The Use of Redundant Modular Codes for Improving the Fault Tolerance of Special Processors for Digital Signal Processing

Alyona V. Makarova[1] Elena P. Stepanova[1] Ekaterina V. Toporkova[1]
Igor A. Kalmykov[1]

[1] North-Caucasus Federal University
Stavropol, Russia
kia762@yandex.ru

Abstract

The purpose of the research is to increase the fault tolerance of high-speed special processors for digital signal processing (DSP). Achieving this goal is possible due to parallelization of computations. It is shown in the paper that, to provide signal processing in real time, it is necessary to use algebraic structures having the properties of a ring and a field, in particular, a residue number system (RNS) and a polynomial residue number system (PRNS). Application of new modular technologies in the DSP problems, due to parallelization at the level of operations of independent low-bit data processing, allows not only to increase the speed of computing, but also to ensure obtaining the correct result in the conditions of interference in the transmission and the equipment failure. This paper presents a new algorithm for error correction on the basis of calculation of a truncated convolution. The use of this algorithm allows developing special processors for digital signal processing (SP for DSP), capable of maintaining the state of operability in the case of failures due to reconfiguration of the structure.

Introduction

Modern information-communication systems widely use special processors (SP), which, using a mathematical model of orthogonal frequency division multiplexing (OFDM), allow ensuring high interference immunity, the transmission of information in real time, stability with respect to multipath propagation of radio waves, and a number of other advantages. An improvement of the performance of the special processor for DSP can be achieved by the use of parallel computing techniques. However, this leads to a decrease in reliability of the computing system. It is possible to resolve this contradiction by using corrective non-positional modular codes. Therefore, the expansion of the corrective capacity of modular codes, as well as the development of a new method of finding and fixing errors that allow improving the fault tolerance of SP for DSP, is a crucial task.

Main Part. The Purpose of Research

Each sphere of application of the special processors for DSP imposes specific requirements for the composition and structure of the computing device. With the development of networks and data transmission systems, a trend is observed: increasing the requirements for the data transmission speed, reliability and quality of the services provided. This leads to revitalization of the work on the development of new organization principles of radiocommunication.

In: S. Hölldobler, A. Malikov, C. Wernhard (eds.): *YSIP2 – Proceedings of the Second Young Scientist's International Workshop on Trends in Information Processing, Dombai, Russian Federation, May 16–20, 2017*, published at http://ceur-ws.org.

In recent years, there has been an increased interest in the use of perspective types of signal-code designs of OFDM (Orthogonal Frequency Division Multiplexing). However, along with some advantages, the SP for OFDM, using a mathematical model of fast Fourier transform (FFT), have several shortcomings. These include insufficient speed of orthogonal transformation of signal, as well as an increase in the complexity of SP for OFDM, which leads to a decrease in its reliability.
It is possible to eliminate these shortcomings due to providing the property of fault tolerance during the operation of SP for DSP. Therefore, the aim of this work is to improve the fault tolerance of SP for DSP by expanding the corrective abilities of PRNS codes and using new methods of finding and correcting errors.

The Material and Methods of Research

Modular codes are currently widely used in many fields. For example, in [Moh02, Omo07, Yat13], the feasibility of using the codes of residual classes system when performing the FFT is demonstrated. The use of low-bit residues and parallel data processing allow improving the execution speed of the FFT. In [Cher95], the usage of modular codes for the construction of digital filters is suggested. In the papers [Gor14, Jun11, Kal15, Chu13], the methods and algorithms for improving the fault tolerance of the residue classes SP are shown. The work [Step16] presents a way to correct the errors due to failures in the operation of the AES algorithm encoder. The satellite communication systems may become a priority use of the modular code [Pash05]. Using the modular code allows improving the efficiency of realization of the spaced-out reception. In [Kat13], an example of the modular code application in the systems of secondary processing of navigation data is given. Using the RNS code has allowed increasing the computation speed and reducing the errors in determining the space-time coordinates of the client.
Using the modular codes of a polynomial residue number system (PRNS) allows improving the efficiency of implementation of DSP by switching from the processing of one-dimensional signals to the processing of multi-dimensional signals using an isomorphism generated by the Chinese Remainder Theorem (CRT) [Gor14, Kal14]. The PRNS code is a set of residues $A(z) = (a_1(z), a_2(z), \ldots, a_k(z))$, where $A(z) \equiv a_i(z)\ mod\ p_i(z), i = 1, 2, \ldots, k$, obtained by dividing the polynomial $A(z)$ by pairwise relatively prime modules $p_i(z)$. The application of PRNS allows carrying out the digital processing in parallel

