НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА СИСТЕМНОГО АНАЛІЗУ

В.А. КРАСНОБАЕВ, С.А. КОШМАН

УДК 681.04

МЕТОД РЕАЛИЗАЦИИ АРИФМЕТИЧЕСКОЙ ОПЕРАЦИИ СЛОЖЕНИЯ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПРИНЦИПА КОЛЬЦЕВОГО СДВИГА

Аннотация. Рассмотрен метод реализации арифметической операции сложения в системе остаточных классов (СОК). Метод основан на использовании принципа кольцевого сдвига (ПКС). Особенность данного метода состоит в том, что результат реализации операции сложения чисел можно определить путем последовательных циклических сдвигов двоичных разрядов информационного содержимого блоков данных по соответствующим модулям СОК. Использование ПКС позволяет исключить влияние межразрядных связей между слагаемыми, что способствует повышению быстродействия выполнения операции сложения двух чисел в СОК.

Ключевые слова: система счисления, система остаточных классов, кольцевой регистр сдвига, быстродействие реализации арифметических операций, достоверность вычислений, компьютерные системы и компоненты.

ВВЕДЕНИЕ

В позиционной двоичной системе счисления (ПДСС) выполнение арифметической операции сложения предполагает последовательную обработку разрядов чисел по правилам, определяемым содержанием данной операции [1–3]. Обработка операций продолжается до тех пор, пока ни будут последовательно определены значения всех промежуточных результатов (от младших разрядов числа к старшим) с учетом всех логических связей между двоичными разрядами слагаемых. Таким образом, ПДСС, в которой представляются и обрабатываются данные в современных компьютерных системах и компонентах (КСК), обладает существенным недостатком — наличием межразрядных связей между двоичными разрядами слагаемых, что влияет на быстродействие и достоверность вычислений КСК. Поэтому естественно изыскание возможностей создания и использования такой машинной арифметики, применяемой в КСК, в которой поразрядные логические связи между обрабатываемыми двоичными разрядами слагаемых были бы ослаблены либо вообще отсутствовали. В этом аспекте обращает на себя внимание непозиционная система счисления в остаточных кассах (СОК) [4–6].

ПОСТАНОВКА ЗАДАЧИ

Метод представления целых чисел в СОК вмещает три основных свойства непозиционных кодовых структур (НКС): независимость, равноправность и малоразрядность остатков, совокупность которых определяет НКС в СОК. Использова-

ние этих свойств открывает широкие возможности в построении не только новой машинной арифметики и методов реализации модульных арифметических операций, но и принципиально новой схемной реализации КСК в СОК [7–9].

Реализация арифметической операции сложения двух чисел $A=(a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B=(b_1, b_2, \ldots, b_i, \ldots, b_n)$ в СОК осуществляется сложением соответствующих остатков a_i и b_i по основаниям (модулям) m_i $(i=\overline{1, n})$ независимо по каждому из n оснований. Малоразрядность остатков a_i и b_i в представлении слагаемых чисел $A=(a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B=(b_1, b_2, \ldots, b_i, \ldots, b_n)$ дает возможность осуществить модульную операцию сложения $(a_i+b_i) \bmod m_i$ на основе использования малоразрядных сумматоров по модулю. В этом случае время выполнения операции сложения чисел $A=(a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B=(b_1, b_2, \ldots, b_i, \ldots, b_n)$ определяется временем, необходимым для получения результата операции $(a_n+b_n) \bmod m_n$ по наибольшему m_n основанию упорядоченной СОК ($a_i < a_{i+1}$, где $i=\overline{1, n}$). Отметим основные недостатки сумматорного варианта реализации модульной арифметической операций $(a_i+b_i) \bmod m_i$ сложения в СОК.

1. Сложность синтеза двоичных k_i-разрядных сумматоров ($k_i=[\log_2(m_i-1)]+1$) по модулю m_i.

2. Значительные временные затраты, используемые при сложении $(a_n+b_n) \bmod m_n$ для больших разрядных сеток КСК, определяемые в СОК значением m_n — наибольшим из оснований.

