Journal of Theoretical and Applied Information Technology
31st October 2015. Vol.80. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPLICATION OF MODULAR TECHNOLOGIES IN THE LARGE-SCALE ANALYSIS OF SIGNALS

IGOR ANATOL'EVICH KALMYKOV
North-Caucasian Federal University, Pushkina str., 1, Stavropol, 355009, Russia
KONSTANTIN ALEKSANDROVICH KATKOV
North-Caucasian Federal University, Pushkina str., 1, Stavropol, 355009, Russia
LEONID IVANOVICH TIMOSHENKO
North-Caucasian Federal University, Pushkina str., 1, Stavropol, 355009, Russia
ANDREI VALER'EVICH DUNIN
North-Caucasian Federal University, Pushkina str., 1, Stavropol, 355009, Russia
TATIANA ALEKSANDROVNA GISH
North-Caucasian Federal University, Pushkina str., 1, Stavropol, 355009, Russia

ABSTRACT

The purpose of the research is to improve the accuracy of the large-scale analysis of signals. This goal can be achieved through the use of algebraic systems having the properties of a ring and a field. The paper presents the implementation of the discrete Haar wavelet transform in the finite Galois field GF (17). To detect and correct the errors that can occur during the operation of a special processor for digital signal processing (DSP) due to malfunction and failure of equipment, an algorithm is developed for calculating a positional characteristic. The use of new modular technologies in the DSP problems enables, by virtue of parallelization at the level of operations and processing the short-bit data, not only to increase the calculation accuracy, but also to ensure obtaining the correct result.

Keywords: *Discrete Wavelet Transform Of Signal, Residue Number System, Polynomial System Of Residue Classes, Error Correction, Positional Characteristics*

1. INTRODUCTION

Acceleration of the process of informatization of modern society, as well as the progress in the field of computer technology have contributed to the widening applications of the methods of digital signal processing. To provide a real time scale for the primary and secondary processing of the received signal, there is proposed to use the algebraic structures having the properties of a ring and a field, in particular, the nonpositional modular codes (MC).

Presently, when performing digital signal processing, the methods and algorithms of the large-scale analysis are used. Application of modular arithmetic will improve the efficiency of the discrete wavelet transformation of signals, providing their high precision and speed. Therefore, the development of a method of integer-valued large-scale signal analysis, based on algebraic structures with the properties of a ring and a field, is a topical problem.

2. METHODS

2.1. Analysis Of The Main Areas Of Application Of Modular Technologies

The most characteristic feature of recent years is the expansion of the application fields of modular arithmetic. The conducted analysis allows identifying the fundamental directions, where the advantages of nonpositional modular codes are manifested most vividly.

The basis of the first direction is the classical methods and algorithms of DSP which use orthogonal transformations of signals in the field of complex numbers [1], [9], [13], [14], [19], [21]. Parallel data processing through the computing channels, determined by the bases of a residue number system (RNS), and the short-bit character of residues allow increasing the speed of signal processing. However, the special processor for digital signal processing, functioning in some RNS, must perform also the non-modular operations together with the modular ones. In the work [14] the algorithms of carrying out both modular and non-modular operations are considered in sufficient detail. A special attention is paid to the algorithms

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of direct transformation from a positional code to an RNS code, as well as the algorithms of inverse transformation from RNS to the positional code. In addition, the author presented efficient algorithms of scaling, division, multiplication and addition, as well as their hardware implementations for the set of moduli $2^n-1, 2^n, 2^n+1$. In the paper [12] there is presented an algorithm of secondary processing of navigation data, which enables to reduce the positioning error by virtue of multiple pseudorange measurement in the presence of a local area of increased ionization in the selected working constellation of satellites. To provide the real-time secondary signal processing, there is proposed to use parallel computing in some RNS. Application of the RNS code allows increasing the number of measurements, resulting in reducing the error of determination of the space-time coordinates of the consumer.

Since the residue number system belongs to non-positional number systems, then it is necessary to carry out both for the efficient operation.

To provide high accuracy of performance of the DSP algorithms, in the works [3], [6], [11] there is proposed to use a polynomial system of residue classes (PSRC). Moreover, the decrease of error in carrying out orthogonal transformations of the signal is due to using the integer algebraic systems with the properties of a ring and a field.

The second direction of using the algebraic systems with the properties of a ring and a field is connected with the construction of cryptographic systems. In the work [6] the application is demonstrated of the neural network technologies and residue number systems in cryptography. The author paid a special attention to the questions of application of RNS in the cryptographic systems with an open and a secret key. There are developed some neural network technologies for the systems of authentication, steganography and the random number generation in cryptographic systems. The application of modular algebraic systems allows constructing pseudo-random functions (PRF) of increased efficiency. For example, in the paper [7] there is presented a calculation algorithm for a PRF, realized in a finite Galois field

$$F((s_1,...,s_n,h),(x_1,...,x_n)) = g^{\left(\prod_{i=1}^{n}(s_i+x_i)\right)^{-1}}, \quad (1)$$

where h is the primitive element of the multiplicative group; $(g,s_1,...,s_n)$ are the keys of the PRF, determining its strength; $(x_1,...,x_n)$ is the input sequence.

