Structural and Informational Diversity of Digital Filters Based on Multivariate Arithmetic of Finite Field

Alexander Veligosha
Military Academy of Strategic Rocket Forces
Serpuhov, Russian Federation
aveligosha@mail.ru

Dmitrii Kaplun, Alexander Voznesenskiy,
Danil Bogaevskiy
Saint Petersburg Electrotechnical University "LETI"
St. Petersburg, Russian Federation
dikaplun@etu.ru

***Abstract*–In modern computing systems, one of the most commonly used algorithms for digital signal processing is digital filtering. Digital filters are implemented by various hardware. One of the main properties of any hardware structure is its fault tolerance. The main way to increase fault tolerance is the introduction of redundancy, as a rule, hardware redundancy. In existing computational structures, the introduction of redundancy is associated with an increase in computation time and hardware costs, which in some cases is unacceptable. To eliminate the drawbacks of these methods and ensure the reliability of the results of calculations, it is proposed to investigate the possibility of using multivariate finite field arithmetic to ensure the structural and information reliability of digital filters.**

I. Introduction

One of the most important properties of the residue number system (RNS) codes is its natural corrective abilities. The redundancy of the corrective RNS codes lies in the fact that the number of computing channels of the computing device increases while maintaining information reliability and structural diversity as opposed to the data processed range [1].

The detailed studies of the corrective RNS codes, the opportunity of their application in the construction of digital filters is held in [2], [3]. The using of the natural corrective capabilities of the RNS codes allows to detect and correct computation errors of any given multiplicity and to build the diversified structure of the digital filters (DF).

The diversified property of the DF structure means that any failed computational modular channel (several channels) can be replaced with computational channels in the control modules. This allows:

1) To provide the required degree of the diversity DF structure by reducing the correcting ability without decreasing the data range.

2) To implement all signal processing procedures in the DF codes without increasing hardware costs, since the imposition of the additional computational control channels is necessary to detect and correct errors and ensure the structural reliability of a non-position filter [4].

The interesting approach is described in [1], [5], where the possibility of providing structural and informational diversity of the DFs structures based on the using of a multivariate algebra of a finite field and a generalized polyadic number system was shown. As highlighted in [5-8], a generalized polyadic system can be used in constructing algorithms for searching and correcting errors in the RNS codes, which ensures the diversity of the DF structures.

II. Generalized Polyadic System

The generalized polyadic system (GPS) is a mixed number system, which is often used for performing the inverse transformation from the RNS code to the position code [1], [5], [9], [10]. Mutually simple bases $p_1, p_2, ..., p_k$ are selected in this system, by means of which an arbitrary number A is presented in the form:

$$A = b_k(p_1p_2...p_{k-1}) + b_{k-1}(p_1p_2...p_{k-2}) + ... + b_3(p_1p_2) + b_2p_1 + b_1 \quad (1)$$

where b_i is the coefficients of the GPS; $i = 1, 2, ..., k$.

Consider a redundant modular code, which contains two control bases. Then the set of bases is determined by $p_1, p_2, ..., p_k, p_{k+1}, p_{k+2}$. In addition, the control base implementation leads to expansion of the range to a value:

$$P_{total} = \prod_{i=1}^{k+2} p_i = P_{work}p_{k+1}p_{k+2} \quad (2)$$

Then the A number can be represented as:

$$\begin{aligned} A &= b_1 + b_2p_1 + ... + b_k(p_1p_2...p_{k-1}) + ... \\ &+ b_{k+1}(p_1p_2...p_{k-1}p_k) + b_{k+2}(p_1p_2...p_{k+1}) = \\ &= b_1 + b_2p_1 + ... + b_k(p_1p_2...p_{k-1}) + b_{k+1}P_{work} + b_{k+2}P_{work}p_{k+1}. \end{aligned} \quad (3)$$

The number is represented as a set of coefficients $A = (b_1, b_2, \ldots, b_k, b_{k+1}, b_{k+2})$ in redundant GPS code. The analysis of the (3) expression shows that only the two highest coefficients of GPS b_{k+1} and b_{k+2} are multiplied by the value of the working range when representing the number A.

If the condition such that the A number belongs to the working range, i.e. when $A < P_{work}$, the expression (3) takes the form

$$\begin{aligned} & A = b_1 + b_2 p_1 + \ldots + b_k (p_1 p_2 \ldots p_{k-1}) + \ldots \\ & + b_{k+1}(p_1 p_2 \ldots p_{k-1} p_k) + b_{k+2}(p_1 p_2 \ldots p_{k+1}) = \\ & = b_1 + b_2 p_1 + \ldots + b_k (p_1 p_2 \ldots p_{k-1}) + 0 \cdot P_{work} + 0 \cdot P_{work} p_{k+1} . \end{aligned} \tag{4}$$

In accordance with the expression (4) it is got $A = (b_1, b_2, ..., b_k, 0, 0)$. Thus, it is obvious that if the highest coefficients of the generalized polyadic system are equal to zero, then the corresponding number belongs to the working range. If the range of numbers that can be represented in the RNS code and generalized system polyadic match, then the equality

$$A = (\alpha_1, \alpha_2, ..., \alpha_k, \alpha_{k+1}, \alpha_{k+2}) = (b_1, b_2, ..., b_k, b_{k+1}, b_{k+2}) \tag{5}$$

In this, the values of GPS coefficients satisfy the condition

$$0 \le b_i \le p_i - 1 , \tag{6}$$

where $i = 1, 2, \ldots, k+2$.

