УДК 621.391

В.А. Краснобаев[1], И.А. Чернецкая[1], С.А. Кошман[2], А.М. Мартыненко[1]

[1] *Полтавский национальный технический университет имени Ю. Кондратюка, Украина*
[2] *Харьковский национальный технический университет сельского хозяйства имени П. Василенко, Украина*

МЕТОД ОБРАБОТКИ ДАННЫХ В КЛАССЕ ВЫЧЕТОВ

В статье рассмотрен метод реализации операции сложения чисел в классе вычетов (КВ). Метод основан на использовании принципа кольцевого сдвига (ПКС). Приведены примеры реализации операции сложения чисел в КВ на основе ПКС.

Ключевые слова: *непозиционная система счисления класса вычетов, принцип кольцевого сдвига, арифметические целочисленные модульные операции.*

Введение

В настоящее время решение вычислительных научно-технических задач требует значительных объемов расчетов, проводимых в реальном времени функционирования системы обработки данных (СОД). В этом аспекте проводимые исследования поиска методов и средств повышения производительности переработки цифровой информации весьма важны и актуальны.

В СОД действия производятся над числами, представленными в виде специальных машинных кодов в принятой системе счисления. Под системой счисления (СС) понимается способ обозначения чисел с целью определения их количественного значения посредством символов, имеющих определенные количественные признаки. Символы, применяемые для изображения чисел, называются цифрами. В зависимости от способа изображения чисел, посредством цифр, существующие СС условно делят на позиционные и непозиционные системы счисления.

В любой позиционной системе счисления (ПСС) выполнение арифметических операций предполагает последовательную обработку разрядов операндов по правилам данной операции и она не может быть закончена до тех пор, пока не будут определены последовательно результаты всех предыдущих межразрядных операций с учетом всех связей между разрядами. Таким образом, ПСС, используемые в современных вычислительных системах, в которых представляется и обрабатывается информация, обладают существенным недостатком – наличием межразрядных связей между двоичными разрядами чисел, которые накладывают свой отпечаток на принципы и методы реализации арифметических операций [1, 2].

Исходя из вышеизложенного материала, можно сделать следующие основные выводы:

- недостатки вычислительных средств в ПСС – значительное время реализации арифметических операций и низкая достоверность функционирования операционных устройств. Это обусловлено «сильными» межразрядными связями;
- один из возможных путей решения этой проблемы – это привлечение новых, нестандартных и оригинальных идей в области создания машинной арифметики, например использование недвоичных ПСС и т.д., которые позволили бы ослабить либо вообще устранить все межразрядные связи. Один из эффективных путей ослабления либо устранения межразрядных связей – создание для СОД новой недвоичной машинной арифметики.

Результаты исследований показали, что одним из перспективных и действенных направлений повышения пользовательской производительности, надежности и достоверности вычислительных средств является разработка и внедрение новой машинной арифметики на основе использования теоретических положений некоторых разделов теории чисел (теория делимости, теория сравнения и пр.) [3]. Это так называемые модулярные системы счисления, в частности, непозиционная система счисления в классе вычетов (КВ). Модулярные СС обладают максимальным уровнем внутреннего параллелизма в организации процесса реализации целочисленных арифметических операций.

Класс вычетов, обладает ценным свойством независимости друг от друга остатков числа по принятой системе оснований. Это открывает широкие возможности создания не только новой машинной модулярной арифметики, но и принципиально новой схемной реализации архитектуры СОД, которая, в свою очередь, заметно расширяет применение машинной арифметики. Основными преимуществами КВ являются возможность разработки и внедрения высокоэффективных алгоритмических и аппаратных архитектур вычислительных структур параллельно-конвейерного типа. При этом обеспечивается, во-первых, высокая степень интеграции и унификации арифметических блоков и вычислительных узлов и, во-вторых, использования уникальных корректирующих свойств непозиционных кодовых структур при обнаружении и исправлении, а также при контроле ошибок в динамике вычислительного процесса, т.е. в реальном времени решения задачи без останова вычислений. И, наконец, использования свойств КВ позволяет организовать высокопроизводительную реализацию вычислительных процессов, требующих больших объемов вычислений в реальном времени.

В этом аспекте данное обстоятельство обуславливает важность и актуальность поисков методов повышения производительности, надежности и достоверности СОД на основе использования КВ.

