Performance of Residue Number System Based DS-CDMA over Multipath Fading Channels Using Orthogonal Sequences (1)

LIE-LIANG YANG, LAJOS HANZO
Department of Electronics and Computer Science,
University of Southampton, SO 17, 1BJ, U.K
lly97v@ecs.soton.ac.uk, lh@ecs.soton.ac.uk
hppt://www-mobile.ecs.soton.ac.uk

Abstract. This paper is concerned with a new direct-sequence spread-spectrum multiple-access communication system based on the so-called residue number system (RNS) or redundant residue number system (RRNS). The system operates in a multipath fading environment, and a RAKE receiver structure with maximum ratio combining is used for demodulation. Approximations to the error probabilities are given by using Gaussian statistics for the multiple-access and the multipath interference. Concatenated codes employing residue number system product codes (RNS-PC) as the inner codes and nonbinary Reed-Solomon (RS) codes as the outer codes are adopted to improve the system performance. The performance of the system is determined for a range of different length RNS-PC schemes. The results show that, for a given outer RS code and a given number of moduli of the inner RNS-PC, the performance of the system can be optimized by varying the relative number of information moduli and redundant moduli of the inner RNS-PC and the moduli's values.

1. INTRODUCTION

A direct-sequence code division multiple-access (DS-CDMA) communication system, in which a set of M-ary orthogonal pseudo-random noise (PN) sequences is assigned to each user has been proposed by Enge and Sarwate in [1], and the performance has been analyzed, when the channel impairments are considered as a combination of additive white Gaussian noise (AWGN) and multiple-access interference. Under this communication model, $k = \log_2 M$ bits of information is transmitted in a symbol period. In [2], the above system has been discussed by Enge and Sarwate, when impulsive noise channels are considered. Instead of nonfading channels, Chase and Pahlavan have investigated the performance of the M-ary DS-CDMA system with diversity in the presence of multipath and multiple access interference in [3].

In the above system, $M = 2^k$ PN sequences are employed by each user to transmit $k = \log_2 M$ bits in a single symbol period, and the number of PN sequences of the system increases exponentially with increasing k. In other words, the number of the correlators or matched filters in the receiver of an M-ary DS-CDMA system increases exponentially with increasing k, when a correlation receiver or a matched filter receiver is considered, respectively. This essentially limits the length k of every transmitted symbol, since the complexity of the receiver is proportional to the number of correlators or matched filters. For example, if we assume that there are 100 mobile users, who are transmitting information from a base station in a cell, and $k = 8$ bit symbols are transmitted from a set of $M = 2^8$, then at least 51,200 ($=2 \times 100 \times 28$) PN sequences are utilized simultaneously in the cell for the forward channel (base-to-mobile) and reverse channel (mobile-to-base). The base station has at least 25,600 correlators or matched filters and must synchronize with the 25,600 PN sequences of the mobiles in the cell. Each mobile has to acquire and track 256 PN sequences of the forward channel, and has at least 256 correlators or matched filters, in order to receive the 8 bit symbols sent by the base station. This complexity might be unacceptable concerning both the mobiles and the base stations.

To combat this problem, various spread-spectrum schemes capable of sending multiple bits per symbol period have been proposed in [4, 5]. In [4], Vandendorpe has proposed a communication system based on the combination of multitone modulation and DS spread-spectrum techniques, in which multiple information bits are transmitted in parallel and each bit modulates a carrier. Another multiple bit per symbol transmission method has been proposed in [5] using the combination of a set of random orthogonal sequences (or codes) according to combinational mathematics.

In recent years, the so-called residue number system

(1) The work was supported by the Sino-British Fellowship Trust of Royal Society. The financial support of the European Community, Brussels, Belgium and that of the Engineering and Physical Sciences Research Council, Swindon, UK is also gratefully acknowledged.

(RNS) arithmetic has attracted considerable attention for designing high-speed special-purpose digital hardware that is suitable for very large scale integration (VLSI). Digital systems that are structured around RNS arithmetic units may play an important role in ultra speed dedicated real-time systems that support pure parallel processing of integer-valued data [6 - 14]. The RNS has two important properties for digital processing applications [6]: the ability to use carry-free arithmetic and the lack of ordered significance among residue digits. The first property allows each digit of the representation to be processed separately from the others by a dedicated module. The second property implies that any erroneous digit can be discarded without affecting the result, provided that sufficient resolution remains in the reduced system in order to unambiguously represent the result. With these inherent properties of the RNS, residue arithmetic offers a variety of new approaches to the realization of digital signal processing algorithms [7 - 9], such as digital modulation and demodulation [10], and the fault-tolerant design of arithmetic units [11]. It also offers new approaches to the design of error-detection and error-correction codes [12 - 14].

In this paper, a new communication system based on the combination of the so-called residue number system (RNS) or the so-called redundant residue number system (RRNS) [6] and spread-spectrum techniques is proposed. We will show that the complexity of the receiver can be reduced by decreasing the number of correlators or matched filters. However, signal processing units for binary-to -residue and residue-to-binary conversion have to be designed for the transmitter and the receiver, respectively, as we will highlight during our forthcoming discussions with reference to Figs. 1 and 2. The performance of the proposed system will be analyzed, when random signature sequences are applied by using Gaussian approximations. Specifically, we are concerned with the bit error probabilities of the demodulated signals or the decoded signals at the output of the receiver. The channel itself is modeled as a multipath Rayleigh fading channel, and diversity reception based on maximum ratio combining (MRC) is adopted in the receiver, in order to improve the performance. The well-known concatenated code that employs an RNS product code [15] (RNS-PC) as inner code and a nonbinary RS code as outer code is adopted for error correction and error detection. The inner code is used to detect and/or correct the residue errors, and the nonbinary RS code with errors-only decoding or errors-and-erasures decoding is used to correct the symbol errors or to fill the symbol erasures.

The remainder of the paper is outlined as follows. In section 2, we present the description of the system and the channel model. Section 3 describes the receiver structure. System analysis and derivation of the conditional symbol error probability are given in section 4. In section 5, the performance of the uncoded system is analyzed, while in section 6, the concatenated coded system is evaluated. Numerical results are presented in section 7. Finally, in section 8 we present our conclusions.

