POZNAN UNIVERSITY OF TECHNOLOGY ACADEMIC JOURNALS
No Electrical Engineering 2012

Zenon ULMAN, Maciej CZYŻAK, Robert SMYK
Gdansk University of Technology

FPGA IMPLEMENTATION OF REVERSE RESIDUE CONVERSION BASED ON THE NEW CHINESE REMAINDER THEOREM II- Part I

This work describes a derivation and an implementation of the algorithm of conversion from the Residue Number System (*RNS*) to the binary system based on the new form of the Chinese Remainder Theorem (*CRT*) termed the *New CRT II*. This form of the *CRT* does not require the modulo M operation, where M is the residue number system range, but a certain number of multipliers is needed. Because in the FPGA environments the multipliers or the special DSP blocks are available, so they can be used in the converter realization. The aim of the work is to examine experimentally the needed hardware amount and the influence of the multipliers on the maximum pipelining frequency operation. In Part I the derivation of the conversion algorithm is described.

1. INTRODUCTION

The Residue Number System (*RNS*) was proposed in 1957[1] by Svoboda and 1958 by Svoboda and Valach [2] and was later described in [3],[4],[5]. The foundations of the residue system were established nearly 2000 years ago in ancient China, when an approach to computations in residue arithmetic was introduced that evolved later into the Chinese Remainder Theorem finally formulated by Euler in 1736. The primary goal of this system was the devising of the mathematical tool that could be used for the design of more reliable subsystems of early computers. The other aim was fast realization of arithmetic operations. Because of its advantages, the residue arithmetic is competitive in comparison to the binary arithmetic in specific applications that make use of the advantages of this arithmetic. The residue arithmetic has been successfully used in application areas such as *FFT* processors, *FIR* filters, digital image processing, telecomunication, calculation of correlation and many others which require large number of multiplications and additions. The most important advantage of the residue arithmetic is the carry-free and parallel realization of addition, subtraction and multiplication in several small integer rings instead of in one large integer ring. The other are the fault tolerance and modularity. The latter is especially important because it allows to design fine-grained systems in which the higher pipelining rates can be attained. However, there are also difficult operations such as sign detection, scaling, division and reverse conversion (Residue-to-Binary Conversion, *RNS/B*). Several algorithms of conversion have been presented in the literature [6-12]. The known algorithms are based on the *CRT* or Mixed Radix System (*MRS*) and require modulo *M* operation or the realization of the *MRS* process. Wang [13] proposed two new algorithms for increasing parallelism and speed for conversion of numbers from the *RNS* to the binary system (*RNS/B* conversion, reverse conversion). These algorithms allow to avoid modulo *M* operation. Wang has called these algorithms the *New CRT I* and *NewCRT II*.

This part of the work work presents the algorithm of the *RNS/B* conversion based on the *New CRT II*. In Section 2 a short review of the *RNS* is given. In Section 3 the *MRS* is reviewed. In Section 4 the *RNS/B* conversion based on the *New CRT II* is derived. In Section 5 the numerical example of the *RNS/B* conversion by the *New CRT II* is given.

2. RESIDUE NUMBER SYSTEM

The number *X* is represented in the *RNS* as the *n*-tuple $(x_n, x_{n-1}, \ldots, x_1)$, where x_i, *i*=1,2,...,*n*, are the residues of *X*, with respect to the set of numbers termed the *RNS* base $B = \{m_n, m_{n-1}, \ldots, m_1\}$. For the given RNS representation, the number *X* can be determined by using the Chinese Remainder Theorem

$$X = \left|\sum_{j=1}^{n} X_j\right|_M = \sum_{j=1}^{n} X_j - k \cdot M, \tag{1}$$

where $X_j = M_j \cdot \left|M_j^{-1} \cdot x_j\right|_{m_j}$, $j = 1, 2, \ldots, n$, $M = \prod_{j=1}^{n} m_j$, $M_j = M / m_j$, $\left|M_j \cdot M_j^{-1}\right|_{m_j} = 1$. The multiplicative inverse $\left|M_j^{-1}\right|_{m_j}$ exists always when $\gcd(M_j, m_j) = 1$. As the alternative conversion techniques may serve the *MRS* and core function [10]. The main important property of the *RNS* is the possibility of performing addition, subtraction and multiplication on the individual digits without carries between the digits.

3. MIXED-RADIX SYSTEM (MRS) ASSOCIATED TO THE BASE B WITH THE RNS

Using the same base *B* as for the *RNS*, the number X can be represented in the weighted system, associated with the *RNS*, the mixed-radix system as follows:

$$X = \sum_{j=1}^{n} a_j w_j = a_1 + a_2 m_1 + a_3 m_1 m_2 + \ldots + a_n m_1 m_2 \ldots m_{n-1}, \qquad (2)$$

where the weights $w_j = \prod_{i=1}^{j-1} m_i$ for $2 \le j < n$, $w_1 = 1$. The digits are calculated as $a_j = \left|Y_j\right|_{m_j}$, where $Y_j = (Y_{j-1} - a_{j-1}) / m_{j-1}$, $Y_1 = X$.

