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

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

***Abstract*—A novel signaling scheme is presented, where a set of orthogonal signals is transmitted in parallel. The signals 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's performance can be substantially improved by exploiting a number of advantageous properties of the RNS arithmetic.**

In Part I of this paper, we focus our attention on the system's description and on the associated background of the RNS arithmetic, as well as on the performance evaluation of the residue number system arithmetic, using both nonredundant and redundant moduli based orthogonal signaling schemes, over an additive white Gaussian noise (AWGN) channel. Redundant RNS codes are introduced in order to protect the transmitted information. The detection techniques used in this novel system are different from conventional detectors. Specifically, a novel decision algorithm, referred to as a ratio statistic test, 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. We argue that the demodulated/decoded information can be obtained by decoding the retained or undiscarded symbols upon exploiting the properties of the RNS arithmetic. Our numerical results show that the proposed scheme constitutes a high-efficiency parallel transmission method for high-bit-rate communication, achieving a coding gain of 2 dB at a bit error rate of 10^{-6} over AWGN channels.

***Index Terms*—Code-division multiple access (CDMA), error control, orthogonal signalling, parallel signalling, ratio statistic test, redundant residue number system (RRNS), residue number system (RNS).**

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 number system representation, using, for example, a base of 2, 8, 16, etc., for implementation, ultimately favoring the weighted binary system. In a conventional system—where the operands of the signal-processing steps are represented by the conventional weighted number 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 nonweighted, 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]–[22].

An RNS is defined [1] by the choice of v number of 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 of $0 \leq N < M_I$, where $r_i = N \pmod{m_i}$ represents the so-called residue digits of N upon division by the moduli m_i and $M_I = \prod_{i=1}^{v} m_i$ can be referred to as the information dynamic range, i.e., the legitimate range of the information symbols N. This is true, simply because the v number of moduli unambiguously describe any integer information symbol N in this range. In the above process, the algorithm that transforms any conventional weighted number system to the residue number system is defined as the residue number system transform (RNST). According to the so-called Chinese reminder theorem (CRT) [8], 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 [1]–[11], the RNS has to be designed with redundant moduli, yielding a so-called 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 $m_{v+j} \geq \max\{m_1, m_2, \ldots, m_v\}$ [5], [8], [10]. 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 number of 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 [5], [13]. There are two inherent features that render the RNS and RRNS attractive in comparison to conventional weighted

Manuscript received October 26, 1999; revised November 20, 2001. This work was supported by Motorola ECID, Swindon, U.K.; the European Community, Brussels, Belgium; the Engineering and Physical Sciences Research Council, Swindon, U.K.; the Mobile Virtual Centre of Excellence, U.K.; and The Royal Society, U.K.

The authors are with the Department of Electronics and Computer Science, University of Southampton, SO17 1BJ Southampton, U.K. (e-mail: lly@ecs.soton.ac.uk; lh@ecs.soton.ac.uk).

Digital Object Identifier 10.1109/TVT.2002.804850

number systems, such as, for example, the binary weighted number system representation. These two features are [1], [5]: 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[1], [5]. 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 above 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 resultant reduced RNS system in order to unambiguously describe the nonredundant information symbol.

As 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 neighbor, 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 code can be used for self-checking, error detection, and error correction in digital processors. The RRNS coding 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, the RRNS coding approach [1] is the only one where it is possible to use the very same arithmetic module in the very same way for the generation of both the information part and the parity part of an 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 operands or signals, while they are being processed in the transceivers, but also for enhancing the system's performance over the communication channel [11]. 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 [23], [24], [29]—where a set of M mutually orthogonal signals is utilized for the transmission of data—is a widely used arrangement. An example of orthogonal signals suitable for MOK is constituted by 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 pseudorandom spreading codes [25]–[30] are employed for M-ary signalling. A practical manifestation of such a scheme is the 64-ary uplink of the well-known IS-95 system. The results of this paper are applicable to this scenario; however, all the operations are cast here in the context of the RNS, which lends itself to a range of convenient novel detection procedures.

Explicitly, the nonbinary RRNS code symbols are amenable to transmission using M-ary orthogonal signaling schemes. Hence, in this two-part paper, we focus our attention on studying the performance of the RNS and RRNS codes in the context of M-ary orthogonal signaling schemes.

The contribution of this two-part paper is a generalized performance analysis of RNS-based MOK over Gaussian and multipath Rayleigh fading channels. In this, Part I, 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's performance 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 this 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 this paper is organized as follows. Section II presents the communication model, while Sections III and IV provide 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 proposed communication system 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 $(r_1, r_2, \ldots, r_u)$. 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

$$\left\{\begin{array}{c} U_{10}(t), U_{11}(t), \ldots, U_{1(m_1-1)}(t); \\ U_{20}(t), U_{21}(t), \ldots, U_{2(m_2-1)}(t); \\ \ldots\ldots; \\ U_{u0}(t), U_{u1}(t), \ldots, U_{u(m_u-1)}(t) \end{array}\right\} \tag{1}$$

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

$$\xi_i = \frac{1}{2}\int_0^T |U_{ij}(t)|^2\, dt \tag{2}$$

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

$$\int_0^T U_{ij}(t)U^*_{i'j'}(t)dt = \begin{cases} 2\xi_i, & (i = i', j = j') \\ 0, & \text{(otherwise).} \end{cases} \tag{3}$$

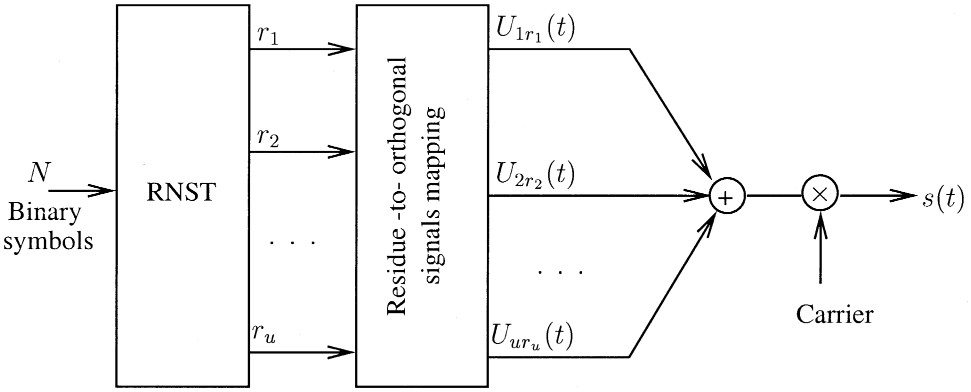

Fig. 1. The transmitter block diagram.

