ISSN 0146-4116, Automatic Control and Computer Sciences, 2010, Vol. 44, No. 5, pp. 292–301. © Allerton Press, Inc., 2010.
Original Russian Text © V.P. Suprun, D.A. Gorodecky, 2010, published in Avtomatika i Vychislitel'naya Tekhnika, 2010, No. 5, pp. 59–71.

# Realization of Addition and Multiplication Operations in Unitary Codes

**V. P. Suprun and D. A. Gorodecky**

*Belarusian State University, Faculty of Mechanics and Mathematics, pr. Nezavisimosti 4, Minsk, 220030 Belarus*
*e-mail: suprun@bsu.by, danila.gorodecky@gmail.com*

Received June 22, 2010

**Abstract**—This article discusses the implementation of the basic operations of modular arithmetic, addition and multiplication, for the case of data presentation in unitary codes. Analytical descriptions of the functions that are implemented at the outputs of the modular adder and the modular multiplier are proposed. We give logical schemes of the adder and multiplier by modulo three. These schemes are more efficient compared to their counterparts.

**Keywords:** modular arithmetic, computing device, unitary codes, modular adder, modular multiplier logic scheme

**DOI:** 10.3103/S014641161005007X

## 1. INTRODUCTION

The use of a modular arithmetic apparatus allows us to improve the performance of computing devices through parallel and independent processing of digital signals. The modular presentation of information provides more reliable detection and correction of errors in its storage and transfer, as well as the performance (computing) of arithmetic operations [1, 2].

At present, a number of methods of synthesis of adders and multipliers for a given modulo have been developed (see, for example, [2–5]).

In this paper the synthesis of devices that implement the double arithmetic operations of addition and multiplication in unitary codes by modulo $P$ is shown. As an example, we considered in detail the implementation of these operations for the values of the modulo $P = 3$ and $P = 5$. This paper gives a schematic diagram that implements some superposition of these operations. This scheme is synthesized by applying the method of block-structured synthesis [6].

## 2. BASIC CONCEPTS AND PROPERTIES

Application of unitary codes is widespread in the computing method of data presentation. Operand $A$ in a unitary code by modulo $P$ is represented by means of a $p$-bit binary vector $(a_0, a_1, ..., a_{p-1})$, where $a_i = 1$ if and only if where $A \equiv i \pmod P$, where $i = 0, 1, ..., p - 1$.

Since the binary vector $(a_0, a_1, ..., a_{p-1})$ contains exactly one unit, then the following equality is true:

$$a_0 + ... + a_{i-1} + a_i + a_{i+1} + ... + a_{p-1} = 1, \quad (1)$$

which, given the fact that $1 - a_i = \bar{a}_i$, is equivalent to the expression

$$a_0 + ... + a_{i-1} + a_{i+1} + ... + a_{p-1} = \bar{a}. \quad (2)$$

Devices that implement the operations of addition $A + B = S \pmod P$ and multiplying $A \cdot B = R \pmod P$ in unitary codes by modulo $P$ will be denoted as $\Re_1$ (modular adder) and $\Re_2$ (modular multiplier), respectively. Input $A$, $B$ and output $S$, $R$ operands are defined by $p$-bit unitary binary vectors

$$A = (a_0, a_1, ..., a_{p-1}),\ B = (b_0, b_1, ..., b_{p-1}),\ S = (s_0, s_1, ..., s_{p-1}) \text{ and } R = (r_0, r_1, ..., r_{p-1}),$$

where $s_k = 1$ and $r_k = 1$ if and only if $A + B = k \pmod P$ and $A \cdot B = k \pmod P$, respectively, where $k = 0, 1, ..., p - 1$.

The main property of logic functions

$$S_k = S_k(a_0, a_1, ..., a_{p-1}, b_0, b_1, ..., b_{p-1}) \text{ and } R_k = R_k(a_0, a_1, ..., a_{p-1}, b_0, b_1, ..., b_{p-1}),$$

which are realized at the output of $\Re_1$ and $\Re_2$, respectively, where $k = 0, 1, ..., p-1$, can be formulated with help of the following two assertions.

**Assertion 1.** The definition of the operation $A + B = S \pmod P$ implies that $S_k = 1$ if and only if $a_i + b_j = 2$, where $i + j = k \pmod P$ and $i, j = 0, 1, ..., p-1$.

**Assertion 2.** The definition of $A \cdot B = R \pmod P$ implies that $R_k = 1$ if and only if $a_i + b_j = 2$, where $i \cdot j = k \pmod P$ and $i, j = 0, 1, ..., p-1$.

Later, as a criterion of the optimality of the scheme $S(\Re)$ of computing device $\Re$, we will use its characteristics such as complexity of $l(\Re)$ (number of inputs of the logic elements), the depth $g(\Re)$ (which usually determines the performance of the scheme), and the number of external leads $m(\Re)$. In this regard, the effectiveness of the synthesized logic circuits below $S(\Re_1)$, $S(\Re_2)$, $S(\Re^*)$ of the devices $\Re_1$, $\Re_2$, $\Re^*$ will be evaluated against the values of these characteristics.

In the following are given the analytical representations of functions that are implemented at the outputs of the adder $\Re_1$ and multiplier $\Re_2$ for the condition that $P = 3$ and $P = 5$.

## 3. ADDITION OF UNITARY CODES BY MODULO THREE

Consider the addition operation $A + B = S \pmod 3$ in unitary codes, where $A = (a_0, a_1, a_2)$, $B = (b_0, b_1, b_2)$, $S = (s_0, s_1, s_2)$, and $S_k = 1$ if and only if $A + B = k \pmod 3$ and $k = 0, 1, 2$.

