УДК 681.321

Мохаммед Джасим Мохаммед,
М. И. Луханин, В. А. Краснобаев, Н. С Деренько

Методы и алгоритмы обработки информации в модулярной арифметике

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Анализ задачи и обзор литературных источников. Малоразрядность остатков в представлении чисел в модулярной арифметике (МА), например в системе остаточных классов (СОК), дает возможность широкого выбора вариантов системотехнических решений при реализации модульных операций.

Известно [1 – 3], что существует четыре принципа реализации арифметических операций в МА: сумматорный принцип (СП) (на базе малоразрядных двоичных сумматоров [1]); табличный принцип (ТП) (на основе использования ПЗУ [4]); прямой логический принцип реализации арифметических операций, основанный на описании модульных операций на уровне систем переключательных функций, посредством которых формируются значения двоичных разрядов результирующих вычетов (в качестве элементной базы для технической реализации данного принципа целесообразно использовать систолические и программируемые логические матрицы, а также ПЛИС [3]); принцип кольцевого сдвига (ПКС), основанный на использовании кольцевых регистров сдвига (КРС) [5 – 8].

Отсутствие межразрядных связей между двоичными разрядами операционного устройства (ОУ) системы обработки информации (СОИ) в процессе реализации модульных операций на основе ТП или ПКС является одной из главных и наиболее привлекательных особенностей модулярной арифметики. Если ТП и методы его реализации хорошо известны и довольно глубоко исследованы, то ПКС был предложен сравнительно недавно, поэтому для его широкого использования необходимо решить ряд задач, связанных с выбором рациональной структуры ОУ СОИ, что в свою очередь непосредственно связано с методами и алгоритмами обработки информации в МА на основе ПКС.

Цель статьи – рассмотрение практической возможности использования ПКС в МА при разработке и реализации методов и алгоритмов обработки информации в реальном времени.

