NEW NON-COPRIME CONJUGATE-PAIR BINARY TO RNS MULTI-MODULI FOR RESIDUE NUMBER SYSTEM

Mansour Bader[1], Andraws Swidan[2], Mazin Al-hadidi[1]

[1]Department of Computer Engineering,
Al-Balqa'a Applied University, Salt, Jordan.
[2]Department of Computer Engineering,
Jordan University, Amman, Jordan.

ABSTRACT

In this paper a new Binary-to-RNS converters for multi-moduli RNS based on conjugate-pair as of the set { $2^{n1} - 2$, $2^{n1} + 2$, $2^{n2} - 2$, $2^{n2} + 2$, …, $2^{nN} - 2$, $2^{nN} + 2$ } are presented. $2^{n} - 2$ and $2^{n} + 2$ modulies are called conjugates of each other. Benefits of Multi-moduli RNS processors are; relying on the sets with pairs of conjugate moduli : 1) Large dynamic ranges. 2) Fast and balanced RNS arithmetic. 3) Simple and efficient RNS processing hardware. 4) Efficient weighted-to-RNS and RNS-to-Weighted converters. [1] The dynamic range (M) achieved by the set above is defined by the least common multiple (LCM) of the moduli. This new non-coprime conjugate-pair is unique and the only one of its shape as to be shown.

KEYWORDS

Binary , Conjugate-Pair , Dynamic range, LCM, Multi-moduli.

1. INTRODUCTION

RNS is known to support parallel, carry-free, high-speed arithmetic , because it is considered as an integer system, that is appropriate for implementing fast digital signal processors [1] . It is also has main importance in Encryption and Cryptography fields. Other applications include – but not limited to - Digital Signal Processing, correlation, error detection and correction [1 - 3].

RNS basis form is a set of relatively prime integers P = { m1, ….., mk } where gcd (mi, mj) = 1 for $i \neq j$. In this paper we are showing that the new non-coprime moduli set presented in [2] could be used in the new non-coprime multi-moduli conjugate-pair Weighted-to-RNS converters.

The set P for prime case is the moduli set with the dynamic range (M) of the system $M = \pi$ mi. But for our case and since each conjugate has the number 2 as a common factor other than the number 1 as in the prime one, the $M = \prod_{1}^{k} \mathrm{mi} \,/\, 2^{\wedge}(k-1)$.

For both cases coprime and non-coprime; any integer x€ [0, M – 1] has an RNS representation X = (x1 , … , xk), where xi = X mod mi .

Dhinaharan Nagamalai et al. (Eds) : CoSIT, SIGL, AIAPP, CYBI, CRIS, SEC, DMA - 2017
pp. 105– 111, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70411

The new thing we come up with here is working with a full non-prime moduli set (i.e. for this case) gcd (mi, mj) $\neq$ 1 for $i \neq j$ (1)

RNS systems based on non coprime moduli have also been studied in literature [2] –[5].

Although as discussed in [2] that non-coprime has little studies upon, we still have strong sense that it deserves to work on.

The rest of this paper is organized as follows. In Section 2, overview of the new Non-coprime multi moduli is proposed. Section 3 presents the realization of the proposed forward converter of the new non-coprime conjugate-pair multi-moduli , while the paper is concluded in Section 4.

2. OVERVIEW OF NEW NON-COPRIME MULTI –MODULI

Since almost all previous work stated that [1][3][5] " The basis for an RNS is a set of relatively prime integers; that is :

$$S = \{ q_1, q_2, \dots , q_L \}, \text{ where } (q_i , q_j) = 1 \text{ for } i \neq j \tag{2}$$

with (qi , qj) indicating the greatest common divisor of qi and qj .

The set S is the moduli set while the dynamic range of the system (i.e. M) is the product Q of the moduli qi in the set S. Any integer X belonging to ZQ = { 0, 1 2, ... , Q -1 } has an RNS representation" .

$$X \xrightarrow{\text{RNS}} (X_1, X_2, \dots , X_L) \tag{3}$$

$$X_i = < X >_{qi} , \quad i = 1, 2, ... , L \tag{4}$$

Where $<X>_q$ is X mod q.

