Further Comments on “Residue-to-Binary Converters Based on New Chinese Remainder Theorems”

Jean-Luc Beuchat

Abstract—Ananda Mohan suggested that the first New Chinese Remainder Theorem introduced by Wang can be derived from the constructive proof of the well-known Chinese Remainder Theorem (CRT) and claimed that Wang’s approach is the same as the one proposed earlier by Huang. Ananda Mohan’s proof is however erroneous and we show here that Wang’s New CRT I is a rewriting of an algorithm previously sketched by Hitz and Kaltofen.

I. INTRODUCTION

A Residue Number System (RNS) is defined by a set of \( n \) pairwise relatively prime numbers \( P_1, \ldots, P_n \in \mathbb{N} \). Let \( M = \prod_{i=1}^{n} P_i \). Then, any integer \( X \) belonging to \( \mathbb{Z}/M\mathbb{Z} = \{0, \ldots, M - 1\} \) has a unique RNS representation given by \( (x_1 = |X|_{P_1}, \ldots, x_n = |X|_{P_n}\mathrm{RNS}) \), where \( |X|_{P_i} \) denotes \( X \mod P_i \). The major advantage of the RNS, which explains its popularity in digital signal processing, is that addition, subtraction, and multiplication on large integers \( X \) and \( Y \in \mathbb{Z}/M\mathbb{Z} \) are replaced by \( n \) modular operations performed in parallel, and whose operands are bounded by the moduli \( P_i \):

\[
|X \circ Y|_M = (|x_1 \circ y_1|_{P_1}, \ldots, |x_n \circ y_n|_{P_n}),
\]

where \( \circ \) denotes addition, subtraction, or multiplication. However, an RNS is not a positional number system, thus making conversion to integer, comparison, and division difficult to perform. The constructive proof of the Chinese Remainder Theorem (CRT) provides an algorithm to design a residue-to-binary converter:

\[
X = \sum_{i=1}^{n} s_i \frac{x_i}{|s_i|_{P_i}} \mod M,
\]

where \( s_i = M/P_i \) and \( |1/s_i|_{P_i} \) is the multiplicative inverse of \( s_i \) modulo \( P_i \). The main drawback of this approach is that it requires multiplication by the \( s_i \)'s, which are large numbers, and modulo \( M \) operations. The Mixed Radix System (MRS) associated with each RNS offers another conversion scheme. A number \( X \in \mathbb{Z}/M\mathbb{Z} \) is represented by an \( n \)-tuple \((x'_1, x'_2, \ldots, x'_n)\mathrm{MRS}\) such that \( X = x'_1 + x'_2 P_1 + x'_3 P_1 P_2 + \ldots + x'_n P_1 P_2 \cdots P_{n-1} \) and \( x'_i < P_i \) for all \( i \in \{1, \ldots, n\} \). The Mixed Radix Conversion (MRC) is however a strictly sequential process.

II. HUANG’S ALGORITHM

Huang proposes a way to compute Equation (1) without modulo \( M \) operations [3]. He defines

\[
X_i = s_i \frac{x_i}{|s_i|_{P_i}}.
\]

By noting that

\[
|X_i|_{P_j} = \begin{cases} x_i & \text{if } i = j, \\ 0 & \text{otherwise}, \end{cases}
\]

and

\[
X_1 = (x_1, 0, \ldots, 0, 0)\mathrm{RNS},
X_2 = (0, x_2, 0, \ldots, 0, 0)\mathrm{RNS},
\ldots = \ldots,
X_n = (0, 0, 0, \ldots, 0, x_n)\mathrm{RNS},
\]

Huang suggests to compute the MRS representations of the \( X_i \)'s by means of tables. Let \( x'_{i,j} \) denote the \( j \)th MRS digit of \( X_i \). It is worth noticing that \( x'_{i,j} = 0 \) when \( j < i \):

\[
X_1 = (x'_{1,1}, x'_{1,2}, x'_{1,3}, \ldots, x'_{1,n-1}, x'_{1,n})\mathrm{MRS},
X_2 = (0, x'_{2,2}, x'_{2,3}, \ldots, x'_{2,n-1}, x'_{2,n})\mathrm{MRS},
\ldots = \ldots,
X_n = (0, 0, 0, \ldots, 0, x'_{n,n})\mathrm{MRS}.
\]