Thus, the coefficients of the GPS vary in the field (ring) on the corresponding module p$_i$. Consider the algorithms that allow to calculate the GPS coefficients.

III. Calculation the GPS coefficients

An iterative algorithm is presented for calculating GPS coefficients in [5]. Analysis of the expression (3) shows that it is possible to use the following algorithm for obtaining the coefficients of the GPS:

1) The initial value of the number A is divided by the first base p$_1$. The resulting residue $b_1 = rest\left(\frac{A}{p_1}\right)$ is the first GPS coefficient.

2) The quotient $A_1 = \left[\frac{A}{p_1}\right]$ is divided by the second base $p2$. The resulting residue $b_2 = rest\left(\frac{A_1}{p_2}\right)$ is the second GPS coefficient.

3) The quotient $A_2 = \left[\frac{A_1}{p_2}\right]$ is divided by the third base $p3$. The resulting residue $b_3 = rest\left(\frac{A_2}{p_3}\right)$ is the third coefficient of the GPS.

4) The quotient from the previous step $A_{k-1} = \left[\frac{A_{k-2}}{p_{k-1}}\right]$ is the b_k GPS coefficient.

Consider an example explaining the considered algorithm of calculating GPS coefficients. As working bases it is chosen $p_1 = 7, p_2 = 17, p_3 = 23, p_4 = 31$.

An arbitrary number $A = 14237$ is chosen, which belongs to the working range $P_{work} = 84847$. Then the code of the GPS number has the form $A = (b_1, b_2, b_3, b_4)$.

To calculate the first GPS coefficient it is determined $b_1 = rest\left(\frac{A}{p_1}\right) = rest\left(\frac{14237}{7}\right) = 6$. In this quotient is $A_1 = \left[\frac{A}{p_1}\right] = \left[\frac{14237}{7}\right] = 2033$.

To calculate the second GPS coefficient it is determined $b_2 = rest\left(\frac{A_1}{p_2}\right) = rest\left(\frac{2033}{17}\right) = 10$. In this quotient is $A_2 = \left[\frac{A_1}{p_2}\right] = \left[\frac{2033}{17}\right] = 119$.

To calculate the third GPS coefficient it is determined $b_3 = rest\left(\frac{A_2}{p_3}\right) = rest\left(\frac{119}{23}\right) = 4$.

The value of the fourth GPS coefficient is $b_4 = \left[\frac{A_2}{p_3}\right] = \left[\frac{119}{23}\right] = 5$.

Thus, the number A, represented in the generalized polyadic system, has the form $A = (6, 10, 4, 5)$. Checking the correctness of the number A representation in the GPS:

$$\begin{aligned} & A = b_1 + b_2 p_1 + b_3 p_1 p_2 + b_4 p_1 p_2 p_3 = \ldots \\ & = 6 + 10 \cdot 7 + 4 \cdot 119 + 5 \cdot 2737 = 14237 \end{aligned}$$

The result shows the correctness of the number A representation in the GPS. However, in a number of applications, the transition to the coefficients of the generalized polyadic system must be made from the RNS code.

IV. Calculation the GPS coefficients from the RNS code

An algorithm is presented that makes it possible to calculate the GPS coefficients from the RNS code in [1], [5]. To determine the coefficients of the generalized polyadic system, the following expressions are used:

$$b_k = rest\ A_k \bmod p_k \tag{7}$$

where A_k is determined by the recurrence formula:

$$A_j = (A_{j-1} - \alpha_{j-1}) w_{j-1} \tag{8}$$

where $A_1 = A$; $w_j = p_j^s$ is the formal inverse of the j^{th} base on the s^{th} base ($s \ne k$); α_{j-1}^* is a set of residues for all modules which numbers are higher than the number $j-1$; $j = 1, 2, ..., k$.

In doing so, all operations for calculating the GPS coefficients are performed in the finite field arithmetic.

Using this algorithm for calculating GPS coefficients, consider an example. It is chosen $p_1 = 7, p_2 = 17, p_3 = 23, p_4 = 31$ as working bases. Choose an arbitrary number A = 14237, which belongs to the working range $P_{work} = 84847$. Then it's got the code RNS number $A = (6, 8, 0, 8)$. The inverse values of w_j , which are used in this algorithm, are calculated and presented in Table I.

