UDC 681.3.04

METHOD OF TABULAR REALIZATION OF ARITHMETIC OPERATIONS IN THE SYSTEM OF RESIDUAL CLASSES

Viktor Krasnobayev[1], Sergey Koshman[2], Alina Yanko[3]

[1] V.N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
krasnobayev@karazin.ua

[2] Kharkov National Technical University of Agriculture named after Peter Vasylenko, Artyoma st., 44, Kharkiv, 61002, Ukraine
s_koshman@ukr.net

[3] Poltava National Technical Yuri Kondratyuk University, Pershotravnevyi avenue 24, Poltava, 36011, Ukraine
al9_yanko@ukr.net

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
kuznetsov@karazin.ua

Received on August 2016

***Abstract**: In this article the method of increase of productivity and reliability of functioning of the data processing system is suggested based on the use of position-independent computing system in the residual classes (SRC). The developed method takes into account properties of symmetry of tables of realization of basic arithmetic operations and is based on the use ¼ part of the numerical data of the aggregate tables, realizing module operations multiplication, summation and deduction in SRC. Method of bit-by-bit tabular realization is recommended in the digital information processing systems for the productivity improvement of decision of computing tasks.*

***Keywords:** specialized digital devices and systems, base of non-position number system, modular number system, cryptographic transformations.*

Introduction

Stormy development of the computing engineering presently allows to provide the control of operating parameters of the real-time systems in the set limits, that in the turn allows to warn emergency situations. Treatment of large volumes of information for the comparatively short interval of time with the set level of reliability of functioning is the distinctive feature of such systems. The existent data processing system (DPS) functioning in the binary base notation system (BNS) not always are able to decide the set problems in accordance with the produced requirements. One of basic lacks of such DPS is the sequential processing of information, because information submitted in BNS that is stipulating the presence of bit-to-bit communications. This circumstance does not allow parallelizing the decided algorithms at the level of elementary microoperation. The objective of the paper is to develop method of digit-by-digit tabular realization of arithmetic operations in the system of residual classes.

1 Analysis of the last researches

Application of untraditional architectures which are built by with the use of the notation systems (NS) of possessing the maximal level of internal parallelism is grounded in literature [1]. One of such NS is the system of residual classes (SRC). Short form of the residues is one of the SRC properties that allows to use the tabular method of realization of arithmetic operations, which, as is generally known, provides the ultra-high computing speed, i.e. the result of arithmetic operation can be got in the moment of receipt of entrance operands (for one cycle), what is unattainable for BNS.

Simultaneously with this circumstance wide introduction of technologies of the Programmable Logic Device allows successfully realizing the methods of tabular information processing in SRC at creation of fast-acting and high-fail-safe structures of DPS [2-4].

2 Basic materials of researches

The search of ways of increase of productivity and reliability of information processing resulted in the necessity of development of tabular method of realization of module operations.

Known tabular method of realization of operation of module multiplication in SRC, will be realized by means of the use of code of tabular multiplication (CTM) [5–7]. In this case the table $a_i b_i (\bmod m_i)$ of module multiplication for arbitrary base m_i SRC is symmetric in relation to left (main) and right diagonals, and also vertical and horizontal lines. Symmetry in relation to a left diagonal is determined to commutability operation $a_i b_i$ of multiplication, and symmetry in relation to a right diagonal is determined to, that

$$(m_i - a_i)(m_i - b_i) \equiv a_i b_i (\bmod m_i).$$

Symmetry in relative to a vertical and horizontal line is determined from the condition of multiple of value of the module to the sum of symmetric numbers of table of multiplication

$$a_i b_i + a_i (m_i - b_i) \equiv 0 (\bmod m_i),$$
$$a_i b_i + b_i (m_i - a_i) \equiv 0 (\bmod m_i).$$

Coming foregoing from is obvious, that for tabular realization of operation of module multiplication $a_i b_i (\bmod m_i)$ it is enough to have numerical information only about its eighth part. Hereof is possibility to simplify the table of module multiplication, due to the exception from the operating device (OD) of DPS of part of surplus equipment (elements And in the blocks of matrix circuit). For the most effective realization of operation $a_i b_i (\bmod m_i)$ methods allowing in four times to decrease the table of module multiplication are used. The decision the set problem is possible as a result of development and application of the special codes.

