A Residue Number System Based Parallel Communication Scheme Using Orthogonal Signaling: Part I-System Outline

Lie-Liang Yang, Member, IEEE, and Lajos Hanzo, Senior Member, IEEE

Dept. of Electronics and Computer Science,
University of Southampton, SO17 1BJ, UK.
Tel: +44-1703-593 125, Fax: +44-1703-594 508
Email: lh@ecs.soton.ac.uk
http://www-mobile.ecs.soton.ac.uk

1Acknowledgement: The valued comments and critique of the anonymous Reviewers is gratefully acknowledged. The kind assistance of Kai Yen in finding the distribution of the ratio statistic test is gratefully acknowledged.

2This work has been submitted to the IEEE for possible publication. Copyright may be transferred without notice, after which this version will be superseded.
A Residue Number System Based Parallel Communication Scheme Using Orthogonal Signaling: Part I-System Outline

Lie-Liang Yang, Member, IEEE, and Lajos Hanzo, Senior Member, IEEE

Dept. of Electronics and Computer Science,
University of Southampton, SO17 1BJ, UK.
Tel: +44-1703-593 125, Fax: +44-1703-594 508
Email: lh@ecs.soton.ac.uk
http://www-mobile.ecs.soton.ac.uk

Abstract

A novel signaling scheme is presented, where a set of orthogonal signals is transmitted in parallel, which are selected according to the so-called residue number system (RNS). Hence the system is essentially a multiple code parallel communication scheme using high modulation alphabets. It is demonstrated that the system performance can be substantially improved by exploiting a number of advantageous properties of the RNS arithmetic.

In part I of the paper, we focus on the system description, the background of the RNS arithmetic, as well as on the performance evaluation of the residue number system arithmetic, using both non-redundant and redundant moduli based orthogonal signaling schemes, over an AWGN channel. Redundant Residue Number System (RRNS) codes are introduced in order to protect the transmitted information. A novel decision algorithm, referred to as a ratio statistic test (RST) is designed, which implies dropping some of the lowest-reliability demodulation outputs, before the residue digits are transformed back to binary symbols. This improves the system’s performance. This dropping technique is different from the conventional ‘errors-and-erasures’ decoding, where the erased symbols (or bits) should be computed and filled during decoding. It is argued that the demodulated/decoded information can be obtained by decoding the retained or un-discarded symbols upon exploiting the properties of the residue number system arithmetic. Numerical results show that the proposed scheme constitutes a high efficiency parallel transmission method for high-bit-rate communication, achieving a coding gain of 2dB at a BER of $10^{-6}$ over AWGN channels.

Indexing Terms-CDMA, Orthogonal signalling, Parallel signalling, Residue number system, Redundant residue number system, Error-control, Ratio statistic test.

I. INTRODUCTION

Flexible, high-bit-rate, low bit error rate (BER) communication is becoming an issue of increasing importance. Conventionally, communication system design is based on the well-known weighted num-
ber system representation, using for example a base of 2, 8, 16, etc. for implementation, ultimately favouring the weighted binary system. In a conventional binary system, due to the carry forward required by the weighted number system a bit error may affect all the bits of the result. By contrast, the so-called residue number system (RNS) [1] is a non-weighted, carry-free number system, which has received wide attention due to its robust self-checking, error-detection, error-correction and fault-tolerant signal processing properties [1]-[14].

An RNS is defined [1] by the choice of \( v \) positive integers \( m_i \), \((i = 1, 2, \ldots, v)\) referred to as moduli. If all the moduli are pairwise relative primes, any integer \( N \), describing the information symbols to be transmitted in this paper, can be uniquely and unambiguously represented by the so-called residue sequence \((r_1, r_2, \ldots, r_v)\) in the range \( 0 \leq N < M_I \) where \( r_i = N \pmod{m_i} \) represents the residue digits of \( N \) upon division by \( m_i \), and \( M_I = \prod_{i=1}^{v} m_i \) is the information dynamic range, ie the legitimate range of the information symbols \( N \). In the above process the algorithm that transforms any conventional weighted number system to the residue number system is defined as residue number system transform (RNST). According to the so-called Chinese reminder theorem (CRT) [6], for any given \( v \)-tuple of residues \((r_1, r_2, \ldots, r_v)\), where \( 0 \leq r_i < m_i \), there exists one and only one integer \( N \) such that \( 0 \leq N < M_I \) and \( r_i = N \pmod{m_i} \), which allows us to uniquely recover the message \( N \) from the received residue digits. The process that transforms the residue number system to the weighted number system is defined as the inverse RNST (IRNST).

For incorporating error control [3][6], the RNS has to be designed with redundant moduli, which is referred to as a redundant RNS (RRNS) code. An RRNS code is obtained by appending an additional \((u - v)\) number of moduli \( m_{v+1}, m_{v+2}, \ldots, m_u \), to the previously introduced RNS, in order to form an RRNS code of \( u \) positive, pairwise relative prime moduli. The so-called redundant moduli have to obey \( m_{v+j} \geq \max \{m_1, m_2, \ldots, m_v\} \). Now an integer \( N \) in the range \([0, M_I]\) is represented as a \( u \)-tuple residue sequence, \((r_1, r_2, \ldots, r_u)\) with respect to the \( u \) moduli and consequently forms an RRNS\((u, v)\) code.

The RNS and RRNS have drawn wide attention in the field of designing high-speed parallel signal processing structures [3][7]. There are two inherent features that render the RNS and RRNS attractive in comparison to conventional weighted number systems, such as for example the binary representation. These two features are [1], [3]:1) the carry-free arithmetic and 2) the lack of ordered significance amongst the residue digits. The first property implies that the operations related to the different residue digits are mutually independent and hence the errors occurring during addition, subtraction and multiplication operations, or due to the noise induced by transmission and processing, remain confined to their original residues. In other words, these errors do not propagate and hence
do not contaminate other residue digits due to the absence of a carry forward. The second property of the RNS arithmetic implies that redundant residue digits can be discarded without affecting the result, provided that a sufficiently high dynamic range is retained by the reduced system in order to unambiguously describe the non-redundant information symbol.

As it is well known in VLSI design, usually systolic architectures are invoked to divide a processing task into several simple tasks performed by small, (ideally) identical, easily designed processors. Each processor communicates only with its nearest neighbour, simplifying the interconnection design and test, while reducing signal delays and hence increasing the processing speed. Due to its carry-free property, the RNS arithmetic further simplifies the computations by decomposing a problem into a set of parallel, independent residue computations.

The properties of the RNS arithmetic suggest that an RRNS can be used for self-checking, error-detection and error-correction in digital processors. The RRNS technique provides a useful approach to the design of general-purpose systems, capable of sensing and rectifying their own processing and transmission errors. For example, if a digital filter is implemented using the RRNS with sufficient redundancy, then errors in the processed signals can be detected and corrected by the RRNS-based decoding. Furthermore, it seems that the RRNS approach [1] is the only one, in which it is possible to use the very same arithmetic module in the very same way for computations of both the information part and the parity part of a RRNS codeword. In conventional communication system design, error protection of signals in the process of signal processing and during signal transmission is treated separately. However, in most situations the RRNS can be used not only for the protection of the signals while they are being processed in the transceivers, but also for enhancing the system’s performance over the communication channel. From this point of view, the communication system might be simplified by simplifying the whole encoding and decoding procedure.

