УДК 681.142 **doi: 10.20998/2522-9052.2018.1.07**

В. А. Краснобаев [1], С. А. Кошман [1], В. А. Чеснок [1], А. С. Янко [2]

[1] Харьковский национальный университет имени В. Н. Каразина, Харьков
[2] Полтавский национальный технический университет имени Юрия Кондратюка, Полтава

ТАБЛИЧНЫЙ МЕТОД ОБРАБОТКИ ЦИФРОВОЙ ИНФОРМАЦИИ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Предметом изучения в статье являются процессы обработки информации в системах обработки информации, которые построены на основе непозиционной системы счисления в остаточных классах (СОК). **Целью** статьи является разработка табличного метода обработки цифровой информации, представленной в СОК. **Задачи**: исследовать особенности применения табличной арифметики в СОК; исследовать существующие табличные методы реализации модульных арифметических операций; разработать усовершенствованный табличный метод реализации арифметических операций в СОК, который позволит сократить количество оборудования матричных схем. Используемыми **методами** являются: методы анализа и синтеза, а также методы теории чисел. Получены следующие результаты. Проанализирована цифровая структура таблиц модульных операций сложения, вычитания и умножения, на основании чего разработан новый оригинальный табличный метод реализации арифметических операций в СОК. Данный метод основан на использовании кода табличного умножения, который приобрел новое качество и стал универсальным табличным кодом для выполнения трех арифметических операций. Данный метод даёт возможность синтезировать конструктивно простое и быстродействующее операционное устройство в СОК. **Выводы**. Научная новизна полученных результатов состоит в следующем: усовершенствован табличный метод обработки цифровой информации, который, несмотря на информационное различие свойств цифровых данных структур таблиц, реализующих модульные операции в СОК, позволяет реализовать всего по 0,25 части полных таблиц, что ранее предполагалось невозможным. Результаты исследований целесообразно использовать в системах и устройствах обработки больших массивов цифровой информации в реальном времени.

Ключевые слова: система обработки информации; система счисления в остаточных классах,; табличная арифметика; класс вычетов; массив цифровой информации.

Введение

Задача решение трудоемких вычислительных научно-практических задач состоит в основном в необходимости проведения значительных объемов вычислений в реальном времени. Таким образом, важны и актуальны исследования, посвященные совершенствованию существующих и разработки новых методов и средств повышения производительности переработки цифровой информации систем обработки информации (СОИ) реального времени, в частности, табличных методов обработки цифровой информации.

Целью статьи является разработка табличного метода обработки цифровой информации, представленной в непозиционной системе счисления в остаточных классах (СОК).

Анализ последних исследований

Все позиционные системы счисления (ПСС), используемые в современных СОИ, в которых представляется и обрабатывается информация, обладают существенным недостатком – наличием межразрядных связей в обрабатываемых операндах. Это обстоятельство обуславливает основное ограничение по повышению производительности СОИ в ПСС [1].

В современных литературных источниках отмечается, что одним из действенных практических направлений повышения пользовательской производительности вычислительных средств является внедрение нетрадиционных методов представления и обработки информации в числовых системах с параллельной структурой, и в частности, в так называемых модулярных системах счисления, обладающих максимальным уровнем внутреннего параллелизма в организации процесса переработки информации. К таким системам счисления относится и непозиционная система счисления в остаточных классах – классе вычетов [2-4].

Одно из свойств СОК - малоразрядность остатков, представляющих операнд. Именно это свойство позволяет существенно повысить быстродействие выполнения арифметических операций счет возможности применения (в отличии от ПСС) табличной арифметики, где арифметические операции сложения, вычитания и умножения выполняются практически в один такт [5-8].