The conducted studies have shown that the cryptostrength of such PRF corresponds to the complexity of solving the λ-DDH problem. In the works [16], [18], [4] there is shown the expedience of the PRF realization in the electronic commercial systems. In addition, in the work [Pashintsev, 2014] an algorithm is presented for determining the status of a satellite of the satellite communication system which is used for remote control of environmentally hazardous technologies, and this algorithm uses the PRF defined by equation (1).

The foundation of the third direction consists of the methods and algorithms for providing fault-tolerance of the specialized computing devices. The introduction of additional redundant bases allows detecting and correcting errors that arise in the operation of special processors due to malfunctions and failures. In the works [18], [10], [2] there are presented algorithms and their circuit implementations, which allow correcting errors with the help of nonpositional modular codes.

A new direction of application of the algebraic systems with the properties of a ring and a field is the large-scale analysis of signals. The novelty of this approach lies in the fact that the use of RNS enables to increase the speed of carrying out the discrete wavelet transform and to reduce the computation errors through the use of integer coefficients of the filters. In addition, RNS can correct the errors that may occur during the functioning of the special processor for digital signal processing due to malfunctions and failures. Thus, the development of new modular technologies allowing increasing the efficiency of carrying out the large-scale analysis of signals is an urgent task.

2.2. Realization Of The Discrete Haar Wavelet Transform

In recent years, there begins to take shape a new direction of application of nonpositional codes. It is related to carrying out the large-scale analysis of signals in a finite field GF (p). The increased interest to the discrete wavelet transforms (DWT) is due to the fact that such orthogonal transformations of signals allow calculating the time-frequency characteristics of signals with smaller errors. Let us consider carrying out the large-scale analysis of signals based on the discrete Haar wavelet

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

transform, which is described in the form of matrices

$$\mathbf{T} = \mathbf{HFH}^T, \quad (2)$$

where **F** is the matrix of the signal, **H** is the matrix of the transformation, and **T** is the result of transformation of the signal.

When constructing the matrices of the discrete Haar wavelet transform, there are utilized the basic Haar functions hk(z), for which the quantity $z \in [0,1]$ is given on a continuous closed interval.

For k = 0, the value of the basic function is defined as

$$h_0(z) = h_{00}(z) = \left(\sqrt{N}\right)^{-1}. \quad (3)$$

The calculation of other basic Haar DWT functions is carried out as follows

$$h_k(z) = h_{lq}(z) = \frac{2^{\frac{l}{2}}}{\sqrt{N}} \begin{cases} 1 & for \ \frac{q-1}{2^l} \le z < \frac{q-0,5}{2^l} \\ -1 & for \ \frac{q-0,5}{2^l} \le z < \frac{q}{2^l} \\ 0 & in\ other\ cases \end{cases}, \quad (4)$$

where q and l are the values determined by the index $k = 0, 1, ..., N\text{-}1$; $N = 2^n$; $z \in [0,1]$.

Suppose it is necessary to perform the Haar DWT for the sample vector containing 8 points. Then the matrix to perform the discrete wavelet transform has the following form

$$H_8 = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \end{bmatrix} \quad (5)$$

On the basis of analysis of equality (5) it can be concluded that it is possible to perform the Haar transform using a finite field GF (p) with the characteristic different from two, that is, $p \neq 2$. This conclusion is based on the possibility of integer calculation of $\sqrt{2} \bmod p$. Thus, there is a possibility of transition from the classical Haar DWT to the calculation of the Haar wavelet transform in a finite field. Such transition should ensure the reduction of calculation errors by eliminating the use of irrational values of the Haar coefficients.

2.3. Realization Of The Integer Discrete Haar Wavelet Transform In The Field GF (17)

As an example, let us take a finite Galois field having the characteristic p = 17. Such a choice is conditioned by the fact that there exists in this field $\sqrt{2} \bmod 17 \equiv 6$. Hence, the normalizing factor of the Haar DWT in GF (17) will be equal to $\left(\sqrt{8}\right)^{-1} \bmod 17 \equiv 10$. Then the matrix, determining the Haar wavelet transform, will assume, according to equality (5), the following form

$$H_8 = 10 \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 16 & 16 & 16 & 16 \\ 6 & 6 & 11 & 11 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 6 & 11 & 11 \\ 2 & 15 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 15 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 15 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 15 \end{bmatrix} \quad (6)$$

Let us perform normalization of matrix (6). Then the Haar DWT in the field GF(17) is defined as

$$W(i) = H_8^{norm} X(i) = \begin{bmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 10 & 10 & 10 & 10 & 7 & 7 & 7 & 7 \\ 9 & 9 & 8 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 9 & 8 & 8 \\ 3 & 14 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 14 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 14 \end{bmatrix} \quad (7)$$

Moreover, the requirements for the Haar DWT are completely fulfilled for this matrix

$$\sum_{i=0}^{N-1} h_{ij}(z) \equiv 0 \ mod\ p; \ \sum_{i=0}^{N-1} h_{ij}^2(z) \equiv 1 \ mod\ p;$$

$$\sum_{i=0}^{N-1} h_{ij}(z) h_{ab}(z) \equiv 0 \ mod\ p. \quad (8)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where $\forall i \neq a \; or \; j \neq b$.

