<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>A residue-to-binary converter for a new five-moduli set (Published version)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Cao, Bin; Chang, Chip Hong; Srikanthan, Thambipillai</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>2007</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/6026">http://hdl.handle.net/10220/6026</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>IEEE Transactions on Circuits and Systems-I: Regular Papers © copyright 2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE. This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder. <a href="http://www.ieee.org/portal/site">http://www.ieee.org/portal/site</a>.</td>
</tr>
</tbody>
</table>
A Residue-to-Binary Converter for a New Five-Moduli Set

Bin Cao, Chip-Hong Chang, Senior Member, IEEE, and Thambipillai Srikanth, Senior Member, IEEE

Abstract—The efficiency of the residue number system (RNS) depends not only on the residue-to-binary converters but also the operand sizes and the modulus in each residue channel. Due to their special number theoretic properties, RNS with a moduli set consisting of moduli in the form of $2^n \pm 1$ is more attractive than those with other forms of moduli. In this paper, a new five-moduli set RNS $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1, 2^{n-1} - 1\}$ for even $n$ is proposed. The new moduli set has a dynamic range of $(5n - 1)$ bits. It incorporates two additional moduli to the celebrated three-moduli set, $\{2^n - 1, 2^n, 2^n + 1\}$ with VLSI efficient implementations for both the binary-to-residue conversion and the residue arithmetic units. This extension increases the parallelism and reduces the size of each residue channel for a given dynamic range. The proposed residue-to-binary converter relies on the properties of an efficient residue-to-binary conversion algorithm for $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$ and the mixed-radix conversion (MRC) technique for the two-moduli set RNS. The hardware implementation of the proposed residue-to-binary converter employs adders as the primitive operators. Besides, it can be easily pipelined to attain a high throughput rate.

Index Terms—Mixed-radix conversion (MRC), residue arithmetic, residue number system (RNS), residue-to-binary converter, VLSI.

I. INTRODUCTION

The inherent carry-free operations, parallelism, and fault-tolerant properties of the residue number system (RNS) have made it an important candidate for high-performance and fault-tolerant applications [1], [2]. During the past decade, the RNS has received considerable attention in computationally intensive applications where the key operations required are addition, subtraction and multiplication, such as digital filters, correlators, fast Fourier transform (FFT), image processing, and digital communications [3]–[8].

To interface the highly parallel residue arithmetic based processing with the prevailing binary number system, a typical RNS-based processor must possess at least two components: the binary-to-residue converter which converts the binary data into their residue representations, and the residue-to-binary converter, which converts the RNS-represented results into their binary weighted representations. Besides these two overhead components, a typical RNS should include the residue arithmetic units (RAUs) which perform the necessary arithmetic operations required by the applications. The degree of RNS’s complexity involved in the hardware implementation of each component depends largely on the moduli set. The architectures of the RNS for general moduli sets have been widely studied. Well-balanced residue channels with low wastage on dynamic ranges are readily obtained from general moduli sets. However, due to the lack of special number theoretic properties of general moduli sets, the residue-to-binary converters and RAUs for the general moduli set RNS are usually implemented with large number of adders and ROMs, which are area intensive and computationally inefficient, particularly for ASIC implementation of RNS involving large dynamic range [1], [2], [9]–[13]. Although the cost of memory has been driven low nowadays, the number of ROMs and the access time incurred by the need to read these ROMs iteratively make their implementations in application-specific integrated circuit (ASIC) implementations unfavorable.

Special moduli sets have been used extensively to reduce the hardware complexity in the implementation of RNS architectures, especially for the residue-to-binary converters [14]–[32]. Among the special moduli sets, those employ moduli of the forms $2^n$ and $2^n \pm 1$ are the most popular choices. This type of moduli not only eases the design of efficient binary-to-residue and residue-to-binary converters, but the modular arithmetic operators in their RAUs can also be readily realized with highly efficient architectures, such as the modular adders and modular multipliers in [33]–[42]. The three-moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ has gained unprecedented popularity by virtue of its inherent number theoretic properties in Chinese Remainder Theorem (CRT), and several very efficient memoryless residue-to-binary converters have been proposed for this triple moduli set [14], [16], [21]–[23].