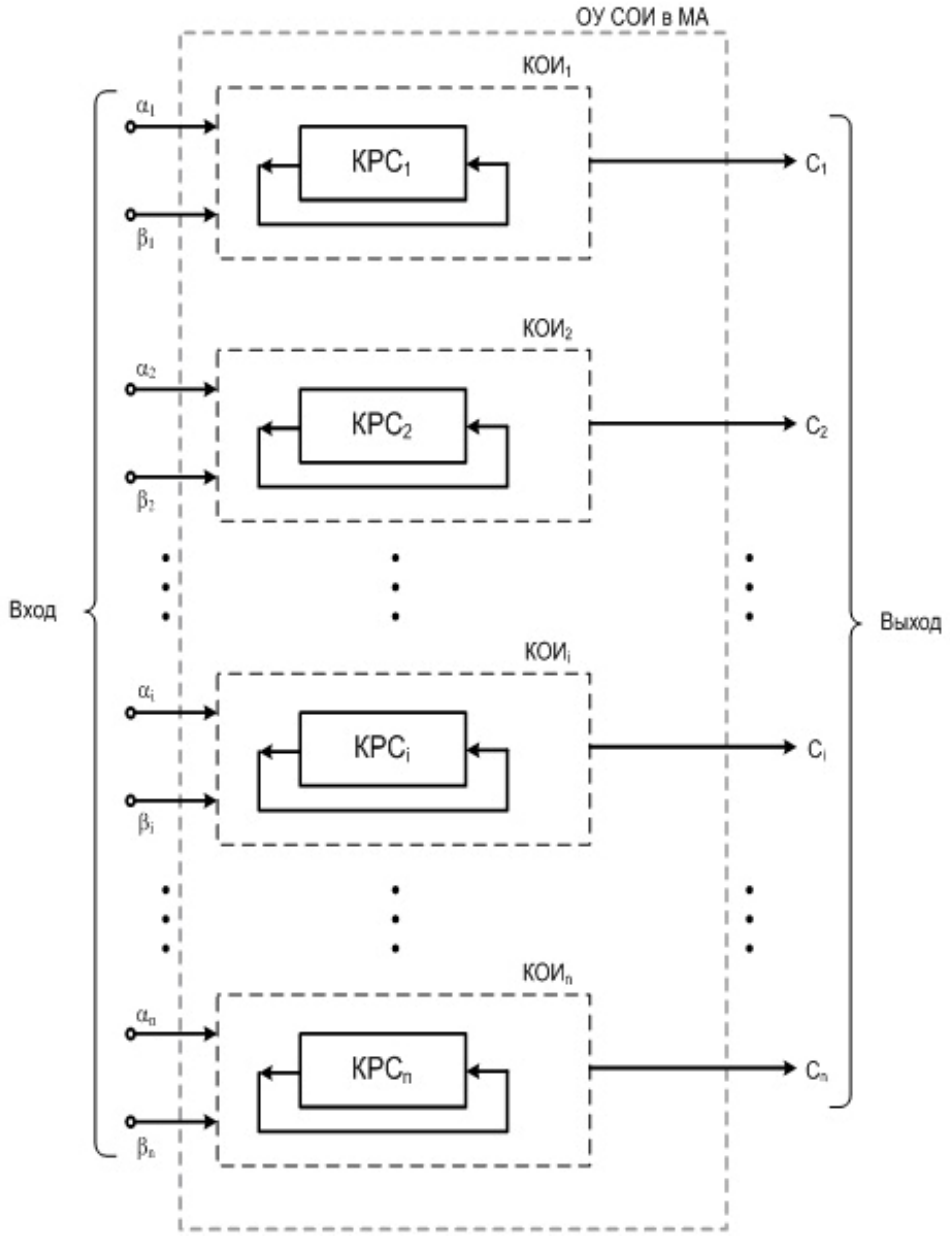
Основная часть. Согласно таблице Кэли для аддитивных операций (см. работу [2]) нужная строка таблицы модульного сложения (вычитания) может быть получена путем последовательного циклического сдвига элементов первой строки (столбца). Системотехнической основой для алгоритмов реализации методов арифметических операций в МА на основе ПКС являются кольцевые регистры сдвига. В этом случае структурная схема ОУ СОИ в МА представляет собой n (по числу оснований СОК) независимых и параллельно во времени функционирующих каналов обработки информации (КОИ) (рисунок).

В качестве примера рассмотрим реализацию ПКС для $m_i = 7$. В этом случае исходное состояние содержимого КРС для операции $(\alpha+\beta)\mathrm{mod}7$ соответствует первой строке таблицы Кэли, т.е.

$$000 – 001 – 010 – 011 – 100 – 101 – 110. \qquad (1)$$

В общем случае максимальная длительность реализации модульной операции сложения - вычитания в условных временных тактах t равна $t = \left]\log_2 m_i\right[\cdot m_i$, где один разряд КРС состоит из $\left]\log_2 m\right[$ двоичных разрядов (метод двоичного позиционно-остаточного кодирования [6]). Очевидно, что с ростом величины основания (модуля) m_i СОК существенно уменьшается быстродействие реализации модульных операций в МА.

Существует возможность получения результата выполнения модульных операций, используя ПКС, на основе унитарного кодирования содержимого разрядов КРС (метод унитарного позиционно-остаточного кодирования [8]). При этом максимальная длительность выполнения модульной операции сложения - вычитания равна значению $t = m_i$, а исходное состояние (1) кольцевого регистра для m_i=7 можно представить в следующем виде:



Упрощенная структурная схема операционного устройства системы обработки информации в МА

$$0 - 0 - 0 - 1 - 0 - 1 - 1. \qquad (2)$$

Рассмотрим алгоритм формирования исходного состояния кольцевого регистра сдвига для m_i = 4 [9]. При этом необходимо получить следующую совокупность остатков: 00, 01, 10, 11. Формирование исходного содержимого понятно из приведенного ниже алгоритма, справа от которого расположена соответствующая циркулянтная матрица состояний кольцевого регистра:

$$\begin{array}{r} 00 \\ 01 \\ 11 \\ \hline 0011 \end{array} \qquad \begin{pmatrix} 0011 \\ 0110 \\ 1100 \\ 1001 \end{pmatrix}.$$