$$\begin{cases} X_1(s) = \sum\limits_{j=0}^{d-1} x_1(j) {b_1}^{j_l}\ mod\ p_1(z) \\ \vdots \\ X_k(s) = \sum\limits_{j=0}^{d-1} x_k(j) {b_k}^{j_l}\ mod\ p_k(z), \end{cases} \tag{1}$$

where $x_i(j) \equiv x(j)\ mod\ p_i(z); {b_i}^{\pm j_l} \equiv b^{\pm j_l}\ mod\ p_i(z); X_i(s) \equiv X(s)\ mod\ p_i(z)$; b is the primitive root; $x(j)$ is the input sequence of the signal; $X(s)$ are the spectral components of the input signal; $d = 2^v - 1$ is the dimension of the input vector.
However, the transition to parallel computing leads to an increase in the circuit expenses, which negatively affects the reliability of operation of the SP for DSP. It is possible to resolve this contradiction by giving them the property of fault tolerance. The use of modular codes allows solving this problem. In this case, the expansion of the corrective abilities of the PRNS codes will increase the efficiency of this solution.
It is shown in [Gor14] that, to correct a single-bit error, i.e., a distortion of one digit of the residue of the PRNS code, $\Delta a_i(z) = z^n$, where $n = 0, \ldots, deg\ p_i(z) - 1$, it suffices to have two control bases $p_{k+1}(z), p_{k+2}(z)$, for which

$$deg\ p_{k-1}(z) \le deg\ p_k(z) \le deg\ p_{k+1}(z) \le deg\ p_{k+2}(z), \tag{2}$$

where $deg\ p_i(z)$ is the degree of the irreducible polynomial $p_i(z)$; k is the number of working bases.
A PRNS code is considered to be admissible, if

$$deg\ A(z) < P_1(z) = \prod_{i=1}^{k} p_i(z), \tag{3}$$

where $P_1(z)$ is the range of admissible combinations.
The introduction of redundant modules leads to extension of the PRNS code range

$$P(z) = \prod_{i=1}^{k+2} p_i(z) = P_1(z) \prod_{i=k+1}^{k+2} p_i(z) = P_1(z)P_2(z). \tag{4}$$

An error, transforming a correct combination $A = (a_1(z), a_2(z), \ldots, a_{k+2}(z))$ into the combination $A^* = (a_1(z), \ldots, a_i^*, \ldots, a_{k+2}(z))$, realizes a transition of the code beyond the limits of the range $P_1(z)$, where $a_i(z) \equiv A(z) \ mod \ p_i(z)$, $a_i^*(z) = a_i(z) + \Delta a_i(z)$ is a distorted residue of the PRNS code, $\Delta a_i(z) = z^n$ is the depth of the error $n = 0, \ldots, deg \ p_i(z) - 1$.
Consider a situation where an error has occurred with respect to one base $p_i(z)$, but several bits are distorted in the residue. This error will be called a single-bit error. If two control bases satisfying the condition (2) are used in the ordered PRNS code, this code is capable of correcting single-bit errors that distort several bits of one residue of the PRNS code.
Let an error with respect to the i-th base occur in the PRNS code. Then the code has the form

$$A^*(z) = (\alpha_1(z), \ldots, \alpha_i^*(z), \ldots, \alpha_{k+2}(z)), \tag{5}$$

where $\alpha_i^*(z) = \alpha_i(z) + \Delta\alpha_i(z)$.
If an error occurred with respect to the j-th base, the PRNS code has the form

$$A^{**}(z) = (\alpha_1(z), \ldots, \alpha_j^{**}(z), \ldots, \alpha_{k+2}(z)), \tag{6}$$

