

An improved RNS generator $2^n \pm k$ based on threshold logic

Abstract— This paper proposes a new scheme for designing residue generators using threshold logic, which is derived on the basis of the periodicity of the series of powers of 2 taken modulo $2^n \pm k$. In addition, a new algorithm is presented for obtaining a new set of partition which take advantages in terms of area and delay in the topology presented. Experimental results in the analized range of k and n show that new proposed circuits using the novel partition are 71% faster and provide area savings of 84%, when compared with similar circuits using the partitioning methods presented to date.

Keywords- generator modulo A , residue number systems, binary-to residue number systems converter, threshold logic.

I. INTRODUCTION

Residue arithmetic has been used in digital computing systems for many years [1]. The modular characteristic of the Residue Number System (*RNS*) offers the potential for high-speed and parallel arithmetic. *RNS* is a carry-free arithmetic system that improves the computation performance, and exhibits more parallelism and smaller area [1-2]. Arithmetic operations, e.g. addition, subtraction, and multiplication can be carried out on residue digits independently and concurrently more efficiently than the conventional two's complement systems [1]. *RNS* has shown significant efficiency in implementing different types of Digital Signal Processing (*DSP*) applications, such as filtering [3], FFT computation [4], fault-tolerant computer systems [5], communication [6], and cryptography [7].

Whatever the application, *RNS* uses a number of residue generators which forms binary-to-residue converters [1,8-10]. However, residue converters can compromise the speed of the whole system. The most well-known *RNS* moduli set is formed by three-moduli *RNS* $\{2^n - k, 2^n, 2^n + k\}$ with $k = 1$. This moduli set has attracted attention since it is well suited for effective regular *VLSI* implementations [11] and very efficient combinational converters from/to the binary system exist [12]. Different moduli sets have been proposed for the direct/reverse conversion to increase the parallelism and the dynamic range to $m = 4n$, for example $\{2^n \pm 1, 2^n \pm 3\}$ [13], and $\{2^n \pm 1, 2^{2n}\}$ [14]. In addition, another four moduli set can be derived $\{2^n + k_1, 2^n + k_2, 2^n + k_3, 2^n + k_4\}$ with k_1, k_2, k_3 and k_4

positive/negative odd numbers or zero, chosen in such a way that a valid group of co-prime numbers is obtained [8]. The generators $2^n \pm k$ with k odd and $k \geq 3$ are more complex than the ones with $k = 1$. However, some applications of this sorts of residue generators to the field of *DSP* have been proposed in [5], [15]. At the present, one of the most efficient generator mod $2^n \pm k$ are implemented using the periodic properties of powers of two [15]. This paper uses a quite different approach based on the concept of threshold gate [16], in comparison with the traditional approaches, to build any moduli set with an appropriate dinamic range. In order to build the generator mod $2^n \pm k$ the periodic properties of the powers of two modulo $2^n \pm k$, $|2^j|_A$ is used.

Herein improved designs for residue generators mod A based on threshold logic are proposed. This paper is organized as follows. Section II presents the topology based on threshold gates and the parameters which define them. Section III introduces the mathematical groundwork for the periodicity of the series powers of 2 carried out by mod A . In addition, a new efficient algorithm to compute the periodicity of any A is proposed. Section IV details the proposed general design. Section V presents a complexity analysis, in terms of delay and area, of the obtained circuits which are completed with the experimental results of Section VI. A summary of the work proposed is presented in Section VII.

II. GENERATOR MOD A

An n -input Boolean function $f(x_{m-1}, \dots, x_1, x_0)$, which can be defined by $(n+1)$ real numbers (threshold T and weights w_{m-1}, \dots, w_1, w_0 , where weight w_i is associated with variable x_i) in such a way that:

$$f(x_{m-1}, \dots, x_1, x_0) = \begin{cases} 1 & \text{iff } \left(\sum_{i=0}^{m-1} w_i x_i \geq T \right) \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where $x_i \in [0, 1]$ and the multiplication and summation are arithmetic rather logic operations, is called a threshold function.