В [1] рассмотрено влияние основных свойств КВ на структуру и принципы функционирования СОД. Кратко охарактеризуем основные свойства КВ.

1. Независимость остатков. Это свойство дает возможность построить СОД в виде набора независимых вычислительных трактов (BT_i) (отдельных самостоятельных процессоров, функционирующих по своему определенному модулю m_i). При этом время выполнения арифметической операции в КВ определяется максимальным временем реализации в вычислительном тракте СОД. Ошибки, возникающие за счет отказов (сбоев) схем двоичных разрядов в произвольном вычислительном тракте СОД, не «размножаются» в соседние тракты (остаются в пределах одного остатка), что дает возможность повысить достоверность вычислений в КВ.

2. Равноправность остатков. Любой остаток a_i числа $A = (a_1, a_2, \ldots, a_n)$ в КВ содержит информацию обо всем исходном числе. Использования этого свойства вместе с первым, а также используя методы структурного резервирования, можно синтезировать надежностную модель СОД в КВ, соответствующую модели динамического резервирования в ПСС. В этом случае информационные тракты $m_1 \ldots m_n$ СОД в КВ играют роль рабочих элементов, а тракты $m_{n+1} \ldots m_{n+k}$ – роль резервных элементов, где k – количество контрольных (резервных) оснований.

3. Малоразрядность остатков**.** Это свойство позволяет существенно повысить быстродействие выполнения арифметических операций за счет малоразрядности построения вычислительных трактов СОД в КВ (малоразрядности представления остатков числа).

Известно [2], что существует четыре принципа реализации арифметических операций в КВ: сумматорный принцип (СП) (на базе малоразрядных двоичных сумматоров); табличный принцип (ТП) (на основе использования ПЗУ); 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); принцип кольцевого сдвига (ПКС), основанный на использовании кольцевых регистров сдвига (КРС) (табл. 1).

Таблица 1

Методы реализации арифметических операций в КВ

№ п.п.	Наименование метода реализации арифметических операций в КВ	Суть метода	Время реализации арифметических операций в КВ
1	Двоичный метод	Метод основан на использовании n двоичных сумматоров по модулям m_i $(i = \overline{1, n})$.	Определяется время выполнения модульной операции $(a_n \oplus b_n) \bmod m_n$ по наибольшему m_n по величине модулю КВ.
2	Метод логических функций	Метод основан на использовании логических элементов И, ИЛИ и НЕ.	Зависит от длины последовательности выполняемых логических операций, а также от времени "срабатывания" логических элементов.
3	Табличный (матричный) метод	Метод основан на использовании n матричных ПЗУ по модулям m_i $(i = \overline{1, n})$.	Время выполнения арифметических операций не зависит от величин модулей КВ. Оно равно времени "срабатывания" двухвходового логического элемента И в узле ПЗУ.
4	Метод кольцевого сдвига данных	Метод основан на использовании n кольцевых регистров сдвига по модулям m_i $(i = \overline{1, n})$.	Время сложения и вычитания двух чисел в КВ определяется временем реализации модульной операции $(a_i \pm b_i) \bmod m_i$ для модуля m_i для которого выполняется условие $K_{1i} \cdot K_{2i} = \max$.

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

Цель данной статьи – разработка высокопроизводительного метода реализации целочисленных арифметических операций в КВ на основе использования принципа кольцевого сдвига (ПКС).

Основная часть

Согласно таблице Кэли для аддитивных операций нужная строка (столбец) таблицы модульного сложения или вычитания может быть получена путем последовательного циклического сдвига элементов первой строки (столбца). Системотехнической основой для реализации арифметических операций над целочисленными данными в КВ на основе ПКС является кольцевые регистры сдвига. В этом случае структурная схема ОУ СОД в КВ представляет собой n (по числу оснований) независимых и параллельно во времени функционирующих каналов (ВТ) обработки данных (рис. 1).

