© International Journal of Combinatorial Optimization Problems and Informatics, Vol. 9, No. 1, Jan-April 2018, pp. 81-84. ISSN: 2007-1558.

Reliability Improvement of Information Systems by Residue Number System Code

Anton Nazarov[1], Nikolay Chervyakov[1], AndreiTchernykh[2], MikhailBabenko[1]
North-Caucasus Federal University, Stavropol, Russia[1]
CICESE Research Center, Ensenada, Baja California, México[2]
ncherviakov@ncfu.ru, mgbabenko@ncfu.ru, kapitoshking@mail.ru, chernykh@cicese.mx

Abstract. One of the most popular current methods of improving there liability of data communication systems is error-correcting codes to correct decoding errors that occur during data transmission on communication channels by introducing some redundancy in their encoding. This paper describes the main steps of error corrections using the Redundant Residue Number System as the data encryption. The features of the implementation of algorithms in terms of reducing the time delay and hardware costs are presented.

Keywords: Residue Number System, Redundant Residue Number System, Mixed Radix Conversion, Error Control Codes.

1 Introduction

Modern control of errors in information systems is one of the most important problems. Wireless systems are characterized by unfavorable data transmission medium, large signal interference, dynamic changing distance between the devices, etc. [1, 2]. The protection from noise in data transmission systems operating in conditions of autonomy and remoteness is of the particular importance [3, 4]. In this case, the transmitted and received signals are exposed to a variety of adverse impacts. Accumulated changes in the signal caused by noise may adversely impact the data quality. In this context, the most important issue is to ensure the noise immunity of the transmitted signal.

2 Residue Number System (RNS)

Let us consider a vector $X = (x_1, x_2, \dots, x_n)$, where components are natural numbers satisfying the condition $0 \le x_i \le m_i - 1$, where $i = 1,2, \dots, n$; and $m_1, \dots, m_n$ are pairwise relatively prime natural numbers which are called modules RNS.

It is obvious that the number of different (i.e., they are different by at least one component) vectors of this type is the product of $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$ which is called RNS range. Thus, RNS modules $m_1, \dots, m_n$ makes it possible to encode non-negative integers from $0 \le X \le M - 1$ range. Encoding numbers in RNS are implemented by the following rule:

$$x_i = X \bmod m_i,\ i = 1,2, \dots, n.$$

This method of representing numbers is non-positional and has a number of advantages over the traditional positional form of number representation: modular operations such as addition and multiplication can be performed in parallel for each module due to the lack of bit carries. It leads to multiple reductions of time delays in the execution of these operations. Operand rank is reduced by decomposition of the original number on the remains of the modules RNS.

One of the most optimal methods of coding numbers in RNS in terms of hardware and time costs is the method proposed in [5]. Consider this method based on the following example.

Example. Let $X = 2460034527$ and modulus $m = 7$.

Given X can be represented in binary system as:

$$X = 10010010\ 10100001\ 00100101\ 11011111$$

Received Dec 2, 2017 / Accepted Jan 22, 2018

Divide this form of X on 4 parts by 8 bits. For next computations find constants $\omega_k = N^i \ mod \ 7$, where $k = 0..3$, $i = 0, 8, 16, 24$:

$$\omega_0 = |2^0|_7 = 1; \omega_1 = |2^8|_7 = 4; \omega_2 = |2^{16}|_7 = 2; \omega_3 = |2^{24}|_7 = 1.$$

Following calculations:

$$||11011111|_{111} \cdot \omega_0|_7 = ||223|_7 \cdot 1|_7 = 6$$
$$||00100101|_{111} \cdot \omega_1|_7 = ||37|_7 \cdot 4|_7 = 1$$
$$||10100001|_{111} \cdot \omega_2|_7 = ||161|_7 \cdot 2|_7 = 0$$
$$||10010010|_{111} \cdot \omega_3|_7 = ||146|_7 \cdot 1|_7 = 6$$
$$|6 + 1 + 0 + 6|_7 = |13|_7 = 6$$

According to calculations $|X|_7 = 6$, which corresponds to real value.

3 Error Detection, Localization and Correction

Using of RNS in data encoding has all the properties of error-correcting codes, so as in any error-correcting codes, an opportunity to correct errors in decoding is caused by redundancy in encoding. In the case of *n*-modular RNS, we need to calculate two additional residue modulus m_{n+1}, m_{n+2}, to correct a single error (three additional residue to correct a double error; four – to correct the triple error, etc.), where $m_{n+2} > m_{n+1} > m_i$, $i = 1,2, \dots, n$ [5]. So, the product $m_1 \cdot m_2 \cdot \dots \cdot m_n$ is called the working range of RNS, and $m_1 \cdot m_2 \cdot \dots \cdot m_n \cdot m_{n+1} \cdot m_{n+2}$ is called the full range of Redundant RNS (RRNS).