В общем случае табличное операционное устройство СКСОИ для реализации арифметических операций (которые реализуется в унитарном коде) представляет собой двухвходовое ПЗУ. Для каждого из входов количество входных шин для l-байтовой ($8l$ двоичных разряда) СОИ равно 2^{8l}. При этом общее количество логических схем совпадения “И” в узлах ПЗУ (которое в основном и определяет общее количество оборудования табличного операционного устройства СОИ) равно

$$N_{1\,\text{ПСС}} = 2^{8l} \times 2^{8l} = 2^{16l}.$$

В этом случае $N_1 = 2^{16} = 65536$, что является приемлемым количеством оборудования для современного развития элементной базы. Однако, как отмечалось выше, тенденция развития средств обработки цифровой информации направлена на увеличение длины разрядной сетки СОИ. Уже сейчас предлагается к практическому использованию СОИ для $l = 2$.

В этом случае

$$N_{4\text{ПСС}} = 2^{32} \times 2^{32} = 2^{64} \text{ и } N_{8\text{ПСС}} = 2^{64} \times 2^{64} = 2^{128}.$$

Очевидно, что табличный метод реализации арифметических операций в ПСС практически не применим. Поиск путей повышения производительности обработки информации привел к необходимости разработки табличного метода реализации модульных операций, использование которого позволит повысить эффективность применения табличной арифметики в СОК.

Отметим основные достоинства табличного варианта построения СОИ в СОК:

- табличные схемы имеют высокую надежность, так как реализуются в виде компактных ПЗУ; в этом случае весь тракт СОИ строится по блочному принципу, что улучшает ремонтопригодность СОИ (уменьшается время восстановления $T_в$);

- простота табличных схем и дешифраторов, имеющих количество выходов, соответствующих основанию СОК;

- высокое быстродействие; результат операции может быть получен в момент поступления входных операндов, т.е. в один такт; время выполнения арифметических операций в СОК сравнимо с тактовой частотой вычислителя, что принципиально невозможно для позиционных вычислительных машин при существующей элементной базе.

Известен табличный метод реализации операции модульного умножения в СОК, который реализуется посредством использованием кода табличного умножения (КТУ). В этом случае таблица $a_i\beta_i \ (mod\ m_i)$ модульного умножения для произвольного основания m_i СОК симметрична относительно левой (главной) и правой диагоналей, а также вертикали и горизонтали. Симметричность относительно левой диагонали определяется коммутативностью операции $a_i\beta_i$ умножения, а симметричность относительно правой диагонали определяется тем, что

$$(m_i - a_i)(m_i - \beta_i) \equiv a_i\beta_i (\mathrm{mod}\, m_i).$$

Симметричность относительно вертикали и горизонтали определяется из условия кратности значения модуля сумме симметричных чисел таблицы умножения

$$a_i\beta_i + a_i(m_i - \beta_i) \equiv 0 (\mathrm{mod}\, m_i)$$

$$a_i\beta_i + \beta_i(m_i - a_i) \equiv 0 (\mathrm{mod}\, m_i)$$

Исходя из вышеизложенного очевидно, что для табличной реализации операции модульного умножения $a_i\beta_i (\mathrm{mod}\, m_i)$ достаточно иметь числовую информацию только об ее восьмой части. Отсюда возникает возможность упростить таблицу модульного умножения.

Для наиболее эффективной реализации операции $a_i\beta_i (\mathrm{mod}\, m_i)$ применяются методы специального кодирования, позволяющие в четыре раза уменьшить таблицу модульного умножения. Решение поставленной задачи возможно в результате применения специальных кодов.

Рассмотрим один из вариантов выполнения операции модульного умножения посредством использования КТУ (табл. 1 и 2 для $m_i = 5$).

Таблица 1. **Код табличного умножения**

a_i	КТУ		a_i	КТУ	
	γ_a	a_i'		γ_a	a_i'
1	0	1	3	1	2
2	0	2	4	1	1

Таблица 2. **Таблица модульного умножения**

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

Пусть даны входные операнды a_i и β_i. Значения $a_i(\beta_i)$, лежащие в диапазоне $[0,(m_i-1)/2)$, могут быть закодированы произвольным способом, а значения $a_i(\beta_i)$, лежащие в диапазоне $[(m_i+1)/2, m_i-1)$, кодируется, как $m_i - a_i(m_i - \beta_i)$. Для отличия диапазонов вводится следующий индекс (признак) КТУ:

$$\gamma_a(\gamma_\beta) = \begin{cases} 0, \text{ если } 0 \le a_i(\beta_i) \le (m_i-1)/2, \\ 1, \text{ если } (m_i+1)/2 \le a_i(\beta_i) \le m_i - 1. \end{cases}$$