2. SYSTEM DESCRIPTION AND CHANNEL MODEL

A residue number system is defined [12, 13] by the choice of v possible integers m_i, ($i = 1, 2,\ldots, v$) referred to as moduli. If all the moduli are pairwise relative primes, any integer X, describing a message 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 $0 \le X < M$, where $r_i = X \pmod{m_i}$ represents the residue of X upon division by m_i, and $M = \prod_{i=1}^{v} m_i$ is the dynamic range. According to the so-called Chinese reminder theorem (CRT) [13 - 15], for any given v-tuple $(r_1, r_2,\ldots, r_v)$, where $0 \le r_i < m_i$, $i = 1, 2,\ldots,v$ there exists one and only one integer X such that $0 \le X < M$ and $r_i = X \pmod{m_i}$. It can be shown that the numerical value of M can be computed [13 - 15] by using

$$X = \sum_{i=1}^{v} r_i T_i M_i \pmod{M}$$

where $M_i = M/m_i$ and the integers T_i are computed a *priori* by solving the congruences:

$$T_i M_i = 1 \pmod{m_i}$$

However, the real-time implementation of the CRT is not practical, as it requires modular operations with respect to a large integer M. In order to avoid processing large valued integers, fast algorithms for the computation of X have been proposed in [16, 17].

Following the definition of the RNS, it can be shown that $\sum_{i=1}^{v} m_i$ sequences are required, in order to transmit k bits information in one symbol period, provided that the condition $M = \prod_{i=1}^{v} m_i \ge 2^k$ is satisfied. Hence, the number of correlators required in the receiver is proportional to $\sum_{i=1}^{v} m_i$, as opposed to $M = \prod_{i=1}^{v} m_i$, which is the number of required correlators in the receiver of a traditional orthogonal CDMA system [1], having the same number of transmitted bits per symbol period as the above RNS-based system.

For incorporating error control (both error correction and error detection are included), we are concerned with the so-called RRNS [12 - 15], which is obtained by appending additional $(u - v)$ moduli $m_{v+1}, m_{v+2},\ldots, m_u$, referred to as redundant moduli, to the previously introduced RNS, in order to form an RRNS of u positive, pairwise relative prime moduli. The product $m_{v+1}, m_{v+2},\ldots, m_u$ is denoted by M_R. Now an integer X in the range $[0, M)$ is represented as a u-tuple, $(r_1, r_2,\ldots, r_u)$, corresponding to u moduli. The RNS-based DS-CDMA communication system, which will be discussed in this paper is based on the above mathematical principles.

2.1. *The transmitted signals*

The block diagram of the proposed CDMA communication system based on the RNS is shown in Fig. 1. As mentioned before, the information to be transmitted is first transformed to a residue sequence, namely $(r_1, r_2,\ldots, r_u)$,

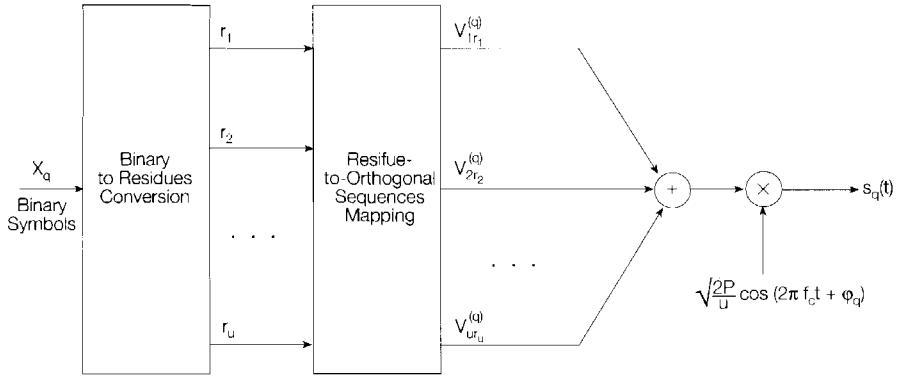

Fig. 1 - The transmitter's block diagram for user q.

as seem in Fig. 1. The residue digits are then mapped to u number of orthogonal sequences and multiplexed for transmission.

In the system, each of the Q users is assigned a random PN sequence set consisting of $\sum_{i=1}^{u} m_i$ orthogonal sequences of length N_s, which will be quantified during our forthcoming discourse. The $\sum_{i=1}^{u} m_i$ orthogonal spread-spectrum sequences of user q are expressed as

$$V^{(q)} = \{V^{(q)}_{10}, V^{(q)}_{11},\ldots, V^{(q)}_{1(m_1-1)};\ldots; V^{(q)}_{u0}, V^{(q)}_{u1},\ldots, V^{(q)}_{u(m_u-1)}\} \quad (1)$$

$$V^{(q)}_{ij} = (V^{(q)}_{ij,0}, V^{(q)}_{ij,1}, \ldots, V^{(q)}_{ij,N_s-1}) \quad (2)$$

where the number of m_i orthogonal sequences from the subset $\{V^{(q)}_{i0}, V^{(q)}_{i1}, \ldots, V^{(q)}_{i(m_i-1)}\}$ for $i = 1, 2,\ldots, u$ is used for the transmission of residue r_i, which takes one out of m_i possible values. The orthogonal sequence length of $N_s = T_s/T_c$ represents the number of chips per symbol interval and T_c is the duration of the waveform chip.

Let the q-th user's data signal $b_q(t)$ be a sequence of rectangular pulses of bit duration T, which takes values of +1 or −1 with equal probability. We assume that there are N code pulses in each data pulse, that is $T = NT_c$. Then, the RNS-based DS-CDMA scheme transmits multiple bits per symbol and takes values from the set $\{0, 1, 2,\ldots, \prod_{i=1}^{u} m_i\}$. Initially, we assume that the u moduli are all used for information transmission, that is $(v = u)$. The symbol duration T_s is given by $T[\log_2 \prod_{i=1}^{u} m_i]$, where $[x]$ represents the largest integer less than or equal to x. For a fixed chip rate of $T_c^{-1} = NT^{-1}$, a signature sequence of length $N_s = N[\log_2 \prod_{i=1}^{u} m_i]$ is used within each symbol.

