Abstract—The residue number system (RNS) is popular in high performance computation applications because of its carry-free nature. The challenges of RNS systems design lie in the moduli set selection and in the reverse conversion from residue representation to weighted representation. In this paper, we proposed a fully parallel reverse conversion algorithm for the moduli set \( \{r^n - 2, r^n - 1, r^n\} \), based on simple mathematical relationships. Also an efficient hardware realization of this algorithm is presented. Our proposed converter is very faster and results to hardware savings, compared to the other reverse converters.

Keywords—Reverse converter, residue to weighted converter, residue number system, multiple-valued logic, computer arithmetic.

I. INTRODUCTION

THE conventional arithmetic carries propagation based on a weighted number system is the reason for performance degradation in hardware computing systems. The residue number system is a non-weighted number system which speeds up arithmetic operations by dividing them into smaller parallel operations [1], [2]. Since the arithmetic operations in each moduli are independent of the others, there is no carry propagation among them and so RNS leads to carry-free addition, multiplication and borrow-free subtraction [3]. RNS is one of the most popular techniques for reducing the power dissipation and the computation load in VLSI systems design [4]. Some applications of the RNS are real-time processing, digital filters [5],[7], digital signal processing (DSP) [8],[9], the RSA encoding algorithm [12] and digital communication [13]. The architecture of the RNS is naturally fault tolerant and consequently, it is used to error detection, error correction and fault tolerance [15].

Despite binary logic in which logical levels are restricted to two possible states, there exists an alternative named multiple-valued logic. In MVL, the number of discrete signal values or logic states extends beyond two. Arithmetic units implemented with MVL achieve more efficient use of silicon resource and circuit interconnections [20]. There is a clear mathematical attraction of using multiple-valued number representation in MVL. The modular arithmetic that is inherent in MVL can be match with modular arithmetic needed in RNS.

The concept of MVL-RNS was introduced by Soderstrand et al. [17] to design a high speed FIR digital filter. The reverse converter proposed in [17] is based on chinese remainder theorem (CRT) and implemented with read-only memories (ROM’s). This converter is practical to implement small and medium RNS dynamic ranges and it is not appropriate for large dynamic ranges. In [18], new RNS systems based on the moduli of forms \( r^n - 2, r^n - 1 \) and \( r^n + 1 \) are presented. Abdallah et al. in [18] developed a systematic framework utilizing high-radix arithmetic for efficient MVL-RNS implementations and proposed many radix-r moduli sets. This moduli sets are not pairwise relatively prime that resulting in reduced dynamic ranges and unbalanced moduli. The reverse converter presented in [18] is based on CRT and because of the scale-down factors that used to makes moduli pairwise relatively prime, conversion delay and cost are increased. In [19], a new moduli set \( \{r^n - 2, r^n - 1, r^n\} \) where \( r=2k+1, k=1,2,... \) for MVL-RNS was proposed. This moduli set includes pairwise relatively prime and balanced moduli that offers large dynamic range and simple realization of related circuits. The reverse converter presented in [19] is based on CRT and requires many multiplications and reductions, so its area and delay complexities have been increased.

In this paper, a fully parallel reverse conversion algorithm dedicated to the moduli set \( \{r^n - 2, r^n - 1, r^n\} \) where \( r=2k+1, k=1,2,... \) and an efficient hardware realization are presented. Our proposed converter is faster and has lower hardware cost than the other MVL-based reverse converters for three-modulus sets.

The rest of paper is organized as follows. In section II we introduce the necessary background. The conversion algorithm and its hardware realization are presented in section III. Section IV makes comparison and section V is conclusion.

II. BACKGROUND

Residue Number System: A residue number system is defined in terms of a relatively-prime moduli set \( \{P_1, P_2, \ldots, P_n\} \) that is \( \gcd(P_i, P_j)=1 \) for \( i \neq j \) and \( i,j=1,2,,..,n \). A weighted number \( X \) can be represented as \( X=(x_1, x_2, \ldots, x_n) \), where

\[ x_i = X \mod P_i = \left\lfloor \frac{X}{P_i} \right\rfloor \text{ with } 0 \leq x_i < P_i \]

Such a representation is unique for any integer \( X \) in the range \([0,M-1]\), where \( M=P_1P_2\ldots P_n \) is the dynamic range of the moduli set \( \{P_1, P_2, \ldots, P_n\} \).

