ISSN 0146-4116, Automatic Control and Computer Sciences, 2011, Vol. 45, No. 2, pp. 70–79. © Allerton Press, Inc., 2011.
Original Russian Text © V.P. Suprun, 2011, published in Avtomatika i Vychislitel'naya Tekhnika, 2011, No. 2, pp. 18–28.

Single-Level Schematic Realization of Basic Operations of Modular Arithmetic in Unitary Codes

V. P. Suprun

Faculty of Mechanics and Mathematics, Belarussian State University, av. Nezavisimosti 4, Minsk, 220030 Belarus
E-mail: suprun@bsu.by

Received October 6, 2010

Abstract—Some problems in the schematic realization of basic operations of modular arithmetic (operations of addition and multiplication modulo 5 and modulo 7) for the case of data representation in unitary codes are considered. Single-level logical schemes of modular adders and multipliers synthesized using EXCLUSIVE OR with a threshold are presented. These logical schemes are more efficient (in both complexity and depth) than the existing analogs.

Keywords: modular arithmetic, unit, unitary codes, modular adder, modular multiplier, logical scheme.

DOI: 10.3103/S0146411611020088

1. INTRODUCTION

It is known [1, 2] that the apparatus of modular arithmetic makes it possible to enhance the performance of computer mechanisms due to parallel and independent processing of digital signals. In addition, the modular representation of data provides the more reliable detection and correction of errors for its storage and transfer as well as for executing arithmetic operations.

At present, there are methods for synthesizing adders and multipliers (units for the multiplication of numbers) if the input and output operands are represented in unitary codes [3–6]. The interest in the data representation in unitary codes is explained by the fact that the unitary coding is widely used in circuit technology, automata theory, neural networks, and other fields of science and technology dealing with data transfer and transformation.

This work considers some problems of synthesizing single-level logical schemes of adders and multipliers in unitary codes modulo 5 and modulo 7. The logical schemes synthesized here contain EXCLUSIVE OR elements with a given threshold. Due to their peak performance, these logical schemes are more preferable than their existing analogs. In addition, the synthesized schemes have low constructive complexity, which is controlled by the number of inputs of logical elements.

2. MAIN CONCEPTS AND PROPERTIES

Unitary codes are widely used in computers as a means of data representation [2, 3].

An operand A in a unitary code modulo P is represented through a p-unit binary vector $(a_0, a_1, \ldots, a_{p-1})$, where $a_k = 1$ if and only if $A = k(\mathrm{mod}\ P)$, where $k = 0, 1, \ldots, p-1$.

It follows from this definition that the binary vector $(a_0, a_1, \ldots, a_{p-1})$ contains exactly a single unity; therefore, $a_0 + a_1 + \ldots + a_{p-1} = 1$. Because $1 - a_0 = \overline{a_0}$, we have

$$a_1 + a_2 + \ldots + a_{p-1} = \overline{a_0}. \tag{1}$$

Equality (1) can be generalized in the following way:

$$i + a_{i+1} + \ldots + a_{p-1} = \overline{a_0} + \overline{a_1} + \ldots + \overline{a_i}, \tag{2}$$

where $0 \le i \le p-2$.

As in [6], computer mechanisms realizing the operations of addition $A + B = S$ and multiplication $A \cdot B = R$ in unitary codes modulo P are denoted as $\Re_1$ (modular adder) and $\Re_2$ (modular multiplier), respectively. The input A and B and output S and R operands in unitary codes are given through p-unit binary vectors:

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

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 $k = 0, 1, \ldots, p-1$.

The main property of the logical functions

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

which are realized on outputs of units $\Re_1$ and $\Re_2$, respectively, where $k = 0, 1, \ldots, p-1$, is formulated in [6] in the form of the following two propositions.

Proposition 1. The logical function satisfies the condition $S_k = 1$ if and only if

$$a_i + b_j = 2, \text{ where } i + j = k \pmod P \text{ and } i, j = 0, 1, \ldots, p-1.$$

Proposition 2. The logical function satisfies the condition $R_k = 1$ if and only if

$$a_i + b_j = 2, \text{ where } i \cdot j = k \pmod P \text{ and } i, j = 0, 1, \ldots, p-1.$$

Hereafter, as a criterion for the optimality of the single-level logical schemes $S(\Re_1)$ and $S(\Re_2)$, we use their complexity $l(\Re_1)$ and $l(\Re_2)$ (the number of inputs of logical units) and the number of external outputs $m(\Re_1)$ and $m(\Re_2)$.

