ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

A NOVEL APPROACH TO RESIDUE NUMBER SYSTEM DESIGN

Seyed Mostafa Mirhosseini[1], Amir Sabbagh Molahosseini[2], Mehdi Hosseinzadeh[3,4]
[1]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
[2]Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran
[3]Iran University of Medical Sciences, Tehran, Iran
[4]University of Human Development, Sulaimaniyah, Iraq
E-mail: s.m.mirhoseini@srbiau.ac.ir

The Residue Number System (RNS) has been considered as an efficient parallel tool to increase the performance of computational systems. However, RNS consists of several parts that lead to complexity of RNS. In this paper, a new approach to RNS system design based on unification of the carry-propagate adders (CPAs) of the arithmetic units of RNS with reverse converter is presented. The proposed method eliminates the complex modular CPA for some of channels and improves the current reverse converter designs by shifting some complex additions from arithmetic channel of RNS to the reverse converter. Experimental results show a significant reduction in area, power consumption and the delay in comparison with the previous design.

Ключевые слова: Residue Number System, computational system, adder, reverse conversion

DOI: 10.18469/ikt.2017.15.2.01

Introduction

Since the past decade, the computing industry has intensively tried to decrease the power consumption of portable systems. While lots of works have been done in this area, Residue Number System (RNS) has emerged as a viable nontraditional approach to increase the performance. The main functionality of RNS is that it decomposes complex arithmetic circuits into simpler ones [1]. Instead of performing large computations, every arithmetic's such as long bit multiplication is broken down into little parallel modulo multiplications. Despite the advantages of the RNS based arithmetic systems, the usage of this system has been rather restricted. The main limit is the additional hardware required especially for conversion from RNS to binary number. Therefore, every work that aims to make this component smaller, faster and less power consumer leads to make the RNS system more efficient and practical.

So far, many reverse converters architecture has been offered [1-6] but some drawbacks still can be seen in those designs. They are designed independently of arithmetic unit. Moreover, the New CRT-II [2], being the one of the newest algorithms in reverse converter design, makes the reverse converter smaller than the previous designs, but slower due to the use of many modular CPAs. This paper aims to address these challenges by considering some properties that have been ignored in overall design of RNS systems.

The three-moduli set $\{2^n-1, 2^n, 2^n+1\}$ has interesting attributes and consequently has been widely investigated. However, extensions of this moduli set have been introduced in order to increase the Dynamic Range, such as the $\{2^n-1, 2^n, 2^n+1, 2^{n+1}-1\}$ [4] or $\{2^k, 2^n-1, 2^n+1, 2^{n+1}-1\}$, $\{2^k, 2^n-1, 2^n+1, 2^{n-1}-1\}$[5], and $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^n+1, 2^{2n+1}-1\}$ [6].

In this paper, by taking into account some properties of reverse converter, the last modular adder of the addition or multiplication in arithmetic unit are considered together with the reverse converter to increase the performance. The proposed method eliminates the last adder that is slow in arithmetic unit and replaces it with a faster adder in reverse converter. This strategy not only results in speed up but also in overall area reduction.

The Proposed Approach

The RNS is composed of three basic components: forward converter, arithmetic unit and the reverse converter [1]. However, there are limited works on all of these three components that has been considered together. In this paper for the first time, the reverse converter design is done based on the final

modular adder of the arithmetic unit. It means that the final modular adder that has the same modulus as the modular adder in the beginning of the reverse converter is considered as a part of reverse converter instead of a part of arithmetic unit.

There are two common adders in computer arithmetic [1]: carry-propagate adder (CPA) and carry-save adder (CSA). The CSA has three input operands while CPA has two operands. Besides, CSA is faster and simpler than CPA adder that uses the complex parallel prefix structure to increase the speed. The issue of parallel prefix for increasing the speed has become more serious when it comes about the modular adder. However, CSA generates redundant output in the form of carry and sum binary vectors. It should be mentioned that the proposed technique can be only applied on the reverse converters that uses the new CRT-II [2] formula since only in this type of formula the modulo of adder in input of the converter can be the same as the modulo of one of the arithmetic unit modulus.