Assertion 1 implies that the logical functions $S_0$, $S_1$, and $S_2$ realized at the output of the adder $\Re_1$ can be represented as

—$S_0 = 1$ if and only if $a_0 + b_0 = 2$, $a_1 + b_2 = 2$ or $a_2 + b_1 = 2$;

—$S_1 = 1$ if and only if $a_0 + b_1 = 2$, $a_1 + b_0 = 2$ or $a_2 + b_2 = 2$;

—$S_2 = 1$ if and only if $a_0 + b_2 = 2$, $a_1 + b_1 = 2$ or $a_2 + b_0 = 2$.

Simpler analytical descriptions of the functions $S_0$, $S_1$, and $S_2$ are represented by the following assertion.

**Assertion 3.** The function $S_0 = 1$ if and only if $a_1 + b_1 = a_2 + b_2$, the function $S_1 = 1$ if and only if $a_0 + b_0 = a_1 + b_1$, and function $S_2 = 1$ if and only if $a_0 + b_0 = a_2 + b_2$.

***Proof.*** To prove the assertion for the function $S_0$, it is necessary to consider three cases, namely, the conditions $a_0 + b_0 = 2$, $a_1 + b_2 = 2$, and $a_2 + b_1 = 2$. For this we will use property (1) of unitary binary code $A = (a_0, a_1, a_2)$ and $B = (b_0, b_1, b_2)$ of the form $a_0 + a_1 + a_2 = 1$ and $b_0 + b_1 + b_2 = 1$.

If $a_0 + b_0 = 2$, then $a_0 = 1$, $b_0 = 1$ and $a_1 = a_2 = b_1 = b_2 = 0$, i.e., $a_1 + b_1 = a_2 + b_2 = 0$.

If $a_1 + b_2 = 2$, then $a_1 = 1$, $b_2 = 1$ and $a_2 = b_1 = 0$, i.e., $a_1 + b_1 = a_2 + b_2 = 1$.

If $a_2 + b_1 = 2$, then $a_2 = 1$, $b_1 = 1$ and $a_1 = b_2 = 0$, i.e., $a_1 + b_1 = a_2 + b_2 = 1$.

The proof for the functions $S_1$ and $S_2$ is carried out by analogy.

Hence, the functions $S_0$, $S_1$, $S_2$ can be represented as follows:

$$S_0 = \begin{cases} 1, & \text{if } a_1 + b_1 = a_2 + b_2; \\ 0, & \text{otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, & \text{if } a_0 + b_0 = a_1 + b_1; \\ 0, & \text{otherwise,} \end{cases} \tag{3}$$

$$S_2 = \begin{cases} 1, & \text{if } a_0 + b_0 = a_2 + b_2; \\ 0, & \text{otherwise.} \end{cases}$$

Taking into account the equality $1 - a_2 = \bar{a}_2$ and $1 - b_2 = \bar{b}_2$, it can be argued that the conditions for $a_1 + b_1 = a_2 + b_2$ and $a_1 + b_1 + \bar{a}_2 + \bar{b}_2 = 2$ are equivalent (by analogy with these conditions, the following

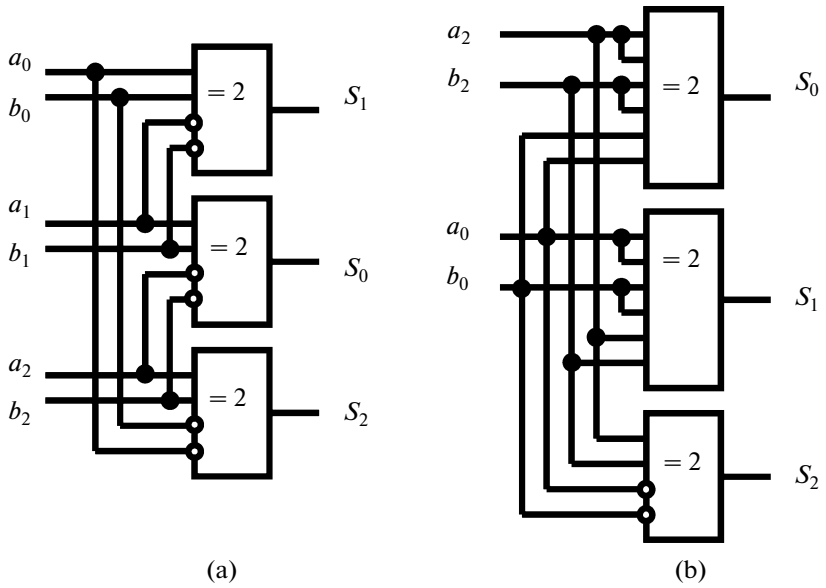


**Fig. 1.** Logic schemes of modular adder $\Re_1$(a) the scheme of $S_1(\Re_1)$; (b) the scheme of $S_2(\Re_1)$.

conditions are equivalent: $a_0 + b_0 = a_1 + b_1$ and $a_0 + b_0 + \bar{a}_1 + \bar{b}_1 = 2$,as well as $a_0 + b_0 = a_2 + b_2$ and $\bar{a}_0 + \bar{b}_0 + a_2 + b_2 = 2$).