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 nonredundant 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 $\{U_{1r_1}(t), U_{2r_2}(t), \ldots, U_{ur_u}(t)\}$, is combined in the transmitter of Fig. 1. This composite signal modulates the carrier, yielding the transmitted signal expressed as

$$s(t) = \text{Re}\left[\sum_{i=1}^{u} U_{ir_i}(t) \exp\left(j2\pi f_c t\right)\right] \tag{4}$$

for $0 \leq t < T$, where f_c is the carrier frequency. Since in the proposed system u number of orthogonal signals are combined linearly, as seen in (4), high peak-to-average amplitude ratios can be encountered, potentially resulting in nonlinear distortion, unless "infinite dynamic range" linear amplification is assumed. Techniques minimizing the envelope fluctuations after linear combining of multiple signals have been proposed in a number of publications [31], [32]. However, due to space limitations, these issues are beyond the scope of this paper.

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

$$\xi = \int_0^T s^2(t)dt = \sum_{i=1}^{u} \xi_i \tag{5}$$

where the orthogonal signals' power ξ_i was expressed in (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 low-pass equivalent received signal may be expressed in the form of

$$r(t) = \alpha e^{j\phi} \sum_{i=1}^{u} U_{ir_i}(t - \tau) + N(t) \tag{6}$$

where α represents the channel attenuation factor, τ 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 (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 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 codes, 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 code, where $m_1 < m_2 < \cdots < m_u$. Let N be the integer message associated with a nonbinary 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 the nonbinary integer message 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 in Fig. 2—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

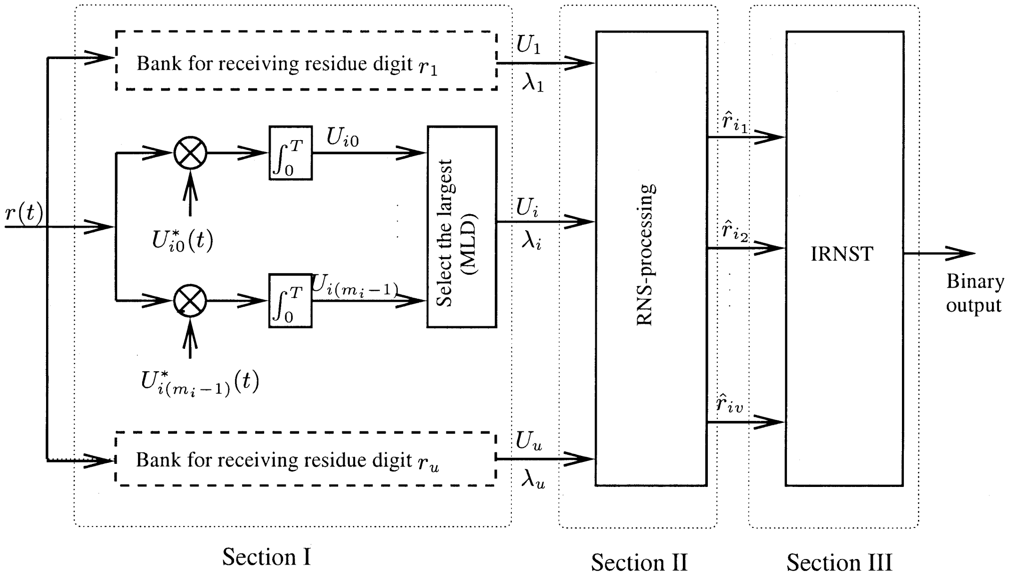

Fig. 2. The receiver block diagram with RNS processing.

the retained MLD outputs can be corrected using the RRNS decoder. The variables λ_i for $i = 1, 2, \ldots, u$ in Fig. 2 are computed in the process of demodulating the residue digits. 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 [6]–[8]. They are so-called maximum-distance-separable codes [8]. An 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 is capable of detecting $(u - v)$ or less residue digit errors or correct up to $t_{\max} = [(u - v)/2]$ residue digit errors. Alternatively, an RRNS(u, v) code is capable of correcting a maximum of t residue 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 [6]–[8].

However, if we let d be the number of discarded residue digits, where $d \leq u - v$, then an RRNS(u, v) code is converted to a RRNS$(u - d, v)$ code after d out of the u residue digits and their corresponding moduli 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 decoding, error-dropping-only decoding, and error-dropping-and-correction decoding. 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). The estimation of the information symbol N ensues according to known RNS decoding algorithms [14], [15].

The structures of the transmitter and receiver in the RNS-based or the RRNS-based parallel communication systems suggest that the moduli have to be selected according to the following criteria.

1) For a given information dynamic range N, the information can be uniquely and unambiguously represented by a residue digit sequence with respect to the moduli.
2) Since the sum of the modulus values determines the number of required correlators, the number of moduli and the modulus values must be selected such that their product is maximized and their sum is minimized. Hence, for a given number of moduli, the modulus values have to be selected to be as close to each other as possible for the sake of maximizing their product and minimizing their sum.

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 characterization—can directly proceed to Section V.

III. Average Bit Error Rate Without RNS Processing

In this section, we derive the expression of the BER 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, $\prod_{i=1}^{u} m_i$). Note that the expressions of the BER are reduced to the corresponding conventional formulas for the M-ary orthogonal signalling scheme discussed in [23], when $u = 1$.

Due to the independence of different residue digits in the RNS, we may compute the system's BER by first computing the error probabilities for receiving the residue digits separately. Then the system's average BER can be obtained by exploiting the previously stated properties of the RNS arithmetic, it will become explicit during our further discourse.

When a coherent receiver is considered, the set of decision variables can be written as [23]

$$\begin{aligned} U_{ij} =& \mathrm{Re}\left[e^{-j\phi}\int_0^T r(t)U_{ij}^*(t)dt\right] \\ j =& 0,1,\ldots,m_i-1 \end{aligned} \tag{7}$$

for receiving residue digit r_i $(i=1,2,\ldots,u)$, where ϕ 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, . . ., 0). Then, the decision variables can be expressed as

$$U_{i0} = 2\alpha\xi_i + N_{i0} \tag{8}$$

$$U_{ij} = N_{ij} \tag{9}$$

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

$$N_{ij} = \mathrm{Re}\left[e^{-j\phi}\int_0^T N(t)U_{ij}^*(t)dt\right] \tag{10}$$

are zero-mean Gaussian random variables with variance $\sigma_i^2 = 2\xi_i N_0$. Consequently, the probability density functions (pdfs) 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 [23]. After normalization by the mean-square noise power of σ_i, the above distributions are given by

$$\begin{aligned} f_{U_{i0}}(x) =& \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{\left(x-\sqrt{2\gamma_i}\right)^2}{2}\right), \\ & \text{for } i = 1,2,\ldots,u \end{aligned} \tag{11}$$

$$\begin{aligned} f_{U_{ij}}(x) =& \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right), \\ & \text{for } j = 1,2,\ldots,(m_i-1) \text{ and for a given } i \end{aligned} \tag{12}$$

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 $U_{ij,\max} = \max\{U_{ij} \text{ for all } j \neq 0\}$ for a given i, then the pdf of $U_{ij,\max}$ can be expressed as (Appendix I)

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

where $Q(y)$ is the Q-function defined as $Q(y) = 1/\sqrt{2\pi}\int_y^\infty \exp\left(-t^2/2\right)dt$.