The method of determination of result of operation of module multiplication $a_i' b_i' (\bmod m_i)$ in SRC by means of the use of CTM is following: if two operands are set in CTM $a_i = (\gamma_a, a_i')$ and $b_i = (\gamma_b, b_i')$, in order to get product of these numbers with respect to base m_i, it is enough to find product of $a_i' b_i' (\bmod\ m_i)$ and invert its generalized index γ_i in case if γ_a it is differs from γ_b, i.e.

$$a_i b_i (\bmod\ m_i) = (\gamma_i, a_i' b_i' (\bmod\ m_i)),$$

where:

$$\gamma = \begin{cases} \overline{\gamma}_i, \text{ if } \gamma_a \neq \gamma_b, \\ \gamma_i, \text{ if } \gamma_a = \gamma_b; \end{cases}$$

and

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

Foregoing conclusions behave only to realization of operation of module multiplication [1].

During realization of arithmetic operations of summation and deduction basic difficulty consists that it is enough difficultly to synthesize the tabular algorithms of implementation of these module operations, because the tables of realization of operations of summation and deduction are different on the digital structure, hereupon, its do not possess those properties of symmetry, which the tables of module multiplication are possess. However got it is accomplished other results can be, exploring marketability one module operation by tables realizing operation reverse to her, and the opposite.

At research of digital properties of tables of module operations of summation and deduction [8] a next analytical correlation is proved

$$\begin{aligned} &\left[(\gamma_a, a_i') + (\gamma_b, b_i')\right] + \\ &+ \left\{\left[m_i - (\gamma_a, a_i')\right] - (\gamma_b, b_i')\right\} = 0 (\bmod m_i), \end{aligned} \qquad (1)$$

where $a_i=(\gamma_a,a_i')$, $b_i=(\gamma_b,b_i')$ – input operands represented in the special code of tabular presentation of operands offered in this article (SCTPO). We will write down expression (1) in a this form

$$(\gamma_a,a_i')+(\gamma_b,b_i')=m_i-\left\{\left[m_i-(\gamma_a,a_i')\right]-(\gamma_b,b_i')\right\}. \quad (2)$$

It ensues from expression (2), that for the receipt of result of operation of module summation in SCTPO it is enough to know the result of operation of module deduction, i.e. there is possibility effectively (from point of diminishment of amount of equipment of ROM) to use CTM simultaneously for three module operations: multiplication, summation and deduction. On the basis of expression (2) we will consider a method by means of which it will be possible to carry out implementations of any of three arithmetic operations in SRC: multiplication, summation and deduction. Operation of module summation is carried out by means of the algorithm described by expression (2). We will make the algorithm of implementation of operation of module summation by a table, for implementation of operation of module deduction $(a_i'-b_i')\bmod m_i$. In compliance with expression (2) we will consider the method of realization of operation of module summation.

1. The minuend $a_i=(\gamma_a,a_i')$ is inverted on the module of m_i, i.e. we will get the following expression: $\bar{a}_i=((\gamma_a+1)\bmod 2,a_i')$. We abandon a subtrahend (γ_b,b_i') without the changes.

2. By means of ROM realizing operation of module deduction, on input operands a_i' and b_i' the result of operation is determined as $(a_i'-b_i')\bmod m_i$. As well as for the algorithm of module multiplication the index of γ_i result of operation of module deduction is formed in compliance with the values of indexes of the corresponding operands, i.e. in concordance with the values $(\gamma_a+1)\bmod 2$ and γ_b, where:

$$\gamma_i=\begin{cases}\bar{\gamma},\text{ if } (\gamma_a+1)\bmod 2\neq\gamma_b,\\ \gamma,\text{ if } (\gamma_a+1)\bmod 2=\gamma_b.\end{cases}$$

Consequently, the result of operation of module deduction will have the following form:

$$\left(\gamma_i,(a_i'-b_i')\bmod m_i\right).$$

3. We invert the got result of module deduction on the module of m_i, i.e.

$$\left((\gamma_i+1)\bmod 2,(a_i'-b_i')\bmod m_i\right).$$

For construction of tables of basic arithmetic operations there is most showy application of method of the special encoding, which is described higher, and is allowed simultaneously to decrease the size of tables of summation, deduction and multiplication in four times.