In this regard, the representation of functions $S_0$, $S_1$, $S_2$ by (3) can be rewritten as

$$S_0 = \begin{cases} 1, & \text{if } a_1 + \bar{a}_2 + b_1 + \bar{b}_2 = 2; \\ 0, & \text{otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, & \text{if } a_0 + \bar{a}_1 + b_0 + \bar{b}_1 = 2; \\ 0, & \text{otherwise,} \end{cases} \qquad (4)$$

$$S_2 = \begin{cases} 1, & \text{if } \bar{a}_0 + a_2 + \bar{b}_0 + b_2 = 2; \\ 0, & \text{otherwise.} \end{cases}$$

Figure 1(a) shows the logical scheme $S_1(\Re_1)$ of the adder $\Re_1$, synthesized on the basis of representations (4). Scheme $S_1(\Re_1)$ consists of three logical elements EXCLUSIVE OR with a threshold two and has the following characteristics: $l(\Re_1) = 12$, $g(\Re_1) = 1$, and $m(\Re_1) = 9$.

Since property (1) means that $a_1 = 1 - a_0 - a_2$ and $b_1 = 1 - b_0 - b_2$, then the following chain of equivalent transformations is true:

$$a_1 + \bar{a}_2 + b_1 + \bar{b}_2 = 2, \quad (1 - a_0 - a_2) + \bar{a}_2 + (1 - b_0 - b_2) + \bar{b}_2 = 2,$$
$$1 - a_0 - a_2 + (1 - a_2) + 1 - b_0 - b_2 + (1 - b_2) = 2, \quad a_0 + 2a_2 + b_0 + 2b_2 = 2.$$

Since $\bar{a}_1 = a_0 + a_2$ and $\bar{b}_1 = b_0 + b_2$, then the conditions $a_0 + \bar{a}_1 + b_0 + \bar{b}_1 = 2$ and $2a_0 + a_2 + 2b_0 + b_2 = 2$ are also equivalent.

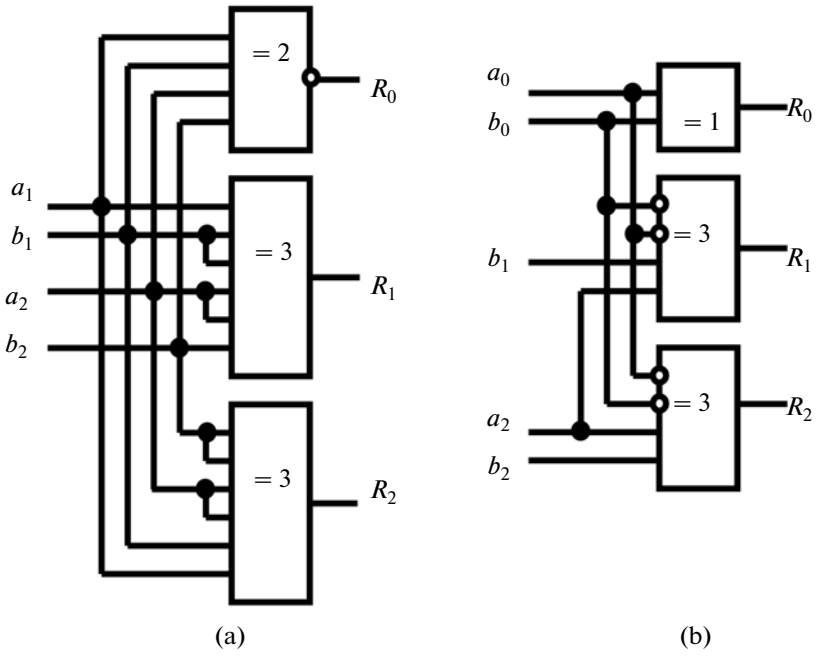


**Fig. 2.** Logic schemes of the modular multiplier $\Re_2$ (a) the scheme $S_1(\Re_2)$, (b) the scheme $S_2(\Re_2)$.

In this regard, the system of representations (4) is equivalent to the system

$$S_0 = \begin{cases} 1, & \text{if } a_0 + 2a_2 + b_0 + 2b_2 = 2; \\ 0, & \text{otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, & \text{if } 2a_0 + a_2 + 2b_0 + b_2 = 2; \\ 0, & \text{otherwise,} \end{cases} \qquad (5)$$

$$S_2 = \begin{cases} 1, & \text{if } \bar{a}_0 + a_2 + \bar{b}_0 + b_2 = 2; \\ 0, & \text{otherwise.} \end{cases}$$

Figure 1(b) shows the logical scheme of $S_2(\Re_1)$ of the adder $\Re_1$ synthesized on the basis of formulas (5). The scheme $S_2(\Re_1)$ contains three elements EXCLUSIVE OR with threshold two and has the characteristics $l(\Re_1) = 16$, $g(\Re_1) = 1$, and $m(\Re_1) = 7$.

The main advantage of the logic circuit is the minimumy number of $S_2(\Re_1)$ external findings, equal to seven (four inputs and three outputs).

Logic circuits $S_1(\Re_1)$ and $S_2(\Re_1)$ (Fig. 1) of the adder of unitary codes by modulo three $\Re_1$ are more effective in complexity, depth, or the number of external leads in comparison with all known analogs (see, for example, invention patents Republic of Belarus 13247, 3270, 2473, 2314, and 2305).

## 4. MULTIPLICATION OF UNITARY CODES FOR MODULO THREE

Consider the multiplication operation $A \cdot B = R \pmod 3$ in the unitary codes, where $A = (a_0, a_1, a_2)$, $B = (b_0, b_1, b_2)$, $R = (r_0, r_1, r_2)$, and $R_k = 1$ if and only if $A \cdot B = k \pmod 3$ and $k = 0, 1, 2$.