where $\alpha_j^{**}(z) = \alpha_j(z) + \Delta\alpha_j(z), j \neq i$.
Since modular codes are non-positional codes, the positional characteristics (PC) are used for the detection and correction of errors in these codes. They show the location of an erroneous code combination of the modular code with respect to the range $P_1(z)$. The work [Gor14] presents an algorithm and a circuit realization of the calculation of an interval number, the physical meaning of which is defined as $L(z) = [A(z)/P_1(z)]$. If the PRNS code does not contain errors, i.e., $deg \ A(z) < deg \ P_1(z)$, then the value of the interval number is zero, i.e., $L(z) = 0$. If an error occurs in the PRNS code, $L(z) \neq 0$. Let us determine the intervals within which the erroneous code combinations of PRNS fall

$$L^*(z) = \left[\frac{A^*(z)}{P_1(z)}\right] = \left[\frac{(A(z) + \Delta\alpha_i^*(z)B_i(z)) \ mod \ P(z)}{P_1(z)}\right], \tag{7}$$

$$L^{**}(z) = \left[\frac{A^{**}(z)}{P_1(z)}\right] = \left[\frac{\left(A(z) + \Delta\alpha_j^{**}(z)B_j(z)\right) \ mod \ P(z)}{P_1(z)}\right], \tag{8}$$

where $P(z) = \prod_{i=1}^{k+2} p_i(z)$ is the complete range of the PRNS code.
If the code combinations do not fall into one and the same interval, then we have

$$L^*(z) + L^{**}(z) \geq 1. \tag{9}$$

Let the combination $A(z) = 0$. Then expressions (7) and (8) can be represented in the form

$$L^*(z) = \left[\frac{(\Delta\alpha_i^*(z)B_i(z)) \ mod \ P(z)}{P_1(z)}\right], \tag{10}$$

$$L^{**}(z) = \left[\frac{\left(\Delta\alpha_j^{**}(z)B_j(z)\right) \ mod \ P(z)}{P_1(z)}\right]. \tag{11}$$

It is known that the orthogonal bases of the PRNS code are defined in the following way

$$B_i(z) = m_i(z)\frac{P(z)}{p_i(z)} = m_i(z)\frac{P_1(z)p_{k+1}(z)p_{k+2}(z)}{p_i(z)} \tag{12}$$

$$B_j(z) = m_j(z)\frac{P(z)}{p_j(z)} = m_j(z)\frac{P_1(z)p_{k+1}(z)p_{k+2}(z)}{p_j(z)} \tag{13}$$

We substitute equalities (12) and (13) into expressions (10) and (11). Then we get

$$L^*(z) = \left[\frac{(\Delta\alpha_i^*(z)m_i(z)p_{k+1}(z)p_{k+2}(z))\ \ mod\ P(z)}{p_i(z)}\right], \tag{14}$$

$$L^{**}(z) = \left[\frac{\left(\Delta\alpha_j^{**}(z)m_j(z)p_{k+1}(z)p_{k+2}(z)\right)\ \ mod\ P(z)}{p_j(z)}\right]. \tag{15}$$

As is known, the interval number runs over all the values modulo $P_2(z) = \prod\limits_{i=k+1}^{k+2} p_i(z)$. Then expressions (14) and (15) can be represented as follows

$$L^*(z) = \left(\frac{\Delta\alpha_i^*(z)m_i(z)}{p_i(z)}\right)\ mod\ P_2(z), \tag{16}$$

$$L^{**}(z) = \left(\frac{\Delta\alpha_j^{**}(z)m_j(z)}{p_j(z)}\right)\ mod\ P_2(z). \tag{17}$$

Let us use the isomorphism generated by the Chinese Remainder Theorem, and move on to the multi-dimensional representation of the intervals in the form of the modular code

$$L^*(z) = \left(L_{k+1}^*(z), L_{k+2}^*(z)\right) = \left(\left|\frac{\Delta\alpha_i^*(z)m_i(z)}{p_i(z)}\right|_{p_{k+1}(z)}^+, \left|\frac{\Delta\alpha_i^*(z)m_i(z)}{p_i(z)}\right|_{p_{k+2}(z)}^+\right), \tag{18}$$

$$L^{**}(z) = \left(L_{k+1}^{**}(z), L_{k+2}^{**}(z)\right) = \left(\left|\frac{\Delta\alpha_j^{**}(z)m_j(z)}{p_j(z)}\right|_{p_{k+1}(z)}^+, \left|\frac{\Delta\alpha_j^{**}(z)m_j(z)}{p_j(z)}\right|_{p_{k+2}(z)}^+\right). \tag{19}$$