During realization of operations by tabular methods additional diminishment of equipment due to that a not single table is built which will realize a result in a binary code is possible in a number of cases, but k to more shallow tables realizing solutions on each of to digits of result, where k – is register capacity, necessary for storage of number on the examined base $k=\left[\log_2(m_i-1)\right]+1$.

Thus very often unification of tables occurs, i.e. reduction of amount of different types of tables necessary for realization of arithmetic unit. The chart of realization of the generalized $\otimes$ arithmetic operation ($\otimes$ – it is multiplication, summation and deduction) on the arbitrary module of m_i is represented in the table 1, and symmetry in relation to a vertical line, horizontal line and diagonals is similarly indicated. Subject to symmetry of tables of realization of basic arithmetic operations (multiplication, summation and deduction), and also on the basis of the methods of reduction of tables considered above, is information taken in the table 2 ¼ part of table 1, and in particular, its second quadrant. In a table 3 numeric data of the second quadrant of the table 1 are represented in a binary code. On the basis of the table 3 we will take in a table 4 values respective to the first (low-order position) digit of result. Thus for realization of DPS we will use only those table elements (blocks) 4, which correspond to the single values of low-order position digit of result.

Table 1 – Table of realization of the generalized arithmetic operation to the module of m

$b \backslash a$	a_0	…	$a_{\frac{m-1}{2}}$	$a_{\frac{m+1}{2}}$	…	a_{m-1}
b_0	$(a_0 \otimes b_0) \bmod m = c_{00}$	…	$(a_{\frac{m-1}{2}} \otimes b_0) \bmod m = c_{(\frac{m-1}{2})0}$	$(a_{\frac{m+1}{2}} \otimes b_0) \bmod m = c_{(\frac{m+1}{2})0}$	…	$(a_{m-1} \otimes b_0) \bmod m = c_{(m-1)0}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$(a_0 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{0(\frac{m-1}{2})}$	…	$(a_{\frac{m-1}{2}} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(\frac{m-1}{2})(\frac{m-1}{2})}$	$(a_{\frac{m+1}{2}} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(\frac{m+1}{2})(\frac{m-1}{2})}$	…	$(a_{m-1} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(m-1)(\frac{m-1}{2})}$
$b_{\frac{m+1}{2}}$	$(a_0 \otimes b_{\frac{m+1}{2}}) \bmod m = c_{0(\frac{m+1}{2})}$	…	$(a_{\frac{m-1}{2}} \otimes b_{\frac{m+1}{2}}) \bmod m = c_{(\frac{m-1}{2})(\frac{m+1}{2})}$	$(a_{\frac{m+1}{2}} \otimes b_{\frac{m+1}{2}}) \bmod m = c_{(\frac{m+1}{2})(\frac{m+1}{2})}$	…	$(a_{m-1} \otimes b_{\frac{m+1}{2}}) \bmod m = c_{(m-1)(\frac{m+1}{2})}$
…	…	…	…	…	…	…
b_{m-1}	$(a_0 \otimes b_{m-1}) \bmod m = c_{0(m-1)}$	…	$(a_{\frac{m-1}{2}} \otimes b_{m-1}) \bmod m = c_{(\frac{m-1}{2})(m-1)}$	$(a_{\frac{m+1}{2}} \otimes b_{m-1}) \bmod m = c_{(\frac{m+1}{2})(m-1)}$	…	$(a_{m-1} \otimes b_{m-1}) \bmod m = c_{(m-1)(m-1)}$

Table 2 – Second quadrant of the table 1

$b \backslash a$		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		$(a_0 \otimes b_0) \bmod m = c_{00}$	$(a_1 \otimes b_0) \bmod m = c_{10}$	$(a_2 \otimes b_0) \bmod m = c_{20}$		$(a_{\frac{m-1}{2}} \otimes b_0) \bmod m = c_{(\frac{m-1}{2})0}$
b_1	b_{m-1}	$(a_0 \otimes b_1) \bmod m = c_{01}$	$(a_1 \otimes b_1) \bmod m = c_{11}$	$(a_2 \otimes b_1) \bmod m = c_{21}$	…	$(a_{\frac{m-1}{2}} \otimes b_1) \bmod m = c_{(\frac{m-1}{2})1}$
b_2	b_{m-2}	$(a_0 \otimes b_2) \bmod m = c_{02}$	$(a_1 \otimes b_2) \bmod m = c_{12}$	$(a_2 \otimes b_2) \bmod m = c_{22}$	…	$(a_{\frac{m-1}{2}} \otimes b_2) \bmod m = c_{(\frac{m-1}{2})2}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$(a_0 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{0(\frac{m-1}{2})}$	$(a_1 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{1(\frac{m-1}{2})}$	$(a_2 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{2(\frac{m-1}{2})}$	…	$(a_{\frac{m-1}{2}} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(\frac{m-1}{2})(\frac{m-1}{2})}$