This paper investigates the problem of the synthesis of single-level logical schemes $S(\Re_1)$ and $S(\Re_2)$ under the condition that $P = 5$ and $P = 7$.

3. ADDITION OF UNITARY CODES MODULO 5

Let us consider the operation of addition $A + B = S \pmod 5$ in unitary codes, where

$A = (a_0, a_1, a_2, a_3, a_4)$, $B = (b_0, b_1, b_2, b_3, b_4)$, $S = (s_0, s_1, s_2, s_3, s_4)$, and $s_k = 1$ if and only if

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

It follows from statement 1 that the logical functions S_0, S_1, S_2, S_3, and S_4, realized at outputs of the modular adder $\Re_1$, can be expressed as the following conditions:

- $S_0 = 1$ if and only if $a_0 + b_0 = 2$, $a_1 + b_4 = 2$, $a_2 + b_3 = 2$, $a_3 + b_2 = 2$, or $a_4 + b_1 = 2$;
- $S_1 = 1$ if and only if $a_0 + b_1 = 2$, $a_1 + b_0 = 2$, $a_2 + b_4 = 2$, $a_3 + b_3 = 2$, or $a_4 + b_2 = 2$;
- $S_2 = 1$ if and only if $a_0 + b_2 = 2$, $a_1 + b_1 = 2$, $a_2 + b_0 = 2$, $a_3 + b_4 = 2$, or $a_4 + b_3 = 2$;
- $S_3 = 1$ if and only if $a_0 + b_3 = 2$, $a_1 + b_2 = 2$, $a_2 + b_1 = 2$, $a_3 + b_0 = 2$, or $a_4 + b_4 = 2$;
- $S_4 = 1$ if and only if $a_0 + b_4 = 2$, $a_1 + b_3 = 2$, $a_2 + b_2 = 2$, $a_3 + b_1 = 2$, or $a_4 + b_0 = 2$.

In view of the fact that each of the unitary codes $A = (a_0, a_1, a_2, a_3, a_4)$ and $B = (b_0, b_1, b_2, b_3, b_4)$ contains just a single unity, the logical functions S_0, S_1, S_2, S_3, and S_4 can be expressed analytically as the following equations:

$$S_0 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 5b_0 + b_1 + 2b_2 + 3b_3 + 4b_4 = 6, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 4b_0 + 5b_1 + b_2 + 2b_3 + 3b_4 = 6, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 3b_0 + 4b_1 + 5b_2 + b_3 + 2b_4 = 6, \\ 0, \text{ otherwise,} \end{cases} \quad (3)$$

$$S_3 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 2b_0 + 3b_1 + 4b_2 + 5b_3 + b_4 = 6, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_4 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + b_0 + 2b_1 + 3b_2 + 4b_3 + 5b_4 = 6, \\ 0, \text{ otherwise.} \end{cases}$$

The logical scheme $S_1(\mathfrak{R}_1)$ of the adder $\mathfrak{R}_1$, synthesized on the basis of equations (3), contains five elements of EXCLUSIVE OR with a threshold of 6 Patent for invention of Republic of Belarus 13821. The constructive complexity of the scheme $S_1(\mathfrak{R}_1)$ is $l(\mathfrak{R}_1) = 150$ and the number of its external outputs is $m(\mathfrak{R}_1) = 15$.

Because $a_0 + a_1 + a_2 + a_3 + a_4 = 1$ and $b_0 + b_1 + b_2 + b_3 + b_4 = 1$, the system of equations (3) yields the following:

$$S_0 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 4b_0 + b_2 + 2b_3 + 3b_4 = 4, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 3b_0 + 4b_1 + b_3 + 2b_4 = 4, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 2b_0 + 3b_1 + 4b_2 + b_4 = 4, \\ 0, \text{ otherwise,} \end{cases} \quad (4)$$

$$S_3 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + b_0 + 2b_1 + 3b_2 + 4b_3 = 4, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_4 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + b_1 + 2b_2 + 3b_3 + 4b_4 = 4, \\ 0, \text{ otherwise.} \end{cases}$$

The logical scheme $S_2(\mathfrak{R}_1)$, synthesized on the basis of equations (4), contains five elements of EXCLUSIVE OR with a threshold of 4 and has the following characteristics: $l(\mathfrak{R}_1) = 100$ and $m(\mathfrak{R}_1) = 14$.