In some high-performance and fault-tolerant signal processing applications [7], [43], [44], the level of parallelism provided by the three-moduli set is compromised by the increased dynamic range. The demand for the increased granularity of parallelism and dynamic range calls for the necessity to expand the three-moduli set. Moduli sets obtained by adding moduli in the form of $2^n \pm 1$ to the celebrated three-moduli set are called supersets. Four-moduli superset $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} + 1\}$ was proposed by Bhardwaj et al. in [24], but two of the moduli are in the form of $2^n + 1$, causing the excess of the dynamic range comparatively larger. Vinod et al. proposed a more efficient four-moduli superset $\{2^n - 1, 2^n, 2^n + 1, 2^n+1 - 1\}$ [25], and its residue-to-binary converters are improved by Cao et al. [26] using the efficient conversion algorithm for the three-moduli set $\{2^n - 1, 2^n, 2^n + 1\}$. To minimize the waste of dynamic range, the same authors also proposed a new supplementary four-moduli superset $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$ in [26] with compatible conversion efficiency in its residue-to-binary converter.
Skavantzos et al. proposed a class of conjugate moduli sets in [20]. Although these are high-cardinality sets, the moduli are not pairwise relatively prime, resulting in reduced dynamic ranges, asymmetric moduli channel length and long conversion delay. Skavantzos also proposed a five-moduli set \( \{2^{n}−1, 2^{n}, 2^{n+1} + 1, 2^{n+2} + 2^{(n+1)/2} + 1, 2^{n} − 2^{(n+1)/2} + 1 \} \) [28]. As the two extended moduli are not in the form of \( 2^{n} \) or \( 2^{n} ± 1 \), it is difficult to design VLSI efficient architectures for the binary-to-residue conversion and the modular arithmetic operators. To minimize the hardware cost, reuse of the modular multipliers from the RNS arithmetic processing unit has been exploited. In [29], Mathew et al. proposed a five-moduli set \( \{2^{3n}, 2^{3n}−1, 2^{3n} + 1, 2^{3n} − 2(3n+1)/2 + 1, 2^{3n} + 2(3n+1)/2 + 1 \} \). It has the same disadvantages as [28]. Hiasat [32] proposed a similar five-moduli set, where the residue-to-binary converter is more efficient than those for [28] and [29]. In [31], Skavantzos and Stouraitis proposed a new five-moduli set \( \{2^{n+1}, 2^{n} − 2^{n−1}, 1, 2^{n−1} + 1, 2^{n−1} + 1 \} \), where all the moduli are in the form of \( 2^{n} \) or \( 2^{n} ± 1 \). Therefore, its RAU is efficient than those of [28], [29], [32]. The disadvantage is that it is not co-prime for any value of \( n \), resulting in the reduced dynamic range and increased complexity of the residue-to-binary conversion algorithm. There are two moduli in the form of \( 2^{n}+1 \). According to [33]–[41], the operations modulo \( 2^{n}−1 \) are more efficient than those for modulo \( 2^{n}−1 \), therefore, it is better to reduce the number of moduli in the form of \( 2^{n}−1 \).

In this paper, we propose a new five-moduli superset \( \{2^{n} − 1, 2^{n}, 2^{n+1} + 1, 2^{n+1} + 1, 2^{n+1} + 1 \} \), which is valid for even values of \( n \). This moduli set is efficient for both the binary-to-residue converters and for the modular operations, as the moduli are in the form of \( 2^{n} \) or \( 2^{n} ± 1 \). Furthermore, there is only one modulus in the form of \( 2^{n}+1 \). Our proposed algorithm for its residue-to-binary converter is based on the mixed-radix conversion (MRC) technique and the conversion algorithm for the four-moduli superset \( \{2^{n} − 1, 2^{n}, 2^{n+1} + 1, 2^{n+1} + 1 \} \) [26], [27] wherein an efficient residue-to-binary converter for the popular three-moduli set proposed in either [22] or [23] has been adopted. The fundamental idea of decomposing the moduli set is borrowed from the pioneering work of New Chinese Remainder Theorem first introduced in [15]. The derived residue-to-binary converter is based on adders. Such adder-based design has the advantage of being design automation friendly and can be readily pipelined to suit the throughput rate constrained by the application.

MRC can also be used for the calculation of \( X \) [1]. For a simple two-moduli set \( \{P_{1}, P_{2}\} \), the integer \( X \) can be converted from its residue representation \( (x_{1}, x_{2}) \) by MRC as follows:

\[
X = a_{1} + a_{2}P_{1} = x_{1} + P_{1} \cdot \left[ (x_{2} − x_{1})/1 \right] P_{1} P_{2} \tag{2}
\]

where \( 1/P_{1} P_{2} \) is the multiplicative inverse of \( P_{1} \) modulo \( P_{2} \), and the coefficients \( a_{1} \) and \( a_{2} \) are the mixed-radix digits of \( X \).

If the integers \( X \) and \( Y \) have RNS representations \( (x_{1}, x_{2}, x_{3}, \ldots, x_{n}) \) and \( (y_{1}, y_{2}, \ldots, y_{n}) \) respectively, then the RNS representation of \( Z = X + Y \) is given by \( (z_{1}, z_{2}, \ldots, z_{n}) \), where \( z_{i} = x_{i} \otimes y_{i} P_{1} \) and \( \otimes \) denotes one of the operations of addition, subtraction or multiplication [1]. This means that arithmetic operation on large numbers can be performed by a collection of smaller arithmetic operations, and these operations can be performed in each residue channel concurrently and independently without inter-channel carry propagation.

### III. Residue-to-Binary Converter for the Proposed RNS

The aim of this section is to establish the number theoretic framework for the efficient conversion of the residue number represented in the proposed superset to its binary equivalent. We decompose the superset \( \mathcal{S} \) into two subsets, \( \mathcal{S}_{1} = \{2^{n} − 1, 2^{n}, 2^{n+1} + 1, 2^{n+1} − 1 \} \) and \( \mathcal{S}_{2} = \{2^{n}(2^{2n}−1)(2^{n}−1), 2^{n−1} \} \). Being a new moduli set, we shall first prove that it is pairwise prime. It is well acknowledged that the moduli of \( \mathcal{S}_{1} = \{2^{n}−1, 2^{n}, 2^{n}+1, 2^{n+1}−1 \} \) are pairwise prime when \( n \) is even [25], [26]. Therefore, we shall prove that the elements of \( \mathcal{S}_{1} \) are all relative prime to the fifth element of \( \mathcal{S}_{2} = 2^{n}−1 \) for even value of \( n \). As \( 2^{n} \) is an even number, it is apparent that it is relative prime to \( 2^{n−1}−1 \). Assume that \( 2^{n}−1 \) is not relative prime to \( 2^{n−1}−1 \), and let \( \gcd(2^{n}−1, 2^{n−1}−1) = k \) for some integer \( k > 1 \). Then we have \( (2^{n}−1)(2^{n−1}−1) = m\cdot k \), where \( m \) is an integer. As both \( 2^{n}−1 \) and \( 2^{n−1}−1 \) are odd numbers, their common divisor cannot be an even number. Therefore, \( k \) must be odd and \( m\cdot k \) can never be a power-of-two term. However, \( (2^{n}−1)−(2^{n−1}−1) = 2^{n−1} \) which contradicts the hypothesis that \( (2^{n}−1)−(2^{n−1}−1) = m\cdot k \) is not a power-of-two term. Therefore, the assumption of \( 2^{n}−1 \) is not pairwise prime to \( 2^{n−1}−1 \) is incorrect. This proves that \( 2^{n}−1 \) is pairwise prime to \( 2^{n−1}−1 \). The pairwise primality of other moduli of \( \mathcal{S}_{1} \) with \( 2^{n−1}−1 \) can be proven in a similar manner.

