This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

Extended Closed-form Expressions for the Robust Symmetrical Number System Dynamic Range and an Efficient Algorithm for its Computation

Phillip E. Pace *Senior Member, IEEE*, Pantelimon Stănică, Brian L. Luke,
Thomas W. Tedesso *Student Member, IEEE*

***Abstract*—The robust symmetrical number system (RSNS) is a number theoretic transform based on $N \geq 2$ sequences that can extract the maximum amount of information from symmetrical folding waveforms. The sequences, based on coprime moduli, exhibit an integer Gray code property making the RSNS well-suited for many applications that benefit from an inherent error detection and correction capability such as analog-to-digital converters, direction finding arrays and radar waveform design. To use the RSNS, it is necessary to know the greatest length of combined sequences without ambiguities, called the dynamic range $\widehat{M}$, for which only a few closed-form expressions currently exist. In this paper, an efficient algorithm for computing $\widehat{M}$ and its position within the combined set of sequences is presented and shown to be independent of the size of the moduli. The algorithm is used to generate the equations for several groups of additional moduli arrangements. Closed form expressions for $\widehat{M}$ are conjectured and proved using the obtained congruence equations that define the ambiguity locations.**

I. Introduction

THE most common type of waveform in engineering science is the symmetrical folding waveform (e.g., sinusoids). Symmetrical folding waveforms appear naturally in many engineering disciplines and system analysis techniques. To extract the maximum amount of information from symmetrical folding waveforms, symmetrical number systems, each consisting of $N \geq 2$ integer sequences, were formulated based on coprime modular systems. Symmetrical number systems include the *symmetrical number system* (SNS), the *optimum symmetrical number system* (OSNS) and the *robust symmetrical number system* (RSNS). To effectively utilize symmetrical number systems, the dynamic range, $\widehat{M}$, defined as the greatest length of distinct, paired sequences ($N-$tuples) that contain no ambiguities, as well as its beginning position within the combined $N-$sequences must be known. Closed-form expressions for $\widehat{M}$ have been reported for the SNS and the OSNS in [1] and [2], respectively. Unlike the SNS and OSNS, a general closed-form expression for the RSNS $\widehat{M}$ does not exist and closed-form expressions have only been reported for a limited number of specific cases [3]–[5]. As a result, the use of an algorithm is required to determine $\widehat{M}$ and the beginning position of the sequence for moduli sets that are not covered by the limited number of cases.

The RSNS has an inherent integer Gray code property that makes the RSNS particularly attractive for error control in both analog and digital signal processing applications. The RSNS has been shown to be useful in software radio systems for sample rate conversion [6], and in electronic [7], [8], photonic [9] and superconducting [10] folding analog-to-digital converters. Due to the inherent symmetry within the modulus, a new theoretic transform for error detection and control was reported in [11] and applied to code division multiple access wireless communications [12]. The complexity of direction finding antenna systems is also reduced through use of the RSNS by decomposing the spatial filtering operation into a number of parallel sub-operations [13]. Consequently, each sub-operation only requires a complexity in accordance with that modulus and a much higher spatial resolution is achieved after the results of these less complex sub-operations are recombined. The use of the RSNS in radar waveform design has also been reported in [14] to extend the capabilities for target detection.

In this paper, we present an efficient algorithm to compute the $\widehat{M}$ and its beginning position within the sequence, for a general set of N coprime moduli. The algorithm is derived by considering the location and distance between all of the vector ambiguity pairs for the combined $N-$sequences. To simplify our derivation, we define the center of ambiguity (COA) as the midpoint between the ambiguity pairs. Analysis of all the ambiguity pairs leads to an upper bound on $\widehat{M}$ that is used to improve the algorithm's efficiency. An $N = 3$ example is provided to demonstrate the steps of the algorithm. Also, the algorithm's complexity is computed and compared to that of a naïve search approach. We demonstrate that our algorithm's complexity is independent of the moduli size and represents an improvement by several orders of magnitude when compared to the naïve search approach. Our algorithm is then applied to several different groups of moduli sets and is used to generate additional closed-form expressions for $\widehat{M}$. The closed-form expressions for $\widehat{M}$ are developed for several additional $N = 3$ and $N = 4$ cases and are verified by deriving the closed-form

P. E. Pace is with the Dept. of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA; Email: pepace@nps.edu

P. Stănică is with the Dept. of Applied Mathematics, Naval Postgraduate School, Monterey, CA; Email: pstanica@nps.edu

B. L. Luke is with the Navy Cyber Defense Operations Command, Virginia Beach, VA; Email: brian.luke@navy.mil

T. W. Tedesso is a Ph.D. candidate with the Dept. of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA; Email: twtedess@nps.edu.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Extended Closed-form Expressions for the Robust Symmetrical Number System Dynamic Range and an Efficient Algorithm for its Computation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Department of Electrical and Computer Engineering,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
IEEE Transactions on Information Theory 60:3 (2014), 1-11.

14. ABSTRACT

The robust symmetrical number system (RSNS) is a number theoretic transform based on N 2 sequences that can extract the maximum amount of information from symmetrical folding waveforms. The sequences, based on coprime moduli, exhibit an integer Gray code property making the RSNS well-suited for many applications that benefit from an inherent error detection and correction capability such as analog-to-digital converters, direction finding arrays and radar waveform design. To use the RSNS, it is necessary to know the greatest length of combined sequences without ambiguities, called the dynamic range cM, for which only a few closed-form expressions currently exist. In this paper, an efficient algorithm for computing cM and its position within the combined set of sequences is presented and shown to be independent of the size of the moduli. The algorithm is used to generate the equations for several groups of additional moduli arrangements. Closed form expressions for cM are conjectured and proved using the obtained congruence equations that define the ambiguity locations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**11**	

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

expressions from the congruence equations.

The paper is structured as follows. In Section II, we briefly review the RSNS formulation. In Section III, RSNS ambiguities are introduced. In Section IV, minimal ambiguity pairs are defined and a series of lemmas and theorems are presented that provide the details of our algorithm and the efficiency of our solution. An $N = 3$ example is also provided to demonstrate the steps of the algorithm. In Section V, the algorithm's run time complexity is compared to that of a naïve search approach. The complexity for both computations is derived demonstrating the algorithm efficiency and its independence from the size of the N moduli. In Section VI, the results for several groups of moduli sets are used to generate an extended group of closed-form expressions for $\widehat{M}$. In section VII, we provide concluding remarks and areas of further research.

Throughout this paper, we use the Vinogradov symbols $\gg$, $\ll$ and the Landau symbols O, o with their usual meanings. We recall that $f \ll g$, $g \gg f$ and $f = O(g)$ are all equivalent and mean that $|f(x)| < c|g(x)|$ holds with some constant c, for x sufficiently large. Also, $f = o(g)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. For a positive real number x we write $\log x$ for the maximum between 2 and the natural logarithm of x.

II. Robust Symmetrical Number System

The RSNS is a modular based number system consisting of $N \geq 2$ integer sequences with each sequence associated with a coprime modulus, m_i. The RSNS is based on the following sequence:

$$\left\{x_m^{'}\right\} = [0, 1, 2, \ldots, m-1, m, m-1, \ldots, 2, 1]. \quad (1)$$

To form the $N-$sequence RSNS, each term in (1) is repeated N times in succession. Therefore, the integers within one folding period of a sequence are:

$$\begin{aligned}\{x_m\} =&[0, \ldots, 0, 1, 1, \ldots, 1, \ldots, m-1, \ldots, m-1,\\ &m, \ldots, m, m-1, \ldots, m-1, \ldots, 1, \ldots, 1].\end{aligned} \quad (2)$$

This results in a periodic sequence with a period of $P_m = 2Nm$ [4], [9]. Each sequence corresponding to m_i is also shifted left (or right) by $s_i = i - 1$ where $i \in \{1, 2 \ldots, N\}$ and the shift values, $s_i = \{s_1, s_2, \ldots, s_N\}$, form a complete residue system modulo N. The resulting structure of the N sequences ensures that two successive RSNS vectors (paired terms from all N sequences) when considered together, differ by only one integer resulting in an acyclic integer Gray code property [4], [15]. Although the RSNS is cyclic and has integer Gray code properties, it differs from an (m, N)-Gray code in the following ways: all the $N-$tuples in an RSNS are not distinct, and the maximum value of each element in an $N-$tuple is not m, but rather m_i, where i represents the elements of the $N-$tuple [0, 1, …, $N-1$].