We further simplify equations (4) by using property (1). Because

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

the system of equations (4) is equivalent to the following system of equations:

$$S_0 = \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + 3b_0 + \overline{b_1} + b_3 + 2b_4 = 4, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + 2b_0 + 3b_1 + \overline{b_2} + b_4 = 4, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + b_0 + 2b_1 + 3b_2 + \overline{b_3} = 4, \\ 0, \text{ otherwise,} \end{cases} \quad (5)$$

$$S_3 = \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + b_1 + 2b_2 + 3b_3 + \overline{b_4} = 4, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_4 = \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + \overline{b_0} + b_2 + 2b_3 + 3b_4 = 4, \\ 0, \text{ otherwise.} \end{cases}$$

The logical scheme $S_3(\Re_1)$, synthesized on the basis of equations (5), is shown in Fig. 1a. The scheme $S_3(\Re_1)$ contains five elements of EXCLUSIVE OR with a threshold of 4 and has the following characteristics: $l(\Re_1) = 70$ and $m(\Re_1) = 14$.

To further simplify the analytical expressions of the functions S_0, S_1, S_2, S_3, and S_4, we use property (2) of the unitary binary code. This property yields that

$$1 + a_2 + a_3 + a_4 = \overline{a_0} + \overline{a_1}, \quad 1 + b_0 + b_3 + b_4 = \overline{b_1} + \overline{b_2}, \quad 1 + b_0 + b_1 + b_4 = \overline{b_2} + \overline{b_3},$$
$$1 + b_0 + b_1 + b_2 = \overline{b_3} + \overline{b_4}, \quad 1 + b_1 + b_2 + b_3 = \overline{b_0} + \overline{b_4} \quad \text{and} \quad 1 + b_2 + b_3 + b_4 = \overline{b_0} + \overline{b_1}.$$

In that case, we obtain from (5) the system of equations

$$S_0 = \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + 2b_0 + 2\overline{b_1} + \overline{b_2} + b_4 = 6, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + b_0 + 2b_1 + 2\overline{b_2} + \overline{b_3} = 6, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + b_1 + 2b_2 + 2\overline{b_3} + \overline{b_4} = 6, \\ 0, \text{ otherwise,} \end{cases} \tag{6}$$

$$S_3 = \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + \overline{b_0} + b_2 + 2b_3 + 2\overline{b_4} = 6, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_4 = \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + 2\overline{b_0} + \overline{b_1} + b_3 + 2b_4 = 6, \\ 0, \text{ otherwise.} \end{cases}$$

The logical scheme $S_4(\Re_1)$ synthesized on the basis of equations (6) is shown in Fig. 1b. The logical scheme $S_4(\Re_1)$ contains five elements of EXCLUSIVE OR with a threshold of 6 and has the following characteristics: $l(\Re_1) = 60$ and $m(\Re_1) = 14$.

The synthesized logical schemes $S_2(\Re_1)$, $S_3(\Re_1)$, and $S_4(\Re_1)$ of the modular adder $\Re_1$, designed for executing the operation $A + B = S \pmod 5$ in unitary codes, are superior (in complexity and/or depth) to existing analogs (see, for example, Patents for invention of Republic of Belarus 2991, 10834, and 13821).

4. MULTIPLICATION OF UNITARY CODES MODULO 5

Let us consider the operation of multiplication $A \cdot B = R \pmod 5$ in unitary codes, where

$A = (a_0, a_1, a_2, a_3, a_4)$, $B = (b_0, b_1, b_2, b_3, b_4)$, $R = (r_0, r_1, r_2, r_3, r_4)$, and $r_k = 1$ if and only if

$A \cdot B = k \pmod 5$ and $k = 0, 1, 2, 3, 4$.

Proposition 2 yields that the logical functions R_0, R_1, R_2, R_3, and R_4, realized on outputs of the modular multiplier $\Re_2$, can be expressed as the following conditions:

- $R_0 = 1$ if and only if $a_0 = 1$ or $b_0 = 1$;
- $R_1 = 1$ if and only if $a_1 + b_1 = 2$, $a_2 + b_3 = 2$, $a_3 + b_2 = 2$, or $a_4 + b_4 = 2$;
- $R_2 = 1$ if and only if $a_1 + b_2 = 2$, $a_2 + b_1 = 2$, $a_3 + b_4 = 2$, or $a_4 + b_3 = 2$;
- $R_3 = 1$ if and only if $a_1 + b_3 = 2$, $a_2 + b_4 = 2$, $a_3 + b_1 = 2$, or $a_4 + b_2 = 2$;
- $R_4 = 1$ if and only if $a_1 + b_4 = 2$, $a_2 + b_2 = 2$, $a_3 + b_3 = 2$, or $a_4 + b_1 = 2$.