Addition, subtraction and multiplication on residues can be performed in parallel without any carry propagation among the residue digits. Hence, by converting the arithmetic of large numbers to a set of the parallel arithmetic of smaller numbers, the RNS representation yields significant speed up.

The challenges of the RNS system design lie in the moduli set selection and in the conversion of the residues to the

Manuscript received September 9, 2007.

M. Hosseinzadeh and A. Sabbagh are with the Department of Computer Engineering, Islamic Azad University Science and Research Branch, Tehran, Iran, (emails: hosseinzadeh@sr.iau.ac.ir; amir.sabbagh@sr.iau.ac.ir).

K. Navi is with the Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran, (email: navi@sbu.ac.ir).
equivalent weighted number. The importance of the moduli selection is due to the fact that the dynamic range, the speed as well as the hardware complexity of RNS systems depend on the forms as well as the number of the moduli chosen. Transforming a weighted integer number to the residue representation is called forward conversion and getting back to the weighted representation is referred to as reverse conversion. Forward conversion is conceivably simple and consists of several modulo adders but the reverse conversion involves considerable degree of complexity and includes a lot of modulo operations. The algorithms of reverse conversion are based primarily on Chinese remainder theorem and mixed-radix conversion (MRC).

Chinese Remainder Theorem: by CRT, the number \( X \) can be computed by

\[
X = \left( \sum_{i=1}^{n} x_i N_i P_i \right) M_i^{-1} \mod M
\]

where \( M_i = M/P_i \) and \( N_i = M_i^{-1} \mod P_i \) is the multiplicative inverse of \( M_i \) modulo \( P_i \).

Mixed-Radix Conversion: the number \( X \) can be computed by the formula

\[
X = a_n P_n + \ldots + a_i P_i + a_1 P_1 + a_0
\]

where \( a_0 \) are the mixed-radix coefficients and they can be obtained from the residues by

\[
a_n \equiv (x_n - a_1) P_1^{-1} \mod P_1 - a_2 P_2^{-1} \mod P_2 - \ldots - a_{n-1} P_{n-1}^{-1} \mod P_{n-1} \mod P
\]

where \( n \geq 1 \) and \( a_i = x_i \).

The CRT requires modular additions and multiplications and it is not efficient for the implementation. The MRC is a sequential algorithm and requires modular multiplications and subtractions that is not suitable for efficient hardware realization. In the next section we proposed a novel conversion algorithm which depends on simple mathematical relationships without using CRT or MRC.

The RNS with Moduli Set \( \{ r^n - 2, r^n - 1, r^n \} \): In [19], a new moduli set \( \{ r^n - 2, r^n - 1, r^n \} \) where \( r = 2k + 1, k = 1,2, \ldots \) was introduced for RNS. This moduli set contains pairwise relatively prime moduli for all different values of \( n \), so the dynamic range is greater than the dynamic range of similar moduli sets in [19]. Because of using of high radix (\( r > 2 \)), this RNS can be simply realized in MLV and can provides very large dynamic range for different radix-\( r \) values.

Forward conversion in this RNS is performed as follows. Suppose a 3\( n \)-digit radix-\( r \)-number \( Y \)

\[
Y = (y_{3n-1}y_{3n-2} \ldots y_{3n}y_{3n-1})
\]

We must compute the residues \((x_3, x_2, x_1)\) corresponding to moduli set \( \{ r^n - 2, r^n - 1, r^n \} \). First we calculate the residue in moduli \( r^n \). So we have

\[
x_1 = Y \mod r^n = (y_{3n-1} \ldots y_{3n}y_{3n-1}) \mod r^n
\]

\[
= (y_{3n-1} \ldots y_{3n}y_{3n-1}) r^n + (y_{n-1} \ldots y_{1}y_{0}) \mod r^n
\]

