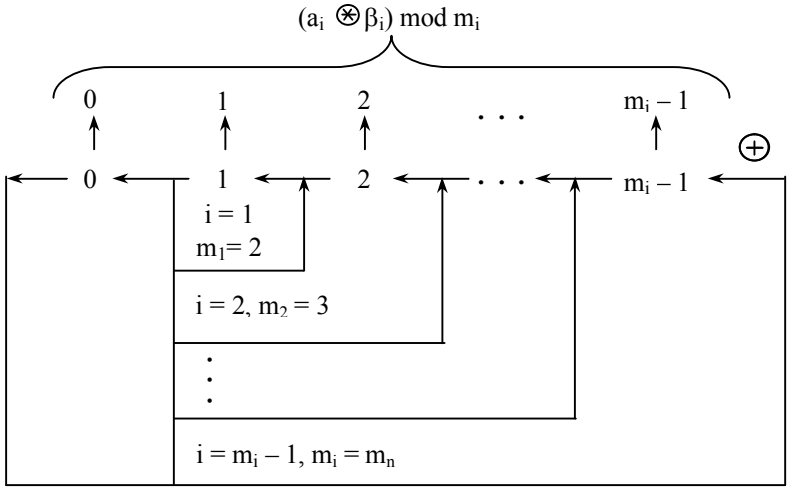


Рис. 4. Схема реализации обобщенной арифметической операции для произвольного модуля МСС

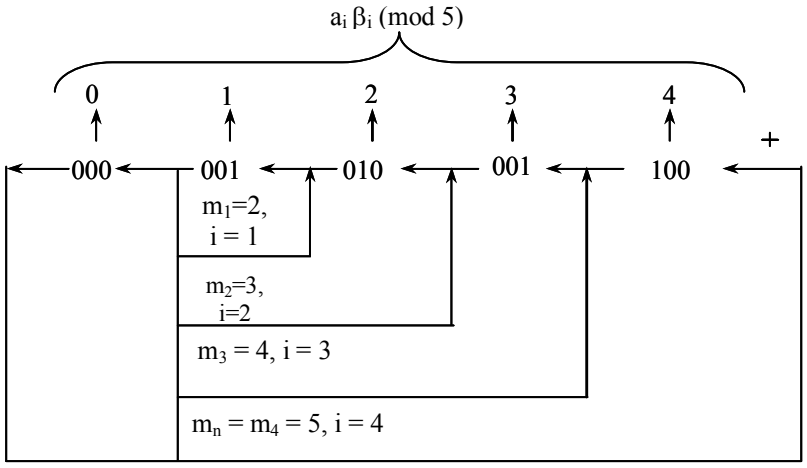


Рис. 5. Схема реализации операции модульного умножения для $m_i = 5$

Исходя из выражения (15), целесообразно оперировать средним $t_{ср}$ и максимальным t_{max} временем реализации модульных операций

$$t_{max}^{(x)} = \sum_{i=2}^{n} t_{ij\ max}\ , \qquad (16)$$

$$t_{ср}^{(x)} = \sum_{i=2}^{n} t_{ij\ max}\ /(n-1)\,. \qquad (17)$$

В соответствии с выражением (13) запишем формулы (16), (17) в виде

$$t_{max}^{(x)} = k\tau\cdot(m_n - 1)m_n/2\,, \qquad (18)$$

$$t_{ср}^{(x)} = k\tau\sum_{i=2}^{n}(m_i - 2)/2\,, \qquad (19)$$

а для операции сложения (вычитания) формула (4) представится в виде

$$t_{max}^{(+)} = k\tau\cdot(m_n - 1)\,, \qquad (20)$$

$$t_{ср}^{(+)} = k\tau\cdot\sum_{i=1}^{n}(m_i - 1)/n\,. \qquad (21)$$

Отметим, что в каждом из контуров можно применить разработанные выше алгоритмы сокращения времени установления нужной строки таблицы данной модульной операции. В этом случае, результат операции модульного умножения будет определяться за время меньшее, чем то, что определяется выражениями (16) – (19). Известно [1], что время реализации операций сложения $t_{слож}$ и умножения $t_{умн}$ в ПСС определяется следующими выражениями:

$$t_{слож} = \tau + (\rho - 1)(\tau_и + \tau_{или} + \tau)\,, \qquad (22)$$

$$t_{умн} = \rho(\tau + t_{слож})\,, \qquad (23)$$

где ρ – количество двоичных разрядов в представлении операндов (разрядная сетка СОИУ): $\tau_и$ ($\tau_{или}$) – время прохождения сигнала через элемент И (ИЛИ) (время «срабатывания» соответствующего логического элемента). Принимая во внимание, что $\tau_и \approx \tau_{или} \approx \tau/2$, запишем выражения (22) и (23) в виде

$$t_{слож} = \tau\,(2\rho - 1), \qquad (24)$$

$$t_{умн} = 2\tau\rho^2. \qquad (25)$$

Проведем сравнительный анализ времени реализации арифметических операций в ПСС и в МСС для однобайтового ($l = 1$) и четырехбайтового ($l = 4$) машинного слова. Для $l = 1$ ($\rho = 8$) МСС может представляться набором следующих оснований: $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$; для $l = 4(\rho = 32) – m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$, $m_9 = 23$, $m_{10} = 29$.