Assuming that the binary representation of the k-bit data symbol of user q transmitted in $[dT_s, (d + 1)T_s]$ is X_q and that $0 \le X_q < \prod_{i=1}^{u} m_i$, then in order to send the data symbol, X_q is first converted to residues with respect to the moduli $m_1, m_2,\ldots, m_u$. Let the integer message X_q be represented by the residues as

$$(r_1, r_2,\ldots, r_u) \quad (3)$$

where $r_i = X_q \pmod{m_i}$, $(i = 1, 2,\ldots, u)$. Then u specific PN sequences $(V^{(q)}_{1r_1}, V^{(q)}_{2r_2},\ldots, V^{(q)}_{ur_u})$ are selected from the the sequence set of (1) according to eq. (3), and modulated onto the carrier to form the transmitted signal representing X_q. The signal transmitted by user q in the period $[dT_s, (d + 1)T_s]$ can be written as

$$s_q(t) = \sqrt{\frac{2P}{u}} \sum_{i=1}^{u} PN^{(q)}_{ir_i}(t)\cos\left(2\pi f_c t + \varphi_q\right) \quad (4)$$

$$PN^{(q)}_{ir_i}(t) = \sum_{n=-\infty}^{\infty} V^{(q)}_{ir_i,\rho} P_{T_c}(t - nT_c) \quad (5)$$

where f_c is the carrier frequency, and $\rho = n - [n/N_s] \cdot N_s$, such that $V^{(q)}_{ir_i,\rho}$ is the ρ-th chip of the PN sequence $V^{(q)}_{ir_i}$ for a given chip index n in eq. (5). Furthermore, it was shown in the Appendix that the average power of $\sum_{i=1}^{u} PN^{(q)}_{ir_i}(t)$ is u, when random signature sequences are concerned, hence, the average transmitted power of the signal represented by eq. (4) is P. The rectangular chip waveform $P_{T_c}(t)$ of eq. (5) has a duration of T_c, and $P_\tau(t) = 1$ for $0 \le t < \tau$ and $P_\tau(t) = 0$, otherwise, while φ_q represents the phase angle introduced by the q-th user's carrier modulation.

2.2. *The channel model*

We assume that the channel between the q-th transmitter and the corresponding receiver is a multipath Rayleigh fading channel. The complex lowpass equivalent representation of the impulse response experienced by user q is given by

$$h_q(t) = \sum_{l=1}^{L} \alpha_{ql}\,\delta\left(t - \tau_{ql}\right)\exp\left(j\phi_{ql}\right) \quad (6)$$

where α_{ql}, ϕ_{ql} and fql represent the attenuation factor, delay and phase shift for the l-th multipath component of the channel, respectively, while L is the total number of diversity paths and $\delta(t)$ is the Delta-function. We assume that the channel fading is sufficiently slow, so that the multipath parameters can be estimated from the received signal without error. Furthermore, we assume that the q-th user's multipath attenuations $\{\alpha_{ql}, l = 1, 2,\ldots, L\}$ in eq. (6) are independent and identically distributed (i.i.d) ran-

dom variables with zero means and variance of $E\{\alpha^2\} = \sigma^2$. The path phases $\{\phi_{ql}, l = 1, 2,\ldots, L\}$ are assumed to be uniformly distributed random variables in $[0,2\pi]$, while the q-th user's path delays of $\{\tau_{ql}, q = 1, 2,\ldots, Q; l = 1, 2,\ldots, L\}$ are modeled as random variables that are mutually independent of each other and uniformly distributed in $[0, T_s]$. We also assume that the received signal powers are the same for all the Q users. Then the received signal generated by the Q users is expressed as

$$r(t) = \sum_{q=1}^{Q} y_q(t) + n(t) \tag{7}$$

where

$$y_q(t) = \sum_{l=1}^{L} \alpha_{ql} \left[\sqrt{\frac{2P}{u}} \sum_{i=1}^{u} PN_{ir_i}^{(q)}\left(t - \tau_{ql}\right) \right] \cdot \cos\left(2\pi f_c t + \theta_{ql}\right) \tag{8}$$

and $\theta_{ql} = \varphi_{ql} + \phi_{ql} - 2\pi f_c \tau_{ql}$, while $n(t)$ is modeled as AWGN with zero mean and double-sided power spectral density of $N_0/2$.

3. Receiver Model

In order to combat the multipath distortion and achieve an improved performance, diversity combining is employed. For the multipath Rayleigh fading channels, the combiner that achieves the best performance is the one, in which each receiver branch output is multiplied by the corresponding complex-valued path gain α_{ql}. Let the first user be the reference user, i.e. $q = 1$, and consider the coherent correlator RAKE receiver with maximal ratio combining (MRC), as shown in Fig. 2, where the superscript of the reference user's signal has been omitted for convenience. We assume that the d-th data symbol, which takes the value X_d is received. Then, provided $\{\tau_{1l}, l = 1, 2,\ldots, L\}$ and $\{\theta_{1l}, l = 1, 2,\ldots, L\}$ are perfectly estimated, according to Fig. 2, the output decision variable Z_{ij}, for $i = 1, 2,\ldots, u$, and $j = 0, 1,\ldots, (m_i - 1)$, can be expressed as

$$Z_{ij} = \sum_{l=1}^{L} Z_{ijl} = \sum_{l=1}^{L} \int_{dT_s+\tau_{1l}}^{(d+1)T_s+\tau_{1l}} r(t)\alpha_{1l} PN_{ij}\left(t - \tau_{1l}\right) \cdot \cos\left(2\pi f_c t + \theta_{1l}\right) \mathrm{d}t = \sum_{l=1}^{L} \sqrt{\frac{P}{2u}}\, T_s \cdot \left[D_0 \delta\left(r_i - j\right) + \sum_{\underbrace{\eta=1}_{\lambda\neq i \text{ for } \eta=l}}^{L} \sum_{\lambda=1}^{u} I_{s,\lambda l} + \sum_{q=2}^{K} \sum_{\eta=1}^{L} \sum_{\lambda=1}^{u} I_{m,\lambda l}^{(q,1)} + N_l \right] \tag{9}$$