As the superset \( \mathcal{S} \) can be decomposed into \( \mathcal{S}_{1} \) and \( \mathcal{S}_{2} \), a residue-to-binary converter of the four moduli superset, \( \mathcal{S}_{1} = \{2^{n}−1, 2^{n}, 2^{n}+1, 2^{n}−1 \} \), can be used to recover an interim integer \( X^{(2)} \) from the residues \( x_{1}, x_{2}, x_{3}, x_{4} \) of \( \mathcal{S}_{1} \) [26]. The final binary equivalent, \( X \) of \( \{x_{1}, x_{2}, x_{3}, x_{4}\} \) in \( \mathcal{S} \) can then be calculated from the residues \( \{X^{(2)}, x_{5}\} \) correspond to the two-moduli set \( \mathcal{S}_{2} = \{2^{n}(2^{2n}−1)(2^{n}−1), 2^{n−1}−1 \} \) by (2).

According to the conversion algorithm of [26], the interim integer \( X^{(2)} \) can be calculated by

\[
X^{(2)} = x_{2} + 2^{n}(2^{2n}Z + 2^{n}Y_{2} + Y_{1} − Z) = x_{2} + 2^{n}\cdot T \tag{3}
\]

where \( Y_{1}, Y_{2} \) are the output signals of the residue-to-binary converter for the triple moduli set \( \{2^{n}−1, 2^{n}, 2^{n}+1 \} \), \( Z \) is the output of the residue-to-binary converter for the four-moduli superset \( \mathcal{S}_{1} \). Therefore, \( T \) is a \((3n+1)\)-bit integer.
By applying (2) to the resultant \( S_2 \), the binary equivalent \( X \) of the proposed superset can be obtained from its residues by

\[
X = X^{(2)} + 2^n(2^{2n} - 1)(2^{n+1} - 1)\bar{h}_0(x_5 - X^{(2)})_{2^{n-1}-1}
\]

(4)

where \( \bar{h}_0 \) is the multiplicative inverse of \( 2^n(2^{2n} - 1)(2^{n+1} - 1) \) modulo \( 2^{n-1} - 1 \), thus

\[
|\bar{h}_02^n(2^{2n} - 1)(2^{n+1} - 1)|_{2^{n-1}-1} = 1.
\]

(5)

Since

\[
|2^n|_{2^{n-1}-1} = |2(2^{n-1} - 1) + 2|_{2^{n-1}-1} = 2^{n+1} - 1
\]

and

\[
|2^n - 1|_{2^{n-1}-1} = |3|_{2^{n-1}-1} = 3
\]

the left-hand side (LHS) of (5) can be simplified as follows:

\[
|k_02^n(2^{2n} - 1)(2^{n+1} - 1)|_{2^{n-1}-1} = |k_0 \cdot 2 \cdot 3 \cdot 3|_{2^{n-1}-1} = 18|k_0|_{2^{n-1}-1}.
\]

(6)

The solution to (5) is provided by the following Lemma.

**Lemma 1:** For any even number \( n \) \( (n > 2) \), the solution of the modular equation

\[
|18 \cdot k_0|_{2^{n-1}-1} = 1
\]

is given by the following.

When \( n = 6k - 2 \), \( k = 1, 2, 3, \ldots \)

\[
k_0 = 2^{n-3} + \frac{2}{9}(2^{n-1} - 1) = 2^{6k-5} + \frac{2}{9}(2^{6k-6} - 1).
\]

(8)

When \( n = 6k, k = 1, 2, 3, \ldots \)

\[
k_0 = 2^{n-2} + \frac{1}{9}(2^{n-1} - 5) = 2^{6k-2} + \frac{1}{9}(2^{6k-1} - 5).
\]

(9)

When \( n = 6k + 2, k = 1, 2, 3, \ldots \)

\[
k_0 = 2^{n-2} + \frac{8}{9}(2^{n-1} - 1) = 2^{6k+2} + \frac{8}{9}(2^{6k} - 1).
\]

(10)

**Proof of (8):** When \( n = 6k - 2 \), LHS of (7) becomes

\[
|18 \cdot \left(2^{6k-5} + \frac{2}{9}(2^{6k-6} - 1)\right)|_{2^{n-1}-1} = \left|5 \cdot 6^{6k-3} - 4\right|_{2^{n-1}-1} = 1.
\]

**Proof of (9):** When \( n = 6k \), LHS of (7) becomes

\[
|18 \cdot \left(2^{6k-2} + \frac{1}{9}(2^{6k-1} - 5)\right)|_{2^{n-1}-1} = \left|11 \cdot 6^{6k-1} - 10\right|_{2^{n-1}-1} = 1.
\]

**Proof of (10):** When \( 6k + 2 \), LHS of (7) becomes

\[
|18 \cdot \left(2^{6k+2} + \frac{8}{9}(2^{6k} - 1)\right)|_{2^{n-1}-1} = \left|17 \cdot 6^{6k+1} - 16\right|_{2^{n-1}-1} = 1.
\]

This completes the proof.

