Error correction algorithm developed for special-purpose computing devices based on polynomial modular codes

I A Kalmykov¹, N S Sidorov¹, K T Tyncherov², A A Vorohov³

¹ Federal State Autonomous Educational Institution for Higher Education "North-Caucasus Federal University", 1, Pushkin St., Stavropol, 355009, Russian Federation
² Ufa State Petroleum Technological University, Branch of the University in the City of Oktyabrsky, 54a, Devonskaya St., Oktyabrsky, Republic of Bashkortostan, 452607, Russian Federation
³ Novosibirsk State Technical University, 20, Karl Marks ave., Novosibirsk, 630073, Russian Federation

E-mail: kia762@yandex.ru

Abstract. Special-purpose computing devices (SPCD) are used to solve tasks that require either real-time processing of a large amount of data, including digital processing of audio/video signals and OFDM systems, or high accuracy, like friend-or-foe identification for satellite communications systems. To achieve this goal, it is proposed to use parallel processing at various levels. Parallel computing increases circuit costs though, which incites SPCD to fail. The most promising solution to this contradiction lies in the use of position-independent redundant polynomial modular codes (PMC). These codes aim to increase the speed of data processing through the parallelization of computation at the level of arithmetic operations. What is more, thanks to independent and parallel processing of residues, they have the potential to detect and correct errors caused by the failures to occur during computation and during transmission over communication lines due to interference. Therefore, it is crucial to develop an error correction algorithm for special-purpose computing devices based on polynomial modular codes.

1. Introduction

Modern special-purpose computing devices (SPCD) have complex architecture. Increased requirements for computation rates have led to stepping up the concept of parallel computing. Parallel computing is widely used in digital processing of audio and video signals [1,2], for a small-scale signal analysis [3], in systems supporting OFDM technology [4], friend-or-foe identification systems [5].

However, parallel computing requires increased circuit costs for the implementation of SPCD. Thus, the following contradiction is evident: on the one hand, constantly growing speed requirements lead to the need for parallel computing, but, on the other hand, this increases the frequency of failures and the off time due to troubleshooting challenges. It is possible to solve this contradiction through an increase in fault tolerance of parallel SPCD. It is proposed in [6] to achieve this goal through the use of failure masking. However, the “2 of 3” method, with its simplicity of implementation, has a significant drawback – major circuit costs.

This drawback can be eliminated with redundant polynomial modular codes (PMC). These codes provide an increased processing speed due to parallelization of computation at the level of arithmetic
operations. Moreover, due to independent and parallel processing of residues, polynomial modular codes have the potential to detect and correct errors caused by the failures to arise during computation, and during transmission over communication lines due to interference. Therefore, it is crucial to develop an error correction algorithm for special-purpose computing devices based on polynomial modular codes.

2. Materials and methods

2.1 Techniques for code modularity

Modular codes that fall within position-independent codes can be divided into two classes. The first class is based on the residue numeral system (RNS) [8]. For their construction, the system is defined by a set of \( m \) integers \( m_1, m_2, ..., m_n \), for which \( (m_i, m_j) = 1 \), \( i \neq j \) is true. The product of all \( m_i \) sets a range

\[
M^n = \prod_{i=1}^{n} m_i. \tag{1}
\]

Thus, any integer \( W < M^n \) can be represented by a sequence \( W = (w_1, w_2, ..., w_n) \), where \( w_i \equiv W \mod m_i \). RNS codes permit the following operations to be performed

\[
W + Q = ((w_1 + q_1) \mod m_1, ..., (w_n + q_n) \mod m_n), \tag{1}
\]

\[
W - Q = ((w_1 - q_1) \mod m_1, ..., (w_n - q_n) \mod m_n), \tag{2}
\]

\[
W \cdot Q = ((w_1 \cdot q_1) \mod m_1, ..., (w_n \cdot q_n) \mod m_n), \tag{3}
\]

where \( Q \equiv q_i \mod m_i \); \( i = 1, 2, ..., n \).

The expressions (1)-(3) show that arithmetic operations are performed in parallel, which allows for computations at maximum speed. Therefore, RNS codes are used in digital signal processing [8], digital filtering [9] and multi-scale signal analysis [10,11].