3. Низкая достоверность вычислений $(a_i+b_i) \bmod m_i$ ввиду возможных ошибок, возникающих в процессе определения величин $S_i=(a_i \oplus b_i) \bmod 2 \vee c_{i-1}$ сумм в одноразрядных двоичных позиционных сумматорах; за счет возможных ошибок, возникающих в процессе формирования значений $C_{i+1}=a_{i+1} \wedge b_{i+1} \vee \vee (a_{i+1} \vee b_{i+1}) \wedge c_i$ переносов между одноразрядными двоичными сумматорами, от младшего разряда числа к старшему разряду, совокупность которых составляет k_i-разрядный двоичный сумматор по модулю m_i ($k_i=[\log_2(m_i-1)]+1$), а также за счет возможного искажения значения C_{i+1} переносов при осуществлении процесса переносов промежуточных значений поразрядного суммирования $(a_i+b_i) \bmod m_i$ в пределах данного остатка по основанию m_i СОК [2, 9].

МЕТОД РЕАЛИЗАЦИИ АРИФМЕТИЧЕСКОЙ ОПЕРАЦИИ СЛОЖЕНИЯ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

В [10] сформулирован принцип технической реализации целочисленных арифметических операций по модулю m_i — принцип кольцевого сдвига (ПКС). Особенность методов реализации арифметических операций, основанных на использовании ПКС, состоит в том, что результат, например, модульной операции сложения чисел можно определить путем последовательных циклических сдвигов двоичных разрядов информационного содержимого блока данных.

Как было отмечено, ПКС можно использовать при реализации арифметической операции сложения чисел $A=(a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B=(b_1, b_2, \ldots, b_i, \ldots, b_n)$ в СОК. В этом случае результат арифметической операции сложения в СОК определяется совокупностью остатков $(a_i+b_i) \bmod m_i$ по произвольному модулю m_i СОК, которая задана набором $\{m_i\}$ $(i=\overline{1, n})$ оснований. Результат операции в остатке по модулю m_i СОК в схеме сложения $(a_i+b_i) \bmod m_i$ определяется только за счет циклических сдвигов информационного содержимого разрядов регистра (сдвигающего регистра) кольцевого сдвига (РКС). В этом случае отсутствует необходимость (которая существует в ПДСС) определения величин $S_i=(a_i \oplus b_i) \bmod 2 \vee c_{i-1}$ и $C_{i+1}=a_{i+1} \wedge b_{i+1} \vee \vee (a_{i+1} \vee b_{i+1}) \wedge c_i$. Это дает возможность повысить быстродействие реализации арифметической операции сложения чисел $A=(a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B=(b_1, b_2, \ldots, b_i, \ldots, b_n)$ в СОК, а также повысить достоверность реализации этой операции.

Пусть $G_1 = (Z, \{+\})$ — аддитивная абелева группа целых чисел и $G_2 = (Z_{m_i}, \oplus)$ — аддитивная абелева группа вычетов целых чисел по модулю m_i. Зададим отображение F аддитивной абелевой группы целых чисел G_1 на аддитивную абелевую группу вычетов целых чисел G_2 по модулю m_i. Для любого целого числа A образ $F(A)$ равен остатку $a_i \equiv A(\mathrm{mod}\, m_i)$ от деления числа A на модуль m_i СОК. Легко проверить, что для любых целых чисел (слагаемых) A и B имеет место следующее равенство:

$$F(A+B) = F(A) + F(B),$$

т.е. для целых чисел остаток $(A+B) \bmod m_i$ от деления суммы чисел $A+B$ на модуль m_i равен сумме по модулю m_i остатков $a_i \equiv A(\mathrm{mod}\, m_i)$ и $b_i \equiv B(\mathrm{mod}\, m_i)$ от деления на модуль m_i каждого слагаемого A и B. Следовательно, данное отображение F аддитивной абелевой группы целых чисел G_1 на аддитивную абелевую группу вычетов целых чисел по модулю m_i есть гомоморфизм.