Suppose that in the event of errors with respect to the i-th and j-th bases of the PRNS code, where $j \neq i$, the coincidence of intervals takes place. Then the expression (9) assumes the form

$$L^*(z) + L^{**}(z) = 0. \tag{20}$$

Thus, we arrive at the equalities

$$\left|\frac{\Delta\alpha_i^*(z)m_i(z)}{p_i(z)}\right|_{p_{k+1}(z)}^+ - \left|\frac{\Delta\alpha_j^{**}(z)m_j(z)}{p_j(z)}\right|_{p_{k+1}(z)}^+ = 0, \tag{21}$$

$$\left|\frac{\Delta\alpha_i^*(z)m_i(z)}{p_i(z)}\right|_{p_{k+2}(z)}^+ - \left|\frac{\Delta\alpha_j^{**}(z)m_j(z)}{p_j(z)}\right|_{p_{k+2}(z)}^+ = 0. \tag{22}$$

Let us convert to a common denominator. We get

$$\left|\frac{\Delta\alpha_i^*(z)m_i(z)p_j(z) + \Delta\alpha_j^*(z)m_j(z)p_i(z)}{p_i(z)p_j(z)}\right|_{p_{k+1}(z)}^+ = 0, \tag{23}$$

$$\left|\frac{\Delta\alpha_i^*(z)m_i(z)p_j(z) + \Delta\alpha_j^*(z)m_j(z)p_i(z)}{p_i(z)p_j(z)}\right|_{p_{k+2}(z)}^+ = 0. \tag{24}$$

However, the values

$$\left|\Delta\alpha_i^*(z)m_i(z)p_j(z) + \Delta\alpha_j^*(z)m_j(z)p_i(z)\right|_{p_{k+1}(z)}^+ \neq 0, \tag{25}$$

$$\left|\Delta\alpha_i^*(z)m_i(z)p_j(z) + \Delta\alpha_j^*(z)m_j(z)p_i(z)\right|_{p_{k+2}(z)}^+ \neq 0, \tag{26}$$

Hence, the assumption of the coincidence of intervals under the occurrence of a single-bit error in different bases of the PRNS code while using two control bases satisfying condition (2) is incorrect. Thus, the PRNS code is able

to correct any errors that occur with respect to one base. Consider a new algorithm for detecting and correcting errors in the modular code. To correct an error in the PRNS code, we use positional characteristics (PC). In the paper [Gor14], an algorithm and a circuit realization of calculation of an interval number are presented. In [Lie99], the leading coefficients of a generalized polyadic system are used as PC. In [Ham12], the algorithm of projection of the PRNS code is proposed to be used for the error correction. However, the algorithms mentioned above require substantial circuit and time expenses. It is possible to reduce them by virtue of a PC-truncated convolution. To perform the transition from PRNS into a positional representation (PR), we use

$$A(z) = \sum_{i=1}^{k+1} a_i(z)B_i(z) \ mod \ P(z) = \sum_{i=1}^{k+1} |a_i(z)m_i(z)|^+_{p_i(z)} M_i(z), \tag{27}$$

where $B_i(z)$ is the orthogonal basis; $M_i(z) = P(z)/p_i(z)$; $m_i(z)$ is the weight of the basis; $B_i(z) \equiv l \ mod \ p_i(z)$. Suppose that an error has taken place with respect to the j-th base of PRNS, its depth being equal to $\Delta a^*_j(z)$. Let us transform the erroneous PRNS code into PR

$$A^*(z) = \sum_{i=1}^{k+1} |a_i(z)m_i(z)|^+_{p_i(z)} M_i(z) + \left|\Delta a^*_j(z)m_j(z)\right|^+_{p_j(z)} M_j(z). \tag{28}$$