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 $U_{ij,\max}$, which can be computed as [23]

$$\begin{aligned} P_i(C) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}&\left[1-Q(y)\right]^{m_i-1} \\ &\cdot\exp\left(-\frac{\left(y-\sqrt{2\gamma_i}\right)^2}{2}\right)dy \end{aligned} \tag{14}$$

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

$$P_s(C) = \prod_{i=1}^{u} P_i(C). \tag{15}$$

Finally, the BER $P_b(\varepsilon)$ can be approximated as [23]

$$P_b(\varepsilon) \approx \frac{1}{2}\left(1-P_s(C)\right) \tag{16}$$

when $M=\prod_{i=1}^{u} m_i$ is sufficiently high.

When $u=1$, (16) is simply reduced to the BER of the conventional M-ary orthogonal signaling system [23]. However, if the conventional M-ary orthogonal signaling system has the same number of bits per symbol, as the RNS-based system, then

$$M = \prod_{i=1}^{u} m_i \tag{17}$$

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.

In the context of the well-known 64-ary IS-95 system, clearly a total of 64 correlators are required in order to detect the 6-bit symbols transmitted. By contrast, in our proposed RNS-based system, we may opt for using the relative prime moduli of three, four, and seven. The demodulation of each of the associated residues in Fig. 2 requires only three, four, and seven correlators, respectively. Explicitly, only $3+4+7=14$ correlators are required at the receiver, instead of 64 in the conventional IS-95-like M-ary system.

As a more extreme example of a futuristic system, let us consider the system in the first line of [36, Table I], 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. Hence, the complexity of the receiver is significantly decreased in terms of the number of correlators required. However, in RNS- or RRNS-based parallel communication systems, an RNST unit is required at the transmitter side and an IRNST unit is required at the receiver side in order to implement binary-to-residue and residue-to-binary conversions, respectively. The complexity of the IRNST converter can be significantly decreased when using systematic RRNS codes and the so-called mixed radix conversion (MRC) based on base extension (BEX) algorithm [19]. In the following section, we derive the BER expressions 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 this paper, an approximation is proposed for evaluating the BER over the AWGN channel in order to render the numerical analysis tractable. By contrast, accurate BER computations are invoked over Rayleigh fading channels in Part II of this paper [36]. We also assume an equal energy for the different residue digits in the following analysis. We note furthermore that all equations derived in this section and in [36, Section IV] are suitable for the average BER computation of Reed–Solomon (RS) coded systems [35] using similar design criteria. To characterize the BER performance of RS codes, we simply replace the corresponding moduli m_i of the RRNS codes in the computations by a constant modulus of $m = 2^b$, which is the dynamic range of the RS coded symbols; b is the number of bits per RS coded symbol. In [36, Section IV], we will elaborate on this issue further, emphasizing that the corresponding RS-coded system constitutes the special scenario of $b =$ constant number of bits per symbol.

The properties of the RNS arithmetic indicate that if an 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 [29], [30], [34], [35], where the lowest reliability symbols are erased and error-and-erasure decoding is employed at the receiver. 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 [34] 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 [34]:

$$\lambda_i = \frac{{}^1\max_i\left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}}{{}^2\max_i\left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}} \tag{18}$$

where ${}^1\max_i\{\cdot\}$ and ${}^2\max_i\{\cdot\}$ represent the maximum and the "second maximum" of the correlator outputs of $\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\}$, 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 is concerned. More explicitly, let the residue sequence (0, 0, …, 0) be transmitted. Then the noise-contaminated pdfs of U_{i0} and $U_{ij,\max}$ for $i = 1, 2, \ldots, u$, which are given in (11) and (13), are shown in Fig. 3 for an AWGN channel at a bit-SNR of 2 dB. 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 $U_{ij,\max}$ 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 $U_{ij,\max}$ are most likely to reside in the area of **E**. Since these decision regions are comparable in size, we often arrive at erroneous decisions. Accordingly, we can argue that the absolute value of λ_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 λ_i for the RST are the lowest reliability outputs. The exact pdfs of λ_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

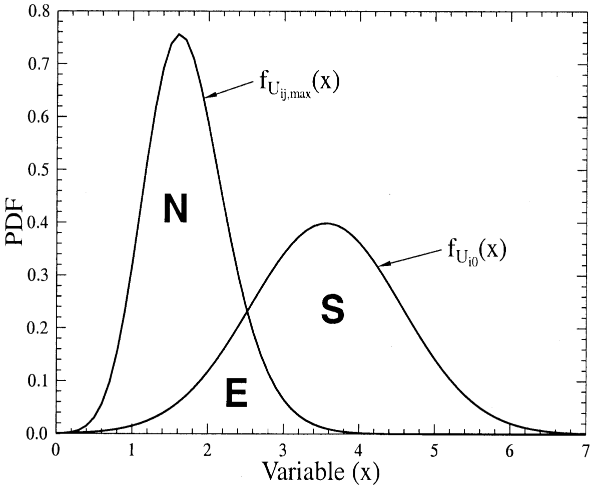

Fig. 3. The noise-contaminated pdf $f_{U_{i0}}(x)$, $f_{U_{ij},\max}(x)$ according to (11) and (13) for the modulus of $m_i = 16$ and an AWGN channel SNR per bit of $\gamma_b = 2$ dB.

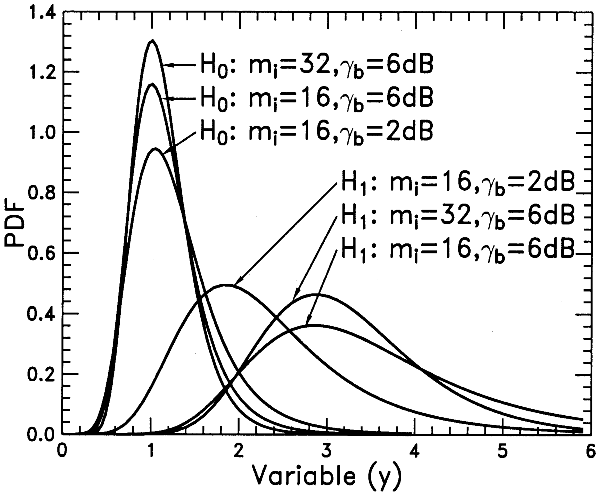

Fig. 4. The pdf of $|\lambda_i| = \left|{}^1\max_i\{\cdot\}/{}^2\max_i\{\cdot\}\right|$ according to (19) under the hypothesis of H_1 and H_0, using the moduli of $m_i = 16$ and 32 at an AWGN channel SNR per bit of $\gamma_b = 2$ and 6 dB.

$$f_{|\lambda_i|}(y|H_\theta) = f_{\lambda_i}(y|H_\theta) + f_{\lambda_i}(-y|H_\theta),\ y \geq 0 \tag{19}$$

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 2 and 6 dB 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 $y = 1$—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 $\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\}$ are 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 (18) obeys

$$\begin{aligned}&{}^1\max\left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}\\ &\qquad = {}^1\max\left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}. \end{aligned} \tag{20}$$

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 (18), obeys

$$\begin{aligned}&{}^2\max\left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}\\ &\quad \leq {}^2\max\left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}\\ &\quad \leq {}^1\max\left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}. \end{aligned} \tag{21}$$

It can be shown mathematically that under the erroneous decision hypothesis H_0 and for a given SNR per bit, we have

$$\begin{aligned}&{}^2\max\left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}\\ &\qquad \approx {}^1\max\left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}\end{aligned}$$

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 $f_{U_{ij,\max}}(x)$ 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 on the basis of the results of Part II [36] 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 toward infinity.

