UDC 681.04

K.V. YASKOVA[1], V.I. BARSOV[2], V.A. KRASNOBAYEV[1], S.A. KOWMAN[1], KHERY ALI ABDYLLAH[3]

[1] Kharkiv National Technical University of Agriculture named after P. Vasylenko, Ukraine
[2] Ukrainian Engineering Pedagogical Academy, Kharkiv, Ukraine
[3] National aerospace university named after N.E. Zhukovsky "KhAI", Ukraine

METHOD OF REALIZATION OF ARITHMETIC OPERATIONS ON THE BASIS OF THE USE OF MODULYARNOY NUMBER SYSTEM

In this article we consider two arithmetic operation realizations in modular arithmetics, based on the ring shift principle. The method of binary position and remainder encoding has proved to be very efficient comparing to the method of unitary position and residual encoding. It allows to substantially increase the speed of summation and deduction operations. An essential difference of this method is that the initial content of digits of circular shift register is represented in the unitary code.

Key words: *fast-acting, number system in remaining classes, method of ring shift.*

Introduction

With beginning of development of the computing engineering the fast-acting became one of major its descriptions. The delay in treatment of information can result in the receipt of wrong result of calculations of COMPUTER.

There are different methods of increase of fast-acting of COMPUTER. In the given article we will consider one of methods based on application of modular arithmetic (MA). Development of method of treatment of information in the modular number system on the basis of the use of principle of ring shift (PRS) principle is the purpose of the article.

1. Analysis of the last researches

There are four principles of realization of arithmetic operations in modular arithmetic. First principle of summator, which is founded on the base of low-discharge summarizations, the second principle tabular is based on the use of permanent data storage, the third principle is carried out on the use of boolean functions, fourth - principle of ring shift.

Because first three principles are enough known and widely considered in modern literature, therefore it is very interestingly and important to consider the questions of technical realization of modular operations of addition and subtraction based on PRS.

2. Basic materials of researches

In [1, 2, 3] it is considered the principle of realization of arithmetic operations in MA – the ring shift principle, the particularity of which lies in the fact that the result of the arithmetic operation $(\alpha_i \pm \beta_i) \bmod m_i$ upon the arbitrary module of MA set by the aggregate of bases $\{m_j\}$ $(j = \overline{1,n})$ is determined only at the expense of cyclic shifts of the set digital structure.

Actually, the well-known Kally theorem is setting the isomorphism between the elements of the finite Abelian group and the elements of the permutation group. In this case the summation matrix for an arbitrary m_i module of MA will be set by tabl. 1 (by tabl. 2 for m_i=5)

Table 1

The Kally table for an arbitrary value of m_i

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	...	$m_i - 2$

One of the consequences of the Kaly theorem is the conclusion that reflection of the elements of the Abelian group upon the group of all of the integer numbers is homomorphous. This circumstance allows to organize the process of determination of the result of arithmetic operations in MA by means of using PRS.

Table 2

The Kally table for an arbitrary value of 5

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

Thus, the operand in MA is represented by the set of *n* remainders formed by means of subsequent division of the initial number *A* by *n* mutually paired prime integers $\{m_i\}$ for $(i = \overline{1,n})$. In this case the aggregate of remainders $\{m_i\}$ is directly equaled to the amount *n* of prime Galois fields having the form of $\sum_{i=1}^{n} GF(m_i)$.

In order to consider the method of realization of arithmetic operations in MA it would be sufficient to consider the option of for an arbitrary finite Galois field $GF(m_i)$ at $i = const$, i.e., for the specific reduced system of deductions upon the module m_i.

Let the Kally table (Table 1) is made for the set operation of modular summation $(\alpha_i + \beta_i) \bmod m_i$, in the field GF ($m_i$). From the existence of a neutral element in the field $GF(m_i)$ it follows that tabl. 1 contains a row (a column), in which the elements of the given field are arranged in the ascending order. And from the fact that in the field of deductions $GF(m_i)$ these elements are different (the order of the group is equal to m_i) it follows that each row (column) of Table 1 contains all of the field elements exactly one time each. The use of the above particularities allows to realize the operations of modular summation and deduction in MA by applying PRS with the help of *n* ring $M = m_i([\log_2(m_i - 1)] + 1)$ – digit shifting registers.