Метод определения результата операции модульного умножения $a_i'\beta_i' (\mathrm{mod}\ m_i)$ в СОК посредством использования КТУ следующий: если заданы два операнда в КТУ $a_i = (\gamma_a, a_i'), \beta_i = (\gamma_\beta, \beta_i')$, то для того, чтобы получить произведение этих чисел по модулю m_i, достаточно найти произведение $a_i'\beta_i' (\mathrm{mod}\ m_i)$ и инвертировать его обобщенный индекс γ_i в случае, если γ_a отлично от γ_β, т.е.

$$a_i\beta_i (\mathrm{mod}\ m_i) = (\gamma_i, a_i'\beta_i' (\mathrm{mod}\ m_i)),$$

где

$$\gamma = \begin{cases} \overline{\gamma}_i, \text{ если } \gamma_a \ne \gamma_\beta, \\ \gamma_i, \text{ если } \gamma_a = \gamma_\beta; \end{cases}$$

$$a_i' = \begin{cases} a_i, \text{ если } \gamma_a = 0, \\ m_i - a_i, \text{ если } \gamma_a = 1. \end{cases}$$

При использовании данного метода табличное ПЗУ, реализующее операцию модульного умножения, конструктивно уменьшаются в четыре раза.

При выполнении операции табличными методами в некоторых случаях возможно дополнительное уменьшение оборудования за счет того, что строится не единая таблица для модульных операций, а k боле мелких таблиц, позволяющих

дать ответы по каждому из k разрядов результата, где k – разрядность регистра, необходимая для хранения цифр остатка по рассматриваемому основанию m_i СОК.

Основные материалы исследований

До сих пор вопросы эффективной реализации арифметических операций сложения и вычитания с использованием КТУ в литературе либо не рассматривались, либо такая реализация считалась большинством исследователей теоретически и практически невозможной.

Основная практическая трудность заключается в том, что довольно сложно синтезировать табличные алгоритмы выполнения этих модульных операций, так как таблицы реализации модульных операций сложения и вычитания различны по своей цифровой структуре вследствие чего они не обладают теми свойствами симметрии, которыми обладают таблицы модульного умножения. Однако совершенно иные результаты можно получить, исследуя возможности реализации одной модульной операции с помощью таблиц, реализующих обратную ей операцию, и наоборот.

При исследовании цифровых свойств таблиц модульных операций сложения и вычитания (табл. 1 и 2 для $m_i = 5$) выведено и доказано следующее аналитическое соотношение

$$\begin{aligned}&\left[\left(\gamma_a, a_i'\right)+\left(\gamma_\beta, \beta_i'\right)\right]+\\&\left\{\left[m_i-\left(\gamma_a, a_i'\right)\right]-\left(\gamma_\beta, \beta_i'\right)\right\}=0\left(\operatorname{mod} m_i\right),\end{aligned} \quad (1)$$

где $a_i = \left(\gamma_a, a_i'\right)$, $\beta_i = \left(\gamma_\beta, \beta_i'\right)$ – входные операнды, представленные в КТУ.