Szabo and Tanaka’s algorithm [5] allows one to determine all the MRS digits of \( X_i \) from \( x_{i,j} \). Since \( x'_{1,1} = x_1 \) [5], this conversion step requires \( n(n+1)/2 - 1 \) tables. The addition of the \( X_i \)'s is then performed in the MRS. Recall that the sum of two digits of weight \( P_1 \ldots P_i \) generates a carry \( v \) if it can.
be written as \( u + vP_{t+1} \), with \( u < P_{t+1} \). At the end of this addition process, Huang gets:
\[
X = |x'_1 + x'_2 P_1 + \ldots + x'_n P_{n-1} + qM|_M
= x'_1 + x'_2 P_1 + \ldots + x'_n P_{n-1},
\]
where \( q \in \mathbb{N} \) is the output carry. Since arithmetic is performed modulo \( M \), \( qM \) vanishes and Huang obtains eventually the MRS digits of \( X \).

**Example 1** Let \( P_1 = 11 \), \( P_2 = 13 \), and \( P_3 = 17 \). The RNS representation of \( X = 514 \) is then \( X = (8, 7, 4)_\text{RNS} \). The \( X_i \)'s are defined by:
\[
(8, 0, 0)_\text{RNS} = (8, 4, 12)_\text{MRS} = 1768, \\
(0, 7, 0)_\text{RNS} = (0, 3, 5)_\text{MRS} = 748, \\
(0, 0, 4)_\text{RNS} = (0, 0, 3)_\text{MRS} = 429.
\]
Let us compute the sum of the \( X_i \)'s in MRS. By propagating the carries, we eventually obtain the MRS digits of \( X \):
\[
X = |8 + 7 \cdot P_1 + 20 \cdot P_1 P_2|_M \\
= |8 + 7 \cdot P_1 + (3 + P_3) \cdot P_1 P_2|_M \\
= |8 + 7 \cdot P_1 + 3 \cdot P_1 P_2 + P_1 P_2 P_3|_M \\
= 8 + 7 \cdot P_1 + 3 \cdot P_1 P_2 \\
= (8, 7, 3)_\text{MRS} = 514.
\]

### III. Hitz and Kaltofen’s Remark

The main drawback of Huang’s method lies in the \( n(n + 1)/2 - 1 \) tables involved in the conversion of the \( X_i \)'s from RNS to MRS. Hitz and Kaltofen [4] suggest to carry out the products \( |x_i|/s_i|_{P_i} \) by means on \( n \) modular multipliers, where the constants \( |1/s_i|_{P_i} \) are precomputed. Then, they look at the MRS representation of the constants \( s_i = (s_{i,1}, \ldots, s_{i,n})_\text{MRS} \), and evaluate Equation (1) in MRS. Since \( s_i \) is a product of moduli, we know that \( s_{i,j} = 0 \) if \( j < i \). Furthermore, the MRS representation of \( s_n = M/P_n \) is \((0, \ldots, 0, 1)_\text{MRS} \). Thus, \( n(n + 1)/2 - 1 \) multiplications are required in this step. Then, it suffices to compute the sum of the \( s_i \cdot |x_i|/s_i|_{P_i} \) in MRS in order to get the MRS digits of \( X \). Hitz and Kaltofen describe an architecture which efficiently deals with the carries to perform this task in [4].

**Example 2 (Example 1 continued)** Let us apply Hitz and Kaltofen’s approach to convert \( X = (8, 7, A)_\text{RNS} \). First of all, we compute the products \( |x_i|/s_i|_{P_i} \) and obtain:
\[
|x_1|/s_1|_{P_1} = 8, \quad |x_2|/s_2|_{P_2} = 4, \quad |x_3|/s_3|_{P_3} = 3.
\]
The MRS representations of the \( s_i \)'s are given by:
\[
s_1 = (1, 7, 1)_\text{MRS} = 221, \\
s_2 = (0, 4, 1)_\text{MRS} = 187, \\
s_3 = (0, 0, 1)_\text{MRS} = 143.
\]

Thus,
\[
X = 8 \cdot (1, 7, 1)_\text{MRS} + 4 \cdot (0, 4, 1)_\text{MRS} + 3 \cdot (0, 0, 1)_\text{MRS} \\
= [8 + 72 \cdot P_1 + 15 \cdot P_1 P_2|_M \\
= [8 + 7 \cdot P_1 + 20 \cdot P_1 P_2|_M \\
= [8 + 7 \cdot P_1 + 3 \cdot P_1 P_2 + P_1 P_2 P_3|_M \\
= 8 + 7 \cdot P_1 + 3 \cdot P_1 P_2 + P_1 P_2 P_3|_M \\
= (8, 7, 3)_\text{MRS} = 514.
\]