При m_i = 4 быстродействие выполнения операций модульного сложения-вычитания увеличивается в два раза. В этом случае исходное значение содержимого разрядов КРС имеет вид 0 0 1 1. Исходное состояние разрядов КРС для m_i >4 будет определяться аналогично. Так, например, при m_i = 7 получим

$$\begin{array}{r} 000 \\ 001 \\ 010 \\ 011 \\ \hline 0001011 \end{array} \qquad \begin{pmatrix} 0001011 \\ 0010110 \\ 0101100 \\ \dots \\ 1000101 \end{pmatrix}.$$

Быстродействие реализации арифметических операций ОУ СОИ при использовании метода унитарного позиционно-остаточного кодирования увеличивается в $]\log_2 7[= 3$ раза. Рассмотрим известный в теории функций метод реализации арифметических операций в МА, основанный на построении нормальных периодических систем с равномерным распределением дробных долей. Пусть ρ и q – натуральные числа. Составим ρ-значное разложение чисел 0, 1, 2, . . . , $q^\rho - 1$ в системе счисления с основанием q:

0 = 00 …00;
1 = 00 …01;
. . .

$$q^\rho - 1 = q-1\,q-1 \dots q-1\,q-1. \qquad (3)$$

Нормальной периодической системой $P_\rho(q)$ называется последовательность из $q^\rho + \rho - 1$ знаков вида

$$\delta_1\delta_2\delta_3\dots\delta_{q^\rho+\rho-1}, \qquad (4)$$

где каждое δ_ν - целое число из отрезка [0,q-1], обладающее тем свойством, что совокупность ρ-значных чисел

$$\delta_1\delta_2\dots\delta_\rho, \delta_2\delta_3\dots\delta_{\rho+1}, \dots, \delta_{q^\rho}\delta_{q^\rho+1}\dots\delta_{q^\rho+\rho+1},$$

получающихся из соседних знаков последовательности (4), совпадает с совокупностью всех возможных ρ-значных чисел вида (3).

Рассмотрим при конкретных значениях ρ=2 и q=2 возможные двоичные разложения чисел 0, 1, 2, 3. Получим следующие значения

0=00, 1=01, 2=10, 3=11. (5)

В этом случае нормальная периодическая система имеет вид $P_2(2)$=11001 и совокупность двухзначных чисел 11, 10, 00, 01, полученных из этой системы, совпадает с совокупностью двоичных чисел вида (5). Отметим, что при q=2 ρ=p.

Правило построения нормальной периодической системы для случая двоичной системы счисления следующее. Первые ρ двоичных чисел выбирают равными единице. Справа приписывают нуль и полученное ρ-значное двоичное число без первого левого двоичного знака сравнивают с исходным. После этого процесс приписывания нулей и сдвиг на один знак вправо продолжается. Сравнение полученного нового числа производится со всеми предыдущими до тех пор, пока ρ-значные числа впервые совпадают. Единицу приписывают справа только в том случае, когда добавление нуля приводит к уже встречавшемуся ρ-значному числу. В этом случае процесс приписывания заканчивается, далее происходит сдвиг на один знак с последующим сравнением. Тогда любой новый двоичный знак (ноль или единица) приводит к ρ-значному числу, которое уже встречалось. Приведенный алгоритм наиболее эффективно использовать при модулях $m=2^p$. В частности, при $m=2^3$ имеем

P3(2)=1110001011. (6)

При использовании алгоритма формирования исходного состояния КРС выигрыш в быстродействии численно равен значению ρ нормальной периодической системы $P_\rho(2)$, т.е. в данном случае – трем. Учитывая, что матрица исходных состояний кольцевого регистра является циркулянтом, последние два знака последовательности (6) можно удалить. В этом случае в окончательном варианте начальное содержимое разрядов КРС будет равно

1 – 1 – 1 – 0 – 0 – 0 – 1 – 0.