Таблица 3. **Таблица модульного сложения**

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

Таблица 4. **Таблица модульного вычитания**

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

Запишем выражение (1) в виде

$$\begin{aligned}&\left(\gamma_a, a_i'\right)+\left(\gamma_\beta, \beta_i'\right)=\\&=m_i-\left\{\left[m_i-\left(\gamma_a, a_i'\right)\right]-\left(\gamma_\beta, \beta_i'\right)\right\}.\end{aligned} \quad (2)$$

Из выражения (2) следует, что для получения результата операции модульного сложения в КТУ достаточно знать результат операции модульного вычитания, т.е. возникает возможность эффективно (с точки зрения уменьшения количества оборудования ПЗУ) использовать КТУ одновременно для трех модульных операций: умножения, сложения и вычитания. На основании выражения (2) рассмотрим метод, посредством которого можно будет осуществлять выполнения любой из трех арифметических операций в СОК: умножение, сложение и вычитание. Операция модульного сложения осуществляется посредством алгоритма, описанного выражением (2). Составим алгоритм выполнения операции модульного сложения с помощью таблицы, для выполнения операции модульного вычитания

$$\left(a_i' - \beta_i'\right) \operatorname{mod} m_i .$$

В соответствии с выражением (2) рассмотрим алгоритм реализации операции модульного сложения.

1. Уменьшаемое $a_i = \left(\gamma_a, a_i'\right)$ инвертируется по модулю m_i, т.е. получим следующее выражение: $\overline{a}_i = \left(\left(\gamma_a + 1\right) \operatorname{mod} 2, a_i'\right)$. Вычитаемое $\left(\gamma_\beta, \beta_i'\right)$ оставляем без изменений.

2. Посредством ПЗУ, реализующего операцию модульного вычитания, по входным операндам a_i' и β_i' определяется результат операции

$$\left(a_i' - \beta_i'\right) \operatorname{mod} m_i .$$

Как и для алгоритма модульного умножения, индекс γ_i результата операции модульного вычитания формируется в соответствии со значениями индексов соответствующих операндов, т.е. в соответствии со значениями $(\gamma_a + 1) \operatorname{mod} 2$ и γ_β, где:

$$\gamma_i = \begin{cases} \overline{\gamma}, \text{ если } \left(\gamma_a + 1\right) \operatorname{mod} 2 \neq \gamma_\beta, \\ \gamma, \text{ если } \left(\gamma_a + 1\right) \operatorname{mod} 2 = \gamma_\beta. \end{cases}$$

Следовательно, результат операции модульного вычитания будет иметь следующий вид:

$$\left(\gamma_i, \left(a_i' - \beta_i'\right) \operatorname{mod} m_i\right).$$

3. Полученный результат модульного вычитания инвертируем по модулю m_i:

$$\left(\left(\gamma_i + 1\right) \operatorname{mod} 2, \left(a_i' - \beta_i'\right) \operatorname{mod} m_i\right).$$

Это и будет искомый результат модульного сложения.

Таким образом, несмотря на различие цифровой структуры таблиц модульных операций сложения, вычитания и умножения, создан новый ориги-

нальный табличный метод реализации арифметических операций в СОК.

На основании данного метода можно синтезировать конструктивно простое и высоконадежное операционное устройство СОИ в СОК, основу которого составляют три отдельных коммутатора, каждый из которых реализует только 0,25 части соответствующей полной таблицы модульных операций умножения (табл. 2) и вычитания (табл. 4) (первый коммутатор – II-квадрант таблицы умножения (табл. 5); второй и третий коммутаторы – соответственно I (табл. 7) и II (табл. 6) квадранты табл. 4 вычитания).

В этом плане код табличного умножения приобрел новое качество и стал универсальным табличным кодом для выполнения трех арифметических операций в СОК.

Таблица 5. **2-й квадрант таблицы 2**

β_i \ a_i		1	2
		4	3
1	4	1	2
2	3	2	4

Таблица 6. **2-й квадрант таблицы 4**

β_i \ a_i		1	2
		4	3
1	4	0	1
2	3	4	0

Таблица 7. **1-й квадрант таблицы 4**

β_i \ a_i		2	1
		3	4
1	4	2	3
2	3	1	2

Таблица 8. **2-й квадрант таблицы 3**

β_i \ a_i		1	2
		4	3
1	4	2	3
2	3	3	4

Таблица 9. **1-й квадрант таблицы 3**

β_i \ a_i		2	1
		3	4
1	4	4	0
2	3	0	1

Выводы

В статье предложен метод обработки цифровой информации в СОК, основанный на табличном принципе.