For our case of **non-coprime** , equation number 4 becomes :

$$X_i = < X >_{qi} , \quad i = 2, 3, ... , L \tag{5}$$

For both cases (i.e. Coprime and Non-coprime), if X, Y have RNS representations { X1, ….., XM}, { Y1, … , YM}, the RNS representation of W = X * Y (* denotes addition, subtraction or multiplication) is

$$W \xrightarrow{\text{RNS}} \{ W1, \dots , WM \}; Wi = < Xi * Yi > qi, i = 1, \dots , L \tag{6}$$

Another thing to notice here is that our new proposed non-coprime conjugate-pair multi-moduli set is also conjugate even by dividing it by the common factor among its moduli (i.e. number 2 in this case), the shape is to be discussed in another paper. However it has the following form :

$\{ 2^{n1-1} - 1, 2^{n1-1} + 1, 2^{n2-1} - 1, 2^{n2-1} + 1, \ldots, 2^{nN-1} - 1, 2^{nN-1} + 1 \}$.

The proposed Non-coprime multi-moduli set form is :

$S = \{ 2^{n1} - 2, 2^{n1} + 2, 2^{n2} - 2, 2^{n2} + 2, \ldots, 2^{nN} - 2, 2^{nN} + 2 \}$.

It is clear that each conjugate-pair on the numbers line is 4 spaces apart. As discussed in [2] it was shown that having the shape of the new non-coprime moduli set (i.e. $\{ 2^n - 2, 2^n , 2^n + 2 \}$) being 4 spaces apart from each other helped in the Forward conversion process (FC) of the moduli. The same space for our new non-coprime multi-moduli is useful indeed.

Lets take an example to show what is meant by the spaces above.

Ex.$_1$ Let n1 = 3 , n2 = 4 for the set S.

Then the set S = { 6, 10, 14, 18 }.

Numbers (6 , 10) and (14 , 18) are 4 spaces from each other on the numbers line. This is true for any value taken for { n1, n2 … , nN }, notice that n1 < n2 < … < nN ; n1 >= 2.

This is need for the management process to prepare the multi-moduli in good shape.

Least Common Multiple (LCM) is must be used for the non-coprime case, since there is a common factor among the modulus numbers.

3. NEW NON-COPRIME MULTI-MODULI PROPOSED FORWARD CONVERTER

This section is preferred to be divided into two sections in order to show simply how it works. Then from the multi-moduli shape provided it is generalized for size of (N).

In the first section, we are going to take N = 2, thus the multi-moduli would consist of 4 modulus values. The second sub-section we are having N = 3, so there would be 6 modulus inside the multi-moduli set. Forward conversion (i.e. Binary to RNS) is to be implemented for each case.

3.1 VALUES SET OF 4-MODULUS

The multi-moduli set will be of the form, when we take N = 2 :

$S = \{ 2^{n1} - 2, 2^{n1} + 2, 2^{n2} - 2, 2^{n2} + 2 \}$.

If we take as the first example showed n1 = 3 , n2 = 4 . The shape of the set was :

S1 = { 6, 10, 14, 18 }.

M (i.e. Dynamic Range of the set) is calculated through the LCM. For the set S1 it is equal to

$6 * 10 * 14 * 18 / 2^{L-1}$, where L = the size of the set. (7)

For this case L = 4, so M = 1890 .

That means any number in the range [0 – 1889] has a unique representation among the proposed set. This dynamic range is larger than the range for { $2^{n1} - 2$, 2^{n1} , $2^{n1} + 2$ } which equals 120. i.e. 1890 >> 120.

It is also having a larger range than the set { $2^{n2} - 2$, 2^{n2} , $2^{n2} + 2$ } which has M = 1008. i.e. 1890 > 1008.

This is due we are working with 4-moduli set rather than 3-moduli set, and by neglecting the middle modulus (i.e. 2^n) and having the conjugate of n1 , n2 instead. Mathematically it could be shown as :

M1 = 6 * 8 *10 / 4 , M2 = 14 * 16 * 18 / 4 while M3 = 6 * 10 * 14 * 18 / 8 .