Исходя из этого можно организовать процесс определения результата арифметической модульной операции сложения $(a_i + b_i) \bmod m_i$ посредством использования ПКС. Так, число в СОК представляется набором из n остатков $\{a_i\}$, образованных путем последовательного деления исходного числа A на n попарно простых чисел (модулей) $\{m_i\}$, для $i = \overline{1, n}$ [1, 3]. Так, из числа, заданных n различных натуральных чисел m_1, m_2, …, m_n (модули СОК), попарно простыми числами называются те из них, для которых наибольший общий делитель (НОД) любых двух разных чисел равен единице, т.е. НОД $(m_i, m_j) = 1$ при $i \neq j$.

Отметим некоторые важные свойства данных в таблице Кэли (табл. 1). Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в таблице Кэли для реализации сложения $(a_i + b_i) \bmod m_i$ есть строка, в которой элементы данного поля стоят в порядке возрастания. 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 только единожды. Согласно таблице Кэли необходимая строка таблицы $(a_i + b_i) \bmod m_i$ модульного сложения может быть получена путем последовательного циклического сдвига элементов первой строки. Системотехнической основой для синтеза средств (устройств) реализации метода арифметической операции в СОК на основе ПКС могут применяться часто используемые в ПДСС регистры кольцевого сдвига.

При изложении метода реализации арифметической операции сложения чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК достаточно рассмотреть вариант для конкретной приведенной системы вычетов по модулю m_i (множество всех чисел полной системы вычетов по модулю m_i, взаимно простых с m_i). Пусть для заданной операции модульного сложения $(a_i + b_i) \bmod m_i$ составлена таблица Кэли (см. табл. 1). Для значения модуля $m_i = 5$ таблица Кэли представлена в табл. 2.

Таблица 1

Значение β	**Результаты расчетов операции модульного сложения** $(a_i + b_i) \bmod m_i$				
	$\alpha = 0$	$\alpha = 1$	$\alpha = 2$	…	$\alpha = m_i - 1$
$\beta = 0$	0	1	2	…	$m_i - 1$
$\beta = 1$	1	2	3	…	0
$\beta = 2$	2	3	4	…	1
…	…	…	…	…	…
$\beta = m_i - 1$	$m_i - 1$	0	1	…	$m_i - 2$

Таблица 2

Значение β	Результаты расчетов операции сложения по модулю $m_i = 5$				
	$\alpha = 0$	$\alpha = 1$	$\alpha = 2$	$\alpha = 3$	$\alpha = 4$
$\beta = 0$	0	1	2	3	4
$\beta = 1$	1	2	3	4	0
$\beta = 2$	2	3	4	0	1
$\beta = 3$	3	4	0	1	2
$\beta = 4$	4	0	1	2	3

Перечисленные свойства таблицы Кэли позволяют реализовать операцию модульного сложения чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК путем использования ПКС в схеме сложения $(a_i + b_i) \bmod m_i$ для каждого из n остатков a_i числа $A = (a_1, a_2, ..., a_i, ..., a_n)$. Для каждого остатка a_i из числа n формируется m_i разрядов (от нулевого разряда до $(m_i$-1)-го разряда) РКС. Количество двоичных разрядов каждого разряда РКС равна $[\log_2 (m_i - 1)] + 1$.

Представленный в статье метод реализации арифметической операции сложения чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК на основе использования ПКС состоит в следующем.

1. По числу n остатков чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в n схемах сложения $(a_i + b_i) \bmod m_i$ $(i = \overline{1, n})$ устанавливается исходное состояние каждого разряда РКС. Для этого в соответствующие разряды РКС (от нулевого до $(m_i - 1)$-го двоичного разряда) заносятся значения первой строки табл. 1 модульного сложения $(a_i + b_i) \bmod m_i$ в двоичном коде.

2. По значению a_i — первого слагаемого суммы $(a_i + b_i) \bmod m_i$ числа $A = (a_1, a_2, ..., a_i, ..., a_n)$ определяется номер разряда исходного информационного содержимого РКС, который и будет представлять результат модульной операции $(a_i + b_i) \bmod m_i$ в i-м остатке СОК.