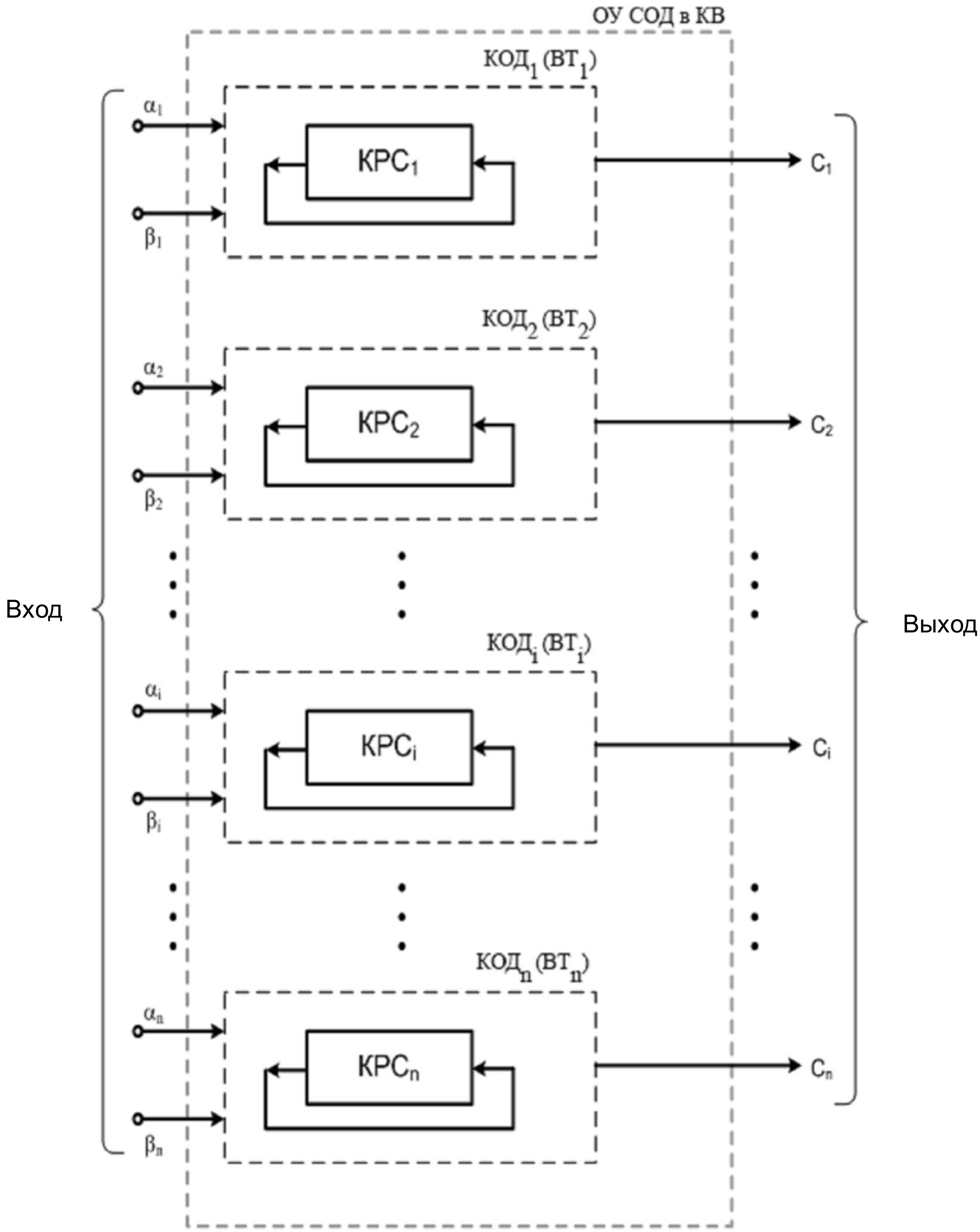

Рис. 1. Упрощенная структурная схема операционного устройства СОД в КВ

В [4] сформулирован принцип реализации целочисленных арифметических операций в МСС - ПКС, особенность которого заключается в том, что результат арифметической операции $(a_i \pm b_i) \bmod m_i$ по произвольному m_i модулю КВ, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется без процесса переносов, а 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 МСС будет задана табл. 2.

Таблица 2

Таблица Кэли для произвольного значения m_i

	a_i				
b_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

Одно 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 КВ посредством использования ПКС. Так, операнд в КВ представляется набором из n остатков $\{a_i\}$, образованных путем последовательного деления исходного числа A на n попарно простых чисел $\{m_i\}$, для значений $(i = \overline{1,n})$. В этом случае совокупность остатков $\{m_i\}$ непосредственно отождествляется с суммой $\sum_{i=1}^{n} GF(m_i)$ n простых полей Галуа.