Each sequence is extended periodically with period $2Nm$ as $x_{h+n2Nm} = x_h$ where $n \in \{0, \pm1, \pm2, \ldots\}$. Therefore, x_h is a symmetrical residue of $(h + n2Nm)$ modulo $2Nm$. An integer, h, is represented by a vector, $X_h = [x_{1,h}, x_{2,h}, \ldots, x_{N,h}]^T$, of N paired integers from each sequence at h. For example, a left-shifted, three-sequence RSNS with $m_i = \{3, 4, 5\}$ is displayed in Table I and Fig. 1. The integer, $h = 5$, is represented by the vector, $X_h = [1, 2, 2]^T$. Also the integer Gray code property is evident.

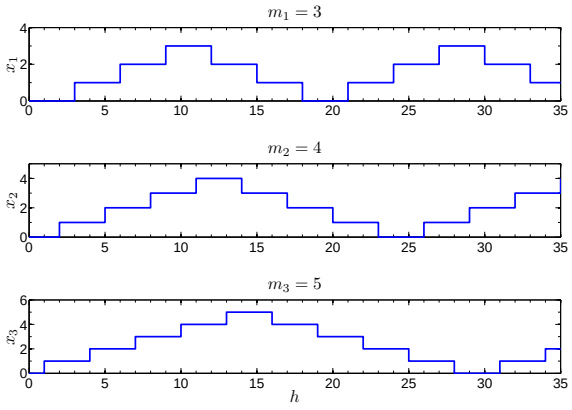

Fig. 1. RSNS structure for $m_i = \{3, 4, 5\}$.

Since the integer values within each modulus consists of $2Nm$ integers, the symmetrical residues are determined by first subtracting an integer number of $2Nm$ integers as

$$n_i = h - \left\lfloor \frac{h}{2Nm_i} \right\rfloor 2Nm_i. \quad (3)$$

The symmetrical residue x_h is then calculated as [4], [9]

$$x_h = \begin{cases} \left\lfloor \dfrac{n_i - s_i}{N} \right\rfloor, & s_i \leq n_i \leq Nm_i + s_i + 1 \\ \left\lfloor \dfrac{2Nm_i + N - n_i + s_i - 1}{N} \right\rfloor, & Nm_i + s_i + 2 \leq n_i \leq 2Nm_i + s \end{cases} \quad (4)$$

The N-sequence RSNS is periodic with a fundamental period of

$$P_f = 2NM, \quad (5)$$

where $M = \prod_{i=1}^{N} m_i$ is the dynamic range of a *residue number system* (RNS) [3], [4], [13].

Closed-form expressions for $\widehat{M}$ exists for only few specific cases. In [4], a closed-form expression for a $N = 2$ RSNS is reported, where

$$\widehat{M} = \begin{cases} 4m_1 + 2m_2 - 5, & \text{when } m_2 \leq m_1 + 2 \\ 4m_1 + 2m_2 - 2, & \text{when } m_2 \geq m_1 + 3 \end{cases} \quad (6)$$

and $5 \leq m_1 < m_2$. The other published closed-form expression for $\widehat{M}$ is when $N = 3$ and $m_i = \{m-1, m, m+1\}$ with m even and $m > 3$ [4], [13]. In this case,

$$\widehat{M} = \frac{3}{2}m^2 + \frac{15}{2}m + 7. \quad (7)$$

III. RSNS Ambiguities

In the fundamental period of an N-sequence RSNS, there are three ambiguity types, Type 0, Type 1, and Type 2 that are illustrated in Fig. 2. Type 0 ambiguities occur periodically in each sequence. Type 1 ambiguities occur across the folds of each waveform in each sequence, and Type 2 ambiguities occur due to the N sequential repeated integers within each

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

TABLE I
$N = 3$ RSNS STRUCTURE FOR $m_i = \{3, 4, 5\}$.

	h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 . . .
X_h	$m_1 = 3$	0	0	0	1	1	1	2	2	2	3	3	3	2	2	2	1	1 . . .
	$m_2 = 4$	0	0	1	1	1	2	2	2	3	3	3	4	4	4	3	3	3 . . .
	$m_3 = 5$	0	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5	4 . . .

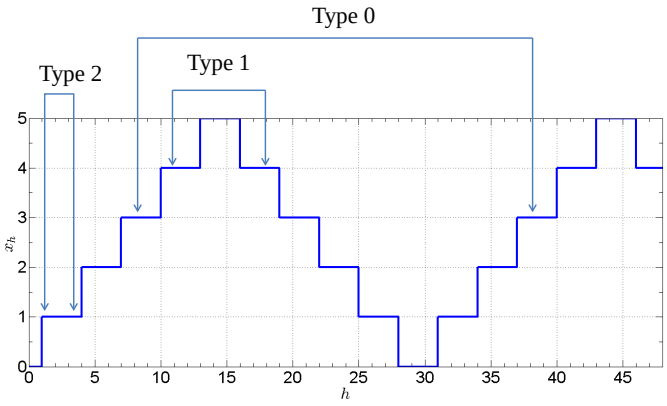

Fig. 2. Single sequence ambiguity types (N=3, m=5).

sequence. Each sequence can be decimated into N subsequences where each subsequence is composed of values from the original sequences at $h \equiv 0 \bmod N$, $h \equiv 1 \bmod N, \ldots$, and $h \equiv (N-1) \bmod N$. By examining these subsequences, the Type 2 ambiguities are eliminated leaving only Type 0 and Type 1 ambiguities [4]. Subsequently, the complexity of the problem of determining $\widehat{M}$ is reduced. Table II illustrates the subsequence structure for a single sequence of a $N = 3$ RSNS. By analyzing the parity of the RSNS in Table I, it can be shown that the parity of the sequence repeats at a period of $2N$ [4], [16].

The ambiguity locations can be determined by solving the congruence equations for each combination of Type 0 and Type 1 ambiguities that exist. To determine $\widehat{M}$, the ambiguity locations are determined by solving congruence equations for all combinations of Type 1 and Type 0 ambiguities, and the largest span of unambiguous values is identified, which is equal to $\widehat{M}$. The various combinations of Type 1 and Type 0 ambiguities are referred to by three digit *Case Numbers* where the first digit refers to the number of Type 1 ambiguities that exist and ranges from zero to N. The second digit represents the particular assignment of Type 0 and Type 1 ambiguities to specific sequences, and third digit of the case number represents the subsequence index and ranges from zero to $N-1$ [4]. For example, for an $N = 3$ RSNS, in Case 220, the 2 as the first digit specifies that there are two Type 1 ambiguities (and therefore one Type 0 ambiguity) for the three sequences. The 2 as the second digit signifies that the particular order of the ambiguities is the second largest binary value $(101_2 = 5)$. The 0 in the third digit of the example case label indicates that the ambiguities are computed for the 0^{th} subsequence only (see [4], [16] for further details). Table III summarizes the solution to the congruence equations and defines the COA for all possible case numbers for an N-sequence RSNS [4], [16].

In Table III, the value of h_s is determined by solving a set of congruence equations using the Chinese Remainder Theorem (CRT). The congruence equations are generated from a matrix that is formed by collecting the Type 1 symmetrical residue numerators into a matrix form with each column index corresponding to its associated modulus. The matrix has a unique structure where the first column is $[0, -1, -2, \ldots, -N+1]^T$ and the subsequent columns are generated by circular shifting the previous column up and incrementing each value by one [4]. The shift matrix is an $N \times N$ matrix defined as

$$h_s \implies \begin{bmatrix} 0 & 0 & \cdots & \cdots & \cdots & 0 \\ -1 & -1 & \cdots & \cdots & -1 & N-1 \\ -2 & \cdots & \cdots & -2 & N-2 & \vdots \\ \vdots & \cdots & \iddots & \iddots & \iddots & \vdots \\ -N+2 & -N+2 & \iddots & \iddots & \iddots & 2 \\ -N+1 & 1 & \cdots & \cdots & 1 & 1 \end{bmatrix}. \tag{8}$$

The congruence equations are formed based on the sequences containing the Type 1 ambiguities and the subsequences that contains the ambiguities.

