Design of a Residual Adder in Computer Systems

Victor Krasnobayev[a], Alexander Kuznetsov[a,b], Victoria Popenko[a], and Tetiana Kuznetsova[a]

[a] *V. N. Karazin Kharkiv National University, 4Svobody sq., Kharkiv, 61022, Ukraine*
[b] *JSC "Institute of Information Technologies," 12 Bakulin str., Kharkiv, 61166, Ukraine*

Abstract

The purpose of this article is to consider an algorithm for synthesizing the structure of the adder of two residuals a_i and b_i numbers $A=(a_1,a_2,...,a_i,...,a_k)$ and $B=(b_1,b_2,...,b_i,...,b_k)$ for an arbitrary value of the module m_i of the residual class system (RCS), by organizing inter-bit connections between binary one-bit adders (BOA), the combination of which makes up the structure of modulo adder. The algorithm for the synthesis of adders by arbitrary modules is based on the usage of existing adders by module $M=2^n-1$, which consists of a set of sequentially located BOA, by introducing and using additional inter-bit connections of the form $\mathrm{X}_{\downarrow i\uparrow j}$. Specific examples of the synthesis of structures of binary adders for various values of the RCS modules m_i are given.

Keywords

Residual class system, non-positional code structures, binary one-bit adders.

1. Introduction

The operation of adding two numbers is the main operation, which is implemented by a computer system (CS), both in a positional binary notation (PN) and in a non-positional notation of residual classes [1–4]. The adder of two numbers is the main part of the operating device of CS in PN. Adders of two numbers by the module m_i are also elements of CS along with positional adders [5–8]. In RCS, the modular addition operation $(a_i+b_i)\bmod m_i$ is implemented on the basis of the usage of low-bit modulo m_i adders [9–13]. One of the methods for implementation of the modular addition operation $(a_i+b_i)\bmod m_i$ is based on the usage of structures of positional low-bit binary adders [14–17]. This approach provides a wide range of options for the implementation of the structure of such adders. This allows to fully use available practical experience in the design and selection of structures of binary adders [4, 12, 18]. The purpose of the article is to consider an algorithm for synthesizing the structure of an adder of two residues of numbers by module.

2. Design of a Residual Adder

The article discusses the synthesis of an adder of two residues of numbers by an arbitrary RCS module m_i. Synthesis of modulo adder is a procedure for constructing the structure of a non-positional adder from positional binary one-bit adders (BOA). In a non-positional adder by an arbitrary module m_i, an addition circuit is used, which is implemented in the structure of adder by module $M=2^n-1$. This is achieved by organizing and using additional inter-bit connections $\mathrm{X}_{\downarrow i\uparrow j}$, in the general case, between the j^{th} and the i^{th} BOA of the adder module M.

An arbitrary initial structure of a n-bit binary adder by the module $M=2^n-1$ is shown in Fig. 1.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: v.a.krasnobaev@gmail.com (A.1); kuznetsov@karazin.ua (A.2); vita.popenko@gmail.com (A.3); kuznetsova.tatiana17@gmail.com (A.4)
ORCID: 0000-0001-5192-9918 (A.1); 0000-0003-2331-6326 (A.2); 0000-0003-1217-1862 (A.3); 0000-0001-6154-7139 (A.4)

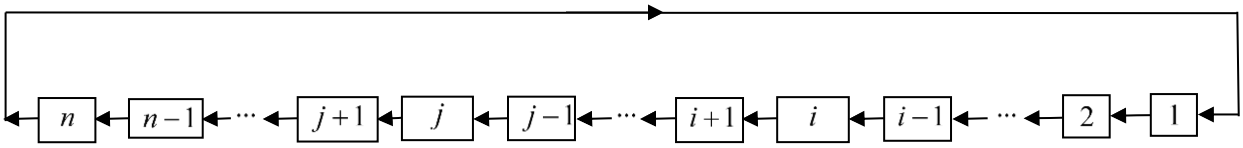

Figure 1: The structure of a binary adder by module $M = 2^n - 1$

The task of an adder by module m_i synthesis is to ensure the modular addition of two residues for given modules by means of an adder by module $M = 2^n - 1$. In this article, this is achieved by introducing into the adder by module M additional links of the form $\mathrm{X}_{\downarrow i \uparrow j}$, where the sign $\mathrm{X}_{\downarrow i \uparrow j}$ denotes the connection between the output of the j-th BOA and the input of the i^{th} BOA. A diagram of the organization of such an additional connection between the output of the j^{th} BOA and the input of the i^{th} BOA is shown in Fig. 2.