При рассмотрении метода реализации целочисленных арифметических операций в КВ 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. Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в табл. 2 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. 2 содержатся все элементы поля ровно по одному разу. Использование перечисленных свойств позволяет реализовать операции модульного сложения и вычитания в КВ путем применения ПКС посредством n кольцевых $M = m_i([\log_2(m_i-1)]+1)$ -разрядных КСР). Пусть произвольная алгебраическая система представлена в виде $S = (G, \otimes)$, где G – непустое множество; $\otimes$ – тип операции, определенной для любых двух элементов a_i, $b_i \in G$. 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 $0,\ \pm1,\ \pm2, \ldots$. (Если основание m_i КВ простое число, то Z/m_i - поле). Данное обстоятельство обусловливает возможность реализации арифметической операции сложения и вычитания в КВ без межразрядных переносов путем кольцевого сдвига содержимого разрядов КСР [5].

В данной статье на основе использования ПКС предлагается метод реализации целочисленной арифметической операции сложения в КВ. Суть разработанного в статье метода состоит в том, что исходная цифровая структура для каждого модуля (основания) КВ представляется в виде содержимого первой строки таблицы модульного сложения $(a_i + b_i) \bmod m_i$ вида

$$P_{исх}^{(m_i)} = \left[P_0(a_0)\Big(P_1(a_1)\Big(\ldots\Big(P_{m_i-1}(a_{m_i-1})\right],$$

где $\Big($ - операция конкатенации (присоединение, склеивание); $P_v(a_v)$ - k-разрядный двоичный код, соответствующий значению a_v-го остатка $(a_v = \overline{0, m_i - 1})$ числа по модулю m_i КВ; $k = [\log_2(m_i-1)+1]$.

Для заданного конкретного модуля m_i=5, исходная цифровая структура содержимого КСР имеет вид (табл. 3):

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

Таблица 3

Таблица Кэли для m_i = 5

b_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

Таким образом, посредством используемых в ПСС кольцевых регистров сдвига, легко реализовать целочисленные арифметические операции в КВ. При этом степени циклических перестановок определяется следующими выражениями:

$$\left[P_0(\alpha_0)\middle\|P_1(\alpha_1)\middle\|\ldots\middle\|P_{m_i-1}(a_{m_i-1})\right]^Z =$$

$$= \left[P_z(a_z)\middle\|P_{z+1}(a_{z+1})\middle\|\ldots\middle\|P_0(a_0)\middle\|\ldots\middle\|P_{m_i-1}(a_{m_i-1})\right];$$

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

$$= \left[P_{m_i-1-z}(a_{m_i-1-z})\middle\|\ldots\middle\|P_{m_i-z}(a_{m_i-z1})\right\|$$

$$\left\|\ldots\middle\|P_0(a_0)\middle\|P_1(a_1)\middle\|\ldots\middle\|P_{m_i-z-2}(a_{m_i-z-2})\right].$$

Отметим, что

$$\left[P_0(a_0)\Big(P_1(a_1)\Big(\ldots\Big(P_{m_i-1}(a_{m_i-1})\right]^{m_i} = \varepsilon,$$

т.е. при $z = m_i$ все элементы упорядоченного множества $\left\{P_j(a_i)\right\}$ $(j = \overline{0, m_i - 1})$ остаются на исходном месте.

При технической реализации данного метода первый операнд (остаток) a_i числа A определяет номер разряда $P_{a_i}(a_{a_i})$, с содержимым конечного результата модульной операции по модулю m_i, а второй операнд b_i числа B - число разрядов КРС (величина $b_i k$ определяет количество двоичных разрядов), на которые необходимо провести сдвиги исходного содержимого КРС.

Очевидно, что время сложения двух остатков $(a_i + b_i) \bmod m_i$ чисел A и B в КВ определится математическим выражением

$$T^{(+)}_{\substack{КВ\\m_i}} = K_{1i} \cdot K_{2i} \cdot t_{сдв},$$

где K_{1i} – значение второго b_i слагаемого в сумме $(a_i + b_i) \bmod m_i$ (количество разрядов КРС на которое в положительном направлении сдвигается исходное содержимое КРС), т.е $K_{1i} = \overline{0, m_i - 1}$;

K_{2i} – количество двоичных разрядов в одном разряде КРС по модулю m_i, т.е $K_{2i} = \left[\log(m_i - 1)\right] + 1$;

$K_{1i} \cdot K_{2i}$ – количество сдвигаемых в положительном (против часовой стрелки) направлении двоичных разрядов КРС;

$t_{сдв} = 3 \cdot \tau_B$ – время сдвига одного двоичного разряда;

τ_B – время срабатывания одного логического вентиля (элемента И, ИЛИ).