$$\left(i = 1,2,\ldots,u;\ j = 0,1,\ldots,m_i - 1\right)$$

for receiving residue r_i, where $r_i = X_d \pmod{m_i}$, and Z_{ijl} as well as Z_{ij} physically represent the outputs due to multipath propagation and that of the MRC stage, respectively. The relevant variables in eq. (9) are defined as

$$D_0 = \alpha_{1l}^2 \tag{10}$$

$$I_{s,\lambda l} = \frac{\alpha_{1l}\,\alpha_{1\eta}\cos\left(\theta_{1\eta} - \theta_{1l}\right)}{T_s} \cdot \left[V_{\lambda r_\lambda}(d-1) R\left(\tau_{1\eta} - \tau_{1l}\right) + V_{\lambda r_\lambda}(d) \hat{R}\left(\tau_{1\eta} - \tau_{1l}\right) \right] \tag{11}$$

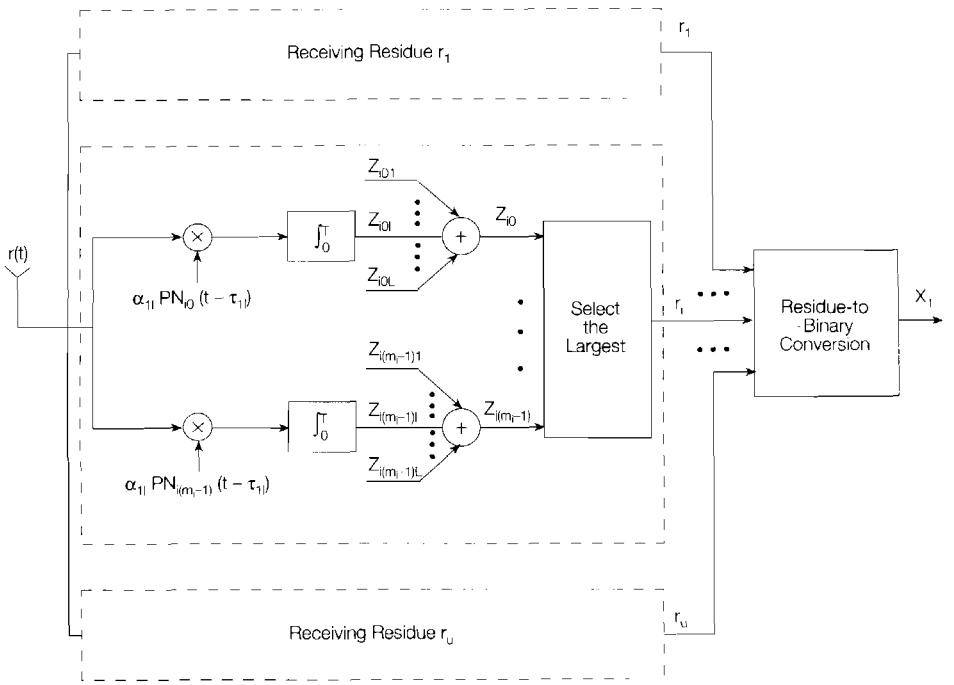

Fig. 2 - The RAKE receiver for the reference signals ($\omega_c = 2\pi f_c$).

$$I_{m,\lambda l}^{(q,1)} = \frac{\alpha_{1l}\,\alpha_{q\eta}\cos\left(\theta_{q\eta}-\theta_{1l}\right)}{T_s} \cdot \left[V_{\lambda r_\lambda}^{(q)}(d-1)\,R\left(\tau_{q\eta}-\tau_{1l}\right)+V_{\lambda r_\lambda}^{(q)}(d)\,\hat{R}\left(\tau_{q\eta}-\tau_{1l}\right)\right] \tag{12}$$

$$N_l = \left(\sqrt{\frac{P}{2u}}\,T_s\right)^{-1} \int_{dT_s}^{(d+1)T_s} n(t)\,\alpha_{1l}\,PN_{ij}\left(t-\tau_{1l}\right) \cdot \cos\left(2\pi f_c t+\theta_{1l}\right)\mathrm{d}t \tag{13}$$

In eqs. (9) to (13), N_l is the term due to the presence of AWGN, $I_{s,\lambda l}$ is the self-interference inflicted to the l-th branch of the RAKE receiver due to multipath of the reference user, while $I_{m,\lambda l}^{(q,1)}$ is the multiple-access interference (MAI) due to the signal transmitted by the q-th ($q > 1$) user. Furthermore, $V_{\lambda r_\lambda}^{(q)}(d-1)\,R(\tau_{q\eta}-\tau_{1l})$ and $V_{\lambda r_\lambda}^{(q)}(d)\,\hat{R}(\tau_{q\eta}-\tau_{1l})$ are the continuous-time partial cross-correlation functions [19] of the sequences V_{ij} and $V_{\lambda r_\lambda}^{(q)}$. Note that $V_{\lambda r_\lambda}^{(q)}(d-1)$ and $V_{\lambda r_\lambda}^{(q)}(d)$ are transmitted by the q-th user during $[(d-1)\,T_s, dT_s]$ and $[dT_s, (d-1)\,T_s]$, respectively.

The receiver uses the maximum likelihood decision rule for the detection of residue r_i. For an orthogonal signaling scheme, this decision rule is reduced to selecting the maximum from the set $\{Z_{ij}, j = 0, 1,\ldots, m_i - 1\}$, and the index of the largest decision variable in Fig. 2 denotes the estimation of the transmitted residue r_i. This decision rule is optimum for transmission over an AWGN channel using an orthogonal signaling scheme. However, the MAI is not necessarily Gaussian, hence, this receiver is actually not optimal. It is commonly used, however, for its simplicity.

Using the same method, the estimates of all other transmitted residues of the residue sequence $(r_1, r_2,\ldots, r_u)$ can be obtained by selecting the maximum from the set $\{Z_{ij}, j = 0, 1,\ldots, m_i - 1\}$ for $i = 1,\ldots, u$. Let the received sequence be expressed by $(\hat{r}_1, \hat{r}_2,\ldots, \hat{r}_u)$, then, the transmitted data symbol can be recovered by transforming this residue sequence into its corresponding binary representation. Now let us derive the expressions of the conditional and the unconditional error probabilities in the forthcoming two sections.