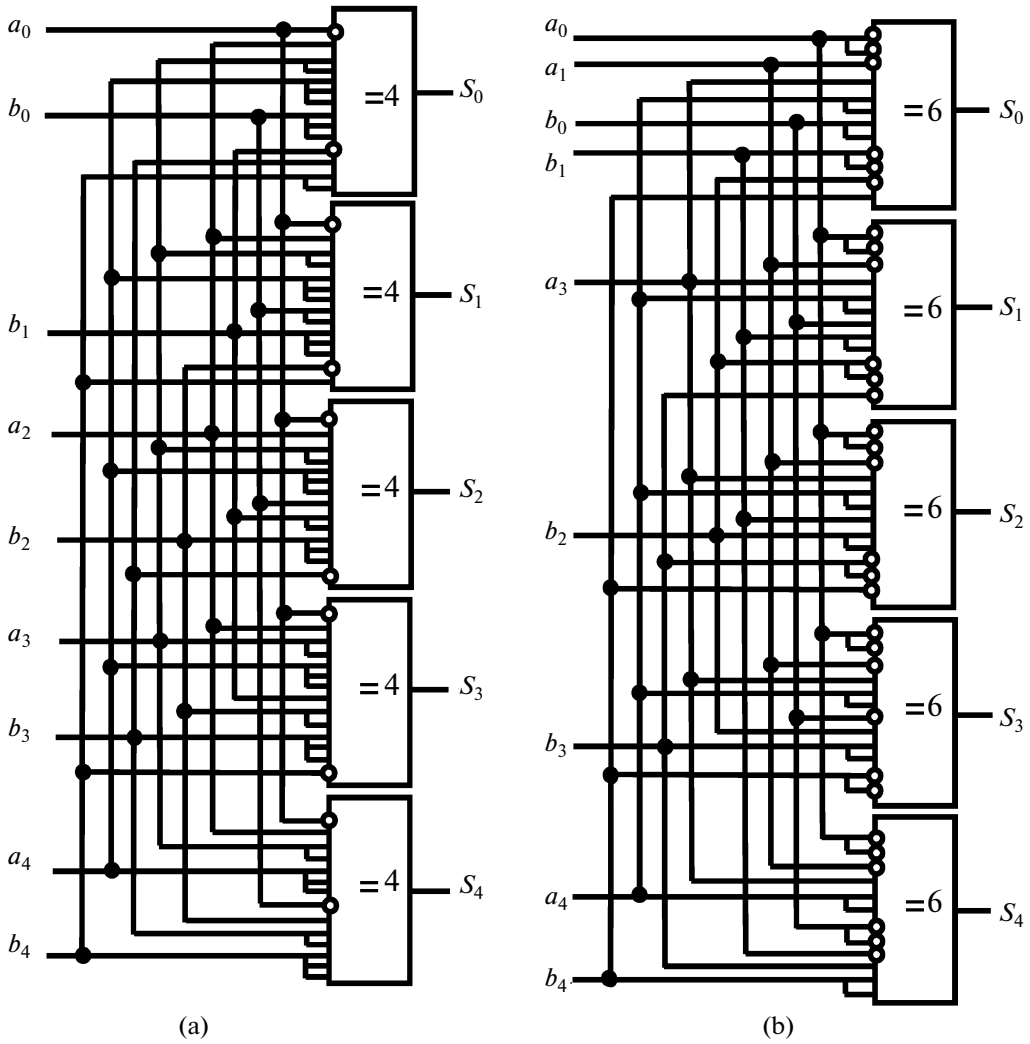

Fig. 1. Logical scheme of the modular adder $\mathfrak{R}_1$: (a) scheme $S_3(\mathfrak{R}_1)$; (b) scheme $S_4(\mathfrak{R}_1)$.

Because each of the unitary codes $A = (a_0, a_1, a_2, a_3, a_4)$ and $B = (b_0, b_1, b_2, b_3, b_4)$ contains just a single unity, the logical functions R_0, R_1, R_2, R_3, and R_4, can be expressed analytically as the following equations:

$$R_0 = a_0 \vee b_0,$$

$$R_1 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 4b_1 + 2b_2 + 3b_3 + b_4 = 5, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_2 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 3b_1 + 4b_2 + b_3 + 2b_4 = 5, \\ 0, \text{ otherwise,} \end{cases} \quad (7)$$

$$R_3 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 2b_1 + b_2 + 4b_3 + 3b_4 = 5, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_4 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + b_1 + 3b_2 + 2b_3 + 4b_4 = 5, \\ 0, \text{ otherwise.} \end{cases}$$

The logical scheme $S_1(\Re_2)$ of the multiplier $\Re_2$, synthesized on the basis of equations (7), contains an element OR and four elements of EXCLUSIVE OR with a threshold of 5 (Patent for invention of Republic of Belarus 13493). The scheme $S_1(\Re_2)$ has a constructive complexity $l(\Re_2) = 82$ and the number of external outputs $m(\Re_2) = 15$.