IV. Efficient Algorithm for Computing $\widehat{M}$

We develop an efficient algorithm to efficiently compute $\widehat{M}$ for N RSNS integer sequences with arbitrary coprime moduli, m_i, where $m_i \geq 2$, by first considering all the minimal pair ambiguity locations (h_1, h_2). For the general $N-$sequence RSNS case, we let $C = \{(h_1, h_2) \mid 0 \leq h_1 < h_2 < P_f\}$, where $X_{h_1} = X_{h_2}$. A pair $(h_1, h_2) \in C$ is minimal if there does not exist a pair $\left(\tilde{h}_1, \tilde{h}_2\right) \in C$ such that $h_1 \leq \tilde{h}_1 < \tilde{h}_2 \leq h_2$ and if the shorter sequence length, $\tilde{h}_2 - \tilde{h}_1 < h_2 - h_1$. The largest distance between *consecutive* minimal pairs $h_2 - h_1 - 1$ is the $\widehat{M}$ and $h_1 + 1$ is the starting position of $\widehat{M}$. We will also demonstrate in Theorem 7 that $\widehat{M} < P_f$. It then follows that $\widehat{M} < M = \prod m_i$, the dynamic range of the RNS.

In [4], it was demonstrated that the distance between ambiguous vector pairs is always odd; therefore, we define the midpoint between the ambiguous vector pairs as $COA = (h_2 + h_1)/2$. Given two minimal pairs, $P_1 = (h_1, h_2) \in C$ with COA_{P_1} and $P_2 = (h_1', h_2') \in C$ with COA_{P_2} where $COA_{P_1} < COA_{P_2}$, the pairs are defined as consecutive if there does not exist a minimal pair $P_3 = (h_1'', h_2'') \in C$ with COA_{P_3} such that $COA_{P_1} < COA_{P_3} < COA_{P_2}$. Therefore, if $(h_1, h_2) \in$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

TABLE II
SINGLE SEQUENCE RSNS STRUCTURE ILLUSTRATING THREE SUBSEQUENCES FOR AN $N = 3$ RSNS.

$m_i = 3$	x_h	0	0	0	1	1	1	2	2	2	3	3	3	2	2	2	1	1	1	0
$h \equiv 0 \bmod 3$	x_h	0			1			2			3			2			1			0
$h \equiv 1 \bmod 3$	x_h		0			1			2			3			2			1		
$h \equiv 2 \bmod 3$	x_h			0			1			2			3			2			1	
	h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

TABLE III
SUMMARY OF N-SEQUENCE RSNS AMBIGUITY EXPRESSIONS. AMBIGUITIES EXIST AT h AND $h + k$. INDEX i DENOTES THE SEQUENCES WITH TYPE 1 AMBIGUITIES AND THE INDEX j DENOTES THE SEQUENCES CONTAINING TYPE 0 AMBIGUITIES.

Case Number	h is	k is a multiple of	COA
010	Anywhere in P_f	$2N\prod_{i=1}^{N} m_i$	None
$1X0$	$h = aNm_i - \frac{k}{2}$	$2N\frac{M}{m_i}$	aNm_i
$1XX$	$h = aNm_i + h_s - \frac{k}{2}$	$2N\frac{M}{m_i}$	$h_s + aNm_i$
$2X0\cdots(N-1)X0$	$h = aN\prod_i m_i - \frac{k}{2}$	$2N\prod_j m_j$	$aN\prod_i m_i$
$2XX\cdots(N-1)XX$	$h = aN\prod_i m_i + h_s - \frac{k}{2}$	$2N\prod_j m_j$	$h_s + aN\prod_i m_i$
$N10$	$h = aN\prod_{n=1}^{n=N} m_n - \frac{k}{2}$	2N	$aN\prod_{n=1}^{n=N} m_n$
$N1X$	$h = aN\prod_{n=1}^{n=N} m_n + h_s - \frac{k}{2}$	2N	$h_s + aN\prod_{n=1}^{n=N} m_n$

C and $(h_1', h_2') \in C$ are consecutive minimal pairs, then the maximal size, $\widehat{M} = (h_2 - 1) - (h_1 + 1) + 1 = h_2 - h_1 - 1$, is the dynamic range of the RSNS. Furthermore, $h_1 + 1$ is the beginning position of the dynamic range. Since $\widehat{M}$ is computed using consecutive minimal pairs $(h_1, h_2) \in C$ and $(h_1', h_2') \in C$, only the positions of the minimal pairs that can affect the length of $\widehat{M}$ are required to be computed and the rest can be ignored.

The algorithm for computing $\widehat{M}$ relies on a number of lemmas, most of which are the result of an analysis of the locations of all vector ambiguities provided in [4]. Table III summarizes the $N-$channel RSNS vector ambiguity locations. The rows in Table III separate the locations of the ambiguity pairs into seven categories based on the *type* of ambiguity.

A. Theoretical Basis for Algorithm

The basis for our efficient algorithm for determining $\widehat{M}$ is presented in a series of lemmas and theorems. From this theoretical foundation, the steps of the algorithm are developed and presented in Section IV-B.

Lemma 1. *There are 2^N distinct cases of repeated ambiguity pairs, each with a different ambiguity length and* COA *spacing. All but one of the 2^N cases have N subcases that have the same* number *of* COAs *and ambiguity* lengths *in P_f, but the* COA *for each of the subcases is shifted by a particular value, h_{s_i}.*

The N COA *shifts (one for each subcase) are computed by solving a set of N congruence equations using the CRT. The subcase where $h_{s_0} = 0$ is called the base case and is shown in rows 2, 4, and 6 in Table III.*

Proof. See the ambiguity analysis discussion in Section II of [4]. □

Lemma 2. *Minimal pairs are computed using the first multiple of k from the third column in Table III.*

Proof. Any vector pair computed using a higher multiple of k forms a vector pair that encompasses and is symmetric about the vector pair obtained using the lower multiple of k. Therefore, any vector pair computed using other than the first multiple of k is not minimal [4]. □

Lemma 3. *For every ambiguity pair with a* COA *at h, there is an ambiguity pair with the same length at $h + P_f/2$.*

Proof. Given a general *COA* for any case at

$$h = a\left(N\prod_i m_i\right), \tag{9}$$

where the subscripts i are the indices of all vector elements with Type 1 ambiguity, there is also a *COA* at $h+P_f/2$ because

$$\begin{aligned} a\left(N\prod_i m_i\right) + \frac{P_f}{2} &= a\left(N\prod_i m_i\right) + N\prod_{n=1}^{N} m_n \\ &= a\left(N\prod_i m_i\right) + N\left(\prod_i m_i \prod_j m_j\right) \\ &= \left(a + \prod_j (m_j)\right)\left(N\prod_i (m_i)\right) \\ &= b\left(N\prod_i m_i\right), \end{aligned} \tag{10}$$

where a and b are any integers, j corresponds to the vector elements with Type 0 ambiguities, and i corresponds to the vector elements with Type 1 ambiguities. The result is that ambiguity pairs are symmetric about $P_f/2$. □

Lemma 4. *There is always an ambiguity with a* COA *at $h = 0$ and $h = P_f/2$ with a length of $2N + 1$, which is also the ambiguity with the smallest length.*

Proof. This is straightforward via inspection of row 6 in Table III. □

Lemma 5. *Using Lemma 3 and Lemma 4, only ambiguities from $-N$ to $P_f/2 + N$ need to be considered when computing $\widehat{M}$.*

Proof. Since Lemma 3 showed that ambiguity pairs are symmetric about $P_f/2$, and $\widehat{M}$ is computed from minimal ambiguity pair locations, the same length $\widehat{M}$ exists from $h = 0$ to $h = P_f/2$ as exists from $h = P_f/2$ to $h = P_f$. □

Lemma 6. *[4] The dynamic range is upper bounded by*

$$\widehat{M} \leq B_{\widehat{M}} := N \min_{I \subseteq \{1,\ldots,n\}} \left[\prod_{i \in I} m_i + 2 \prod_{j \in \bar{I}} m_j \right] - 1, \quad (11)$$

where $\bar{I}$ is the set complement, that is, $\bar{I} = \{1, \ldots, n\} \setminus I$.