4. Performance Analysis: Conditional Symbol Error Probability

Due to the assumptions that $\{\alpha_{ql}\}$, $\{\phi_{ql}\}$ and $\{\tau_{ql}\}$ are modeled as independent random variables for different users q and/or for different diversity paths l, and since random signature sequences are used, the self-interference term $I_{s,\lambda l}$ given by eq. (11) and the multiple-access interference term $I_{m,\lambda l}^{(q,1)}$ given by eq. (12) are also independent random variables. From eqs. (11) and (12), we know that the moments of all random variables $I_{s,\lambda l}$ and $I_{m,\lambda l}^{(q,1)}$ are finite. Consequently, the Liapounoff version of the central-limit theorem [21] holds. Moreover, N_l is Gaussian, since $n(t)$ is Gaussian. Thus Z_{ij} is asymptotically Gaussian. Hence, in this section and the following two sections, we evaluate the performance of the RNS-based CDMA system by using Gaussian approximations. According to eqs. (9) to (13), we can arque that the approximation becomes tight, as the number of simultaneous users Q, the number of moduli u and the number of possible diversity path L increase.

4.1. *Noise analysis*

The noise term N_l, which is given by eq. (13) is a Gaussian random variable with zero-mean and variance $u\alpha_{1l}^2\,N_0/2E_s$ conditioned on a given fading attenuation α_{1l}, where $E_s = E_b\,[\log_2 \prod_{i=1}^{u} m_i]$ is the transmitted energy per symbol period and E_b is the energy per bit.

4.2. *Multipath interference analysis*

The multipath induced self-interference term given by eq. (11) is from the reference user, which includes two contributions: the self-interference from the $L-1$ path signals of residue r_i and the self-interference from the $(u-1)$ L path signals of the other $(u-1)$ residues. The term $I_{s,\lambda l}$ can be approximated as a Gaussian random variable with zero-mean and its variance conditioned on a given fading attenuation α_{1l} can be expressed as [22]

$$\sigma^2\left(I_{s,\lambda l}\middle|\alpha_{1l}\right) = \frac{\alpha_{1l}^2}{3N\left[\log_2 \prod_{i=1}^{u} m_i\right]} E\left\{\alpha_{1\eta}^2\right\} \tag{14}$$

when a rectangular chip waveform is used.

4.3. *Multiple-Access Interference (MAI) analysis*

The multiple-access interference term, due to the q-th interfering user is given by eq. (12). It can also be approximated as a Gaussian random variable with zero-mean and conditional variance of [22]

$$\sigma^2\left(I_{s,\lambda l}^{(q,1)}\middle|\alpha_{1l}\right) = \frac{\alpha_{1l}^2}{3N\left[\log_2 \prod_{i=1}^{u} m_i\right]} E\left\{\alpha_{1\eta}^2\right\} \tag{15}$$

when a rectangular chip waveform is used.

4.4. *Decision statistic and conditional symbol error probability*

In this subsection, the symbol error probability conditioned on the magnitude of the L diversity paths $\{\alpha_{1l}, l = 1, 2,\ldots, L\}$ is derived by treating all interferences as additional noise. First, we obtain the error probabilities for receiving the residues $(r_1, r_2,\ldots, r_u)$, respectively, and then the symbol error probability is computed according to the properties of the RNS. Assuming that the variance of the different diversity branch attenuations is $E\{\alpha_{q\eta}^2\} =$

σ^2, after normalization by $\sqrt{P/2u}\ T_s$, the decision statistics of eq. (9) can be approximated as that of a Gaussian random variable, having a mean given by:

$$E\left[Z_{ij}\middle|\{\alpha_{1l}\}\right]=\sum_{l=1}^{L}\alpha_{1l}^2 \tag{16}$$

and its variance can be computed according to eqs. (9) - (15), which is given by:

$$\sigma^2\left(Z_{ij}\middle|\{\alpha_{1l}\}\right)= \left[\frac{(uL-1)\sigma^2}{3N_s}+\frac{(K-1)uL\sigma^2}{3N_s}+\left(\frac{2E_s}{uN_0}\right)^{-1}\right]\cdot\sum_{l=1}^{L}\alpha_{1l}^2 \tag{17}$$

where $N_s = N\,[\log_2 \prod_{i=1}^{u} m_i]$.

Consequently, the error probability conditioned on the diversity path attenuation $\{\alpha_{1l},\ l = 1, 2,\ldots, L\}$ for receiving residue r_i, $i = 1, 2,\ldots, u$ can be expressed as [18]

$$p_{m_i}\left(\varepsilon\middle|\{\alpha_{1l}\}\right)\approx\frac{(m_i-1)}{2}\operatorname{erfc}\left(\sqrt{\frac{\gamma}{2}}\right) \tag{18}$$

where erfc $(x) = 2\pi^{-1/2}\int_x^{\infty}\exp(-t^2)\,dt$ is the complementary error function [18], and

$$\gamma=\gamma_c\sum_{l=1}^{L}\alpha_{1l}^2 \tag{19}$$

$$\gamma_c=\left[\frac{(uL-1)\sigma^2}{3N_s}+\frac{(K-1)uL\sigma^2}{3N_s}+\left(\frac{2E_s}{uN_0}\right)^{-1}\right]^{-1} \tag{20}$$

If we assume that all the moduli are used just for transmitting information and there are no redundant moduli in residue number system for error-detection and error-correction, or in other words, if the dynamic range of the binary information data is in the interval $[0, \prod_{i=1}^{u} m_i)$, then the symbol is received correctly, if and only if, all the received residues are correct. Hence, after obtaining the conditional error probabilities for receiving residues $(r_1, r_2,\ldots, r_u)$ in eq. (18), the total symbol error probability conditioned on the diversity path attenuations $\{\alpha_{1l},\ l = 1, 2,\ldots, L\}$ can be computed by:

$$p\left(\varepsilon\middle|\{\alpha_{1l}\}\right)=1-\prod_{i=1}^{u}\left[1-p_{m_i}\left(\varepsilon\middle|\{\alpha_{1l}\}\right)\right] \tag{21}$$

The unconditional error probability will be computed by treating the α_{1l} terms as Rayleigh distributed random variables in the following section.