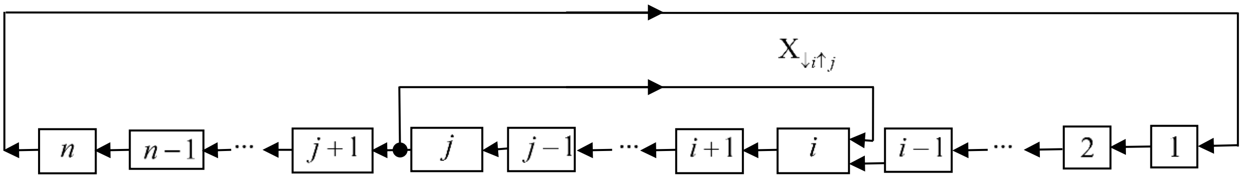

Figure 2: Diagram of an adder by module $M = 2^n - 1$ with one additional connection $\mathrm{X}_{\downarrow i \uparrow j}$

The essence of constructing adders by module RCS is as follows. In the initial adder by module $M = 2^n - 1$, on the basis of certain rules, additional connections $\mathrm{X}_{\downarrow i \uparrow j}$ are formed [8, 12, 17]. The usage of additional connections $\mathrm{X}_{\downarrow i \uparrow j}$ in the adder by module $M = 2^n - 1$ allows synthesizing an adder for performing the operation of adding the residues of numbers by module m_i, since the introduction of additional connections $\mathrm{X}_{\downarrow i \uparrow j}$ changes the weights of individual bits of the adder and reduces the module of the adder from the initial value M to the required modulus value m_i.

In the general case, the modulo adder synthesis algorithm consists of a sequence of performing the following operations.

1. Obtaining the structure of the adder by module $M = 2^n - 1$, where

$$n = [\log_2(m_i - 1)] + 1.$$

2. Determination of the adder binary bits S_i for which equality $S_i = 0$ is true. The process of determining the condition $S_i = 0$ is based on the representation of the module in binary code.

3. Additional connection $\mathrm{X}_{\downarrow i \uparrow j}$ begins with the most significant bit of the adder.

4. Additional connection $\mathrm{X}_{\downarrow i \uparrow j}$ goes to the BOA input, for which $S_i = 0$.

3. Examples of Residual Adders

Two examples of synthesis of structures of adder are considered.

Example 1. $m_i = 53$. The stages of the synthesis of an adder by the module of RCS are as follows.

1. In accordance with the size of the module $m_i = 53$, the number n of BOA of an adder by the module $M = 2^n - 1$ is determined. For the module $m_i = 53$ there is

$$n = [\log_2(m_i - 1)] + 1 = [\log_2(53 - 1)] + 1 = 6.$$

The structure of the adder by module

$$M = 2^n - 1 = 63$$

will be the following (Fig. 3).

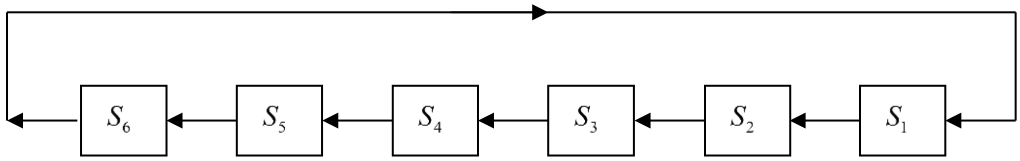

Figure 3: Initial structure of adder by module $M = 2^6 - 1$

The initial structure of the adder by module $m_i = 53$ without additional connections $X_{\downarrow i \uparrow j}$ will be the same.