Analysis of (28) shows that going beyond the working range $P_1(z)$ is caused by the second term. To perform the correction, we need to calculate the quantity $M_i(z)$ for each base of PRNS. Then we calculate the degree of the working range

$$N = deg \ P_1(z) = \sum_{i=1}^{k} deg \ p_i(z) \tag{29}$$

In the polynomials $M_i(z)$ we drop the digits, the degree of which will be less than $N - deg \ p_i(z) = N_i$. As a result, we obtain the constants $K_i(z)$. If the PRNS code does not contain an error, then $deg \ A(z) < deg \ P_1(z)$. In this case, the convolution of the products of the residues $a_i(z)$, the basis weight $m_i(z)$ and the constants $K_i(z)$ must be equal to zero

$$S(z) = \sum_{i=1}^{k+1} |a_i(z)m_i(z)|^+_{p_i(z)} K_i(z) = 0. \tag{30}$$

If the code $A^*(z) = \left(a_1(z), a_2(z), \ldots, a^*_j(z), \ldots, a_{k+1}(z)\right)$ contains an error, than the convolution equals

$$S(z) = \sum_{i=1}^{k+1} |a_i(z)m_i(z)|^+_{p_i(z)} K_i(z) + \left|\Delta a^*_j(z)m_j(z)\right|^+_{p_j(z)} K_j(z) = \left|\Delta a^*_j(z)m_j(z)\right|^+_{p_j(z)} K_j(z). \tag{31}$$

Based on the value of $S(z)$, one can determine the location of the error and its depth.

Results of Research and Their Discussion

Let us carry out the calculations of the numbers of the intervals $L(z)$, into which the erroneous combinations of the PRNS code fall under the occurrence of errors inside one residue. Suppose that we choose $p_1(z) = z+1$, $p_2(z) = z^2+z+1$, $p_3(z) = z^4+z^3+z^2+z+1$ as the information moduli of PRNS, while $p_4(z) = z^4+z^3+1$ and $p_5(z) = z^4+z+1$, as the control moduli. The range of admissible combinations $P_1(z) = \prod_{i=1}^{3} p_i(z) = z^7+z^6+z^5+z^2+z+1$. Consider an error which has taken place with respect to the base $p_5(z)$, its depth being $\Delta a_5(z) = z+1$. The orthogonal basis will be $B_5(z) = m_5(z) \prod_{i=1}^{4} p_i(z) = z^{12}+z^9+z^8+z^6+z^4+z^3+z^2+z$. We make use of equality (7)

$$L_5^{0011}(z) = \left[\frac{(z+1)\left(z^{12}+z^9+z^8+z^6+z^4+z^3+z^2+z\right)}{z^7+z^6+z^5+z^2+z+1}\right] = z^6+z^4+z^4+z = 1010110_2 = 56_{10}$$

The research results are given in Table 1.

Table 1: Intervals of single-bit errors of the PRNS code

$p_i(z)$	$\Delta a_i(z)$	$L(z)$	$p_i(z)$	$\Delta a_i(z)$	$L(z)$	$p_i(z)$	$\Delta a_i(z)$	$L(z)$	$p_i(z)$	$\Delta a_i(z)$	$L(z)$
$p_1(z)$	1	96	$p_3(z)$	0001	9B	$p_4(z)$	0001	98	$p_5(z)$	0001	32
$p_2(z)$	01	A7	$p_3(z)$	0010	136	$p_4(z)$	0010	130	$p_5(z)$	0010	64
$p_2(z)$	10	14F	$p_3(z)$	0011	1AD	$p_4(z)$	0011	1A8	$p_5(z)$	0011	56
$p_2(z)$	11	1E8	$p_3(z)$	0100	6C	$p_4(z)$	0100	60	$p_5(z)$	0100	C8
			$p_3(z)$	0101	F7	$p_4(z)$	0101	F8	$p_5(z)$	0101	FA
			$p_3(z)$	0110	15A	$p_4(z)$	0110	150	$p_5(z)$	0110	AC
			$p_3(z)$	0111	1C1	$p_4(z)$	0111	1C8	$p_5(z)$	0111	9E
			$p_3(z)$	1000	D8	$p_4(z)$	1000	C0	$p_5(z)$	1000	190
			$p_3(z)$	1001	43	$p_4(z)$	1001	58	$p_5(z)$	1001	1A2
			$p_3(z)$	1010	1EE	$p_4(z)$	1010	1F0	$p_5(z)$	1010	1F4
			$p_3(z)$	1011	175	$p_4(z)$	1011	168	$p_5(z)$	1011	1C6
			$p_3(z)$	1100	B4	$p_4(z)$	1100	A0	$p_5(z)$	1100	158
			$p_3(z)$	1101	2F	$p_4(z)$	1101	38	$p_5(z)$	1101	16A
			$p_3(z)$	1110	182	$p_4(z)$	1110	190	$p_5(z)$	1110	13C
			$p_3(z)$	1111	119	$p_4(z)$	1111	108	$p_5(z)$	1111	10E