However, using the exact pdfs of $f_{|\lambda_i|}(y|H_\theta)$ 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, in this part of this paper, we invoke approximations in order to simplify the analysis, noting that for Rayleigh channels, we will provide exact equations in Part II [36]. First, under the error-free decision hypothesis H_1, the pdfs of ${}^1\max\{\cdot\}$ and ${}^2\max\{\cdot\}$ can be approximated by the individual pdfs in (11) and (13), respectively, when the SNR per bit is sufficiently high, which leads to the terms of $[1 - Q(y)]$, $P_i(C)$, and $Q(y - \sqrt{2\gamma_i})$ becoming near unity in the effective area of $f_{{}^1\max}(y|H_1)$ and $f_{{}^2\max}(y|H_1)$. These approximations also imply that under the error-free decision hypothesis H_1, the pdfs of ${}^1\max\{\cdot\}$ and ${}^2\max\{\cdot\}$ are the unconditional pdfs of the correlator output matched to the transmitted residue digit and the maximum among the other correlator outputs mismatched to the transmitted residue digit, respectively. Using the above approximation, we can obtain the pdf of λ_i under H_1, which is formulated as shown in (22) at the bottom of the page, where $P_i(C)$ represents the probability that U_{i0} exceeds $U_{ij,\max}$, i.e., $P_i(C)$ is the correct reception probability of residue digit r_i, which is given by (14).

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 ${}^1\max\{\cdot\}$ and ${}^2\max\{\cdot\}$ 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 to the exact BER.

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 (16).

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 lowest reliability MLD outputs before RRNS$(u - d, v)$ decoding. Since a RRNS$(u - d, v)$ code can correct up to $t_{\max} = [(u - v - d)/2]$ residue digit errors [8], a symbol is recovered without errors after IRNST if t and s follow a) $0 \leq t \leq t_{\max}$ or b) $t_{\max} + 1 \leq t \leq t_{\max} + d$ and

$$f_{\lambda_i}(y|H_1) = \begin{cases} \frac{(m_i-1)}{2\pi P_i(C)} \int_0^\infty x \cdot \exp\left(-\frac{x^2}{2}\right) & \\ \cdot\left\{[Q(x)]^{m_i-2} \exp\left(-\frac{\left(xy+\sqrt{2\gamma_i}\right)^2}{2}\right) + [1 - Q(x)]^{m_i-2} \exp\left(-\frac{\left(xy-\sqrt{2\gamma_i}\right)^2}{2}\right)\right\} dx, & y \leq 1 \\ \frac{(m_i-1)}{2\pi P_i(C)} \int_0^\infty x \cdot \exp\left(-\frac{x^2}{2}\right) [1 - Q(x)]^{m_i-2} \exp\left(-\frac{\left(xy-\sqrt{2\gamma_i}\right)^2}{2}\right) dx, & y > 1 \end{cases} \tag{22}$$

$s \geq t - t_{\max}$, where a) indicates that there were less than $t_{\max}$ 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 $t - t_{\max}$, which is the number of errors in excess of the error-correction capability $t_{\max} = [(u - v - d)/2]$ of 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, $d = 0$—i.e., dropping no low-confidence residues—leads to $s = 0$, and hence $t_{\max} = [(u - v)/2]$ number of residue errors can be corrected by the associated RRNS(u, v) code. 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

$$P_s(C) = \sum_{t=0}^{t_{\max}} \left\{ \sum_{Q\binom{u}{t}} \left[\underbrace{\prod_{m=1}^{t} (1 - P_{j_m}(C))}_{\text{error}} \underbrace{\prod_{n=1, n\neq m}^{u} P_{j_n}(C)}_{\text{correct}} \right] \right\} \tag{23}$$

where $\prod_{()=1}^{0}(\cdot) = 1$, $\{j_1, j_2, \ldots, j_u\}$ is a possible mapping of $\{1, 2, \ldots, u\}$, and $Q\binom{u}{t}$ 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 $\sum_{Q\binom{u}{t}}$ represents all possible selections of t elements from $\{1, 2, \ldots, u\}$.

B. Error-Dropping-Only RNS Processing

In this case, $t_{\max} = 0$—i.e., no residue error correction takes place—and hence $(u - v) = d$ number of lowest confidence residues can be dropped. The symbol is recovered correctly after IRNST in Fig. 2, if and only if all the t number of residue digit errors inflicted by the channel 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

$$P_s(C) = \sum_{t=0}^{d} \left\{ \sum_{Q\binom{u}{t}} \left[\prod_{m=1}^{t} (1 - P_{j_m}(C)) \prod_{n=1, n\neq m}^{u} P_{j_n}(C) \right] \right\} \cdot P(d, t) \tag{24}$$

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

$$P(d, t) = \sum_{n=0}^{d-t} \left\{ \frac{t}{2^{t-1}} \sum_{Q\binom{u-t}{n}} \left[\prod_{i=1}^{n} \int_0^1 f_{|\lambda_{\nu_i}|}(y|H_1)dy \right] \cdot \left[\prod_{j=1, j\neq i}^{u-t} \int_1^{\infty} f_{|\lambda_{\nu_j}|}(y|H_1)dy \right] \right\} \tag{25}$$

where $\{|\lambda_{\nu_1}|, |\lambda_{\nu_2}|, \ldots, |\lambda_{\nu_{(u-t)}}|\}$ represents a possible mapping of $\{|\lambda_{m_1}|, |\lambda_{m_2}|, \ldots, |\lambda_{m_{(u-t)}}|\}$. Note that in deriving (25), we used the approximation of $\int_0^1 f_{|\lambda_i|}(y|H_0)dy = 1/2$. The detailed derivations of (25) and (27) can be found in Part II of this paper [36].