The classical method of the error detection involves the conversion number represented by RRNS in the positional notation for the first *n* residues and the comparison it with a dynamic range of RNS (if a recovered number of falls in the working range, there is no error).

If a recovered number is larger than dynamic range, there is an error occurred during data transmission. In terms of optimization of hardware and time costs to recover positional representation number, the use of Mixed-Radix-Conversion (MRC) with the same set of modules as the RNS moduli set is suggested [6].

As a method of localization of the module in which an error has occurred, we use the projection method [6]. Under the projection *i* of the number, we mean a presentation of the numbers in reduced RNS, which is the source of RNS from which the module *i* is excluded. This representation is obtained by deleting the residue *i* in original record numbers. If we need to control multiple system error, we have to reduce the amount of the alleged errors.

The localization method is the following. If we exclude wrong residues, the code in the resulting abbreviated RNS does not contain errors. Consequently, in the new RNS, a number should be within the working range. However, if the module is excluded in the correct code, an error will be also contained in the abbreviated RNS. Therefore, the number of abbreviated RNS will exceed the working range. In comparison with the value of the working range, it is proposed to use the mentioned above MRC [6].

Let us consider MRC based on the example.

Example. Let moduli set for RNS and MRC is $m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 7$, then $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$;

$$\left|\left(\frac{M}{m_1}\right)^{\varphi(m_1)}\right|_M = \left|\left(\frac{210}{2}\right)^1\right|_{210} = 105; \left|\left(\frac{M}{m_2}\right)^{\varphi(m_2)}\right|_M = \left|\left(\frac{210}{3}\right)^2\right|_{210} = 70;$$
$$\left|\left(\frac{M}{m_3}\right)^{\varphi(m_3)}\right|_M = \left|\left(\frac{210}{5}\right)^4\right|_{210} = 126; \left|\left(\frac{M}{m_4}\right)^{\varphi(m_4)}\right|_M = \left|\left(\frac{210}{7}\right)^6\right|_{210} = 120.$$

The values $C_{ij} = \left(\frac{M}{m_i}\right)^{\varphi(m_i)}$:

$$C_{11} = 1, C_{12} = 1, C_{13} = 2, C_{14} = 3;$$
$$C_{21} = 0, C_{22} = 2, C_{23} = 1, C_{24} = 2;$$

$$C_{31} = 0,\ C_{32} = 0, C_{33} = 1, C_{34} = 4;$$

$$C_{41} = 0,\ C_{42} = 0, C_{43} = 0, C_{44} = 4.$$

Let $X = 73_{(10)} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)_{(\mathrm{RNS})} = (1,1,3,3)_{(\mathrm{RNS})}$. We need to find that representation in mixed radix based on MRC $X = (a_1, a_2, a_3, a_4)_{(\mathrm{MRC})}$. Then:

$$\alpha_1 C_{11} = 1,\ \alpha_1 C_{12} = 1,\ \alpha_1 C_{13} = 2,\ \alpha_1 C_{14} = 3;$$

$$\alpha_2 C_{21} = 0,\ \alpha_2 C_{22} = 2,\ \alpha_2 C_{23} = 1,\ \alpha_2 C_{24} = 2;$$

$$\alpha_3 C_{31} = 0,\ \alpha_3 C_{32} = 0,\ \alpha_3 C_{33} = 3,\ \alpha_3 C_{34} = 12;$$

$$\alpha_4 C_{41} = 0,\ \alpha_4 C_{42} = 0,\ \alpha_4 C_{43} = 0,\ \alpha_4 C_{44} = 12.$$

$$X_{(MRC)} = \alpha_1(C_{11}, C_{12}, \dots, C_{1n}) + \alpha_2(C_{21}, C_{22}, \dots, C_{2n}) + \cdots + \alpha_n(C_{n1}, C_{n2}, \dots, C_{nm}).$$

Add up the columns modulo m_i considering the carry propagation:

			RNS's moduli $m_1 m_2 m_3 m_4$
$X_{(\mathrm{RNS})} \rightarrow$	$\alpha_1 = 1$	$\rightarrow$	[1 1 2 3]
	$\alpha_2 = 1$	$\rightarrow$	[0 2 1 2]
	$\alpha_3 = 3$	$\rightarrow$	[0 0 3 12]
	$\alpha_4 = 3$	$\rightarrow$	[0 0 0 12]
		$X_{(\mathrm{MRC})} =$	[1 0 2 1]
		Carry	$\searrow_{+1} \searrow_{+1}$

The procedure of the error correction is to choose a projection that does not contain an incorrect residue and to recovery the numbers of the MRC projection positional representation of the number. Note that the correction of an error based on this method requires the calculation of $n + 1$ projections (Fig. 1), while correction the error by using the Chinese remainder theorem (CRT) requires the calculation of $n + 2$ projections (Fig. 2).