In a generator mod A with m input , $\{x_{m-1}, \dots, x_1, x_0\}$ and a outputs represented as a set of residues $\{s_{a-1}, \dots, s_1, s_0\}$, where $a = \lceil \log_2 A \rceil$. The generator converts an integer $X = \sum_{j=0}^{m-1} 2^j x_j$ into $|X|_A = \sum_{j=0}^{a-1} 2^j s_j$, i.e., it computes:

$$|X|_A = \left| \sum_{j=0}^{m-1} 2^j x_j \right|_A \quad (2)$$

The direct division of X by A to find the remainder is an inefficient solution. The technique proposed in [1] give us an improved algorithm based on the expression:

$$|X|_A = \left| \sum_{j=0}^{m-1} \left| 2^j \right|_A x_j \right|_A = \sum_{i=0}^{a-1} 2^i s_i \quad (3)$$

If the values of $|2^j|_A$ are directly available, $|X|_A$ can be computed by merely adding mod A these terms $|2^j|_A$ for which $x_j = 1$. In addition, these functions are periodic functions and so they can be implemented [16] by using separate TG networks.

Figure 1 shows an efficient topology to implement a residue generator mod A in a single TG network [17]. The threshold gate network has m inputs $\{x_{m-1}, \dots, x_1, x_0\}$ with associated weights $\{|2^{m-1}|_A, \dots, |2^1|_A, |2^0|_A\}$, represented on the left side of each threshold gate, which provides the sequences of residues. The value of the threshold, T , is showed in the lower right corner of each gate. Lets define the summatory of the sequence of residues as:

$$S = \left| \sum_{j=0}^{m-1} |2^j|_A \right|, \quad (4)$$

which has a size of bits of $t = \lfloor \log_2(S) \rfloor$. The value of $S = Q \cdot A + R$, provides the the quotient Q , $Q = \lfloor S/A \rfloor$. The $(r+1)$ bit binary number $[S_{a+r}, \dots, S_{a+1}, S_a]$, where

$$r = \lfloor \log_2(Q) \rfloor, \quad (5)$$

represents the quotient Q , and the a-bit number $[S_{a-1}, \dots, S_1, S_0]$ is the binary representation of the remainder R . In terms of delay, the division operation is implemented in

$$L = (\lceil \log_2 A \rceil + \lfloor \log_2(Q) \rfloor) \quad (6)$$

levels by using also L threshold gates. In terms of area, the main contribution of hardware is not given by the weights of the inputs but by the exponential increase of the weights associated to the quotient output, $2^r A$. This topology presents an unfeasible power-delay trade-off for a large values of r . Therefore, a more efficient scheme which reduces the value of the quotient is required. The proposal scheme is based on the periodic properties of powers of two mod A .

III. PERIODIC PROPERTIES OF $|2^j|_A$

The periodicity of the series of $|2^j|_A$ [15] will be of key importance for designing new generators mod A .

A. Generator Mod A based on the $P(A)$ concept

This sort of generator is based on the adapted definition of period of the odd module A $P(A)$ [18] which is described as follows:

- *Definition 1:* The period of the odd module A $P(A)$ is the minimum distance between two distinct 1's in the sequence of residues of powers of 2 taken mod A , i.e $P(A) = \min\{j \mid j > 0 \text{ and } |2^j|_A = 1\}$. $P(A)$ is simply called the *period of A* [15].

B. Generator Mod A based on the $HP(A)$ concept

This sort of generator is based on the adapted definition of half-period of the odd module A $HP(A)$ [18] which is described as follows:

- *Definition 2:* The half-period of the odd module A $HP(A)$ is the minimum distance between a pair of subsequent 1 and $A-1$ in the sequence of residues of powers of 2 taken mod A . (Note that $A-1 \bmod A \equiv -1$).

Whereas $P(A)$ exists for any A , $HP(A)$ exists for some A only. $HP(A)$ is called a half-period because if it exists then $P(A) = 2 \cdot HP(A)$. Several rules between them are derived in [15] given a generalization of the concept widely used in the case of $k = -1$. This concept sets that

$$|2^{za}|_{2^a+k} = 1, z \text{ nonnegative integer and } k = -1, \quad (7)$$

and with the concept of $P(A)$ is derived that

$$|2^{zP(A)+j}|_A = |2^j|_A, z \text{ nonnegative integer}, \quad (8)$$

similarly with the concept of $HP(A)$ is derived that

$$|2^{zHP(A)+j}|_A = (-1)^z \cdot |2^j|_A, z \text{ nonnegative integer}. \quad (9)$$

C. Generator Mod A based on a novel algorithm

Realising on the possibility of using positive and negative residues in the sequence of powers of two (as in the $HP(A)$ case) a new algorithm is presented here. This algorithm reduces the weight of the residue values to obtain a minimal weighted contribution at the final summatory of the sequence of residues, see at (4). This summatory is maximum when all inputs are logic ones $S = S_{\max}$.