Таким образом, для произвольного модуля m_i КВ время сложения двух остатков a_i и b_i равно

$$T^{(+)}_{\substack{КВ\\m_i}} = 3 \cdot K_{1i} \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_B.$$

В этом случае максимально возможное значение $T^{(+)}_{\substack{КВ\\m_i}}$ для произвольного модуля m_i КВ равно

$$T^{(+)}_{\substack{КВ\\m_i\\max}} = 3 \cdot (m_i - 1) \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_B,$$

а для данного КВ максимальное время сложения двух чисел

$$A = (a_1, a_2, \cdots, a_n) \text{ и } B = (b_1, b_2, \cdots, b_n)$$

равно

$$T^{(+)}_{\substack{КВ\\m_n\\max}} = 3 \cdot (m_n - 1) \cdot \left\{\left[\log_2(m_n - 1)\right] + 1\right\} \cdot \tau_B,$$

В общем случае время сложения двух чисел

$$A = (a_1, a_2, \cdots, a_n) \text{ и } B = (b_1, b_2, \cdots, b_n)$$

в КВ определится временем $T^{(+)}_{\substack{КВ\\m_i}}$ реализации модульной операции $(a_i + b_i) \bmod m_i$ в BT_i, для которого выполняется условие $K_{1i} \cdot K_{2i} = \max$ из всех вычислительных трактов $BT_j (j = \overline{1, n};\ i \neq j)$. Приведем примеры конкретного выполнения операции сложения двух чисел в КВ для однобайтового $(l = 1)$ процессора.

Для $l = 1$ основания КВ могут быть следующие $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ и $m_4 = 7$.

Пример 1. Пусть второй операнд равен $B = (10, 10, 100, 001)$. Тогда для $BT_1(m_1 = 3)$ имеем, что $b_1 = 10$, $K_{11} = 2$, $K_{21} = \left[\log(m_i - 1)\right] + 1 = 2$, и $K_{11} \cdot K_{21} = 2 \cdot 2 = 4$;

для $BT_2(m_2 = 4)$ имеем $b_2 = 10$, $K_{12} = 2$, $K_{22} = 2$, и $K_{12} \cdot K_{22} = 2 \cdot 2 = 4$;

для $BT_3(m_3 = 4)$ – $b_3 = 100$, $K_{13} = 4$, $K_{23} = 3$, и $K_{13} \cdot K_{23} = 4 \cdot 3 = 12$;

для $BT_4(m_4 = 7)$ – $b_4 = 001$, $K_{14} = 1$, $K_{24} = 3$, и $K_{14} \cdot K_{24} = 1 \cdot 3 = 3$.

Как видно наибольшее количество сдвигаемых двоичных разрядов производится в третьем BT_3, а именно 12.

Таким образом, время реализации двух чисел A и B, определяемое в КВ на основе принципа кольцевого сдвига количественным значением второго слагаемого B, и равно

$$T^{(+)}_{\substack{КВ\\m_3}} = K_{13} \cdot K_{23} \cdot 3 \cdot \tau_B = 12 \cdot 3 \cdot \tau_B = 36 \cdot \tau_B.$$

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

для $BT_1(m_1 = 3)$, $b_1 = 2(10)$, $K_{11} = 2$, $K_{21} = 2$ и $K_{11} \cdot K_{21} = 2 \cdot 2 = 4$;

для $BT_2(m_2 = 4)$, $b_2 = 3(11)$, $K_{12} = 3$, $K_{22} = 2$ и $K_{12} \cdot K_{22} = 3 \cdot 2 = 6$;

для $BT_3(m_3 = 5)$, $b_3 = 1(001)$, $K_{13} = 1$, $K_{23} = 3$ и $K_{13} \cdot K_{23} = 1 \cdot 3 = 3$;

для $BT_4(m_4 = 7)$, $b_4 = 1(001)$, $K_{14} = 1$, $K_{24} = 3$ и $K_{14} \cdot K_{24} = 1 \cdot 3 = 3$.