5. Uncoded performance: average error probability

The symbol error probability given in eq. (21) is conditioned on the random variables $\{\alpha_{1l},\ l = 1, 2,\ldots, L\}$, representing the fading diversity path amplitudes. Hence, the (unconditional) average error probability depends on the probability distribution of $\sum_{l=1}^{L}\alpha_{1l}^2$. Since aij is Rayleigh-distributed, $\sum_{l=1}^{L}\alpha_{1l}^2$ is a Chi-square-distributed random variable with $2L$ degree of freedom, and the probability density function of $\gamma = \gamma_c \sum_{l=1}^{L}\alpha_{1l}^2$ in eq. (19) is given by [18]:

$$p(\gamma)=\frac{1}{(L-1)!\,\bar{\gamma}_c^{L}}\gamma^{L-1}\exp\left(-\gamma/\bar{\gamma}_c\right) \tag{21}$$

where $\bar{\gamma}_c = \gamma_c\, E\,\{\alpha_{1l}^2\} = \gamma_c\,\sigma^2$.

Due to the individual residue error probabilities $p_{m_i}(\varepsilon|\ \{\alpha_{1l}\})$ being independent random variables, the average symbol error probability can be computed as the expected value of the symbol probabilities of eq. (21), which is given by:

$$\bar{P}_s(\varepsilon)=E\left[P\left(\varepsilon\middle|\{\alpha_{1l}\}\right)\right]=1-\prod_{i=1}^{u}\left\{1-E\left[p_{m_i}\left(\varepsilon\middle|\{\alpha_{1l}\}\right)\right]\right\} \tag{23}$$

where

$$E\left[p_{m_i}\left(\varepsilon\middle|\{\alpha_{1l}\}\right)\right]=\int_0^{\infty}p_{m_i}\left(\varepsilon\middle|\{\alpha_{1l}\}\right)p(\gamma)\,d\gamma= (m_i-1)\left(\frac{1-\mu}{2}\right)^{L}\sum_{k=0}^{L-1}\binom{L-1+k}{k}\left(\frac{1+\mu}{2}\right)^{k} \tag{24}$$

and

$$\mu=\sqrt{\frac{\bar{\gamma}_c}{2+\bar{\gamma}_c}} \tag{25}$$

Finally, the bit error probability of the uncoded RNS based DS-CDMA system is computed from the symbol error probability of eq. (23), as follows [18]:

$$\bar{P}_b=\frac{2^{k-1}}{2^k-1}\bar{P}_s(\varepsilon) \tag{26}$$

where $k = [\log_2 \prod_{i=1}^{u} m_i]$ is the number of bits per symbol.

6. Coded performance

It is well known that the performance of a digital communication system can be improved by using error correction coding. However, fading-induced channel memory can degrade the coded performance. Usually, in order to disperse the burst errors, interleaving is used before coding. Unfortunately, long interleaving is unacceptable for voice communication, since a large interleaving may lead to long delays.

Reed-Solomon (RS) codes [18] are an efficient class of linear codes using multi-bit symbols that are maximum distance separable. They exhibit powerful burst error and erasure correction capability. An extended code RS (N_t, K_t), where N_t is the number of coded symbols and K_t is the number of information symbols, respectively, can correct up to $[(N_t - K_t)/2]$ random symbol errors, or detect up to $(N_t - K_t)$ symbol errors.

Alternatively, it is capable of correcting up to $(N_t - K_t)$ symbol erasures. Moreover, it is capable of correcting n_t or less random symbol errors and n_e symbol erasures, simultaneously, if and only if $2n_t + n_e \le N_t - K_t$.

Residue number system product codes (RNS-PC) constitute a class of codes constructed according to the characteristics of the RNS arithmetic [15]. They are also maximum distance separable codes. A RNS (u, v) code has a minimum distance of $(u - v + 1)$. It is able to detect $(u - v)$ or less residue errors and correct up to $[(u - v)/2]$ residue errors. Furthermore, a RNS (u, v) code is capable of correcting a maximum of t residue errors and simultaneously detect a maximum of $\beta > t$ residue errors, if and only if $t + \beta \le u - v$.

In this section, we estimate the performance of a system, in which a code is constructed using the well known concatenated coding principle employing a RNS-PC code as the inner code, and a non-binary RS code as the outer code. The inner code is used not only to correct or detect residue errors, but also to decide, which non-binary RS code symbol is erasured. When the inner RNS (u, v) code is detected in error and the erroneous residues cannot be corrected, the RNS-PC decoding marks the decoded symbol as an erasure. Otherwise, a RS code symbol is obtained by RNS (u, v) decoding. However, the decoded symbol may be still in error due to the limited correction capability of the RNS (u, v) code. Hence, a RS codeword may contain three types of symbols: correct symbols, erasured symbols and erroneous symbols before RS decoding. The outer RS decoding may correct these symbol errors and fill the symbol erasures.

We assume that a redundant residue number system (RRNS) is constructed using the moduli $(m_1, m_2, \ldots, m_u)$, where $(m_1, m_2, \ldots, m_v)$, $(v < u)$ are defined as the information moduli, $(m_{v+1}, m_{v+2}, \ldots, m_u)$ as the redundant moduli, and $m_{v+j} \ge \max\{m_1, m_2, \ldots, m_v\}$ for $j = 1, 2, \ldots, u - v$. The interval $[0, M = \prod_{i=1}^{v} m_i)$ is the information symbols' dynamic range, and $[0, MM_R)$ is the RNS (u, v) code's dynamic range, where $M_R = \prod_{i=v+1}^{u} m_i$. Notice that since the information symbols' dynamic range is $[0, M)$, not $[0, MM_R)$ as in the RRNS, the energy for transmitting a signal, now must be reduced according to $E_s = E_b [\log_2 \prod_{i=1}^{v} m_i]$, and the previous number of chips per symbol, N_s, must be replaced by $N [\log_2 \prod_{i=1}^{v} m_i]$, when the error probabilities are computed. The encoding procedure of the concatenated code is performed as follows:

1) Encode K_t information symbols using a RS (N_t, K_t) code, assuming that a symbol is constituted by k bits, and $2^k \le M$ but $2^{k+1} > M$;
2) Each symbol of the RS (N_t, K_t) code is encoded into a RNS (u, v) code by computing the residues with respect to the moduli $\{m_1, m_2, \ldots, m_u\}$, and expressing the encoded result as $\{r_1, r_2, \ldots, r_u\}$;
3) The u residues are transmitted by selecting u orthogonal spreading PN sequences, as discussed in previous sections.