Analysis of the table shows that the conducted research has confirmed the expansion of the corrective abilities of the PRNS codes. For example, due to this, the PRNS code can correct 49 errors, while, on the other hand, using [Gor14], one can correct only 15 errors. Hence, the use of two control bases satisfying (3) allows correcting any errors that occur in one residue of PRNS.

Consider the application of the developed method of error correction in the PRNS code. Let the working bases be chosen to be the polynomials $p_1(z) = z + 1,\ p_2(z) = z^3 + z + 1$, while $p_3(z) = z^3 + z^2 + 1$, to be the control ones. Then the range $P_1(z) = \prod_{i=1}^{2} p_i(z) = z^4 + z^3 + z^2 + z$, where $deg\ P_1(z) = 4$. Then the constants $M_1(z) = z^6+z^5+z^4+z^3+z^2+z+1, M_2(z) = z^4+z^2+z+1; M_3(z) = z^4+z^3+z^2+1$. Let us calculate the values of weights of the first orthogonal basis. To this end, we find $d_1 = M_1(z)\ mod\ p_1(z) = \left|z^6 + z^5 + z^4 + z^3 + z^2 + z + 1\right|^+_{z+1} = 1$. Hence, $m_1(z) = 1$, since $d_1(z)m_1(z) \equiv l\ mod\ p_i(z)$. Now we calculate the weight of the basis $B_2(z)$. We get $d_2 = M_2(z)\ mod\ p_2(z) = \left|z^4 + z^2 + z + 1\right|^+_{z^3+z+1} = 1$. Since $d_2(z) = 1$, we have $m_2(z) = 1$. For the basis $B_3(z)$, we obtain $d_3 = M_3(z)\ mod\ p_3(z) = \left|z^4 + z^3 + z^2 + 1\right|^+_{z^3+z+1} = z^2 + z + 1$. Since the value $d_3(z) \neq 1$, the weight of $B_3(z)$ equals $m_3(z) = z^2 + 1$. This is determined from the condition

$$|d_3(z)m_3(z)|^+_{p_3(z)} = \left|\left(z^2 + z + 1\right)\left(z^2 + 1\right)\right|^+_{z^3+z^2+1} = \left|z^4 + z^3 + z + 1\right|^+_{z^3+z^2+1} = 1.$$

Let us calculate the constants $K_i(z)$. Since $deg\ p_1(z) = 1$, we have $K_1(z) = z^6 + z^5 + z^4$. Since $deg\ p_2(z) = 3$, we obtain $K_2(z) = z^4 + z^2$. Because $deg\ p_3(z) = 3$, we arrive at $K_3(z) = z^4 + z^3 + z^2$.

Let the PRNS code $A(z) = z^3 + z^2 + z + 1 = \left(0, z^2, z\right)$ be delivered at the input of the correction block. Since $deg\ A(z) < deg\ P_1(z) = 4$, PRNS does not contain an error. Let us carry out the calculation of the convolution. We determine the products of $a_i(z)$ and $m_i(z)$. We get $d_1(z) = |a_1(z)m_1(z)|^+_{p_1(z)} = 0$; $d_2(z) = |a_2(z)m_2(z)|^+_{p_2(z)} = z^2$; $d_3(z) = |a_3(z)m_3(z)|^+_{p_3(z)} = \left|z(z^2 + 1)\right|^+_{z^3+z^2+1} = z^2 + z + 1$.