Отметим, что время реализации арифметических операций в МСС по принципу кольцевого сдвига определяется временем реализации данной модульной операции для максимального по величине модуля m_n МСС, т.е. для $l = 1$ – это модуль $m_n = m_4 = 7$, а для $l = 4$ – это модуль $m_n = m_{10} = 29$. В соответствии с формулами (18) – (23) рассчитаем максимальное и среднее время для реализации арифметических операций (табл. 5) без применения алгоритмов их ускорения в МСС и для двоичных ПСС. Из табл. 5 видно, что применение принципа кольцевого сдвига, даже без применения алгоритмов повышения быстродействия выполнения модульных операций, позволяет уменьшить, по сравнению с ПСС, время реализации модульной операции арифметического умножения в при приемлемом времени выполнения модульной операции сложения (вычитания) в МСС. Отметим, что с увеличением величины l эффективность применения ПКС для выполнения арифметической операции умножения в классе вычетов возрастает.

Рассмотрим пример конкретной реализации операции модульного умножения при $m_n = 5$ (табл. 4). В соответствии с выражением (10) ООКС для $m_n = 5$ представим в виде

$$\left\{K_{ij}\right\} = \left\{K_{2j}^{z_{2j}} K_{3j}^{z_{3j}} K_{4j}^{z_{4j}}\right\}. \qquad (26)$$

В общем виде ООКС разложим по строкам и контурам.

По строкам:

$$j = 2,\ K_2 = \left\{ K_{22}^{z_{22}} K_{32}^{z_{32}} K_{42}^{z_{42}} \right\},$$

$$j = 3,\ K_3 = \left\{ K_{23}^{z_{23}} K_{33}^{z_{33}} K_{43}^{z_{43}} \right\},$$

$$j = 4,\ K_4 = \left\{ K_{24}^{z_{24}} K_{34}^{z_{34}} K_{44}^{z_{44}} \right\}.$$

По контурам:

$$i = 2,\ K_2 = \left\{ K_{22}^{z_{22}} K_{23}^{z_{23}} K_{24}^{z_{24}} \right\},$$

$$i = 3,\ K_3 = \left\{ K_{32}^{z_{32}} K_{33}^{z_{33}} K_{34}^{z_{34}} \right\},$$

$$j = 4,\ K_4 = \left\{ K_{42}^{z_{42}} K_{43}^{z_{43}} K_{44}^{z_{44}} \right\}.$$

На основании соотношения (26) ООКС для соответственно второй (j = 2), третьей (j = 3) и четвертой (j = 4) строк табл. 4 будет иметь следующий вид:

$$K_2 = \left\{ K_{22}^{(0)} K_{32}^{(2)} K_{42}^{(3)} \right\},\ K_3 = \left\{ K_{23}^{(1)} K_{33}^{(2)} K_{43}^{(2)} \right\},$$

$$K_4 = \left\{ K_{24}^{(1)} K_{34}^{(1)} K_{44}^{(1)} \right\}.$$

Общий алгоритм образования ПОКС для $m_n = 5$ представлен в табл. 6 (см. рис. 5). Определим время t_j установления j-й строки табл. 6 в соответствии с выражением (13): $t_2 = 15\ \tau$, $t_3 = 15\ \tau$, $t_4 = 9\ \tau$ ($k = [\log_2(m_n - 1)] + 1 = 3$). Отметим, что в соответствии с выражением (23) максимальное время установления j-й строки $t_{max}^{(x)} = 30\tau$ ($t_{cp}^{(x)} = 13{,}5\tau$). Данное обстоятельство подтверждает, что реальная эффективность применения ПКС выше, чем та, что определяется выражениями (18) и (21).

Таблица 5

Максимальное и среднее время реализации арифметических операций

l (m_n)	t [τ]					
	ПСС		МСС			
	сложение (вычитание)	умножение	Сложение (вычитание)		умножение	
			максимальное	среднее	максимальное	среднее
$l = 1$, ($m_n = 7$)	17	128	18	11,5	63	22,5
$l = 4$, ($m_n = 29$)	65	2048	140	59,5	2030	297,5

Таблица 6

Общий алгоритм образования ПОКС для $m_n = 5$

Номер устанавливаемой строки матрицы $j = \beta = \overline{2,4}$	Номер контура $i = \overline{2,4}$	ПОКС $z_{i,j}$	Исходное содержимое КСР	ОКС (z_i) $K_{i,j}$	ООКС $\{K_{i,j}\}$
j = 2	i = 4	$z_{42} = 3$	0 2 3 4 1 0 3 4 1 2 0 4 1 2 3	$K_{42}^{(3)}$	$K_2 = \left\{K_{22}^{(0)} K_{32}^{(2)} K_{42}^{(3)}\right\}$
	i = 3	$z_{32} = 2$	0 1 2 4 3 0 2 4 1 3	$K_{32}^{(2)}$	
	i = 2	$z_{22} = 0$	0 2 4 1 3	$K_{22}^{(6)}$	