From Assertion 2 it follows that the logic functions $R_0$, $R_1$, and $R_2$ implemented at the outputs of the multiplier $\Re_2$ can be represented as

—$R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$;

—$R_1 = 1$ if and only if $a_1 + b_1 = 2$ or $a_2 + b_2 = 2$;

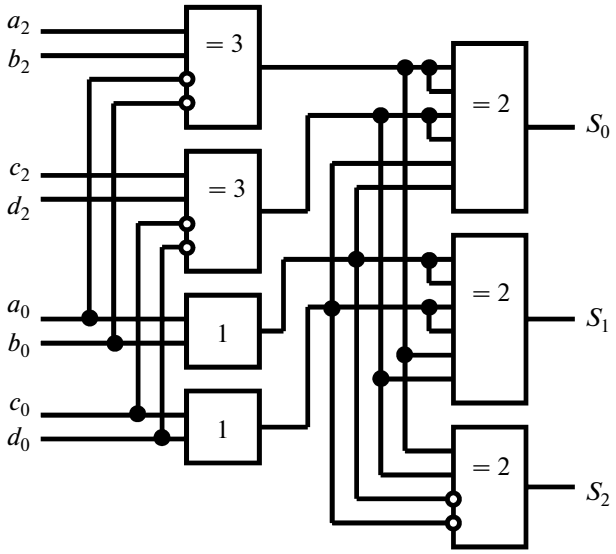


**Fig. 3.** The logic scheme $S(\mathfrak{R}^*)$ of the computing device $\mathfrak{R}^*$.

—$R_2 = 1$ if and only if $a_1 + b_2 = 2$ or $a_2 + b_1 = 2$.

A simple analytical description of the functions $R_0$, $R_1$, and $R_2$ is represented by the following assertions.

**Assertion 4.** The function $R_0 = 0$ if and only if the condition $a_1 + a_2 + b_1 + b_2 = 2$, the function $R_1 = 1$ if and only if the condition $a_1 + 2a_2 + 2b_1 + b_2 = 3$; and function $R_2 = 1$ if and only if the condition $a_1 + 2a_2 + b_1 + 2b_2 = 3$.

***Proof.*** Thus, a function of $R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$, then $R_0 = 0$ if and only if $a_0 + b_0 = 0$, i.e., $a_1 + a_2 + b_1 + b_2 = 2$.

The condition of $a_1 + b_1 = 2$ is equivalent to $a_1 = b_1 = 1$, and the condition $a_2 + b_2 = 2$ is equivalent to $a_2 = b_2 = 1$. In this regard, a combination of two terms of $a_1 + b_1 = 2$ or $a_2 + b_2 = 2$ is equivalent to one condition $a_1 + 2a_2 + 2b_1 + b_2 = 3$.

Similarly, the set of conditions $a_1 + b_2 = 2$ or $a_2 + b_1 = 2$ is equivalent to one condition $a_1 + 2a_2 + b_1 + 2b_2 = 3$.

Figure 2(a) shows the logical scheme of $S_1(\mathfrak{R}_2)$ of the multiplier $\mathfrak{R}_2$ which contains an elment EXCLUSIVE OR with the threshold of two and two elements EXCLUSIVE OR with a threshold of three. Scheme $S_1(\mathfrak{R}_2)$ has the following characteristics: $l(\mathfrak{R}_2) = 16$, $g(\mathfrak{R}_2) = 1$, and $m(\mathfrak{R}_2) = 7$ (Patent invention Republic of Belarus 12448).

In Fig. 2(a) scheme $S_1(\mathfrak{R}_2)$ exceeds the existing analogs in some characteristics (see, for example, patents for invention Republic of Belarus 6568, 12000).

It should be noted that there are simpler analytical representations of logic functions $R_0$, $R_1$, $R_2$.

**Proposition 5.** The function $R_0 = 1$ if and only if the condition $a_0 \vee b_0 = 1$ holds, the function $R_1 = 1$ if and only if the condition $a_2 + b_1 + \bar{a}_0 + \bar{b}_0 = 3$ holds (or $a_1 + b_2 + \bar{a}_0 + \bar{b}_0 = 3$), the function $R_2 = 1$ if and only if the condition $a_2 + b_2 + \bar{a}_0 + \bar{b}_0 = 3$ holds.

***Proof.*** Since the function $R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$, then $R_0 = a_0 \vee b_0$.

Properties of unitary codes (1) and (2) at the condition that P = 3, take the form $a_0 + a_1 + a_2 = 1$, $b_0 + b_1 + b_2 = 1$, $a_1 + a_2 = \bar{a}_0$, and $b_1 + b_2 = \bar{b}_0$. Then the following two chains of equivalent transformations will hold:

$$1)\ a_1 + 2a_2 + 2b_1 + b_2 = 3, \quad a_1 + 2a_2 + 2b_1 + b_2 = 1 + (a_0 + a_1 + a_2) + (b_0 + b_1 + b_2),$$
$$a_2 + b_1 = 1 + a_0 + b_0, \quad a_2 + b_1 - a_0 - b_0 = 1, \quad a_2 + b_1 + \bar{a}_0 + \bar{b}_0 = 3;$$
$$2)\ a_1 + 2a_2 + b_1 + 2b_2 = 3, \quad a_1 + 2a_2 + b_1 + 2b_2 = 1 + (a_0 + a_1 + a_2) + (b_0 + b_1 + b_2),$$
$$a_2 + b_2 = 1 + a_0 + b_0, \quad a_2 + b_2 - a_0 - b_0 = 1, \quad a_2 + b_2 + \bar{a}_0 + \bar{b}_0 = 3.$$