In this way we compare two values of residue $|2^j|_A = b_j$ (positive value of the residue) and $|2^j|_A = b_j - A$ (the negative value), given both esentially the correct residue number, the first in range $[0, +A)$ and the second one in $(-A, 0]$. The

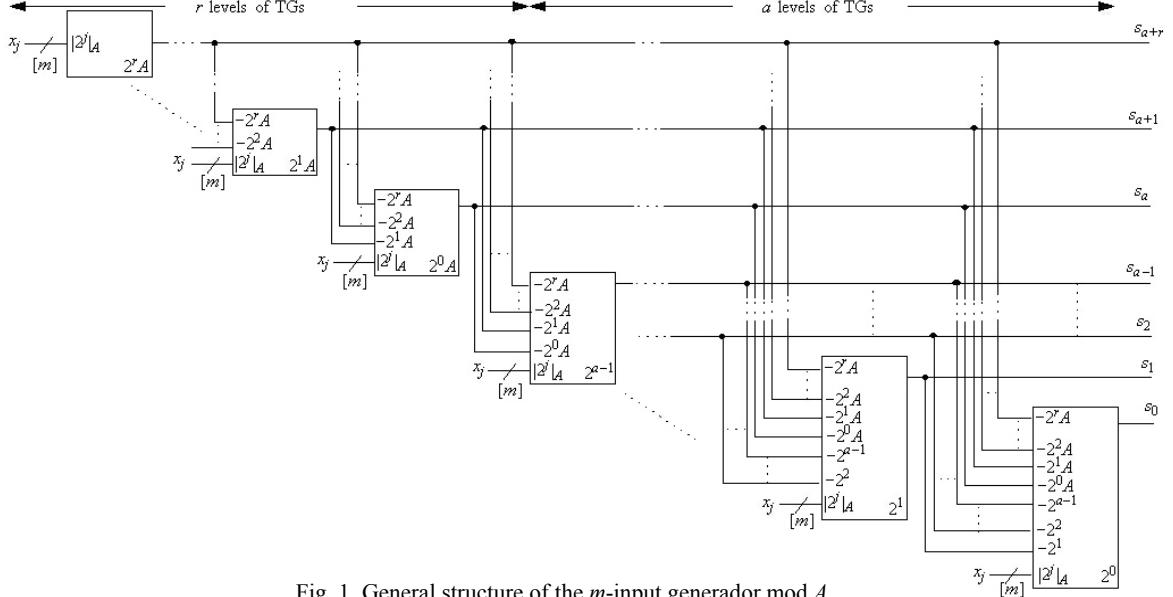


Fig. 1. General structure of the m -input generator mod A .

minimum value of residues, denoted by v_j in the range $(-(A-1)/2, +(A-1)/2)$, are obtained choosing the lesser between $|b_j|$ or $|b_j - A|$, i.e. iff $|b_j| > (A-1)/2$, $v_j = |b_j - A|$ and $v_j = |b_j|$ otherwise. Taking into account this idea, a novel algorithm is described realising that:

$$|2^{j+1}|_A = |2 \cdot v_j|_A \quad (10)$$

and applying (10) recursively we can derived the new algorithm (algorihtm 1). Note that, with algorithm 1, the set of partitions can be derived easily without any residue computation. Up to now, to obtain the set of partitions the calculation of each $|2^j|_A$ was needed. However, with this novel algorithm, cases presented in [15] can be derived without any residue calculation. Different cases to obtain the residue sequence have been denoted as: case 1, case 2 and case 3 if they are $P(A)$ based, $HP(A)$ based, and based on a minimal summatory of contributions, respectively. For example, to pass from case 3 to case 1 it is only needed to add to Algorithm 1 the lines 11 to 18. In addition, to pass from case 1 to case 2 lines 19 to 28 needed to be added.