Let the arbitrary algebraic system be represented in the form $S = \langle G, \otimes \rangle$, where *G* is the non-empty set; $\otimes$ is the type of operation determined for any of two elements $\alpha_i, \beta_i \in G$.

The operation of summation $\oplus$ in the set of the classes of deductions *R* generated by the ideal *J* forms up a new ring called the class of deductions ring *R*/*J*. It can be represented in the form of Z/m_i where *Z* is the set of integers 0, ±1, ±2, (If the base of MA m_i is the prime integer, then Z/m_i is the field).

As it is indicated above just this circumstance is stipulating the possibility of realization of the arithmetic operation of summation in MA without any bit-to-bit transfers by means of the ring shift.

On the basis of the principle suggested in [8] there was developed the method of realization of arithmetic operations in MA (the method of binary position and remainder encoding). The essence of the developed method lies in the fact that the initial digital structure for each module (base) of TMS is represented in the form of the contents of the first row (column) of the modular summation (deduction) table $(\alpha_i + \beta_i) \bmod m_i$ of the form

$$P_{init}^{(m_i)} = [P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-1}(\alpha_{m_i-1})], \quad (1)$$

where $\|$ is the operation of concatenation (gluing); $P_v(\alpha_v)$ is the k-bit binary code correspondent to the value of the a_v-th remainder $(\alpha_v = \overline{0, m_i - 1})$ of the number upon the module m_i; $k = [\log_2(m_i - 1) + 1]$. For the set specific module $m_i = 5$ the initial digital structure of the RSR content has the following representation

$$P_u^{(5)} = [000 \| 001 \| 010 \| 011 \| 100].$$

Thus, by means of the ring shift registers used in BNS it is easy to realize the arithmetic operations in MA, where the degrees of cyclic permutations as considered on the basis of (1) are determined by the following expressions

$$\begin{aligned} &[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-1}(\alpha_{m_i-1})] = \\ &= [P_z(\alpha_z) \| P_{z+1}(\alpha_{z+1}) \| ... \| P_0 \alpha_0 \| ... \| P_{m_i-1}(\alpha_{m_i-1})]^z, \end{aligned} \quad (2)$$

$$\begin{aligned} &[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-1}(\alpha_{m_i-1})]^{-z} = \\ &= [P_{m_i-1-z}(\alpha_{m_i-1-z}) \| ... \| P_{m_i-z}(\alpha_{m-z_i}) \| \\ &\| ... \| P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-z-2}(\alpha_{m_i-z-2})] \end{aligned} \quad (3)$$

We note that $[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i-1}(\alpha_{m_i-1})]^{m_i}$, i.e., at $z = m_i$ all the elements of the ordered set $\{P_j(\alpha_j)\}$ for $(j = \overline{0, m_i - 1})$ remain at the initial position.

During the technical realization of the given method the first operand α_i is determining the number α_i of the digit $P_{\alpha_i}(\alpha_{\alpha_i})$ with the content of the modular operation result upon the module mi and the second operand β_i – the number of RSR digits (of $\beta_i k$ – bit binary digits) upon which it is necessary to perform the shifts of the initial (1) content of the RSR pursuant to the algorithms (2), (3).

The main drawbacks of the suggested method for realization of arithmetic operations in MA include comparatively larger time for execution of integer-number arithmetic modular operations that increases the efficiency of using of PRS.

This drawback is stipulated by the fact that the structure $P_{init}^{(m_i)}$ (see (1)) is represented by the set of initial remainders of the first row of the matrix $(\alpha_i + \beta_i) \bmod m$, which are reflected by the binary code. In this case the time for realization of the modular summation of two operands $A = (\alpha_1, \alpha_2, ..., \alpha_{n-1}, \alpha_n)$ and $B = (\beta_1, \beta_2, ..., \beta_{n-1}, ...\beta_n)$ in MA is determined by the expression

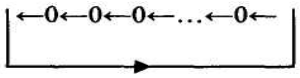
$$t = k\beta_{max\,i}\tau, \qquad (4)$$

where τ is the time of shift of one binary digit of PRS.