Другой метод повышения производительности выполнения модульных операций сложения - вычитания в МА, основанный на использовании ПКС, предполагает унитарное кодирование содержимого разрядов КРС [8]. В этом случае исходное содержимое разрядов КРС для произвольного модуля m МА можно представить в виде информационной структуры $P_{\text{исх}}^{(m)}$ вида (7), т.е. как унитарный m-разрядный код

$$P_{\text{исх}}^{(m)} = P(\alpha_j) \| P(\alpha_{j-1}) \| \ldots \| P(1) \| P(0), \quad (7)$$

где $\|$ – операция конкатенации (операция склеивания, или оператор последовательного присоединения символов); $P(\alpha_j)$ - двоичный разряд цифровой структуры (7), единичное состояние которого соответствует значению операнда α, представленного унитарным кодом $\alpha_j = \overline{0, m-1}$. При этом исходное состояние КРС состоит из m-двоичных разрядов и первый операнд α, отображаемый унитарным кодом, заносится в α-й единичный разряд кольцевого регистра, переводя его в единичное состояние. Второй операнд β указывает на число сдвигов двоичных разрядов содержимого КРС, определяя время реализации

арифметических операций по модулю, т.е. t = β. В общем виде данный унитарный код, состоящий из совокупности строк (столбцов) единичной матрицы I, представляет собой нелинейный эквидистантный равновесный код вида

$$I = \begin{pmatrix} 100...0 \\ 010...0 \\ ... \\ 000...1 \end{pmatrix}.$$

Для оценки быстродействия алгоритма реализации модульных операций сложения - вычитания будем использовать данные таблицы Кэли, где содержатся величины времен сдвигов t_{ij} для каждой пары операндов α и β. При этом показателем для оценки времени реализации арифметических операций выбрано значение $T_{m,}$ где

$$T_m = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1} t_{ij} .$$

Табл. 1 представлена модифицированная таблица Кэли для алгоритма, основанного на выборе исходного состояния КРС и реализации операции $(\alpha+\beta)$mod7, табл. 2 – соответственно таблица Кэли для типового варианта унитарного кодирования операндов и такой же модульной операции. В первом случае при нечетном m_i имеем $T_m = 2\left(1+\frac{m-1}{2}\right)\frac{m-1}{2} = \frac{m\left(m^2-1\right)}{2}$, при m_i = 11 – T_{11}=660, а если m_i-четное, то

$$T_m = 2\left(1+\frac{m}{2}\right)\frac{m^2}{2} - 4\left(1+\frac{m}{2}\right)\frac{m}{2} = \frac{m}{2}\left(m^2-4\right).$$

Для второго алгоритма значение T_m составляет величину

$$T_m = \frac{0+(m-1)}{2}m^2 = \frac{m^2}{2}(m-1),$$

т.е. если m_i =11, то T_{11} =605. В этом случае имеем выигрыш в быстродействии реализации модульных операций в МА порядка 10%.

Таблица 1

Модифицированная таблица Кэли

β/α	0	1	2	3	4	5	6
0	3	2	1	1	3	0	2
1	2	1	1	3	0	2	3
2	1	1	3	0	2	3	2
3	1	3	0	2	3	2	1
4	3	0	2	3	2	1	1
5	0	2	3	2	1	1	3
6	2	3	2	1	1	3	0

Таблица 2

Таблица Кэли для варианта унитарного кодирования

β/α	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6

Для оценки быстродействия алгоритмов выполнения модульных операций методами, основанными на ПКС, будем использовать интегральный критерий R [9].