In accordance with the assertion proved above, logic functions $R_0$, $R_1$, $R_2$ can be represented as follows:

$$R_0 = a_0 \vee b_0,$$
$$R_1 = \begin{cases} 1, & \text{if } \bar{a}_0 + \bar{b}_0 + a_2 + b_1 = 3; \\ 0, & \text{otherwise,} \end{cases} \tag{6}$$
$$R_2 = \begin{cases} 1, & \text{if } \bar{a}_0 + \bar{b}_0 + a_2 + b_2 = 3; \\ 0, & \text{otherwise.} \end{cases}$$

Figure 2(b) shows a logic circuit $S_2(\Re_2)$ synthesized by using (6). The scheme $S_2(\Re_2)$ contains an element OR and two elements EXCLUSIVE OR with a threshold of three and has the following characteristics: $l(\Re_2) = 10$, $g(\Re_2) = 1$, and $m(\Re_2) = 8$.

The scheme $S_1(\Re_2)$ has a smaller number of external leads, and the scheme $S_2(\Re_2)$ has less complexity (by the number of inputs of logic elements).

## 5. COMPUTATIONAL DEVICE FOR MODULO THREE

Let the device $\Re$ implement some superposition of the operations of addition and multiplication. In the synthesis of the device, $\Re$ can use a block-structured method of logic synthesis [6]. The method consists of the following. Originally it is formed by the structure of the device $\Re$, consisting of interconnected "units," realizing the arithmetic operations of addition and multiplication. Then each of the "units" is replaced by a suitable (for this structure) logic scheme.

As an example, consider the problem of synthesizing device $\Re^*$, designed for implementation in the unitary codes of arithmetic operation $A \cdot B + C \cdot D = S \pmod 3$.

The structure of the device $\Re^*$ contains one "unit" of addition and two "units" of multiplication. If we substitute the "units" into the appropriate logic schemes $S_2(\Re_1)$ and $S_2(\Re_2)$ which are shown in Fig. 1(b) and Fig. 2(b), we obtain a logic scheme $S(\Re^*)$ of the device $\Re^*$, shown in Fig. 3.

The logic scheme $S(\Re^*)$ contains two elements OR, two elements EXCLUSIVE OR with a threshold of three, and three elements EXCLUSIVE OR with a threshold of two and has the following characteristics: $l(\Re^*) = 28$, $g(\Re^*) = 2$, and $m(\Re^*) = 11$. The logic scheme $S(\Re^*)$ is more effective compared with their counterparts (see the patent for the invention Republic of Belarus 9341, 10535).

## 6. ADDITION OF UNITARY CODES BY MODULO FIVE

Consider the addition operation A + B = S (mod 5) in unitary codes, where

$$A = (a_0, a_1, a_2, a_3, a_4),\ B = (b_0, b_1, b_2, b_3, b_4),\ S = (s_0, s_1, s_2, s_3, s_4), \text{ and } S_k = 1$$

if and only if $A + B = k \pmod 5$, where $k = 0, 1, 2, 3, 4$.

Assertion 1 implies that the logic functions of $S_0$, $S_1$, $S_2$, $S_3$, and $S_4$ realized at the output of the adder $\Re_1$ can be represented as

—$S_0 = 1$ if and only if either of the equalities holds $a_0 + b_0 = 2, a_1 + b_4 = 2, a_2 + b_3 = 2, a_3 + b_2 = 2, a_4 + b_1 = 2$;
—$S_1 = 1$ if and only if either of the equalities holds $a_0 + b_1 = 2, a_1 + b_0 = 2, a_2 + b_4 = 2, a_3 + b_3 = 2, a_4 + b_2 = 2$;
—$S_2 = 1$ if and only if either of the equalities holds $a_0 + b_2 = 2, a_1 + b_1 = 2, a_2 + b_0 = 2, a_3 + b_4 = 2, a_4 + b_3 = 2$;
—$S_3 = 1$ if and only if either of the equalities holds $a_0 + b_3 = 2, a_1 + b_2 = 2, a_2 + b_1 = 2, a_3 + b_0 = 2, a_4 + b_4 = 2$;
—$S_4 = 1$ if and only if either of the equalities holds $a_0 + b_4 = 2, a_1 + b_3 = 2, a_2 + b_2 = 2, a_3 + b_1 = 2, a_4 + b_0 = 2$.

In the following we will give simpler analytical descriptions of the functions $S_0$, $S_1$, $S_2$, $S_3$, $S_4$.

**Assertion 6.** The function $S_0 = 1$ if and only if $a_1 + b_1 = a_4 + b_4$ and $a_2 + b_2 = a_3 + b_3$, the function $S_1 = 1$ if and only if $a_0 + b_0 = a_1 + b_1$ and $a_2 + b_2 = a_4 + b_4$; function $S_2 = 1$ if and only if $a_0 + b_0 = a_2 + b_2$ and $a_3 + b_3 = a_4 + b_4$; function $S_3 = 1$ if and only if $a_0 + b_0 = a_3 + b_3$ and $a_1 + b_1 = a_2 + b_2$, the function $S_4 = 1$ if and only when $a_0 + b_0 = a_4 + b_4$ and $a_1 + b_1 = a_3 + b_3$.

***Proof.*** To prove the assertion (relative to the description of the function $S_0$) we should consider five cases, i.e., $a_0 + b_0 = 2$, $a_1 + b_4 = 2$, $a_2 + b_3 = 2$, $a_3 + b_2 = 2$, and $a_4 + b_1 = 2$.