2. Module $m_i = 53$ in binary code $S_6\ S_5\ S_4\ S_3\ S_2\ S_1$ is 110101, which means

$$S_6 = 1,\ S_5 = 1,\ S_4 = 0,\ S_3 = 1,\ S_2 = 0 \text{ and } S_1 = 1.$$

From the form of the module $m_i = 53$ which is represented in the binary code,

$$S_2 = S_4 = 0$$

is determined.

3. Based on the obtained results, the structure of the adder by the module $m_i = 53$ is represented in the following form

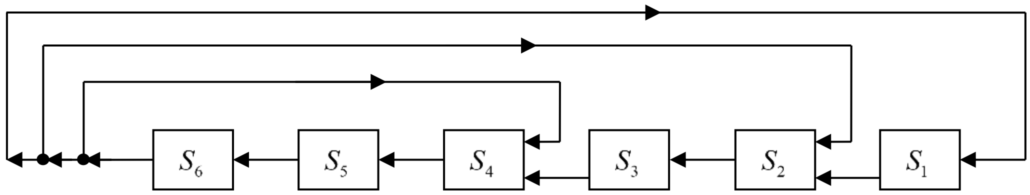

Figure 4: Structure of adder by modulo $m_i = 53$

In accordance with the synthesis method, two additional connections $X_{\downarrow 4 \uparrow 6}$ and $X_{\downarrow 2 \uparrow 6}$ are introduced into the adder by module $M = 2^6 - 1$. In order to check the correctness of the synthesis of the adder by module $m_i = 53$, the value of the RCS module $M = m_i$ for a given adder structure is determined. Based on the given structure of the adder (Fig. 4), a number of structures of individual parts of the adder by the module $m_i = 53$ are composed. The first part of the adder structure is shown in Fig. 5.

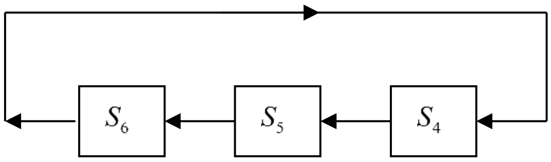

Figure 5: First part of the structure of adder by module m_i

The first part of the adder structure module M_1 will be the following

$$M_1 = \tau_3 \cdot \tau_5 \cdot \tau_4 - 1\,.$$

The second part of the adder structure is shown in Fig. 6.

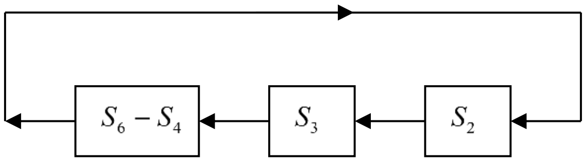

Figure 6: Second part of the structure of adder by module m_i

For this part of the adder, the structure module M_2 will be the following

$$M_2 = M_1 \cdot \tau_3 \cdot \tau_2 - 1 = (\tau_6 \cdot \tau_5 \cdot \tau_4 - 1) \cdot \tau_3 \cdot \tau_2 - 1 .$$

For adder, by module, the value of module $M = m_i$ of RCS will be determined as follows (fig. 4-6)

$$m_i = M_2 \cdot \tau_1 - 1 = \left[(\tau_6 \cdot \tau_5 \cdot \tau_4 - 1) \cdot \tau_3 \cdot \tau_2 - 1 \right] \cdot \tau_1 - 1 = \left[(2^3 - 1) \cdot 2^2 - 1 \right] \cdot 2 - 1 = 53 .$$

Based on the performed calculations, there is the conclusion that the synthesis of the adder by module $m_i = 53$ (fig. 4) was carried out correctly.

Example 2. $m_i = 97$. The stages of the synthesis of an adder by the module of RCS are as follows.

1. In accordance with the size of the module $m_i = 97$, the number n of BOA of an adder by the module $M = 2^n - 1$ is determined. For the module $m_i = 97$ there is

$$n = \left[\log_2 (m_i - 1) \right] + 1 = \left[\log_2 (97 - 1) \right] + 1 = 7 .$$

The structure of the adder by module

$$M = 2^n - 1 = 2^7 - 1 = 127$$

will be the following (Fig. 7).