TABLE I. FORMAL INVERSE VALUE

	$mod\ p_1 = 7$	$mod\ p_2 = 17$	$mod\ p_3 = 23$	$mod\ p_4 = 31$
$w_1 = p_1^{-1} \bmod p_i$	-	5	10	9
$w_2 = p_2^{-1} \bmod p_i$	5	-	19	11
$w_3 = p_3^{-1} \bmod p_i$	4	3	-	27
$w_4 = p_4^{-1} \bmod p_i$	5	11	3	-

According to equality (7), it was found the first coefficient of the GPS $b_1 = \alpha_1 \bmod p_1 = 6$.

It is possible to determine a second coefficient GPS, using expression (8). In this case, the calculations occur on the basis of the code RNS. Then:

$$A_2 = (A_1 - b_1)w_1 = ((6,8,0,8) - (6,8,0,8))(0,5,10,9) =$$
$$= (0,2,17,2)(0,5,10,9) = (-,10,9,18).$$

As a result, $b_2 = \alpha_2 = 10$.

Hence, one can determine the third GPS ratio using the expression (8). Then

$$A_3 = (A_2 - b_2)w_2 = ((\_,10,9,18) - (-,10,10,10))(-,0,19,11) =$$
$$= (-,0,22,8)(\_,0,19,11) = (\_,\_,4,26).$$

As a result, $b_3 = \alpha_3 = 4$.

One can determine the fourth GPS coefficient, using the expression (8). Then

$$A_4 = (A_3 - b_3)w_3 = ((\_,\_,4,26) - (\_,\_,4,4))(\_,\_,0,27) =$$
$$= (\_,\_,0,22)(\_,\_,0,27) = (\_,\_,\_,5).$$

As a result, $b_3 = \alpha_3 = 4$.

One can determine the fourth GPS coefficient, using the expression (8). Then

$$A_4 = (A_3 - b_3)w_3 = ((\_,\_,4,26) - (\_,\_,4,4))(\_,\_,0,27) =$$
$$= (\_,\_,0,22)(\_,\_,0,27) = (\_,\_,\_,5).$$

As a result, $b_4 = \alpha_4 = 5$

Therefore, the number was transferred from the RNS code A = (6, 8, 0, 8) to the GPS code A = (6, 10, 4, 5).

There are other algorithms for converting from modular code to GPS code. An iterative algorithm is presented for converting to a generalized polyadic system in [5]. To implement this algorithm, expression (1) is converted to:

$$A = a_1 + p_1(a_2 + p_2(a_3 + ... + p_{n-2}(a_{n-1} + p_{n-1}a_n)...)) \quad (9)$$

Then to calculate the coefficients of the GPS are used

$$\begin{aligned} a_1 &= A - \left[A/p_1\right]p_1 = A - A_1\,p_1; \\ A_1 &= \left[A/p_1\right] \\ a_2 &= A_1 - \left[A_1/p_2\right]p_2 = A_1 - A_2\,p_2; \\ A_2 &= \left[A_1/p_2\right] \\ &\dots \\ a_n &= A_{n-1} - \left[A_{n-1}/p_n\right]p_n = A_{n-1} - A_n\,p_n; \\ A_n &= \left[A_{n-1}/p_n\right] \end{aligned} \quad (10)$$

It is obvious, the presented algorithm for recalculating the code of RNS into the coefficients of the GPS can be implemented using modular operations. Analysis of expression (10) shows that to perform this algorithm, one needs to perform $2(n-1)$ modular operations, where n is the number of bases of the RNS.

Define a constant in the form of

$$\tau_{kj} = (1/p_k)\bmod p_j = p_k^{-1} \bmod p_j \quad (11)$$

In this case, the GPS coefficients are calculated as follows

$$\begin{aligned} a_1 &= \alpha_1 \\ a_2 &= (\alpha_2 - a_1)\tau_{12} \bmod p_2 \\ a_3 &= ((\alpha_3 - a_1)\tau_{13} - a_2)\tau_{23} \bmod p_3 \\ &\dots \\ a_n &= ((\alpha_n - a_1)\tau_{1n} - a_2)\tau_{2n} - a_3)\tau_{3n} - ... - a_{n-1})\tau_{(n-1)n} \bmod p_n \end{aligned} \quad (12)$$

Consider an example of translating the RNS code into a code of a generalized polyadic system. As working bases it is used $p_1 = 7, p_2 = 17, p_3 = 23, p_4 = 31$. Choose an arbitrary number $A = 14237$, which belongs to the working range $P_{work} = 84847$. Then, the RNS code of the number A is represented $A = (6, 8, 0, 8)$. Find constants used in the algorithm:

$$\begin{aligned} \tau_{12} &= 7^{-1} \bmod 17 = 5 \\ \tau_{13} &= 7^{-1} \bmod 23 = 10 \\ \tau_{14} &= 7^{-1} \bmod 31 = 9 \\ \tau_{23} &= 17^{-1} \bmod 23 = 19 \\ \tau_{24} &= 17^{-1} \bmod 31 = 11 \\ \tau_{34} &= 23^{-1} \bmod 31 = 27 \end{aligned} .$$