Hitz and Kaltofen also point out that the multiplications by the \( x_i \)'s could be saved thanks to the second form of the CRT:
\[
X = \sum_{i=1}^{n} \frac{1}{s_i|_{P_i}} \cdot x_i \mod M.
\]
Since
\[
\frac{1}{s_i|_{P_i}} = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise},
\end{cases}
\]
we obtain another formula to compute \( X \) from the \( x_i \)'s:
\[
X = |x_1 \cdot (1, 0, 0, \ldots, 0, 0)_\text{RNS} + x_2 \cdot (0, 1, 0, \ldots, 0, 0)_\text{RNS} + \ldots + x_n \cdot (0, 0, 0, \ldots, 0, 1)_\text{RNS}|_M.
\]
The disadvantage of this approach is that the \( s_i |1/s_i|_{P_i} \)'s are larger than the \( s_i \)'s, thus leading to larger carries [4]. Therefore, Hitz and Kaltofen did not further investigate this solution. We will prove in the next section that this algorithm turns out to be Wang’s New CRT I. It is worth noticing that Huang stores the MRS digits of all numbers belonging to \( \mathbb{Z}/M\mathbb{Z} \), whereas Hitz and Kaltofen only need the MRS digits of the \( s_i \)'s or \( |1/s_i|_{P_i} \)'s (\( n(n + 1)/2 \) numbers).

**Example 3 (Example 1 continued)** Let us now convert \( X = (8, 7, 4)_\text{RNS} \) according to the second form of the CRT given by Equation (2). Szabo and Tanaka’s algorithm allow us to compute the MRS digits of the constants \( s_1 |1/s_1|_{P_1} \):
\[
s_1 |1/s_1|_{P_1} = (1, 7, 1)_\text{MRS} = 221, \\
s_2 |1/s_2|_{P_2} = (0, 6, 10)_\text{MRS} = 1496, \\
s_3 |1/s_3|_{P_3} = (0, 0, 5)_\text{MRS} = 715.
\]

Thus, we have
\[
X = 8 \cdot (1, 7, 1)_\text{MRS} + 7 \cdot (0, 6, 10)_\text{MRS} + 4 \cdot (0, 0, 5)_\text{MRS} \\
= [8 + 98 \cdot P_1 + 98 \cdot P_1 P_2|_M \\
= [8 + 7 \cdot P_1 + 105 \cdot P_1 P_2|_M \\
= [8 + 7 \cdot P_1 + 3 \cdot P_1 P_2 + 6 \cdot P_1 P_2 P_3|_M \\
= (8, 7, 3)_\text{MRS} = 514.
\]
IV. Wang’s New CRT I Revisited

Wang’s New CRT I is based on the following identity [1]:

\[ X = |x_1 + k_1(x_2 - x_1)P_1 + k_2(x_3 - x_2)P_2 + \ldots + k_{n-1}(x_n - x_{n-1})P_1 \ldots P_{n-1}|_M, \]  

(3)

where

\[ k_i = \left\lfloor \frac{1}{\prod_{j=1}^{i-1} P_j \prod_{j=i+1}^{n} P_j} \right\rfloor, \]  

(4)

with \( 1 \leq i \leq n - 1 \). According to Wang, the New CRT I is a fast conversion algorithm substantially different from the CRT approach. Let us prove that Equation (3) is a rewriting of the CRT defined by Equation (2). Consider three pairwise prime integers \( a, b, \) and \( c \). The following property holds:[1]

\[ a \left\lfloor \frac{1}{ac} \right\rfloor_b = \left\lfloor \frac{1}{c} \right\rfloor_{ab} - b \left\lfloor \frac{1}{bc} \right\rfloor_{a \cdot b}. \]  

(5)

If \( a = P_2 \ldots P_n, b = P_1, \) and \( c = 1 \), we have:

\[ s_1 \left\lfloor \frac{1}{s_1} \right\rfloor_{P_1} = a \left\lfloor \frac{1}{ac} \right\rfloor_b = 1 - P_1 \left\lfloor \frac{1}{P_1 P_2 \ldots P_n} \right\rfloor_{P_1 \ldots P_n} = 1 - k_1 P_1 \mid P_1 \ldots P_n. \]