The $M$-ary orthogonal keyed (MOK) communication scheme [15] - where a set of $M$ mutually orthogonal signals is utilized for the transmission of data - is a widely used arrangement [16]. Examples of orthogonal signals suitable for MOK are sine waves having $M$ number of uniformly spaced frequencies, leading to $M$-ary Frequency Shift Keying (MFSK). In the field of code division multiple access (CDMA) spread-spectrum communications, typically waveforms using $M$ number of orthogonal pseudo-random spreading codes [17]-[20] are employed for $M$-ary signalling. Explicitly, the non-binary RRNS code symbols are amenable to transmission using $M$-ary orthogonal signaling schemes. Hence, in this two-part paper, we focus on studying the performance of the RNS and RRNS in the context of $M$-ary orthogonal signaling schemes.

The contribution of this two-part paper is that we offer a generalized performance analysis of RNS-
based MOK over Gaussian and multipath Rayleigh fading channels. In the first part, we concentrate on the system’s description, on the inherent properties of the RNS and on its performance evaluation over additive white Gaussian noise (AWGN) channels. We will investigate the system under different design criteria, using different number of redundant moduli. The effects of forward error control (FEC) coding, interleaving, diversity combining, etc. over Rayleigh fading channels are treated in Part II of the paper. Our numerical results show that the system’s BER performance can be improved by exploiting the inherent properties of the RNS arithmetic.

The remainder of part I is organized as follows. Section II presents the communication model, while Section III and IV present the performance analysis of the RNS arithmetic based orthogonal signaling system with or without redundant moduli. Our numerical results and their interpretations are given in Section V, while our conclusions are offered at the end of part II. Let us first consider the communication model.

II. Communication Model

A. Transmitter and Channel Model

The transmitter block diagram of the proposed RNS-based orthogonal communication system is shown in Fig.1. As mentioned before, the information to be transmitted is transformed by the RNST block to the residue sequence \((r_1, r_2, \ldots, r_u)\), and the residue digits are then mapped to a set of orthogonal signals \((U_{1r_1}(t), U_{2r_2}(t), \ldots, U_{ur_u}(t))\) and multiplexed for transmission. More rigorously, let

\[
\begin{align*}
\left\{ & U_{10}(t), U_{11}(t), \ldots, U_{1(m_1-1)}(t); \\
& U_{20}(t), U_{21}(t), \ldots, U_{2(m_2-1)}(t); \\
& \quad \vdots \\
& U_{u0}(t), U_{u1}(t), \ldots, U_{u(m_u-1)}(t). \right. \\
\end{align*}
\]

be a set of \(\sum_{i=1}^{u} m_i\) complex-valued orthogonal signals, which are used for signal transmission. The subset \(\{U_{i0}(t), U_{i1}(t), \ldots, U_{i(m_i-1)}(t)\}\) of Eq.(1) for \(i = 1, 2, \ldots, u\) is used for the transmission of the residue digit \(r_i\). In Eq.(1), the orthogonal signals’ power is given by:

\[
\xi_i = \frac{1}{2} \int_0^T |U_{ij}(t)|^2 dt
\]

for \(i = 1, 2, \ldots, u\) and \(j = 0, 1, \ldots, m_i - 1\), if we assume that each signal of the orthogonal signal set used for transmitting a specific residue digit has equal power, where \(T\) represents the signaling interval duration. The orthogonality is expressed as:

\[
\int_0^T U_{ij}(t)U_{ij'}^*(t) dt = \begin{cases} 2\xi_i, & (i = i', j = j') \\ 0, & \text{(otherwise).} \end{cases}
\]
In order to transmit an information symbol, whose value is $N$, which is confined to the dynamic range $0 \leq N < \prod_{i=1}^{u} m_i$ of the system using non-redundant RNS, the symbol is first transformed to the RNS representation of $(r_1, r_2, \ldots, r_u)$, which we refer to as the residue sequence. Then the orthogonal signal set \( \{U_{1r_1}(t), U_{2r_2}(t), \ldots, U_{ur_u}(t)\} \) is obtained from the residue sequence as seen in Fig.1, i.e. by assigning an orthogonal code to each residue digit $r_i$. We note that if for practical reasons perfect code orthogonality cannot be maintained, each residue digit of a symbol interferes with other residue digits of the same symbol, inevitably degrading the system’s performance. Finally, the set of $u$ orthogonal signals, \( \{U_{1r_1}(t), U_{2r_2}(t), \ldots, U_{ur_u}(t)\} \) are combined in the transmitter of Fig.1 and this composite signal modulates the carrier, yielding the transmitted signal expressed as:

$$s(t) = \text{Re}\left[\sum_{i=1}^{u} U_{ir_i}(t) \exp(j2\pi f_c t)\right]$$

for $0 \leq t < T$, where $f_c$ is the carrier frequency. Since in the proposed system multiple orthogonal signals are combined linearly, as seen in Eq.(4), high peak-to-average amplitude ratios can be encountered, potentially resulting in nonlinear distortion. Techniques minimizing the envelope fluctuations after linear combining of multiple signals have been proposed in a number of publications [21]-[22]. However, due to space limitations these issues are beyond the scope of this contribution.

According to Eqs.(2) and (3), the total energy of $s(t)$ per symbol period can be directly computed as

$$\xi = \int_0^T s^2(t) dt = \sum_{i=1}^{u} \xi_i,$$

where the orthogonal signals’ power $\xi_i$ was expressed in Eq.(2)

We assume that the channel has no bandwidth limitations, simply attenuates the signaling waveforms transmitted, delays them in time and corrupts them by the addition of Gaussian noise. Hence, the lowpass equivalent received signal may be expressed in the form of:

$$r(t) = \alpha e^{j\phi} \sum_{i=1}^{u} U_{ir_i}(t - \tau) + N(t),$$

where $\alpha$ represents the channel attenuation factor, $\tau$ is the time delay, $\phi = -2\pi f_c \tau$ is the delay-induced phase rotation and $N(t)$ represents a zero mean Gaussian stationary random process with single-sided power spectrum density of $N_0$. Let us now consider the receiver’s operation with the aid of Fig.2.

**B. The Receiver**

Fig.2 portrays the proposed coherent receiver designed for receiving the RNS-based orthogonal signals in the form of Eq.(6). The receiver is constituted by three Sections. Section I consists of $u$ number of banks of correlators, where each bank is dedicated to receiving one residue digit from the set of
\{r_1, r_2, \ldots, r_u\}. According to the first property of the RNS arithmetic, the operations based on the residue digits belonging to the different moduli, \(m_i, \ i = 1, 2, \ldots, u\) are mutually independent, hence the receiver banks of different residue digits in Fig.2 are independent. Therefore, each bank structure of the receiver in Fig.2 is optimum for the AWGN channels considered in part I of this paper, and the receiver is optimum for the given received power of each residue digit. However, we will see in Section V that for a given total transmitted power, different system error probabilities are achieved by distributing different transmitted powers for the transmission of different residue digits.

According to the second property of the RNS arithmetic, if the RNS is designed with redundant moduli using the RRNS, then some of the channel-impaired received residue digits can be discarded as an error correction measure, provided that a sufficiently high dynamic range is retained by the reduced-range system, in order to unambiguously decode the result. The above statement can be augmented as follows. Let \(\{m_1, m_2, \ldots, m_u\}\) be a set of \(u\) moduli of an RRNS, where \(m_1 < m_2 < \cdots < m_u\). Let \(N\) be the value of an information symbol, which is now expressed as the residues \((r_1, r_2, \ldots, r_u)\) with respect to the above moduli. If the dynamic range of \(N\) is \([0, \prod_{i=1}^{v} m_i]\), where \(v \leq u\), then \(N\) can be recovered from any \(v\) out of the \(u\) number of residue digits and their relevant moduli. This property implies that - after the maximum likelihood detection (MLD) stage of the \(u\) receiver banks - \(d\) \((d \leq u - v)\) number of MLD outputs can be dropped before the IRNST stage, while still recovering the transmitted symbol \(N\) using the retained MLD outputs, provided that the retained MLD outputs are those matched to the related residue digits. Alternatively, the residue digit errors in the retained MLD outputs can be corrected using the redundant redundant residue number system decoder. The variables \(\lambda_i\) for \(i = 1, 2, \ldots, u\) in Fig.2 are computed in the process of demodulating the residue digits and they are used as the metrics for making decisions as to which MLD outputs will be dropped before RRNS decoding, an issue that will be discussed in Section IV.