As values of $|2^j|_A$ are always less than A , weights associated with primary inputs in the TG network are drastically reduced from 2^j to $|2^j|_A$, $j = 0, \dots, m-1$. So, the set of input variables $\{x_{m-1}, \dots, x_1, x_0\}$ can be partitioned into Γ_i sets, where $\Gamma_i = \{x_q \mid |2^q|_A = i\}$, and $-(A-1) \leq i \leq A-1$. In addition, the sets are fitted into $0 \leq i \leq A-1$, $-A+1 < i < A-1$, $-\lfloor A/2 \rfloor + 1 \leq i \leq \lfloor A/2 \rfloor - 1$ in case 1, 2 and 3 respectively.

Algorithm 1 to obtain an array of residue values $\{v_{m-1}, \dots, v_1, v_0\}$ with a minimal cost function in S_{\max}

```

1: for  $j = 1 : m$ 
2:    $v_1 = 1 \& v_{j+1} = 2 \cdot v_j$  ;
3:   if  $v_{j+1} > \lceil A/2 \rceil$ 
4:      $v_{j+1} = 2 \cdot v_j - A$  ;
5:   elseif  $v_{j+1} < -\lceil A/2 \rceil$ 
6:      $v_{j+1} = 2 \cdot v_j + A$  ;
7:   else
8:      $v_{j+1} = 2 \cdot v_j$  ;
9:   end
10: end
11: for  $j = 1 : m$ 
12:   if  $v_j < 0$ 
13:      $b_j = v_j + A$  ;
14:   else
15:      $b_j = v_j$  ;
16:   end
17: end
18: for  $j = 1 : m$ 
19:   if  $b_j == A-1$ 
20:     for  $i = j : (\lceil A/2 \rceil - 1) + j$ 
21:        $b_j = b_i - A$  ;
22:     end
23:   else
24:      $b_j = b_j$  ;
25:   end
26: end

```

↑
Case 1
↓

↑
Case 1
↓

↑
Case 2
↓

IV. DESIGN PROCEDURE

In this section, we present a new scheme of the m -input generator mod A based on threshold gates for the three different ways of partitioning presented in the previous section. The new generator mod A can be design by using the following procedure.

Step 1: Obtaining the sequence of residues for m bits by means of the proposed algorithm.

Step 2: Standardize the range of the ouput of the residue generator to form the Γ_i sets in a positive range $0 \leq i \leq A-1$ as is in case 1. In cases 2 and 3 the residue generator output without any correction is in a range positive and negative. In [15] is proposed the addition of a correction term to obtain a typical range $0 \leq i \leq A-1$ in case 2. The correction value COR is chosen as the minimum value that satisfies

$$\left| \sum_{j \in v_j < 0} \bar{b}_j + COR \right|_A = 0.$$

From [15] is derived that:

$$S = \sum_{j=0}^{m-1} |b_j| + COR \quad (11)$$

$$|X|_A = \left| \sum_{j \in b_j > 0} b_j + \sum_{j \in b_j < 0} \bar{b}_j + COR \right|_A \quad (12)$$

Is important to clarify that the COR factor in case 3 is obtained in the same way only replacing b_j by v_j . From now on and due to the COR is a constant, the correction factor is added to the threshold value of each TG of the residue generator.

Step 3: Once the sequence is defined and corrected we make the partition of the set of input bits $\{x_{m-1}, \dots, x_1, x_0\}$ onto Γ_i sets finishing the preparatory steps.

Step 4: The last step consist in calculating the value of r , which depends of the maximum summatory of all residue contributions $S_{\max} = \sum_{j=0}^{m-1} |2^j|_A + COR$ as is showed in (5).

Example 1: Figure 2 shows the average performance of the quotient (Q), for the new residue generator proposed for each value of n in the range of k odd numbers $\in [-7, +7]$. The analysis is carried out for three different ways of separating the partitions (cases 1, 2, and the proposed case 3). As seen Figure 2, a significant reduction in the value of Q is achieved with the proposed algorithm providing advantages in terms of area and delay.

Example 2: Design of the 20-bits new generator mod 37 with three different cases of separation of the partitions. Figures 3a, 3b, and 3c depict the description of the topology for cases 1, 2, and 3 respectively.