To perform the Haar DWT in the finite field, we use the expression (7). As a result of performing the Haar DWT over the input vector having 8 discrete samples, we obtain the decomposition of the signal in the basis

$$X(i) = \left| W(0,0)a_{0,0} + W(1,0)d_{1,0} + W(2,0)d_{2,0} + W(2,1)d_{2,1} + W(4,0)d_{4,0} + W(4,3)d_{4,3} + W(4,2)d_{4,2} + W(4,1)d_{4,1} \right|_{17}^{+}$$

A characteristic feature of any orthogonal transformation of signals is its invertibility. Let us make use of the invertibility property of the discrete Haar wavelet transform for the recovery of the original signal. For this purpose we transpose the Haar matrix given by the expression (5).

$$X(i) = H_8^T W(i) = \begin{bmatrix} 10 & 10 & 9 & 0 & 3 & 0 & 0 & 0 \\ 10 & 10 & 9 & 0 & 14 & 0 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 3 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 14 & 0 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 3 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 14 & 0 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 3 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 14 \end{bmatrix} \times \begin{bmatrix} W_a(0,0) \\ W_d(1,0) \\ W_d(2,0) \\ W_d(2,1) \\ W_d(4,0) \\ W_d(4,3) \\ W_d(4,2) \\ W_d(4,1) \end{bmatrix} mod\, 17 \quad . \tag{9}$$

The use of modular technologies makes it possible not only to obtain highly accurate result of transformations of signals, but also provide carrying out the procedures of detecting and correcting the errors that arise during the operation of specialized computing devices implementing the Haar DWT.

2.4. Development Of An Algorithm Of Error Correction With The Help Of Redundant RNS

If we select the relevant characteristics of the finite field, which can act as bases of the modular code, then the Haar DWT can be calculated in the RNS. In this case, the code allows correcting the single errors. To do this, we choose two redundant bases of the residue number system pk+1 and pk+2, which should satisfy the following condition

$$p_k p_{k-1} < p_{k+1} p_{k+2}, \tag{10}$$

where k is the number of working bases.

The code of the residue number system is considered permissible, if it belongs to the working range of the system

$$P^* = \prod_{i=1}^{k} p_i \; . \tag{11}$$

Now, the error, transforming the correct combination $A = (b_1, b_2, ..., b_{k+2})$ of the residue number system into a combination $\tilde{A} = (b_1, ..., \tilde{b}_i, ..., b_{k+2})$, where $b_i \equiv A mod\, p_i$, $\tilde{b}_i = b_i + \Delta b_i$ is a distorted residue of the RNS, Δb_i is the depth of the error, which carries out the transition of the distorted number outside of the working range. Therefore, to correct the error, the positional characteristics (PC) are used in the codes of the residue number system. Among the positional characteristics, a special place is occupied by the interval number, which is defined as

$$l_{\text{int}} = \left[A / P^* \right]. \tag{12}$$

If a number, represented in the RNS, belong to the working range, then the value of the interval number is equal to zero, i.e. l = 0. When an error in the number arises, A will not belong to the working range.

Since the division operation is non-modular, it is reduced to a set of modular operations. Let us make use of the Chinese Remainder Theorem (CRT), with the help of which there is carried out the reverse transition from the code of the residue number system into a positional representation (PR). Then we have the equality

$$A = b_1 B_1 + b_2 B_2 + ... + b_{k+2} B_{k+2} \, mod\, P = \sum_{i=1}^{k+2} b_i B_i \, mod\, P \quad , \tag{13}$$

where $P = \prod_{i=k+1}^{k+2} p_i$ is the complete range of the ordered redundant residue number system.

The basis of this algorithm is a similarity property of orthogonal bases of the complete and non-redundant residue number system, according to which there holds the relation

$$B_i^* \equiv B_i \, mod\, P^* , \tag{14}$$

where B_i^* are the orthogonal bases of the non-redundant RNS; B_i are the orthogonal bases of the complete RNS.

Then, using equality (14), we obtain the expression

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$B_i = \left\lfloor B_i \left(P^*\right)^{-1} \right\rfloor P^* + B_i^* = K_i P^* + B_j^* .$$

(15)

Substituting the last equality into the expression (12), we get the following result

$$l = \left[\sum_{i=1}^{k+2} b_i \left(K_i P^* + B_i^* \right) + RP \left(P^*\right)^{-1} \right].$$

(16)

where R is the rank of the complete system of bases of the residue number system. $P_{cont} = \prod_{i=k+1}^{k+2} p_i$ is a composite modulus of the RNS.