Под интегральным критерием R сравнительной оценки производительности выполнения арифметических модульных операций для ПКС условимся понимать отношение общего количества сдвигов разрядов КРС при выполнении данной операции (для каждой пары операндов), при определенном модуле m и типе операции к соответствующей величине $T_{m,}$ т.е

$$R = \frac{m^2}{2}\left(m-1\right)/T_m. \qquad (8)$$

В качестве примера рассмотрим двухуровневую структуру тракта обработки информации (ТОИ) СОИ, реализованного по ПКС. Она состоит из трех кольцевых регистров сдвига и преобразователя. Первый КРС реализует операцию $(\alpha_1 * \beta_1)\,\mathrm{mod}\,m_1$, второй – $(\alpha_2 * \beta_2)\,\mathrm{mod}\,m_2$ (m_1 и m_2 – составные подмодули модуля m, а $\alpha = (\alpha_1, \beta_1)$ и $\beta = (\alpha_2, \beta_2)$). В третьем КРС формируется результат операции по модулю m. При этом ее максимальная длительность

$$T = \frac{m}{m_1} + m_1.$$

Рассмотрим практические методы реализации модульных операций в МА, основанных на ПКС. Так, один из возможных эффективных методов основан на использовании закономерности распределения в поле матрицы результатов выполнения арифметических операций (табл. 3). Содержимое нижней половины строк табл. 3 можно получить путем переноса начала отсчета разрядов КРС. Заменив последовательность значений содержимого КРС 0, 1, 2, 3, 4, 5 на 3, 4, 5, 0, 1, 2, получим значения в верхних трех строках идентичные значениям нижних строк. Эта процедура позволяет выбирать в качестве исходного состояния разрядов КРС строку при β = 0 (для β=5, 0, 1) либо при β =3 (для β=2, 3, 4), которая формируется путем коммутации выходов операнда α, представленного в унитарном коде, с соответствующими входами кольцевого регистра. Необходимые значения результата операции определяются путем сдвига содержимого КРС вправо или влево. Схематично получение необходимых значений строк для операций модульного сложения и вычитания можно представить в виде

$$\begin{array}{c} 5\ 01234 \\ \underline{1-\uparrow 1+} \\ \underline{1-\uparrow 1+} \\ \overline{(\alpha+\beta)\bmod 6} \end{array}.$$

Стрелка указывает исходное содержимое определенного разряда КРС, а значения “1-“ и “1+” определяют количество тактов сдвига и их направление. Следовательно, для проведения операции модульного вычитания в схеме реализации операции модульного сложения достаточно изменить направление сдвига содержимого разрядов КРС.

Таблица 3

Матрица операции модульного сложения

$\beta\backslash\alpha$	0	1	2	3	4	5
5	5	0	1	2	3	4
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3

Общим случаем является вариант метода разбивки порядка содержимого КРС по модулю m на d интервалов с выбором середины оси. В зависимости от соотношения операндов α и β производится выбор средней точки на оси, а затем осуществляется сдвиг содержимого кольцевого регистра вправо или влево от оси. В этом случае максимальное количество сдвигов

$$T = \left]\frac{m-d}{2d}\right[. \qquad (9)$$

Характерно, что при d=1 согласно (9) имеем вариант унитарного кодирования информации, а для m=d получим характеристики, свойственные табличному методу реализации модульной операции. Исходя из временных требований к обработке информации ОУ СОИ можно найти оптимальное значение величины d на основании заданных требований к обработке информации. Для данного метода получим следующее значение искомого времени:

$$T_m = 2d\left(1+\frac{m-d}{2}\right)\frac{m-d}{2d}\cdot\frac{m}{2d} = \left]\frac{m}{4d}\right[\cdot\left(m^2-d^2\right),$$

т.е. если m = 11, то R≈2,59. Модифицированная матрица Кэли для m=6 представлена табл. 4.

Таблица 4

Модифицированная таблица Кэли для операции $(\alpha+\beta)\bmod 6$

$\beta\backslash\alpha$	0	1	2	3	4	5
5	1	0	1	1	0	1

Продолжение таблицы 4

0	0	1	1	0	1	1
1	1	1	0	1	1	0
2	1	0	1	1	0	1
3	0	1	1	0	1	1
4	1	1	0	1	1	0

Следующий алгоритм реализации арифметических операций предполагает использовать паузы между тактовыми импульсами при продвижении содержимого КРС в соответствии значению α первого операнда. При этом существенно уменьшается количество используемого оборудования ОУ СОИ, однако длительность бинарной операции будет равна max(α , β), что отражено в табл. 5 [9].