That is, each of the rows in Table III produce a unique set of minimal pairs and the row that has the smallest local $\widehat{M}$ (the one that minimizes (11)) provides an upper bound on $\widehat{M}$ for the RSNS. Any ambiguity pair that has a length greater than $B_{\widehat{M}}$ does not affect $\widehat{M}$ and can be ignored (i.e., $\widehat{M}$ is smaller than the distance between the minimal pair and therefore cannot be the vector pair).

As an example, let $N = 3$, $m_i = \{3, 4, 5\}$. We first compute the expressions inside the minimum of (11), for each of the 2^n subsets $I \subseteq \{1, 2, \ldots, n\}$, that is,

$$\begin{aligned} B_1 &= [1 + 2(3 \cdot 4 \cdot 5)] = 121 \\ B_2 &= [3 + 2(4 \cdot 5)] = 43 \\ B_3 &= [4 + 2(3 \cdot 5)] = 34 \\ B_4 &= [5 + 2(3 \cdot 4)] = 29 \\ B_5 &= [(3 \cdot 4) + 2(5)] = 22 \\ B_6 &= [(3 \cdot 5) + 2(4)] = 23 \\ B_7 &= [(4 \cdot 5) + 2(3)] = 26 \\ B_8 &= [(3 \cdot 4 \cdot 5) + 2(1)] = 65. \end{aligned}$$

By using Lemma 6,

$$B_{\widehat{M}} = 3 \min_i (B_i) - 1 = 3 \cdot 22 - 1 = 65.$$

Theorem 7. *Assuming $M \geq 4$, we can take as upper bound for $\widehat{M}$*

$$B_{\widehat{M}} \quad \leq \quad N\lceil 2\sqrt{2M} \rceil - 1. \quad (12)$$

Moreover, if $N \geq 3$, the dynamic range of the RSNS is always smaller than the dynamic range of the RNS, that is,

$$\widehat{M} \quad < \quad M.$$

Proof. See Appendix. □

For the case $N = 3$, we can derive an exact expression for the upper bound on $\widehat{M}$, which we do in the next lemma.

Lemma 8. *In the case of 3-channel RSNS of coprime moduli $m_1 < m_2 < m_3$, the dynamic range is upper bounded by*

$$B_{\widehat{M}} = \begin{cases} N(m_1 m_2 + 2m_3) - 1 & \text{if } \ m_1 m_2 \geq m_3 \\ N(m_3 + 2m_1 m_2) - 1 & \text{if } \ m_2 m_2 < m_3. \end{cases} \quad (13)$$

Proof. We need to minimize the expressions (from (11)):

$$\begin{aligned} \alpha_1 &= m_1 m_2 + 2m_3 \\ \alpha_2 &= m_1 m_3 + 2m_2 \\ \alpha_3 &= m_2 m_3 + 2m_1 \\ \alpha_4 &= m_1 m_2 m_3 + 2 \\ \alpha_5 &= 1 + 2m_1 m_2 m_3 \\ \alpha_6 &= m_1 + 2m_2 m_3 \\ \alpha_7 &= m_2 + 2m_1 m_3 \\ \alpha_8 &= m_3 + 2m_1 m_2. \end{aligned} \quad (14)$$

By inspection, it is easy to see that $\alpha_1 < \alpha_2 < \alpha_3 < \alpha_4$ and $\alpha_8 < \alpha_7 < \alpha_6 < \alpha_5$. That is, we need to only compare α_1 and α_8, which is equivalent to comparing $m_1 m_2$ and m_3. □

For instance, if $N = 3$ and $m_i = \{3, 4, 5\}$, since $m_1 m_2 \geq m_3$, $B_{\widehat{M}} = 3(3 \cdot 4 + 2 \cdot 5) - 1 = 65$.

B. Efficient Algorithm Steps

Using Lemmas 1 through 8, the efficient algorithm for computing $\widehat{M}$ follows the steps below:

- S1. Define N as the number of coprime moduli $(m_i)_{1 \leq i \leq N}$, $M = \prod_{i=1}^{N} m_i$, and fundamental period of the RSNS $P_f = 2MN$.
- S2. Compute the upper bound $B_{\widehat{M}}$ for the dynamic range, (12) of Theorem 7, or (13) of Lemma 8, if $N = 3$.
- S3. Compute the number of ambiguity cases for the particular RSNS using Table III and the limits imposed by Lemma 1. Compute the minimal-pair distance for all ambiguity pair cases using multiplication of corresponding entries in the matrix of size $N \times 2^N$, which is the matrix containing as columns all of the N subcases of the 2^N distinct cases of repeating ambiguity pairs, and eliminate all ambiguity pair cases that have a length greater than the dynamic range upper bound (step S2).
- S4. Compute the remaining minimal pair ambiguity locations (h_1, h_2) using Table III and Lemmas 2 and 5.
- S5. Sort the matrix of minimal pairs (h_1, h_2) such that h_2 is monotonically increasing. Vector subtract the start positions of consecutive minimal pairs $(h_1(p) - h_1(p+1))$ and remove all minimal pairs where the result is negative. The remaining minimal pairs are the only *consecutive* minimal pairs.
- S6. Compute the vector of distances between endpoints of consecutive minimal pairs $(h_2(p+1) - h_1(p) - 1)$. The dynamic range $\widehat{M}$ is the largest value in the resulting vector.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

C. Example

Consider the RSNS from Table I where $N = 3$, $m_i = \{3, 4, 5\}$. Table III provides the general $N-$sequence ambiguity expressions and Table I of reference [4] provides the general ambiguity pair equations for the $N = 3$ case (we give a particular case of that table in our Table IV, for the moduli $m_i = \{3, 4, 5\}$).

S1. Define $N = 3$, $M = \prod_{i=1}^{N} m_i = 60$, and $P_f = 360$.
S2. Compute the dynamic range upper bound by using Theorem 7 (in which case, $\lceil 6\sqrt{120} \rceil - 1 = \lceil 65.7267 \rceil - 1 = 65$), or (since $N = 3$) Lemma 8 (in which case, $3(3 \cdot 4 + 2 \cdot 5) - 1 = 65$).
S3. Table IV shows all possible ambiguity cases (using Table III, or Table I in [4]) and points out (above the double line) the rows that have ambiguity pairs with a length (min k) greater than $B_{\widehat{M}} = 65$, which can be ignored in the computation of $\widehat{M}$.

TABLE IV
ALL AMBIGUITY CASES (AFTER [4], $a \in \mathbb{Z}$)

Case Label	Ambiguities occur at h and $h+k$, where h is	min k
Case 010	Any position	360
Case 110	$h_{\text{Case 110}} = a \cdot 9 - 60$	120
Case 111	$h_{\text{Case 111}} = a \cdot 9 - 59$	
Case 112	$h_{\text{Case 112}} = a \cdot 9 - 58$	
Case 120	$h_{\text{Case 120}} = a \cdot 12 - 45$	90
Case 121	$h_{\text{Case 121}} = a \cdot 12 - 44$	
Case 122	$h_{\text{Case 122}} = a \cdot 12 - 46$	
Case 130	$h_{\text{Case 130}} = a \cdot 15 - 36$	72
Case 131	$h_{\text{Case 131}} = a \cdot 15 - 38$	
Case 132	$h_{\text{Case 132}} = a \cdot 15 - 37$	
Case 210	$h_{\text{Case 210}} = a \cdot 36 - 15$	30
Case 211	$h_{\text{Case 211}} = a \cdot 36 + h_{s1} - 15$	
Case 212	$h_{\text{Case 212}} = a \cdot 36 + h_{s2} - 15$	
Case 220	$h_{\text{Case 220}} = a \cdot 45 - 12$	24
Case 221	$h_{\text{Case 221}} = a \cdot 45 + h_{s1} - 12$	
Case 222	$h_{\text{Case 222}} = a \cdot 45 + h_{s2} - 12$	
Case 230	$h_{\text{Case 230}} = a \cdot 60 - 9$	18
Case 231	$h_{\text{Case 231}} = a \cdot 60 + h_{s1} - 9$	
Case 232	$h_{\text{Case 232}} = a \cdot 60 + h_{s2} - 9$	
Case 310	$h_{\text{Case 310}} = a \cdot 180 - 3$	6
Case 311	$h_{\text{Case 311}} = a \cdot 180 + h_{s1} - 3$	
Case 312	$h_{\text{Case 312}} = a \cdot 180 + h_{s2} - 3$	

The base cases (all cases ending in zero in Table IV) do not have shifts applied to the COA (i.e., $h_{s0} = 0$). The shifts h_{s1} and h_{s2} in Table IV are computed, according to the procedure described in [4], as the least positive solutions to the following two sets of congruence equations ($h_{s1} = 73$, $h_{s2} = 119$):

$$\frac{h_{s1}-1}{3} \equiv 0 \bmod 3 \qquad \frac{h_{s2}-2}{3} \equiv 0 \bmod 3$$
$$\frac{h_{s1}-1}{3} \equiv 0 \bmod 4 \qquad \frac{h_{s2}+1}{3} \equiv 0 \bmod 4$$
$$\frac{h_{s1}+2}{3} \equiv 0 \bmod 5 \qquad \frac{h_{s2}+1}{3} \equiv 0 \bmod 5.$$

S4. Minimal pair ambiguity locations (h_1, h_2) are computed using Table IV for $h = -3$ to $h = 183$. All minimal pairs are provided in Table V.
S5. The *consecutive* minimal pairs are shown in Table V.