C. Error-Dropping-and-Correction RNS Processing

If the RNS processing of Fig. 2 is designed using error dropping and correction, i.e., $t_{\max} > 0$, $d > 0$, then the transmitted symbol can be recovered correctly if the residue digit errors encountered 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

$$P_s(C) = \sum_{t=0}^{d+t_{\max}} \left\{ \sum_{Q\binom{u}{t}} \left[\prod_{m=1}^{t} (1 - P_{j_m}(C)) \cdot \prod_{n=1, n\neq m}^{u} P_{j_n}(C) \right] \right\} \cdot P(s \geq t - t_{\max}) \tag{26}$$

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

$$P(s \geq t - t_{\max}) = \sum_{n=0}^{d+t_{\max}-t} \left\{ \frac{t}{2^{t-1}} \binom{t}{t_{\max}} \cdot \sum_{Q\binom{u-t}{n}} \left[\prod_{i=1}^{n} \int_0^1 f_{|\lambda_{\nu_i}|}(y|H_1)\, dy \right] \cdot \left[\prod_{j=1, j\neq i}^{u-t} \int_1^{\infty} f_{|\lambda_{\nu_j}|}(y|H_1)\, dy \right] \right\} \tag{27}$$

where $\{|\lambda_{\nu_1}|, |\lambda_{\nu_2}|, \ldots, |\lambda_{\nu_{(u-t)}}|\}$ represents a possible mapping of $\{|\lambda_{m_1}|, |\lambda_{m_2}|, \ldots, |\lambda_{m_{(u-t)}}|\}$ and we used the approximation of $\int_0^1 f_{|\lambda_i|}(y|H_0)dy = \int_1^\infty f_{|\lambda_i|}(y|H_0)dy = 1/2$ in the derivation of (27).

We note here that instead of the above RRNS codes, 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 RS-coded symbol—and a similar BER performance is maintained for an $\mathrm{RS}(u, v, t)$ and an $\mathrm{RRNS}(u, v, t)$ code. This is because both codes constitute a class of maximum-distance-separable codes [35]. An $\mathrm{RS}(u, v)$ code can correct up to $[(u - v)/2]$ errors and detect up to $[u - v]$ errors. Moreover, an $\mathrm{RS}(u, v)$ code can correct up to $t_{\max}$ errors and d erasures, if and only if $2t_{\max} + d \leq u - v$. Hence, upon using an $\mathrm{RS}(u, v)$ code for the protection of the parallel transmitted information instead of the $\mathrm{RRNS}(u, v)$ 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 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 [35]. 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, 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 zero-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 relative prime 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 $m_1 \approx m_2 \approx m_3$ due to $M_I = \prod_{i=1}^u m_i$. 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 (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 $E_b/N_0 = 8$ dB. Then the total SNR for transmitting the three residue digits can be computed by $\gamma = \log_2(m_1m_2m_3) \cdot E_b/N_0$. Hence, by changing one of the γ_1, γ_2, γ_3 values, say, γ_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 suggest that the equal residue energy scheme is not the optimum one. More explicitly, the point where the three curves intersect represents the BER when equal residue energy is assumed, i.e., $\mathrm{SNR} = 10\log_{10}\left([\log_2(m_1m_2m_3) \cdot E_b/N_0)/3\right] = 13.8$ dB. To achieve the optimum BER performance, the curves indicate 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.

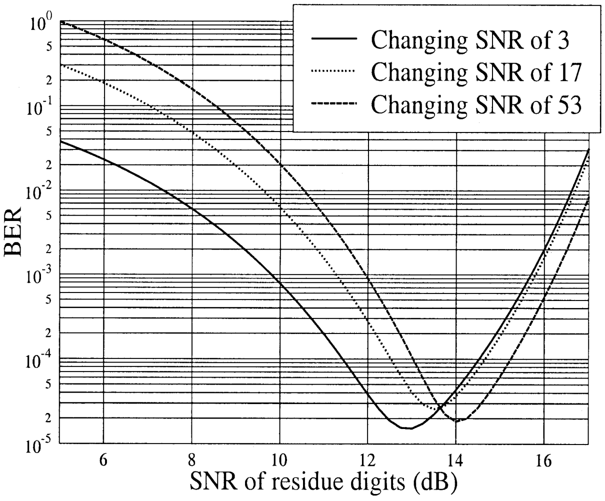

Fig. 5. BER versus residue digit SNR γ_1, γ_2, and γ_3 for the RNS system when unequal energy is distributed for the residue digits r_1, r_2, and r_3 $(m_1 = 3, m_2 = 17, m_3 = 53)$ computed from (16) and (14).

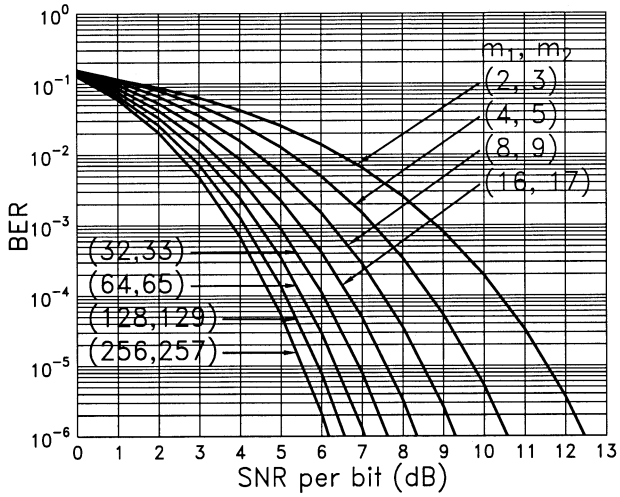

Fig. 6. BER performance of various nonredundant RNS-based orthogonal signaling schemes with $u = 2$ moduli and a dynamic range of $M = m_1m_2$ computed from (16) and (14).

The BER performance of various nonredundant RNS-based systems using $u = 2$ moduli was computed according to (16) and (14). 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 the relative prime moduli increased—in fact, when the product of the two moduli increased—the BER decreased gracefully.

TABLE I
THE PARAMETERS RELATED TO THE NUMERICAL COMPUTATIONS OF FIG. 7

d	t_{max}	k	m_1	m_2	m_3	m_4	m_5	m_6	m_7
0	0	25	29	31	32	33	35		
1	0	25	29	31	32	33	35	37	
2	0	25	29	31	32	33	35	37	41
0	1	25	29	31	32	33	35	37	41

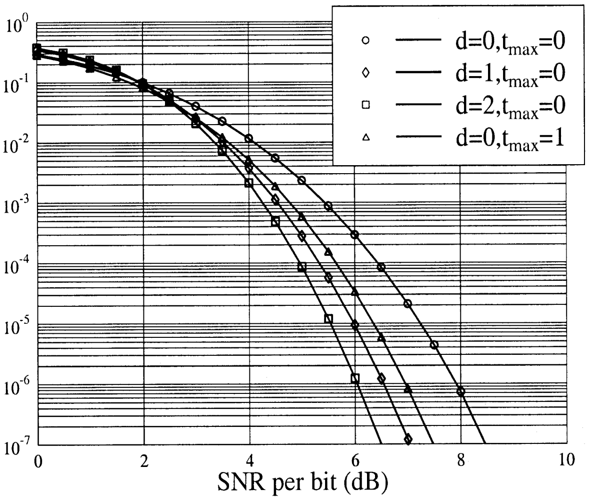

Fig. 7. BER versus SNR performance for the RRNS-based orthogonal signaling system with parameters given in Table I using (24), (25), and (16).