Таблица 5

Исходное содержимое разрядов КРС для $(\alpha+\beta)$ mod7

$\beta\backslash\alpha$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	1	2	3	4	5	6
2	2	2	2	3	4	5	6
3	3	3	3	3	4	5	6
4	4	4	4	4	4	5	6
5	5	5	5	5	5	5	6
6	6	6	6	6	6	6	6

Для определения значения T_m воспользуемся теорией конечных разностей. В табл. 6 приведена количественная связь между временем T_m и величиной модуля m_i для $m=\overline{1,7}$.

Таблица 6

Значения величин T_m и m_i

m_i	1	2	3	4	5	6	7
T_m	0	3	13	34	70	125	203

Рассмотрим первые разности в виде

T1, T2, T3, T4, T5, T6, T7, … (10)

последовательности ΔT_1, ΔT_2, ΔT_3, ΔT_4, ΔT_5, ΔT_6, …, где $\Delta T_i=T_{i+1}-T_i$ (i=1, 2, 3, ...). Аналогично определяются и последовательности высших разностей

T1, T2, T3, T4, T5, T6, T7,

ΔT1, ΔT2, ΔT3, ΔT4, ΔT5, ΔT6,

Δ2T1, Δ2T2, Δ2T3, Δ2T4, Δ2T5,

Δ3T1, Δ3T2, Δ3T3, Δ3T4,… .

Тогда для последовательности, соответствующей табл. 6, имеем

0, 3, 13, 34, 70, 125, 203,

3, 10, 21 ,36, 55, 78,

7, 11, 15, 19, 23,

4, 4, 4, 4,

0, 0, 0, .

Следовательно, имеем разностное линейное однородное уравнение четвертого порядка $\Delta^4 T_m = 0$. Для его решения используем теорию возвратных последовательностей. Разностному уравнению соответствует возвратное уравнение четвертого порядка

$$T_{m+4} = 4 \cdot T_{m+3} - 6T_{m+2} + 4T_{m+1} - T_m, \qquad (11)$$

решение которого определяется по формуле

$$T_m = B_0 + B_1 (m-1) + B_2 (m-1)^2 + B_3 (m-1)^3. \qquad (12)$$

Чтобы найти коэффициенты B_0, B_1, B_2 и B_3, достаточно решить следующую систему алгебраических уравнений, образующих базис для (11):

$$\begin{cases} B_0 = T_1 = 0, \\ B_0 + B_1 + B_2 + B_3 = T_2 = 3, \\ B_0 + 2B_1 + 4B_2 + 8B_3 = T_4 = 13, \\ B_0 + 3B_1 + 9B_2 + 27B_3 = T_4 = 34. \end{cases}$$

Из данной системы находим требуемые коэффициенты и, подставляя их в формулу (12), получаем

$$T_m = \frac{m(m-1)(4m+1)}{6},$$

откуда для m=11 имеем R≈0,73, т.е. производительность обработки информации СОИ в МА несколько снижена по сравнению с методом унитарного позиционно-остаточного кодирования. Отметим, что существенно меньшими временными затратами на реализацию аддитивной операции отличается циркулянтный алгоритм, суть которого сводится к предварительному определению меньшего из операндов α и β и затем использованию его для изменения состояний разрядов КРС [8]. При этом если $\alpha < \beta$, то единица из нулевого разряда кольцевого регистра сдвигается вправо в $(\alpha - \beta)$-й разряд. В противном случае производится сдвиг влево содержимого КРС в $(\beta-\alpha)$-й разряд, что соответствует значениям табл. 7.