Performing simplifications of the expression (16), we have the equality

$$l = \left(\sum_{i=1}^{k+r} b_i K_i + \left[\sum_{j=1}^{k} \alpha_j B_j^* \left(P^*\right)^{-1} \right] + RP\left(P^*\right)^{-1} \right) \bmod P_{cont}$$

, (17)

The main shortcoming of this circuit realization is the use of the composite modulus Pcont . This problem can be solved by the transition to multidimensional data processing. Then the expression (17) will assume the form

$$\begin{cases} l^{k+1} = \left(\sum_{i=1}^{k+r} b_i K_i + \left[\sum_{j=1}^{k} \alpha_j B_j^* \left(P^*\right)^{-1} \right] + RP\left(P^*\right)^{-1} \right) mod\ p_{k+1} \\ l^{k+2} = \left(\sum_{i=1}^{k+r} b_i K_i + \left[\sum_{j=1}^{k} \alpha_j B_j^* \left(P^*\right)^{-1} \right] + RP\left(P^*\right)^{-1} \right) mod\ p_{k+2} \end{cases}$$

(18)

3. RESULTS

3.1. Performing The Direct And Inverse Discrete Haar Wavelet Transform In The Field GF (17)

Consider an example of realization of the Haar DWT in GF (17). Let there be given the 8-point input sequence $X(i) = [1,\ 1,\ 4,\ 4,\ 0,\ 0,\ 0,\ 1]$. Perform the large-scale analysis of the digital signal according to (2). We make use of the normalized Haar matrix, defined by the expression (7). Then

$$W(i) = H_8^{norm} x(i) = \begin{bmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 10 & 10 & 10 & 10 & 7 & 7 & 7 & 7 \\ 9 & 9 & 8 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 9 & 8 & 8 \\ 3 & 14 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 14 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 14 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 4 \\ 4 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \\ 14 \\ 8 \\ 0 \\ 0 \\ 0 \\ 14 \end{bmatrix}$$

. (19)

Where

$$W_\varphi(0,0) = \sum_{i=0}^{7} x(i)\varphi_{00}(i) = \left|10\cdot 1 + 10\cdot 1 + 10\cdot 4 + 10\cdot 4 + 10\cdot 1\right|_{17}^{+} = \left|110\right|_{17}^{+} = 8 .$$

The remaining components are calculated analogously. Using the field GF(17), there are obtained the values of the Haar DWT, which can be written in the form $W(i) = [8, 5, 14, 8, 0, 0, 0, 14]$. The obtained results allow representing the original sequence in the basis of the discrete Haar wavelet transform

$$X(i) = \left|8\varphi_{0,0} + 5\psi_{1,0} + 14\psi_{2,0} + 8\psi_{2,1} + 0\psi_{4,0} + 0\psi_{4,3} + 0\psi_{4,2} + 14\psi_{4,1}\right|_{17}^{+}$$

. (20)

Thus, the expression (19) can be represented in the form

$$x(nT) = \underbrace{\underbrace{\underbrace{8\varphi_{0,0}}_{V_0} + \underbrace{5\psi_{1,0}}_{W_0}}_{V_1=V_0\oplus W_0} + \underbrace{14\psi_{2,0} + 8\psi_{2,1}}_{W_1}}_{V_2=V_1\oplus W_1} + \underbrace{0\psi_{4,0} + 0\psi_{4,3} + 0\psi_{4,2} + 14\psi_{4,1}}_{W_2}}_{V_3=V_2\oplus W_2}$$

. (21)

Let us perform the inverse discrete Haar wavelet transform, using the expression (9). As the initial data, we will use $W(i) = [8, 5, 14, 8, 0, 0, 0, 14]$. Then we obtain the following result

$$X(i) = H_8^T W(i) = \begin{bmatrix} 10 & 10 & 9 & 0 & 3 & 0 & 0 & 0 \\ 10 & 10 & 9 & 0 & 14 & 0 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 3 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 14 & 0 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 3 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 14 & 0 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 3 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 14 \end{bmatrix} \times \begin{bmatrix} 8 \\ 5 \\ 14 \\ 8 \\ 0 \\ 0 \\ 0 \\ 14 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 4 \\ 4 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

.