Case 1: The number of partitions is $P(37) = 36$. In this case the addition of COR is not needed, since there are no partitions with negative weights. The partition in this

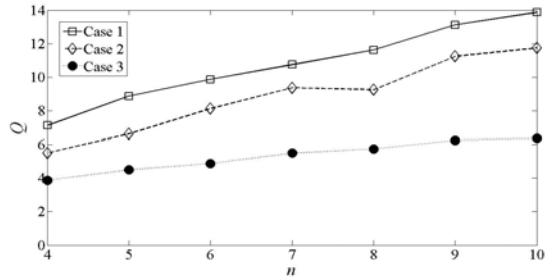


Fig. 2. Average of Q for $2^n \pm k$, k odd numbers $\in [-7, +7]$.

case is $\Gamma_1 = \{x_0\}$, $\Gamma_2 = \{x_1\}$, ..., $\Gamma_{35} = \{x_{19}\}$ so the addition of COR to the thresholds, is not needed. Consequently, the maximum summation is $S_{\max} = \sum_{j=0}^{19} |2^j|_{37} = 402$. The maximum value of the quotient is $Q = \lfloor 402/37 \rfloor = 10$ and $r = 3$.

Case 2: In this case $20 > HP(37)$ since $HP(37) = 18$. In this case exists a correction factor $COR = 34$ obtained by $|3 + COR|_A = 0$. In this case 34 is added to all thresholds in each TG. The resulting partition are $\Gamma_1 = \{x_0, \bar{x}_{18}\}$, $\Gamma_2 = \{x_1, \bar{x}_{19}\}$, $\Gamma_4 = \{x_2\}$, ..., $\Gamma_{18} = \{x_{17}\}$. Therefore, the maximum summation is $S_{\max} = \sum_{j=0}^{19} |2^j|_{37}| + COR = 368$. The value of the quotient is $Q = \lfloor 368/37 \rfloor = 9$ and $r = 3$.

Case 3: A correction factor, $COR = 3$, is also required, obtained by $|71 + COR|_A = 0$, which is added to all thresholds in each TG. The partition in this case is $\Gamma_1 = \{x_0, \bar{x}_{18}\}$, $\Gamma_2 = \{x_1, \bar{x}_{19}\}$, $\Gamma_4 = \{x_2\}$, ..., $\Gamma_{18} = \{x_{17}\}$. The maximum summation is $S_{\max} = \sum_{j=0}^{19} |2^j|_{37}| + COR = 177$. The quotient is $Q = \lfloor 177/37 \rfloor = 4$ with a word lenght of $r = 2$.

Figure 3 shows that in terms of delay there are benefits in the topology using the proposed way of partitioning in comparison with the traditional ways presented in [15]. \square

V. COMPLEXITY ESTIMATION AND COMPARISON

The improved efficiency of the proposed residue generators mod A is achieved by the use of the proposed way of partitioning, which reduces the number of comparisons required. The novel residue generator mod A based on the proposed algorithm (case 3) is compared with cases 1 and 2, reported in [15]. All the designs were designed following the procedure described and proposed in Section III. In order to obtain a reliable comparison of area and delay between them, the implementation used to build the threshold gates needed to be selected. The β -driven [19] approach has been chosen.

A. Delay Estimation

The delay requirements of the topologies have been estimated in terms of threshold gates. To properly estimate the