Таблица 7

Модифицированная таблица Кэли для m_i=7

$\beta\backslash\alpha$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	0	1	2	3	4	5
2	2	1	0	1	2	3	4
3	3	2	1	0	1	2	3
4	4	3	2	1	0	1	2
5	5	4	3	2	1	0	1
6	6	5	4	3	2	1	0

Используя теорию конечных разностей, получаем соотношение

$$T_m = \frac{m(m^2-1)}{3} \qquad (13)$$

при начальных условиях B_0=0, B_1=2, B_2=8 и B_3=20 и

$$R = \frac{3m}{2(m+1)}$$

при m=11 R≈1,38.

Существенно уменьшить аппаратурные затраты без снижения быстродействия выполнения аддитивных операций позволяет алгоритм, использующий ПКС. В этом случае инверсный выход последнего разряда КРС соединен с входом первого разряда, образуя замкнутое кольцо передачи информации (аналог счетчика Джонсона). При этом коэффициент счета увеличивается в два раза по сравнению с обычным кольцевым счетчиком при сохранении основных достоинств последнего, что позволяет (в отличие от СП) эффективно использовать большие по величине модули СОК. Код, в котором работает счетчик Джонсона, называют кодом Либау - Крейга. К его достоинству следует отнести то, что состояния 01 или 10 для двух соседних разрядов в течение одного цикла функционирования счетчика имеют место только один раз независимо от длины кодовой комбинации. Поэтому для технической реализации процесса преобразования кода необходимы лишь простейшие двухвходовые элементы. Второе достоинство счетчика Джонсона заключается в том, что в ходе счета только один триггер меняет свое состояние, и поэтому на выходах не возникают ложные пики напряжения, обусловленные задержками сигналов в разных разрядах, что, в свою очередь, повышает достоверность обработки информации.

Приведенный в работе [2] метод реализации модульных арифметических операций в МА, основанный на анализе четности величин входных операндов α, β, позволил создать ряд эффективных (с точки зрения быстродействия реализации арифметических операций) алгоритмов для его реализации.

Сокращение в ОУ СОИ диапазона обработки информации входных операндов до величины $(m_i-1)/2$ дало возможность существенно повысить быстродействие получения результата сложения (вычитания) вычетов по заданному модулю m_i. Количества сдвигов разрядов КРС для $(\alpha+\beta) \bmod 7$ даны в табл. 8.

Таблица 8

Таблица содержимого разрядов КРС для операции $(\alpha+\beta) \bmod 7$

$\alpha\ (\alpha')$ / $\beta\ (\beta')$	0 (0)	1 (0)	2 (1)	3 (1)	4 (2)	5 (2)	6 (3)
0 (0)	0	0	0	0	0	0	0
1 (1)	1	1	1	1	1	1	1
2 (1)	1	1	1	1	1	1	1
3 (2)	2	2	2	2	2	2	2
4 (2)	2	2	2	2	2	2	2
5 (3)	3	3	3	3	3	3	3
6 (3)	3	3	3	3	3	3	3

Определяя значения $\alpha' = (\alpha-1)/2$ и $\beta' = (\beta+1)/2$ путем составления соответствующих таблиц количества сдвигов разрядов КРС, находим:

если m – нечетное число, то при реализации операции $(\alpha+\beta) \bmod m$

$$T_m = \frac{m}{4}\left(m^2 - 1\right),$$

а при $(\alpha\text{-}\beta)\,\mathrm{mod}m$ $T_m = \frac{m}{4}(m-1)^2$;

если m - четное число, то при реализации операции $(\alpha+\beta)$ modm

$$T_m = \frac{m^3}{4},$$

а при $(\alpha\text{-}\beta)\,\mathrm{mod}m$ $T_m = \frac{m^2}{4}(m-2)$.

При m=11 получим $R = 2\frac{m^2}{m+1} \approx 1{,}83$.

Следующий алгоритм основан на взаимосвязи результата реализуемой аддитивной операции с направлением сдвига кольцевого регистра [6]. Обозначим через $\Omega_+ = \beta$ положительный сдвиг вправо на β разрядов содержимого КРС. Результаты анализа взаимосвязи модульной операции и направления сдвига содержимого КРС представлены в табл. 9.