If $a_0 + b_0 = 2$, then $a_0 = 1$ and $b_0 = 1$. Then $a_1 + b_1 = a_4 + b_4 = a_2 + b_2 = a_3 + b_3 = 0$, i.e., $a_1 + b_1 = a_4 + b_4$ and $a_2 + b_2 = a_3 + b_3$.

If $a_1 + b_4 = 2$, then $a_1 = 1$ and $b_4 = 1$. Then $a_1 + b_1 = a_4 + b_4 = 1$ and $a_2 + b_2 = a_3 + b_3 = 0$.

If $a_2 + b_3 = 2$, then $a_2 = 1$ and $b_3 = 1$. Then $a_1 + b_1 = a_4 + b_4 = 0$ and $a_2 + b_2 = a_3 + b_3 = 1$.

If $a_3 + b_2 = 2$, then $a_3 = 1$ and $b_2 = 1$. Then $a_1 + b_1 = a_4 + b_4 = 0$ and $a_2 + b_2 = a_3 + b_3 = 1$.

If $a_4 + b_1 = 2$, then $a_4 = 1$ and $b_1 = 1$. Then $a_1 + b_1 = a_4 + b_4 = 1$ and $a_2 + b_2 = a_3 + b_3 = 0$.

Hence, the validity of the assertion for the function $S_0$ follows. The allegations regarding the remaining functions $S_1$, $S_2$, $S_3$, and $S_4$ are proved by a similar scheme.

As

$$\bar{a}_3 = 1 - a_3, \quad \bar{b}_3 = 1 - b_3, \quad \bar{a}_4 = 1 - a_4, \quad \text{and} \quad \bar{b}_4 = 1 - b_4,$$

it can be argued that the conditions

$$a_1 + b_1 = a_4 + b_4 \text{ and } a_2 + b_2 = a_3 + b_3$$

are equivalent to the conditions

$$a_1 + b_1 + \bar{a}_4 + \bar{b}_4 = 2 \quad \text{and} \quad a_2 + b_2 + \bar{a}_3 + \bar{b}_3 = 2.$$

Similarly, we can prove that the conditions

$$a_0 + b_0 = a_1 + b_1 \quad \text{and} \quad a_2 + b_2 = a_4 + b_4, \; a_0 + b_0 = a_2 + b_2 \quad \text{and} \quad a_3 + b_3 = a_4 + b_4,$$
$$a_0 + b_0 = a_3 + b_3 \quad \text{and} \quad a_1 + b_1 = a_2 + b_2, \; a_0 + b_0 = a_4 + b_4 \quad \text{and} \quad a_1 + b_1 = a_3 + b_3;$$

are equivalent to the conditions

$$a_0 + b_0 = \bar{a}_1 + \bar{b}_1 = 2 \quad \text{and} \quad a_2 + b_2 = \bar{a}_4 + \bar{b}_4 = 2, \; a_0 + b_0 = \bar{a}_2 + \bar{b}_2 = 2 \quad \text{and} \quad a_3 + b_3 = \bar{a}_4 + \bar{b}_4 = 2,$$
$$a_0 + b_0 = \bar{a}_3 + \bar{b}_3 = 2 \quad \text{and} \quad a_1 + b_1 = \bar{a}_2 + \bar{b}_2 = 2, \; a_0 + b_0 = \bar{a}_4 + \bar{b}_4 = 2 \quad \text{and} \quad a_1 + b_1 = \bar{a}_3 + \bar{b}_3 = 2,$$

respectively.

Based on the above reasoning, it follows that the description of logic functions $S_0$, $S_1$, $S_2$, $S_3$, $S_4$ through the assertion 6, is equivalent to the system of conditions

$$S_0 = \begin{cases} 1, & \text{if } a_1 + b_1 + \bar{a}_4 + \bar{b}_4 = 2 \text{ and } a_2 + b_2 + \bar{a}_3 + \bar{b}_3 = 2, \\ 0, & \text{otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, & \text{if } a_0 + b_0 + \bar{a}_1 + \bar{b}_1 = 2 \text{ and } a_2 + b_2 + \bar{a}_4 + \bar{b}_4 = 2, \\ 0, & \text{otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, & \text{if } a_0 + b_0 + \bar{a}_2 + \bar{b}_2 = 2 \text{ and } a_3 + b_3 + \bar{a}_4 + \bar{b}_4 = 2, \\ 0, & \text{otherwise,} \end{cases} \tag{7}$$

$$S_3 = \begin{cases} 1, & \text{if } a_0 + b_0 + \bar{a}_3 + \bar{b}_3 = 2 \text{ and } a_1 + b_1 + \bar{a}_2 + \bar{b}_2 = 2, \\ 0, & \text{otherwise,} \end{cases}$$

$$S_4 = \begin{cases} 1, & \text{if } a_0 + b_0 + \bar{a}_4 + \bar{b}_4 = 2 \text{ and } a_1 + b_1 + \bar{a}_3 + \bar{b}_3 = 2, \\ 0, & \text{otherwise.} \end{cases}$$

System of conditions (7) can be used in the synthesis of logic scheme $S(\Re_1)$ of the adder $\Re_1$ intended to implement the addition operation $A + B = S \pmod 5$. In this case, logic scheme S ($\Re_1$) will contain ten elements EXCLUSIVE OR with a threshold two (each of which has four inputs), and the five elements AND, and will have the following characteristics: $l(\Re_1) = 50$, $g(\Re_1) = 2$ and $m(\Re_1) = 15$.

Synthesized in this way logic scheme $S(\Re_1)$ of the modular adder $\Re_1$ will be more efficient compared with existing analogs (see, for example, patents for invention Republic of Belarus 2991, 10834).