Окончание табл. 6

j = 3	i = 4	$z_{43} = 2$	0 2 3 4 1 0 3 4 1 2	$K_{43}^{(2)}$	$K_3 = \{K_{23}^{(1)} K_{33}^{(2)} K_{43}^{(2)}\}$
	i = 3	$z_{33} = 2$	0 4 1 3 2 0 1 3 4 2	$K_{33}^{(2)}$	
	i = 2	$z_{23} = 1$	0 3 1 4 2	$K_{23}^{(1)}$	
j = 4	i = 4	$z_{44} = 1$	0 2 3 4 1	$K_{44}^{(1)}$	$K_4 = \{K_{24}^{(1)} K_{34}^{(1)} K_{44}^{(1)}\}$
	i = 3	$z_{34} = 1$	0 3 4 2 1	$K_{34}^{(1)}$	
	i = 2	$z_{24} = 1$	0 4 3 2 1	$K_{24}^{(1)}$	

Основным недостатком последнего рассмотренного метода реализации арифметических операций в классе вычетов является длительность их выполнения, что снижает эффективность использования ПКС. Этот недостаток обусловлен тем, что структура $P_{\text{исх}}^{(m_i)}$ (1) представлена набором исходных остатков первой строки матрицы $(a_i \pm \beta_i) \bmod m_i$, отображаемых двоичным кодом. В этом случае время реализации модульного сложения двух операндов $A = (a_1, a_2, \ldots, a_n)$ и $B = (\beta_1, \beta_2, \ldots, \beta_n)$ в МСС определяется выражением

$$t_{\text{слож}} = K\beta_{\max\, i}\tau, \qquad (27)$$

где τ – время сдвига одного бита информации (одного двоичного разряда), где $\beta_{\max\, i} = \max\{\beta_i\} \in B$ для $i = \overline{1,n}$.

Выводы

1. На основе сформулированного ПКС в статье предложено использовать для реализации арифметических операций в МСС метод двоичного кодирования.

2. Разработан алгоритм реализации данного метода, а также алгоритм, позволяющие сократить время реализации арифметических операций в МСС. Проведенный расчет времени реализации арифметических операций в МСС, даже без учета влияний алгоритмов повышения быстродействия, показал высокую эффективность использования предложенного метода.

3. Рассмотренные методы и алгоритмы могут быть рекомендованы к практическому использованию для устройств обработки информации СОИУ, функционирующих в реальном времени с повышенными требованиями по отказоустойчивости.

Список литературы

1. *Методы многоверсионной обработки информации в модулярной арифметике: моногр. / [В.И. Барсов, В.А. Краснобаев, А.А. Сиора, И.В. Авдеев]. – Х.: МОН, УИПА, 2008. – 460 с.*
2. *Модели и методы повышения отказоустойчивости и производительности управляющих вычислительных комплексов специализированных систем управления реального времени на основе применения непозиционных кодовых структур модулярной арифметики: моногр. / [В.И. Барсов, Л.С. Сорока, В.А. Краснобаев, Хери Али Абдуллах]. – Х.: МОН, УИПА, 2008. – 147 с.*
3. *Барсов В.И. Методология параллельной обработки информации в модулярной системе счисления: моногр. / В.И. Барсов, Л.С. Сорока, В.А. Краснобаев. – Х.: МОН, УИПА, 2009. – 288 с.*
4. *Система обработки информации и управления АСУ ТП на основе применения кодов в модулярной арифметике: моногр. / [В.И. Барсов, В.А. Краснобаев, И.А. Фурман, и др.]. – Х.: МОН, УИПА, 2009. – 159 с.*
5. *Модели и методы параллельной реализации логических операций в АСУ ТП: моногр. / [В.И. Барсов, В.А. Краснобаев, И.А. Фурман, и др.]. – Х.: МОН, УИПА, 2009. – 138 с.*

Поступила в редколлегию 29.11.2011

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

ЗАСТОСУВАННЯ МЕТОДУ ДВІЙКОВОГО КОДУВАННЯ РЕАЛІЗАЦІЇ МОДУЛЬНИХ ОПЕРАЦІЙ В СИСТЕМАХ ОБРОБКИ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ

В.І. Барсов, В.А. Краснобаєв, В.О. Жадан, Є.О. Сотник

Розглянуто можливість застосування методу двійкового кодування, заснованого на використанні принципу кільцевого зсуву, при реалізації модульних операцій в системі обробки інформації та управління.

Ключові слова: *модулярна система числення, кільцевий зсувний регістр, принцип кільцевого зсуву, система обробки інформації та управління.*

APPLICATION OF THE IMPLEMENTATION OF MODULAR BINARY ENCODING OPERATIONS INFORMATION HANDLING SYSTEM CONTROL

V.I. Barsov, V.A. Krasnobaev, V.O. Zhadan, Ye.A. Sotnik

The possibility of applying the method of binary encoding based on the use of the principle of circular shift in the implementation of modular operations in the processing and control.

Keywords: *modular numbering system, circular shift register, the principle of ring-shear system and information processing.*