Given the properties of the RNS arithmetic, here we propose RRNS codes for error-control. RRNS codes can be constructed according to the characteristics of the RNS arithmetic [4]-[6]. They are so-called maximum-distance-separable codes [6]. A RRNS\((u, v)\) code, where the information dynamic range is \([0, \prod_{i=1}^{v} m_i]\) and the total code dynamic range is \([0, \prod_{i=1}^{u} m_i]\), has a minimum distance of \((u - v + 1)\) and hence it is capable of detecting \((u - v)\) or less residue digit errors or correct up to \(t_{\text{max}} = \lfloor (u - v)/2 \rfloor\) residue digit errors. Alternatively, a RRNS\((u, v)\) code is capable of correcting a maximum of \(t\) residue digit errors and simultaneously detect a maximum of \(\beta > t\) residue errors, provided that \(t + \beta \leq u - v\).
Algorithms for RRNS decoding can be found in [4]-[6].

However, if we let \( d \) be the number of discarded residue digits, where \( d \leq u - v \), then, a RRNS\((u,v)\) is converted to a RRNS\((u-d,v)\) after \( d \) out of the \( u \) residue digits are discarded. Hence, the reduced RRNS\((u-d,v)\) code can detect up to \( [u - v - d] \) residue digit errors and correct up to \( [(u - v - d)/2] \) residue digit errors. This property suggests that the RRNS\((u,v)\) decoding can be designed by first discarding \( d \) \( (d \leq u - v) \) out of the \( u \) outputs of the MLDs in Section I of Fig.2, which is followed by RRNS\((u - d,v)\) decoding. Since the discarded outputs are not required to be considered in the RRNS\((u - d,v)\) decoding, the decoding procedure is therefore simplified.

Accordingly, as seen in Fig.2, Section II of the receiver is used to implement the above RNS-processing, such as ‘error-correction only’, ‘error-dropping only’ as well as ‘error-dropping-and-correction’. The performance of this system will be analyzed in the forthcoming Sections.

After the RNS-processing, the set of \( v \) retained residue digits of the RNS-processing outputs are input to the IRNST block of Fig.2 (Section III), and the estimation of the information symbol \( N \) ensues according to known RNS decoding algorithms [8]-[9]. Now, we focus our attention on the performance analysis of the proposed algorithms. We note here that readers mainly interested in the system’s BER performance, rather than in its mathematical characterisation, can proceed to Section V.

III. AVERAGE BIT-ERROR RATE WITHOUT RNS-PROCESSING

In this section, we derive the expression of the bit error probability for the proposed system over AWGN channels without RNS-processing. This implies that \( v = u \) and all moduli are used for signal transmission, or in other words, the dynamic range of the transmitted symbols is given by \([0, \prod_{i=1}^{\omega} m_i]\).

Note that the expressions of the bit error rate are reduced to the corresponding conventional formulae for the \( M \)-ary orthogonal signalling scheme discussed in [15] [pp.248-254], when \( u = 1 \).

Due to the independence of different residue digits of the RNS, we may compute the system’s bit error probability by first computing the error probabilities for receiving the residue digits separately. Then the system’s average error probability per bit can be obtained by exploiting the properties of the RNS arithmetic.

When a coherent receiver is considered, the set of decision variables can be written as [15][p.248,
\[ U_{ij} = \text{Re} \left[ e^{-j\phi} \int_0^T r(t)U_{ij}^*(t)dt \right] \]
\[ j = 0, 1, \ldots, m_i - 1 \]

Eq. (4.2.43)]:

for receiving residue digit \( r_i \), \( i = 1, 2, \ldots, u \), where \( \phi \) is the carrier phase. Let us assume that the orthogonal sequences \( \{ U_{i0}(t), i = 1, 2, \ldots, u \} \) are selected for transmitting the residue sequence \( (0, 0, \ldots, 0) \). Then, the decision variables can be expressed as:

\[ U_{i0} = 2\alpha \xi_i + N_{i0}, \quad (8) \]
\[ U_{ij} = N_{ij}, \quad (9) \]

for \( j = 1, 2, \ldots, (m_i - 1) \) and a given \( i \), where

\[ N_{ij} = \text{Re} \left[ e^{-j\phi} \int_0^T N(t)U_{ij}^*(t)dt \right] \]

are zero mean Gaussian random variables with variance \( \sigma_i^2 = 2\xi_i N_0 \). Consequently, the probability density functions (PDF) of the decision variables \( U_{i0}, i = 1, 2, \ldots, u \) and \( U_{ij}, j = 1, 2, \ldots, m_i - 1 \) for a given index \( i \) are given by [15][p.248, Eq.(4.2.48)]. After normalization by the mean-square noise power of \( \sigma_i \), the above distributions are given by:

\[ f_{U_{i0}}(x) = \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{(x - \sqrt{2\gamma_i})^2}{2} \right), \text{ for } i = 1, 2, \ldots, u, \quad (11) \]
\[ f_{U_{ij}}(x) = \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{x^2}{2} \right), \text{ for } j = 1, 2, \ldots, (m_i - 1) \text{ and for a given } i, \quad (12) \]

where \( \gamma_i = \alpha^2 \xi_i / N_0 \) denotes the output signal-to-noise ratio (SNR) of the demodulator dedicated to receiving residue digit \( r_i \). Moreover, if we let \( U_{ij,\text{max}} = \max \{ U_{ij} \text{ for all } j \neq 0 \} \) for a given \( i \), then the PDF of \( U_{ij,\text{max}} \) can be expressed as (Appendix I):

\[ f_{U_{ij,\text{max}}}(x) = \frac{m_i - 1}{\sqrt{2\pi}} [1 - Q(x)]^{m_i-2} \exp \left( -\frac{x^2}{2} \right), \quad (13) \]

where \( Q(y) \) is the Q-function, which is defined as:

\[ Q(y) = \frac{1}{\sqrt{2\pi}} \int_y^\infty \exp \left( -\frac{t^2}{2} \right) dt. \quad (14) \]

The probability \( P_i(C) \) of correctly receiving the residue digit \( r_i \) is the probability that \( U_{i0} \) exceeds all other decision variables \( U_{i1}, U_{i2}, \ldots, U_{i(m_i - 1)} \) within its residue bank in Fig. 2, or the probability that \( U_{i0} \) exceeds \( U_{ij,\text{max}} \), which can be computed as [15][p.249, Eq.(4.2.51)]:

\[ P_i(C) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^\infty [1 - Q(y)]^{m_i-1} \exp \left( -\frac{(y - \sqrt{2\gamma_i})^2}{2} \right) dy \quad (15) \]
for \( i = 1, 2, \ldots, u \).