System of equations (7) is simplified by analogy with the simplification of system of equations (4). Because $a_1 + a_2 + a_3 + a_4 = \overline{a_0}$ and $b_1 + b_2 + b_3 + b_4 = \overline{b_0}$, system of equations (7) yields

$$
\begin{aligned}
R_0 &= a_0 \vee b_0,\\
R_1 &= \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + \overline{b_0} + 3b_1 + b_2 + 2b_3 = 5,\\ 0, \text{ otherwise,}\end{cases}\\
R_2 &= \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + \overline{b_0} + 2b_1 + 3b_2 + b_4 = 5,\\ 0, \text{ otherwise,}\end{cases}\\
R_3 &= \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + \overline{b_0} + b_1 + 3b_3 + 2b_4 = 5,\\ 0, \text{ otherwise,}\end{cases}\\
R_4 &= \begin{cases} 1, \text{ if } \overline{a_0} + a_2 + 2a_3 + 3a_4 + \overline{b_0} + 2b_2 + b_3 + 3b_4 = 5,\\ 0, \text{ otherwise.}\end{cases}
\end{aligned}
\tag{8}
$$

The logical scheme $S_2(\Re_2)$ synthesized on the basis of equations (8) is shown in Fig. 2a. The scheme $S_2(\Re_2)$ contains an element OR and four elements of EXCLUSIVE OR with a threshold of 5 and has the following characteristics: $l(\Re_2) = 58$ and $m(\Re_2) = 14$.

To simplify system of equations (8), we use property (2) of the unitary binary code. This property yields that

$$
\begin{gathered}
1 + a_2 + a_3 + a_4 = \overline{a_0} + \overline{a_1}, \quad 1 + b_1 + b_2 + b_3 = \overline{b_0} + \overline{b_4}, \quad 1 + b_1 + b_2 + b_4 = \overline{b_0} + \overline{b_3},\\
1 + b_1 + b_3 + b_4 = \overline{b_0} + \overline{b_2}, \quad \text{and} \quad 1 + b_2 + b_3 + b_4 = \overline{b_0} + \overline{b_1}.
\end{gathered}
$$

Using the above equalities, we obtain the system of equations

$$
\begin{aligned}
R_0 &= a_0 \vee b_0,\\
R_1 &= \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + 2\overline{b_0} + 2b_1 + b_3 + \overline{b_4} = 7,\\ 0, \text{ otherwise,}\end{cases}\\
R_2 &= \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + 2\overline{b_0} + b_1 + 2b_2 + \overline{b_3} = 7,\\ 0, \text{ otherwise,}\end{cases}\\
R_3 &= \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + 2\overline{b_0} + \overline{b_2} + 2b_3 + b_4 = 7,\\ 0, \text{ otherwise,}\end{cases}\\
R_4 &= \begin{cases} 1, \text{ if } 2\overline{a_0} + \overline{a_1} + a_3 + 2a_4 + 2\overline{b_0} + \overline{b_1} + b_2 + 2b_4 = 7,\\ 0, \text{ otherwise.}\end{cases}
\end{aligned}
\tag{9}
$$

The logical scheme $S_3(\Re_2)$ of the modular multiplier $\Re_2$, synthesized on the basis of equations (9), is shown in Fig. 2b. The scheme $S_3(\Re_2)$ contains an element OR and four elements of EXCLUSIVE OR with a threshold of 7 and has the following characteristics: $l(\Re_2) = 50$ and $m(\Re_2) = 14$.