TABLE V
ALL MINIMAL PAIRS, AND ALL *consecutive* MINIMAL PAIRS (SHADED)

h_1	COA	h_2	h_1	COA	h_2
−3	0	3	68	83	98
−14	1	16	**78**	**90**	**102**
−4	11	26	93	108	123
4	13	22	94	109	124
16	28	40	106	118	130
17	29	41	**116**	**119**	**122**
21	36	51	111	120	129
22	37	52	124	133	142
33	45	57	123	135	147
32	47	62	129	144	159
50	59	68	130	145	160
51	60	69	140	155	170
57	72	87	151	163	175
70	73	76	152	164	176
62	74	86	170	179	188
			177	180	183

S6. The consecutive minimal pairs that have the largest distance between them are displayed in **bold font** with a shaded background in Table V. The result is an $\widehat{M} = 43$ starting at $h = 79$, and ending at $h = 121$, which agrees with the results in [4], [7].

V. ALGORITHM EFFICIENCY

We compute the complexity of the computation of the bound (11) and compare the efficiency of our algorithm with the naïve search algorithm of [3]. We use the "prime" big-oh notation $O'(\cdot)$ for functions in both M, N (to see the dependence on N), and the big-oh notation $O(\cdot)$ for functions in M, which is the relevant parameter (the O-constant will be dependent on N). For every $0 \le k \le N$, and every subset I of cardinality k, we perform $k-1$ multiplications for the first term in the minimum computation of (11), plus, a division and a doubling for the second term (since $2\prod_{j\in\bar{I}} m_j = 2M/\prod_{i\in I} m_i$ reusing the previous computation). Including the sorting for a set of cardinality 2^N with complexity $O(N2^N)$, the complexity for the bound computation of Lemma 6 is

$$\begin{aligned} &O\left(N2^N + N + \sum_{k=0}^{N} k\binom{N}{k}2^k\right) \\ &= O\left(N2^N + 2N3^{N-1}\right) \\ &= O\left(N3^N\right), \end{aligned}$$

using the identity $\sum_{k=0}^{n} k\binom{n}{k}z^k = nz(z+1)^{n-1}$. Applying (12) significantly reduces the above complexity to $O(1)$, as a function of M (at the expense of possibly increasing the upper bound). The $\widehat{M}$ computation process described in Section IV-B was implemented using MATLAB. A search of current research did not reveal any existing efficient computational

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

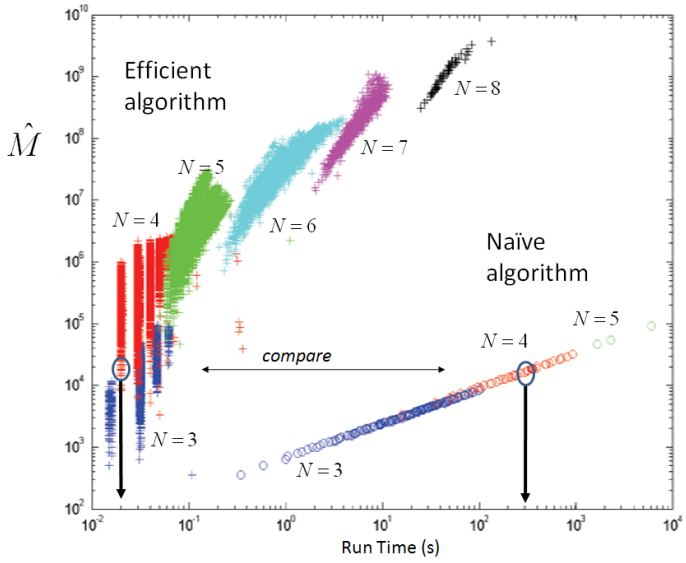

Fig. 3. Log-log plot of $\widehat{M}$ vs. run time using the improved and naïve algorithms.

algorithms for finding and comparing *all* pairs of $N\times 1$ vectors in an $N\times P_f$ vector space, except for a naïve search algorithm used in [5]. The naïve search algorithm starts by creating an $N \times P_f$ matrix with each of the *columns* consisting of the integer values within each RSNS modulus sequence, as shown in Table I. A double nested for–loop then determines the beginning position of each ambiguity h_1, which are then sorted. A second double nested for–loop is then used to determine the end position h_2 of each ambiguity where no other ambiguities are enclosed. The maximum length is then calculated and is $\widehat{M}$ with the matrix index corresponding to the correct beginning and end positions.

Now, we compare the time complexities (arithmetical operations, and comparisons) of both algorithms in the modulus M (assuming N fixed). The naïve approach uses a matrix of size $N\times(2NM)$ and for each column, it checks for the first match (ambiguity) in the remaining columns of the matrix, so it uses N comparisons (for each components of every vector) plus an addition for the range counter. Therefore, the worst case complexity of finding ambiguities and the distance between them is

$$\ll \sum_{h=0}^{P_f-1} N(P_f-h) = NP_f^2 - N\frac{P_f(P_f-1)}{2} \qquad (15)$$

$$= \frac{NP_f(P_f+1)}{2} = M(2MN+1)N^2 = O'(M^2N^3) \qquad (16)$$

(since the RSNS fundamental period is $P_f = 2NM$). We then sort the obtained list of size $\ll P_f = 2NM$, which can be done in $O'(MN(\log M + \log N))$, resulting in a total time complexity of

$$\text{Naive Time Complexity} = O'(M^2N^3) = O(M^2)$$

for the dynamic range computation. Now, we examine the time complexity of our algorithm. The first step is the same for both, and we disregard its complexity (as it is quite low, that is, $O'(N)$, compared to the other steps' complexities). The second step can be done in $O(1)$ using our Theorem 7, Lemma 8. The third step uses a sorted bin of size $N\times 2^N$ and performs $O'(N^2 2^N)$ additions/multiplications on rows, and $O'(N2^{2N})$ additions/multiplications on columns (see [4] for further details on this step). The sorting of Step 3 is done in $O'(N2^N)$ operations. Step 4 as well as Step 6 need $O'(2^N)$ operations, and Step 5 needs $O'(N2^N)$, for a total worst case time complexity of

$$\text{Improved Time Complexity} = O'(N2^{2N}) = O(1).$$

Remark 9. *The main advantage of our algorithm is that it removes the apparent dependence on the size of the moduli in the number of operations needed to compute the dynamic range.*

Fig. 3 shows a log–log plot of $\widehat{M}$ versus computation time for the two algorithms using hundreds of $N-$channel moduli sets. Each "+" represents the $\widehat{M}$ obtained using the algorithm presented in this paper, and has a corresponding "$\circ$" on the same horizontal axis (up to $\widehat{M} \approx 10^9$), which is the $\widehat{M}$ computed using the naïve search algorithm. The results are displayed where the two computation methods produced the same results for $\widehat{M}$ (up to 10^4 s). For example, with $N = 4$ moduli with $\widehat{M} = 2\times 10^4$, the naïve algorithm takes 300 s to produce the answer, while the efficient algorithm described above only takes 0.02 s.