We consider the method for realization of arithmetic operations in MA, which is deprived of the above drawback. It is the method of unitary position and residual encoding according to which the informational structure $P_{init}^{(m_i)}$ of the arbitrary module m_i, of MA is represented in the form of a unitary $(m_i - 1)$ – bit code.

$$P_{init}^{(m_i)} = [P(\alpha_{i-1}) \| P(\alpha_{i-2}) \| ... \| P(1) \| P(0)], \qquad (5)$$

where $P(\alpha_j)$ is the binary digit of the digital structure (5), the unitary condition of which corresponds to the value of the operand α_j represented by a unitary code ($\alpha_j = \overline{0, m_i - 1}$). In this case the initial condition of PRS includes $m_i - 1$ binary digits and schematically can be represented in the form of



As this takes place, the first operand α_j represented by a unitary code upon an arbitrary module m_i of MA is entered into the *j*-th digit of PRS, i.e., transfers the *j*-th binary digit into the unitary condition.

The second operand β_j is pointing out to the number by the shift z of the PRS content determining the time of realization of arithmetic operations upon the module m_i of MA, i.e.

$$t_{next} = \beta_i \tau \qquad (6)$$

We note that the time of realization of arithmetic operation *A+B* in MA will be determined by the time of performing of the operation for the maximal value ($\beta_{masx}\,(i = \overline{1, n})$) of the remainder from the set $\{\beta_i\}$ for the given operand $B = (\beta_1, \beta_2, ...\beta_3)$, i.e.,

$$t_{next} = \beta_{max\,i}\tau \qquad (7)$$

Analysis of the expressions (6) and (7) demonstrates that the developed method of unitary representation reduces by $k = [\log_2(m_i - 1) + 1]$ times the time of performing of the arithmetic operations as compared to the method of binary encoding.

Conclusions

Two methods of realization of arithmetic operations in the modular number system on the basis of the use principle of ring shift are considered in the given article. At consideration of these methods showed high efficiency.

The method of unitary encoding from point of time of realization of arithmetic operations showed MA on comparison with a method of binary encoding.

Promotes applications of this method fast-acting of implementation of arithmetic operations on the basis of application of principle ring shift.

References

1. Dolgov V.I. Methods and algorithms for realization of arithmetic operations in the system of remainder classes / V.I. Dolgov, V.A. Krasnobayev, I.V. Kononova // Russia: Electron. Modeling. - 1990. – P. 70-72.

2. Krasnobayev V.A. Algorithms for realization of modular multiplication operation in the system of remainder classes / V.A. Krasnobayev, V.P. Irkhin // Russia: Electron. Modeling. - 1993. – P. 20-26.

3. Krasnobayev V.A. Methods for realization of modular operations in the systems of digital data processing / V.A. Krasnobayev // Russia: Radiotekhnika. - 2001. – P. 130-134.

4. Краснобаев В.А. Отказоустойчивые вычислительные системы на основе модулярной арифметики: концепции, методы и средства / В.А. Краснобаев, В.И. Барсов, Е.В. Яськова // Радіоелектронні і комп'ютерні системи. - 2007. - №8 (27). – С. 82-90

5. Khere Ali Abdullah. Принципи реалізації модульних операцій в модулярній арифметиці / Khere Ali Abdullah, К.В. Яськова, В.А. Краснобаєв // Проблеми енергозабезпечення та енергозбереження в АПК України: Вісник ХНТУСГ імені Петра Василенка, вип. 57, том 2. – Х., 2007. – С. 100-104.

6. Яськова К.В. Технічна реалізація операцій модульного складання і віднімання в модулярній арифметиці / К.В. Яськова, Хері Алі Абдуллах, М.С. Деренько, В.А. Краснобаєв // Проблеми енергозабезпечення та енергозбереження в АПК України: Вісник ХНТУСГ імені Петра Василенка. - Вип. 73, том 2. – Х., 2008. – С. 49-51.

7. Krasnobayev V.A. Universal algorithms for compression of table digital data of the results of performance of arithmetic operations in the system of remainder classes / V.A. Krasnobayev, Ya.V. Ilyushko, A.A Zamula // Russia: Radiotekhnika. - 2005. – P. 217-225.

