УДК 681.04

В. А. КРАСНОБАЕВ, д-р. техн. наук

МЕТОДЫ РЕАЛИЗАЦИИ МОДУЛЬНЫХ ОПЕРАЦИЙ В СИСТЕМАХ ЦИФРОВОЙ ОБРАБОТКИ ИНФОРМАЦИИ

В ряде источников показана высокая эффективность применения системы счисления в остаточных классах (СОК) при решении отдельных задач обработки цифровой информации (решение задач фильтрации, БПФ, ДПФ и др.) [1-4]. В этом аспекте целесообразны теоретические и практические исследования путей дальнейшего повышения эффективности решения задач цифровой обработки (в частности, осуществление операции преобразования Фурье [5]) информации на основе использования свойств СОК.

В [6] детально рассмотрено влияние основных свойств СОК на структуру и принципы функционирования ЭВМ. В частности, показано, что малоразрядность остатков α_i дает возможность реализации арифметических операций в СОК либо на базе малоразрядных двоичных сумматоров, либо в табличном варианте. 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 остатка m_i СОК. При табличном варианте реализации арифметических операций отсутствуют межразрядные связи между обрабатываемыми операндами вообще, однако для достаточно большой разрядной сетки ЭВМ (для больших по величине модулей СОК) резко увеличивается количество и сложность оборудования операционного устройства (ОУ). Важно и актуально рассмотреть промежуточный вариант реализации арифметических операций в СОК, основанный на применении кольцевого сдвига путем использования кольцевых сдвигающих регистров (КСР).

В [7] сформулирован новый принцип реализации арифметических операций в СОК принцип кольцевого сдвига (ПКС), особенность которого заключается в том, что результат арифметической операции $(\alpha_i \pm \beta_i) \bmod m_i$ по произвольному модулю СОК, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется только за счет циклических сдвигов заданной цифровой структуры. Действительно, известная теорема Кэли устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. В этом случае матрица сложения для произвольного m_i модуля СОК будет задана табл. 1 (для $m_i = 5$ – табл. 2).

Таблица 1

β_i	α_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	...	$m_i - 2$

Таблица 2

β_i	α_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 группу всех целых чисел является гомоморфным. Это обстоятельство позволяет организовать процесс определения результата арифметических операций в СОК посредством использования ПКС.

Операнд в СОК представляется набором из n остатков $\{\alpha_i\}$, образованных путем последовательного деления исходного числа A на n взаимно попарно простых чисел $\{m_i\}$ для $(i = \overline{1,n})$. В этом случае совокупность остатков $\{m_i\}$ непосредственно отождествляется с суммой n простых полей Галуа вида $\sum_{i=1}^{n} GF(m_i)$.

Известно, что преобразование Фурье связано с вычисление полинома вида $P(x) = \sum_{i=1}^{n-1} \alpha_i x^i$. Одно из приложений преобразования Фурье – вычисление свертки $\sum_{i=1}^{n} \alpha_i \beta_i$ двух n - мерных векторов $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ и $B = (\beta_1, \beta_2, ..., \beta_n)$. Таким образом, эта операция является полным аналогом реализации арифметических операций умножения двух чисел A и B в СОК с последующим сложением компонент типа $\alpha_i \beta_i (\mathrm{mod}\ m_i) + \alpha_j \beta_j (\mathrm{mod}\ m_j)$.

Для рассмотрения метода реализации арифметических операций в СОК достаточно рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i = const , т. е. для конкретной приведенной системы вычетов по модулю m_i.

Пусть для заданной операции модульного сложения $(\alpha_i + \beta_i) \mathrm{mod}\ m_i$ в поле $GF(m_i)$ 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 позволяет реализовать операции модульного сложения и вычитания в СОК путем применения ПКС посредством n кольцевых $M = m_i([\log_2(m_i - 1)] + 1)$ - разрядных сдвигающих регистров (КСР).