Based on the presented algorithm, one can obtain the following coefficients of the generalized polyadic number system:

$$b_1 = \alpha_1 = 6;$$

$$b_2 = (\alpha_2 - b_1)\tau_{12} \bmod p_2 = \left|((8-6)\cdot 5\right|_{17}^{+} = 10.$$

$$\begin{aligned} b_3 &= ((\alpha_3 - b_1)\tau_{13} - b_2)\tau_{23} \bmod p_3 = \ldots \\ &= \left|((0-6)\cdot 10 - 10)\cdot 19\right|_{23}^{+} = 4 \end{aligned}.$$

$$\begin{aligned} b_4 &= \left|(((\alpha_4 - b_1)\tau_{14} - b_2)\tau_{24} - b_3)\tau_{34}\right|_{p_4}^{+} = \ldots \\ &= \left|(((8-6)\cdot 9 - 10)\cdot 11 - 4)\cdot 27\right|_{31}^{+} = 10 \end{aligned}$$

As a result of the conversion, the RNS code of the number $A = (6,\ 8,\ 0,\ 8)$ is converted into the GPS code of the number $A = (6,\ 10,\ 4,\ 10)$. This result coincided with the result was obtained on the basis of an iterative algorithm.

However, the considered algorithms are iterative in nature, and this fact leads to a decrease in the speed of the non-modular conversion operation RNS code to GPS code. This drawback can be eliminated by the development of the algorithm for transform to GPS based on Chinese remainder theorem (CRT) [6], [7].

V. The Algorithm for Transform to GPS Based on Chinese Remainder Theorem

According to the CRT, the value of the number is determined in the positional numeral systems (PNS).

$$A = \alpha_1 B_1 + \ldots + \alpha_{k+r} B_{k+r} = \sum_{i=1}^{k+r} \alpha_i B_i \bmod P_{total} \qquad (13)$$

where B_i is the orthogonal i^{th} basis value of the modular code.

For implementation the developed algorithm, it is necessary to represent the orthogonal bases in the form of GPS coefficients. In this case, one can write

$$\begin{aligned} B_1 &= 1 + b_2^1 p_1 + b_3^1 p_1 p_2 + b_4^1 p_1 p_2 p_3 + \ldots + b_{k+r}^1 \prod_{i=1}^{k+r-1} p_i \\ B_2 &= 0 + b_2^2 p_1 + b_3^2 p_1 p_2 + b_4^2 p_1 p_2 p_3 + \ldots + b_{k+r}^2 \prod_{i=1}^{k+r-1} p_i \\ B_3 &= 0 + 0 + b_3^3 p_1 p_2 + b_4^3 p_1 p_2 p_3 + \ldots + b_{k+r}^3 \prod_{i=1}^{k+r-1} p_i \qquad (14) \\ &\ldots \\ B_{k+r} &= 0 + 0 + 0 + 0 + \ldots + 0 + b_{k+r}^{k+r} \prod_{i=1}^{k+r-1} p_i \end{aligned}$$

.

where b_i^j is the j^{th} GPS coefficient of the i^{th} orthogonal basis of the RNS code.

To transfer from RNS code in GPS code, one must first multiply the remainder of the modular code by the corresponding values of the GPS orthogonal basis coefficients. And then add the obtained values module p_i, $i = 1,\ 2,\ \ldots,\ k + r$, taking into account the number of transitions beyond the previous module p_{i-1}. So one can get:

$$\begin{aligned} b_1 &= 1\cdot\alpha_1, \\ b_2 &= (\alpha_1 b_2^1 + \alpha_2 b_2^2) \bmod p_2, \\ b_3 &= (\alpha_1 b_3^1 + \alpha_2 b_3^2 + \alpha_3 b_3^3 + \gamma_2) \bmod p_3, \\ &\ldots \\ b_{k+r} &= (\alpha_1 b_{k+r}^1 + \alpha_2 b_{k+r}^2 + \alpha_3 b_{k+r}^3 + \ldots + \alpha_{k+r} b_{k+r}^{k+r} + \gamma_{k+r-1}) \bmod p_{k+r}. \end{aligned} \qquad (15)$$

where γ_i – the number of transitions is outside the p_i; $i = 1,\ 2,\ \ldots,\ k + r$.