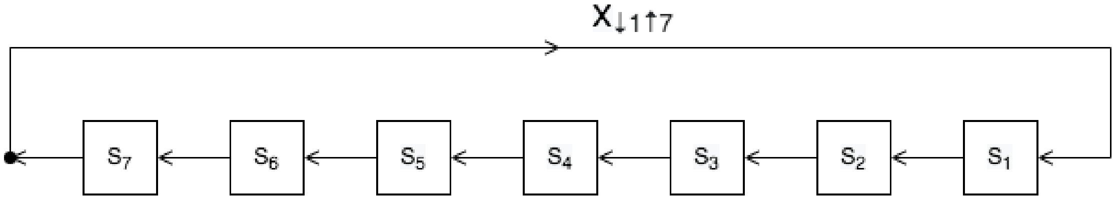

Figure 7: Initial structure of adder by module $M = 2^7 - 1$

2. Module $m_i = 97$ in binary code $S_7 S_6\ S_5\ S_4\ S_3\ S_2\ S_1$ is 1100001, which means

$$S_7 = 1, S_6 = 1, S_5 = S_4 = S_3 = S_2 = 0, S_1 = 1 .$$

3. Based on the obtained results, the structure of the adder by the module $m_i = 97$ is represented in Fig. 8.

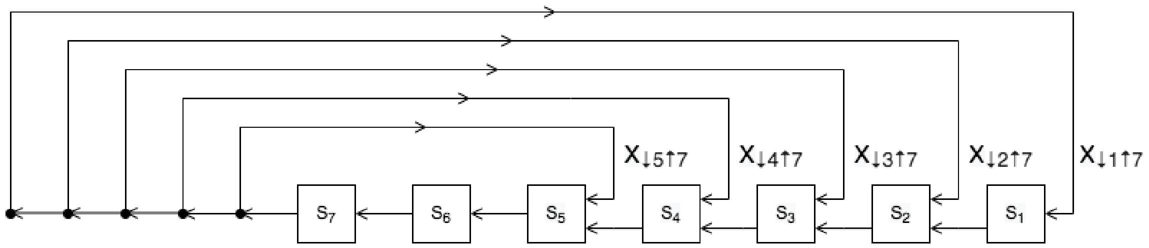

Figure 8: Structure of adder by modulo $m_i = 97$

In accordance with the synthesis method, four additional connections $X_{\downarrow 5 \uparrow 7}, X_{\downarrow 4 \uparrow 7}, X_{\downarrow 3 \uparrow 7}, X_{\downarrow 2 \uparrow 7}$ are introduced into the adder by module $M = 2^7 - 1$. In order to check the correctness of the synthesis of the adder by module $m_i = 97$, the value of the RCS module $M = m_i$ for a given adder structure is determined.

The first part of the adder structure is shown in Fig. 9.

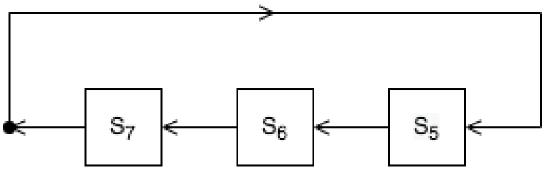

Figure 9: First part of the structure of adder by module m_i

The first part of the adder structure module M_1 will be the following $M_1 = \tau_7 \cdot \tau_6 \cdot \tau_5 - 1$. The second part of the adder structure is shown in Fig. 10.

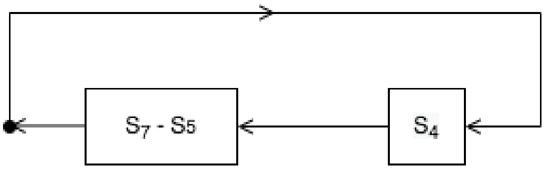

Figure 10: Second part of the structure of adder by module m_i

The first part of the adder structure module M_2 will be the following $M_2 = M_1 \cdot \tau_4 - 1$. The third part of adder structure is shown in Fig. 11.