The closed form expressions provided by Lemma 1 in their original forms are not amenable to hardware realization. Two special properties of modulo \( 2^n - 1 \) arithmetic, proposed by Szabo and Tanaka [1] and used extensively in [26], are exploited to simplify the implementations of the solutions. These properties are introduced here as Properties 1 and 2.

**Property 1:** Multiplying an \( n \)-bit binary number \( x \) by \( r \) power of 2 in modulo \( 2^n - 1 \) is equivalent to a circular left shift operation

\[
x \cdot 2^r \equiv C_{LS}(x, r)
\]

where \( C_{LS}(x, r) \) denotes a circular shift of the \( n \)-bit binary number \( x \) by \( r \) bits to the left.

If the multiplicand is negative, we have the following.

**Property 2:**

\[
-x \cdot 2^r \equiv C_{LS}(x, r)
\]

where \( \bar{x} \) is the 1’s complement of the \( n \)-bit binary number \( x \).

Properties 1 and 2 can be utilized to eliminate the logic circuits needed to implement the modulo \( 2^n - 1 \) multiplication by powers of 2. Only re-wiring of bits is required which incurs virtually no hardware cost and delay. In order to take advantage of Properties 1 and 2 for efficient hardware implementation, the expressions of \( k_0 \) under the three different ranges of \( n \) are expanded into differences of geometrical series.

For the case of \( n = 6k - 2 \) \( (k \geq 2) \)

\[
k_0 = 2^{6k-5} + \frac{2}{9}(2^{6k-6} - 1)
\]

\[
= 2^{6k-5} + \sum_{i=0}^{k-2}(2^{6i+4} - 2^{6i+1})
\]

\[
= 2^{6k-5} + 2^4 + 2^{6+1+4} + \ldots + 2^{6(k-2)+4}
\]

\[
= 2^{6k-3} + 2^4 + 2^{6+1+4} + \ldots + 2^{6(k-2)+6}
\]

\[
= 2^{6k-3} + 2^4 + 2^{6+1+4} + \ldots + 2^{6n-9}.
\]

(13)

When \( n = 6k \) \( (k \geq 2) \)

\[
k_0 = 2^{6k-2} + \frac{1}{9}(2^{n-1} - 5)
\]

\[
= 2^{6k-2} + \sum_{i=0}^{k-1}2^{6i+2} - 1 - \sum_{i=0}^{k-2}2^{6i+5}
\]

\[
= 2^{6k-2} + 2^2 + 2^{6+1+2} + \ldots + 2^{6(k-1)+2}
\]

\[
= 2^{6k-2} + 2^2 + 2^{6+1+5} + \ldots + 2^{6(k-2)+5}
\]

\[
= 2^{6k-2} + 2^2 + 2^{6+1+2} + \ldots + 2^{6n-7}.
\]

(14)
When \( n = 6k + 2 \)

\[
k_0 = 2^{6k} + \frac{8}{9} \cdot 2^{6k} - 1
\]

\[
= 2^{6k} + \sum_{i=1}^{k} (2^{6i} - 2^{6i-3})
\]

\[
= 2^{6k} + (2^{6+1} + 2^{6+2} + \ldots + 2^{6k})
\]

\[
= (2^{6+3} + 2^{6+2} + \ldots + 2^{6i-3})
\]

\[
= 2^{n+2} + (2^{6+2} + 2^{6+3} + \ldots + 2^{n+2})
\] (15)

If we let

\[
L = \left| x_5 - X(2^i) \right|_{2n-1-1}
\]

(16)

\[
R = k_0 \left| x_5 - X(2^i) \right|_{2n-1-1} = |k_0 \cdot L|_{2n-1-1}.
\]

(17)

Then (4) can be expressed as follows:

\[
X = X(2^i) + 2^{n} \cdot (2^{2n-1})(2^{n+1} - 1)R.
\]

(18)

By substituting \( X(2^i) \) of (3) into (16), \( L \) can be calculated by

\[
L = \left| x_5 - x_2 - 2^n \cdot T \right|_{2n-1-1} = \left| x_5 - x_2 - 2 \cdot T \right|_{2n-1-1}
\]

\[
= \left| x_5 - x_2 - 2 \left( 2^{n+1} - 1 \right) Z + 2 \left( Y_{2} \cdot Y_1 \right) \right|_{2n-1-1}
\]

\[
= \left| x_5 - x_2 - 2 \left( 2^{n+1} - 1 \right) Z - 2 \cdot 2^{n+1} Y_2 - 2Y_1 \right|_{2n-1-1}
\]

\[
= \left| x_5 - x_2 - 6Z - 4Y_2 - 2Y_1 \right|_{2n-1-1}.
\]

(19)

For ease of addressing bit level manipulations, the residues are also represented in their binary forms as follows: \( x_1 = (X_{1,1,n-1}, X_{1,1,n-2}, \ldots, X_{1,0}) \), \( x_2 = (X_{1,2,n-1}, X_{1,2,n-2}, \ldots, X_{1,0}) \), \( x_3 = (X_{3,3,n-1}, X_{3,3,n-2}, \ldots, X_{3,0}) \), \( x_4 = (X_{4,4,n-1}, X_{4,4,n-2}, \ldots, X_{4,0}) \), and \( x_5 = (X_{5,5,n-1}, X_{5,5,n-2}, \ldots, X_{5,0}) \). \( Y_1, Y_2, \) and \( Z \) are similarly expressed in their binary forms as follows: \( Y_1 = (Y_{1,1,n-1}, Y_{1,1,n-2}, \ldots, Y_{1,0}) \), \( Y_2 = (Y_{2,1,n-1}, Y_{2,1,n-2}, \ldots, Y_{2,0}) \), \( Z = (Z_{1,1,n-1}, Z_{1,1,n-2}, \ldots, Z_{1,0}) \). Furthermore, let \( x_3 = x_2 - 2^{n+1} X_{2,n-1} \), \( Z_{2} = Z - 2^{n+1} Z_{n-1} - 2^{n+1} Y_{2,n-1} \), \( Y_{1,2} = Y_2 - 2^{n+1} Y_{2,n-1} \), and \( Y_{1,1} = Y_1 - 2^{n+1} Y_{2,n-1} \). \( Z_{1,2} \), \( Z_{1,1} \), and \( Y_{1,1} \) are the lowest \( n-1 \) bits of \( x_2, X_{2,n-1}, \) and \( Y_{2,n-1} \), respectively. By substituting these terms into the expression of \( L \) in (19), we have