3. По значению b_i — второго слагаемого суммы $(a_i + b_i) \bmod m_i$ числа $B = (b_1, b_2, ..., b_i, ..., b_n)$ путем b_i сдвигов исходного содержимого каждого разряда РКС в положительном (против часовой стрелки) направлении устанавливается окончательное информационное содержимое РКС.

4. Полученное информационное содержимое разрядов (от нулевого до $(m_i - 1)$-го двоичного разряда) всех n РКС определяет результат операции сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК. Результат сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ определяется как совокупность из n значений сумм остатков $(a_i + b_i) \bmod m_i$ $(i = \overline{1, n})$, полученных в соответствующих разрядах РКС (см. п. 2).

В общем случае для произвольного основания m_i СОК исходная цифровая структура разрядов РКС определяется в виде содержимого первой строки таблицы модульного сложения $(a_i + b_i) \bmod m_i$ (см. табл. 1) и может быть представлена в следующем виде:

$$P_{\text{исх}}^{(m_i)} = [P_0(a_0) \,\|\, P_1(a_1) \| \ldots \| P_v(a_v) \| \ldots \| P_{m_i - 1}(a_{m_i - 1})], \qquad (1)$$

где $\|$ — операция конкатенации (присоединения, склеивания); $P_v(a_v)$ — v-й $(v = \overline{0, m_i - 1})$ разряд РКС; a_v — информационное содержимое v-го разряда РКС, представленное k-разрядным двоичным кодом $(k = [\log_2 (m_i - 1) + 1])$, который соответствует возможному значению a_v-го остатка $(a_v = \overline{0, m_i - 1})$ в двоичном коде числа по модулю m_i.

В общем виде для модуля $m_i = 5$ исходная цифровая структура содержимого разрядов $P_\upsilon(a_\upsilon)$ ($\upsilon = \overline{0,4}$) РКС имеет вид (см. табл. 2)

$$P_{\text{исх}}^{(5)} = [P_0(a_0) \| P_1(a_1) \| P_2(a_2) \| P_3(a_3) \| P_4(a_4)]$$

или

$$P_{\text{исх}}^{(5)} = [000 \| 001 \| 010 \| 011 \| 100]. \quad (2)$$

Таким образом, посредством широко используемых в ПДСС регистров кольцевого сдвига (в частности, в криптографии [11–13]) легко реализовать арифметическую операцию сложения чисел в СОК. При этом степень Z циклических перестановок (сдвигов) исходя из (1) определяется следующим выражением:

$$[P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1})]^{(Z)} =$$

$$= [P_z(a_z) \| P_{z+1}(a_{z+1}) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \| \ldots \| P_{z-1}(a_{z-1})]. \quad (3)$$

При технической реализации предложенного метода первое из a_i слагаемое определяет номер разряда РКС, содержимое которого является результатом операции $(a_i + b_i) \bmod m_i$. Второе из b_i слагаемое определяет число Z разрядов РКС ($b_i \cdot k_i$ двоичных разрядов), на которое необходимо сдвинуть исходное (1) содержимое РКС в соответствии с выражением (3).

Для сравнительного анализа времени реализации целочисленной арифметической операции сложения в ПДСС и в СОК рассчитаем время выполнения операции сложения двух чисел $A = (a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_i, \ldots, b_n)$ в СОК с использованием ПКС. Для ПКС в схеме определения значения $(a_i + b_i) \bmod m_i$ ($i = \overline{1, n}$) время t модульного сложения двух остатков a_i и b_i определяется в основном временем $t_{\text{с}}$ сдвига исходного содержимого разрядов РКС (в дальнейшем полагаем $t \approx t_{\text{с}}$).

Время сдвига цифрового содержимого разрядов РКС определяется выражением

$$t_{\text{с}} = Z \cdot k_i \cdot \tau, \quad (4)$$

где Z — количество сдвигаемых разрядов КСР; $k_i = [\log_2(m_i - 1)] + 1$ — количество двоичных разрядов в одном разряде РКС схемы определения остатка $(a_i + b_i) \bmod m_i$; $\tau = 3 \cdot \tau_{\text{в}}$ — время сдвига одного двоичного разряда (время срабатывания одного триггера); $\tau_{\text{в}}$ — время срабатывания одного логического вентиля (элемента И, НЕ, ИЛИ).