Пусть произвольная алгебраическая система представлена в виде $S = \langle G, \otimes \rangle$, где G - непустое множество; $\otimes$ - тип операции, определенной для любых двух элементов α_i, $\beta_i \in G$. Операция $\oplus$ 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,.... Если основание СОК m_i – простое число, то Z/m_i - поле. Данное обстоятельство, как указывалось выше, и обусловливает возможность реализации арифметической операции сложения в СОК без межразрядных переносов путем кольцевого сдвига (посредством применения КСР).

На основе предложенного в [7] принципа разработан метод реализации арифметических операций в СОК (метод двоичного кодирования). Суть разработанного метода состоит в том, что исходная цифровая структура для каждого модуля (основания) СОК представляется в виде содержимого первой строки (столбца) таблицы модульного сложения (вычитания) $(\alpha_i \pm \beta_i) \mathrm{mod}\ m_i$ вида:

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

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 ; $k = \left[\log_2(m_i - 1) + 1\right]$. Для заданного модуля m_i=5 исходная цифровая структура содержимого КСР имеет вид:

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

Таким образом, посредством используемых в ПСС кольцевых регистров сдвига легко реализовать арифметические операции в СОК. При этом степени циклических перестановок, исходя из (1), определяются следующими выражениями:

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

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-1}(\alpha_{m_i-1}) \right]^{-z} = \left[P_{m_i-1-z}(\alpha_{m_i-1-z}) \| .. \| P_{m_i-z}(\alpha_{m_i-z1}) \| \right.$$
$$\left. \| ... \| P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-z-2}(\alpha_{m_i-z-2}) \right] \qquad (3)$$

Отметим, что $\left[P_0(\alpha_0)\|P_1(\alpha_1)\|...\|P_{m_i-1}(\alpha_{m_i-1})\right]^{m_i} = \varepsilon$, т.е. при $z = m_i$ все элементы упорядоченного множества $\{P_j(\alpha_i)\}$ $(j = \overline{0, m_i - 1})$ остаются на исходном месте. При технической реализации данного метода первый операнд α_i определяет номер α_{α_i} разряда $P_{\alpha_i}(\alpha_{\alpha_i})$ с содержимым результата модульной операции по модулю m_i, а второй операнд β_i - число разрядов КРС ($\beta_i k$ -двоичных разрядов), на которые необходимо провести сдвиги исходного (1) содержимого КРС в соответствии с алгоритмами (2), (3). Основными недостатками предложенного в работе [7] метода реализации арифметических операций в СОК является сравнительно большое время его реализации, что снижает эффективность использования ПКС. Этот недостаток обусловлен тем, что структура $P_{исх}^{(m_i)}$ (1) представлена набором исходных остатков первой строки матрицы $(\alpha_i + \beta_i) \bmod m_i$, отображаемых двоичным кодом. В этом случае время реализации модульного сложения двух операндов $A = (\alpha_1, \alpha_2, ..., \alpha_{n-1}, \alpha_n)$ и $B = (\beta_1, \beta_2, ..., \beta_{n-1}, \beta_n)$ в СОК определяется выражением [8]:

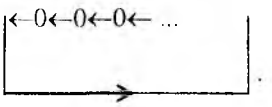
$$t_{сл} = k\beta_{max\ i}\tau, \tag{4}$$

где τ - время сдвига одного бита информации (одного двоичного разряда).

Рассмотрим метод реализации арифметических операций в СОК. Для метода унитарного кодирования, информационная структура $P_{исх}^{(m_i)}$ произвольного модуля m_i СОК, представляется в виде унитарного (m_i-1)-разрядного кода:

$$P_{исх}^{(m_i)} = \left[P(\alpha_{i-1})\|P(\alpha_{i-2})\|...\|P(1)\|P(0)\right], \tag{5}$$