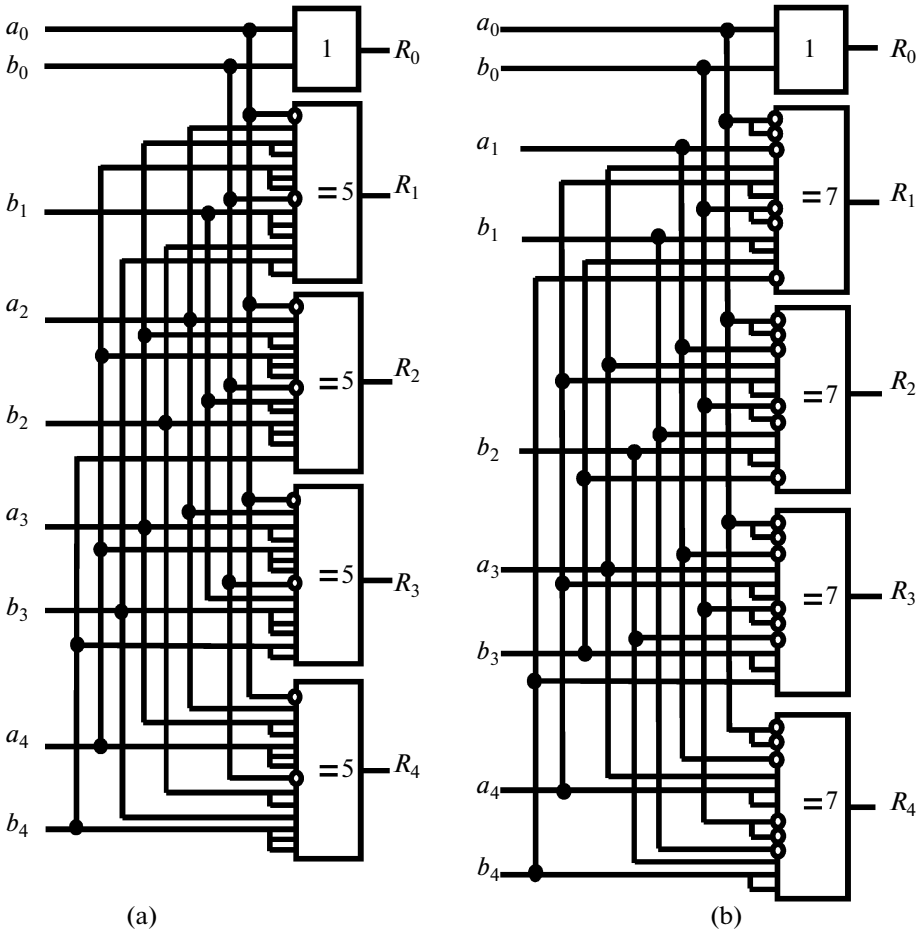

Fig. 2. Logical scheme of the modular multiplier $\Re_2$: (a) scheme $S_2(\Re_2)$; (b) scheme $S_3(\Re_2)$.

The logical schemes $S_2(\Re_2)$ and $S_3(\Re_2)$ of the modular multiplier $\Re_2$, designed for executing the operation $A \cdot B = R \pmod 5$ in unitary codes, are superior (in complexity and/or depth) to existing analogs (see, for example, Patents for invention of Republic of Belarus 10531, 10652, and 13493).

5. ADDITION OF UNITARY CODES MODULO 7

Let us consider the operation of addition $A + B = S \pmod 7$ in unitary codes, where

$A = (a_0, a_1, a_2, a_3, a_4, a_5, a_6)$, $B = (b_0, b_1, b_2, b_3, b_4, b_5, b_6)$, $S = (s_0, s_1, s_2, s_3, s_4, s_5, s_6)$, and $s_k = 1$ if and only if $A + B = k \pmod 7$ and $k = 0, 1, \ldots, 6$.

It follows from statement 1 that the logical functions S_0, S_1, S_2, S_3, S_4, S_5, and S_6, realized at outputs of the modular adder $\Re_1$, can be expressed as the following system of equations:

$$S_0 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 7b_0 + b_1 + 2b_2 + 3b_3 + 4b_4 + 5b_5 + 6b_6 = 8, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 6b_0 + 7b_1 + b_2 + 2b_3 + 3b_4 + 4b_5 + 5b_6 = 8, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 5b_0 + 6b_1 + 7b_2 + b_3 + 2b_4 + 3b_5 + 4b_6 = 8, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_3 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 4b_0 + 5b_1 + 6b_2 + 7b_3 + b_4 + 2b_5 + 3b_6 = 8, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_4 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 3b_0 + 4b_1 + 5b_2 + 6b_3 + 7b_4 + b_5 + 2b_6 = 8, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_5 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + 2b_0 + 3b_1 + 4b_2 + 5b_3 + 6b_4 + 7b_5 + b_6 = 8, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_6 = \begin{cases} 1, \text{ if } a_0 + 2a_1 + 3a_2 + 4a_3 + 5a_4 + 6a_5 + 7a_6 + b_0 + 2b_1 + 3b_2 + 4b_3 + 5b_4 + 6b_5 + 7b_6 = 8, \\ 0, \text{ otherwise.} \end{cases}$$