Table 3 – Information of the second quadrant of table 1 represented in a binary code

$b \backslash a$		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		$c_{00_k}, c_{00_{(k-1)}}, \dots$ $\dots, c_{00_1}, c_{00_0}$	$c_{10_k}, c_{10_{(k-1)}}, \dots$ $\dots, c_{10_1}, c_{10_0}$	$c_{20_k}, c_{20_{(k-1)}}, \dots$ $\dots, c_{20_1}, c_{20_0}$	…	$c_{(\frac{m-1}{2})0_k}, c_{(\frac{m-1}{2})0_{(k-1)}}, \dots$ $\dots, c_{(\frac{m-1}{2})0_1}, c_{(\frac{m-1}{2})0_0}$
b_1	b_{m-1}	$c_{01_k}, c_{01_{(k-1)}}, \dots$ $\dots, c_{01_1}, c_{01_0}$	$c_{11_k}, c_{11_{(k-1)}}, \dots$ $\dots, c_{11_1}, c_{11_0}$	$c_{21_k}, c_{21_{(k-1)}}, \dots$ $\dots, c_{21_1}, c_{21_0}$	…	$c_{(\frac{m-1}{2})1_k}, c_{(\frac{m-1}{2})1_{(k-1)}}, \dots$ $\dots, c_{(\frac{m-1}{2})1_1}, c_{(\frac{m-1}{2})1_0}$
b_2	b_{m-2}	$c_{02_k}, c_{02_{(k-1)}}, \dots$ $\dots, c_{02_1}, c_{02_0}$	$c_{12_k}, c_{12_{(k-1)}}, \dots$ $\dots, c_{12_1}, c_{12_0}$	$c_{22_k}, c_{22_{(k-1)}}, \dots$ $\dots, c_{22_1}, c_{22_0}$	…	$c_{(\frac{m-1}{2})2_k}, c_{(\frac{m-1}{2})2(k-1)}, \dots$ $\dots, c_{(\frac{m-1}{2})2_1}, c_{(\frac{m-1}{2})2_0}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_k}, c_{0(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{0(\frac{m-1}{2})_1}, c_{0(\frac{m-1}{2})_0}$	$c_{1(\frac{m-1}{2})_k}, c_{1(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{1(\frac{m-1}{2})_1}, c_{1(\frac{m-1}{2})_0}$	$c_{2(\frac{m-1}{2})_k}, c_{2(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{2(\frac{m-1}{2})_1}, c_{2(\frac{m-1}{2})_0}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_k}, c_{(\frac{m-1}{2})(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{(\frac{m-1}{2})(\frac{m-1}{2})_1}, c_{(\frac{m-1}{2})(\frac{m-1}{2})_0}$

By a similar appearance, based on a table 3, we will take in the tables of 5-7 values the proper to the second, *k-1* and *k* (*high-order position*) the digits of result of the generalized arithmetic operation.

Table 4 – Values of the first digit of result of the table 3

a / b		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		c_{00_0}	c_{10_0}	c_{20_0}	…	$c_{(\frac{m-1}{2})0_0}$
b_1	b_{m-1}	c_{01_0}	c_{11_0}	c_{21_0}	…	$c_{(\frac{m-1}{2})1_0}$
b_2	b_{m-2}	c_{02_0}	c_{12_0}	c_{22_0}	…	$c_{(\frac{m-1}{2})2_0}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_0}$	$c_{1(\frac{m-1}{2})_0}$	$c_{2(\frac{m-1}{2})_0}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_0}$