Assume now that \( 2 \leq i \leq n - 1, a = P_{i+1} \ldots P_n, b = P_i, \) and \( c = P_i \ldots P_{i-1} \). We obtain:

\[ s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} = a \left\lfloor \frac{1}{ac} \right\rfloor_b \cdot P_i \ldots P_{i-1} = \mid k_{i-1} - k_i P_i \mid P_i \ldots P_n \cdot P_1 \ldots P_{i-1}. \]

Eventually, we note that:

\[ s_n \left\lfloor \frac{1}{s_n} \right\rfloor_{P_n} = \left\lfloor \frac{1}{P_1 \ldots P_{n-1} P_n} \right\rfloor_{P_1 \ldots P_{n-1}} = k_{n-1} \cdot P_1 \ldots P_{n-1}. \]

Starting from Wang’s New CRT I, we have:

\[ X = |x_1 + k_1(x_2 - x_1)P_1 + k_2(x_3 - x_2)P_2 + \ldots + k_{n-1}(x_n - x_{n-1})P_1 \ldots P_{n-1}|_M \]

\[ = \mid (1 - k_1 P_1)x_1 + (k_1 - k_2 P_2)x_2 P_1 + \ldots + (k_{n-2} - k_{n-1} P_{n-1})x_{n-1} P_1 \ldots P_{n-2} + k_{n-1} P_{n-1} \mid M \]

\[ = \mid 1 - k_1 P_1 x_1 + k_1 - k_2 P_2 x_2 P_1 + \ldots + k_{n-2} - k_{n-1} P_{n-1} x_{n-1} P_1 \ldots P_{n-2} + k_{n-1} x_{n-1} P_1 \ldots P_{n-1} |_M \]

\[ = \sum_{i=1}^{n} s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} x_i \mod M, \]

which is the second form of the CRT defined by Equation (2). Note that the \( k_i \)'s are the MRS digits of numbers congruent to the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s modulo \( M \). We have:

\[ s_1 \left\lfloor \frac{1}{s_1} \right\rfloor_{P_1} \equiv \{1, -k_1, 0, \ldots, 0\}_{MRS} \mod M, \]

\[ s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \equiv \{0, \ldots, 0, k_{i-1}, -k_i, 0, \ldots, 0\}_{MRS} \mod M, \]

\[ s_n \left\lfloor \frac{1}{s_n} \right\rfloor_{P_n} \equiv \{0, \ldots, 0, k_{n-1}\}_{MRS} \mod M, \]

where \( 2 \leq i \leq n - 1 \). Therefore, Ananda Mohan is wrong when he writes in [2] that Wang suggests to use the MRS representation of the \( X_i \)'s, which is the technique described by Huang. We give two examples to illustrate that Wang rediscovered the second form of the CRT (Equation (2)) and that the explicit computation of the \( k_i \)'s is useless.

Example 4 (Example 1 continued) Let us convert now \( X = (8, 7, 4)_{RNS} \) according to Equation (3). We find that \( k_1 = 201 \) and \( k_2 = 5 \). We easily check that:

\[ s_1 \left\lfloor \frac{1}{s_1} \right\rfloor_{P_1} = (1, 7, 1)_{MRS} \equiv (1, -201, 0)_{MRS} \mod M, \]

\[ s_2 \left\lfloor \frac{1}{s_2} \right\rfloor_{P_2} = (0, 6, 10)_{MRS} \equiv (0, 201, -5)_{MRS} \mod M, \]

\[ s_3 \left\lfloor \frac{1}{s_3} \right\rfloor_{P_3} = (0, 0, 5)_{MRS}. \]

In order to avoid a multiplication by 201, Wang recommends to work with the following set of constants [1]:

\[ a_i = \begin{cases} |1 - k_1 P_1|_{P_1 P_2 \ldots P_n} & \text{if } i = 0, \\ |k_i - k_{i+1} P_{i+1} \ldots P_n|_{P_1 \ldots P_{i-1}} & \text{if } 1 \leq i \leq n - 2, \\ |k_{n-1}|_{P_{n-1}} & \text{if } i = n - 1. \end{cases} \]

He suggests to compute the MRS digits of \( a_0 \) and \( a_i \prod_{j=1}^{i} P_j \), \( 1 \leq i \leq n - 1 \). From the previous results, it is obvious that these numbers are nothing but the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s. Therefore, Wang performs the following operations:

1) computation of the \( k_i \)'s, i.e. the MRS digits of numbers congruent to the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s modulo \( M \);
2) computation of the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s from the \( k_i \)'s;
3) computation of the MRS digits of the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s according to Szabo and Tanaka's algorithm.