\[
L = \left| x_5 - x_2 - 2^2 Z_{1,2} - 2^2 Z_{1,1} - 2^2 Y_2 - 2^2 Y_{1,2} + 2^2 Y_1 - 2^{n+1} Y_{2,n-1} \right|_{2n-1-1}
\]

\[
= \left| 2^{n+1} + 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} \right|_{2n-1-1}
\]

\[
= \left| 2^{n+1} + 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} - 2^{n+1} Z_{n-1} \right|_{2n-1-1}
\]

(20)

Properties 1 and 2 can then be used to simplify (20) to

\[
L = \sum_{i=1}^{13} L_i \left| 2^{n-1-1} \right.
\]

(21)

where

\[
L_1 = (X_{1,0,n-1}, X_{1,0,n-2}, \ldots, X_{1,0})
\]

(22a)

\[
L_2 = (X_{2,0,n-1}, X_{2,0,n-2}, \ldots, X_{2,0})
\]

(22b)

\[
L_3 = CLS_{n-1}(Z_{1,1}^d, 1) = (Z_{2,1}^d, Z_{2,2}^d, \ldots, Z_{2,0})
\]

(22c)

\[
L_4 = CLS_{n-1}(Z_{1,2}^d, 2) = (Z_{2,1}^d, Z_{2,2}^d, \ldots, Z_{2,n-2})
\]

(22d)
Fig. 2. Calculation of \( L \).

Thus, only one \((8,2^{n+1} - 1)\) multi-operand modular adder (MOMA) \([16], [21]\) is required. The architecture is shown in Fig. 2.

Once \( L \) has been obtained, \( R \) can be calculated by (17) for the three different cases of \( k_0 \). When \( n = 6k - 2 \), the expanded form of \( k_0 \) given by (13) is substituted into (17) and with the aid of Property 1 and Property 2, we have

\[
R = \left| \left( 2^{n-3} + (2^4 + 2^{n+1} + \cdots + 2^{n-6}) \right) - \left( 2^1 + 2^{n+1} + \cdots + 2^{n-9} \right) \right| \cdot L \left\|_{2^{n-1} - 1} \right.
\]

\[
\text{CLS}_{n-1}(L, n - 3) + \text{CLS}_{n-1} \left( \left( L, 4 \right) + \text{CLS}_{n-1}(L, 10) \right) + \cdots + \text{CLS}_{n-1}(L, n - 6) + \text{CLS}_{n-1}(L, 1)
\]

\[
+ \text{CLS}_{n-1}(L, 7) + \text{CLS}_{n-1}(L, 13) + \cdots + \text{CLS}_{n-1}(L, n - 9) \right| \cdot \left( 2^{n-1} - 1 \right)
\]

(26)

When \( n = 6k \), substituting \( k_0 \) of (14) into (17), we have

\[
R = \left| \left( 2^{n-2} + (2^2 + 2^{n+2} + \cdots + 2^{n-4}) \right) - \left( 2^0 + 2^5 + 2^{n+5} + \cdots + 2^{n-7} \right) \right| \cdot L \left\|_{2^{n-1} - 1} \right.
\]

\[
\text{CLS}_{n-1}(L, n - 2) + \text{CLS}_{n-1}(L, 2) + \text{CLS}_{n-1}(L, 8) + \cdots + \text{CLS}_{n-1}(L, n - 4)
\]

\[
+ \text{CLS}_{n-1}(L, 5) + \text{CLS}_{n-1}(L, 11) + \cdots + \text{CLS}_{n-1}(L, n - 7) \right| \cdot \left( 2^{n-1} - 1 \right)
\]

(27)

When \( n = 6k + 2 \), substituting \( k_0 \) of (15) into (17), we have

\[
R = \left| \left( 2^{n-2} + (2^6 + 2^{n+2} + \cdots + 2^{n-2}) \right) - (2^{n-3} + 2^{2^3} + \cdots + 2^{n+5}) \right| \cdot L \left\|_{2^{n-1} - 1} \right.
\]

\[
\text{CLS}_{n-1}(L, n - 2) + \text{CLS}_{n-1}(L, 6) + \text{CLS}_{n-1}(L, 12) + \cdots + \text{CLS}_{n-1}(L, n - 2)
\]

\[
+ \text{CLS}_{n-1}(L, 3) + \text{CLS}_{n-1}(L, 9) + \cdots + \text{CLS}_{n-1}(L, n - 5) \right| \cdot \left( 2^{n-1} - 1 \right)
\]

(28)

Therefore, only one \((2k - 1, 2^{n+1} - 1)\) MOMA is required for \( n = 6k - 2 \), and one \((2k + 1, 2^{n+1} - 1)\) MOMA is required for \( n = 6k \) or \( n = 6k + 2 \). Fig. 3 shows the architecture for the calculation of \( R \) when \( k = 3 \) and \( n = 6k - 2 = 16 \), where only one \((5, 2^{15} - 1)\) MOMA is required.