Учитывая вышеизложенное, а также что $t \approx t_{\text{с}}$, время t модульного сложения $(a_i + b_i) \bmod m_i$ двух остатков a_i и b_i определяется следующим образом:

$$t = 3 \cdot b_i \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_{\text{в}}. \quad (5)$$

Поскольку $b_i = \overline{0, m_i - 1}$, то максимально возможное значение t для произвольного модуля m_i СОК ($b_i = m_i - 1 = \max$) определяется как

$$t = 3 \cdot (m_i - 1) \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_{\text{в}}, \quad (6)$$

а минимальное время t равно нулю ($b_i = 0$). Очевидно, что время t модульного сложения $(a_i + b_i) \bmod m_i$ двух остатков a_i и b_i при использовании ПКС зависит от величины b_i.

Очевидно, что время $T_{\text{СОК}}^{(+)}$ сложения двух чисел $A = (a_1, a_2, \ldots, a_i, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_i, \ldots, b_n)$ в СОК на основе использования ПКС определяется временем t реализации модульной операции $(a_i + b_i) \bmod m_i$, для которой выполняется условие

$$b_i \cdot k_i = \max \quad (7)$$

из всех возможных значений парных произведений $b_j \cdot k_j$ ($j = \overline{1, n};\ i \neq j$). Условие (7) лежит в основе определения времени $T^{(+)}_{\text{СОК}}$ реализации операции сложения двух чисел: $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК.

ПРИМЕРЫ ВЫПОЛНЕНИЯ ОПЕРАЦИИ СЛОЖЕНИЯ ДВУХ ЧИСЕЛ В СОК

Рассмотрим примеры конкретного выполнения операции сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК для однобайтового ($l = 1$) сумматора. Пусть значение $\rho = 8 \cdot l$ — величина в двоичных разрядах обрабатываемых в позиционном сумматоре *l*-байтовых машинных слов (разрядная сетка сумматора). В ПДСС для $l = 1$ ($\rho = 8 \cdot l = 8 \cdot 1 = 8$ двоичных разрядов) основания СОК могут определяться следующими значениями: $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$.

Пример 1. Пусть имеем второе слагаемое $B = (10 \| 10 \| 100 \| 001)$. Тогда:

— для $m_1 = 3$ имеем $b_1 = 2(10),\ k_1 = [\log(m_1 - 1)] + 1 = 2;\ b_1 \cdot k_1 = 2 \cdot 2 = 4;$

— для $m_2 = 4$ имеем $b_2 = 2(10),\ k_2 = [\log(m_2 - 1)] + 1 = 2;\ b_2 \cdot k_2 = 2 \cdot 2 = 4;$

— для $m_3 = 5$ имеем $b_3 = 4(100),\ k_3 = [\log(m_3 - 1)] + 1 = 3;\ b_3 \cdot k_3 = 4 \cdot 3 = 12;$

— для $m_4 = 7$ имеем $b_4 = 1(001),\ k_4 = [\log(m_4 - 1)] + 1 = 3;\ b_4 \cdot k_4 = 1 \cdot 3 = 3.$

Как видно, наибольшее количество, т.е. 12, сдвигаемых двоичных разрядов выполняется в схеме сложения $(a_3 + b_3) \bmod m_3$ по модулю $m_3 = 5$.

Таким образом, для примера 1 время сложения двух чисел A и B в СОК на основе ПКС определяется величиной

$$T^{(+)}_{\text{СОК}} = b_3 \cdot k_3 \cdot 3 \cdot \tau_{\text{в}} = 4 \cdot 3 \cdot 3 \cdot \tau_{\text{в}} = 36 \cdot \tau_{\text{в}}.$$

Пример 2. Пусть имеем второе слагаемое $B = (10, 11, 001, 001)$. Тогда

— для $m_1 = 3$ имеем $b_1 = 2(10),\ k_1 = [\log(m_1 - 1)] + 1 = 2;\ b_1 \cdot k_1 = 2 \cdot 2 = 4;$