It is known that the orthogonal basis can be represented as [1], [6]

$$B_i = m_i P_i = m_i \frac{P_{total}}{p_i}.$$

To reduce the number of exceedances beyond the base limit of the RNS code, a modification of this algorithm allows for the calculation of the GPS coefficients. Then

$$\begin{aligned} b_1 &= 1\cdot\alpha_1, \\ b_2 &= (\left|\alpha_1 m_1\right|_{p_1}^{+} P_2^1 + \left|\alpha_2 m_2\right|_{p_2}^{+} P_2^2) \bmod p_2, \\ b_3 &= (\left|\alpha_1 m_1\right|_{p_1} P_3^1 + \left|\alpha_2 m_2\right|_{p_2}^{+} P_3^2 + \left|\alpha_3 m_3\right|_{p_3}^{+} P_3^3 + \gamma_2^*) \bmod p_3, \\ &\ldots \\ b_{k+r} &= (\left|\alpha_1 m_1\right|_{p_1} P_{k+r}^1 + \left|\alpha_2 m_2\right|_{p_2}^{+} P_{k+r}^2 + \ldots \\ &+ \left|\alpha_{k+r} m_{k+r}\right|_{p_{k+r}}^{+} P_{k+r}^3 + \gamma_{k+r-1}^*) \bmod p_{k+r}. \end{aligned} \qquad (16)$$

where P_i^j – j^{th} GPS coefficient of i^{th} value of the constant P_i RNS code; γ_i^* – the number of transitions beyond the module p_i; $i = 1,\ 2,\ \ldots,\ k + r$.

In this case, one can use the following representation of the constants RNS in the form of GPS

$$\begin{aligned} P_1 &= 1 + P_2^1 p_1 + P_3^1 p_1 p_2 + P_4^1 p_1 p_2 p_3 + \ldots + P_{k+r}^1 \prod_{i=1}^{k+r-1} p_i \\ P_2 &= 0 + P_2^2 p_1 + P_3^2 p_1 p_2 + P_4^2 p_1 p_2 p_3 + \ldots + P_{k+r}^2 \prod_{i=1}^{k+r-1} p_i \\ P_3 &= 0 + 0 + P_3^3 p_1 p_2 + P_4^3 p_1 p_2 p_3 + \ldots + P_{k+r}^3 \prod_{i=1}^{k+r-1} p_i \qquad (17) \\ &\ldots \\ P_{k+r} &= 0 + 0 + 0 + 0 + \ldots + 0 + P_{k+r}^{k+r} \prod_{i=1}^{k+r-1} p_i \end{aligned}$$

In order to increase the speed of calculating the GPS coefficients based on the formulated algorithm, it is possible to use CAS-adders [9]. The block diagram calculation of the GPS coefficients is represented on the Fig. 1. This block is intended to translate a code combination consisting of six residues into a code of a generalized polyadic system. Consider an example using the proposed modified algorithm for calculating GPS coefficients. Let the mathematical model of Haar's Discrete Wavelet Transform be set, implemented in the RNS.

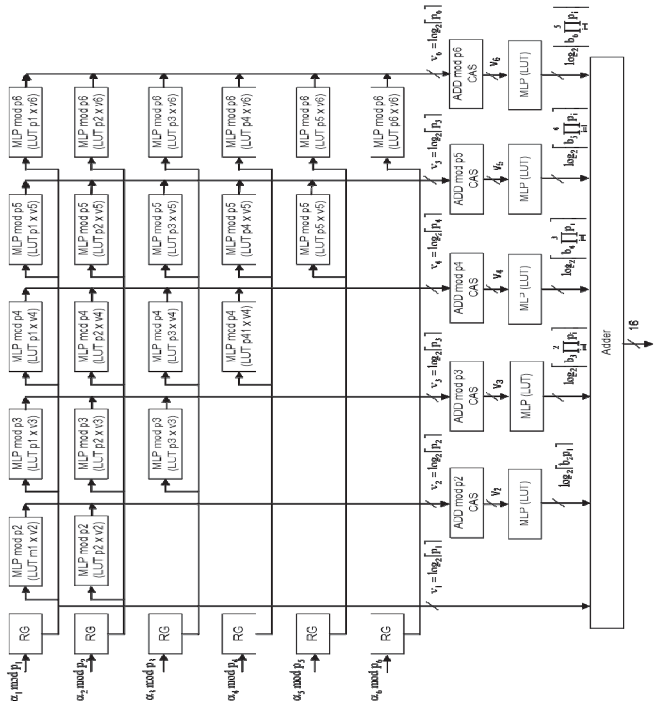

Fig. 1. Structure of the device for calculating the GPS coefficients

As the working bases was selected $p_1 = 7, p_2 = 17, p_3 = 23, p_4 = 31$. In implementing two reference bases of the algorithm are used $p_5 = 41$ and $p_6 = 47$. Then the full range is: $P_{total} = 163500169$. Choose a number $A = 14237$ which belongs to the working range equal to $P_{work} = 84847$.