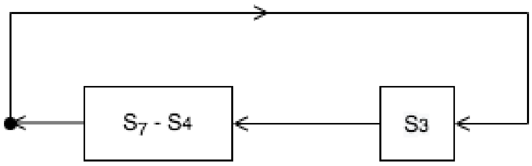

Figure 11: Third part of the structure of adder by module m_i

The first part of the adder structure module M_3 will be the following $M_3 = M_2 \cdot \tau_3 - 1$. The fourth part of the adder structure is shown in Fig. 12.

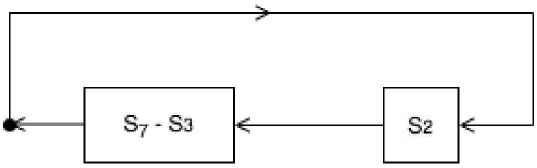

Figure 12: Fourth part of the structure of adder by module m_i

The first part of the adder structure module M_4 will be the following $M_4 = M_3 \cdot \tau_2 - 1$. The fifth part of the adder structure is shown in Fig. 13.

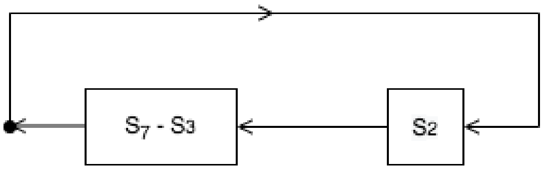

Figure 13: Fifth part of the structure of adder by module m_i

The first part of the adder structure module M_5 will be the following $M_5 = M_4 \cdot \tau_1 - 1$.

The value of module m_i :

$$M_1 = \tau_7 \cdot \tau_6 \cdot \tau_5 - 1 \text{ (Fig. 9);}$$

$$M_2 = M_1 \cdot \tau_4 - 1 = (\tau_7 \cdot \tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1 \text{ (Fig. 10);}$$

$$M_3 = M_2 \cdot \tau_3 - 1 = \left[(\tau_7 \cdot \tau_6 \cdot \tau_5 - 1)\tau_4 - 1\right]\tau_3 - 1 \text{ (Fig. 11);}$$

$$M_4 = M_3 \cdot \tau_2 - 1 = \left\{\left[(\tau_7 \cdot \tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1\right] \cdot \tau_3 - 1\right\} \cdot \tau_2 - 1 \text{ (Fig. 12);}$$

$$M_5 = M_4 \cdot \tau_1 - 1 = \left(\left\{\left[(\tau_7 \cdot \tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1\right] \cdot \tau_3 - 1\right\} \cdot \tau_2 - 1\right) \cdot \tau_1 - 1 \text{ (Fig. 13).}$$

In this case, the result of the synthesis of the adder by module $m_i = 97$ (Fig. 8) is correct.

The given examples of the synthesis of the structure of adders by the module of RCS confirm the possibility of practical usage of the algorithm which is considered in the article.

4. Conclusions

The article considers an algorithm for synthesizing the structure of adders by the module m_i of RCS. The algorithm for the synthesis of adders is based on the usage of existing adders by modules $M = 2^n - 1$, which are widely used in CS, operating both in the PN and in the RCS. The article directly provides an algorithm for the synthesis of an adder by module m_i. The algorithm is implemented by introducing and using additional inter-bit connections $\mathrm{X}_{\downarrow i \uparrow j}$. The article formulates the rules for introducing these additional connections. The usage of additional connections (based on the structure of adder by module $M = 2^n - 1$) allows creating an adder that implements the operation of adding two residues a_i and b_i of numbers. A set of k adders by the module is an adder of two numbers $A = (a_1, a_2, ..., a_i, ..., a_k)$ and $B = (b_1, b_2, ..., b_i, ..., b_k)$ in RCS. Specific examples of the synthesis of adders by the module for various values of the RCS modules m_i are given.

5. Acknowledgments

This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.

6. References

[1] A. Yadin, Computer Systems Architecture, 1st ed., Chapman and Hall/CRC, Boca Raton, Taylor & Francis Group, CRC Press, 2016. doi:10.1201/9781315373287.

[2] S. A. Wright, Performance Modeling, Benchmarking and Simulation of High Performance Computing Systems, Future Generation Computer Systems 92 (2019) 900–902. doi:10.1016/j.future.2018.11.020.