— для $m_2 = 4$ имеем $b_2 = 3(11),\ k_2 = [\log(m_2 - 1)] + 1 = 2;\ b_2 \cdot k_2 = 3 \cdot 2 = 6;$

— для $m_3 = 5$ имеем $b_3 = 1(001),\ k_3 = [\log(m_3 - 1)] + 1 = 3;\ b_3 \cdot k_3 = 1 \cdot 3 = 3;$

— для $m_4 = 7$ имеем $b_4 = 1(001),\ k_4 = [\log(m_4 - 1)] + 1 = 3;\ b_4 \cdot k_4 = 1 \cdot 3 = 3.$

Как видно, наибольшее количество (т.е. 6) сдвигаемых двоичных разрядов выполняется в схеме сложения $(a_2 + b_2) \bmod m_2$ по модулю $m_2 = 4$. Время сложения двух чисел A и B в СОК на основе ПКС определяется величиной

$$T^{(+)}_{\text{СОК}} = b_2 \cdot k_2 \cdot 3 \cdot \tau_{\text{в}} = 3 \cdot 2 \cdot 3 \cdot \tau_{\text{в}} = 18 \cdot \tau_{\text{в}}.$$

Особенность использования в СОК ПКС заключается в том, что время выполнения операции сложения зависит от величины второго b_i слагаемого суммы $(a_i + b_i) \bmod m_i$ и может быть различным. Время $T^{(+)}_{\text{СОК}}$ сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК можно характеризовать как максимальным $T^{(+)}_{\text{СОКМАКС}}$ временем, так и возможным средним $T^{(+)}_{\text{СОКСРЕД}}$ временем сложения. Далее время сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК будет определяться выражением $T^{(+)}_{\text{СОКМАКС}}$. Исходя из выражения (6) максимальное время сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК определится как

$$T^{(+)}_{\text{СОКМАКС}} = 3 \cdot (m_n - 1) \cdot \{[\log_2 (m_n - 1)] + 1\} \cdot \tau_{\text{в}}. \qquad (8)$$

Отметим, что существуют алгоритмы, которые позволили синтезировать ряд технических решений (устройств) для реализации целочисленной модульной арифметической операции сложения на основе использования ПКС. При этом

Таблица 3

Величина l разрядной сетки компьютерной системы	Совокупность оснований системы остаточных классов	Максимальное m_n основание СОК	Разрядность максимального m_n основания СОК	Относительное T^+ время сложения		Выигрыш во времени, %
				ПДСС	СОК	
Однобайтовая ($l = 1$) разрядная сетка ($\rho = 8$)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$	$m_4 = 7$	$k_4 = 3$	15	9	40
Двухбайтовая ($l = 2$) разрядная сетка ($\rho = 16$)	$m_1 = 2$, $m_2 = 5$, $m_3 = 7$, $m_4 = 9$, $m_5 = 11$, $m_6 = 13$	$m_6 = 13$	$k_6 = 4$	31	24	22

максимальное время $T^{(+)}_{\text{СОКМАКС}}$ выполнения операции сложения гарантировано уменьшается как минимум в два раза [14]. В этом случае время $T^{(+)}_{\text{СОК}}$ сложения двух чисел $A = (a_1, a_2, ..., a_i, ..., a_n)$ и $B = (b_1, b_2, ..., b_i, ..., b_n)$ в СОК определится выражением $T^{(+)}_{\text{СОК}} = T^{(+)}_{\text{СОКМАКС}}/2$. Тогда время сложения двух чисел в СОК определится как

$$T^{(+)}_{\text{СОК}} = 3 \cdot (m_n - 1) \cdot \{[\log_2 (m_n - 1)] + 1\} \cdot \tau_{\text{в}} / 2. \qquad (9)$$

Известно [9], что время $T^{(+)}_{\text{ПСС}}$ сложения чисел A и B в ПСС определяется по формуле

$$T^{(+)}_{\text{ПСС}} = (2 \cdot \rho - 1)\, t_{\text{с}} = (16 \cdot l - 1) \cdot 3 \cdot \tau_{\text{в}}, \qquad (10)$$

где $\rho = 8 \cdot l$ — разрядная сетка позиционного сумматора; $t_{\text{с}} = 3 \cdot \tau_{\text{в}}$ — время суммирования в $(i+1)$-м двоичном разряде позиционного сумматора значений $a_{i+1} + b_{i+1} + c_i$, т.е. время определения значений C_{i+1} и S_{i+1}.