After the receiver provides the estimates of the u residues, the code can be decoded as follows:

1) The residue errors are detected and/or corrected using RNS (u, v) decoding. If no residue errors are detected, because there are no residue errors or there are undetectable residue errors in the RNS (u, v) code, or since the residue errors are corrected by the RNS (u, v) decoder, an estimate of a RS code symbol is obtained. Otherwise, if uncorrectable residue errors are detected in the RNS (u, v) code, the RS code symbol is marked as an erasure.
2) Following the above estimation of all symbols of a full RS (N_t, K_t) codeword, the symbol errors of the RS codeword are corrected and the erasures are filled by the RS (N_t, K_t) decoder. Otherwise, a "decoding failure" is declared.

Upon using the above decoding procedure, the average symbol error probability, after error-correction only decoding, can be expressed as [18]:

$$\overline{P}(\varepsilon) \approx \frac{1}{N_t} \sum_{i=\lfloor (N_t - K_t)/2 + 1 \rfloor}^{N_t} i \binom{N_t}{i} p_t^i (1 - p_t)^{N_t - i} \tag{27}$$

where p_t is the symbol error probability after RNS-PCerror-correction only decoding but before the RS error-correction only decoding.

The average symbol error probability, after errors-and-erasures decoding, can be expressed as [20]:

$$p\left(\varepsilon \middle| \{\alpha_{1l}\}\right) = 1 - \prod_{i=1}^{u} \left[1 - p_{m_i}\left(\varepsilon \middle| \{\alpha_{1l}\}\right)\right] \tag{21}$$

where $j_0(i) = \max(N_t - K_t + 1 - 2i, 0)$. Note that $\bar{P}(\varepsilon)$ is the joint average probability of the uncorrectable RS symbol errors plus that of the erasures that cannot be filled, while p_t is the probability of symbol error and p_e is the probability that a symbol is erasured, respectively. Assuming that the average error probabilities. $\bar{p}_{m_1}(\varepsilon)$, $\bar{p}_{m_2}(\varepsilon), \ldots, \bar{p}_{m_u}(\varepsilon)$ for receiving the residues $\{r_1, r_2, \ldots, r_u\}$ are given by eq. (24), then p_t and p_e in eqs. (27), (28) are computed as the probabilities of erroneous RNS-PC decoding, as follows:

$$p_t = 1 - \sum_{i=0}^{[(u-v)/2]} P\left[\binom{u}{i}, \varepsilon\right]$$

assuming an error-correction only RNS (u, v) code, where $P[\binom{u}{i}, \varepsilon]$ is the probability that i out of the u residues are received erroneously, but the others error-freely. For example,

$$P\left[\binom{3}{1}, \epsilon\right] = \overline{P}_{m_1}(\epsilon)\left[1 - \overline{P}_{m_2}(\epsilon)\right]\left[1 - \overline{P}_{m_3}(\epsilon)\right] +$$
$$\overline{P}_{m_2}(\epsilon)\left[1 - \overline{P}_{m_1}(\epsilon)\right]\left[1 - \overline{P}_{m_3}(\epsilon)\right] +$$
$$\overline{P}_{m_3}(\epsilon)\left[1 - \overline{P}_{m_1}(\epsilon)\right]\left[1 - \overline{P}_{m_2}(\epsilon)\right]$$

where $\bar{P}_{m_1}(\epsilon)$, $\bar{P}_{m_2}(\epsilon)$, $\bar{P}_{m_3}(\epsilon)$ are given by eq. (24), and the above equation represents the probability of receiving residues of r_1, r_2, and r_3 in error.

For a t-residue error-correction and $\beta > t$ residue error-detection RNS (u, v) code, where $t + \beta \le u - v$, p_t and p_e can be expressed as

$$p_t = 1 - \sum_{i=0}^{\beta} P\left[\binom{u}{i}, \varepsilon\right]$$
$$p_e = \sum_{i=t+1}^{\beta} P\left[\binom{u}{i}, \varepsilon\right] \tag{29}$$

Watson and Hastings have shown [12] that:

$$p_t \approx \frac{1}{M_R}\bar{P}_R(\varepsilon)$$
$$p_e \approx \frac{M_R - 1}{M_R}\bar{P}_R(\varepsilon) \tag{30}$$

for the residue error-detection only RNS (u, v) code, where again $M_R = \prod_{i=v+1}^{u} m_i$ and

$$\bar{P}_R(\varepsilon) = 1 - \prod_{i=1}^{u}\left[1 - \bar{p}_{m_i}(\varepsilon)\right] \tag{31}$$

is the average error probability of the RNS (u, v) code or the average symbol error probability of the RS code.

7. Numerical Results and Discussions

The performance of the proposed RNS-based DS-CDMA system was numerically evaluated and we provide the corresponding performance results for a range of system parameters in this section. Notice that the system is reduced to the traditional M-ary orthogonal DS-CDMA system discussed in [1], when $u = 1$.