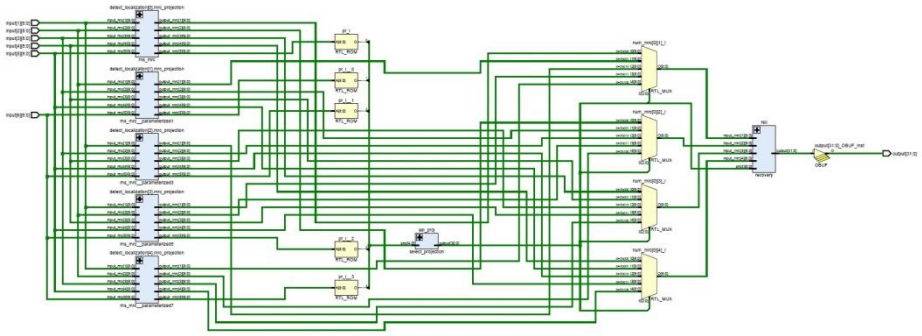

Fig. 1. Architecture of the circuit for error correction based on MRC.

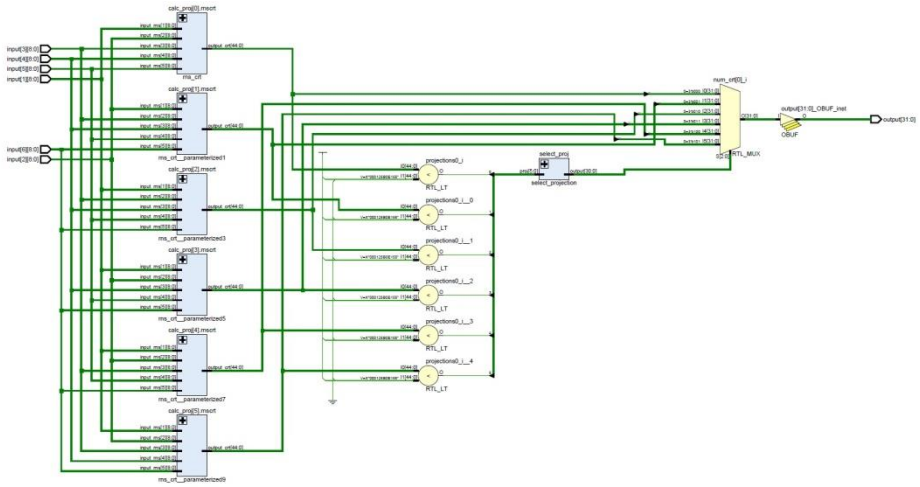

Fig. 2. Architecture of the circuit for error correction based on CRT

Furthermore, all possible products $\alpha_i C_{ij}$ can be pre-calculated and stored in the circuit memory.

4 Conclusion

An approach to encoding, error correction and data decoding described in the paper can improve the reliability of the data communication system. It is the optimum in terms of hardware costs of encoding device, error correction and data decoding device. The circuits based on proposed method require 1,2-1,3 times less energy and in 1,5-1,6 times less resources than circuits based on CRT, in average. However, the architecture based on CRT has the advantage in speed compared with the proposed technique.

References

1. Chervyakov N.I., Babenko M.G., Deryabin M.A., Shabalina M.N., Ba A. The develop-ment of secure mobile computing network based on secret sharing schemes // IEEE NWRussia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW). – 2016. – pp. 180-184.
2. Tchernykh, A., Schwiegelsohn, U., Talbi, E.-G., Babenko, M.: Towards Understanding Uncertainty in Cloud Computing with risks of Confidentiality, Integrity, and Availabil-ity. J Comput Sci. Elsevier. DOI: 10.1016/j.jocs.2016.11.011 (2016)
3. Tchernykh A., Pecero J.E., Barrondo A., Schaeffer E. Adaptive energy efficient sched-uling in Peer-to-Peer desktop grids // Future Generation Computer Systems, vol. 36. – 2014. – pp. 209-220.
4. Kliazovich D., Pecero J.E., Tchernykh A., Bouvry P., Khan S.U., Zomaya A.Y. CA-DAG: Modeling communication-aware applications for scheduling in cloud computing // Journal of Grid Computing, vol. 14, no. 1. – 2016. pp. 23-39.
5. Chervyakov N.I., Babenko M.G., Nazarov A.S., Garianina A.I. Realization Problems of Cryptographic Transformations by Transfer of Modular Data In Security Systems // In-ternational IEEE-Siberian Conference on Control and Communications SIBCON-2015. – 2015. – Art. no. 7146986.
6. Chervyakov N.I., Lyakhov P.A., Babenko M.G., Garyanina A.I., Lavrinenko I.N., Lav-rinenko A.V., Deryabin M.A. An efficient method of error correction in fault-tolerant modular neurocomputers // Neurocomputing, vol. 205. – 2016. – pp. 32-44.