INTEGRATION, the VLSI journal 55 (2016) 22–29

Contents lists available at ScienceDirect

INTEGRATION, the VLSI journal

journal homepage: www.elsevier.com/locate/vlsi

Method for designing two levels RNS reverse converters for large dynamic ranges

Hector Pettenghi [a,1,*], Ricardo Chaves [b,*], Roberto de Matos [c], Leonel Sousa [d]

[a] Department of Electrical and Electronic Engineering (CTC/UFSC) 88040 Florianópolis, Brazil
[b] INESC-ID, IST, Universidade de Lisboa, 1000-029 Lisbon, Portugal
[c] Department of Electrical and Electronic Engineering (CTC/UFSC) 88040 Florianópolis, Brazil
[d] INESC-ID, IST, Universidade de Lisboa, 1000-029 Lisbon, Portugal

ARTICLE INFO

Article history:
Received 21 September 2015
Received in revised form
23 February 2016
Accepted 23 February 2016
Available online 2 March 2016

Keywords:
Residue Number Systems
RNS-to-Binary converters
Adder-based converters

ABSTRACT

In the last years, research on Residue Number Systems (RNS) has targeted larger dynamic ranges in order to further explore their inherent parallelism. In this paper, we start from the traditional 3-moduli set $\{2^n, 2^n-1, 2^n+1\}$, with an equivalent $3n$-bit dynamic range, and propose horizontal and vertical extensions to scale the dynamic range and enhance the parallelism according to the requirements. Two different methods to design general reverse converters for extended moduli sets to the desired dynamic ranges are introduced. Previous converters require complex weight selection of the inputs or complex final conversion steps. In this work the weight selection of the multiplicative terms associated to the inputs is reduced to additions of $2n$-bit length and the final conversion step requires only one comparison. Experimental results suggest that the proposed approaches achieve significant area reductions, up to 61% lower area reductions, in comparison with the state-of-the-art for generic DR purposes. Despite having identical delay metrics as the existing generic state of the art, Area-Delay-Product efficiency metrics improvements up to 2.7 times can be achieved. The obtained results also validate the improved scalability of the proposed approaches, allowing for better results with the increase of n and the DR.

1. Introduction

Residue arithmetics, based on Residue Number Systems (RNS), have been in use in digital processing systems for many years [1]. RNS is a carry-free arithmetic system with modular characteristics offering the potential for high-speed and parallel computation. Arithmetic operations, such as addition, subtraction, and multiplication, can be carried out more efficiently than in the conventional binary systems [1], independently and concurrently, in several residue channels. The adoption of RNS has provided significant efficiency improvements for different types of Digital Signal Processing (DSP) applications [1], while allowing for an easier scaling for applications with larger dynamic ranges requirements, such as in adaptive filtering and cryptography [2].

The choice of the moduli set is of key importance in order to obtain balanced moduli sets. Moduli sets with a large number of channels can improve the arithmetic computation at the cost of reverse conversion performance.

With efficient reverse converters, capable of supporting large moduli sets, it is possible to compensate this extra cost, especially when several arithmetic operations have to be performed, such as in cryptographic or signal processing systems. In these cases the use of multiple arithmetic moduli channels can lead to better performance metrics.

To support these moduli sets, reverse converters need to be devised. Consequently, reverse conversion structures are usually presented whenever a novel moduli set is proposed. To devise these conversion structures the Chinese Remainder Theorem (CRT) [1], the mixed-radix conversion (MRC) [3] and the New CRT-I [4] algorithms are considered. Each of the moduli sets presented below have an associated conversion structure.

As mentioned before, in applications such as in cryptography [5], very large operands are used for. However, the level of parallelism and the achievable Dynamic Range (DR) provided by the traditional three-moduli set $\{2^n, \overbrace{2^n+1, 2^n-1}^{2^n \pm 1}\}$, with a DR of around $3n$-bit [6,7], are not enough.

[*] Corresponding author.
E-mail addresses: hector@eel.ufsc.br (H. Pettenghi), ricardo.chaves@inesc-id.pt (R. Chaves), roberto@eel.ufsc.br (R.d. Matos), las@inesc-id.pt (L. Sousa).
[1] Tel.: +55 48 3721 2359; fax: +55 48 3721 9280.

http://dx.doi.org/10.1016/j.vlsi.2016.02.004
0167-9260/© 2016 Elsevier B.V. All rights reserved.