8. Akushskyi I.Ya. Machine arithmetic in residual classes / I.Ya. Akushskyi, D.I. Yuditskyi. – M., 1968 – 440 p.

9. Bleighut R. Fast algorithms for digital processing of signals / R. Bleighut. – Moscow: Mir, 1989. – 448 p.

10. Kravchenko V.S. Methods and microelectronic devices for digital filtering of signals and images based on the theoretical and numerical transformations / V.S. Kravchenko, A.M. Krot // Russian: Foreign radio electronics. Achievements of present-day radio electronics. - 1997. – P. 3-31.

11. Chervyakov N.I. High-speed digital processing of signals using position-independent arithmetic / N.I. Chervyakov, K.T. Tyncherov, A.V. Veligosha // Russian: Radiotekhnika, 1997. – P. 23-27.

12. Lavrinenko D.I. Application of fast Fourier transformation in cryptographic transformers / D.I Lavrinenko // Russian: Radiotekhnika. – 2000. – P. 75-79.

13. Zhikharev V.Ya. Methods and means of data processing in position-independent base notation system in residual classes / V.Ya. Zhikharev, Ya.V. Ilyushko, L.G. Kravets, V.A. Krasnobayev. – Russian: Volyn, Zhytomyr, 2005. – P. 220.

14. Zhikharev V.Ya. Methods and algorithms for realization of arithmetic operations in the class of deductions / V.Ya. Zhikharev, Yunes El Handass, V.A. Krasnobayev // Russian: Open information and computer integrated technologies. – 2003. – P. 84-101.

Поступила в редакцию 12.12.2008

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков, Украина.

МЕТОД РЕАЛИЗАЦИИ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МОДУЛЯРНОЙ СИСТЕМЫ СЧИСЛЕНИЯ

Е.В. Яськова, В.И. Барсов, В.А. Краснобаев, С.А. Кошман, Khery Ali Abdyllah

В данной статье рассмотрено два метода реализации арифметических операций в модулярной арифметики на основе использования принципа кольцевого сдвига. Высокую эффективность показал метод унитарного позиционного – остаточного кодирования, по сравнению с методом двоичного позиционного - остаточного кодирования. Данный метод позволяет существенно повысить быстродействие реализации операций сложения и вычитания. Существенное отличие данного метода состоит в том, что исходное содержимое разрядов кольцевого регистра сдвига представляется унитарным кодом

Ключевые слова: быстродействие, система счисления в остаточных классах, метод кольцевого сдвига.

МЕТОД РЕАЛІЗАЦІЇ АРИФМЕТИЧНИХ ОПЕРАЦІЙ НА ОСНОВІ ВИКОРИСТАННЯ МОДУЛЯРНОЇ СИСТЕМИ ЧИСЛЕННЯ

К.В. Яськова, В.И. Барсов, В.А. Краснобаєв, С.А. Кошман, Khery Ali Abdyllah

В даній статті розглянуто два методи реалізації арифметичних операцій в модулярной арифметики на основі використання принципу кільцевого зсуву. Високу ефективність показав метод унітарного позиційного - залишкового кодування, в порівнянні з методом двійкового позиційного - залишкового кодування. Даний метод дозволяє істотно підвищити швидкодію реалізації операцій складання і віднімання. Істотна відмінність даного методу полягає в тому, що початковий вміст розрядів кільцевого регістра зсуву представляється унітарним кодом

Ключові слова: швидкодія, система числення в залишкових класах, метод кільцевого зсуву.

Яськова Екатерина Викторовна – аспирант кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенка, Харьков, Украина.

Барсов Валерий Игоревич – канд. техн. наук, доцент, декан факультета радиоэлектроники, электромеханики и компьютерных систем, заведующий кафедрой систем управления технологическими процессами и объектами Украинской инженерно-педагогической академии, Харьков, Украина.

Краснобаев Виктор Анатольевич – д-р техн. наук, проф. кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенка, Харьков, Украина, e-mail: krasnobaev_va@rambler.ru.

Кошман Сергей Александрович – старший преподаватель кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенка, Харьков, Украина, e-mail: s_koshman@ukr.net.

Khery Ali Abdyllah – аспирант Национального аэрокосмического университета им. Н.Е. Жуковского "ХАИ", Харьков, Украина.