Since no redundant moduli are considered in this section, a symbol is received correctly if and only if all residue digits are received correctly. Hence, the probability \( P_s(C) \) of correct symbol recovery can be expressed as the product of receiving all residue digits constituting the symbol correctly, which is given by:

\[
P_s(C) = \prod_{i=1}^{u} P_i(C)
\]

and hence the bit error probability \( P_b(\varepsilon) \) can be derived following a similar approach to Proakis’ [15][p.249], yielding:

\[
P_b(\varepsilon) \approx \frac{1}{2}(1 - P_s(C)),
\]

when \( M = \prod_{i=1}^{u} m_i \) is a large integer, implying a high number of bits/symbol.

When \( u = 1 \), Eq.(17) is simply reduced to the bit error probability of the conventional \( M \)-ary orthogonal signaling system [15][p.248]. However, if the conventional \( M \)-ary orthogonal signaling system has the same number of bits per symbol period, as the RNS-based system, then

\[
M = \prod_{i=1}^{u} m_i
\]

must be satisfied. This implies that for the conventional \( M \)-ary orthogonal signaling system \( M = \prod_{i=1}^{u} m_i \) number of correlators are required, in order to demodulate \( \log_2(\prod_{i=1}^{u} m_i) \)-bit symbols, in contrast to the proposed RNS-based parallel orthogonal signaling scheme, in which only \( (\sum_{i=1}^{u} m_i) \) number of correlators are necessitated.

As an example, let us consider the system in the first line of Table I in Part II of the paper, transmitting \( k = 30 \) bits per symbol and hence requiring \( 2^{30} = 1,073,741,824 \) correlators, which is clearly impractical for any application. By contrast, the proposed RNS-based system needs \( 29 + 31 + 32 + 33 + 35 + 37 + 41 = 238 \) correlators. This attractive implementational advantage provides a strong justification for investigating the proposed RRNS-based \( M \)-ary transceivers. In the following section we derive the expressions of the bit error probabilities for the RNS-based system having redundant moduli, i.e. after RNS-processing in Fig.2.

### IV. Average Bit-Error Rate with RNS-Processing

In this section we derive the BER expression of the RRNS-based orthogonal system, when redundant moduli are considered. In this part of the paper an approximation is proposed for computing the BER over the AWGN channel, in order to render the numerical computations tractable. By contrast, accurate BER computations are invoked over Rayleigh fading channels in Part II of the paper. We also assume an equal energy for the different residue digits in the following analysis. We also note
that all equations derived in this section and in section IV of Part II are suitable for the average BER computation of Reed-Solomon (RS) coded systems [25] using similar design criteria. In order to characterise the BER performance of RS codes, we simply replace the corresponding moduli \( m_i \) of the RRNS in the computations by a constant value of \( m = 2^b \), which is the dynamic range of the RS coded symbols and \( b \) is the number of bits per RS coded symbol. In Section IV of Part II we will elaborate on this issue further.

The properties of the RNS arithmetic indicate that, if a RNS-based orthogonal signaling scheme is designed with \((u-v)>0\) number of redundant moduli, then up to \((u-v)\) number of MLD outputs in Fig.2 can be dropped before the IRNST, while still recovering the transmitted symbol using the retained MLD outputs, provided that the retained MLD outputs are those matched to the related residue digits. Conventionally, this kind of dropping is referred to as ‘erasure’. An example of this is known in the context of RS codes [25], where the lowest-reliability symbols are erased and ‘error-and-erasure’ decoding is employed. In the proposed system we introduced the so-called ratio statistic test (RST). A relative of this test was defined as the ratio threshold test (RTT) by Viterbi [24] due to invoking a threshold in his system. In this paper the RST is used in the demodulation process in order to decide, which MLD outputs of Fig.2 may be dropped in the RNS-processing before RRNS decoding or the IRNST. The RST of the correlator bank for receiving residue digit \( r_i, i = 1, 2, \ldots, u \) is defined as [24]:

\[
\lambda_i = \frac{1}{2} \frac{\max_i \left\{ U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)} \right\}}{\max_i \left\{ U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)} \right\}},
\]

where \( \max_i \{ \cdot \} \) and \( \max_i \{ \cdot \} \) represent the maximum and the ‘second maximum’ of the correlator outputs of \( \left\{ U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)} \right\} \), respectively, which are invoked for detecting residue digit \( r_i \). The RST is based on the fact that an unreliable received signal is likely to have nearly equal energy in both the correlation branch matched to the transmitted signal and the correlation branches mismatched to the transmitted signal, in particular, as far as the second largest one in concerned. More explicitly, let the residue sequence \((0, 0, \ldots, 0)\) be transmitted. Then the noise-contaminated PDFs of \( U_{i0} \) and \( U_{ij,\text{max}} \) for \( i = 1, 2, \ldots, u \), which are given in Eqs.(11) and (13), are shown in Fig.3 for an AWGN channel at a bit-SNR of 2dB. Let us assume that \( H_1 \) and \( H_0 \) represent the hypotheses that a residue digit is demodulated correctly and erroneously, respectively. Then - under the error-free reception hypothesis of \( H_1 \) - the amplitudes of \( U_{i0} \) and \( U_{ij,\text{max}} \) are most likely to reside in the area of \( S \) and \( N \) of Fig.3, respectively. However, if the residue digit \( r_i \) is decided erroneously - i.e. under the hypothesis of \( H_0 \) - both the amplitudes of \( U_{i0} \) and \( U_{ij,\text{max}} \) are most likely to reside in the area of \( E \). Since they are comparable in size, we often arrive at erroneous decisions. Accordingly, we can argue that the absolute
value of $\lambda_i$, i.e $|\lambda_i|$ under the error-free reception hypothesis $H_1$ is usually higher than that under the erroneous reception hypothesis of $H_0$. Consequently, we can assume that the demodulator outputs having the lowest absolute value of $\lambda_i$ for the RST are the lowest-reliability outputs. The exact PDFs of $\lambda_i$ under the assumptions of $H_1$ and $H_0$ are given in Appendix II. Finally, the PDFs of $|\lambda_i|$ under assumptions $H_1$ and $H_0$ can be expressed as:

$$f_{|\lambda_i|}(y|H_0) = f_{\lambda_i}(y|H_0) + f_{\lambda_i}(-y|H_0), \quad y \geq 0,$$

(20)

where $\theta \in \{1, 0\}$.

The exact PDFs of $f_{|\lambda_i|}(y|H_1)$ and $f_{|\lambda_i|}(y|H_0)$ are shown in Fig.4 at SNRs per bit of 2dB and 6dB, when moduli of $m_i = 16$ and $m_i = 32$ are considered. As expected, when a residue digit is demodulated correctly, the value of $|\lambda_i|$ most probably resides in the area of $y > 1$, while under $H_0$, the value of $|\lambda_i|$ is likely to be close to $y = 1$. As evidenced by Fig.4, when increasing the SNR per bit, the distribution of $f_{|\lambda_i|}(y|H_1)$ will shift to the right for a given value of $m_i$. Moreover, when increasing the SNR per bit or the value of $m_i$, the peak of the distribution of $f_{|\lambda_i|}(y|H_0)$ at $y = 1$, i.e. the peak of the distribution under the erroneous decision hypothesis becomes higher. These phenomena can be explained with reference to Fig.3 as follows. Let $U_{i0}$ be the correlator output matched to the transmitted residue digit $r_i$, while $\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\}$ be the correlator outputs mismatched to $r_i$. Then, since $U_{i0}$ was not the maximum correlator output, under the erroneous decision hypothesis $H_0$, the expression of $^{1}\max \{\cdot\}$ in Eq.(19) obeys:

$$^{1}\max \left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\} = \max \left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}. \quad (21)$$