In these cases, horizontal extensions can be used in order to add more moduli to the moduli set. This approach has been considered and proposed in the state-of-the-art, such as the four-moduli sets with a DR of about $4n$-bit: $\{2^n, 2^n \pm 1, \mathbf{2^{n+1}+1}\}$ and $\{2^n, 2^n \pm 1, \mathbf{2^{n+1}-1}\}$ [8,9], $\{2^n, 2^n \pm 1, \mathbf{2^{n-1}+1}\}$ and $\{2^n, 2^n \pm 1, \mathbf{2^{n-1}-1}\}$ [10]. Horizontal extensions of five-moduli sets with a DR of about $5n$-bit have also been proposed: $\{2^n, 2^n \pm 1, \mathbf{2^{n\pm 1}-1}\}$ [11], $\{2^{n+1}, 2^n \pm 1, \mathbf{2^{n+1} \pm 1}\}$ [12], and $\left\{2^n, 2^n \pm 1, \mathbf{2^n \pm 2^{\frac{(n+1)}{2}}+1}\right\}$ [13] that is composed of co-prime moduli for n odd and has been revisited by Hiasat in [14]. The moduli considered in [12] are co-prime numbers for n even, however, complex multiplicative inverses are required, resulting in expensive reverse conversion structures. In [15] the authors propose a full RNS using the 8 moduli set $\{2^{n-5}-1, 2^{n-3}-1, 2^{n-3}+1, 2^{n-2}+1, 2^{n-1}-1, 2^{n-1}+1, 2^n, 2^n+1\}$. The proposed moduli set is not regular, presenting channels with n to $n-5$ bits with non-co-prime moduli, resulting in a lower DR. As in [12], complex multiplicative inverses are required, resulting in costly and complicated hierarchical reverse converter structures. In addition, vertical extensions of channels have also been proposed in order to increase the DR, such as $\{\mathbf{2^{n+\beta}}, 2^n \pm 1\}$ [7], where $0 \le \beta \le n$ is used to increase the DR up to $4n$-bits with a 3-moduli set. This is achieved towards a more balanced moduli set, since the performance difference between the 2^n units and the $2^n \pm k$ arithmetic units. Therefore the overloading of the 2^n channel up to 2^{2n} can be done without affecting the delay in the arithmetic channels.

Moduli sets with both vertically and horizontally extensions have also been recently proposed $\{\mathbf{2^{2n}}, 2^n \pm 1, \mathbf{2^{2n+1}-1}\}$ [16], $\{\mathbf{2^{2n}}, 2^n \pm 1, \mathbf{2^{2n}+1}\}$ [17], and $\left\{\mathbf{2^{n+\beta}}, 2^n \pm 1, \mathbf{2^n} \pm 2^{\frac{n+1}{2}}+1, \mathbf{2^{n+1}+1}\right\}$ and $\left\{\mathbf{2^{n+\beta}}, 2^n \pm 1, \mathbf{2^n \pm 2^{\frac{n+1}{2}}+1}, \mathbf{2^{n-1}+1}\right\}$ with $-\frac{(n-1)}{2} \le \beta \le 3n$ [18]. The proposals [16,17] provide a DR of $\simeq$ $6n$-bits at a cost of unbalancing the moduli set. In contrast, the proposal [18] provides a more balanced moduli set with a maximum DR of $(8n+1)$-bit.

In the paper [19] a method based on New CRT-I for designing RNS reverse converter that uses generic hybrid extended moduli sets of the form $\{\mathbf{2^{n+\beta}}, 2^n \pm 1, \mathbf{2^n \pm k_1}, \mathbf{2^n \pm k_2}, \ldots, \mathbf{2^n \pm k_f}\}$ is presented, with k_j being odd values and $0 \le \beta \le n$. However, this method imposes a complex modular weight selection of the multiplicative terms, V_{ji}, associated to the residue inputs R_i, which is a substantial drawback. Moreover, the modular addition of these weighted inputs requires a large number of comparisons, and consequently a dedicated circuitry is used in the architecture to reduce the complexity of the Final Conversion step (FC). In this work a method is proposed to accommodate the generic moduli set horizontal and vertical extended presented in [19], by reducing the modular values used as the multiplicative terms, V_{ji}, and requiring only a single comparison in the final conversion operation.

The remaining of this paper is organized as follows. A novel method to design reverse converters to the extended moduli sets is presented in Section 2, and an additional technique that minimizes the number of required levels is presented in Section 3. A performance analysis of a case study is presented in Section 4. The efficiency of the state-of-the-art of reverse converters with large DRs is compared with the one achieved with our proposals, in Section 5. Section 6 concludes this paper with some final remarks.

2. Multi-level hybrid extensions of the three-moduli set $\{2^n, 2^n \pm 1\}$

To simplify the presentation of the method and the description of the architectures, the following notation is adopted [14]: (i) the symbol $*$ operates the concatenation of the binary representation of two numbers, and (ii) R_i denotes the residue for m_i.