VI. Further Closed-Form Results for $\widehat{M}$

In this section, closed-form expressions are developed for $\widehat{M}$ for several groups of moduli sets by curve fitting data generated using the efficient algorithm described in Section IV and then verifying that the closed-form expressions satisfy the ambiguity equations of Table III. Curve fitting the data obtained from the algorithm was chosen as a method of generating the closed-form expressions for $\widehat{M}$ because it leveraged the efficiency of our algorithm to generate data for a large groups of moduli sets and curve fitting enabled determining patterns of repeated Start and Stop Case number combinations and visually determining the periodic nature of discontinuities in the plotted data and resolving them. This method also proved to be efficient compared to attempting to derive closed-form expressions for $\widehat{M}$ by iteratively solving the equations of Table III for different moduli sets.

A sample of the data generated using the algorithm is presented in Table VI. The data was analyzed to determine which moduli sets have the same Start and Stop Case numbers, and the value of $\widehat{M}$ was plotted against a variable m that is linearly related to the moduli. Curve-fitting of the plotted data using MATLAB's curve fitting tool box was conducted to generate exact closed-form expressions for $\widehat{M}$. The closed-form expressions were then verified to be accurate by deriving them from the applicable equations listed in Table III. Several groupings of moduli for $N = 3$ and $N = 4$ were examined increasing the number of closed-form expressions for $\widehat{M}$.

For the $N = 3$ case, sequential coprime odd moduli of the form $m_i = \{m-1, m+1, m+3\}$ with m even and $m > 3$ were examined. Also, the case of two odd moduli and one even

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

modulus were examined where $m_i = \{m, m+1, m+3\}$ and $\{m-3, m-1, m\}$ with m even. The final case examined was where the moduli consisted of every other odd number, that is $m_i = \{m, m+4, m+8\}$ where m is odd and $m \geq 3$. The new closed-form expressions derived from curve fitting the data are presented in Table VIII.

To demonstrate the method used to verify the closed-form expressions generated from curve fitting, we examine the case where $N = 3$ and $m_i = \{m-1, m+1, m+3\}$ with m even by generating the closed-form expressions from the equations of Table III. The data was examined, and it was determined that two distinct sets of case numbers are associated with the beginning and ending positions of $\widehat{M}$. When $m \equiv 0 \bmod 4$, the case number associated with the beginning position, *Start Case* of $\widehat{M}$ is Case 211, and the case number associated with the ending position, *Stop Case* of $\widehat{M}$ is Case 220. The value of m was plotted against the value of $\widehat{M}$, and the data was curve fitted to a quadratic polynomial using MATLAB's curve fitting toolbox. From the curve fit data,

$$\widehat{M} = \frac{3}{2}m^2 + \frac{15}{2}m + 7 \tag{17}$$

where $m \equiv 0 \bmod 4$. A sample of the data used to derive (17) is presented in Table VI. The data examined and its corresponding curve fit is illustrated in Fig. 4a. The values of $\widehat{M}$ derived from the algorithm are equal to the values resulting from (17).

Now, we will verify that the curve fit solution satisfies the ambiguity equations of Table III. For the Start Case,

$$h_{211} = a\,(3m_1m_2) + h_{s_{211}} - 3m_3. \tag{18}$$

The congruence equations that are generated from the shift matrix, (8),

$$\begin{aligned} \frac{h_{s_{211}} - 1}{3} &\equiv 0 \bmod m_1 \\ \frac{h_{s_{211}} - 1}{3} &\equiv 0 \bmod m_2, \end{aligned} \tag{19}$$

are solved resulting in $h_{s_{211}} = 1$. The value of a in (18) was derived by solving (18) for a using the values of the beginning position $(h_1 + 1)$ of $\widehat{M}$ and m. The results were curve fitted, resulting in $a = 0.75m + 2$. By substituting the expression for a into (17), we obtain

$$h_{211} = \frac{9}{4}m^3 + 6m^2 - \frac{21}{4}m - 14. \tag{20}$$

For the Stop Case,

$$h_{220} = a(3m_1m_3) + 3m_2. \tag{21}$$

It was determined that $a = 0.75m + 1$ and

$$h_{220} = \frac{9}{4}m^3 + \frac{15}{2}m^2 + \frac{9}{4}m - 6 \tag{22}$$

By solving for $\widehat{M} = h_{220} - h_{211} - 1$, we obtain (17).

When $m \equiv 2 \bmod 4$, the Start Case is Case 211, and the Stop Case is Case 231 as shown in Table VII. The data was curve fitted resulting in

$$\widehat{M} = \frac{3}{2}m^2 + \frac{15}{2}m + 5. \tag{23}$$

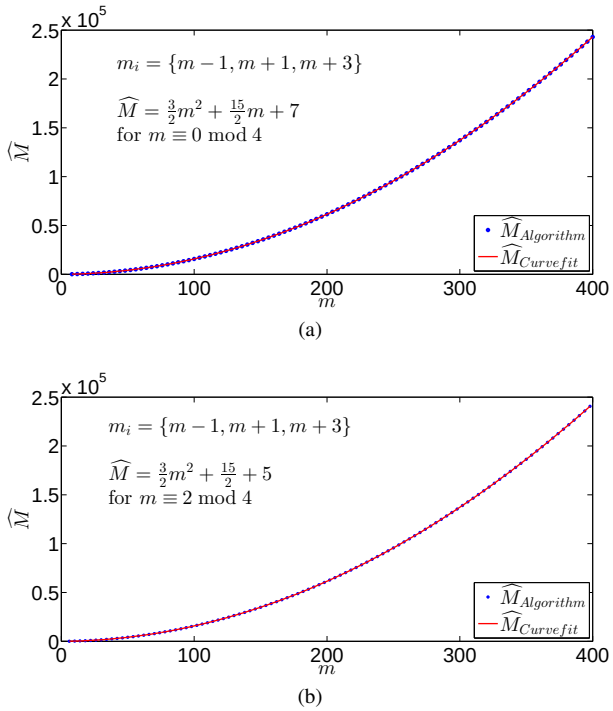

Fig. 4. Curve fitting results for $\widehat{M}$ when (a) $m_i = \{m-1, m+1, m+3\}$ where $m \equiv 0 \bmod 4$, (b) $m_i = \{m-1, m+1, m+3\}$ and $m \equiv 2 \bmod 4$.

Fig. 4b displays the data and closed-form solution generated from curve fitting. Using the same approach, (23) is verified by deriving it from the equations in Table III. For the Stop Case,

$$h_{231} = a\,(3m_2m_3) + h_{s_{231}} + 3m_1. \tag{24}$$

The congruence equations generated from (8)

$$\begin{aligned} \frac{h_{s_{231}} - 1}{3} &\equiv 0 \bmod m_2 \\ \frac{h_{s_{231}} + 2}{3} &\equiv 0 \bmod m_3. \end{aligned} \tag{25}$$

are solved using the CRT, resulting in

$$h_{s_{231}} = \frac{3}{2}m^2 + \frac{15}{2}m + 7. \tag{26}$$

The value of a in (24) was determined to be $a = 0.5m - 1$. These expressions were then substituted into (24) to determine that

$$h_{231} = \frac{3}{2}m^3 + \frac{9}{2}m^2 + 3m - 5. \tag{27}$$

After solving for $\widehat{M} = h_{231} - h_{211} - 1$, we obtain (23) which verifies the result. The closed-form expressions for the other moduli sets examined were verified in a similar manner.

Several groups of $N = 4$ RSNS moduli sets were also examined, and closed-form expressions to $\widehat{M}$ were produced by curve fitting the data generated by the efficient algorithm. The moduli sets examined were

$$m_i = \{m-1, m, m+2, m+4\},$$

$$m_i = \{m, m+1, m+2, m+4\},$$

$$m_i = \{m, m+2, m+3, m+4\},$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

TABLE VI
SAMPLE OF DATA USED IN CURVE FITTING FOR SEQUENTIAL ODD COPRIME MODULI. $m \equiv 0 \bmod 4$

$m-1$	$m+1$	$m+3$	h_1+1	Start Case	h_2-1	Stop Case	$\widehat{M}$
7	9	11	1481	211	1643	220	163
11	13	15	4676	211	4988	220	313
15	17	19	10655	211	11165	220	511
19	21	23	20282	211	21038	220	757
23	25	27	34421	211	35471	220	1051
27	29	31	53936	211	55328	220	1393
31	33	35	79691	211	81473	220	1783
35	37	39	112550	211	114770	220	2221
39	41	43	153377	211	156083	220	2707
43	45	47	203036	211	206276	220	3241
47	49	51	262391	211	266213	220	3823

TABLE VII
SAMPLE OF DATA USED IN CURVE FITTING FOR SEQUENTIAL ODD COPRIME MODULI, WITH $m \equiv 2 \bmod 4$.