где $P(\alpha_j)$ - двоичный разряд цифровой структуры (5), единичное состояние которого соответствует значению операнда $\alpha_i = \alpha_j$, представленного унитарным кодом $(\alpha_j = \overline{0, m_i - 1})$. В этом случае исходное состояние КРС состоит из m_i-1 двоичных разрядов и схематически может быть представлено в виде



При этом первый операнд $\alpha_i = \alpha_j$, отображаемый унитарным кодом по произвольному модулю m_i СОК. заносится в j-й разряд КРС, т.е переводит j-й двоичный разряд в единичное состояние. Второй операнд β_i указывает на число сдвигов z содержимого КРС, определяя время реализации арифметических операций по модулю m_i СОК, т. е.

$$t_{сл} = \beta_i\tau. \tag{6}$$

Отметим, что время реализации арифметической операции A + B в СОК будет определяться временем выполнения операции для максимального значения $(\beta_{max\ i}$ $(i = \overline{1, n})$ остатка из совокупности $\{\beta_i\}$ для данного операнда $B = (\beta_1, \beta_2, ..., \beta_n)$:

$t_{сл} = \beta_{max\ i}\tau$.(7)

Анализ выражений (4 и 7) показывает, что разработанный метод унитарного представления сокращает в $k = \left[\log_2(m_i - 1) + 1\right]$ раз время выполнения арифметических операций по сравнению с методом двоичного кодирования.

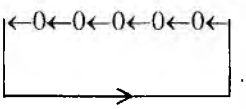
Алгоритм реализации арифметических операций в СОК посредством разработанного метода проиллюстрируем на примере операции сложения A + B для СОК, заданной основанием m_1=2, m_2=3, m_3=5. Пусть A = (0, 10, 100) и B = (1, 01, 010) (см. табл. 3). Так как $\beta_{max\ i} = \beta_3 = 010$, в соответст-

вии с выражением (7) $t_{сл} = \beta_3 \tau$ и алгоритм реализации операции сложения полностью определяется алгоритмом реализации модульного сложения $(\alpha_3 + \beta_3) \bmod m_3$.

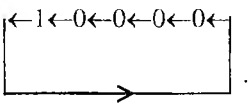
Таблица 3

A в ПСС	A в СОК при			A в ПСС	A в СОК при		
	m_1=2	m_2=3	m_3=5		m_1=2	m_2=3	m_3=5
0	0	00	000	15	1	00	000
1	1	01	001	16	0	01	001
2	0	10	010	17	1	10	010
3	1	00	011	18	0	00	011
4	0	01	100	19	1	01	100
5	1	10	000	20	0	10	000
6	0	00	001	21	1	00	001
7	1	01	010	22	0	01	010
8	0	10	011	23	1	10	011
9	1	00	100	24	0	00	100
10	0	01	000	25	1	01	000
11	1	10	001	26	0	10	001
12	0	00	010	27	1	00	010
13	1	01	011	28	0	01	011
14	0	10	100	29	1	10	100

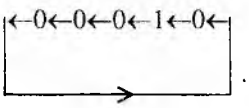
Исходное содержание КРС определяется в виде:



Первый операнд $\alpha_3 = 100$ дешифруется, и значение $\alpha_3 = 4$ в унитарном коде заносится в четвертый разряд КРС, содержание которого принимает вид:



Второй операнд $\beta_3 = 010$ также дешифруется, и полученное значение $\beta_3 = 2$ определяет число z сдвигов в положительном (против часовой стрелки) направлении содержимого КРС. В результате содержимое КРС представим следующим образом:



В соответствии с данными значениями кодов (табл. 4), посредством шифратора, по значению 00010 однозначно определяется результат операции $\alpha_3 + \beta_3$. Аналогично проводятся операции модульного сложения остатков по основаниям m_1 и m_2.