Таким образом, время сложения чисел А и В определяется временем реализации операции $(a_2 + b_2) \bmod m_2$ во втором вычислительном тракте BT_2 и равно

$$T^{(+)}_{\substack{KB \\ m_2}} = K_{12} \cdot K_{22} \cdot 3 \cdot \tau_B = 3 \cdot 2 \cdot 3 \cdot \tau_B = 18 \cdot \tau_B.$$

Проведем сравнительный анализ времени реализации операции сложения двух чисел А и В в ПСС и в КВ. Известно, что в ПСС время $T^{(+)}_{ПСС}$ сложения двух чисел А и В равно

$$T^{(+)}_{ПСС} = (2 \cdot \rho - 1)t_c = (16 \cdot 1 - 1) \cdot 3 \cdot \tau_B,$$

где: $\rho = 8 \cdot 1$ – количество двоичных разрядов 1-байтового машинного слова СОИ; $t_c = 3 \cdot \tau_B$ – время суммирования в одном $(i+1)$-м двоичном разряде позиционного сумматора значений $a_{i+1} + b_{i+1} + c_i$.

Учитывается, что в настоящее время существует процедура уменьшения в два раза максимального времени реализации операции модульного сложения в КВ имеем

$$T^{(+)}_{\substack{KB \\ max}} = T^{(+)}_{\substack{KB \\ m_n}} / 2.$$

В этом случае коэффициент α, который определяет отношения времени реализации операции сложения в ПСС и в КВ, т.е.

$$\alpha = T^{(+)}_{ПСС} / T^{(+)}_{\substack{KB \\ max}} =$$

$$= \frac{(16 \cdot 1 - 1) \cdot 3 \cdot \tau_B \cdot 2}{(m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\} \cdot 3 \cdot \tau_B} =$$

$$= \frac{2 \cdot (16 \cdot 1 - 1)}{(m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\}}.$$

Выводы

В данной статье предложен метод повышения быстродействия реализации целочисленной арифметической операции сложения двух чисел в КВ. Данный метод основан на использовании ПКС. Использование основных свойств КВ позволяет эффективно организовать процесс реализации модульных целочисленных операций в СОД. Рассмотренные примеры выполнения операции сложения в КВ и результаты проведенного анализа эффективности использования данного метода показали их практическую реализуемость.

Данный метод обработки информации рекомендованы к использованию в СОД реального времени.

Результаты изложенных исследований целесообразно также использовать в системах и устройствах обработки больших массивов цифровой информации, представленной в целочисленном виде.

Список литературы

1. *Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.*
2. *Краснобаев В.А. Методы повышения надежности специализированных ЭВМ систем и средств связи / В.А. Краснобаевю – Х.: МО СССР, 1990. – 172 с.*
3. *Виноградов И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 175 с.*
4. *Краснобаев В.А. Принцип реализации арифметических операций в системе остаточных классов / В.А. Краснобаев // АСУ и приборы автоматики. – 1988. – С. 36-38.*
5. *Краснобаев В.А. Методы реализации модульных операций в системах цифровой обработки информации / В.А. Краснобаев // Радиотехника. – 2001. – Вып. 119. – С. 130-134.*

Поступила в редколлегию 26.03.2014

Рецензент: д-р техн. наук, проф. Г.А. Кучук, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ОБРОБКИ ДАНИХ У КЛАСУ ЛИШКІВ

В.А. Краснобаєв, І.О. Черницька, С.О. Кошман, А.М. Мартиненко

У статті розглянуто метод реалізації операції додавання чисел в класі лишків (КЛ). Метод заснований на використанні принципу кільцевого зсуву (ПКЗ). Наведені приклади реалізації операції додавання чисел у КЛ на основі ПКЗ.

***Ключові слова**: непозиційна система числення класу лишків, принцип кільцевого зсуву, арифметичні цілочисельні модульні операції.*

METHOD OF DATA PROCESSING IN RESIDUE CLASSES

V.A. Krasnobaeyv, I.A. Chernytskya, S.A. Koshman, A.M. Martynenko

The article describes the method of realization of the operations of addition of numbers in residue class (RC). The method is based on using the principle of circular shift (PCS). The examples of the operation of adding numbers in the RC based PCS are given.

***Keywords**: nonpositional residue class value system, the principle of circular shift, integer arithmetic modular operations.*