3.2. Searching And Correcting Errors With The Help Of A Redundant Code Of The Residue Number System

Consider an example of calculating the interval positional characteristic. Let there be given an ordered RNS with the working bases p1 = 2, p2 = 3, p3 = 5. As the control bases, we will choose the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

following two bases: p4 = 7 and p5 = 11. Then the working range of this RNS will be equal to Pwork = 30. In this case, the complete range of such system Pcomp = 2310. In this complete system the bases of orthogonal basic sets equal $B_1 = m_1 p_2 p_3 p_4 p_5 = 1155$;
$B_2 = m_2 p_1 p_3 p_4 p_5 = 1540$;
$B_3 = m_3 p_1 p_2 p_4 p_5 = 1386$;
$B_4 = m_4 p_1 p_2 p_3 p_5 = 330$; $B_5 = m_5 p_1 p_2 p_3 p_4 = 210$
, where mi is the weight of the i-th orthogonal basis such that $B_i = m_i P(p_i)^{-1} \equiv 1 mod\, p_i$.

Let us represent the orthogonal bases of the RNS code, according to equality (15) in the following form

$$B_1 = 1155 = K_1 P_{work} + B_1^* = 38 \cdot 30 + 15;$$
$$B_2 = 1540 = K_2 P_{work} + B_2^* = 51 \cdot 30 + 10;$$
$$B_3 = 1386 = K_3 P_{work} + B_3^* = 46 \cdot 30 + 6;$$
$$B_4 = 330 = K_4 P_{work} = 11 \cdot 30;$$
$$B_5 = 210 = K_5 P_{work} = 7 \cdot 30.$$

For this RNS the value Pcont= 77. Suppose we have the number A = (0, 2, 2, 2, 2) = 2. Let us calculate the value of the rank in the non-redundant system defined by the bases p1 = 2, p2 = 3, p3 = 5.

$$R^* = \left[\sum_{j=1}^{3} b_j B_j^* \left(P^*\right)^{-1}\right] = \left[(0 \cdot 15 + 2 \cdot 10 + 2 \cdot 6) 30^{-1}\right] = 1$$

.

Then the value of the interval number for this combination of the RNS code will be equal to

$$l = \left|\sum_{i=1}^{k+2} b_i K_i + R^*\right|_{P_{cont}}^{+} = \left|0 \cdot 38 + 2 \cdot 51 + 2 \cdot 46 + 2 \cdot 11 + 2 \cdot 7 + 1\right|_{77}^{+} = 0$$

Since the interval equals zero, this combination of the RNS does not contain an error and is permissible.

Let an error have occurred with respect to the first base and its depth equals Δ b1 = 1. Then the modular code has the form A* = (1, 2, 2, 2, 2) = 1157. Now we calculate the value of the interval number for this number.

We calculate the value of the rank in the non-redundant system defined by the bases p1 = 2, p2 = 3, p3 = 5.

$$R^* = \left[\sum_{j=1}^{3} b_j B_j^* \left(P^*\right)^{-1}\right] = \left[(1 \cdot 15 + 2 \cdot 10 + 2 \cdot 6) 30^{-1}\right] = 1$$

.

Then the value of the interval number for this combination of the RNS code will be equal to

$$l = \left|\sum_{i=1}^{k+2} \alpha_i K_i + R^*\right|_{P_{cont}}^{+} = \left|1 \cdot 38 + 2 \cdot 51 + 2 \cdot 46 + 2 \cdot 11 + 2 \cdot 7 + 1\right|_{77}^{+} = 38$$

.

We use (18) to compute the positional characteristic for the number A = (0, 2, 2, 2, 2) = 2.

$$\begin{cases} l_4 = \left|\sum_{i=1}^{k+2} b_i K_i + R^*\right|_{p_4}^{+} = \left|0 \cdot 38 + 2 \cdot 51 + 2 \cdot 46 + 2 \cdot 11 + 2 \cdot 7 + 1\right|_{7}^{+} = 0 \\ l_5 = \left|\sum_{i=1}^{k+2} b_i K_i + R^*\right|_{p_5}^{+} = \left|0 \cdot 38 + 2 \cdot 51 + 2 \cdot 46 + 2 \cdot 11 + 2 \cdot 7 + 1\right|_{11}^{+} = 0 \end{cases}$$

.

Since the interval equals zero, this combination of the RNS does not contain an error and is permissible.

Let us carry out the calculation of the positional characteristic for the erroneous number A = (1, 2, 2, 2, 2).

$$\begin{cases} l_4 = \left|\sum_{i=1}^{k+2} b_i K_i + R^*\right|_{p_4}^{+} = \left|1 \cdot 38 + 2 \cdot 51 + 2 \cdot 46 + 2 \cdot 11 + 2 \cdot 7 + 1\right|_{7}^{+} = 3 \\ l_5 = \left|\sum_{i=1}^{k+2} b_i K_i + R^*\right|_{p_5}^{+} = \left|1 \cdot 38 + 2 \cdot 51 + 2 \cdot 46 + 2 \cdot 11 + 2 \cdot 7 + 1\right|_{11}^{+} = 5 \end{cases}$$

The obtained result is different from zero. It means that the combination contains an error. In this case, for the bases p4=7, p5=11 the obtained interval, defined by the residues l = (3, 5), will be equal to

$$l = l_4 B_4^{'} + l_5 B_5^{'} \bmod P_{cont} = 3 \cdot 22 + 5 \cdot 56 \bmod 77 = 38$$

where $B_4^{'} = m_4 p_5 \equiv 1 mod\, p_4$ is the orthogonal basis with respect to the control base $p_4 = 7$; $B_5^{'} = m_5 p_4 \equiv 1 mod\, p_5$ is the orthogonal basis with respect to the second control base $p_5 = 11$.