The dynamic range is equal to the product of the N moduli of a defined set $\left(M = \prod_{i=1}^{N} m_i\right)$, $\hat{m}_i = M/m_i$, and $\left|\hat{m}_i^{-1}\right|_{m_i}$ represents the multiplicative inverse of $\hat{m}_i$ with respect to modulus m_i. A value represented in RNS can be converted back to binary (X) using the CRT [1]:

$$X = \left|\sum_{i=1}^{N} \hat{m}_i \left|\hat{m}_i^{-1}\right|_{m_i} R_i\right|_M = \sum_{i=1}^{N} \hat{m}_i \left|\hat{m}_i^{-1}\right|_{m_i} R_i - MA(X), \tag{1}$$

where $A(X)$ is an integer that depends on the value of X.

As stated above, herein both horizontal and vertical extensions are considered. For the vertical extension the power of two modulus is extended, towards a more balanced moduli set, since the power of two modulus typically allows for more efficient arithmetic operations than the remaining moduli sets for the same word length [18]. This leads to the moduli $\{\mathbf{2^{n+\beta}}, 2^n \pm 1\}$, with $0 \le \beta \le n$, covering DRs up to $(4n)$-bits [7].

In order to achieve arbitrarily wider moduli sets, horizontal moduli set extensions are herein considered by the addition of conjugate moduli pairs to the above moduli set in the same way as [19]. These conjugate moduli pairs are of the form $2^n \pm k_j$, $0 \le j \le f$, with k_j being an odd value in the range $1 \le k_j < 2^{n-1}$ [20] chosen in such a way that all moduli are co-prime with each other. With this, moduli sets of the form $\{\mathbf{2^{n+\beta}}, \mathbf{2^n \pm k_f}, \ldots, \mathbf{2^n \pm k_1}, \mathbf{2^n \pm k_0}\}$ are obtained, with a DR around $(1+\frac{\beta}{n}+2 \times (f+1)) \times n$-bit, for any integer n.

The values of k_j can be chosen in order to obtain the highest possible DR, however a cost function can be used to obtain the most balanced moduli sets and minimizing the number of "1"s in the representation of k_j in order to derive more efficient architectures, such as the ones presented in the following. It should noted that the proposed method can also be used to derive reverse converters for moduli sets with non-conjugate moduli pairs. Herein, we only detail moduli sets with conjugate moduli pairs to simplify the explanation.

In order to illustrate the proposed moduli set extensions, we first derive the extension for the moduli set with $f=1$ and $k_0=1$, resulting in the moduli set $\{\mathbf{2^{n+\beta}}, \mathbf{2^n \pm k_1}, 2^n \pm 1\}$. Following, the derivation and discussion of the limitations of extending the moduli set with conjugate moduli pairs for different f values is also presented.

2.1. Moduli set $\{\mathbf{2^{n+\beta}}, \mathbf{2^n \pm k_1}, 2^n \pm 1\}$

As presented above, let us consider the value $0 \le \beta \le n$. From now on, the values of the moduli sets are ordered in a decreasing order, excluding the 2^n+1 and 2^n-1 (placed in the before-last and last positions), resulting in $m_1 = 2^{n+\beta}$, $m_2 = 2^n + k_1$, $m_3 = 2^n - k_1$, and $m_4 = 2^n + 1$, $m_5 = 2^n - 1$, whereas $\hat{m}_1 = 2^{4n} - 2^{2n}(k_1^2+1) + k_1^2$, $\hat{m}_2 = 2^{n+\beta}(2^{2n}-1)(2^n - k_1)$, $\hat{m}_3 = 2^{n+\beta}(2^{2n}-1)(2^n + k_1)$, $\hat{m}_4 = 2^{n+\beta}(2^n - 1)(2^{2n} - k_1^2)$, and $\hat{m}_5 = 2^{n+\beta}(2^n+1)(2^{2n} - k_1^2)$.

For the proposed extension the following expression $\hat{\hat{m}}_i$ is used:

$$\hat{\hat{m}}_i = \frac{M}{\prod_{j=1}^{i} m_j} \quad \text{with } 1 \le i \le 5. \tag{2}$$

The chosen k_1 needs to satisfy that the resulting moduli set $\{\mathbf{2^{n+\beta}}, \mathbf{2^n \pm k_1}, 2^n \pm 1\}$ is composed of co-prime numbers. For example, $k_1 = 3$ satisfies this condition for $n \ge 3$.

The values of the multiplicative inverses are integer numbers, which can be obtained by applying the condition $\left|(\hat{m}_i)(\hat{m}_i^{-1})\right|_{m_i} = 1$, $1 \le i \le 5$ [14].