The values of orthogonal bases are calculated and represented them in the generalized polyadic number system as:

$$\begin{aligned} B_1 &= m_1 P_1 &&= 23357167 = [1, 12, 19, 8, 29, 6]; \\ B_2 &= m_2 P_2 &&= 19235314 = [0, 5, 20, 21, 21, 5]; \\ B_3 &= m_3 P_3 &&= 7108703 = [0, 0, 6, 24, 1, 2]; \\ B_4 &= m_4 P_4 &&= 105483980 = [0, 0, 0, 7, 13, 30]; \\ B_5 &= m_5 P_5 &&= 119634270 = [0, 0, 0, 0, 16, 34]; \\ B_6 &= m_6 P_6 &&= 52180905 = [0, 0, 0, 0, 0, 15]; \end{aligned} ;$$

One can use the developed algorithm and perform the calculation of the GPS coefficients for the code combination $A = 14237 = (6,\ 8,\ 0,\ 8,\ 10.43)$. This combination is fed to the registers RG (Fig. 1). From the last output, the remnants of the RNS combination are fed to the inputs of the corresponding LUT-tables, which are ROM. The data of LUT-tables stores the results of multiplication of the residue by constants b_i^j, which are the j^{th} coefficient of the GPS i^{th} orthogonal basis of the RNS code.

Consider the calculation of the first remainder of the GPS code. The first remainder of the RNS code is immediately fed to the output of the GPS coefficient calculation unit. In this case, it's got $b_1 = \alpha_1$. When calculating the second GPS coefficient, the transformation is performed

$$b_2 = (\alpha_1 b_2^1 + \alpha_2 b_2^2) \bmod p_2 = \left|6\cdot 12 + 8\cdot 5\right|_{17}^{+} = 10$$

In this case, the number of transitions γ_i beyond the p_2 module limits is calculated, which is taken into account when calculating the third GPS coefficient.

In this example, the number of transitions beyond the modulus $p_2 = 17$ on the first remainder is:

$$\gamma_2^1 = \left[\frac{\alpha_1 b_2^1}{p_2}\right] = \left[\frac{6\cdot 12}{17}\right] = 4 .$$

This indicator for the second remainder is:

$$\gamma_2^2 = \left[\frac{\alpha_2 b_2^2}{p_2}\right] = \left[\frac{8\cdot 5}{17}\right] = 2 .$$

Then the correction value, which must be taken into account when calculating the coefficient b_3, is equal to $\gamma_2 = 6$. For calculating the third GPS coefficient, one can use the expression (15). Then

$$\begin{aligned} b_3 &= (\alpha_1 b_3^1 + \alpha_2 b_3^2 + \alpha_3 b_3^3 + \gamma_2) \bmod p_3 = \ldots \\ &= \left|(6\cdot 19 + 4) + (8\cdot 20 + 2) + 0\cdot 6\right|_{23}^{+} = \\ &= \left|3 + 1 + 0\right|_{23}^{+} = 4. \end{aligned}$$

In this case, the number of transitions γ_i beyond the p_3 module limits is calculated, which is taken into account when calculating the fourth GPS coefficient.

In this example, the number of transitions beyond the modulus $p_3 = 23$ in the first remainder is:

$$\gamma_3^1 = \left[\frac{\alpha_1 b_3^1 + \gamma_2^1}{p_3}\right] = \left[\frac{6\cdot 19 + 4}{23}\right] = 5 .$$

This indicator for the second remainder is:

$$\gamma_3^2 = \left[\frac{\alpha_2 b_3^2 + \gamma_2^2}{p_3}\right] = \left[\frac{8\cdot 20 + 2}{23}\right] = 7 .$$

At the same time, the indicator for the third remainder is equal $\gamma_3^3 = 0$.

Since the sum

$$((\alpha_1 b_3^1 + \gamma_2^1) + (\alpha_2 b_3^2 + \gamma_2^2) + \alpha_3 b_3^3) \bmod p_3 = 4 ,$$

then in implementing this operation, there were no transitions beyond the p_3 module. Then it's got $\gamma_3^{\Sigma} = 0$. Then the correction value, which must be taken into account when calculating the coefficient b_4, is equal to $\gamma_3 = \gamma_3^1 + \gamma_3^2 + \gamma_3^3 + \gamma_3^\Sigma = 12$.

The remaining GPS coefficients are calculated in a similar way. The results of this procedure are represented in Table II.

TABLE II. TRANSLATION FROM MODULAR CODE TO GPS CODE

RNS	b₁	γ₁	b₂	γ₂	b₃	γ₃	b₄	γ₄	b₅	γ₅	b₆
6	6	0	4	4	3	5	22	1	11	4	40
8	0	0	6	2	1	7	20	5	9	4	44
0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	25	1	23	2	7
10	0	0	0	0	0	0	0	0	37	3	14
43	0	0	0	0	0	0	0	0	0	0	34
sum	6	0	10	0	4	0	67	2	80	2	139
b(i)	6	0	10	6	4	12	5	9	0	15	0

As a result of the transfer from the code of RNS to the GPS code

$$A = 14237 = (6,\ 8,\ 0,\ 8,\ 10.43)_{RNS} = \ldots$$
$$= (6,\ 10,\ 4,\ 5,\ 0,\ 0)_{GPS}.$$

Analysis of Table 2 shows, this code combination does not contain errors. This is determined by the fact that the highest GPS coefficients, that is, $b_5 = 0$ and $b_6 = 0$.