4. DISCUSSION

The results presented in this work indicate the possibility of realization of the large-scale analysis of signals using algebraic structures having the properties of a ring and a field. The transition to the integer-valued implementation of the discrete

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

wavelet transformation allows diminishing the calculation errors that are caused by the size of the bit grid. Moreover, the realization of the Haar DWT in the finite field GF (17) has showed that not only the direct and inverse transformations can be performed with zero error, but it is also possible to increase the speed of computations.

To increase the accuracy of the processed data, one can go from one-dimensional to multidimensional signal processing, using an isomorphism generated by the Chinese remainder theorem. If the corresponding characteristics of finite fields GF (p) are chosen as the bases the residue number system, then the discrete Haar wavelet transformation can be represented by the following system of equations

$$\begin{cases} |W(i)|_{p_1}^{+} = \left| |H_N|_{p_1}^{+} |x(i)|_{p_1}^{+} \right|_{p_1}^{+} \\ \vdots \\ |W(i)|_{p_k}^{+} = \left| |H_N|_{p_k}^{+} |x(i)|_{p_k}^{+} \right|_{p_k}^{+} \end{cases}, \quad (22)$$

where $p_1, p_2, \ldots, p_k$ are the characteristics of the finite Galois fields.

The representations of (19) and equation (22) are equivalent from the mathematical point of view. However, if we think about the ease of hardware implementation, they are quite different. In the works [6], [10], [18] there are presented the results of implementation of orthogonal transformations of signals in a ring of polynomials, which serve as bases of a polynomial modular code. The conducted studies have shown the expediency of transition to multi-dimensional signal processing. Thus, selecting the number of bases and their values, one can ensure the required degree of accuracy of the Haar DWT, while reducing to zero the calculation error. The processing of the short-bit residues via parallel computational paths, determined by the RNS bases, enhances the speed of computations. If we take as the working bases of RNS the numbers p1 = 7, p2 = 17, p3 = 23, p4 = 31, then the computations in the integer Haar DWT will be in the range of P* = 84847, which corresponds to the processing of 16-bit data. In addition, the number of bits of the data, entering the computation paths of the residue number system, does not exceed 5 bits. This example clearly demonstrates the advantage of implementation of the integer-valued large-scale analysis of signals in the residue number system, both from the point of view of ensuring the minimum errors and from the point of view of providing higher speed of computation of the Haar DWT. Moreover, the productivity gain will increase with the increase of the number of bits of the processed input vector of signal.

Along with high speed, the nonpositional modular codes allow obtaining the true undistorted result of calculations. The application of the redundant nonpositional modular code allows detecting and correcting errors that occur during the operation of special DWT processor because of malfunctions and failures of the equipment. Since the modular codes are nonpositional, then in order to perform this procedure, it is necessary to calculate the positional characteristic. Currently, the following positional characteristics of nonpositional codes of the residue class have the widest application.

In the works [10], [5] the algorithms are presented that allow detecting and correcting errors in the code of the residue class using an extension procedure for the system of bases. In the foundation of this extension procedure, based on the calculation of the error syndrome with respect to control bases, there is the determination of the difference between the values of the remainders b_{k+1}, b_{n+2} with respect to the control bases of the RNS code $A = (b_1, b_2, \ldots, b_{k+2})$ and the results of computing the remainders b'_{k+1}, b'_{k+2} using the working bases. Mathematically, this algorithm can be represented by the following expression

$$\begin{cases} v_{k+1} = \left| b_{k+1} - b'_{k+1} \right|_{p_{k+1}}^{+} \\ v_{k+2} = \left| b_{k+2} - b'_{k+2} \right|_{p_{k+2}}^{+} \end{cases} \quad (23)$$

where $b'_j = f(b_1, \ldots, b_k);\ j = k+1, k+2$; f is the algorithm of computing the remainders with respect to the working bases.

In the paper [20] an algorithm is presented of the detection and correction of errors using some positional characteristics, namely, the coefficients of a generalized polyadic system (GPS). This algorithm is based on the calculation of coefficients of an intermediate polyadic system, in which the number A is represented in the form

$$A = a_1 + a_2 p_1 + a_3 p_1 p_2 + \ldots + a_{k+2} p_1 p_2 \ldots p_{k+1} \quad (24)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where a_i are the coefficients of the generalized polyadic system; $i = 1, 2, ..., k+2$.