Since the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s only depend on the moduli set, it not necessary to compute the \( k_i \)'s.

Example 5 Wang et al. [7] proposed a converter for the RNS defined by \( P_1 = 2^a, P_2 = 2^b + 1, \) and \( P_3 = 2^c - 1 \). They explained that the \( k_i \)'s of the New CRT I allowed them to achieve better performance in terms of speed and area. Let us show that the same result can be obtained without computing the \( k_i \)'s. Szabo and Tanaka’s conversion algorithm [5] provides us with the MRS digits of the \( s_i \left\lfloor \frac{1}{s_i} \right\rfloor_{P_i} \)'s:

\[ (1, 0, 0)_{RNS} = (1, 1, 2^{n} - 2)_{MRS}, \]

\[ (0, 1, 0)_{RNS} = (0, 2^{n}, 2^{n-1} - 1)_{MRS}, \]

\[ (0, 0, 1)_{RNS} = (0, 0, 2^{n-1})_{MRS}. \]

In the following, we keep the somewhat confusing notation used by Wang et al. [7]: \( x_1 = \lfloor X \rfloor_{P_0}, x_2 = \lfloor X \rfloor_{P_1}, \) and \( x_3 = \]

---

1In order to prove this equality, it suffices to consider the solutions of the Diophantine equation \( ax + by = |1/c|_{ab} \). See for instance [6] for details.
\[ \lvert X \rvert_{P_2} \text{. We have:} \]
\[
X = \left\lfloor x_2 \cdot (1, 0, 0)_{\text{RNS}} + x_3 \cdot (0, 1, 0)_{\text{RNS}} + \\
x_1 \cdot (0, 0, 1)_{\text{RNS}} \right\rfloor_M
\]
\[
= \left\lfloor x_2 + (x^2 + x_3 \cdot 2^n) \cdot 2^n + (x_1 \cdot 2^{n-1} + \\
x_2 \cdot (2^n - 2) + x_3 \cdot (2^{n-1} - 1)) \cdot 2^n \cdot (2^n + 1) \right\rfloor_M
\]
\[
= \left\lfloor x_2 + (x^2 + x_3 \cdot (2^n + 1) - x_3) \cdot 2^n + (x_1 \cdot 2^{n-1} + \\
x_2 \cdot (-2^n) + x_3 \cdot (2^{n-1} - 1)) \cdot 2^n \cdot (2^n + 1) \right\rfloor_M
\]
\[
= x_2 + 2^n \cdot \left( (x_2 - x_3) + \\
(x_1 - 2x_2 + x_3) \cdot 2^{n-1} \cdot (2^n + 1) \right)_{2^n-1},
\]

which is the formula obtained by Wang et al. (see Equation (7) in [7]).

V. Conclusion

We proved that the New CRT I was solely based on the original CRT, of which it was only a mere rewriting, and that Wang rediscovered an algorithm sketched by Hitz and Kaltofen in [4]. We also explained why the comment on the New CRT I by Ananda Mohan [2] is erroneous.

References

[1] Y. Wang, “Residue-to-binary converters based on new Chinese remainder theorems,” IEEE Trans. Circuits Syst. II, vol. 47, no. 3, pp. 197–205, Mar. 2000.
[2] P. V. Ananda Mohan, “Comments on ”Residue-to-binary converters based on new Chinese remainder theorems”,“ IEEE Trans. Circuits Syst. II, vol. 47, no. 12, p. 1541, Dec. 2000.
[3] C. H. Huang, “A fully parallel mixed-radix conversion algorithm for residue number applications,” IEEE Trans. Comput., vol. C–32, no. 4, pp. 398–402, Apr. 1983.
[4] M. A. Hitz and E. Kaltofen, “Integer division in residue number systems,” IEEE Trans. Comput., vol. 44, no. 8, pp. 983–989, Aug. 1995.
[5] N. S. Szabo and R. I. Tanaka, Residue Arithmetic and its Applications to Computer Technology. New York: McGraw-Hill, 1967.
[6] J. von zur Gathen and J. Gerhard, Modern Computer Algebra, 2nd ed. Cambridge University Press, 2003.
[7] Y. Wang, X. Song, M. Aboulhamid, and H. Shen, “Adder based residue to binary number converters for \((2^n - 1, 2^n, 2^n + 1)\),” IEEE Trans. Signal Processing, vol. 50, no. 7, pp. 1772–1779, July 2002.