The main idea of this paper is that in RNS system for some modulus, if the modulo of the final modular adder of the arithmetic unit is the same as the modulo of modular adder that is in the beginning of the reverse converter, this adder can be eliminated and then the Carry and Sum signals are entered to the reverse converter where they are added by an extra CSA that is placed to converter. To explain the proposed method, the main formulas of [4] can be written as follows:

$$X = Z + 2^n(2^{2n+1} - 1)\left|2^n (Y - Z)\right|_{2^{2n}-1}; \quad (1)$$

$$Z = x_1 + 2^n\left|2^n (x_2 - x_1)\right|_{2^{2n+1}-1}; \quad (2)$$

$$Y = x_3 + (2^n + 1)\left|2^{n-1} (x_4 - x_3)\right|_{2^n-1}. \quad (3)$$

Where x_1, x_2, x_3 and x_4 are four residues in the moduli of $2^n, 2^{2n+1} - 1, 2^n + 1$, and $2^n - 1$,respectively. However, in a full RNS system these residues are resulted from a modular multiplication or addition operation where each of them has a modular adder as the final adder. For example, x_2 can be written as:

$$x_2 = \left|s_2 + c_2\right|_{2^{2n+1}-1}. \quad (4)$$

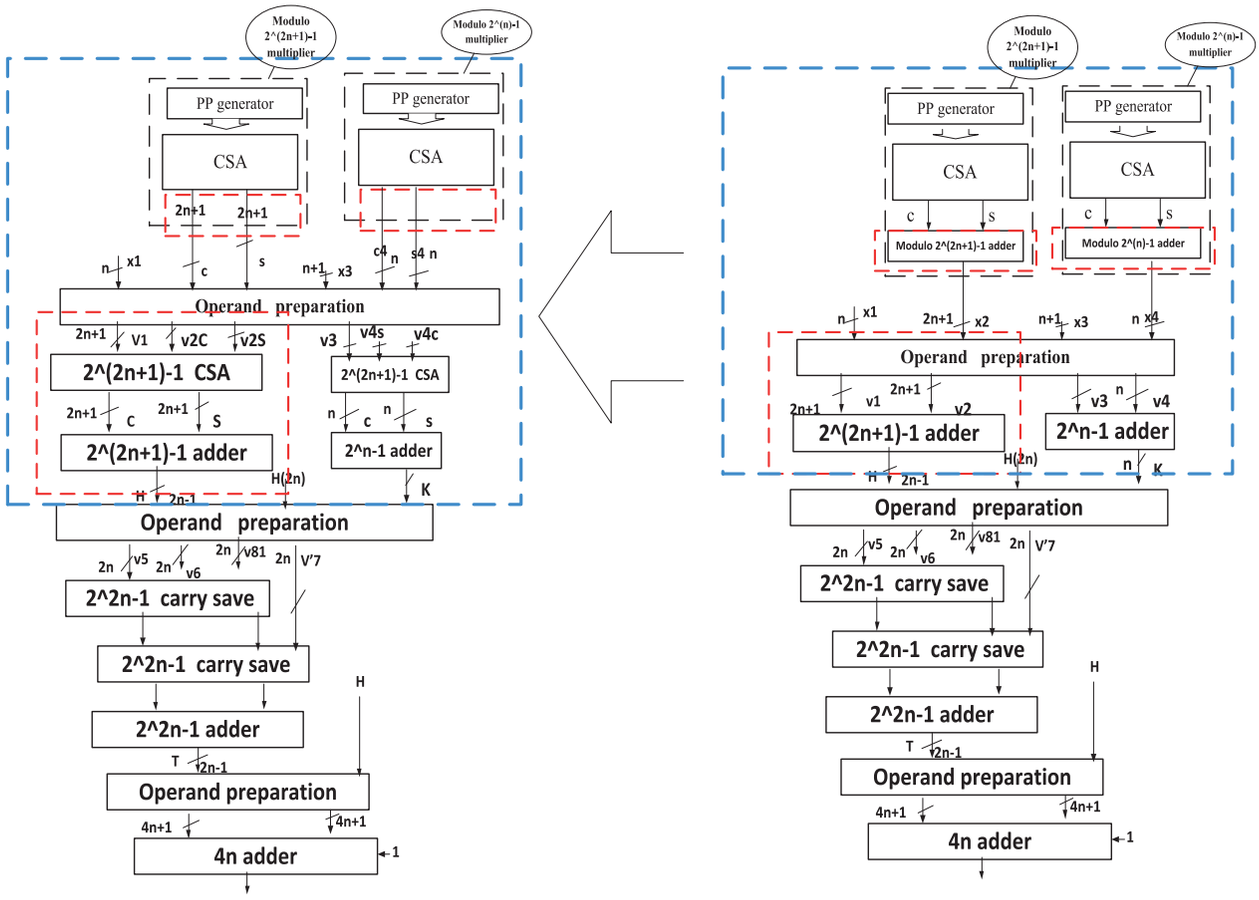

Fig. 1.The previous design including a maultiplier that is connected to a reverse converter in the right and, the new design that is consisted of a multiplier without the last modular adder, and a modified reverse converter in the left

Where, s_2 and c_2 are the redundant results of CSA addition of corresponding partial products. As it can be seen the conversion formulas in (1)-(3) are composed of two terms $2^n|2^n(x_2-x_1)|_{2^{2n+1}-1}$ and $(2^n+1)|2^{n-1}(x_4-x_3)|_{2^n-1}$.. In the term $2^n|2^n(x_2-x_1)|_{2^{2n+1}-1}$, the modulo of x_2 is the same as the result modulo 2^{2n+1}-1.

Therefore, as described before the term x_2 can be replaced by its equivalent from (4) and instead of two cascaded modular CPA additions, a CSA and a modular CPA addition can be performed. Hence, we have:

$$Z = x_1+2^n|2^n(|s_2+c_2|_{2^{2n+1}-1}-x_1)|_{2^{2n+1}-1}= x_1+2^n|2^n(s_2+c_2-x_2)|_{2^{2n+1}-1}. \quad (5)$$

If the residue x_4 is considered as (6), in the same way, *Y* can be written as (7):

$$x_4 = |s_4+c_4|_{2^n-1}; \quad (6)$$

$$Y = x_3+(2^n+1)|2^{n-1}(x_4-x_3)|_{2^n-1} = x_3+(2^n+1)|2^{n-1}(s_4+c_4-x_3)|_{2^n-1}. \quad (7)$$

Where s_4 and c_4 are the redundant results of a CSA. Fig.1 compares the presented method in the left with previous method in right. It can be seen in the proposed method that the modular adder in the end of multiplier is specified by a dotted rectangular shape. This adder can be eliminated as shown in Fig. 1. The outputs of these adders are x_2 and x_4 that are inserted to the converter, respectively. Instead of x_2 and x_4, the corresponding redundant CSA results (s, c) and (s_1, c_1) are entered directly to the converter.

Performance Evaluation

The proposed and previous designs are described in VHDL codes, synthesised and optimized by Synopsys Design Compiler. The 180-nm general-purpose standard cell library was used. Generally, the designs are divided in two groups: *i*) reverse converter of [4] plus modular adders in used its inputs and *ii*) the proposed reverse converter that eliminates the modular adder in input of reverse converts as described in before. For each group the following states were considered:

– full adder (FA) based CPAs is used in reverse converter and modular adder;

– parallel prefix based CPAs is used in reverse converter and modular adder.

Tables 1 and 2 give information about experimental results that have been achieved based on the different designs. The implementations were done for the three circuit parameters: delay, power consumption and area. It must be noted that the comparison was done between the proposed designs and [4].