Проведем оценочный расчет и сравнительный анализ времени выполнения арифметической операции сложения двух чисел в ПДСС и в СОК для однобайтового ($l = 1$) и двухбайтового ($l = 2$) машинных слов. Для $l = 1$ ($\rho = 8$ двоичных разрядов) СОК представляется набором следующих оснований: $m_1 = 3$, $m_2 = 4$, $m_4 = 5$, $m_4 = 7$, а для $l = 2$ ($\rho = 16$ двоичных разрядов) СОК представляется набором оснований $m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 7$, $m_5 = 11, m_6 = 13$. При расчетах используем формулы (8)–(10). Результаты расчетов сравнительного анализа времени $T^{(+)}$ реализации операции сложения чисел в СОК представлены в табл. 3.

Сравнительный анализ результатов расчетов показал эффективность использования ПКС при реализации арифметической операции сложения в СОК.

ЗАКЛЮЧЕНИЕ

Модульность структуры вычислительного процесса в СОК дает возможность использовать ПКС для реализации основных модульных целочисленных арифметических операций. На основании этого в настоящей статье разработан метод реализации арифметической операции сложения в системе остаточных классов на основе использования принципа кольцевого сдвига. Использование ПКС в СОК позволяет устранить основной недостаток существующих КСК, функционирующих в ПДСС, а именно избавиться от влияния межразрядных связей между двоичными разрядами чисел a_i и b_i при выполнении операции сложения $(a_i + b_i) \bmod m_i$, т.е. исключить влияние межразрядных связей между одноразрядными позиционными сумматорами на результат операции сло-

жения $A+B$ двух чисел. В статье показано, что применение ПКС позволяет повысить быстродействие выполнения операции сложения $A+B$ двух чисел.

Использование ПКС может повысить достоверность вычислений (т.е. выполнения операции модульного сложения в СОК) за счет исключения из процесса реализации арифметической операции сложения $(a_i + b_i) \bmod m_i$ возможных ошибок, которые могут иметь место при определении значений сумм S_i и значений C_i сигналов переносов. Достоверность вычислений может увеличиться также за счет исключения возможного влияния искаженного значения C_i сигнала переноса в процессе переноса этого сигнала от *i*-го к $(i+1)$-му одноразрядному позиционному двоичному сумматору. Однако утверждение о возможном повышении достоверности выполнения операции сложения в СОК за счет использования ПКС требует дополнительных исследований. Отметим, что системотехнической основой для синтеза средств (устройств) реализации метода арифметической операции сложения в СОК на основе ПКС могут быть широко используемые в ПДСС регистры сдвига.