Table 5 – Values of the second digit of result of the table 3

a / b		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		c_{00_1}	c_{10_1}	c_{20_1}	…	$c_{(\frac{m-1}{2})0_1}$
b_1	b_{m-1}	c_{01_1}	c_{11_1}	c_{21_1}	…	$c_{(\frac{m-1}{2})1_1}$
b_2	b_{m-2}	c_{02_1}	c_{12_1}	c_{22_1}	…	$c_{(\frac{m-1}{2})2_1}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_1}$	$c_{1(\frac{m-1}{2})_1}$	$c_{2(\frac{m-1}{2})_1}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_1}$

Table 6 – Values of the $k-1$ digit of result of the table 3

a / b		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		$c_{00_{(k-1)}}$	$c_{10_{(k-1)}}$	$c_{20_{(k-1)}}$	…	$c_{(\frac{m-1}{2})0_{(k-1)}}$
b_1	b_{m-1}	$c_{01_{(k-1)}}$	$c_{11_{(k-1)}}$	$c_{21_{(k-1)}}$	…	$c_{(\frac{m-1}{2})1_{(k-1)}}$
b_2	b_{m-2}	$c_{02_{(k-1)}}$	$c_{12_{(k-1)}}$	$c_{22_{(k-1)}}$	…	$c_{(\frac{m-1}{2})2_{(k-1)}}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_{(k-1)}}$	$c_{1(\frac{m-1}{2})_{(k-1)}}$	$c_{2(\frac{m-1}{2})_{(k-1)}}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_{(k-1)}}$

In spite of the fact that the size of every table is diminished and was multiplied the amount of tables, on the whole gaining in an amount the equipment takes place, as to the limit surplus of tables is brief and, as we see, the blocks of table, which correspond to the significant digits of result, will be realized only. Because the result of operation appears by an absolute code, there is no necessity in logical elements forming of the SCTPO index.

Table 7 – Values of the k digit of result of the table 3

b \ a		a_0	a_1	a_2	$\ldots$	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	$\ldots$	$a_{\frac{m+1}{2}}$
b_0		c_{00_k}	c_{10_k}	c_{20_k}	$\ldots$	$c_{(\frac{m-1}{2})0_k}$
b_1	b_{m-1}	c_{01_k}	c_{11_k}	c_{21_k}	$\ldots$	$c_{(\frac{m-1}{2})1_k}$
b_2	b_{m-2}	c_{02_k}	c_{12_k}	c_{22_k}	$\ldots$	$c_{(\frac{m-1}{2})2_k}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_k}$	$c_{1(\frac{m-1}{2})_k}$	$c_{2(\frac{m-1}{2})_k}$	$\ldots$	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_k}$

The results of calculation of amount of logical elements during complete and bit-by-bit tabular realization of tables of the DPS operation device (OD) are resulted in the table 8. It is visible from the table 8, that tabular realization of arithmetic operations in BNS is not effective, and with the increase of digit grid of OD is impracticable.

Table 8 – Results of calculation of amount of equipment of the DPS OD

Capa-city (l)	BNS	Modules of SRC	Complete tabular realization	Bit-by-bit tabular realization	Gain [%]
l=1	$2^8 \cdot 2^8 = 2^{16}$	m=3, m=4, m=5, m=7	263	132	49,81
l=2	$2^{16} \cdot 2^{16} = 2^{32}$	m=2, m=5, m=7, m=9, m=11, m=13	1259	546	56,63
l=3	$2^{24} \cdot 2^{24} = 2^{48}$	m=3, m=4, m=5, m=11, m=13, m=17, m=19	2833	1433	49,42
l=4	$2^{32} \cdot 2^{32} = 2^{64}$	m=2, m=3, m=5, m=7, m=11, m=13, m=17, m=19, m=23, m=29	6943	3788	45,44
l=8	$2^{64} \cdot 2^{64} = 2^{128}$	m=2, m=3, m=5, m=7, m=11, m=13, m=17, m=19, m=23, m=29, m=31, m=37, m=41, m=43, m=47, m=53	39079	24914	36,25

At the same time application of the SRC allows effectively (from point of increase of productivity and diminishment of amount of equipment of matrix circuit) to apply the tabular methods of realization of arithmetic operations.