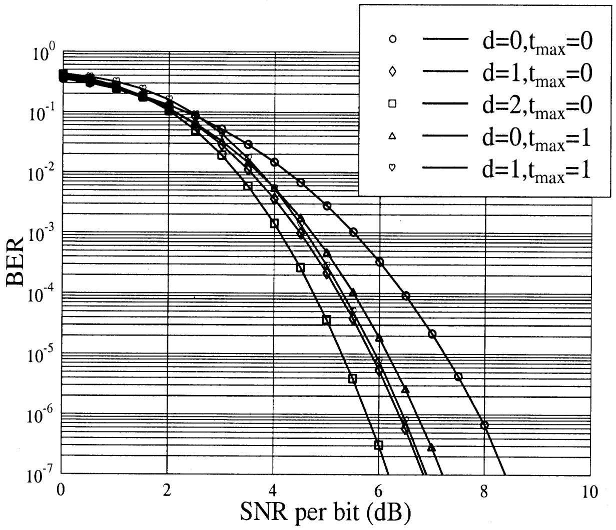

Fig. 8. BER versus SNR performance for the RRNS-based orthogonal signaling system with parameters given in Table II using (26)–(27), and (16).

TABLE II
PARAMETERS RELATED TO THE NUMERICAL COMPUTATIONS OF FIG. 8

d	t_{max}	k	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
0	0	36	29	31	35	36	37	41	43			
1	0	36	29	31	35	36	37	41	43	47		
2	0	36	29	31	35	36	37	41	43	47	53	
0	1	36	29	31	35	36	37	41	43	47	53	
1	1	36	29	31	35	36	37	41	43	47	53	59

This may be explained on the basis of (14), since when the product of m_1, m_2 increases, the dynamic range and the number of bits per residue symbol—$k = \log_2(m_1 m_2)$—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 $k = \log_2(\prod_{i=1}^{5} m_i)$ 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. Upon employing error-dropping-only RNS processing, an SNR gain of about 1.5 or 2.1 dB 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 1-dB SNR gain can be achieved using two redundant moduli at a bit error rate of 10^{-6}. Hence, the RST-assisted RNS-based orthogonal signaling scheme 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 in the scenario considered 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.

APPENDIX I
THE PROBABILITY DENSITY FUNCTION OF THE λTH MAXIMUM

In this Appendix, we derive the pdf of the λth maximum of the independent random variables $\{X_1, X_2, \ldots, X_n\}$, which may be expressed as

$$Y = \max_{\lambda} \{X_1, X_2, \ldots, X_n\} \tag{28}$$

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

$$\begin{aligned}
&P(Y<y)\\
&=P\left(\max_{\lambda}\{X_1,X_2,\ldots,X_n\}<y\right)\\
&=\sum_{i=1}^{n}\sum_{Q\binom{n-1}{\lambda-1}} P\Big(X_{i_1}>X_i, X_{i_2}>X_i,\ldots,X_{i_{\lambda-1}}>X_i;\\
&\qquad X_{j_1}<X_i, X_{j_2}<X_i,\ldots,X_{j_{n-\lambda}}<X_i;\\
&\qquad i_l, j_m\neq i|X_i=Y<y\Big)\\
&=\sum_{i=1}^{n}\sum_{Q\binom{n-1}{\lambda-1}} \int_{-\infty}^{y} P\Big(X_{i_1}>x, X_{i_2}>x,\ldots,X_{i_{\lambda-1}}>x;\\
&\qquad X_{j_1}<x, X_{j_2}<x,\ldots,X_{j_{n-\lambda}}<x;\\
&\qquad i_l, j_m\neq i|X_i=x\Big)f_{X_i}(x)dx \quad (29)
\end{aligned}$$

where $\sum_{Q\binom{n}{i}}$ 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 λth 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, (29) can be expressed as

$$\begin{aligned}
P(Y<y) =&\sum_{i=1}^{n}\sum_{Q\binom{n-1}{\lambda-1}} \int_{-\infty}^{y}\left(\prod_{l=1}^{\lambda-1}P\left(X_{i_l}>x\right)\right)\\
&\cdot\left(\prod_{m=1}^{n-\lambda}P\left(X_{j_m}<x\right)\right)f_{X_i}(x)dx.
\end{aligned} \tag{30}$$

After differentiating the above equation with respect to the variable y, we finally obtained the pdf of (28) as

$$\begin{aligned}
f_Y(y) =&\sum_{i=1}^{n}\sum_{Q\binom{n-1}{\lambda-1}} \left(\prod_{l=1}^{\lambda-1}P\left(X_{i_l}>y\right)\right)\\
&\cdot\left(\prod_{m=1}^{n-\lambda}P\left(X_{j_m}<y\right)\right)f_{X_i}(y).
\end{aligned} \tag{31}$$

Note that when $\lambda = 1$ or $\lambda = n$ and $\{X_i\}$ obey identical distributions, then

$$\sum_{Q\binom{n-1}{0}} \quad \text{and} \quad \sum_{Q\binom{n-1}{n-1}}$$

are equal to one and (31) 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 [33]

$$f_Y(y) = nf_{X_i}(y)\left[P\left(X_j<y\right)\right]^{n-1} \tag{32}$$

$$f_Y(y) = nf_{X_i}(y)\left[P\left(X_j>y\right)\right]^{n-1} \tag{33}$$

respectively.

Appendix 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 (18), 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

$$\begin{aligned}
f_{{}^1\max}(y|H_1) =&\frac{1}{P_i(C)}\left[1-Q(y)\right]^{m_i-1}\\
&\cdot\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{\left(y-\sqrt{2\gamma_i}\right)^2}{2}\right)
\end{aligned} \tag{34}$$

$$\begin{aligned}
f_{{}^2\max}(y|H_1) =&\frac{m_i-1}{P_i(C)}\left[1-Q(y)\right]^{m_i-2}Q\left(y-\sqrt{2\gamma_i}\right)\\
&\cdot\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{y^2}{2}\right)
\end{aligned} \tag{35}$$

where $P_i(C)$ is given by (14). Under the assumption of H_0, the pdfs can be expressed as

$$\begin{aligned}
f_{{}^1\max}(y|H_0) =&\frac{m_i-1}{1-P_i(C)}\left[1-Q\left(y-\sqrt{2\gamma_i}\right)\right]\\
&\cdot\left[1-Q(y)\right]^{m_i-2}\cdot\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{y^2}{2}\right),
\end{aligned} \tag{36}$$

$$\begin{aligned}
f_{{}^2\max}(y|H_0) =&\frac{m_i-1}{1-P_i(C)}Q(y)\left[1-Q(y)\right]^{m_i-3}\\
&\cdot\Bigg\{\left[1-Q(y)\right]\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{\left(y-\sqrt{2\gamma_i}\right)^2}{2}\right)\\
&+(m_i-2)\left[1-Q\left(y-\sqrt{2\gamma_i}\right)\right]\\
&\cdot\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{y^2}{2}\right)\Bigg\}.
\end{aligned} \tag{37}$$