[3] H. Kopetz, (Ed.), Modeling Real-Time Systems, in: Real-Time Systems: Design Principles for Distributed Embedded Applications, Springer US, Boston, MA, 1997, pp. 71–96. doi:10.1007/0-306-47055-1_4.

[4] R. S. Alford, Computer Systems Engineering Management, CRC Press, 2018. doi:10.1201/9781351070829.

[5] P. V A. Mohan, Residue Number Systems, Springer International Publishing, Cham, 2016. doi:10.1007/978-3-319-41385-3.

[6] Y.Zhang, An FPGA implementation of redundant residue number system for low cost fast speed fault tolerant computations, Master's thesis, Nanyang Technological University, Singapore, 2018. doi:10.32657/10220/47113.

[7] E. Vassalos, D. Bakalis, Residue-to-Binary Converter for the New RNS Moduli Set ${2^2n-2, \ 2^n-1, \ 2^n+1}$, in: 2019 Panhellenic Conference on Electronics Telecommunications (PACET), 2019, pp. 1–4. doi:10.1109/PACET48583.2019.8956249.

[8] V. A. Krasnobayev, A. A. Kuznetsov, S. A. Koshman, K. O. Kuznetsova, A Method for Implementing the Operation of Modulo Addition of the Residues of Two Numbers in the Residue Number System, Cybern Syst Anal. 56 (2020) 1029–1038. doi:10.1007/s10559-020-00323-9.

[9] V. M. Amerbaev, R. A. Soloviev, D. V. Telpukhov, Hardware Implementation of Fir Filter Based on Number-theoretic Fast Fourier Transform in Residue Number System, Open Engineering Sciences Journal 1 (2014). doi:10.2174/2352628901401010001.

[10] P. V. A. Mohan, Implementation of Residue Number System Based Digital Filters, Residue Number System 2 (2018). URL: journal.accsindia.org/implementation-of-residue-number-system-based-digital-filters

[11] P. V. A. Mohan, Specialized Residue Number Systems, in: P.V.A. Mohan (Ed.), Residue Number Systems: Theory and Applications, Springer International Publishing, Cham, 2016, pp. 177–193. doi:10.1007/978-3-319-41385-3_8.

[12] V. Krasnobayev, A. Kuznetsov, A. Yanko, B. Akhmetov, T. Kuznetsova, Processing of the Residuals of Numbers in Real and Complex Numerical Domains, in: T. Radivilova, D. Ageyev, N. Kryvinska (Eds.), Data-Centric Business and Applications, Springer International Publishing, Cham, 2021, pp. 529–555. doi:10.1007/978-3-030-43070-2_24.

[13] V. Krasnobayev, A. Kuznetsov, S. Koshman, S. Moroz, Improved Method of Determining the Alternative Set of Numbers in Residue Number System, in: O. Chertov, T. Mylovanov, Y. Kondratenko, J. Kacprzyk, V. Kreinovich, V. Stefanuk (Eds.), Recent Developments in Data Science and Intelligent Analysis of Information, Springer International Publishing, Cham, 2019, pp. 319–328. doi:10.1007/978-3-319-97885-7_31.

[14] M. Bayoumi, G. Jullien, W. Miller, A VLSI implementation of residue adders, IEEE Transactions on Circuits and Systems 34 (1987) 284–288. doi:10.1109/TCS.1987.1086130.

[15] G. Harman, I.E. Shparlinski, Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients, Int Math Res Notices 5 2016 1424–1446. https://doi.org/10.1093/imrn/rnv182.

[16] M. Karpinski, S. Ivasiev, I. Yakymenko, M. Kasianchuk, T. Gancarczyk, Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes, in: 16th International Conference on Control, Automation and Systems (ICCAS), 2016, pp. 1484–1486. doi:10.1109/ICCAS.2016.7832500.

[17] V. Krasnobayev, A. Kuznetsov, V. Popenko, A. Kononchenko, T. Kuznetsova, Determination of Positional Characteristics of Numbers in the Residual Class System, in: IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 151–156. doi:10.1109/DESSERT50317.2020.9125030.

[18] Hard real-time computing systems, Springer US, Boston, MA, 1997. doi:10.1007/b102312.