Посредством данного метода реализуются арифметические операций модульного сложения, вычитания и умножения. Данный метод (в отличии от известных) несмотря на информационное различие свойств цифровых данных структур таблиц, реализующих модульные операции $(a_i \otimes \beta_i) \bmod m_i$ в СОК, позволяют реализовать всего по 0,25 части каждой из полных таблиц что ранее предполагалось невозможным.

Основное преимущество предложенного метода состоит в возможности достижения высокого быстродействия обработки информации. Так результат выполнения арифметической целочисленной операции может быть получен в момент поступления на обработку входных операндов, т.е. практически в один такт.

Таким образом, время выполнения арифметических операций в СОК сравнимо с тактовой частотой вычислителя, что принципиально невозможно для СОИ в ПСС.

Результаты предложенных исследований целесообразно использовать в системах и устройствах обработки больших массивов цифровой информации в реальном времени.

СПИСОК ЛІТЕРАТУРИ

1. Акушский И. Я. Машинная арифметика в остаточных классах / И. Я.Акушский, Д. И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.
2. Krasnobayev V. A. A method for increasing the reliability of verification of data represented in a residue number system / V. A. Krasnobayev, S. A. Koshman, M. A. Mavrina // Cybernetics and Systems Analysis. – 2014. – Vol. 50, Issue 6. – P. 969-976.
3. Krasnobayev V. A. A Method for arithmetic comparison of data represented in a residue number system / V. A. Krasnobayev, A. S. Yanko, S. A. Koshman // Cybernetics and Systems Analysis. – Vol. 52, Issue 1. – P. 145-150.
4. Мороз С.А. Метод верификации данных в системе непозиционных остаточных вычетов / С. А. Мороз, В. А. Краснобаев // Системи управління, навігації та зв'язку. – Полтава : ПНТУ, 2011. – Вип. 2 (18). – С. 134-138.
5. The statistical analysis of a network traffic for the intrusion detection and prevention systems / Kuznetsov A. A., Smirnov A. A., Danilenko D. A., Berezovsky A. V. // Telecommunications and Radio Engineering. – 2015. – Vol. 74. – P. 61-78.
6. Stasev Yu. V. Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes" / Yu. V. Stasev, A. A. Kuznetsov // Cybernetics and Systems Analysis. – 2005. – Vol. 41, Issue 3. – P. 354-363.

7. Krasnobayev V. A. A method for operational diagnosis of data represented in a residue number system / V. A. Krasnobayev, S. A. Koshman // Cybernetics and Systems Analysis. – 2018. – Vol. 54, Issue 2. – P. 336-344.
8. Gorbenko I. Examination and implementation of the fast method for computing the order of elliptic curve / I. Gorbenko, R. Hanzia // European Journal of Enterprise Technologies. – 2017. – Vol. 2, No. 9(86). – P. 11-21.

REFERENCES

1. Akushsky, I.Ya. and Yuditsky, D.I.(1968), *Machine arithmetic in residual classes*, Sov. Radio, Moscow, 440 p.
2. Krasnobayev, V.A., Koshman, S.A. and Mavrina, M.A. (2014), "A method for increasing the reliability of verification of data represented in a residue number system", *Cybernetics and Systems Analysis*, Vol. 50, Issue 6, pp. 969-976.
3. Krasnobayev, V.A., Yanko, A.S. and Koshman, S.A. (2016), "A Method for arithmetic comparison of data represented in a residue number system", *Cybernetics and Systems Analysis*, Vol. 52, Issue 1, pp. 145-150.
4. Moroz, S.A. and Krasnobayev, V.A. (2011), "A data verification method in a non-positional residue number system", *Control, Navigation, and Communication Systems*, No. 2(18), pp. 134-138.
5. Kuznetsov, A.A., Smirnov, A.A., Danilenko, D.A. and Berezovsky, A.V. (2015), "The statistical analysis of a network traffic for the intrusion detection and prevention systems", *Telecommunications and Radio Engineering*, Vol. 74, pp. 61-78.
6. Stasev, Yu.V., Kuznetsov, A.A. (2005), "Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes", *Cybernetics and Systems Analysis*, Vol. 41, Issue 3, pp. 354-363.
7. Krasnobayev V.A. and Koshman S.A. (2018), "A method for operational diagnosis of data represented in a residue number system", *Cybernetics and Systems Analysis*, Vol. 54, Issue 2, pp. 336-344.
8. Gorbenko, I. and Hanzia, R. (2017), "Examination and implementation of the fast method for computing the order of elliptic curve", *European Journal of Enterprise Technologies*, Vol 2, No. 9(86), pp. 11-21.