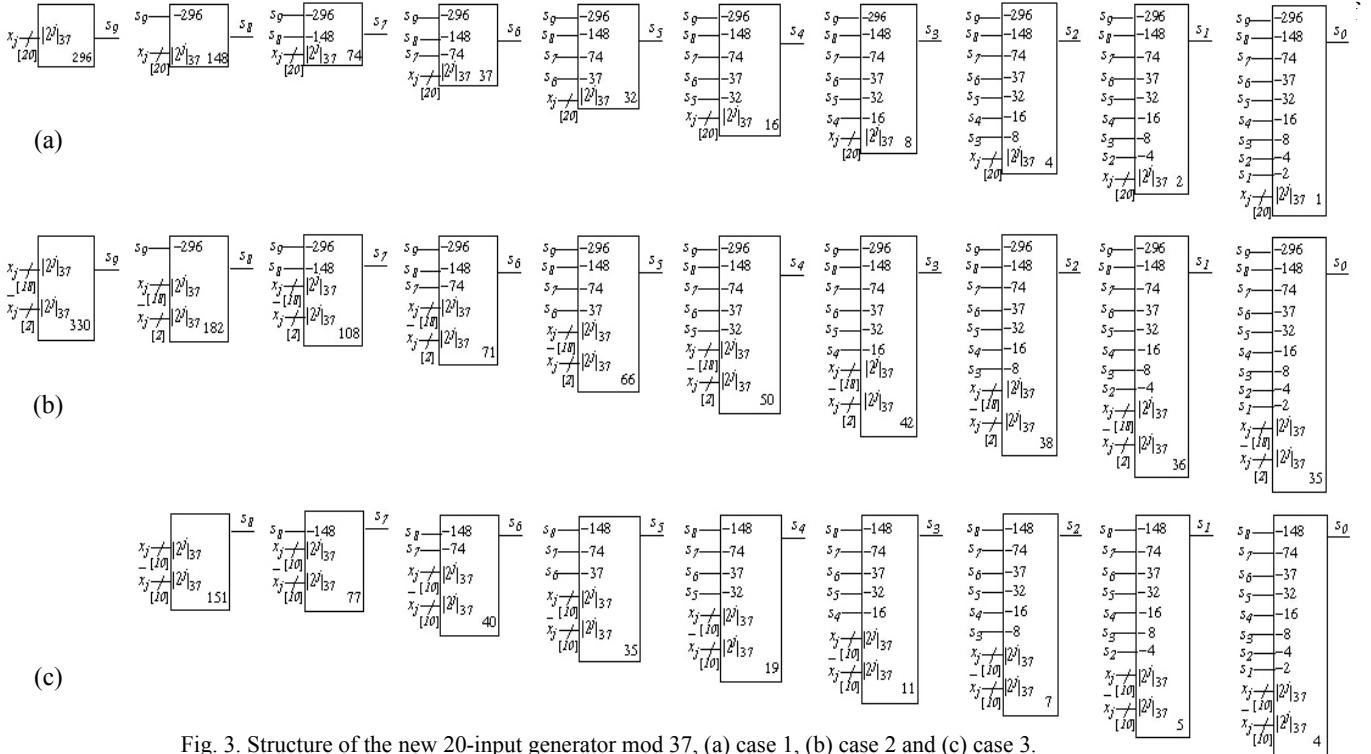


Fig. 3. Structure of the new 20-input generator mod 37, (a) case 1, (b) case 2 and (c) case 3.

delay, we only need to analyze the depth of the stages which provides the value of the quotient, Q , and the residue, R . The first stage of TGs has a depth of r , whereas the second one has a depth of a , as is showed in Figure 1. Thus, delay estimation giving by the overall levels of threshold gates.

$$\text{Delay} = a + r \quad (13)$$

Figure 4a depicts the delay performance, in threshold gate levels for the new residue generator. These values reflect the average results for the several k odd numbers $\in [-7, +7]$, for each n . It is noticeable that the topology of case 3 is faster than the other cases, resulting in a delay reduction of at least 6%.

B. Area Estimation

Let us consider the transistor-input area with an associated weight equal to 1 as the area unit used for this estimation. In our approach, an input x_j with an associated weight $|2^j|_A$ imposes an increase of area transistor of $|2^j|_A$ in comparison with an input with an associated weight equal to 1. Therefore, the measure of the area is carried out as the summation of all weighted contribution for each TG. With this, the overall estimation of area for the topology is:

$$\begin{aligned} \text{Area} &= (2^0 + 2^1 + \dots + 2^r) \cdot A \cdot a + S \cdot (a + r) + \dots \\ &\dots + (2^r \cdot (r-1) + 2^{r-1} \cdot (r-2) + \dots + 2^2) \end{aligned} \quad (14)$$

Figure 4b depicts the average area values, in terms of weighted contributions of inputs for each TG. As above, the average

odd $k \in [-7, +7]$. The obtained estimation suggests a significant area reduction for the topology using the proposed partitioning in comparison with the related art [15]. Thus, area reductions of at least 42%, are expected. The area estimation results indicate an exponential increase with n , for all three cases, giving an unfeasible power-delay trade-off for large values of n .