It is known [1], that calculation of the *MRS* digits can be performed using the residue arithmetic but the *RNS/B* conversion process is immannently sequential and requires *n* computational steps. The sequence of the moduli in the individual weights is arbitrary, therefore the number of the *MRSs* with various weights constructed with use of the same base *B* is equal to the number of permutations of the moduli in the base *B*.

For example, for the *RNS* constructed with the use of two moduli $\{m_1, m_2\}$ every number X in a range of $[0, m_1 m_2)$ can be represented by a vector (x_1, x_2). In the *MRS* formulated in terms of the base $\{m_1, m_2\}$, the number *X* can be determined in two ways:

$$X = \left|X\right|_{m_1 m_2} = a'_1 + a'_2\, m_1, \qquad (3a)$$

or

$$X = \left|X\right|_{m_2 m_1} = a''_1 + a''_2\, m_2, \qquad (3b)$$

where $a'_1 = x_1$, $a'_2 = \left|(x_2 - x_1)\cdot \frac{1}{m_1}\right|_{m_2}$, $a''_1 = x_2$, $a''_2 = \left|(x_2 - x_1)\cdot \frac{1}{m_2}\right|_{m_1}$.

The multiplicative inverses modulo m_2, $\left|\frac{1}{m_1}\right|_{m_2} = \left|m_1^{-1}\right|_{m_2}$ and modulo m_1, $\left|m_2^{-1}\right|_{m_1}$ always exist, because $\gcd(m_1, m_2) = 1$. The above remark can be generalized. For two numbers M_1 and M_2 taken from a disjoint subsets of the base *B*, for example, $M_1 = \prod_{j=1}^{k} m_j$ and $M_2 = \prod_{j=k+1}^{n} m_j$, their multiplicative inverses $\left|M_1^{-1}\right|_{M_2}$ and $\left|M_2^{-1}\right|_{M_1}$ always exist because $\gcd(M_1, M_2) = 1$.

4. THE RNS/B CONVERSION BASED ON NEW CRT II

Let be given a base *B* consisting of *n* moduli with *n* even. The number X from range $[0, M-1]$ is represented by the vector of residues

$$(x_1, x_2, \ldots, x_n) \qquad (4)$$

The *RNS/B* algorithm based on the *New CRT II* can be represented as follows:

1. Take an arbitrary pair of residues from the vector of residues $(x_1, x_2, \ldots, x_n)$, for example (x_1, x_2). This pair represents any number $|X|_{m_1 m_2}$ in the *RNS* with a base $\{m_1, m_2\}$. This number can be represented in the *MRS* using (3) in the following manner

$$|X|_{m_2 m_1} = a''_1 + a''_2 = x_2 + \left|(x_1 - x_2) m_2^{-1}\right|_{m_1} \cdot m_2. \tag{5}$$

The multiplicative inverse $\left|m_2^{-1}\right|_{m_1}$ exists and can be calculated before conversion. The number $|X|_{m_2 m_1}$ can be represented in the binary using (3). In order to obtain the representation of X as $(|X|_{m_1 m_2}, |X|_{m_3 m_4}, \ldots, |X|_{m_{n-1} m_n})$ in *n*-moduli *RNS*, the calculations for the remaining $n/2-1$ pairs of the residues of the vector $(x_1, x_2, \ldots, x_n)$ must be performed.

2. Take an arbitrary pair of the residues from vector (4), for example $\left(|X|_{m_1 m_2}, |X|_{m_3 m_4}\right)$, and using (3) calculate $|X|_{m_1 m_2 m_3 m_4}$, repeat this for the remaining pairs from the vector and get the binary representation of $|X|_{m_1 m_2 m_3 m_4}$.

3. From the vector of residues $(|X|_{m_1 m_2 m_3 m_4}, \ldots, |X|_{m_n m_{n-1} m_{n-2} m_{n-3}})$ take an arbitrary pair of residues and repeat the procedure of the calculation of the corresponding number in the binary system.

The algorithm terminates, when by the above procedure, $|X|_M$ will be represented in the *RNS* by two residues $(|X|_{M_1}, |X|_{M_2})$, where $M_1 = \prod_{j=1}^{k} m_j$, $M_2 = \prod_{j=k+1}^{n} m_j$. Next using (3), we obtain $X = |X|_M = |X|_{M_2} + \left|(|X|_{M_1} - |X|_{M_2}) \cdot M_2^{-1}\right| \cdot M_2$, and hence the value of X can be easily calculated in the binary system.

The *New CRT II* differs from the classical *CRT*, due to the gradually reduction of the number of residues in the residue representation of the number X and in effect allows to obtain the binary representation of *X*. Finally, the operation requires only reduction by the modulus M_1 instead of M, where $M_1 < \sqrt{M}$ if $M_1 < M_2$. All the multiplicative inverses required for conversion do not depend upon the value of X and can be precalculated before the conversion.