Таблица 9

Таблица значений направлений сдвига содержимого разрядов КРС

Тип операции	$0 \le \beta \le \frac{m-2}{2}$	$\frac{m}{2} \le \beta \le m-1$
+	$\Omega_+ = \beta$	$\Omega_- = m - \beta$
−	$\Omega_- = \beta$	$\Omega_+ = m - \beta$

Анализ данного алгоритма показывает, что его “скоростные” параметры соответствуют рассмотренному выше алгоритму. Аналогичные характеристики производительности реализации арифметических операций в МА реализует и алгоритм, использующий свойства симметрии арифметической таблицы, т.е. в этом случае учитываются значения γ_α (γ_β) индексов операндов, которые могут принимать значения, равные 0 или 1 [1].

В заключение рассмотрим циркулянтный алгоритм реализации арифметических операций в МА, суть которого состоит в последовательном вычитании единицы из операндов α и β. При этом если $\alpha>\beta$, то результат модульного вычитания получается непосредственно, а если $\alpha<\beta$, то производится выходное преобразование типа модульного преобразования [m-(α-β)]modm. Реализация операции модульного сложения (α+β) проводится путем использования известного соотношения $(\alpha+\beta)\bmod m =$ $= \left[\alpha - (m-\beta)\right] \bmod m$, т.е. сводится к реализации операции модульного вычитания. Модифицированная таблица Кэли для количественной оценки сдвигов КРС в случае m_i=7 имеет вид, приведенный в табл. 10. Сравнивая ее с таблицей 7, отмечаем их идентичность, следовательно,

$$T_m = \frac{m\left(m^2 - 1\right)}{3}.$$

Таблица 10

Таблица содержимого разрядов КРС для операции $(\alpha + \beta)\, m\, od 7$

$\beta \backslash \alpha$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	0	1	2	3	4	5
2	2	1	0	1	2	3	4
3	3	2	1	0	1	2	3
4	4	3	2	1	0	1	2
5	5	4	3	2	1	0	1
6	6	5	4	3	2	1	0

Выводы. В данной статье рассмотрены эффективные методы и алгоритмы реализации арифметических операций в МА, основанные на использовании ПКС. К практическому использованию предложены два метода реализации арифметических операций в МА, основанных на ПКС: метод двоичного позиционно-остаточного кодирования и метод унитарного позиционно-остаточного кодирования. Проведен анализ эффективности использования данных методов, который показал их практическую реализуемость. Данные методы обработки информации рекомендованы к использованию в системах обработки информации реального времени.

Список литературы

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 444 с.

2. Краснобаев В.А. Методы повышения надежности специализированных ЭВМ систем и средств связи. – Х.: ХВУ, 1990. – 172 с.

3. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации. – Минск: Университетское, 1992. – 256 с.

4. Краснобаев В.А., Илюшко Я.В., Замула А.А. Универсальные алгоритмы сжатия табличных цифровых данных результатов выполнения арифметических операций в системе остаточных классов // Радиотехника. – 2005. – Вып. 141. – С. 217 – 225.

5. Краснобаев В.А. Принцип реализации арифметических операций в системе остаточных классов // АСУ и приборы автоматики . – 1988. – Вып. 86. – С. 82 – 85.

6. Долгов В.И., Краснобаев В.А., Кононова И.В. Метод и алгоритмы реализации арифметических операций в системе остаточных классов // Электронное моделирование. – 1989. – № 5. – С. 15 – 18.

7. Краснобаев В.А., Ирхин В.П. Алгоритм реализации операции модульного умножения в системе остаточных классов // Электронное моделирование. – 1993. – № 5. – С. 20 – 26.

8. Краснобаев В.А. Методы реализации модульных операций в системах цифровой обработки информации // Радиотехника. – 2001. – Вып. 119. – С. 130 – 134.

9. Ирхин В.П. Проектирование непозиционных специализированных процессоров. – Воронеж: Изд-во Воронеж. гос. ун-та, 1999. – 136 с.