Consequently, the pdfs of $\lambda_i = {}^1\max\{\cdot\}/{}^2\max\{\cdot\}$ 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 shown in (38) and (39)

$$f_{\lambda_i}(y|H_1)=\left\{\begin{array}{ll}\frac{m_i-1}{2\pi[P_r(C)]^2P(^1\max>^2\max|H_1)}\int_0^\infty x\exp\left(-\frac{x^2}{2}\right) & \\ \cdot\left\{[Q(xy)]^{M-1}[Q(x)]^{M-2}\left[1-Q\left(x+\sqrt{2\gamma_i}\right)\right]\exp\left(-\frac{\left(xy+\sqrt{2\gamma_i}\right)^2}{2}\right)\right. & \\ \left.+[1-Q(xy)]^{M-1}[1-Q(x)]^{M-2}\left[Q\left(x-\sqrt{2\gamma_i}\right)\right]\exp\left(-\frac{\left(xy-\sqrt{2\gamma_i}\right)^2}{2}\right)\right\}dx, y\le 1 & \\ \frac{m_i-1}{2\pi[P_r(C)]^2P(^1\max>^2\max|H_1)}\int_0^\infty x\exp\left(-\frac{x^2}{2}\right) & \\ \cdot[1-Q(xy)]^{M-1}[1-Q(x)]^{M-2}\left[Q\left(x-\sqrt{2\gamma_i}\right)\right]\exp\left(-\frac{\left(xy-\sqrt{2\gamma_i}\right)^2}{2}\right)dx, & y>1\end{array}\right. \tag{38}$$

$$f_{\lambda_i}(y|H_0)=\left\{\begin{array}{ll}\frac{(m_i-1)^2}{2\pi[P_r(C)]^2P(^1\max>^2\max|H_0)}\int_0^\infty x\cdot Q(x)[1-Q(x)]\exp\left(-\frac{x^2y^2}{2}\right) & \\ \cdot\left\{Q\left(xy+\sqrt{2\gamma_i}\right)[Q(xy)]^{m_i-2}[Q(x)]^{m_i-4}\right. & \\ \cdot\left[Q(x)\exp\left(-\frac{\left(x+\sqrt{2\gamma_i}\right)^2}{2}\right)+(m_i-2)Q\left(x+\sqrt{2\gamma_i}\right)\exp\left(-\frac{x^2}{2}\right)\right] & \\ +[1-Q(xy)]^{m_i-2}\left[1-Q\left(xy-\sqrt{2\gamma_i}\right)\right][1-Q(x)]^{m_i-4} & \\ \left.\cdot\left[[1-Q(x)]\exp\left(-\frac{\left(x-\sqrt{2\gamma_i}\right)^2}{2}\right)+(m_i-2)\left[1-Q\left(x-\sqrt{2\gamma_i}\right)\right]\exp\left(-\frac{x^2}{2}\right)\right]\right\}dx, y\le 1 & \\ \frac{(m_i-1)^2}{2\pi[P_r(C)]^2P(^1\max>^2\max|H_0)}\int_0^\infty x\cdot Q(x)[1-Q(x)]\exp\left(-\frac{x^2y^2}{2}\right) & \\ \cdot[1-Q(xy)]^{m_i-2}\left[1-Q\left(xy-\sqrt{2\gamma_i}\right)\right][1-Q(x)]^{m_i-4} & \\ \cdot\left([1-Q(x)]\exp\left(-\frac{\left(x-\sqrt{2\gamma_i}\right)^2}{2}\right)+(m_i-2)\left[1-Q\left(x-\sqrt{2\gamma_i}\right)\right]\exp\left(-\frac{x^2}{2}\right)\right)dx, & y>1\end{array}\right. \tag{39}$$

at the top of the page, where $P(^1\max>{}^2\max|H_\theta)$. $\theta=0,1$ 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

[1] K. W. Watson, "Self-checking computations using residue arithmetic," *Proceedings IEEE*, vol. 54, no. 12, pp. 1920–1931, Dec. 1966.

[2] L.-L. Yang and L. Hanzo, "Performance of residue number system based DS-CDMA over multipath fading channels using orthogonal sequences," *Eur. Trans. Telecommun.*, vol. 9, pp. 525–536, Nov./Dec. 1998.

[3] ——, "Residue number system arithmetic assisted M-ary modulation," *IEEE Commun. Lett.*, vol. 3, pp. 28–30, Feb. 1999.

[4] W. K. Jenkins and E. J. Altman, "Self-checking properties of residue number error checkers based on mixed radix conversion," *IEEE Trans. Circuits Syst.*, vol. 35, pp. 159–167, Feb. 1988.

[5] E. D. D. Claudio, G. Orlandi, and F. Piazza, "A systolic redundant residue arithmetic error correction circuit," *IEEE Trans. Comput.*, vol. 42, no. 4, pp. 427–432, Apr. 1993.

[6] H. Krishna, K. Y. Lin, and J. D. Sun, "A coding theory approach to error control in redundant residue number system, Part I: theory and single error correction," *IEEE Trans. Circuits. Syst.*, vol. 39, pp. 8–17, Jan. 1992.

[7] J. D. Sun and H. Krishna, "A coding theory approach to error control in redundant residue number system, Part II: Multiple errors detection and correction theory," *IEEE Trans. Circuits Syst.*, vol. 39, pp. 18–32, Jan. 1992.

[8] H. Krishna and J. D. Sun, "On theory and fast algorithms for error correction in residue number system product codes," *IEEE Trans. Comput.*, vol. 42, pp. 840–852, July 1993.

[9] R. J. Cosentino, "Fault-tolerance in a systolic residue arithmetic processor array," *IEEE Trans. Comput.*, vol. 37, pp. 886–890, July 1988.

[10] L.-L. Yang and L. Hanzo, "Minimum-distance decoding of redundant residue number system codes," in *Proc. IEEE ICC'2001*, Helsinki, Finland, June 2001, pp. 2975–2979.

[11] ——, "Redundant residue number system based error correction codes," in *Proc. IEEE VTC'01 (Fall)*, Atlantic City, NJ, Oct. 2001, pp. 1472–1476.

[12] F. Barsi and P. Maestrini, "Error correcting properties of redundant residue number systems," *IEEE Trans. Comput.*, vol. C-22, no. 3, pp. 307–317, Mar. 1973.