Надійшла (received) 13.02.2018
Прийнята до друку (accepted for publication) 11.04.2018

Табличний метод обробки цифровий інформації у системі залишкових класів

В. А. Краснобаєв, С. О. Кошман, В. О. Чеснок, А. С. Янко

Предметом вивчення в статті є процеси обробки інформації в системах обробки інформації, які побудовані на основі непозиційної системи числення в залишкових класах (СЗК). **Метою** статті є розробка табличного методу обробки цифрової інформації, представленої в СЗК. **Завдання:** дослідити особливості застосування табличної арифметики в СЗК; дослідити існуючі табличні методи реалізації модульних арифметичних операцій; розробити вдосконалений табличний метод реалізації арифметичних операцій в СЗК, який дозволить скоротити кількість обладнання матричних схем. Використаними **методами** є: методи аналізу і синтезу, а також методи теорії чисел. Отримані наступні результати. Проаналізована цифрова структура таблиць модульних операцій додавання, віднімання і множення, на підставі чого розроблено новий оригінальний табличний метод реалізації арифметичних операцій в СЗК. Даний метод заснований на використанні коду табличного множення, який придбав нову якість і став універсальним табличним кодом для виконання трьох арифметичних операцій. Даний метод дає можливість синтезувати конструктивно простий і швидкодіючий операційний пристрій в СЗК. **Висновки**. Наукова новизна отриманих результатів полягає в наступному: удосконалено табличний метод обробки цифрової інформації, який, незважаючи на інформаційну відмінність властивостей цифрових даних структур таблиць, що реалізують модульні операції в СЗК, дозволяє реалізувати всього по 0,25 частини повних таблиць, що раніше було неможливим. Результати досліджень доцільно використовувати в системах і пристроях обробки великих масивів цифрової інформації в реальному часі.

Ключові слова: система обробки інформації; система числення в залишкових класах,; таблична арифметика; клас вирахувань; масив цифрової інформації.

Table method for processing digital information in the system of residual classes

V. A. Krasnobaeyv, S. A. Koshman, V. A. Chesnok, A. S. Yanko

In the article **subject** of the study is the data processing in the data processing systems, which are built on the basis of non-positional number system in the residual classes (SRC). The **purpose** of the article is to develop a tabular method for digital data processing presented in the SRC. **Objectives**: to investigate the features of using tabular arithmetic in SRC; to explore the existing tabular methods for implementing modular arithmetic operations; to develop an improved tabular method for implementing arithmetic operations in SRC, which will reduce the number of hardware matrix schemes. The used **methods** are: methods of analysis and synthesis, as well as methods of number theory. The following **results** were obtained. The digital structure of the tables of modular operations of addition, subtraction and multiplication was analyzed, so a new original tabular method for implementing arithmetic operations in the SRC was developed. This method is based on the use of the table multiplication code, which acquired a new quality and became a universal table code for performing three arithmetic operations. This method makes it possible to synthesize a constructively simple and fast operating device in the SRC. **Conclusions**. The scientific novelty of the obtained results is: the table method for processing digital information has been improved, despite the information difference in the properties of the digital data of table structures, implementing modular operations in the SRC, allows to implement only 0.25 parts of complete tables, which was previously supposed impossible. The results of the research should be used in systems and devices for processing large arrays of digital data in real time.

Keywords: data processing system; number system in residual classes; tabular arithmetic; class of residues; array of digital information.