$m-1$	$m+1$	$m+3$	h_1+1	Start Case	h_2-1	Stop Case	$\widehat{M}$
5	7	9	395	211	498	231	104
9	11	13	1745	211	1974	231	230
13	15	17	4631	211	5034	231	404
17	19	21	9629	211	10254	231	626
21	23	25	17315	211	18210	231	896
25	27	29	28265	211	29478	231	1214
29	31	33	43055	211	44634	231	1580
33	35	37	62261	211	64254	231	1994
37	39	41	86459	211	88914	231	2456
41	43	45	116225	211	119190	231	2966
45	47	49	152135	211	155658	231	3524

TABLE VIII
NEW CLOSED-FORM EXPRESSIONS FOR $\widehat{M}$ FOR $N = 3$ RSNS.

$\mathbf{m_i}$	$\widehat{\mathbf{M}}$	$\mathbf{m}$
$\{m-1, m+1, m+3\}$	$\frac{3}{2}m^2+\frac{15}{2}m+7$	$m \equiv 0 \bmod 4$
	$\frac{3}{2}m^2+\frac{15}{2}m+5$	$m \equiv 2 \bmod 4$
$\{m, m+1, m+3\}$	$\frac{3}{2}m^2+\frac{27}{2}m+6$	$m \equiv 2 \bmod 4$ and $m \geq 14$
$\{m-3, m+1, m\}$	$\frac{3}{2}m^2+\frac{3}{2}m$	m is even and $m \neq 6k$ where $k = 1, 2, \ldots$
$\{m, m+4, m+8\}$	$\frac{9}{4}m^2+\frac{63}{4}m+48$	$m \equiv 1 \bmod 8$
	$\frac{3}{2}m^2+\frac{33}{2}m+35$	$m \equiv 3 \bmod 8$
	$\frac{3}{2}m^2+\frac{33}{2}+34$	$m \equiv 5 \bmod 8$
	$\frac{9}{4}m^2+\frac{57}{4}m+45$	$m \equiv 7 \bmod 8$

$$m_i = \{m, m+2, m+4, m+5\},$$

and

$$m_i = \{m, m+2, m+4, m+6\},$$

where m is odd. The closed-form expressions for $\widehat{M}$ are presented in Table IX and were verified in the same manner as the $N = 3$ cases.

VII. CONCLUDING REMARKS

This paper presents an algorithm to compute $\widehat{M}$ and determine its location in the RSNS sequence. The algorithm reduces the computation time by several orders of magnitude compared to a previously reported naïve search algorithm. In addition, we demonstrate that our efficient algorithm removes the apparent dependence on the size of the moduli in the number of operations needed to compute $\widehat{M}$. Linear interpolating the data in Fig. 3, it would take the naïve search algorithm more than 32 years to find $\widehat{M}$ for the same $N = 8$ sequence (of approximately 28 bit moduli) that the efficient algorithm computed in approximately 30 seconds. Moreover, the efficient algorithm uses far less memory than the naïve search algorithm; therefore, it can be used to determine the N sequence $\widehat{M}$ and position for moduli sets with much larger fundamental periods.

The algorithm was also used to generate data sets from which curve fitting produced additional closed-form expressions for $\widehat{M}$ increasing the groups of moduli sets for which analytical expressions for $\widehat{M}$ exist. The new closed-form expressions for $\widehat{M}$ significantly increase the number of analytical expressions that are known for $\widehat{M}$ greatly increasing the utility of the RSNS to solving many types of engineering problems.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2014.2301820, IEEE Transactions on Information Theory

TABLE IX
NEW CLOSED-FORM EXPRESSIONS FOR $\widehat{M}$ FOR $N = 4$ RSNS.

$\mathbf{m_i}$	$\widehat{\mathbf{M}}$	$\mathbf{m}$
$\{m-1, m, m+2, m+4\}$	$10m^2+6m+20$	$m \equiv 3 \bmod 6$ or $m \equiv 5 \bmod 6$ with $m \geq 15$ and $m \neq \{29, 33\}$
$\{m, m+1, m+2, m+4\}$	$10m^2+22m+20$	$m \equiv 1 \bmod 6$ or $m \equiv 3 \bmod 6$ and $m \geq 15$
$\{m, m+2, m+3, m+4\}$	$10m^2+30m-6$	$m = \{25+12k, 29+12k, 31\}$ where $k = 0, 1, 2, \cdots,$
	$10m^2+30m-8$	$m = \{43+12k, 47+12k\}$ and $k = 0, 1, 2, \cdots$
$\{m, m+2, m+4, m+5\}$	$10m_2+54m+20$	$m \geq 39$, $\gcd(m, 5) = 1$, and m is odd
$\{m, m+2, m+4, m+6\}$	$10m^2+38m+56$	$m \geq 13$ and $\gcd(m, 3) = 1$

Further research opportunities are investigating additional moduli sets where closed-form expressions exist, developing a general closed-form expression for $\widehat{M}$, and formulating an overarching theoretical framework that relates the various symmetrical number systems to each other.

APPENDIX
PROOF OF THEOREM 7

Proof. Setting $x = \prod_{i \in I} m_i$, we see that the expression that must be minimized in the right-hand side of (11) is in fact the function

$$f(x) = x + \frac{2M}{x}, x \geq 1.$$

By examining the derivative of $f(x)$, a simple calculus analysis reveals that the function has a global minimum at $x = \sqrt{2M}$, namely $2\sqrt{2M}$, and the first inequality is shown.

The work in [4] contains the proof of $\widehat{M} < M$ for $N = 3$. As examples, if $N = 3$, the smallest size coprime moduli sets are listed in Table X in lexicographical order.

TABLE X
EXAMPLES OF $\widehat{M}_{RSNS}$ AND M FOR $N = 3$

$\mathbf{m_i}$	$\widehat{\mathbf{M}}_{\mathbf{RSNS}}$	$\mathbf{M}$
$\{2, 3, 5\}$	28	30
$\{2, 3, 7\}$	35	42
$\{2, 3, 11\}$	46	66
$\{3, 4, 5\}$	43	60

Now, assume that $N \geq 4$. We need to prove that $N\lceil 2\sqrt{2M} \rceil < M$, for $N \geq 4$. Starting with the simple inequality

$$N\lceil 2\sqrt{2M} \rceil \leq N(2\sqrt{2M}+1),$$

it is sufficient to show that $N(2\sqrt{2M}+1) \leq M$, which is equivalent to $N\sqrt{8M} \leq M - N$, and $8N^2M \leq M^2 + N^2 - 2MN$, that is, $M^2 - 2N(4N+1)M + N^2 > 0$. Looking at the previous inequality as the sign of a concave-up parabola in M, we see that the inequality is true, as long as

$$M > 4N^2 + N + 2N\sqrt{4N^2+2N}. \tag{28}$$

If $N = 4$, then $M \geq 210$, and the right-hand side of (28) is ~ 209.881; if $N = 5$, then $M \geq 2310$, and the right-hand side of (28) is ~ 299.88. Thus, the inequality (28) is true for $4 \leq N \leq 5$.

Next, it is observed that for any $N \geq 3$ (use the fact that the moduli are coprime): if $N = 3$, then

$$M \geq \begin{cases} 2 \cdot 3 \cdot 5 = 30, & N = 3 \\ 2 \cdot 3 \cdot 5 \cdot 7 = 210, & N = 4 \\ etc. \end{cases}$$

$M \geq 2 \cdot 3 \cdot 5 = 30$; if $N = 4$, then $M \geq 2 \cdot 3 \cdot 5 \cdot 7 = 210$, etc. For arbitrary N, an easy inductive procedure reveals that

$$M \geq P_N\#,$$

where $P_N\# = \prod_{k=1}^{N} p_k$ is the primorial function, and p_k is the kth prime. It is well–known (and easily derivable by using the prime number theorem [17]) that $P_N\# = \exp[(1 + o(1))\, n \log n]$.