Let us determine the values $d_i(z)K_i(z)$. We obtain $d_1(z)K_1(z) = 0(z^6+z^5+z^4) = 0$; $d_2(z)K_2(z) = z^2(z^4+z^2) = z^6 + z^4$; $d_3(z)K_3(z) = (z^2 + z + 1)(z^4 + z^3 + z^2) = z^6 + z^4 + z^2$. We only keep the monomials with the degrees no less than $N = 4$. We obtain the truncated values $S_1 = 0$; $S_2 = z^6 + z^4$; $S_3 = z^6 + z^4$. Next, we add two truncated values $S_i(z)$ modulo two

$$S = S_1 + S_2 + S_3 = 0 + (z^6 + z^4) + (z^6 + z^4) = 0.$$

Since the convolution $S = 0$, the PRNS code does not contain an error.

Suppose that an error has occurred with respect to the first base, while its depth equals $\Delta a_1(z) = 1$. Then $a^*_1(z) = a_1(z) + \Delta a_1(z) = 0 + 1 = 1$. Thus, the PRNS code equals $A^*(z) = (1, z^2, z) = z^6 + z^5 + z^4$. Then we have $d_1(z) = |a_1(z)m_1(z)|^+_{p_1(z)} = 1$, $d_2(z) = |a_2(z)m_2(z)|^+_{p_2(z)} = z^2$, $d_3(z) = z^2 + z + 1$. We determine the

product $d_i(z)K_i(z)$. We get $d_1(z)K_1(z) = z^6 + z^5 + z^4$, $d_2(z)K_2(z) = z^6 + z^4$, $d_3(z)K_3(z) = z^6 + z^4 + z^2$. The truncated values equal $S_1 = z^6 + z^5 + z^4$, $S_2 = z^6 + z^4$, $S_3 = z^6 + z^4 + z^2$. Then the convolution

$$S = K_1 + K_2 + K_3 = (z^6 + z^5 + z^4) + (z^6 + z^4) + (z^6 + z^4) = z^6 + z^5 + z^4.$$

Since $S \neq 0$, the PRNS code contains an error. In Table 2, the values of S and the corresponding errors with respect to the working bases of the PRNS code are given.

Table 2: The values of the truncated convolutions S

Bases	Error $\Delta a_i(z)$	Convolution S	Correcting value Δ
$p_1(z) = z + 1$	1	$z^6 + z^5 + z^4$	$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$
$p_2(z) = z^3 + z + 1$	1	z^4	$z^4 + z^2 + z + 1$
	z	z^5	$z^5 + z^3 + z^2 + z$
	z^2	$z^6 + z^4$	$z^6 + z^4 + z^3 + z^2$

After the transformation from the PRNS code to the PR code, we carry out the error correction

$$A(z) = A^*(z) + \Delta(z) = (z^6 + z^5 + z^4) + (z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = z^3 + z^2 + z + 1.$$

Unlike other algorithms for calculating PC, this algorithm of error correction can be used in the construction of fault-tolerant SP for DSP of residue classes, capable of maintaining the state of operability by means of the structure reconfiguration.

Conclusion

The paper demonstrates the possibility of using modular codes in the special processors that implement DSP. Parallelization of computations at the level of arithmetic operations allows not only providing maximum performance of the SP for DSP, but gives the SP the property of fault tolerance. Using the PRNS codes allows detecting and correcting errors that arise in the course of calculations due to failures or malfunctions of the SP for DSP. The proofs presented here allow enhancing the corrective abilities of the PRNS codes. For example, due to this, a PRNS code with two control bases is able to correct 49 errors, while, at the same time, using [Gor14], only 15 errors are corrected. This paper presents a method for detecting and correcting errors, which uses a truncated convolution of the high-order bits of orthogonal bases. The advantage of this method is that it can detect and correct errors in the SP for DSP with reconfigurable structure. This allows maintaining the state of operability of the PRNS SP under the disconnection of the failed computation channels and reconfiguration of the special processor.