Therefore, it is enough to consider the right most \( n \) digits and the rest of digits will be ignored as they are multiples of \( r^n \). Now we investigate the moduli \( r^n - 2 \), the residue of \( Y \) in moduli \( r^n - 2 \) can be calculated as follow

\[
x_2 = Y \mod r^n - 2 = (y_{3n-1} \ldots y_{3n}y_{3n-1}) r^n + (y_{n-1} \ldots y_{1}y_{0}) \mod r^n - 2
\]

(7)

So, the number \( Y \) is partitioned into consecutive \( n \)-digit blocks and then we must sum these blocks by a modular adder. The residue of \( Y \) in moduli \( r^n - 2 \) is obtained as follow

\[
x_3 = Y \mod r^n - 2 = (y_{3n-1} \ldots y_{3n}y_{3n-1}) r^n - 2
\]

Thus, after partitioning \( Y \) into consecutive \( n \)-digit blocks, we should add the least significant block with two times of the next block and with four times of the most significant block. Then, the result must be reduced in moduli \( r^n - 2 \). The details of the hardware realization of forward converter are presented in [19].

III. PARALLEL REVERSE CONVERTER

We now propose a novel conversion algorithm which converts residue number into its equivalent weighted number. The conversion method is based on simple mathematical relationships without using CRT or MRC.

**Theorem**: Given the moduli set \( \{ r^n - 2, r^n - 1, r^n \} \), the residue number \((x_3, x_2, x_1)\) is converted into the radix-\( r \) weighted number by

\[
X = \left( c' \times r^n + b' \times r^{n-1} + x_1 \right) M
\]

(9)

where

\[
c' = \frac{x_1 + x_3 - 2x_2 + 3r^n - 10}{2} \quad \text{if} (x_1 + x_3) \text{ is odd}
\]

(10)

\[
c' = \frac{x_1 + x_3 - 2x_2 + 2(r^n - 4)}{2} \quad \text{if} (x_1 + x_3) \text{ is even}
\]

(11)

\[
b' = \frac{-3x_1 + 4x_2 - x_3 + r^n + 6}{2} \quad \text{if} (x_1 + x_3) \text{ is odd}
\]

(12)

\[
b' = \frac{-3x_1 + 4x_2 - x_3 + 2(r^n + 2)}{2} \quad \text{if} (x_1 + x_3) \text{ is even}
\]

\[
M = (r^n - 2)(r^{n-1}) r^n
\]

(13)

**Proof**: Suppose the 3\( n \)-digit radix-\( r \) number \( X \) that is partitioned into consecutive \( n \)-digit blocks as

\[
X = y \cdot \frac{y_{3n \ldots 2n} + y_{2n \ldots 2n} \ldots y_{n+1 \ldots y_{n+1}}}{c} \cdot \frac{y_{n+1 \ldots y_{n+1}}}{b} \cdot \frac{y_{n+1 \ldots y_{n+1}}}{a}
\]

We know from the previous section that forward conversion is performed by the following equations
\[ x_1 = a \]
\[ x_2 = a + b + c \]
\[ x_3 = a + b + c \]

Equations (15) and (16) can be rewritten as
\[ x_2 = a + b + c - (\alpha \times (r^n - 1)) \]
\[ x_3 = a + b + c - (\beta \times (r^n - 2)) \]

By substituting the value of \( a \) from (14), we have
\[ b + c = x_2 - x_1 + (\alpha \times (r^n - 1)) \]
\[ 2b + 4c = x_3 - x_1 + (\beta \times (r^n - 2)) \]

Therefore, we have
\[ c = \frac{x_1 + x_3 - 2x_2 + 3r^n - 10}{2} \quad \text{if} \quad (x_1 + x_3) \text{ is odd} \]  
\[ b = \frac{\alpha x_1 + 2x_2 - 2x_3 + 2r^n - 4}{2} \quad \text{if} \quad (x_1 + x_3) \text{ is even} \]  
\[ c' = \frac{-3x_1 + 4x_2 - x_3 + r^n + 6}{2} \quad \text{if} \quad (x_1 + x_3) \text{ is odd} \]  
\[ b' = \frac{-3x_1 + 4x_2 - x_3 + 2r^n + 2}{2} \quad \text{if} \quad (x_1 + x_3) \text{ is even} \]

Thus, the values of \( b' \) and \( c' \) are calculated and then the result of concatenating \( x_1, b' \) and \( c' \) should be reduced in order to placed in the dynamic range. So
\[ X = \left( c' \times r^{2n} + b' \times r^n + x_1 \right) \]

The following example clarifies the conversion method.