After the \((n - 1)\)-bit \( R \) has been obtained, the final value of \( X \) can be calculated by (18). Let the binary representation of \( R \) be \( R_{n-2} \cdots R_0 \). First, let

\[
V = (2^{2n} - 1)(2^{n+1} - 1)R.
\]

(29)

By expanding the equation of \( V \), we have

\[
V = 2^{n+1} \left( 2^{2n}R - (2^{n+1}R + R) \right) + R = 2^{n+1} \cdot U + R
\]

where \( U \) is defined as follows:

\[
U = 2^{2n}R - (2^{n+1}R + R)
\]

\[
= \left( (R_{n-2} \cdots R_0)^{(1)}(0)^{(2n)} \right) \cdot 2
\]

\[- \left( (R_{n-2} \cdots R_0)^{(2)} \right) \cdot 2.
\]

(30)

(31)

In (31), the notation \( (R_{n-2} \cdots R_0)^{(k)} \) denotes \( k \) repetitions of the binary string \( R_{n-2} \cdots R_0 \) [28]. Only a \( (3n - 1)\)-bit binary subtractor is needed for the calculation of \( U \), and the resultant \( (3n - 1)\)-bit \( U \) can be concatenated to the left of \( R \) to form the \( 4n\)-bit string \( V \) by (30). By substituting the computed values of \( X^{(2)} \) from (3) and \( V \) from (29) into (18), we have

\[
X = X^{(2)} + 2^n \cdot V = x_2 + 2^n \cdot (T + V).
\]

(32)

A \( 4^n\)-bit binary adder is required to sum the values of \( T \) and \( V \) in (32) and the sum is concatenated to the left of the residue \( x_2 \) to obtain \( X \). Fig. 4 shows the final architecture of the residue-to-binary converter for the proposed five-moduli superset, where "&" denotes the concatenation operation of two numbers. The above algorithm is based on the decomposition of the five-moduli set into \( \{2^n - 1, 2^n, 2^{n+1} + 1, 2^{n+1} - 1\} \) and \( \{2^{n-1} - 1\} \). The second possible decomposition is \( \{2^n - 1, 2^n, 2^{n+1}, 2^{n+1} - 1\} \) and \( \{2^{n-1} - 1\} \), but this will cause the MOMAs for the calculation of \( L \) and \( R \) to become \((n + 1)\)-bit wide as opposed to \((n - 1)\)-bit wide in the above algorithm.
and a 3-\notimes-1 bit subtractor, is used for the calculation of $X$. Substituting (26), $Z = (10000101100)_2$, $X(2) = (101339AF(CC8))_{16}$, and $T = (42C63DBD)_{16}$ are obtained. From (22a) to (22f), we have $L_1 = (0000001110)_{23}$, $L_2 = (1001101111)_{23}$, $L_3 = (1101001111)_{23}$, $L_4 = (1010011111)_{23}$, $L_5 = (1001100000)_{23}$, and $L_6 = (0000000000)_{23}$. From (24), $C_{M,1} = 1$, $C_{M,3} = 0$, $S_{M,1} = 0$, $S_{M,2} = 1$, $S_{M,3} = 1$, and $S_{M,4} = 1$. Thus, according to (23), $C_M = (1111111111)_{23}$ and $S_M = (1111111111)_{23}$. Based on (25) and (26), $L = (1101101111)_{23}$, $R = (111000010)_{23}$. Substituting the value of $R$ into (31), we obtain $U = (1111111111)_{16}$ and (30) yields $V = (EQE3D1F1C2)_{16}$. Finally, by (32), $X = (3849A817654C8)_{16}$.

IV. PERFORMANCE EVALUATION AND COMPARISONS

The performances of our proposed residue-to-binary converter for the new five moduli superset are evaluated in terms of area, delay and power consumption. It is then compared with the residue-to-binary converters for other five-moduli sets.

According to Fig. 4, the proposed residue-to-binary converter consists of one four-moduli set converter, an arithmetic unit for the calculation of $R$ (including the calculation of $L$), one (3n − 1)-bit binary subtractor for the calculation of $U$, one 4n-bit binary adder and some inverters. The calculation of $L$ consists of one (8,2n+1−1) MOMA shown in Fig. 2. The logic gates required for the calculation of $C_M$ and $S_M$ shown in Fig. 1(b) approximate to two full adders (FAs). The calculation of $R$ consists of one (2k−1,2n−1−1) MOMA for $n = 6k−2$, and one (2k+1,2n−1−1) MOMA for $n = 6k$ or $n = 6k+2$. When the 4-stage residue-to-binary converter for the four-moduli set $\{2^{n−1}, 2^n, 2^{n+1}, 1, 2^{n+1}−1\}$ is used [26], the estimated hardware costs in terms of primitive logic elements such as FA, binary adder (add) and subtractor (sub), and modular adder (mod add), are shown in Table I. The total conversion delay is the sum of the delays of the residue-to-binary converter for the three-moduli set $\{2^{n−1}, 2^n, 2^n+1\}$, the calculation of $Z$, the calculation of $R$, the (3n − 1)-bit subtractor, and the 4n-bit adder. To improve the throughput rate, pipelining is usually applied in real implementation.