If this system of equations is transformed by analogy with the transformation of equations (3)–(5), we obtain the system of equations

$$S_0 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3b_0 + 3\overline{b_1} + 2\overline{b_2} + \overline{b_3} + b_5 + 2b_6 = 12, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_1 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 2b_0 + 3b_1 + 3\overline{b_2} + 2\overline{b_3} + \overline{b_4} + b_6 = 12, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_2 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + b_0 + 2b_1 + 3b_2 + 3\overline{b_3} + 2\overline{b_4} + \overline{b_5} = 12, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_3 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + b_1 + 2b_2 + 3b_3 + 3\overline{b_4} + 2\overline{b_5} + \overline{b_6} = 12, \\ 0, \text{ otherwise,} \end{cases} \quad (10)$$

$$S_4 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + \overline{b_0} + b_2 + 2b_3 + 3b_4 + 3\overline{b_5} + 2\overline{b_6} = 12, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_5 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 2\overline{b_0} + \overline{b_1} + b_3 + 2b_4 + 3b_5 + 3\overline{b_6} = 12, \\ 0, \text{ otherwise,} \end{cases}$$

$$S_6 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + 2\overline{b_1} + \overline{b_2} + b_4 + 2b_5 + 3b_6 = 12, \\ 0, \text{ otherwise.} \end{cases}$$

If the modular adder $\Re_1$ is synthesized on the basis of equations (10), the single-level scheme $S(\Re_1)$ contains seven elements of EXCLUSIVE OR with a threshold of 12. In this case, we have the following: $l(\Re_1) = 168$ and $m(\Re_1) = 20$.

6. MULTIPLICATION OF UNITARY CODES MODULO 7

Let us consider the operation of multiplication $A \cdot B = R \pmod 7$ in unitary codes, where $A = (a_0, a_1, a_2, a_3, a_4, a_5, a_6)$, $B = (b_0, b_1, b_2, b_3, b_4, b_5, b_6)$, $R = (r_0, r_1, r_2, r_3, r_4, r_5, r_6)$, and $r_k = 1$ if and only if $A \cdot B = k \pmod 7$ and $k = 0, 1, \ldots, 6$.

Proposition 2 yields that the logical functions R_0, R_1, R_2, R_3, R_4, R_5, and R_6, realized on outputs of the modular multiplier $\Re_2$, can be expressed as the following system of equations:

$$R_0 = a_0 \vee b_0,$$

$$R_1 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 6b_1 + 3b_2 + 2b_3 + 5b_4 + 4b_5 + b_6 = 7, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_2 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 5b_1 + 6b_2 + 4b_3 + 3b_4 + b_5 + 2b_6 = 7, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_3 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 4b_1 + 2b_2 + 6b_3 + b_4 + 5b_5 + 3b_6 = 7, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_4 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 3b_1 + 5b_2 + b_3 + 6b_4 + 2b_5 + 4b_6 = 7, \\ 0, \text{ otherwise.} \end{cases}$$

$$R_5 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 2b_1 + b_2 + 3b_3 + 4b_4 + 6b_5 + 5b_6 = 7, \\ 0, \text{ otherwise.} \end{cases}$$

$$R_6 = \begin{cases} 1, \text{ if } a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + b_1 + 4b_2 + 5b_3 + 2b_4 + 3b_5 + 6b_6 = 7, \\ 0, \text{ otherwise.} \end{cases}$$

Transforming the above-given system of equations by analogy with simplified system (7), we obtain the system of equations

$$R_0 = a_0 \vee b_0,$$

$$R_1 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + 3b_1 + \overline{b_3} + 2b_4 + b_5 + 2\overline{b_6} = 13, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_2 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + 2b_1 + 3b_2 + b_3 + 2\overline{b_5} + \overline{b_6} = 13, \\ 0, \text{ otherwise,} \end{cases}$$

$$R_3 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + b_1 + \overline{b_2} + 3b_3 + 2\overline{b_4} + 2b_5 = 13, \\ 0, \text{ otherwise,} \end{cases} \quad (11)$$

$$R_4 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + 2b_2 + 2\overline{b_3} + 3b_4 + \overline{b_5} + b_6 = 13, \\ 0, \text{ otherwise.} \end{cases}$$

$$R_5 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + \overline{b_1} + 2\overline{b_2} + b_4 + 3b_5 + 2b_6 = 13, \\ 0, \text{ otherwise.} \end{cases}$$

$$R_6 = \begin{cases} 1, \text{ if } 3\overline{a_0} + 2\overline{a_1} + \overline{a_2} + a_4 + 2a_5 + 3a_6 + 3\overline{b_0} + 2\overline{b_1} + b_2 + 2b_3 + \overline{b_4} + 3b_6 = 13, \\ 0, \text{ otherwise.} \end{cases}$$

The logical scheme $S(\Re_2)$ of the modular multiplier $\Re_2$, synthesized on the basis of equations (11), contains an element OR and six elements of EXCLUSIVE OR with a threshold of 13. The complexity and number of outputs of the scheme $S(\Re_2)$ are $l(\Re_2) = 146$ and $m(\Re_2) = 20$, respectively.