Furthermore, when carrying out an erroneous decision, we found that in AWGN the most likely event is that $U_{i0}$ is the second largest correlator output and hence the ‘second maximum’, namely $^{2}\max \{\cdot\}$ in Eq.(19) obeys:

$$^{2}\max \left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\} \leq ^{2}\max \left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\} \leq ^{1}\max \left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}. \quad (22)$$

It can be shown mathematically that under the erroneous decision hypothesis $H_0$ and for a given SNR per bit we have $^{2}\max \left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\} \approx ^{1}\max \left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}$, i.e when using a high value of $m_i$, statistically both the first maximum and the second maximum of the correlator outputs dedicated to receiving the residue digit $r_i$ take a similar value. Consequently, the distribution peak of their ratio, namely that of $f_{|\lambda_i|}(y|H_0)$ at $y = 1$ is increased, when increasing the value of $m_i$. Viewing the same phenomenon from a different perspective in AWGN, for a given value of $m_i$ and for a high SNR per bit, i.e when the effects of noise are negligible, the second maximum of the correlator outputs
dedicated to receiving residue digit \( r_i \) is the most likely error event under \( H_0 \), which is most likely to happen around the crossing point of the curves of \( f_{U_{i0}}(x) \) and \( f_{U_{ij,\text{max}}}(x) \) in Fig.3. Consequently, both the first maximum and the second maximum of the correlator outputs dedicated to receiving residue digit \( r_i \) have a similar value, which increases the PDF peak of their ratio, namely that of \( f_{|\lambda|_i}(y|H_0) \) at \( y = 1 \). Furthermore, from the results of this Part of the paper concerning AWGN and the results of the forthcoming Part II concerning multipath fading we can argue - without a formal proof - that the distribution of \( f_{|\lambda|_i}(y|H_0) \) tends to a Dirac pulse, when increasing the value of \( m_i \) towards infinity.

However, using the exact PDFs of \( f_{|\lambda|_i}(y|H_0) \) in order to estimate the BER after IRNST is an arduous task due to the quadruple or even higher number of embedded integrals involved. Hence, we invoke approximations in order to simplify the computations. Firstly, under the error-free decision hypothesis \( H_1 \), the PDFs of \( 1_{\text{max}} \{ \cdot \} \) and \( 2_{\text{max}} \{ \cdot \} \) can be approximated by the individual PDFs in Eq.\( (11) \) and Eq.\( (13) \), respectively, when the SNR per bit is sufficiently high, which leads to the terms of \([1 - Q(y)], P_i(C)\) and \( Q(y - \sqrt{2\gamma})\) becoming near-unity in the effective area of \( f_{\text{max}}(y|H_1) \) and \( f_{2_{\text{max}}}(y|H_1) \). These approximations also imply that under the error-free decision hypothesis \( H_1 \) the PDFs of \( 1_{\text{max}} \{ \cdot \} \) and \( 2_{\text{max}} \{ \cdot \} \) are the unconditional PDFs of the correlator output matched to the transmitted residue digit and the maximum amongst the other correlator outputs mismatched to the transmitted residue digit, respectively. Using the above approximation, we can obtain the PDF of \( \lambda_i \) under \( H_1 \), which is formulated as:

\[
f_{\lambda_i}(y|H_1) = \begin{cases} \frac{(m_i - 1)}{2\pi P_i(C)} \int_0^\infty x \cdot \exp \left(-\frac{x^2}{2} \right) \cdot \left\{ [Q(x)]^{m_i - 2} \exp \left(-\frac{(xy + \sqrt{2\gamma})^2}{2} \right) + [1 - Q(x)]^{m_i - 2} \exp \left(-\frac{(xy - \sqrt{2\gamma})^2}{2} \right) \right\} \, dx, & y \leq 1, \\\rac{(m_i - 1)}{2\pi P_i(C)} \int_0^\infty x \cdot \exp \left(-\frac{x^2}{2} \right) \left[1 - Q(x)\right]^{m_i - 2} \exp \left(-\frac{(xy - \sqrt{2\gamma})^2}{2} \right) \, dx, & y > 1, \end{cases}
\]

where \( P_i(C) \) represents the probability that \( U_{i0} \) exceeds \( U_{ij,\text{max}} \), ie \( P_i(C) \) is the correct reception probability of residue digit \( r_i \), which is given by Eq.\( (15) \). Secondly, we approximate the PDF of \( |\lambda_i| \) under the erroneous decision hypothesis \( H_0 \) by a Dirac pulse, i.e \( f_{|\lambda|_i}(y|H_0) = \delta(y - 1) \). Note that the first approximation increases the estimated BER, since the PDFs of \( 1_{\text{max}} \{ \cdot \} \) and \( 2_{\text{max}} \{ \cdot \} \) are assumed unconditionally to reside in the area \( E \) of Fig.3, rather than residing there conditionally, which consequently increases the PDF overlap probability that is indicative of the BER. By contrast, the second approximation decreases the estimated BER, since the distribution of \( f_{|\lambda|_i}(y|H_0) \) is more noise-resilient, when \( y > 1 \), since increased noise-samples are required for its corruption. However, when the SNR per bit of the transmitted signal is sufficiently high, the estimated result is very close
Having determined the PDFs of $|\lambda_i|$ under $H_1$ and $H_0$, we now estimate the BER by first estimating the correct symbol probability after the IRNST block in Fig. 2. After obtaining the correct symbol probability, the average BER can be estimated using Eq. (17).

Let $t$ represent the number of residue digit errors encountered in the received RRNS($u, v$) codeword, and let $s \leq d$ represent the actual number of residue digit errors discarded by dropping $d$ number of the lowest-reliability MLD outputs before RRNS($u - d, v$) decoding. Since a RRNS($u - d, v$) code can correct up to $t_{\text{max}} = \left\lfloor \frac{u - v - d}{2} \right\rfloor$ residue digit errors [6], a symbol is recovered without errors after IRNST, if $t$ and $s$ follow: (a) $0 \leq t \leq t_{\text{max}}$ or (b) $t_{\text{max}} + 1 \leq t \leq t_{\text{max}} + d$ and $s \geq t - t_{\text{max}}$, where (a) indicates that there were less than $t_{\text{max}}$ residue digit errors in the RRNS($u, v$) code and hence all were corrected. Condition (b) suggests that there were $t$ residue digits, which were received in error in the RRNS($u, v$) code, but the actual number of discarded errors, $s$, due to dropping $d$ number of the lowest-reliability MLD outputs exceeds $t - t_{\text{max}}$, which is the number of errors in excess of the error-correction capability $t_{\text{max}} = \left\lfloor \frac{u - v - d}{2} \right\rfloor$ of the RNS($u - d, v$). Both situations will lead to decoding success. Hence, the correct symbol probability after the IRNST block of Fig. 2 can be computed according to the following three cases.

A. ‘Error-Correction Only’ RNS-Processing

For this case, $d = 0$ leads to $s = 0$ and $t_{\text{max}} = \left\lfloor \frac{u - v}{2} \right\rfloor$. The residue digit errors are ‘error-correction only’ decoded by the RRNS decoding, but no other RNS-processing is carried out in Fig. 2. Consequently, the correct symbol probability after the IRNST block of Fig. 2 can be expressed as:

$$P_s(C) = \sum_{t=0}^{t_{\text{max}}} \left\{ \sum_{Q^t} \left[ \prod_{m=1}^{t} \left( 1 - P_{j_m}(C) \right) \prod_{n=1, n \neq m}^{u} P_{j_n}(C) \right] \right\}, \quad (24)$$

where $\prod_{i=1}^{0}() = 1$, $\{j_1, j_2, \ldots, j_u\}$ is a possible mapping of $\{1, 2, \ldots, u\}$ and $Q^t$ represents that $t$ out of $u$ of the MLD outputs $\{U_1, U_2, \ldots, U_u\}$ in Fig. 2 were decided wrongly, i.e. $t$ out of $u$ residue digits are received in error before the RNS-processing, but the other $(u - t)$ residue digits are error-free, while $\sum Q^t$ represents all possible selections of $t$ elements from $\{1, 2, \ldots, u\}$.