[13] F. J. Yaylor, "A single modulus complex ALU for signal processing," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-33, pp. 1302–1315, Oct. 1985.

[14] G. Alia and E. Martinelli, "A VLSI algorithm for direct and reverse conversion from weighted binary number system to residue number system," *IEEE Trans. Circuits Syst.*, vol. CAS-31, pp. 1033–1039, Dec. 1984.

[15] R. M. Capocelli and R. Giancarlo, "Efficient VLSI networks for converting an integer from binary to residue numbers and vice versa," *IEEE Trans. Circuits Syst.*, vol. 35, pp. 1425–1430, Nov. 1988.

[16] D. Radhakrishnan and Y. Yuan, "Novel approaches to the design of VLSI RNS multiplier," *IEEE Trans. Circuits Syst. II*, vol. 39, pp. 52–57, Jan. 1992.

[17] G. Alia and E. Martinelli, "A VLSI modulo m multiplier," *IEEE Trans. Comput.*, vol. 40, pp. 873–878, July 1991.

[18] K. M. Elleithy and M. A. Bayoumi, "Fast and flexible architectures for RNS arithmetic decoding," *IEEE Trans. Circuits System II*, vol. 39, pp. 226–235, Apr. 1992.

[19] T. Liew, L.-L. Yang, and L. Hanzo, "Soft-decision redundant residue number system based error correction coding," in *Proc. IEEE VTC'99*, Amsterdam, The Netherlands, Sept. 19–22, 1999, pp. 2974–2978.

[20] L.-L. Yang and L. Hanzo, "Residue number system based multiple code DS-CDMA systems," in *Proc. IEEE VTC'99*, Houston, TX, May 1999, pp. 1450–1454.

[21] ——, "Ratio statistic test assisted residue number system based parallel communication systems," in *Proc. IEEE VTC'99*, Houston, TX, May 1999, pp. 894–898.

[22] K. Yen, L.-L. Yang, and L. Hanzo, "Residual number system assisted CDMA—A new system concept," in *Proc. 4th ACTS Mobile Communications Summit'99*, Sorrento, Italy, June 8–11, 1999, pp. 177–182.

[23] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[24] S. G. Glisic and P. A. Leppanen, *Wireless Communications: TDMA Versus CDMA*. Norwell, MA: Kluwer, 1997.

[25] P. K. Enge and D. V. Sarwate, "Spread-spectrum multiple-access performance of orthogonal codes: Linear receiver," *IEEE Trans. Commun.*, vol. COM-35, pp. 1309–1319, Dec. 1987.

[26] ——, "Spread-spectrum multiple-access performance of orthogonal codes: Impulse noise," *IEEE Trans. Commun.*, vol. 36, pp. 98–105, Jan. 1988.

[27] M. Chase and K. Pahlavan, "Performance of DS-CDMA over measured indoor radio channels using random orthogonal codes," *IEEE Trans. Veh. Technol.*, vol. 42, pp. 61–624, Aug. 1993.

[28] L. M. A. Jalloul and J. K. Holtzman, "Performance analysis of DS-CDMA with noncoherent M-ary orthogonal modulation in multipath fading channels," *IEEE J. Select. Areas Commun.*, vol. 12, pp. 862–870, June 1994.

[29] L.-L. Yang and L. Hanzo, "Performance analysis of coded M-ary orthogonal signaling using errors-and-erasures decoding over frequency-selective fading channels," *IEEE J. Select. Areas Commun.*, vol. 19, pp. 211–221, Feb. 2001.

[30] L.-L. Yang, K. Yen, and L. Hanzo, "A Reed-Solomon coded DS-CDMA system using noncoherent M-ary orthogonal modulation over multipath fading channels," *IEEE J. Select. Areas Commun.*, vol. 18, pp. 2240–2251, Nov. 2000.

[31] R. V. Nee and A. D. Wild, "Reducing the peak-to-average power ratio of OFDM," in *Proc. 48th IEEE VTC'98*, vol. 1–3, 1998, pp. 2072–2076.

[32] W. G. Jeon, K. H. Chang, and Y. S. Cho, "An adaptive data predistorter for compensation of nonlinear distortion in OFDM systems," *IEEE Trans. Commun.*, vol. 45, pp. 1167–1171, Oct. 1997.

[33] J. N. Pierce, "Theoretical diversity improvement in frequency-shift keying," *Proc. IRE*, vol. 46, no. 5, pp. 903–910, May 1958.

[34] A. J. Viterbi, "A robust ratio-threshold technique to mitigate tone and partial-band jamming in coded MFSK systems," in *Proc. IEEE Milit. Commun. Conf.*, Oct. 1982, pp. 22.4-1–5.

[35] S. Lin and D. J. Costello, *Error Control Coding-Fundamentals and Applications*, 1983.

[36] L. L. Yang and L. Hanzo, "A residue number system based parallel communication scheme using orthogonal signaling: Part II—Multipath fading channels," *IEEE Trans. Veh. Technol.*, vol. 51, pp. 1541–1553, Nov. 2002.

Lie-Liang Yang (M'98–SM'02) received the B.Eng. degree in communication engineering from Shanghai TieDao University, Shanghai, China, in 1988 and the M.S. and Ph.D. degrees in communications and electronics from Northern Jiaotong University, Beijing, China, in 1991 and 1997, respectively.

From 1991 to 1993, he was a Lecturer in the Department of Electrical Engineering, East-China Jiaotong University, China. From 1993 to 1997, he was with the Modern Communications Research Institute, Northern Jiaotong University, China. From June to December 1997, he was a Visiting Scientist at the Institute of Radio Engineering and Electronics, Academy of Sciences of the Czech Republic. Since December 1997, he has been with the Communication Group, Department of Electronics and Computer Science, University of Southampton, U.K., where he has been involved in researching various error-correction coding, modulation, and detection techniques, as well as wide-band, broadband, and ultra-wide-band CDMA systems for advanced wireless mobile communication systems. He has published more than 70 papers in journals and conference proceedings.

Dr. Yang received the Royal Society Sino-British Fellowship in 1997.

Lajos Hanzo (M'91–SM'92) received the M.S. degree in electronics in 1976 and the Ph.D degree in 1983, both from the Technical University of Budapest, Hungary.

During his 26-year career in telecommunications, he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the Department of Electronics and Computer Science, University of Southampton, Southampton, U.K., where he holds the Chair in Telecommunications. He has coauthored eight books on mobile radio communications, published about 400 research papers, organized and chaired conference sessions, presented overview lectures, and been awarded a number of distinctions. Currently, he is managing an academic research team working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) U.K., the European IST Programme, and the Mobile Virtual Centre of Excellence (MVCE), U.K. He is an enthusiastic supporter of industrial and academic liaison and offers a range of industrial courses. He is also a Nonexecutive Director of the MVCE

Prof. Hanzo is an IEEE Distinguished Lecturer.