**Example:** Given the moduli set \( \{r^2 - 2, r^2 - 1, r^2\} \) where \( r=3 \) and \( n=3 \), the residue number \((x_3, x_2, x_1) = (0, 12, 14)\) is converted to the weighted number \( X \) by this way

Moduli Set: \( \{3^3 - 2, 3^3 - 1, 3^3\} = \{25, 26, 27\} \)

\( M = 25 \times 26 \times 27 = 17550 \)

\( (x_1, x_2, x_3) = (0, 12, 14) \) is even, so

\[ c' = \frac{14 + 0 - 24 + 46}{2} = 18 \]

and

\[ b' = \frac{-42 + 48 - 0 + 58}{2} = 32 \]

Therefore,

\[ X = \left[ 18 \times 5^6 + 32 \times 3^5 + 14 \right]_{17550} = 14000 \]

It is easy to see that Theorem 1 is very simpler than CRT or MRC. Also Theorem 1 enables us to implement a fully parallel reverse converter for the moduli set \( \{r^2 - 2, r^2 - 1, r^2\} \).

Hardware realization of the proposed reverse converter is based on equations (9)-(11). The computation of (10) requires an \( n \)-digit radix-\( r \) carry save adder (CSA) followed by two \( n \)-digit radix-\( r \) adder and a multiplexer. We check whether \((x_1 + x_3)\) is odd or even by using radix-\( r \) XOR gates. Instead of direct division by 2, we used the multiplication by 2 – 1 and as noted in [18], this multiplication can be performed by existing radix-\( r \) multiplier belonging to the RNS processing hardware. Equation (11) has a similar realization and can be implemented with a CSA tree, two adders, one multiplexer and one multiplier for performing multiplication by 2 – 1. Since \( r_1 \) is an \( n \)-digit radix-\( r \) number, no additional hardware is needed to compute \((r^2 b' + x_3)\). The desired result is the concatenation of \( x_1 \) and \( b' \). Finally, a \( 3n \)-digit radix-\( r \) modular adder is used to perform the addition of \( r^3 c' \) and \((r^2 b' + x_3)\). Fig. 1 shows the hardware architecture of the proposed reverse converter.

IV. PERFORMANCE EVALUATION

The reverse converter proposed in this paper is a novel converter dedicated to the moduli set \( \{r^2 - 2, r^2 - 1, r^2\} \). Therefore, to verify the performance of this converter, it has to be compared with other proposed converters which can convert residue numbers to their equivalent radix-\( r \) weighted representation. Such reverse converters are presented in [19] and [18]. In [19] a CRT-based reverse converter for the moduli set \( \{r^2 - 2, r^2 - 1, r^2\} \) was presented. In [18] four three-moduli sets \( s_1=\{r^2 - 1, r^2 + 1, r^2 + 1\}, s_2=\{r^2 - 1, r^2 + 1, r^2 - 1\}, s_3=\{r^2 - 1, r^2 + 1, r^2 - 1\} \) and \( s_4=\{r^2 - 1, r^2 - 1, r^2 - 1\} \) are proposed and also a conversion algorithm based on CRT with scale-down factors is presented. Since the hardware requirements and conversion speed for the moduli sets \( s_1 \) and \( s_3 \) are the same as the moduli sets \( s_2 \) and \( s_4 \), respectively, we confine our comparison to the reverse converter for moduli sets \( s_1 \) and \( s_3 \). All the hardwares listed in Table I, are radix-\( r \) hardware. An overview of MVL circuits’ implementation can be found in [20], [21]. It should be noted the radix-\( r \) full adder (FA) cell is a \( r \)-input adder cell. Therefore, a radix-\( r \) CSA tree includes \( r \)-to-2 CSA's. Since the CSA tree used in Fig. 1 has 8 inputs, the maximum levels of \( r \)-to-2 CSA in CSA tree is two. So, the total delay of the CSA tree used in Fig. 1 is the delay of two radix-\( r \) FA. Also for \( r=3 \), this CSA tree consists of three 4-to-2 radix-3 CSA and for greater values of \( r \) (\( r>3 \)), it consists of two \( r \)-to-2 CSA. For comparison with other converters, we consider the worst case \( (r=3) \) for CSA tree. The hardware requirements and conversion delays of the reverse converters listed in Table I and II, respectively. It should be noted that we used some radix-\( r \) NOT and XOR gates for calculating negative numbers and checking the value of \((x_1 + x_3)\) for odd or even, respectively. Since these gates are not on the critical delay path and their cost are small, we don't taking into
account these gates in Table I and II.