B. ‘Error-Dropping Only’ RNS-Processing

In this case $t_{\text{max}} = 0$ and hence $u - v = d$. The symbol is recovered correctly after IRNST in Fig. 2, if and only if all the $t$ number of residue digit errors are discarded by dropping the $d$ number of MLD outputs having the lowest value of $|\lambda_i|$. Accordingly, the correct symbol probability after the IRNST
block of Fig.2 can be expressed as:

\[ P_s(C) = \sum_{t=0}^{d} \left\{ \sum_{Q(n)} \left[ \prod_{n=1}^{t} (1 - P_{j_m}(C)) \prod_{n=1, n \neq m}^{u} P_{j_n}(C) \right] \right\} \cdot P(d, t), \quad (25) \]

where \( P(d, t) \) is the probability that \( t \) number of residue digit errors are successfully discarded by dropping \( d \) number of the lowest-reliability MLD outputs in Fig.2.

Let \( A = \{ |\lambda_{m_1}|, |\lambda_{m_2}|, \ldots, |\lambda_{m(u-t)}| \} \) represent the absolute ratio set, for which the residue digits are received correctly. Then, the probability of \( P(d, t) \) can be computed by:

\[ P(d, t) = \sum_{n=0}^{d-t} \left\{ \frac{t}{2^{t-1}} \sum_{Q(n)} \left[ \prod_{i=1}^{n} \int_{0}^{1} f_{|\lambda_{u_i}|}(y|H_1)dy \right] \prod_{j=1, j \neq i}^{u-t} \int_{1}^{\infty} f_{|\lambda_{u_j}|}(y|H_1)dy \right\}, \quad (26) \]

where \( \{ |\lambda_{u_1}|, |\lambda_{u_2}|, \ldots, |\lambda_{u(u-t)}| \} \) represents a possible mapping of \( \{ |\lambda_{m_1}|, |\lambda_{m_2}|, \ldots, |\lambda_{m(u-t)}| \} \). Note that in deriving Eq.(26), we used the approximation of \( f_{|\lambda|}(y|H_0)dy = \frac{1}{2} \). The detailed derivations of Eq.(26) and Eq.(28) can be found in Part II of this paper.

C. ‘Error-Dropping-and-Correction’ RNS-Processing

If the RNS-processing of Fig.2 is designed using ‘error-dropping-and-correction’, i.e \( t_{\text{max}} > 0, d > 0 \), then the transmitted symbol can be recovered correctly, if the residue digit errors due to the channel effects are dropped by dropping \( d \) number of the MLD outputs having the lowest values of \( |\lambda_i| \) and/or corrected by the RRNS\((u - d, v)\) decoding. Hence, the correct symbol probability after the IRNST block of Fig.2 can be expressed as:

\[ P_s(C) = \sum_{t=0}^{d+t_{\text{max}}} \left\{ \sum_{Q(n)} \left[ \prod_{n=1}^{t} (1 - P_{j_m}(C)) \prod_{n=1, n \neq m}^{u} P_{j_n}(C) \right] \right\} \cdot P(s \geq t - t_{\text{max}}), \quad (27) \]

where \( P(s \geq t - t_{\text{max}}) \) is the probability that the number of discarded residue digit errors is not less than \( t - t_{\text{max}} \). Accordingly, \( P(s \geq t - t_{\text{max}}) = 1 \) if \( t \leq t_{\text{max}} \). When \( t > t_{\text{max}} \), we have:

\[ P(s \geq t - t_{\text{max}}) = \sum_{n=0}^{d+t_{\text{max}}-t} \left\{ \frac{t}{2^{t-1}} \left( \frac{t}{t_{\text{max}}} \sum_{Q(n)} \left[ \prod_{i=1}^{n} \int_{0}^{1} f_{|\lambda_{u_i}|}(y|H_1)dy \right] \prod_{j=1, j \neq i}^{u-t} \int_{1}^{\infty} f_{|\lambda_{u_j}|}(y|H_1)dy \right\} \right\}, \quad (28) \]

where \( \{ |\lambda_{u_1}|, |\lambda_{u_2}|, \ldots, |\lambda_{u(u-t)}| \} \) represents a possible mapping of \( \{ |\lambda_{m_1}|, |\lambda_{m_2}|, \ldots, |\lambda_{m(u-t)}| \} \), and we used the approximation of \( f_{\lambda_i}(y|H_0)dy = \int_{1}^{\infty} f_{|\lambda_i|}(y|H_0)dy = \frac{1}{2} \) in the derivation of Eq.(28).

We note here that instead of the above RRNS codes, alternatively the well-known RS codes can be introduced for the protection of the parallel transmitted information.
symbols. Recall that RS codes are based on a constant value of $m = 2^b$ - where $b$ is the number of bits per symbol - and a similar BER performance is maintained for an RS$(u,v,t)$ and an RRNS$(u,v,t)$ code. This is because both codes constitute a class of maximum-distance-separable codes [25]. An RS$(u,v)$ code can correct up to $\left\lfloor \frac{u-v}{2} \right\rfloor$ errors and detect up to $u-v$ errors. Moreover, a RS$(u,v)$ code can correct up to $t_{max}$ errors and $d$ erasures, if and only if $2t_{max} + d \leq u-v$. Hence, upon using a RS$(u,v)$ code for the protection of the parallel transmitted information instead of the RRNS$(u,v)$ scheme described previously, up to $d = u-v$ number of the lowest-reliability outputs of the MLDs can be discarded, yielding a similar BER performance to that of the our proposed RNS-based system. However, if an MLD output is discarded, the RS decoding interprets the related symbol as an erasure, and error-and-erasure correction decoding is used for error correction and erasure filling [25]. Consequently, the decoding procedure cannot be simplified by discarding some outputs of the MLDs in Fig.2, and hence the decoding complexity cannot be decreased. Furthermore, there are very few short RS codes, which are suitable for parallel transmission, while it is easy to design arbitrary-length RRNS codes with a large variety of dynamic ranges. Short RS codes are usually designed by shortening long RS codes, which implies complex decoding algorithms, since shortened RS code decoding typically uses full-length decoding of the padded shortened code. The above similarities and dissimilarities of RS and RRNS codes were mentioned in order to link the less known RRNS codes to their better known relatives. However, RS coding of the parallel transmitted information is not discussed further in this paper.