Таблица 4

Код	
входа шифратора	выхода шифратора
00001	000
00010	001
00100	010
01000	011

Проведем сравнительную оценку времени реализации арифметических операций в СОК и ПСС. Известно [9], что время реализации арифметических операций сложения и умножения в ПСС для l-байтовых $l = \overline{(1,4)}$ машинных слов определяется следующими выражениями:

$$t_{сл}^{(2)} = \tau(2\rho + 1), \qquad (8)$$

$$t_{умн}^{(2)} = \tau\rho^2, \quad (9)$$

где $\rho = 8 \cdot l$. А возможное и максимальное время реализации соответствующих арифметических операций для ПКС при применении метода двоичного представления – выражениями:

$$t_{сл}^{(2)} = (m_n - 1)k\tau, \quad (10)$$

$$t_{умн}^{(2)} = (m_n - 1)m_n k\tau/2. \quad (11)$$

Из выражений (6) и (7) видно, что максимально возможное время при использовании метода унитарного кодирования равно:

$$t_{сл}^{(2)} = (m_n - 1)\tau, \quad (12)$$

а для умножения в СОК:

$$t_{умн}^{(2)} = (m_n - 1)(m_n - 2)\tau, \quad (13)$$

так как $t_{умн}^{(3)} = \alpha_i(\beta_i - 1)\tau$, т. е. операнд α_i в унитарном коде заносится в КРС, а затем последовательно проводится сложение по схеме $\underbrace{\alpha_i + \alpha_i + \alpha_i + ... + \alpha_i}_{\beta_i}$.

Расчет (табл. 5), проведенный в соответствии с выражениями (8) - (13), показал высокую эффективность применения метода унитарного кодирования с точки зрения времени реализации арифметических операций в СОК по сравнению с методом двоичного кодирования и временем реализации таких же операций в ПСС.

Таблица 5

Разрядная сетка ЭВМ $l(m_n)$	Основания СОК $m_i\ (i=\overline{1,n})$	t[τ]					
		ПСС		СОК			
		Сложение	Умножение	Двоичное представление		Унитарное представление	
				Сложение	Умножение	Сложение	Умножение
l=1(m_n=7)	3,4,5,7	17	128	18	63	6	30
l=2(m_n=13)	2,5,7,9,11,13	33	512	48	312	12	132
l=3(m_n=19)	3,4,5,7,11,13,`7,19	49	1152	90	855	18	306
l=4(m_n=29)	2,3,5,7,11,13,17,19,23,29	65	2048	140	2030	28	756

Таким образом, полученные результаты могут быть использованы при оценке вычислительной сложности алгоритмов цифровой обработки информации, основанных на использовании преобразования Фурье.

Список литературы: 1. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. М.: 1968. 440 с. **2.** *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. М.: Мир, 1989. 448 с. **3.** *Кравченко В.Ф., Крот А.М.* Методы и микроэлектронные средства цифровой фильтрации сигналов и изображений на основе теоретико-числовых преобразований // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1997. №6. С.3-31. **4.** *Червяков Н.И., Тынчеров К.Т., Велигоша А.В.* Высокоскоростная цифровая обработка сигналов с использованием непозиционной арифметики // Радиотехника. 1997. №10. С.23-27. **5.** *Лавриненко Д.И.* Применение быстрого преобразования Фурье в криптографических преобразователях// Радиотехника. 2000. Вып. 114. С.75-79. **6.** *Краснобаев В.А.* Основы создания вычислителей на основе остаточных классов // Системи обробки інформації. Харків:НАНУ, ПАНМ, ХВУ. 2001. Вип. 1(11). С.3-7. **7.** *Краснобаев В.А.* Принцип реализации арифметических операций в системе остаточных классов// АСУ и приборы автоматики. 1988. Вып.86. С. 82-85. **8.** *Долгов В.И., Краснобаев В.А., Кононова И.В.* Метод и алгоритмы реализации арифметических операций в системе остаточных классов // Электрон. моделирование. 1990. №5. С.70-72. **9.** *Краснобаев В.А., Ирхин В.П.* Алгоритмы реализации операции модульного умножения в системе остаточных классов // Электрон. моделирование. 1993. №5. С.20-26.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 17.04.2001