The second group consists of polynomial modular codes. These codes feature prime polynomials \( m_i(x) \), where \( i = 1, 2, ..., n \). The product sets a range

\[
M^n(x) = \prod_{i=1}^{n} m_i(x). \tag{4}
\]

Thus, any polynomial \( W(x) \), for which \( \deg W(x) < \deg M^n(x) \) is true, can be uniquely represented by a sequence \( W(x) = (w_1(x), w_2(x), ..., w_n(x)) \), where \( w_i(x) \equiv W(x) \mod m_i(m) \). Then, for a polynomial modular code

\[
W(x) + Q(x) = ((w_1(x) + q_1(x)) \mod m_1(x), ..., (w_n(x) + q_n(x)) \mod m_n(x)), \tag{5}
\]

\[
W(x) - Q(x) = ((w_1(x) - q_1(x)) \mod m_1(x), ..., (w_n(x) - q_n(x)) \mod m_n(x)), \tag{6}
\]

\[
W(x) \cdot Q(x) = ((w_1(x) \cdot q_1(x)) \mod m_1(x), ..., (w_n(x) \cdot q_n(x)) \mod m_n(x)), \tag{7}
\]

where \( Q(x) \equiv q_i(x) \mod m_i(x); \; i = 1, 2, ..., n \).

In this case, summation and subtraction are defined by a finite Galois module. In the target case, the Galois field GF (2) was chosen.

Since polynomial modular codes are position-independent, special-purpose computing devices should contain a direct converter from the positional numeral system (PNS) to PMC, as well as an inverse PMC-to-PNS converter. Inverse transformations are generally allowed by the Chinese remainder theorem

\[
W(x) = \sum_{i=1}^{n} w_i(x)M_i(x) \mod M^n(x) = \sum_{i=1}^{n} w_i(x)g_i(x)m_i^{-1}(x)M^n(x) - r_w(x)M^n(x), \tag{8}
\]
where \(M_i(x) = g_i(x)m_i^{-1}(x)M^n(x)\) is an orthogonal basis for PMC; \(g(x)\) – the weight of \(i\)th basis is so that \(g_i(x)m_i^{-1}(x)M^n(x) \equiv 1 \mod m_i(x)\); \(g(x)\) is a rank of polynomial \(W(x)\).

PMC applications obviously encompass orthogonal signal transformations in telecommunication systems [10], SPN encryption [12], and friend-or-foe identification [5]. Once applied, PMC can not only speed up data processing, but also improve the fault tolerance of special-purpose computing devices based on polynomial modular codes.

2.2 Error detection and correction based on the error syndrome in the extended base system

To ensure single-error correction and detection, two parity bases \(m_{n+1}(x)\) and \(m_{n+2}(x)\) are added into the polynomial modular code \(W(x) = (w_1(x), w_2(x), ..., w_n(x))\). The bases satisfy the condition

\[
\deg m_{n+1}(x) + \deg m_{n+2}(x) \geq \deg m_1(x) + \deg m_{n-1}(x).
\]

Then the list \(W(x) = (w_1(x), ..., w_{n+2}(x))\) is not in error, if the condition is

\[
\deg W(x) < \deg M^n(x).
\]

When an error occurs in \(W(x)\), the \(j\)th remainder \(w_j^*(x) = w_j(x) + \Delta w_j(x)\) changes. As a result, the condition (10) is violated, since

\[
W^*(x) = \sum_{i=1}^{n+2} w_i(x)M_i(x) \mod M^{n+2}(x) = W(x) + [\Delta w_j(x)M_j(x)] \mod M^{n+2}(x),
\]

where \(M^{n+2}(x) = \prod_{i=1}^{n+2} m_i(x)\) is the full-cycle polynomial modular code; \(\Delta w_j(x)\) is the error value on \(j\)th PMC basis; \(j = 1, 2, ..., n + 2\).

Thus, when an error occurs, then \(\deg W^*(x) > \deg M^n(x)\).

The error detection and correction algorithm is based on the projection method in [8]. In this method, residues are sequentially removed from the code \(W^*(x) = (w_1(x), ..., w_j^*(x), ..., w_{n+2}(x))\). A resulting truncated code is transferred to the PNS according to (8). Then the result is compared with \(M^n(x)\). Only when the remainder \(w_j^*(x)\) is removed, the condition (10) will be satisfied. This way, errors are detected and corrected. The main drawback of the method is large circuit and time costs required for detecting and correcting errors. An algorithm based on the extended base system is a means to eliminate this drawback.