V. Numerical Results and Analysis

In this section, the previously derived analytical expressions are numerically evaluated and interpreted. In Fig.5, we evaluated the influence of unequal residue digit energy on the BER. The moduli used were $(m_1,m_2,m_3) = (3,17,53)$, which did not achieve a near-maximum dynamic range, since that requires values close to $m_1 \approx m_2 \approx m_3$. Nevertheless, these different values allowed us to demonstrate the effect of unequal residue energy distribution. The symbol-SNR could be expressed as $\gamma = \alpha^2 \xi / N_0 = \alpha^2 (\xi_1 + \xi_2 + \xi_3) / N_0 = \gamma_1 + \gamma_2 + \gamma_3$ according to Eq.(5). This implied that we could examine the influence of unequal residue energy on the BER by changing the SNR per residue digit. Hence, we let the bit-SNR be $E_b / N_0 = 8dB$. Then the total SNR for transmitting the three residue digits can be computed by $\gamma = \log_2 (m_1 m_2 m_3) \cdot E_b / N_0$. Hence, by changing one of the $\gamma_1$, $\gamma_2$, $\gamma_3$ values, say $\gamma_i$, ($i = 1,2,3$) the other two follow the relation $\gamma_j = (\gamma - \gamma_i) / 2$ for $j \neq i$. Consequently,
three curves were obtained. The curves show that the equal residue energy scheme is not the optimum. Note that the point, where the three curves intersect represents the BER, when equal residue energy is assumed, i.e \( SNR = 10\log_{10} \left( \frac{\log_2(m_1m_2m_3) \cdot E_b/N_0) / 3} {3} \right) = 13.8dB \). In order to achieve the optimum performance, the curves show that less than the average energy should be allocated to those residue digits, whose moduli are less than the average. By contrast, more than average energy should be allocated to moduli larger than the average. However, for systems having approximately equal moduli, e.g. \( 2^n - 1, 2^n, 2^n + 1 \), the equal residue energy scheme can achieve near-optimum BER performance.

The BER performance of various non-redundant RNS-based systems using \( u = 2 \) moduli was computed according to Eq.(17) and (15), and the associated BER curves are shown in Fig.6. Throughout our experiments a range of different moduli values were assumed, which are explicit in the figures. In the computations equal energy residue digits were employed for the RNS-based system. The results show that when the values of moduli increased - in fact when the product of the two moduli increased - the BER decreased gracefully. This may be explained on the basis of Eq.(15), since when the product of \( m_1, m_2 \) increases, the dynamic range and the number of bits per symbol - \( k = \log_2(m_1m_2) \) - also increases, implying that the energy per symbol, or the energy used for transmitting each residue digit increases. Hence, the BER is decreased.

Fig.7 portrays the BER performance computed from the equations of Section IV conditioned on the assumption that the information bit energy was limited. In this figure we evaluated the effect of the error dropping and error correction policies on the BER performance of the proposed RNS-based orthogonal signaling scheme with \( u = 7 \) moduli. The parameters related to the computations were given in Table I, where \( k = \log_2 \left( \prod_{i=1}^{5} m_i \right) \) is the number of bits per symbol. The results of Fig.7 show that by designing the RNS-based orthogonal signaling scheme with redundant moduli, i.e upon using the proposed RRNS-based orthogonal signaling scheme, coding gain can be obtained to improve the BER performance for both ‘error-dropping only’ and ‘error-correction only’ RNS-processing. Using ‘error-dropping only’ RNS-processing, an SNR gain of about 1.5dB or 2.1dB can be achieved, respectively, using one or two redundant moduli at a bit error rate of \( 10^{-6} \). Using ‘error-correction only’ RNS-processing, only about 1dB SNR gain can be achieved using two redundant moduli at a bit error rate of \( 10^{-6} \). Hence, the RNS-based orthogonal signaling scheme with RST is an attractive communication scheme. This is because upon using \( d \) number of redundant moduli we can drop up to \( d \) number of residue digit errors and recover the codeword correctly by using the proposed RST based dropping scheme, while we can only correct up to \( d/2 \) residue digit errors by using our error-correction scheme.

Similarly, in Fig.8 we evaluated the BER performance of the RNS-based orthogonal system, when ‘error-dropping only’, ‘error-correction only’ and ‘error-dropping-and-correction’ RNS-processing were
considered. The parameters concerned were given in Table II. The results show that using the same number of redundant moduli, about twice as high SNR gain can be obtained upon using ‘error-dropping only’ RNS-processing than by ‘error-correction only’ RNS-processing. Part II of this paper considers the associated system performance over Rayleigh channels.

VI. Acknowledgement

The financial support of the following organisations is gratefully acknowledged: Motorola ECID, Swindon, UK; European Community, Brussels, Belgium; Engineering and Physical Sciences Research Council, Swindon, UK; Mobile Virtual Centre of Excellence, UK; The Royal Society, UK.

Appendix

I. The Probability Density Function of the \( \lambda \)-th maximum

In this Appendix we derive the probability density function (PDF) of the \( \lambda \)-th maximum of the independent random variables \( \{X_1, X_2, \ldots, X_n\} \), which may be expressed as:

\[
Y = \max_{\lambda} \{X_1, X_2, \ldots, X_n\},
\]

where \( X_i \) for \( i = 1, 2, \ldots, n \) follows the PDF of \( f_{X_i}(x) \). The distribution function of \( Y \) can be written as:

\[
P(Y < y) = \sum_{i=1}^{n} \sum_{Q(n-1, \lambda-1)} P \left( X_i > X_{i_1}, X_{i_2} > X_{i_1}, \ldots, X_{i_{\lambda-1}} > X_i; X_{j_1} < X_{i_1}, X_{j_2} < X_{i_1}, \ldots, X_{j_{n-\lambda}} < X_{i}; i, j_m \neq i | X_i = Y < y \right)
\]

\[
= \sum_{i=1}^{n} \sum_{Q(n-1, \lambda-1)} \int_{-\infty}^{y} P \left( X_{i_1} > x, X_{i_2} > x, \ldots, X_{i_{\lambda-1}} > x; X_{j_1} < x, X_{j_2} < x, \ldots, X_{j_{n-\lambda}} < x; i, j_m \neq i | X_i = x \right) f_{X_i}(x)dx,
\]

where \( \sum_{Q(n)} \) represents the sum of different selections of \( i \) out of \( n \). Note that at the second step of the above derivation, we assumed that \( X_i = Y \) was the \( \lambda \)-th maximum. Consequently, there were \( \lambda - 1 \) out of the remaining \( (n - 1) \) variables, whose values were lower than \( X_i \), and the values of the remaining \( (n - \lambda) \) variables were higher than \( X_i \). Since \( \{X_i\} \) for \( i = 1, 2, \ldots, n \) are independent random variables, Eq.(30) can be expressed as:

\[
P(Y < y) = \sum_{i=1}^{n} \sum_{Q(n-1, \lambda-1)} \int_{-\infty}^{y} \left( \prod_{l=1}^{\lambda-1} P(X_{i_l} > x) \right)
\]
\[
\left( \prod_{m=1}^{n-\lambda} P(X_{jm} < x) \right) f_{X_i}(x) dx.
\] (31)

After differentiating the above equation with respect to the variable \( y \), we finally obtained the PDF of Eq.(29) as:

\[
f_Y(y) = \sum_{i=1}^{n} \sum_{Q_{(\lambda-1)}} \left( \prod_{i=1}^{\lambda-1} P(X_{i} > y) \right) \left( \prod_{m=1}^{n-\lambda} P(X_{jm} < y) \right) f_{X_i}(y).
\] (32)

Note that when \( \lambda = 1 \) or \( \lambda = n \), and \( \{X_i\} \) obey identical distributions, then \( \sum_{Q_{(\lambda-1)}} \) and \( \sum_{Q_{(n-1)}} \) are equal to 1, and Eq.(32) represents the well-known PDF of the distribution \( Y = \max \{X_1, X_2, \ldots, X_n\} \) or \( Y = \min \{X_1, X_2, \ldots, X_n\} \), where the corresponding PDFs are written as [23]:

\[
f_Y(y) = n f_{X_i}(y) [P(X_j < y)]^{n-1},
\] (33)

and

\[
f_Y(y) = n f_{X_i}(y) [P(X_j > y)]^{n-1},
\] (34)

respectively.