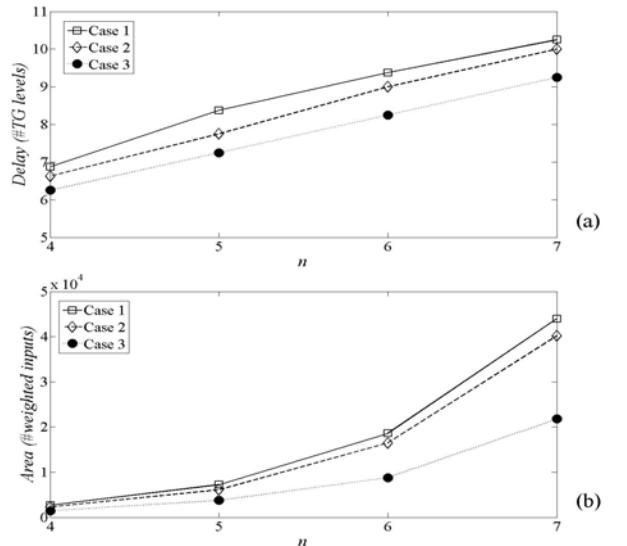


Fig. 4. Average comparisons for $2^n \pm k$, being k odd numbers $\in [-7, +7]$, (a) delay and (b) area.

VI. EXPERIMENTAL RESULTS

In order to evaluate the performance of the proposed residue generators experimental results were also obtained and compared. The topologies have been simulated in CADENCE using $0.13\mu\text{m}$ Standard technology from UMC. Simulations of gates for the β -driven approach with this technology have proven that the fan-in is limited to small values of weighted inputs. Note that the technology used is not optimized for the design of threshold gates. Nevertheless, experimental results for residue generators with 16 input bits with presented topology have been obtained and compared.

Fig. 5 shows the relative differences from the obtained experimental results, regarding area and delay of residue generators modulo $2^4 + k$ for case 2 and 3 in comparison with case 1. The proposed topology with the novel method of partitioning exhibits equal or better area-delay trade-off in comparison with the traditional ways of partitioning presented in [15]. For example, in the particular case of residue generator mod 19, $(2^4 + 3)$, the improvements of area and delay are over 70% when comparing topology 3 with topologies 1 and 2.

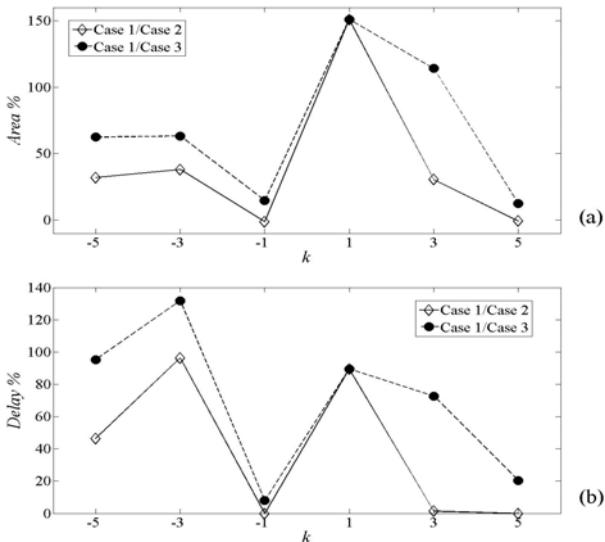


Fig. 5. Experimental results for three cases, (a) area, (b) delay.

VII. CONCLUSIONS

Novel methods to realize residue generators modulo $2^n \pm k$, for threshold logic are presented for any n and k . The threshold logic approach take advantages of the periodic properties of the powers of two modulo $2^n \pm k$. The new scheme reduces the hardware cost in comparison with traditional implementations by means of threshold gates. First, a novel algorithm, which exploits the periodic properties of the series of powers of 2 taken from modulo $2^n \pm k$, provides us with the sequences of residues in a more efficient way when compared with the existing state of the art. With this simpler algorithm, all the design can be derived for any value of n and k . Three different ways to separate the partitions are compared with the new

topology, two of them already reported and a novel one herein proposed. The new idea of separation shows to be advantageous in terms of area and delay confirmed by both the theoretical analysis and the experimental results. These results suggest that improvements up to 84% in area and 71% in delay can be achieved.