In order to obtain more realistic results, the proposed converter is described by structural VHDL. Six-stage pipelining is used to achieve a high throughput. Synopsis Design Compiler is used with the Avant! Libra-Passport V2.6 digital library (3.3-V, 0.35-μm, 4 metal layers) to synthesize the design for different dynamic ranges (DRs). Two optimization options are analyzed. First, the design is area constrained to obtain a minimum area design. Second, increasingly stringent timing constraints are applied to each design progressively until the verge of timing closure. Table II shows the performances of the proposed design optimized for area and Table III shows the results of delay driven optimization. The area cost is measured in terms of the number of equivalent two-input NAND gates of the circuit synthesized by the Design Compiler. The total area cost includes both the cell area and the net interconnection area. For completeness, the default power simulation results invoked by Synopsis Design Compiler are included. The dynamic power reported by the Synopsis power compiler models the switching activity in terms of static probability and toggle rate. This power analysis assumed 50% static probability and a toggle rate of 50% of the fastest clock in the design. From the simulation results, extreme timing driven optimization almost doubles the area costs of the designs in comparison with those optimized for area. In real applications, if the desired delay has already been achieved, the excess timing margin can be traded for the area cost of the design.

Since the proposed five-moduli set is an entirely new five-moduli set, it is difficult to make a judicial comparison of its residue-to-binary converter against the converters of other existing five-moduli sets, such as those proposed in [28], [29], [31], [32]. The disadvantages of these moduli sets have been discussed in the introduction section. In [28] the author assumes that the existing modular multipliers in the arithmetic units can be used for the residue-to-binary conversion. According to the comments from [29], this may severely affect the performance of the system as a whole. The authors in [29] proposed a conversion algorithm for a similar five-moduli set by simplifying the modular multipliers used in [28] to some modular additions. Careful analysis shows that the result of this simplification is trivial, as the required MOMAs with nonspecial moduli and the modular reductions still require similar amount of hardware costs as, if not higher than, those required for the constant multipliers. Hiasat [32] proposed a more efficient algorithm for

### Table I

<table>
<thead>
<tr>
<th>Resources</th>
<th>$n = 6k - 2$</th>
<th>$n = 6k$</th>
<th>$n = 6k + 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>FA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mod $2^n-1$ add</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>mod $2^n$ add</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>mod $2^n-1$ add</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(3n-1)-bit sub</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4n-bit add</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

### Table II

<table>
<thead>
<tr>
<th>$n$</th>
<th>DR (bits)</th>
<th>Area (gates)</th>
<th>Total Delay (ns)</th>
<th>Pipelined Delay (ns)</th>
<th>Power (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>19</td>
<td>1620.8</td>
<td>18.00</td>
<td>5.57</td>
<td>12.68</td>
</tr>
<tr>
<td>8</td>
<td>39</td>
<td>5718.0</td>
<td>28.91</td>
<td>7.93</td>
<td>31.9</td>
</tr>
<tr>
<td>12</td>
<td>59</td>
<td>6130.0</td>
<td>34.74</td>
<td>10.49</td>
<td>51.9</td>
</tr>
<tr>
<td>16</td>
<td>79</td>
<td>8555.0</td>
<td>36.41</td>
<td>10.61</td>
<td>80.9</td>
</tr>
<tr>
<td>20</td>
<td>99</td>
<td>11479.0</td>
<td>39.09</td>
<td>11.02</td>
<td>110.6</td>
</tr>
<tr>
<td>24</td>
<td>119</td>
<td>17477.0</td>
<td>41.73</td>
<td>11.32</td>
<td>144.8</td>
</tr>
<tr>
<td>28</td>
<td>139</td>
<td>21136.0</td>
<td>43.13</td>
<td>11.67</td>
<td>174.8</td>
</tr>
</tbody>
</table>

### Table III

<table>
<thead>
<tr>
<th>$n$</th>
<th>DR (bits)</th>
<th>Area (gates)</th>
<th>Total Delay (ns)</th>
<th>Pipelined Delay (ns)</th>
<th>Power (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>19</td>
<td>3588.0</td>
<td>12.52</td>
<td>4.16</td>
<td>37.1</td>
</tr>
<tr>
<td>8</td>
<td>39</td>
<td>8332.0</td>
<td>17.32</td>
<td>5.48</td>
<td>87.7</td>
</tr>
<tr>
<td>12</td>
<td>59</td>
<td>13829.0</td>
<td>19.99</td>
<td>6.66</td>
<td>147.0</td>
</tr>
<tr>
<td>16</td>
<td>79</td>
<td>19899.0</td>
<td>20.99</td>
<td>7.06</td>
<td>217.7</td>
</tr>
<tr>
<td>20</td>
<td>99</td>
<td>26154.0</td>
<td>22.35</td>
<td>7.41</td>
<td>278.2</td>
</tr>
<tr>
<td>24</td>
<td>119</td>
<td>33477.0</td>
<td>25.10</td>
<td>7.78</td>
<td>339.5</td>
</tr>
<tr>
<td>28</td>
<td>139</td>
<td>41936.0</td>
<td>27.86</td>
<td>7.92</td>
<td>392.1</td>
</tr>
</tbody>
</table>
yet another similar five-moduli set, where the modular multipliers are eliminated, and the number of the CSAs is reduced from 9 in [28] and [29] to 6. All these existing special moduli sets are valid for odd \( n \). In view of the lack of efficient modular adders and multipliers for the two extended moduli that are not of the form \( 2^n \pm 1 \) [33], [38], these moduli sets are envisaged to have inferior performance compared to our proposed five-moduli superset for the binary-to-residue conversion and the residue arithmetic operations. Hence, the most appropriate comparison is to benchmark the performance against another five moduli superset, such as the latest most efficient five moduli superset proposed in [31]. Nevertheless, for the purpose of evaluation, we will still provide an impartial comparison of the efficient implementation of the residue-to-binary converters for all the above four five-moduli sets. Following the same basis of comparison adopted in [32], both residue-to-binary converters of [28] and [32] were implemented as a stand alone entity and synthesized using the same synthesis tools and digital library as before. For generality, reuse of hardware resources from the RNS processing channels as noted in [28] has not considered here to avoid the intricate trade-off on performance due to degree of reusability and the accompanying control and timing circuits. Results generated by both timing and area constrained optimizations are analyzed. The implementations of the converters of [31] and [32] are obtained directly from the algorithms and structures proposed in these papers. Using similar techniques as [29] and [32], we simplify the modular multipliers for the calculation of \( A, B, C, \) and \( D \) of the converter of [28] into constant multiplications. The simplification is described as follows.