Assume $N \geq 6$. It is immediate that

$$P_N\# > (N+1)!.$$

(For the interested reader, a better asymptotic estimate $P_N\# = \exp[(1 + o(1))\, N \log N]$ is well–known [17].) We now show that for $N \geq 6$, the right hand side of the above inequality satisfies

$$(N+1)! > 4N^2 + N + 2N\sqrt{4N^2+2N}, \tag{29}$$

which will imply our claim.

We will prove (29) by induction on N. If $N = 6$, then

$$(6+1)! - \left(4 \cdot 6^2 + 6 + 2 \cdot 6\sqrt{4 \cdot 6^2 + 2 \cdot 6}\right) > 4740,$$

and so, the inequality (29) is true in this case. Assume that the inequality is true for N and we show it for $N+1$, that is, we start from (29) and multiply by $N+2$ on both sides, to get

$$(N+2)! > (N+2) \cdot \left(4N^2 + N + 2N\sqrt{4N^2+2N}\right).$$

It will be sufficient to show that

$$(N+2)\left(4N^2 + N + 2N\sqrt{4N^2+2N}\right) > 4(N+1)^2 + (N+1) + 2(N+1)\sqrt{4(N+1)^2 + 2(N+1)}.$$

Since

$$(N+2)(4N^2+N) - 4(N+1)^2 - (N+1) = 4N^3 + 5N^2 - 7N - 5$$

is increasing and greater than 0, for $N \geq 6$, the previous inequality will follow if

$$(N+2)2N\sqrt{4N^2+2N} > 2(N+1)\sqrt{4(N+1)^2 + 2(N+1)},$$

which by squaring both sides transforms into

$$-24 - 88N - 120N^2 - 40N^3 + 80N^4 + 72N^5 + 16N^6 > 0,$$

which is certainly true for $N \geq 6$. This concludes the proof of Theorem 7. □

REFERENCES

[1] P. E. Pace, R. E. Leino, and D. Styer, "Use of the symmetrical number system in resolving single-frequency undersampling aliases," *IEEE Trans. on Signal Process.*, vol. 45, pp. 1153–1160, May 1997.

[2] P. E. Pace, J. L. Schafer, and D. Styer, "Optimum analog preprocessing for folding ADCs," *IEEE Trans. Circuits Syst. II*, vol. 42, pp. 825–829, Dec. 1995.

[3] B. L. Luke and P. E. Pace, "Computation of the robust symmetrical number system dynamic range," in *Proc. 2010 IEEE Information Theory Workshop (ITW 2010-Dublin)*, pp. 1–5.

[4] ——, "N-sequence RSNS ambiguity analysis," *IEEE Trans. Inf. Theory*, vol. 53, pp. 1759–1766, May 2007.

[5] D. Styer and P. E. Pace, "Two-channel RSNS dynamic range," *IEEE Trans. Circuits Syst. I*, vol. 49, pp. 395–397, Mar. 2002.

[6] D.-M. Pham, A. Premkumar, and A. S. Madhukumar, "Efficient sample rate conversion in software radio employing folding number system," in *2009 IEEE International Conf. Comms. - ICC '09.*, 2009, pp. 1–5.

[7] P. E. Pace, D. Styer, and I. A. Akin, "A folding ADC preprocessing architecture employing a robust symmetrical number system with gray-code properties," *IEEE Trans. Circuits Syst. II*, vol. 47, pp. 462–467, May 2000.

[8] I.-H. Wang and S.-I. Liu, "A CMOS 5-bit 5gsample/sec analog-to-digital converter in 0.13 μm CMOS," *J. Semiconductor Technol. and Sci.*, pp. 28–35, Mar. 2007.

[9] M. R. Arvizo, J. Calusdian, K. B. Hollinger, and P. E. Pace, "Robust symmetrical number system preprocessing for minimizing encoding errors in photonic analog-to-digital converters," *Optical Engineering*, vol. 50, pp. 084 602–1–084 602–11, Aug. 2011.

[10] M. Wicht, M. Schott, and P. E. Pace, "Increasing the flux measurement range of an RF-SQUID resonant detection circuit using the robust symmetrical number system," *IEEE Trans. Appl. Supercond.*, vol. 23, pp. 1 602 910–1 602 910, Feb. 2013.

[11] D.-M. Pham, A. B. Premkumar, and A. S. Madhukumar, "Error detection and correction in communication channels using inverse gray RSNS codes," *IEEE Trans. Commun.*, vol. 59, pp. 975–986, Apr. 2011.

[12] Y. Jakop, A. S. Madhukumar, and A. B. Premkumar, "A robust symmetrical number system based parallel communication system with inherent error detection and correction," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 2742–2747, Jun. 2009.

[13] P. E. Pace, D. Wickersham, D. C. Jenn, and N. S. York, "High-resolution phase sampled interferometry using symmetrical number systems," *IEEE Trans. Antennas Propag.*, vol. 49, pp. 1411–1423, Oct. 2001.

[14] N. Paepolshiri, P. E. Pace, and D. C. Jenn, "Extending the unambiguous range of polyphase P4 CW radar using the robust symmetrical number system," *IET Radar, Sonar & Navigation*, vol. 6, pp. 659–667, Jul. 2012.

[15] M. B. A. P. Hiltgen, K. G. Paterson, "Single-track gray codes," *IEEE Trans. Inf. Theory*, pp. 1555–1561, May 1996.

[16] B. L. Luke and P. E. Pace, "N-sequence RSNS redundancy analysis," in *2006 IEEE Int. Symp. on Information Theory*, pp. 2744–2748.

[17] H. Dubner, "Factorial and primorial primes," *J. Rec. Math.*, pp. 197–203, 1987.

Phillip E. Pace (S87, M90, SM97) received the B.S. and M.S. degrees from Ohio University, Athens, in 1983 and 1986, respectively, and the Ph.D. degree from the University of Cincinnati, Cincinnati, OH, in 1990, all in electrical and computer engineering. He is currently a Professor in the Department of Electrical and Computer Engineering at the Naval Postgraduate School (NPS), Monterey, CA, and the Director for the NPS Center for Joint Services Electronic Warfare. Prior to joining NPS, he spent two years at General Dynamics Corporation, Air Defense Systems Division, as a Design Specialist in the Radar Systems Research Engineering Department. Before that, he was a member of technical staff at Hughes Aircraft Company, Radar Systems Group, for five years. He has been the Chairman of the Navy's Threat Simulator Validation Working Group since October 1998 and was a participant on the Navy's NULKA Blue Ribbon Panel in January 1999. He is the author of two textbooks, Advanced Techniques for Digital Receivers, (Artech House, 2000) and Detecting and Classifying Low Probability of Intercept Radar (Artech House, 2004, 2009) and is an Associate Editor for the Transactions on Aerospace and Electronic Systems (electronic warfare technical area). He has been a Principal Investigator on numerous research projects in the areas of signal processing, electronic warfare, and weapon systems analysis.

Pantelimon Stănică received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. Currently, he is a Professor at the Naval Postgraduate School, in Monterey, California. His research interests are in Cryptology, Number Theory and Discrete Mathematics.

Brian L. Luke received his Ph.D. in Electrical Engineering in 2004 from the Naval Postgraduate School in Monterey, California. He is a Captain in the Navy currently serving as an Information Warfare Officer in the Maryland and Washington DC area.

Thomas W. Tedesso (S'2010) received the B.S. in electrical engineering from Illinois Institute of Technology, Chicago, IL in 1990 and a M.S. in electrical engineering from the Naval Postgraduate School, Monterey, CA, in 1998. He is currently a Ph.D. candidate at the Naval Postgraduate School, Monterey, CA, serving on active duty in the United States Navy. Prior to commencing his doctoral studies in September 2010, he served in various assignments both ashore and afloat as a surface warfare officer trained in naval nuclear propulsion, including Assistant Reactor Officer on USS ENTERPRISE (CVN-65) and Chief Staff Officer of Destroyer Squadron FIFTEEN forward deployed to Yokosuka, Japan. Following completion of his doctoral research in December 2013, he will report to the United States Naval Academy as a permanent military professor.