The algorithm formulated is based on the congruence of parity residues \(w_{n+1}(x), w_{n+2}(x)\) of the polynomial modular code with residues \(\hat{w}_{n+1}(x), \hat{w}_{n+2}(x)\) that are determined by information residues. To do this, the error syndrome is calculated as

\[
\begin{align*}
S_1(x) &= w_{n+1}(x) + \hat{w}_{n+1}(x) \\
S_2(x) &= w_{n+2}(x) + \hat{w}_{n+2}(x)
\end{align*}
\]

(12)

If \(S_1(x) = 0, S_2(x) = 0\), then the PMC combination is not in error. Otherwise, the magnitude of the syndrome can determine the position and value of an error.

To develop the detection and correction algorithm, we use the expression (8) using only \(n\) PMC information bases

\[
W(x) = \sum_{i=1}^{n} w_i(x)g_i^n(x)M^n_i(x),
\]

(13)
where $M^n_i(x) = \frac{M^n(x)}{m_i(x)}$; $i = 1, 2, ..., n$.

The expression (13) avoids the calculation of the rank $rW(x)$ when performing the inverse transformation. We calculate the parity residues $\hat{w}_{n+1}(x), \hat{w}_{n+2}(x)$ using information residues $(w_1(x), ..., w_n(x))$. Then we get

$$\hat{w}_{n+1}(x) = \sum_{i=1}^{n} \left[ w_i(x)g^n_i(x) \right]^T M^n_i(x) \left|_{m_i(x)} \right] =$$

$$= \left[ w_1(x)g^n_1(x) \right]^T \left[ M^n_1(x) \right]_{m_1(x)} + ... + \left[ w_n(x)g^n_n(x) \right]^T \left[ M^n_n(x) \right]_{m_n(x)}.$$

(14)

$$\hat{w}_{n+2}(x) = \sum_{i=1}^{n} \left[ w_i(x)g^n_i(x) \right]^T M^n_i(x) \left|_{m_i(x)} \right] =$$

$$= \left[ w_1(x)g^n_1(x) \right]^T \left[ M^n_1(x) \right]_{m_1(x)} + ... + \left[ w_n(x)g^n_n(x) \right]^T \left[ M^n_n(x) \right]_{m_n(x)}.$$

(15)

The expressions (14) and (15) show that this algorithm can be implemented in parallel, which reduces the time required to calculate the error syndrome.

3. Results and discussion

Let the information moduli $m_1(x) = x + 1$, $m_2(x) = x^2 + x + 1$, $m_3(x) = x^4 + x^3 + x^2 + x + 1$. Then the working range $M^3(x) = \prod_{i=1}^{3} m_i(x) = x^7 + x^6 + x^5 + x^2 + x + 1$. Let us add the parity bases $m_4(x) = x^4 + x^3 + 1$ and $m_5(x) = x^4 + x + 1$, which has extended the range up to $M^5(x) = x^{15} + 1$.

Let us calculate $M^3_i(x)$, where $i = 1, 2, ..., n$ for weight $g^n_i(x)$, value $M^3_i(x) \left|_{m_i(x)} \right.$ and $M^3_i(x) \left|_{m_i(x)} \right.$.

$$M^3_1(x) = x^6 + x^4 + x^3 + x^2 + 1$$

$$M^3_2(x) = m_1(x)m_3(x) = x^5 + 1$$

$$M^3_3(x) = m_1(x)m_2(x) = x^3 + 1$$

Let the polynomial be $W(x) = x^6 - (1, 1, x, x^3 + x^2 + x + 1, x^3 + x^2, x^2 + x + 1)$. Then

$$\hat{w}_4(x) = \sum_{i=1}^{3} \left[ w_i(x)g^3_i(x) \right]^T M^3_i(x) \left|_{m_i(x)} \right.$$ 

$$= \left[ (x^3 + x + 1) + (x + 1)(x^3 + x) + x(x^2 + x + 1)(x^3 + 1) \right]^T = x^3 + x^2 + x + 1.$$

$$\hat{w}_5(x) = \sum_{i=1}^{3} \left[ w_i(x)g^3_i(x) \right]^T M^3_i(x) \left|_{m_i(x)} \right.$$ 

$$= \left[ x + (x + 1)(x^2 + x + 1) + x(x^2 + x + 1)(x^3 + 1) \right]^T = x^3 + x^2.$$