The architecture proposed in [28] consists of two parts. The first part refers to the calculation of \( A, B, C, \) and \( D, \) where four modular multipliers with constants are required. After \( A, B, C, \) and \( D \) have been calculated, \( Z_1 \) to \( Z_{11} \) can simply be obtained by re-wiring. The second part consists of one \((11, 2^{5n} - 1)\)-MOMA. As the implementation of the modular multipliers in the first part was not given in [28], we propose the improved architecture which has been similarly performed by [29] for the calculation of \( A, B, C, \) and \( D \) for a fair comparison. According to [28],

\[
A = x_2 \cdot N_2^{e_2} \equiv x_2 \cdot 2^{n-2} (2^n + 1) \pmod{2^n - 1}.
\]

By solving the modular equation, we obtain

\[
N_2^e = 2^{n-2}.\]

Applying Property 1 to the calculation of \( A \) gives

\[
A = x_2 \cdot 2^{n-2} (2^n - 1) / 2^{(n+1)/2} + 1.
\]

This simplification leads to the substitution of the more complex modulo \( 2^n - 1 \) multiplication with constant by a simpler circular shift operation, which can be achieved by re-routing the signals.

According to [28],

\[
B = x_3 \cdot N_3^{e_3} \equiv x_3 \cdot 2^{n+1} / 2^{(n+1)/2} + 1 \pmod{2^n + 1},
\]

and

\[
D = x_5 \cdot N_5^{e_5} \equiv x_5 \cdot 2^{(n+1)/2} / 2^{n+1} \pmod{2^n + 1}.
\]

We simplify the modular equations, we obtain the multiplicative inverses \( N_3 = 2^{n-2}, N_5 = 2^{n-2} + 2^{(n-3)/2}, \) and \( N_5 = 2^{n-2} - 2^{(n-3)/2}. \) By exploiting the special formats of the constants, the modular multipliers for the calculation of \( B, C, \) and \( D \) can be further optimized to modular additions but not completely eliminated as in the calculation of \( A. \) Having proposed notable improvements to the architecture for the residue-to-binary converter of [28], we proceed to examine its implications on area, delay and power.

Fig. 5 shows the comparison of the costs of silicon area usage of the residue-to-binary converters of our five-moduli superset, Skavantzis’ [28], another five-moduli superset [31] and Hiasat’s [32], simulated at various dynamic ranges and optimized for minimum silicon area. Figs. 6 and 7 show the
V. CONCLUSION

In this paper, we have proposed a new five-moduli superset \(\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1, 2^{n-1} - 1\}\) to provide for increased parallelism and high-speed residue-to-binary conversions. When compared with the existing nonsuperset five-moduli sets, the advantages are obvious because the superset consists of moduli in form of \(2^n \pm 1\), which are proven in the literature to be more efficient for the RAUs. Since the modulo operations in the RAU are performed more frequently than the residue-to-binary conversion, supersets are preferred over nonsuperset moduli sets. Comparing with the existing non co-prime five-moduli superset, our residue-to-binary converter uses less hardware resource due to the elegant multiplicative inverses which have smaller Hamming weights.

REFERENCES


[35] Bin Cao received the B.Eng. degree from Wuhan Institute of Technology, Wuhan, China in 1991, the M.Eng. degree from Zhejiang University, Hangzhou, China in 1996, and the Ph.D. degree from Nanyang Technological University, Singapore in 2006.

[36] From July 1996 to October 2001, he was with Eastern Communications Company, Hangzhou, China. From May 2005, he was with Seagate Technology International, Singapore. His current research interests include computer arithmetic and cryptosystems.

[37] Chip-Hong Chang (S’92–M’98–SM’03) received the B.Eng. (Hons.) from National University of Singapore, Singapore, in 1989, and his M.Eng. and Ph.D. degrees from Nanyang Technological University (NTU), Singapore, in 1993 and 1998, respectively.

[38] He joined the School of Electrical and Electronic Engineering, NTU in 1999, where he is now an Associate Professor. He holds joint appointments as Deputy Director of the Centre for High Performance Embedded Systems (CHiPES) since 2000, and Program Director of the Centre for Integrated Circuits and Systems (CICS) since 2003. His current research interests include low power arithmetic circuits, algorithms and architectures for digital signal processing, and digital watermarking for IP protection. He has authored three book chapters and more than 120 research papers in international refereed journals and conferences.

[39] Thambipillai Srikanthan (SM’92) received the B.Sc. degree (Hons.) in computer and control systems and the Ph.D. degree in system modeling and information systems engineering from Coventry University, Coventry, U.K.

[40] He joined Nanyang Technological University (NTU) in June 1991 and he now holds joint appointments as Professor and Director of the Centre for High Performance Embedded Systems (CHiPES) and Intelligent Devices and Systems (IDeAS) Cluster. His research interests include system integration methodologies for embedded systems, architectural translations of compute intensive algorithms, high-speed techniques for image processing and dynamic-routing. He has authored more than 200 technical papers and has served on a number of administrative and consultative roles during his academic career.

[41] Dr. Srikanthan is a Corporate Member of the Institution of Electrical Engineers, U.K.