7. CONCLUSIONS

This paper proposes analytical expressions for logical functions that are realized at outputs of the modular adder and modular multiplier in unitary codes for $P = 5$ and $P = 7$. Note that single-level schemes of the modular adder $\Re_1$ and modular multiplier $\Re_2$ for $P = 3$ can be found in [6].

The logical schemes $S_4(\Re_1)$ and $S_3(\Re_2)$, which are optimal by complexity and depth, can be efficiently used for synthesizing logical schemes $S(\Re)$ of computer mechanisms of modular arithmetic $\Re$ designed for the realization in unitary codes of more complex arithmetic operations than addition and multiplication. Examples of such "complex" operations are the following: $(A + B) + C = S$, $(A \cdot B)C = R$, $(A + B)C = R$, $A \cdot B + C = S$, $(A + B) + (C + D) = S$, $(A \cdot B)(C \cdot D) = R$, $A \cdot B + C \cdot D = S$, and $(A + B)(C + D) = R$. It should be noted that the logical schemes $S(\Re)$ of the computer mechanism $\Re$ can be synthesized with the help of the method of block-structural synthesis [7].

Analytical expressions (6), (9), (10), and (11) of the logical functions realized at outputs of the modular adders $\Re_1$ and the modular multipliers $\Re_2$ are generalized to the case $P = 2k + 1$, where $k \geq 1$. Here, the complexity of the optimal single-level logical schemes $S(\Re_1)$ and $S(\Re_2)$ is calculated by the formulas $l(\Re_1) = 2k(k + 1)(2k + 1)$ and $l(\Re_2) = 4k^2(k + 1) + 2$, and the number of external outputs is $m(\Re_1) = m(\Re_2) = 3P - 1$.

All the logical schemes of the modular adders $\Re_1$ and the modular multipliers $\Re_2$ mentioned in this paper have been patented in the Republic of Belarus.

REFERENCES

1. Dolgov, A.I., *Diagnostika ustroistv, funktsioniruyushchikh v sisteme ostatochnykh klassov* (Diagnostics of Devices in Residual Class System), Moscow: Radio i Svyaz', 1982.
2. Chervyakov, N.I., Sakhnyuk, P.A., Shaposhnikov, A.V., and Ryadnov, S.A., *Modulyarnye parallel'nye vychislitel'nye struktury neiroprotsessornykh sistem* (Modular Parallel Calculation Structures in Neiroprocessor Systems, Chervyakov, N.I., Ed., Moscow: Fizmatlit, 2003.
3. Kornilov, A.I., Semenov, M.Yu., and Kalashnikov, V.S., Apparatus Optimization Methods of Summators for Two Operands in Residual Class System, *Izv. Vysch. Uchebn. Zaved. Elektronika*, 2004, No. 1, pp. 75–82.
4. Suprun, V.P. and Gorodetskii, D.A., Synthesis of *n*-Operand Modulo-Three Adders, *Avtomatika i vychislitel'naya tekhnika*, 2010, no. 3, pp. 72–80 [Automatic Control Comp. Sci. (Engl. Transl.), vol. 44, no. 3, pp. 171–179].
5. Stempkovskii, A.L., Kornilov, A.I., and Semenov, M.Yu., Peculiarities of Realization of Signal Digital Treatment Devices in Integral Performance with the Modular Arithmetic Use, *Informatsionnye tekhnologii*, 2004, no. 2, pp. 2–9.
6. Suprun, V.P. and Gorodetskii, D.A., Realization of Addition and Multiplication Operations in Unitary Codes, *Avtomatika i vychislitel'naya tekhnika,* 2010, no. 5, pp. 59–71 [Automatic Control Comp. Sci. (Engl. Transl.), vol. 44, no. 5, pp. 292–301].
7. Suprun, V.P. and Gorodetskii, D.A., Method of Block-Structural Synthesis for Calculation Devices of Modular Arithmetic, *Informatika,* 2009, vol. 4, no. 24, pp. 74–79.