It has been assumed that $T_{FA}, T_{MUX}, T_{MUL},$ and $T_{MOA}$ refer to the delays of the radix-$r$ full adder, multiplexer, multiplier and mod $M$ modular adder, respectively.

It is clear from Table I and II that the area and delay of the proposed converter are considerably better than the other converters. Our proposed converter is very faster and results to hardware savings when compared with the converters of [18] and [19]. It must be noted that for a specified dynamic range, the value of $n$ for our reverse converter is smaller than the $n$ for reverse converters of [18].

V. CONCLUSION

In this paper, we proposed a fully parallel reverse conversion algorithm for the moduli set $\{r^n - 2, r^n - 1, r^n\}$, based on simple mathematical relationships. Our proposed conversion algorithm is very simple and resulted to an efficient hardware realization of the reverse converter. In comparison with other reverse converters for MVL based RNS systems, the presented converter has a superior area-time complexity.

REFERENCES


Fig. 1 Block diagram of the proposed reverse converter.

### Table I Comparison of Hardware Requirements

<table>
<thead>
<tr>
<th>Moduli Set</th>
<th>CSA</th>
<th>Adder</th>
<th>Subtractor</th>
<th>Total FA's</th>
<th>Modular Adder (3n)</th>
<th>Multiplier (n)</th>
<th>Multiplexer</th>
</tr>
</thead>
<tbody>
<tr>
<td>[19]</td>
<td>{r^n - 2, r^n - 1, r^n}</td>
<td>--</td>
<td>--</td>
<td>12n</td>
<td>1</td>
<td>3</td>
<td>--</td>
</tr>
<tr>
<td>[18]</td>
<td>{r^n+1, r^n+1, r^n+1}</td>
<td>--</td>
<td>--</td>
<td>13n</td>
<td>1</td>
<td>3</td>
<td>--</td>
</tr>
<tr>
<td>[18]</td>
<td>{r^n, r^n, r^n}</td>
<td>--</td>
<td>--</td>
<td>21n</td>
<td>1</td>
<td>3</td>
<td>--</td>
</tr>
<tr>
<td>Proposed</td>
<td>{r^n - 2, r^n - 1, r^n}</td>
<td>4</td>
<td>4</td>
<td>8n</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

### Table II Comparison of Conversion Delays

<table>
<thead>
<tr>
<th>Moduli Set</th>
<th>Conversion Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>[19]</td>
<td>(5n)T_{FA} + T_{MUL} + T_{MOA}</td>
</tr>
<tr>
<td>[18]</td>
<td>(6n)T_{FA} + T_{MUL} + T_{MOA}</td>
</tr>
<tr>
<td>[18]</td>
<td>(6n)T_{FA} + T_{MUL} + T_{MOA}</td>
</tr>
<tr>
<td>Proposed</td>
<td>(n+2)T_{FA} + T_{MUL} + T_{MOA} + T_{MUX}</td>
</tr>
</tbody>
</table>