## 7. MULTIPLICATION OF UNITARY CODES BY MODULO FIVE

Consider the multiplication $A \cdot B = R \pmod 5$ by a unitary code, where $A = (a_0, a_1, a_2, a_3, a_4)$, $B = (b_0, b_1, b_2, b_3, b_4)$, $R = (r_0, r_1, r_2, r_3, r_4)$, and $R_k = 1$ if and only if $A \cdot B = k \pmod 5$, where $k = 0, 1, 2, 3, 4$.

From Assertion 2 it follows that the logical function $R_0$, $R_1$, $R_2$, $R_3$, and $R_4$ implemented at the outputs of the multiplier $\Re_2$ can be represented as

—$R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$;

—$R_1 = 1$ if and only if either of the equations holds $a_1 + b_1 = 2$, $a_2 + b_3 = 2$, $a_3 + b_2 = 2$, $a_4 + b_4 = 2$;

—$R_2 = 1$ if and only if either of the equations holds $a_1 + b_2 = 2$, $a_2 + b_1 = 2$, $a_3 + b_4 = 2$, $a_4 + b_3 = 2$;

—$R_3 = 1$ if and only if either of the equations holds $a_1 + b_3 = 2$, $a_2 + b_4 = 2$, $a_3 + b_1 = 2$, $a_4 + b_2 = 2$;

—$R_4 = 1$ if and only if either of the equations holds $a_1 + b_4 = 2$, $a_2 + b_2 = 2$, $a_3 + b_3 = 2$, $a_4 + b_1 = 2$;

In the following we will give the simpler analytical descriptions of the functions $R_0$, $R_1$, $R_2$, $R_3$, $R_4$.

**Assertion 7.** The function $R_0 = 0$ if and only if the condition $a_1 + a_2 + a_3 + a_4 + b_1 + b_2 + b_3 + b_4 = 2$ holds, the function $R_1 = 1$ if and only if $a_1 + 2a_4 + 2b_1 + b_4 = 3$ or $a_2 + 2a_3 + b_2 + 2b_3 = 3$; function $R_2 = 1$ if and only if $a_1 + 2a_2 + b_1 + 2b_2 = 3$ or $a_3 + 2a_4 + b_3 + 2b_4 = 3$; function $R_3 = 1$ if and only if $a_1 + 2a_3 + b_1 + 2b_3 = 3$ or $a_2 + 2a_4 + b_2 + 2b_4 = 3$; function $R_4 = 1$ if and only if $a_1 + 2a_4 + b_1 + 2b_4 = 3$ or $a_2 + 2a_3 + 2b_2 + b_3 = 3$.

***Proof.*** A function $R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$, $R_0 = 0$ if and only if $a_1 + a_2 + a_3 + a_4 + b_1 + b_2 + b_3 + b_4 = 2$ (since the latter equality is equivalent to $a_0 + b_0 = 0$).

The condition $a_1 + 2a_4 + 2b_1 + b_4 = 3$ is equivalent to $a_1 = b_1 = 1$ or $a_4 = b_4 = 1$, and the condition $a_2 + 2a_3 + b_2 + 2b_3 = 3$ is equivalent to $a_2 = b_3 = 1$ or $a_3 = b_2 = 1$. Consequently, the function $R_1 = 1$ if and only if either of the equations holds $a_1 + b_1 = 2$, $a_2 + b_3 = 2$, $a_3 + b_2 = 2$, $a_4 + b_4 = 2$.

A similar scheme carried out is proof of the allegations regarding the functions $R_2$, $R_3$, and $R_4$.

From the above assertion 7 we should make a new statement, which allows the use of simplifying the analytical representation of the functions $R_0$, $R_1$, $R_2$, $R_3$, and $R_4$.

**Assertion 8.** The function $R_0 = 1$ if and only if the condition $a_0 \vee b_0 = 1$ holds;

the function $R_1 = 1$ if and only if the following conditions hold:

$$\bar{a}_4 + \bar{b}_1 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3 = 1 \quad \text{or} \quad \bar{a}_3 + \bar{b}_3 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4 = 1,$$

the function $R_2 = 1$ if and only if the following conditions hold:

$$\bar{a}_2 + \bar{b}_2 + a_0 + a_3 + a_4 + b_0 + b_3 + b_4 = 1 \quad \text{or} \quad \bar{a}_4 + \bar{b}_4 + a_0 + a_1 + a_2 + b_0 + b_1 + b_2 = 1,$$

the function $R_3 = 1$ if and only if the following conditions hold:

$$\bar{a}_3 + \bar{b}_3 + a_0 + a_2 + a_4 + b_0 + b_2 + b_4 = 1 \quad \text{or} \quad \bar{a}_4 + \bar{b}_4 + a_0 + a_1 + a_3 + b_0 + b_1 + b_3 = 1,$$

the function $R_4 = 1$ if and only if the following conditions hold:

$$\bar{a}_4 + \bar{b}_4 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3 = 1 \quad \text{or} \quad \bar{a}_3 + \bar{b}_2 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4 = 1.$$