REFERENCES

- [1] N.S. Szabo and R.I. Tanaka, Residue Arithmetic and its Applications to Computer Technology, McGraw-Hill, New York, 1967.
- [2] Garner, "The residue number system", *IRE Trans. Electronic Computer*, vol. EC-8, pp.140-147, Jun.1959.
- [3] G.C. Cardarilli, et al., "Reducing power dissipation in FIR filters using the residue number system", *IEEE Proc. Midwest Symp. on Circuits and Syst.*, pp. 320-323, 2000.
- [4] P. G. Fernandez, et al., "A RNS-Based Matrix-Vector-Multiply FCT Architecture for DCT Computation," *Proc. 43th IEEE Midwest Symposium on Circuits and Systems*, pp. 350-353, 2000.
- [5] S. J. Piestrak, "Self-testing checkers for arithmetic codes with any check base A," in *Proc. 1991 Pacific Rim Int. Symp. Fault-Tolerant Syst.*, Kawasaki, Japan, Sept. 2627, 1991, pp. 162-167.
- [6] J. Ramirez, et al., "Fast RNS FPL-Based Communications Receiver Design and Implementation," *Proc. 12th Int. Conf. Field Programmable Logic*, pp. 472-481, 2002.
- [7] J. Bajard, and L. Imbert, "A Full RNS Implementation of RSA," *IEEE Transactions on Computers*, vol. 53, no. 6, pp. 769-774, Jun 2004.
- [8] M. A. Soderstrand et al., Eds., Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. New York: IEEE Press, 1986.
- [9] W. K. Jenkins and B. J. Leon, "The use of residue number system in the design of finite impulse response filters," *IEEE Trans. Circuits Syst.*, vol. CAS-24, pp. 191-201, Apr. 1977.
- [10] R. M. Capocelli and R. Giancarlo, "Efficient VLSI networks for converting an integer from binary system to residue number system and vice versa," *IEEE Trans. Circuits Syst.*, vol. CAS-35, pp. 1425-1430, Nov. 1988.
- [11] R. Zimmermann, "Efficient VLSI implementation of modulo $(2n+1)$ addition and multiplication", *Proc. of the 14th IEEE Symp. on Computer Architecture*, pp. 158-167, 1999
- [12] D. Gallaher, F. Petry, and P. Srinivasan, "The digital parallel method for fast RNS to weighted number system conversion for specific moduli $(2^k - 1; 2^k; 2^k + 1)$ ", *IEEE Trans. Circuits Syst. II*, vol. 44, pp. 53-67, Jan 1997.
- [13] P.V. Mohan. "New reverse converters for the moduli set $\{2^n-3, 2^n-1, 2^{n+1}, 2^n+3\}$ ", *Int Conf. on Signal Proc. & Communications*, pp 188-192, 2004.
- [14] R. Chaves and L. Sousa. " $\{2^{n+1}, 2^{(n+k)}, 2^{n-1}\}$:A New RNS Moduli Set Extension", *IEEE Euromicro Symposium on Digital System Design: Architectures, Methods and Tools*, IEEE Computer Society, pp. 210-217, Sep2004.
- [15] S.J. Piestrak, "Design of Residue generators and multioperand adders using carry-save adders". *IEEE Trans. on Computers*, Vol. 43, pp. 68-77, Jan. 1994.
- [16] S. Cotofana and Vassiliadis, "Periodic symmetric functions, serial addition, and multiplication with neural networks", *IEEE Trans. on Neural Networks*, Vol. 9, 6, Nov. 1998, pp.1118-1128.
- [17] J.M. Quintana, M.J. Avedillo, H. Pettenghi, "Design of Residue Generators using Threshold Logic". *Proc. IEEE Midwest Symp. on Circuits and Systems*, 46; vol. 3, pp. 1427-1430
- [18] V. Piuri, M. Berzieri, A. Bisaschi, and A. Fabi, "Residue arithmetic for a fault-tolerant multiplier: The choice of the best triple of bases," *Microproc. and Microprogr.*, vol. 20, pp. 15-23, 1988.
- [19] V.I. Varshavsky, " β -driven threshold elements", *Proc. GLSVLSI'98*, Lafayette (USA), 1998, pp.52-58.