II. The Probability Density Functions of the Ratio Statistic Test

Under Assumptions \( H_1 \) and \( H_0 \)

The aim of this Appendix is to derive the PDFs of the RST defined in Eq.(19), both under the hypotheses that the demodulator output is correct \( (H_1) \) and that it is in error \( (H_0) \). Under the assumption of \( H_1 \), the normalized PDFs of the maximum and the ‘second maximum’ of the correlator outputs \( \{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\} \) can be expressed as:

\[
f_{\text{max}}(y|H_1) = \frac{1}{P_i(C)} [1 - Q(y)]^{m_i-1} \cdot \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{(y - \sqrt{2\gamma_i})^2}{2} \right),
\] (35)

\[
f_{\text{second max}}(y|H_1) = \frac{m_i - 1}{P_i(C)} [1 - Q(y)]^{m_i-2} Q(y - \sqrt{2\gamma_i}) \cdot \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{y^2}{2} \right),
\] (36)

where \( P_i(C) \) is given by Eq.(15). Under the assumption of \( H_0 \), the PDFs can be expressed as:

\[
f_{\text{max}}(y|H_0) = \frac{m_i - 1}{1 - P_i(C)} \left[ 1 - Q(y - \sqrt{2\gamma_i}) \right] [1 - Q(y)]^{m_i-2} \cdot \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{y^2}{2} \right),
\] (37)

\[
f_{\text{second max}}(y|H_0) = \frac{m_i - 1}{1 - P_i(C)} Q(y) [1 - Q(y)]^{m_i-3} \left\{ [1 - Q(y)] \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{(y - \sqrt{2\gamma_i})^2}{2} \right) \right\} + (m_i - 2) \left[ 1 - Q(y - \sqrt{2\gamma_i}) \right] \cdot \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{y^2}{2} \right). \] (38)
 Consequently, the PDFs of \( \lambda_i = \frac{1}{\text{max}(\lambda)} \) conditioned on the assumption that the maximum is larger than the ‘second maximum’ and under the assumptions of \( H_1 \) and \( H_0 \) can be derived. Due to space limitations, we do not provide the intervening steps, only the results, which are given by:

\[
f_{\lambda_i}(y|H_1) = \begin{cases} 
\frac{m_i - 1}{2\pi |P_r(C)|^2 P(\text{max} > 2 \text{ max } |H_1|)} \int_0^\infty x \exp \left(-\frac{x^2}{2}\right) \\
\cdot \left\{ (Q(xy))^{M-1}[Q(x)]^{M-2} [1 - Q(x + \sqrt{2\gamma_i})] \exp \left(-\frac{(xy + \sqrt{2\gamma_i})^2}{2}\right) \\
+ [1 - Q(xy)]^{M-1}[1 - Q(x)]^{M-2} [Q(x - \sqrt{2\gamma_i})] \exp \left(-\frac{(xy - \sqrt{2\gamma_i})^2}{2}\right) \right\} dx, 
\end{cases}
\]

\[
\text{for } y \leq 1, \quad (39)
\]

\[
f_{\lambda_i}(y|H_0) = \begin{cases} 
\frac{(m_i - 1)^2}{2\pi |P_r(C)|^2 P(\text{max} > 2 \text{ max } |H_0|)} \int_0^\infty x \cdot Q(x)[1 - Q(x)] \exp \left(-\frac{x^2y^2}{2}\right) \\
\cdot \left\{ Q(x + \sqrt{2\gamma_i}) [Q(xy)]^{m_i-2} [Q(x)]^{m_i-4} \\
\cdot Q(x) \exp \left(-\frac{(x + \sqrt{2\gamma_i})^2}{2}\right) + (m_i - 2)Q(x + \sqrt{2\gamma_i}) \exp \left(-\frac{x^2}{2}\right) \right\} \right\} dx, 
\end{cases}
\]

\[
\text{for } y \leq 1, \quad (40)
\]

\[
\text{for } y > 1,
\]

where \( P(\text{max} > 2 \text{ max } |H_0|, \theta = 0, 1 \) represents the probability that the maximum exceeds the ‘second maximum’ of the correlator outputs \( \{U_i0, U_i1, \ldots, U_{i(m_i-1)}\} \).

**REFERENCES**


Fig. 1

The transmitter block diagram.


TABLE I

The Parameters Related to The Numerical Computations of Fig.7.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$t_{max}$</th>
<th>$k$</th>
<th>$m_1$</th>
<th>$m_2$</th>
<th>$m_3$</th>
<th>$m_4$</th>
<th>$m_5$</th>
<th>$m_6$</th>
<th>$m_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>25</td>
<td>29</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>25</td>
<td>29</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>35</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>25</td>
<td>29</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>35</td>
<td>37</td>
<td>41</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>25</td>
<td>29</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>35</td>
<td>37</td>
<td>41</td>
</tr>
</tbody>
</table>
Section I

Bank for receiving residue digit $r_1$

$\tau(t)$

$U_{i0}^*(t)$

$U_{i0}(t)$

$U_{i1}(m_{i-1})(t)$

Bank for receiving residue digit $r_u$

Select the largest (MLD)

RNS-processing

IRNST

Binary output

Section II

Section III

Fig. 2

The receiver block diagram with RNS-processing.

TABLE II

The Parameters Related to The Numerical Computations of Fig.8.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$t_{\text{max}}$</th>
<th>$k$</th>
<th>$m_1$</th>
<th>$m_2$</th>
<th>$m_3$</th>
<th>$m_4$</th>
<th>$m_5$</th>
<th>$m_6$</th>
<th>$m_7$</th>
<th>$m_8$</th>
<th>$m_9$</th>
<th>$m_{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>36</td>
<td>29</td>
<td>31</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>36</td>
<td>29</td>
<td>31</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td>47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>36</td>
<td>29</td>
<td>31</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td>47</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>36</td>
<td>29</td>
<td>31</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td>47</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>36</td>
<td>29</td>
<td>31</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td>47</td>
<td>53</td>
<td>59</td>
</tr>
</tbody>
</table>
Fig. 3

The noise-contaminated probability density function (PDF) \( f_{U_{i0}}(x) \), \( f_{U_{ij,\text{max}}}(x) \) according to Eqs.(11) and Eq.(13) for the modulus of \( m_i = 16 \) and an AWGN channel SNR per bit of \( \gamma_b = 2dB \).
Fig. 4

The probability density function (PDF) of $|\lambda_i| = \left| \frac{\lambda_{\text{max},i}}{\lambda_{\text{max},1}} \right|$ according to Eq.(20) under the hypothesis of $H_1$ and $H_0$, using the moduli of $m_i = 16$ and 32 at an AWGN channel SNR per bit of $\gamma_b = 2$dB and 6dB.
BER versus residue digit SNR $\gamma_1, \gamma_2$ and $\gamma_3$ for the RNS system, when unequal energy is distributed for the residue digits $r_1, r_2$ and $r_3$, $(m_1 = 3, m_2 = 17, m_3 = 53)$ computed from Eq.(17) and (15).

BER performance of various non-redundant RNS-based orthogonal signaling schemes with $u = 2$ moduli and a dynamic range of $M = m_1m_2$ computed from Eq.(17) and (15).
Fig. 7
BER versus SNR performance for the RRNS-based orthogonal signaling system with parameters given in Table I using Eqs.(25),(26) and (17).

Fig. 8
BER versus SNR performance for the RRNS-based orthogonal signaling system with parameters given in Table II using Eqs.(27)-(28) and (17).