5. THE EXAMPLE OF THE RNS/B CONVERSION

Example 1. Conversion *RNS/B* with the use of the *New CRT II.*

Assume $B = \{11, 13, 15, 16\}$, then $M = 34320$. Moreover, assume $34319 = X \leftrightarrow (10, 12, 14, 15)$.

The *RNS/B* conversion can be carried out as follows:
First the multiplicative inverses $\left|m_2^{-1}\right|_{m_1}$, $\left|m_4^{-1}\right|_{m_3}$ and $\left|M_2^{-1}\right|_{M_1}$ have to be determined. Hence by solving equations $\left|m_2^{-1} \cdot m_2\right|_{m_1}$=1, $\left|m_4^{-1} \cdot m_4\right|_{m_3} = 1$ and $\left|M_2^{-1} \cdot M_2\right|_{M_1}$, we receive $\left|m_2^{-1}\right|_{m_1} = 6$, $\left|m_4^{-1}\right|_{m_3} = 1$ and $\left|M_2^{-1}\right|_{M_1} = 115$, respectively.We can now perform the conversion process.

$$x_{1,2} = x_2 + \left|\left|m_2^{-1}\right|_{m_1} \cdot (x_2 - x_1)\right|_{m_1} \cdot m_2 = 12 + \left|6 \cdot (10 - 12) + 11\right|_{11} \cdot 13 = 142$$

$$x_{3,4} = x_4 + \left|\left|m_4^{-1}\right|_{m_3} \cdot (x_3 - x_4)\right|_{m_1} \cdot m_4 = 15 + \left|1 \cdot (14 - 15) + 15\right|_{15} \cdot 16 = 239$$

$$x_{1,2,3,4} = x_{3,4} + \left|\left|M_2^{-1}\right|_{M_1} \cdot (x_{1,2} - x_{3,4})\right|_{m_1} \cdot M_2 =$$

$$= 239 + \left|115 \cdot (142 - 239 + 143)\right|_{143} \cdot 240 = 34319$$

6. CONCLUSION

This contribution presents the systematic derivation of the *RNS/B* algorithm based on the *New CRT II*. The main advatange of the algorithm is the possibility of avoiding modulo *M* operation, where *M* is the number range of the *RNS*. The range of the modulo operation can be approximately reduced to $\sqrt{M}$. In Part II the implementation of the converter in the *FPGA* environment is presented.

REFERENCES

[1] A. Svoboda, "Rational numerical system of residual classes", Stroje na Zpracovani Informaci, Sbornik V, Nakl. CSAV, s.9-37, Praha 1957.

[2] A. Svoboda, M. Valach,. The numerical system of residual classes in mathematical machines, Proc. Congr. Int. Automa, 1958.

[3] N.S. Szabo and R.J. Tanaka, *Residue Arithmetic and its Applications to Computer Technology*, New York, McGraw-Hill, 1967.

[4] M .Soderstrand *et al*., *Residue Number System Arithmetic*: Modern Applications in Digital Signal Processing, IEEE Press, NY, 1986.

[5] A. Omondi, B. Premkumar, *Residue Number Systems: Theory and Implementation,* London*,* Imperial College Press, 2007.

[6] S.J.Piestrak, Design of residue generators and multioperand modulo adders using carry-save adders, IEEE Trans. Comp., Vol. 43, Jan. 1994, pp. 68-77.

[7] K.M. Elleithy , M.A. Bayoumi, Fast and flexible architectures for RNS arithmetic decoding, IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing, Vol. 39, no. 4, April 1992, pp.226-235.

[8] Z. Wang Z., G.A. Jullien , W.C. Miller , An Improved Residue-To-Binary Converter, IEEE Trans. Circuits Syst.-I: Fundamental Theory and Applications, Vol 47, September 2000, pp. 1437-1440.

[9] S.J. Meehan, S.D. O'Neil , J.J. Vaccaro , An Universal Input And Output Converter, IEEE Trans. Circuit Syst., Vol. CAS-37, June 1990, pp. 1158-1162.

[10] N. Burgess, Scaled And Unscaled Residue Number System To Binary Conversion Techniques Using The Core Function, 1997 IEEE Symposium on Computer Arithmetic, pp. 250-257.

[11] G.C. Cardarilli , M. Re , R. Lojacono , A Systolic Architecture For High Performance Scaled Residue To Binary Conversion, IEEE Trans. Circuits Syst. –I: Fundamental Theory And Applications, Vol. 47, October 2000, pp.667-669.

[12] M.Czyżak, An improved high-speed residue-to-binary converter based on the Chinese Remainder Theorem, Pomiary Automatyka Kontrola, Vol.53, no.4, April 2007, pp.72-75.

[13] Y. Wang, Residue-to-binary Converters Based On the new Chinese Remainder Theorems, IEEE Trans. Circuits and Systems-II: Analog and Digital Signal Processing, Vl. 47, No. 4, September 2000, pp.197-205.