VI. ERROR CORRECTION

Consider the case of an error occurring. Let the error in this code combination occur in the third base and its depth is equal $\Delta\alpha_3 = 1$. Then the forbidden combination has the form $A^* = (6,\ 8,\ 1,\ 8,\ 10.43)$. One can calculate the coefficients of the GPS.

Obviously, the first remainder of the RNS code is immediately fed to the output of the GPS coefficient calculation unit, then $b_1 = \alpha_1$. When calculating the second GPS coefficient, the transformation is performed

$$b_2 = (\alpha_1 b_2^1 + \alpha_2 b_2^2) \bmod p_2 = \left|6 \cdot 12 + 8 \cdot 5\right|_{17}^{+} = 10 .$$

In this case, the number of transitions γ_i beyond the p_2 module limits is calculated, which is taken into account when calculating the third GPS coefficient.

In this example, the number of transitions beyond the modulus $p2 = 17$ on the first remainder is:

$$\gamma_2^1 = \left[\frac{\alpha_1 b_2^1}{p_2}\right] = \left[\frac{6 \cdot 12}{17}\right] = 4$$

The indicator for the second remainder is:

$$\gamma_2^2 = \left[\frac{\alpha_2 b_2^2}{p_2}\right] = \left[\frac{8 \cdot 5}{17}\right] = 2$$

Then the correction value, which must be taken into account when calculating the coefficient b_3, is equal to $\gamma_2 = 6$.

Perform the calculation of the third GPS coefficient. For this one can use the expression (15). Then:

$$b_3 = (\alpha_1 b_3^1 + \alpha_2 b_3^2 + \alpha_3 b_3^3 + \gamma_2) \bmod p_3 = \ldots$$
$$= \left|(6 \cdot 19 + 4) + (8 \cdot 20 + 2) + (1 \cdot 6)\right|_{23}^{+} =$$
$$= \left|3 + 1 + 6\right|_{23}^{+} = 10.$$

In this case, the number of transitions γ_i beyond the p_3 module limits is calculated, which is taken into account when calculating the fourth GPS coefficient.

In this example, the number of transitions beyond the modulus $p_3 = 23$ in the first remainder is:

$$\gamma_3^1 = \left[\frac{\alpha_1 b_3^1 + \gamma_2^1}{p_3}\right] = \left[\frac{6 \cdot 19 + 4}{23}\right] = 5$$

The indicator for the second remainder is:

$$\gamma_3^2 = \left[\frac{\alpha_2 b_3^2 + \gamma_2^2}{p_3}\right] = \left[\frac{8 \cdot 20 + 2}{23}\right] = 7$$

At the same time, the indicator for the third remainder is equal $\gamma_3^3 = 0$. Since the sum

$$((\alpha_1 b_3^1 + \gamma_2^1) + (\alpha_2 b_3^2 + \gamma_2^2) + \alpha_3 b_3^3) \bmod p_3 = 4 ,$$

then in implementing this operation, there were no transitions beyond the p₃ module. Then it's got $\gamma_3^\Sigma = 0$. Then the correction value, which must be taken into account when calculating the coefficient b_4, is equal to

$$\gamma_3 = \gamma_3^1 + \gamma_3^2 + \gamma_3^3 + \gamma_3^\Sigma = 12 .$$

The remaining GPS coefficients are calculated in a similar way. The results of this procedure are represented in Table III.

TABLE III. TRANSLATION FROM MODULAR CODE TO GPS CODE

RNS	b₁	γ₁	b₂	γ₂	b₃	γ₃	b₄	γ₄	b₅	γ₅	b₆
6	6	0	4	4	3	5	22	1	11	4	40
8	0	0	6	2	1	7	20	5	9	4	44
1	0	0	0	0	6	0	24	0	1	0	2
8	0	0	0	0	0	0	25	1	23	2	7
10	0	0	0	0	0	0	0	0	37	3	14
43	0	0	0	0	0	0	0	0	0	0	34
sum	6	0	10	0	10	0	91	2	81	2	141
b(i)	6	0	10	6	10	12	29	9	1	15	2

As a result of the transfer from the code of RNS to the GPS code

$$A^{*} = (6,\ 8,\ 1,\ 8,\ 10,43)_{RNS} = \ldots$$
$$= \left(6,\ 10,\ 10,\ 29,\ 1,\ 2\right)_{GPS}$$

The analysis of Table 3 shows that this code combination contains errors. This is determined by the fact that the highest GPS coefficients are nonzero, that is, $b_5 = 1$ and $b_6 = 2$. Since the two control bases are used, such a redundant RNS code can fix 100% of one-time errors.