Take for M2 case, as it has larger numbers than M1, 16 / 4 < 6 * 10 / 8 **or** by having 6 * 10 / 2 = 30, 30 > 16 when comparing them divided 4 (i.e. having a common base of comparison).

The conversion process works as the follow, each modulus having the shape $2^n - 2$ goes to Converter number 1, while the $2^n + 2$ goes to Converter number 2 that works in parallel.

Converter 1 does its work just as figure 1 in [2] showed, figure 2 in the same paper shows converter 2 work.

Hardware implementation for each case is shown in figures 3, 5 of [2].

3.2 VALUE SET OF 6-MODULUS

When we take N = 3, then the multi-moduli set will be on the form :

S = { $2^{n1} - 2$, $2^{n1} + 2$, $2^{n2} - 2$, $2^{n2} + 2$, $2^{n3} - 2$, $2^{n3} + 2$ }.

If we take n1 = 3 , n2 = 4 and n3 = 5 for simplicity. The shape of the set is :

S2 = { 6, 10, 14, 18, 30 , 34 }.

M (i.e. Dynamic Range of the set) is calculated through the LCM. For the set S2 it is equal to

$6 * 10 * 14 * 18 * 30 * 34 / 2^{L-1}$, where L = the size of the set. (8)

For this case L = 6, so M = 481950.

That means any number in the range [0 – 481949] has a unique representation among the proposed set. This dynamic range is larger than the range for { $2^{n1} - 2, 2^{n1}, 2^{n1} + 2$ } which equals 120.

i.e. 481950 >> 120.

It is also having a very large range than the set { $2^{n2} - 2, 2^{n2}, 2^{n2} + 2$ } which has M = 1008.

i.e. 481950>> 1008.

Finally it has larger range than the set { $2^{n3} - 2, 2^{n3}, 2^{n3} + 2$ } which has M = 8160.

i.e. 481950>> 8160.

This is due we are working with 6-moduli set rather than 3-moduli set for each case, and by neglecting the middle modulus (i.e. 2^n) and having the conjugate of n1 , n2 and n3 instead.

Mathematically it could be shown as :

M1 = 6 * 8 *10 / 4 , M2 = 14 * 16 * 18 / 4 , M3 = 30 * 32 * 34 / 4 while

M4 = 6 * 10 * 14 * 18 * 30 * 34 / 32 .

Take for M3 case, as it has the largest numbers than M1 and M2, 32 / 4 < 6 * 10 * 14 * 18 / 32 **or** by having 6 * 10 * 14 * 18 / 8 = 1890, 1890 > > 16 when comparing them divided 4 (i.e. having a common base of comparison).

The conversion process works as the follow, each modulus having the shape $2^n - 2$ goes to Converter number 1, while the $2^n + 2$ goes to Converter number 2 that both works in parallel.

Converter 1 does its work just as figure 1 in [2] showed, figure 2 in the same paper shows converter 2 work.

Hardware implementation for each case is shown in figures 3, 5 of [2].

4. CONCLUSIONS

A new non-coprime multi-moduli set has been proposed. A general formula for the dynamic range of it was derived. Algorithm of the special non-coprime multi-moduli set has been suggested. Also a new mathematical algorithm for the new non-coprime multi-set has been proposed.

This research revealed that non-coprime moduli set may be suitable for wide variety of cases not limited to co-prime only (i.e. Conjugate in multi-moduli).

ACKNOWLEDGEMENTS

The author would like to thank everyone.

REFERENCES

[1] A. Skavantzos ; Y. Wang, "New efficient RNS-to-weighted decoders for conjugate-pair-moduli residue number systems", IEEE Conference Record of the Thirty-Third Asilomar Conference on Signals, Systems, and Computers, 1999..

[2] Mansour Bader, Andraws Swidan, Mazin Al-Hadidi and Baha Rababah, "A binary to residue conversion using new proposed non-coprime moduli set", Signal & Image Processing : An International Journal (SIPIJ) Vol.7, No.3, June 2016 .