If the bases p1, p2, …, pk+1, pk+2 simultaneously serve as the bases of a residue number system and a GPS, then the variation intervals of the digits at the same positions will coincide. Hence, if we provide matching between the bases of the GPS and the bases of the residue number system, then the following holds

$$A = (b_1, \quad b_2, \quad ..., \quad b_{k+2}) = [a_1, \quad a_2, \quad ..., \quad a_{k+2}] \quad (25)$$

Using the condition that the value of the working range of the RNS is determined by (11), we conclude that the expression (19) assumes the form

$$A = a_1 + a_2 p_1 + ... + a_{k+1} P^* + a_{k+2} P^* p_{k+1}. \quad (26)$$

On the basis of (24) we can claim that if the RNS code of the number A belongs to the working range P*, then the leading coefficients of the GPS, corresponding to the control bases, must be equal to zero

$$a_{k+1} = 0, a_{k+2}(z) = 0 . \quad (27)$$

In the contrary case, the RNS code of the number A contains an error and is outside of the working range of the RNS.

In the paper [8], such positional characteristic as the trace of number is used for the error correction in the codes of the residue number system. An algorithm for computing the trace of number consists in successive subtraction from the original modular code of some minimum numbers represented in the RNS code. These numbers are called zero-making constants; here the modular code of the number A is successively transformed to the form $(0, b_2^1, b_3^1, ..., b_k^1, b_{k+1}^1, b_{k+2}^1)$, and then into the residue class code $(0, 0, b_3^2, ..., b_k^2 b_{k+1}^2, b_{k+r}^2)$, and so forth. Carrying out this procedure during k iterations, we obtain the trace of the number, which was presented by the code $(0, 0, ..., s_{k+1}, s_{k+2})$ of the residue number system.

Application of the classical algorithm for computing the trace of number allows successively obtaining the smallest number that is, first, a multiple of p1, then a number, which is a multiple of the product of the first and second bases $p_1 p_2$, and, eventually, a number, which is a multiple of the working range defined by the expression (11). The major shortcoming of this algorithm of computing the trace of number is the sequential character of the computational process, which does not allow its implementing on the basis of a two-layer neural network. This is due primarily to the fact that the zero-making constants are the smallest possible numbers, whose values are determined at each iteration step.

To apply the developed parallel algorithm for computing the trace of number, it is necessary to replace the zero-making constants by the pseudo-orthogonal numbers. These include orthogonal bases, for which orthogonality is broken with respect to the control bases. The use of pseudo-orthogonal bases as zero-making constants allows going from the successive realization of the algorithm for calculating the trace of number to the parallel one. In connection with this, some additional opportunities are opened up to reduce the realization time of the process of determining the location of error and its depth.

However, the desire to provide high operational speed has led to significant hardware expenditures in the construction of the error correction block. The above algorithms are characterized by considerable circuit and time expenses. In this paper, an algorithm is proposed which allows carrying out error correction under minimal redundancy, introduced into the residue number system. To eliminate the indicated shortcomings, there has been developed an algorithm for calculating the interval of number, which uses the isomorphism of the Chinese remainder theorem. Moreover, the transition to multidimensional calculation of the positional characteristic does not affect the corrective abilities of the RNS modular code. For a given redundancy of the residue number system code, the usage of the developed algorithm allows correcting all the single errors and over 80 percent of the double ones, while requiring smaller circuit expenditures.

In the above example, to correct all single errors with respect to the bases of residue classes, the introduction of two control bases will be required, which can be selected as p5 = 41 и p6 = 47. In the realization of the algorithm given by the expression (17), the calculation of the number's interval will be performed modulo Pcont = 1927, which corresponds to the processing of the operands requiring 11 bits for its representation in the binary code. The application of the algorithm defined by equation (18) allows carrying out an analogous procedure while processing 6-bit data. It is obvious that the second case will require less of hardware and time resources to compute the positional

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

characteristic of the redundant code of the residue number system.

5. CONCLUSION

The realization of the discrete wavelet transform in the algebraic systems having the properties of a ring and a field enhances the calculation accuracy during carrying out the large-scale analysis of signals. The results presented in the paper have showed that the use of modular arithmetic enables to obtain the approximating and detailing coefficients of the expansion of digital signals, the calculation errors of which is completely reduced to zero. Besides, the application of modular codes allows improving the fault-tolerance of the specialized DWT processors. In this paper we present an algorithm of computing a certain PC, namely, the number's interval, which is characterized by minimal circuit and time recourses for its implementation. The use of the proposed modular technologies will enable to design fault-tolerant special processors which carry out the discrete wavelet transform of signals in real time. Concerning the prospects of implementation of modular technologies in DSP, we can note the following. As the practice shows, in the implementation of the large-scale analysis of signals, the Daubechies wavelets are widely used. The approach of the present paper suggests that the use of nonpositional modular codes will improve the accuracy and speed of implementation of such DWT by virtue of switching to the integer-valued parallel computing.