In this, the values $b_5 = 1$ and $b_6 = 2$ are fed to the input of the memory block, in which the values of the error vectors are stored. The error vector $e = \left(0,\ 0,\ 1,\ 0,\ 0,\ 0\right)$ is stored at this address. To correct the error, it is necessary to subtract the error vector from the error code combination of the RNS code. According to the following expression

$$A = A^{*} - e = (6,\ 8,\ 1,\ 8,\ 10,43) - \left(0,\ 0,\ 1,\ 0,\ 0,\ 0\right) = \ldots$$
$$= \left(6,\ 8,\ 0,\ 8,\ 10,\ 43\right).$$

Thus, one can conclude that the proposed algorithm for converting numbers from the code of RNS to the code of GPS is effective in terms of quick response. It is possible to unequivocally determine the fact of the error and carry out its correction.

VII. Conclusion

If errors of greater multiplicity occur (for the considered example, the multiplicity of errors is 1), it is possible to ensure the diversity of the DF structure by redistributing the working and control bases of the RNS code. When one control base is outputted to the operational, the diversity of the DF structure is ensured and one control base will ensure that all one-time errors are detected while preserving the DF function without reducing the range of processed data.

The researches have been shown the feasibility of applying a multivariate finite field arithmetic to provide the required degree of structural and informational diversity of digital filter structures [11], [12].

Acknowledgment

The reported study was funded by RFBR according to the research project № 18-37-20059 (mol_a_ved).

References

[1] A.V. Veligosha, D.I. Kaplun, D.M. Klionskiy, D.V. Bogaevskiy, V.V. Gulvanskiy, I. A. Kalmykov, “Error Correction of Digital Signal Processing Devices using Non-Positional Modular Codes”, *Automatic Control and Computer Sciences*, 2017, Vol. 51, No. 3, pp. 167–173.

[2] Stamenkovic N, “Digital FIR filter architecture based on the residue number system”, *Facta Univ. Ser. Electron. Energ.* 2009, 22, 125–140.

[3] A.V. Veligosha, G.I. Linets, D.I. Kaplun, D.M. Klionskiy, D.V. Bogaevskiy, “Implementation of non-positional digital filters”, *In Proceedings of the XIX IEEE International Conference on Soft Computing and Measurements (SCM)*, St. Petersburg, Russia, 25–27 May 2016, pp. 148–150.

[4] Omondi A.R. and Premkumar B. *Residue Number Systems: Theory and Implementation*. Imperial College Press: London, UK, 2007.

[5] Kaplun D., Butusov D., Ostrovskii V., Veligosha A., Gulvanskii V., “Optimization of the FIR Filter Structure in the Finite Residue Field Algebra”, *Electronics,* Volume 7, Issue 12, December 2018, Art. №372.

[6] Chervyakov N.I., Kalmykov I.A., Shelkunova Yu.O., Beregnoy V.V., “Mathematical model of a neuralnetwork for error correction in a non-positional code of extended Galua field”, *Neurocomput.: Dev. Appl.*, 2003, no. 8–9, pp. 10–16.

[7] Akushskiy I.Y. and Udizkiy D.M., *Machine Arithmetic is Residue Number Classes*, Moscow: Sov. Radio, 1968.

[8] Kalmykov I.A., Veligosha A.V., Kaplun D.I., Klionskiy D.M. Gulvanskiy V.V., “Parallel-pipeline implementation of digital signal processing techniques based on modular codes”, *In Proceedings of the XIX conference on Soft Computing and Measurements (SCM)*, St. Petersburg, Russia, 25–27 May 2016; pp. 213–214

[9] A.V. Veligosha, D.I. Kaplun, D.V. Bogaevskiy, V.V. Gulvanskiy, A.S. Voznesenskiy, I.A. Kalmykov, “Adjustment of adaptive digital filter coefficients in modular codes”, *In Proceedings of the IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW)*, Moscow, Russia, 29 January–1 February 2018, pp. 1167–1170.

[10] Younes D., Steffan P., “Universal approaches for overflow and sign detection in residue number system based on {2n−1, 2n, 2n+1}”, *In Proceedings of the Eighth International Conference on Systems (ICONS)*, Seville, Spain, 27 January–1 February 2013; Volume 1, pp. 77–84.

[11] Cardarilli G.C., Nannarelli A., Re M., “Residue number system for low-power DSP applications”, *In Proceedings of the 41st Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 4–7 November 2007; pp. 1412–1416.

[12] Kaplun D.I., Gulvanskiy V.V. Klionskiy D.M.; Kupriyanov M.S. Veligosha A.V., “Implementation of digital filters in the residue number system”, *In Proceedings of the IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference (ElConRusNW)*, St. Petersburg, Russia, 2–3 February 2016, pp. 220–224.