Tables 3 and 4 show that the proposed method of shifting modular adder from arithmetic unit to the reverse converter results in significant improvement in delay and Energy (Power-Delay Product). For example, the speed up in the first state for n = 12 is more than 26% rather than the previous design. The proposed method has the best speed up when the FA-based CPA is used in adders. Besides, Tables 3 and 4 indicate the amount of PDP improvement of proposed customized adder plus reverse converter over previous design. For example, the PDP improvement has been about 22% for 10-bit in the state-2. Generally, two points can be extracted from experimental results:

– although, the power consumption is not improved in some cases, the gain obtained by speed up is so significant that totally makes the performance better and compensates the power consumption loss;

– the best PDP is related to the state-2 where all CPAs are parallel prefix. Therefore, the proposed method has the best PDP when parallel prefix is used.

In addition, as it was predictable, the efficiency of the proposed technique is contributed to the fact that the design area has been reduced by 13% for 12-bit in compare with the previous design for the state-1. This improvement can also be seen in all states that has been better at least more than 5%.

Table 1. Experimental results for proposed and previous design when FA-based CPAs is used in reverse converter and modular adder

n	Proposed design			Previous design		
	Delay (ns)	Area (um^2)	Power (mw)	Delay (ns)	Area (um^2)	Power (mw)
10	8.39	28962.	23.123	10.6	30935.	21.95
12	10.1	35582.	28.667	12.8	37701.	26.10

Table 2. Experimental results for proposed and previous design when Parallel prefix based CPAs is used in reverse converter and modular adder

n	Proposed design			Previous design		
	Delay (ns)	Area (um^2)	Power (mw)	Delay (ns)	Area (um^2)	Power (mw)
10	3.48	46283.	23.196	4.14	51469	23.127
12	3.68	57942.	28.703	4.51	61581	28.728

Table 3. The percentage of improvement (%) for proposed design over previous method for four parameters: delay, area, power consumption and PDP when FA-based CPAs is used in reverse converter and modular adder

n	Delay (%)	Area (%)	Power (%)	PDP (%)
10	25.73	5.95	–8.9438	14.49
12	26.91	6.26	–5.7	19.56

Table 4: The percentage of improvement (%) for proposed design over previous method for four parameters: delay, area, power consumption and PDP when Parallel prefix based CPAs is used in reverse converter and modular adder

n	Delay (%)	Area (%)	Power (%)	PDP (%)
10	22.55	6.28	0.0870	14.49
12	20.73	8.84	0.6149	21.47

As it can be seen the best performance for area is observed when the parallel prefix adder is used only in arithmetic unit.

Conclusion

In this paper, a new approach to design RNS systems has been introduced. This method is relied on the fact that the reverse converter design and arithmetic unit must be considered together not separately that is common in the previous methods. By taking the advantages of this view, the modular CPA of final arithmetic unit that is one of the main factors in increasing RNS overhead is replaced by a CSA. Experimental results show significant reduction in both speed and power consumption of RNS system that uses the proposed method.

References

1. Parhami B. *Computer Arithmetic: Algorithms and Hardware Design*. Oxford, U.K., Oxford Univ. Press, 2000.
2. Wang Y. Residue-to-binary converters based on new Chinese remainder theorems. *IEEE Trans. Circuits Syst. II, Analog. Digit. Signal Process*, 2000, vol. 47, no. 3, pp. 197-205. doi: 10.1109/82.826745.
3. Wang Y., Abd-el-barr M. A new algorithm for RNS decoding. *IEEE Trans. Circuits Syst. I*, 1996, vol. 43, pp. 998-1001. doi: 10.1109/81.545841.
4. Molahosseini A.S., Navi K., Dadkhah C., Kavehei O., Timarchi S. Efficient Reverse Converter Designs for the New 4-Moduli Sets $\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\}$ and $\{2^n-1, 2^n+1, 2^{2n}, 2^{2n}+1\}$ Based on New CRTs. *IEEE Transactions on Circuits and Systems-I*, 2010, vol. 57, no. 4, pp. 823-835. doi: 10.1109/TCSI.2009.2026681.
5. Patronik P., Piestrak S.J. Design of Reverse Converters for the New RNS Moduli Set $\{2^k, 2^n-1, 2^n+1, 2^{n+1}-1\}$ and $\{2^k, 2^n-1, 2^n+1, 2^{n-1}-1\}$ (odd). *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2014, vol. 61, no. 12, pp. 3436-3449. doi: 10.1109/TCSI.2014. 2337237.
6. Sousa L., Antão S.F. MRC-based RNS Reverse Converters for the Four-Moduli Sets $\{2^n+1, 2^n-1, 2^n, 2^{2n+1}-1\}$ and $\{2^n+1, 2^n-1, 2^{2n}, 2^{2n+1}-1\}$. *IEEE Transactions on Circuits and Systems-II*, 2012, vol. 59, no. 4, pp. 244-248. doi: 10.1109/TCSII.2012. 2188456.
7. Chokshi R., Berezowski K.S., Shrivastava A., Piestrak S. J. Exploiting Residue Number System