Conclusion

Thus, the method of increase of productivity and reliability of the real-time DPS which functions in the SRC is offered in the article. Productivity of calculations of the DPS in the SRC rises due to the use of tabular principle of realization of arithmetic operations by introduction and use of SCTPO. Reliability of functioning of the DPS in the SRC rises due to diminution of intensity of refusals of tabular circuits of realization of arithmetic operations by diminution on 40-60% (depending on a computer word length) of amount of equipment of the DPS OP.

References

[1] Akushskii I. Ya., Yuditskii D. I. Mashinnaya arifmetika v ostatochnykh klassakh. – M.: Sov. radio, 1968. – 440 s.
[2] Kuznecov O. O., Olijnykov R. V., Gorbenko Ju. I., Pushkar'ov A. I., Dyrda O. V., Gorbenko I. D. Obg'runtuvannja vymog, pobuduvannja ta analiz perspektyvnyh symetrychnyh kryptoperetvoren' na osnovi blochnyh shyfriv // Visnyk Nacional'nogo universytetu "L'vivs'ka politehnika". – 2014. – № 806: Komp'juterni systemy ta merezhi. – S. 124 – 141.
[3] Koshman S. A., Deren'ko S. N., Krasnobaev V. A. Tablichnyi metod obrabotki tsifrovoi informatsii v klasse vychetov // Radioelektronni i komp'juterni systemy. – 2006. - № 5 (17). – S. 171–175.
[4] Kuznetsov A. A., Shvager A. S., Fesenko D. A. Sokrytie dannykh v klasternykh failovykh sistemakh // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Khar'kov: KhNURE.–2015. – Vyp. 181. – S. 86-100.
[5] Kuznetsov A. A., Smirnov A. A., Sai V. N. Diskretnye signaly s mnogourovnevoi funktsiei korrelyatsii // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Khar'kov: KhTURE.–2011. – Vyp. 166. – S. 142-152.
[6] 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. – November 2014. – Volume 50, Issue 6, pp 969-976.
[7] Koshman S. O., Barsov V. I., Krasnobajev V. A. Dyversnist' tablychnyh metodiv realizacii' aryfmetychnyh operacij u systemi zalyshkovyh klasiv // Problemy energozabezpechennja ta energozberezhennja v APK Ukrai'ny: Visnyk HNTUSG imeni Petra Vasylenka, vyp. 73, tom 2. - Harkiv, 2008. - S. 70-72.
[8] 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. – January 2016. – Volume 52, Issue 1, pp. 145-150.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua

Надійшло: Серпень 2016

Автори:
Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: krasnobaev_va@rambler.ru
Аліна Янко, аспірантка, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.
E-mail: al9_yanko@ukr.net
Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна.
E-mail: s_koshman@ukr.net

Метод табличної реалізації арифметичних операцій в системі залишкових класів.
Анотація. У статті запропонований метод підвищення продуктивності та надійності функціонування системи обробки інформації заснований на використовуванні непозиційної системи числення у залишкових класах (СЗК). Розроблений метод враховує властивості симетрії таблиць реалізації основних арифметичних операцій і заснований на використовуванні ¼ частини числових даних сукупності таблиць, що реалізовують модульні операції множення, складання та віднімання у СЗК. Метод порозрядній табличній реалізації рекомендований у системах цифрової обробки інформації для підвищення продуктивності рішення обчислювальних задач.

Ключові слова: продуктивність, надійність, система числення у залишкових класах, система обробки інформації, спеціальний код табличного представлення операндів.

Рецензент: Александр Кузнецов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Поступила: Август 2016

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: krasnobaev_va@rambler.ru
Алина Янко, аспирантка, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.
E-mail: al9_yanko@ukr.net
Сергей Кошман, к.т.н., доцент, Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина.
E-mail: s_koshman@ukr.net

Метод табличной реализации арифметических операций в системе остаточных классов.

Аннотация. В статье предложен метод повышения производительности и надёжности функционирования системы обработки информации основанный на использовании непозиционной системы счисления в остаточных классах (СОК). Разработанный метод учитывает свойства симметрии таблиц реализации основных арифметических операций и основан на использовании ¼ части числовых данных совокупности таблиц, реализующих модульные операции умножение, сложение и вычитание в СОК. Метод поразрядной табличной реализации рекомендован в системах цифровой обработки информации для повышения производительности решения вычислительных задач.

Ключевые слова: производительность, надёжность, система счисления в остаточных классах, система обработки информации, специальный код табличного представления операндов.