REFERENCES:

[1] Bankas, E., & Gbolagade, K. (2013). A New Efficient FPGA Design of Residue-to-Binary Converter. *International Journal of VLSI design & Communication Systems (VLSICS), 4*(6). doi: 10.5121/vlsic. 2013.4601.

[2] Barsagaev, A., & Kalmykov, M. (2014). Algorithms for Detection and Correction of Errors in the Modular Polynomial Codes. *International Journal of Experimental Education, 3*(1), 103-107.

[3] Berezhnoi, V., Chervyakov, N., Shchelkunova, Yu., & Shilov, A. (2004). Neural Network Realization in a Polynomial System of Residue Classes of the DSP Operations of Increased Digit Capacity. *Neurocomputers: Development and Application, 5*(6), 94-98.

[4] Camenisch, J., Gross T., & Sommer D. (2012, December 25). *Assertion message signatures. Patent US 8 341 416 B2*.

[5] Chernomazov, S., Kalmykov, M., & Martirosyan, A. (2014). Development of a Detecting Device and Error Correction on the Basis of an Algorithm of Extension of the System of Bases of a Modular Code // Modern Science-Intensive Technologies. 11: 41 - 46.

[6] Chervyakov, N., Shchelkunova, Yu., & Berezhnoi, V. (2003). Mathematical Model of Neural Networks for Studying Orthogonal Transformations in the Extended Galois Fields. *Neurocomputers: Development and Application, 6*, 61-68.

[7] Dagaeva, O., et al. (2013). Systemic Approach to the Application of Pseudo-Random Functions in the Information Security Systems. *Proceedings of the Southern Federal University. Technical Sciences, 12*(149), 228-234.

[8] Gapochkin, A., Kalmykov, M., & Airiyan, A. (2014). Correction of Errors in the Modular Code Based on an Algorithm of Parallel Calculation of Trace. *International Journal of Experimental Education, 8*(3), 34-38.

[9] Gbolagade, K. (2013). An Efficient MRC Based RNS-to-Binary Converter for the $\{2^{2n-1}, 2^{n}, 2^{2n+1}-1\}$ Moduli Set. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2*(4).

[10] Gordenko, D., Resen'kov, D., & Sarkisov, A. (2014). *Methods and algorithms of reconfiguration of nonpositional computational structures for providing fault-tolerance of special processors.* Stavropol: Fabula.

[11] Kalmykov, I., Katkov, K., Naumenko, D., Sarkisov, A., Makarova, A. (2014). Parallel Modular Technologies in Digital Signal Processing. *Life Science Journal, 11*(11s), 435-438.

[12] Katkov, K., & Kalmykov, I. (2013). Application of Parallel Technologies in Navigation Management under the Conditions of Artificial Ionospheric Disturbances. *World Applied Sciences Journal, 26*(1), 108-113. doi: 10.5829/idosi.wasj.2013.26.01.13467

[13] Molahosseini, A., & Navi, K. (2007). New Arithmetic Residue to Binary Converters. *International Journal of Computer Sciences and Engineering Systems, 1*(4), 295-299.

[14] Omondi, A., & Premkumar, B. (2007). *Residue number systems: theory and implementation*. UK: Imperial College Press.

[15] Pashintsev, V., et al. (2014). Methods of the Transmitted Information Protection for the Systems of Remote Monitoring and Control of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

High-Tech Objects. *Bulletin of the North-Caucasus Federal University, 4*(43), 38-43.

[16] Wang, Q. (2011). Compact k-spendable E-cash with Anonymity Control Based Offline TTP. *International Journal of Innovative Computing, Information and Control, 7*(1), 459-469.

[17] Sarkisov, A., Makarova, A., & Kalmykov, M. (2014). Extension of the Methods of Protection of the E-commerce Systems Based on the Modular Algebraic Schemes. *Proceedings of the Southern Federal University. Technical sciences, 2*(151), 218-225.

[18] Sarkisov, A., et al. (2013). Systolic Modular Digital Signal Processor with Reconfigurable Structure. *Bulletin of the North-Caucasian Federal University, 2*(35), 30-34.

[19] Siewobr, H., & Gbolagade, K. (2014). RNS Overflow Detection by Operands Examination. *International Journal of Computer Applications (0975 – 8887), 85*(18).

[20] Strizhkov, N., & Kalmykov, M. (2014). Algorithm of Conversion from a Modular Code to a Polyadic System of Bases for the Systems of Error Detection and Correction. *International Journal of Experimental Education, 3*(1), 127-132.

[21] Chervyakov N. I., Evdokimov A.A. et al. (2012). *Application of artificial neural networks and the residue number systems in cryptography*. Moscow, Fizmatlit.

[22] Younes, D., & Steffan, P. (2013). Universal Approaches for Overflow and Sign Detection in Residue Number System Based on $\{2^{n-1}, 2^{n}, 2^{n+1}\}$. *The Eighth International Conference on Systems (ICONS 2013)*, 77-84.