[3] A. Skavantzos ; Yuke Wang, "Application of new Chinese Remainder Theorems to RNS with two pairs of conjugate moduli", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM 1999). Conference Proceedings, 1999.

[4] M. Abdallah, A. Skavantzos, "On the binary quadratic residue system with non coprirne moduli", IEEE Trans. On Signal Processing, vol. 45, no. 8, pp. 2085-2091, Aug. 1997.

[5] Y. Wang, "New Chinese Remainder Theorems", Proceedings of the Thirty Second Asilomar Conference on Signals Systems and Computers, pp. 165-171, 1998-Nov.

[6] A. Skavantzos, M. Abdallah, "Implementation Issues of the Two-Level Residue Number System with Pairs of Conjugate Moduli", IEEE Trans. On Signal Processing, vol. 47, no. 3, pp. 826-838, March 1999.

[7] A. Skavantzos, M. Abdallah, "Novel Residue Arithmetic Processors for High Speed Digital Signal Processing", Proceedings of the Thirty Second Asilomar Conference on Signals Systems arid Computers, pp. 187-193, 1998-Nov.

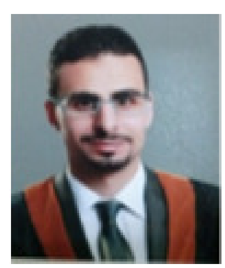
[8] A. Skavantzos ; T. Stouraitis, "Grouped-moduli residue number systems for fast signal processing", IEEE International Symposium on Circuits and Systems, 1999. ISCAS '99.

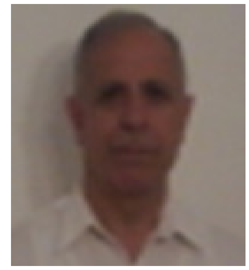
[9] R. Katti, "A new residue arithmetic error correction scheme", IEEE Transactions on Computers, vol. 45, no. 1, January 1996.

[10] Y. Wang, M. N. Swamy, O. Ahmad, "Three number moduli sets based residue number systems", 1998 IEEE International Symposium on Circuits and Systems, 1998.

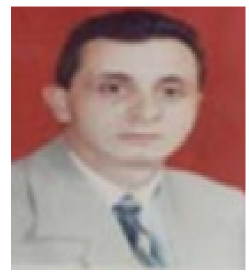
AUTHORS

Mansour Bader holds a MSc in computer engineering and networks, University of Jordan, Jordan, 2016. BSc Computer Engineering, Al-Balqa Applied University, Jordan, 2008. He is a technical support engineer of computer networks at computer center of Al-Balqa Applied University for 8 years and a half.





Dr. Andraws I. Swidan was born in Al-Karak Jordan in 1954. He received his diploma in Computer Engineering (with honours) and Ph.D. in Computer Engineering from LETI Ulianov Lenin, Sanct Peterburg (Leningrad), Russia in 1979 and 1982 respectively. He Joined the Electrical Engineering Department at the University of Jordan in 1983 and was one of the founders of the Computer Engineering Department at the University of Jordan in 1999. Since then he is a professor at the department. He is also an Adjunct Professor with the ECE department of the McGill University, Montreal, Canada. He holds several technical certifications among which the CISSP. He is an IEEE member, Jordanian Engineering Association member Quebec College of engineers member. He is a Canada Professional Engineer (The province of Quebec). He was member of several national and international scientific committees. He holds several patents and tens of publications. His main areas of research interest are: computer arithmetic, computer security, encryption algorithms.



Mazin Al-hadidi has PhD. in Engineering Science (Computing Machines, Systems and Networks), Institute of Problems of Simulation in Power Engineering Academy of Science, Ukraine/Kiev .1990-1994, with grade Excellent. Bachelor and Master Degrees in Engineering (Computer and intellectual systems and networks) Kiev Institute of Civil Aviation Engineers, as a governmental scholarship, Soviet Union / Kiev, 1984-1990, with grade very good. General Secondary 12 Years Certificate in the Science branch, Jordan/Al-Salt, 1984, with grade very good.