for Power-Efficient Digital SignalProcessing in Embedded Processors. *Proc. of 2009 International Conference on Compilers, Architecture, and Synthesis for Embedded Systems*, 2009, pp. 19-28. doi: 10.1145/1629395.1629401.

8. Kalampoukas L. et al. High-Speed Parallel-Prefix Modulo 2^n-1 Adders. *IEEE Trans. Computers*, 2000, vol. 49, no. 7, pp. 673-680. doi: 10.1109/12.863036.

Received 17.01.2017

Seyed Mostafa Mirhosseini, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, e-mail: s.m.mirhoseini@srbiau.ac.ir.

Amir Sabbagh Molahosseini, Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran, e-mail: sabbagh@iauk.ac.ir

Mehdi Hosseinzadeh, Iran University of Medical Sciences, Tehran, Iran; Computer Science, University of Human Development, Sulaimanyah, Iraq. E-mail: hosseinzadeh.m@Iums.ac.ir .

НОВЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Сейед Мостафа Мирхоссеини, Амир Саббаг Молахоссеини, Мехди Хоссеинзаде, Мехди Хоссеинзаде
E-mail: s.m.mirhoseini@srbiau.ac.ir

Система остаточных классов (СОК) рассматривается в качестве эффективного параллельного инструмента повышения производительности вычислительных систем. Однако СОК содержит некоторые компоненты, увеличивающие ее сложность. В данной статье предлагается новый подход к проектированию СОК, основанный на унификации последовательных сумматоров (ПС) в арифметических устройствах СОК для обратного преобразования. Предложенный метод исключает сложные модулярные ПС для некоторых каналов и улучшает существующие обратные преобразователи за счет перемещения некоторых сложных суммирований из арифметического канала СОК в обратный преобразователь. Экспериментальные результаты показывают существенное уменьшение аппаратных затрат, энергопотребления и задержки по сравнению с известными разработками.

Ключевые слова: система остаточных классов, вычислительная система, сумматор, обратное преобразование

Сейед Мостафа Мирхоссеини, Кафедра вычислительной техники (ВТ), научно-исследовательский отдел, Исламский университет Азад, Тегеран, Иран. E-mail: s.m.mirhoseini@srbiau.ac.ir

Амир Саббаг Молахоссеини, Кафедра ВТ, Исламский университет Азад, филиал в г. Керман, Иран. E-mail: sabbagh@iauk.ac.ir

Мехди Хоссеинзаде, Иранский медицинский университет, Тегеран, Иран; Университет развития человека, Сулейманья, Ирак. E-mail: hosseinzadeh.m@Iums.ac.ir

УДК 621.396.1

ОЦЕНКА КОЛИЧЕСТВА АНСАМБЛЕЙ НОВЫХ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ

Жук А.П., Белан Н.В., Карасев И.В., Луганская Л.А.
Северо-Кавказский федеральный университет, Ставрополь, РФ
E-mail: nadya_belan@mail.ru

В работе представлена методика оценки количества вариантов ансамблей многофазных ортогональных сигналов, получаемых при расчете собственных векторов для матрицы различных порядков. В результате сравнительного анализа количества предложенных ансамблей многофазных ортогональных сигналов и известных псевдослучайных хаотических последовательностей выявлено преимущество первых, что позволило сделать вывод о возможности их стохастического использования для передачи информации в радио- и оптическом каналах с целью повышения структурной скрытности сигналов-переносчиков информации.