References

[Beck93] P. E. Beckmann, B. R. Musicus. Fast fault-tolerant digital convolution using a polynomial residue number system. *IEEE Trans. on Signal Processing*, pp. 2300-2313, July 1993.

[Cher95] N. I. Chervyakov, A. V. Veligosha, I. A. Kalmykov, P. E. Ivanov. Digital filters in a system of residual classes. *Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika.* 38(8): 11-20, 1995.

[Chip16] A. F. Chipiga, V. P. Pashintsev, V. A. Tsymbal, S. N. Shimanov. Procedure for calculating the dependence of the energy concealment factor on carrier frequency selection for low-frequency satellite communications system. *Australian Journal of Political Science.* 50(1): 408-414 1 November 2016.

[Chu09] J. Chu, M. Benaissa. Polynomial residue number system $GF(2^m)$ multiplier using trinomials. *In 17th European Signal Processing Conference..* August 24-28, Glasgow, Scotland, 2009.

[Chu13] J. Chu, M. Benaissa. Error detecting AES using polynomial residue number system. *Microprocessors and Microsystems..* 37(2): 228-234, 2013.

[Gor14] D. V. Gordenko, D. N. Rezenkov, A. B. Sarkisov Methods and Algorithms of Reconfiguration of Non-Positional Computational Structures for Providing the Failure Robustness of the Special Processors. *Fabula Publishers,* Stavropol, 2014.

[Ham12] Mahyar Hamidreza. Reliable and High-Speed KASUMI Block Cipher by Residue Number System Code. *World Applied Sciences Journal.* 17(9): 1149-1158, 2012.

[Jun11] Joilson Alves Junior. Using redundant residue number system in increase routing dependability on mobile ad hoc networks. *Journal of Selected Areas in Telecommunications (JSAT).* pp. 67-73, January Edition, 2011.

[Kal14] I. A. Kalmykov, K. A. Katkov, D. O. Naumenko, A. B. Sarkisov, A. V. Makarova. Parallel Modular Technologies in Digital Signal Processing. *Life Science Journal.* 11(11s): 435-438, 2014 / Retrieved April 9, 2016 from http://www.lifesciencesite.com

[Kal15] I. A. Kalmykov, K. A. Katkov, L. I. Timoshenko, A. V. Dunin, T. A. Gish. Application of Modular Technologies in the Large-Scale Analysis of Signals. *Journal of Theoretical and Applied Information Technology.* 80(3): 391-400, 2015. Retrieved April 9, 2016 from http://www.lifesciencesite.com.

[Kat13] K. A. Katkov, I. A. Kalmykov. Application of Parallel Technologies in Navigation Management under the Conditions of Artificial Ionospheric Disturbances. *World Applied Sciences Journal.* 26(1): 108-113, 2013.

[Lie99] T. H. Liew, L-L. Yang. Soft-decision redundant residue number system based error correction coding. *roceeding of vtc99.* 22 September, Amsterdam, Nederland, 1999.

[Moh02] P. V. Mohan. Residue Number Systems. Algorithms and Architectures. *Springer,* 2002.

[Omo07] A. Omondi and B. Premkumar. Residue Number Systems: Theory and Implementation. *Imperial College Press.* UK 2007.

[Pash05] V. P. Pashintsev, M. E. Solchatov, A. Ye. Kondrashin, A. V. Senokosova. Maximal frequency of reflection of a decameter wave from the spherically stratified ionosphere. *Radioelectronics and Communications Systems,* 48(5): 8-14, 2005.

[Step16] E. P. Stepanova, I. A. Kalmykov, E. V. Toporkova, M. I. Kalmykov, R. A. Katkov, D. N. Rezenkov. Application of the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher . *Journal of Digital Information Management.* 14(2): 114-123, April 2016.

[Yat13] V. Yatskiv, N. Yatskiv, Su, Jun, A. Sachenko, Zhengbing, Hu. The use of a modified correction code based on a reside number system in WSN. *In Proc. 7-th IEEE Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems, (IDAACS 2013).* 1: 513-516. Berlin, Germany, 2013.