СПИСОК ЛИТЕРАТУРЫ

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. Москва: Сов. радио, 1968. 440 с.
2. Краснобаев В.А. Методы повышения надежности специализированных ЭВМ систем и средств связи. Харьков: МО СССР, 1990. 172 с.
3. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации. Минск: Университетское, 1992. 256 с.
4. Филиппенко И.Г. Взаимодействующие нейроавтоматы и нейроавтоматно-вычислительные структуры. Под ред. Руденко О.Г. Киев: Каравелла, 2015. 440 с.
5. Krasnobayev V.A., Koshman S.A., Mavrina M.A. A method for increasing the reliability of verification of data represented in a residue number system. *Cybernetics and Systems Analysis*. 2014. Vol. 50, N 6. P. 969–976.
6. Krasnobayev V.A., Yanko A.S., Koshman S.A. A method for arithmetic comparison of data represented in a residue number system. *Cybernetics and Systems Analysis*. 2016. Vol. 52, N 1. P. 145–150.
7. Онищенко С.М. Применение гиперкомплексных чисел в теории инерциальной навигации. Автономные системы. Киев.: Наук. думка, 1983. 208 с.
8. Николайчук Я.Н., Возна Н.Я., Круликовский Б.Б., Пих В.Я. Метод структуризации дискретного косинусного преобразования Фурье в модульной арифметике теоретико-числового базиса Хаара–Крестенсона. *Кибернетика и системный анализ*. 2018. Т. 54, № 3. С. 178–188.
9. Малиновский Б.Н., Брюхович Е.И., Денисенко Е.Л. и др. Справочник по цифровой вычислительной технике (процессоры и память). Под ред. Малиновского Б.Н. Киев: Техніка, 1979. 366 с.
10. Краснобаев В.А. Принцип реализации арифметических операций в системе остаточных классов. *АСУ и приборы автоматики*. 1988. Вып. 86. С. 82–85.
11. Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties. *Cybernetics and Systems Analysis*. 2007. Vol. 43, N 1. P. 1–11.
12. Kuznetsov O., Lutsenko M., Ivanenko D. Strumok stream cipher: Specification and basic properties. *Third International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PICS&T)*. Kharkiv, 2016. P. 59–62.
13. Gorbenko I., Kuznetsov A., Lutsenko M., Ivanenko D. The research of modern stream ciphers. *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PICS&T)*. Kharkov, 2017. P. 207–210.
14. Andrushkevych A., Gorbenko Y., Kuznetsov O., Oliynykov R., Rodinko M. A prospective lightweight block cipher for green IT engineering. In: *Green IT Engineering: Social, Business and Industrial Applications.* Kharchenko V., Kondratenko Y., Kacprzyk J. (Eds.). Cham: Springer. 2018. Vol. 171. P. 95–112. DOI: https://doi.org/10.1007/978-3-030-00253-4_5.

Надійшла до редакції 19.10.2018

В.А. Краснобаєв, С.О. Кошман

МЕТОД РЕАЛІЗАЦІЇ АРИФМЕТИЧНОЇ ОПЕРАЦІЇ ДОДАВАННЯ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ НА ОСНОВІ ВИКОРИСТАННЯ ПРИНЦИПУ КІЛЬЦЕВОГО ЗСУВУ

Анотація. Розглянуто метод реалізації арифметичної операції додавання у системі залишкових класів (СЗК). Метод базується на використанні принципу кільцевого зсуву (ПКЗ). Особливість методу полягає у тому, що результат реалізації операції додавання чисел можна визначити шляхом послідовних циклічних зсувів двійкових розрядів інформаційного вмісту блоків даних за відповідними модулями СЗК. Використання ПКЗ дозволяє позбутися впливу міжрозрядних зв'язків між доданками, що підвищує швидкодію виконання операції додавання двох чисел у СЗК.

Ключові слова: система числення, система залишкових класів, кільцевий регістр зсуву, швидкодія реалізації арифметичних операцій, достовірність обчислень, комп'ютерні системи та компоненти.

V.A. Krasnobayev, S.A. Koshman

THE METHOD OF OPERATIONAL DATA DIAGNOSING REPRESENTED IN THE RESIDUE NUMBER SYSTEM

Abstract. The method of realization of the arithmetic operation of addition in the system of residual classes (SRC) is considered in the article. The method is based on the use of the principle of circular shift (PCS). The peculiarity of this method is that the result of the operation of adding the numbers can be determined by successive cyclic shifts of the bits of the information content of the data blocks by the corresponding modules of SRC. Using PCS allows you to get rid of the influence of inter-bit relationships between the terms, which allows you to increase the speed of the operation of adding two numbers to SRC.

Keywords: number system, residue number system, circular shift register, speed of implementation of arithmetic operations, reliability of calculations, computer systems and components.

Краснобаев Виктор Анатольевич,
доктор техн. наук, профессор кафедры Харьковского национального университета им. В.Н. Каразина, e-mail: v.a.krasnobaev@gmail.com.

Кошман Сергей Александрович,
кандидат техн. наук, доцент кафедры Харьковского национального университета им. В.Н. Каразина, e-mail: s_koshman@ukr.net.