The error syndrome $S_1(x) = 0, S_2(x) = 0$. So the code is not in error.
Let the error value $\Delta w_1(x) = 1$ takes place on the basis $m(x)$. Then, the erroneous residue $w_1^*(x) = w_1(x) + \Delta w_1(x) = 0$ and $W^*(x) = (0, 1, x, x^3 + x^2 + x + 1, x^3 + z^2)$. Let us use the formulated algorithm. Then

$$\hat{w}_4(x) = \sum_{i=1}^{3} w_1(x)g_i^3(x)\left| \frac{M_i^3(x)}{m_i(x)} \right|^{+} = 0 \cdot (x^3 + x + 1) + (x + 1)(x^3 + x) + x(x^2 + x + 1)(x^3 + 1)\left| \frac{3}{x^3 + x^2 + 1} \right| = x^2.$$

$$\hat{w}_5(x) = \sum_{i=1}^{3} w_1(x)g_i^3(x)\left| \frac{M_i^3(x)}{m_i(x)} \right|^{+} = 0 \cdot x + (x + 1)(x^2 + x + 1) + x(x^2 + x + 1)(x^3 + 1)\left| \frac{5}{x^3 + x^2 + x} \right| = x^3 + x^2 + x.$$

The error syndrome $S_1(x) = x^3 + x + 1, S_2(x) = x$. So the code is in error. All single-error non-congruent syndromes were obtained during the study. Then

$$W(x) = (0, 1, x, x^3 + x^2 + x + 1, x^3 + z^2) + (0, 0, 0, 0, 0) = (1, 1, x, x^3 + x^2 + x + 1, x^3 + z^2).$$

The error has been corrected. The effectiveness of the formulated error detection and correction algorithm and projection method was assessed by modeling based on an Altera processor from the Cyclone III family of the EP3C80F484C6 model. Digital circuits were evaluated against the following criteria: the time of the operation to be implemented on the FPGA and the number of FPGA logical elements (LE) exploited. The studies show that for one inverse transformation from PMC to a positional base system reduces circuit costs by 5.55 times and span time by 1.09 times compared to the projection method.

4. Conclusion
The paper presents an algorithm for detecting and correcting errors, based on the extended PMC base system. To evaluate its effectiveness, the above algorithm was compared with the projection method. An Altera processor from the Cyclone III family of the EP3C80F484C model was selected for simulation. A comparative analysis showed that the projection method implemented for the selected example required five inverse PMC-to-PNS converters. Thus, the formulated error detection and correction algorithm based on the extended base system reduces circuit costs by 5.55 times and span time by 1.09 times compared to the projection method.

5. Acknowledgments
This work was supported by the Russian Foundation for Basic Research, project No. 18-07-01020.

References
[1] Paulo S R Dinis 2010 *Digital Signal Processing. System Analysis and Design* (New York: Cambridge University Press)
[2] Antonio A 2016 *Digital Signal Processing* (New York: Mgraw-Hill)
[3] Rogachev M K, Mukhametshin V V and Kuleshova L S 2019 Improving the efficiency of using resource base of liquid hydrocarbons in Jurassic deposits of Western Siberia *Journal of Mining Institute* 240 711–715 DOI: 10.31897/PMI.2019.6.711
[4] Schulze H, Luders C 2005 Theory end Application of OFDM and CDMA. *Wideband Wireless Communications* (London: John Wiley&Sons.Ltd)
[5] Kalmykov I A, Pashintsev V P, Zhuk A P, Chistousov N K 2019 *International Journal of Engineering and Advanced Technology (IJEAT)* 8(5) p.p. 2557-2562
[6] Ajaankar S C, Kotle M T 2014 *International Journal of Emerging Engineering Research and Technology* 2(2) pp 187-191
[7] Shao P, Wu Z, Zhou X 2017 *Soft Comput* 21 pp 2631–2642
[8] Omondi A, Premkumar B 2007 *Residue Number Systems: Theory and Implementation* (London: Imperial College Press)
[9] Yaskin S A, Mukhametshin V V, Andreev V E and Dubinskiy G S 2018 Forecasting the parameters of non-stationary water flooding of oil deposits *IOP Conference Series: Earth and Environmental Science (IPDME 2018 – International Conference on Innovations and Prospects of Development of Mining Machinery and Electrical Engineering)* 194(6) 1-5 DOI: 10.1088/1755-1315/194/6/062037
[10] Katkov K A, Timoshenko L I, Dunin A V 2015 *Journal of Theoretical and Applied Information Technology* 80(3) pp 391-400
[11] Tyncherov K T, Selivanova M V 2017 *International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017* DOI: 10.1109/ICIEAM.2017.8076360
[12] Chu J, Benaissa M 2013 Error Detecting AES Using Polynomial Residue Number System. *Microprocessors and Microsystems* 37 pp 228-234