***Proof.*** Since the function $R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$, then $R_0 = a_0 \vee b_0$,

as

$$a_0 + a_1 + a_2 + a_3 + a_4 = 1, \quad b_0 + b_1 + b_2 + b_3 + b_4 = 1 \quad \text{and} \quad 1 - a_i = \bar{a}_i, \quad 1 - b_i = \bar{b}_i \ (\text{where } i = 0, 1, 2, 3, 4),$$

then the following equivalent transformation of the analytic representation of function $R_1$ is true:

$$
\begin{aligned}
1)\ & a_1 + 2a_4 + 2b_1 + b_4 = 3,\\
& a_1 + 2a_4 + 2b_1 + b_4 = 1 + (a_0 + a_1 + a_2 + a_3 + a_4) + (b_0 + b_1 + b_2 + b_3 + b_4),\\
& a_4 + b_1 = 1 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3,\\
& 2 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3 - a_4 - b_1 = 1,\\
& \bar{a}_4 + \bar{b}_1 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3 = 1,\\
2)\ & a_2 + 2a_3 + b_2 + 2b_3 = 3,\\
& a_2 + 2a_3 + b_2 + 2b_3 = 1 + (a_0 + a_1 + a_2 + a_3 + a_4) + (b_0 + b_1 + b_2 + b_3 + b_4),\\
& a_3 + b_3 = 1 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4,\\
& 2 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4 - a_3 - b_3 = 1,\\
& \bar{a}_3 + \bar{b}_3 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4 = 1.
\end{aligned}
$$

The proof of the assertion concerning the submission of functions $R_2$, $R_3$, and $R_4$ is similar.

From assertion 8, it follows that

$$R_0 = a_0 \vee b_0,$$

$$R_1 = \begin{cases} 1, & \text{if } \bar{a}_4 + \bar{b}_1 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3 = 1 \text{ or } \bar{a}_3 + \bar{b}_3 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4 = 1,\\ 0, & \text{otherwise,} \end{cases}$$

$$R_2 = \begin{cases} 1, & \text{if } \bar{a}_2 + \bar{b}_2 + a_0 + a_3 + a_4 + b_0 + b_3 + b_4 = 1 \text{ or } \bar{a}_4 + \bar{b}_4 + a_0 + a_1 + a_2 + b_0 + b_1 + b_2 = 1,\\ 0, & \text{otherwise,} \end{cases}$$

$$R_3 = \begin{cases} 1, & \text{if } \bar{a}_3 + \bar{b}_3 + a_0 + a_2 + a_4 + b_0 + b_2 + b_4 = 1 \text{ or } \bar{a}_4 + \bar{b}_4 + a_0 + a_1 + a_3 + b_0 + b_1 + b_3 = 1,\\ 0, & \text{otherwise,} \end{cases}$$

$$R_4 = \begin{cases} 1, & \text{if } \bar{a}_4 + \bar{b}_4 + a_0 + a_2 + a_3 + b_0 + b_2 + b_3 = 1 \text{ or } \bar{a}_3 + \bar{b}_2 + a_0 + a_1 + a_4 + b_0 + b_1 + b_4 = 1,\\ 0, & \text{otherwise.} \end{cases}$$

The system of conditions presented above can be used in the synthesis of logic scheme $S(\Re_2)$ of the multiplier $\Re_2$ designed to implement the multiplication operation $A \cdot B = S \pmod 5$. Synthesized with the same logic scheme $S(\Re_2)$ will contain eight EXCLUSIVE OR with a threshold elements, each of which has eight inputs, and five elements OR. Scheme $S(\Re_2)$ will have the following characteristics:

$$l(\Re_2) = 74, \quad g(\Re_2) = 2, \quad \text{and} \quad m(\Re_2) = 15.$$

The logic scheme $S(\Re_2)$ exceeds the existing analogs in some characteristics (see, for example, patents for invention Republic of Belarus 10531, 10652, 13493).

## 8. CONCLUSIONS

This paper proposes analytical representations of logic functions, realized at the outputs of the modular adder and a modular multiplier, provided that $P = 3$ and $P = 5$. Based on the application of the proposed approach, analytical representations are synthesized for logic adders and multipliers, differing by complexity and number of external leads. The synthesized logic schemes of adders and multipliers exceed all existing analogues in complexity, depth, or number of external leads. As an example, the problem of synthesis of the device that implements the superposition of the operations of addition and multiplication was consider. To solve this problem, we used the method of [6].

For all logic schemes presented in the article, patents for an invention of the Republic of Belarus were prepared and filed.

## REFERENCES

1. Dolgov, A.I., *Diagnostika ustroystv, funksioniruyushih v sisteme ostatochnyh klassov* (Diagnostic of Devices Operating in the Residue Number System), Moscow: Radio i Svyaz', 1982.
2. Chervyakov, N.I., Sakhnyuk, P.A., Shaposhnikov, A.V., and Ryadnov, S.A., *Modulyarnye parallelnye vychislitel'nye structury neyroprocessornyh sistem* (Modular Parallel Computing Structures of Neuroprocessor Systems), Moscow: Fizmatlit, 2003.
3. Kornilov, A.I., Semenov, M.Yu., and Kalashnikov, V.S., Methods of Apparatus Optimization of Adders for Two Operands in the Residue Number System, *Izv. Vyssh. Uchebn. Zaved., Elektronika*, 2004, no. 1, pp. 75–82.
4. Suprun, V.P., and Gorodecky, D.A., Synthesis of *n*-Operand Adders by Modulo 3, *Avtom. Vych. Tekh.*, 2010, no. 3, pp. 72–80.
5. Stempkovskii, A.L., Kornilov, A.I., and Semenov, M.Yu., Implementation Details of the Realization of Digital Signal Processing Devices in the Integrated Execution Using Modular Arithmetic, *Inf. Tekhnol.*, 2004, no. 2, pp. 2–9.
6. Suprun, V.P., and Gorodecky, D.A., The Method of Block-Structured Synthesis of Computing Devices of Modular Arithmetic, *Informatika*, 2009, no. 4 (24), pp. 74–79.