In Fig. 3 and Fig. 4, the *BER* versus $\sigma^2 E_b/N_0$ performance of the RNS-based DS-CDMA scheme with $u = 3$

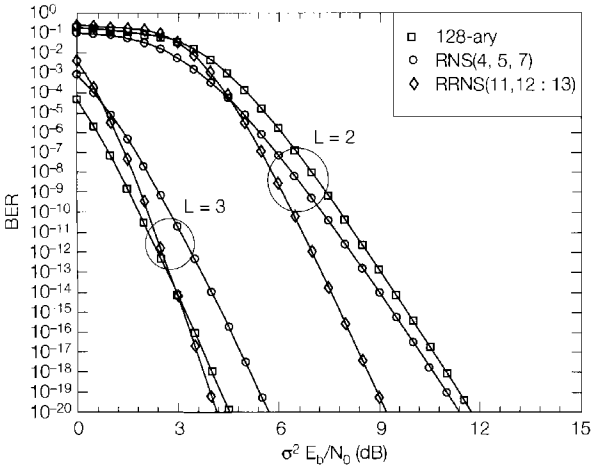

Fig. 3 - Performance comparison of RNS-based ($u = 3$) and M-ary orthogonal ($u = 1$) DS-CDMA system with $Q = 1$ user, $N = 256$ chips per bit, $L = 2$ and 3 diversity paths and RS (128, 99) coding.

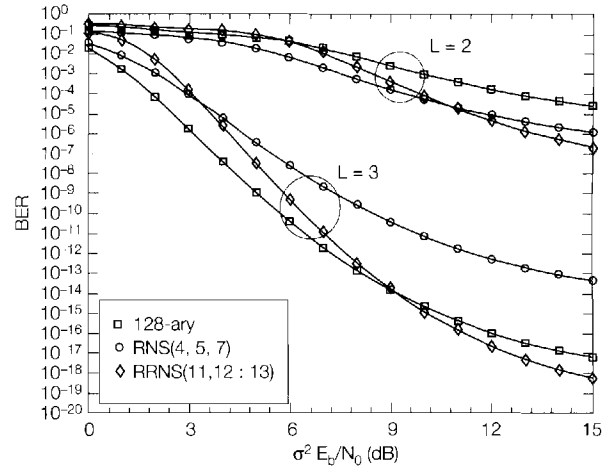

Fig. 4 - Performance comparison of RNS-based ($u = 3$) and M-ary orthogonal ($u = 1$) DS-CDMA system with $Q = 50$ user, $N = 256$ chips per bit, $L = 2$ and 3 diversity paths and RS (128, 99) coding.

and that of M-ary orthogonal DS-CDMA (that is $u = 1$,) are evaluated and compared. In Fig. 3, we let the number of users $Q = 1$, hence, there is no multiple-access interference to the reference signal. However, in Fig. 4, we let $Q = 50$. We assume that an extended RS (128, 99) outer code is adopted for error correction and erasure-filling and a 7 bit Reed-Solomon code symbol is transmitted per symbol period, which corresponds to operating over the Galois Field GF (128). Hence, the average symbol energy is $7\,E_b$ and there are $7N$ chips per symbol. Furthermore, when $u = 1$, M is equal to $2^7 = 128$ for M-ary orthogonal DS-CDMA. When $u = 3$, we let the three relative prime moduli, m_1, m_2, m_3, be 4, 5, 7 corresponding to a non-redundant or to a "no residue error detection" RNS-based DS-CDMA system. Since the product of the moduli obeys $m_1\, m_2\, m_3 = 140 > 128$, any 7 bit symbol can be uniquely represented by a residue sequence (r_1, r_2, r_3) with respect to m_1, m_2, m_3. However, for the RRNS with $(u - v) = 1$ redundant modulus or residue error detection system, we opted for m_1, m_2, m_3 given by 11, 12, 13, respectively, where m_1, m_2 are the information moduli and $m_1\, m_2 = 132 > 128$, while $m_3 = 13$ is the redundant modulus. Usually, for a given dynamic range, i.e., a given number of bits per symbol, the moduli are selected according to the following criteria:

a) the symbol can be uniquely and unambiguously represented by a so-called residue sequence with respect to the moduli;
b) since the sum of the modulus values determines the number of required correlators, the modulus values are selected as close to each other as possible, in order that their product is maximized and their sum is minimized.

Let us consider the single-user performance first, as portrayed in Fig. 3. Firstly, observe that all the three systems have substantially improved performances, when $L = 2$ is increased to $L = 3$, although the largest

improvement was observed in the context of the conventional M-ary DS-CDMA system, characterized by curve "square". When comparing the non-redundant RNS (4, 5, 7) scheme of curve "circle" to the redundant RRNS (11, 12, 13) system, there is a cross-over point for $L = 2$ around $\sigma^2 E_b/N_0 = 5$ dB and for $L = 3$ in the vicinity of 1 dB, above which the RRNS (11, 12, 13) system performs better. Since these $\sigma^2 E_b/N_0$ values are in the useful practical operating range of DS-CDMA systems, the improvements are beneficial in practical terms. Should, however, the $\sigma^2 E_b/N_0$ value experienced fall below these thresholds, the RNS (4, 5, 7) systems will slightly outperform the RRNS (11, 12, 13) arrangement. Furthermore, at $L = 2$ the conventional M-ary DS-CDMA system is outperformed by both RNS-based schemes, despite the reduced complexity of the proposed schemes due to their lower number of correlators. However, for $L = 3$ the best performance was guaranteed by the M-ary DS-CDMA scheme, when $\sigma^2 E_b/N_0$ does not exceed 3 dB, otherwise, the RRNS (11, 12, 13) achieves the best *BER* performance. Lastly, in the complexity comparison also the RNS coding complexity must be taken into account. Similar general conclusions can be drawn also from Fig. 4, where $Q = 50$ users were considered. However, due to the multiple access and matipath interference, the cross-over points of curves "circle" and "diamond" for the RNS (4, 5, 7) and RRNS (11, 12, 13) schemes are shifted to the right-hand side.

Fig. 5 portrays the *BER* versus $\sigma^2 E_b/N_0$ performance with parameters $L = 3$, $N = 256$ and $Q = 10,50,100$ users. The inner code is RRNS (3, 2), where $m_1 = 11$, $m_2 = 12$, $m_3 = 13$ and m_3 is the redundant moduli for error detection. Notice the graceful degradation of the performance as the number of active users, Q, increases.

In Fig. 6, we evaluated the influence of RNS-PC coding on the approximations to the average bit error probability after RS (128, 99) decoding. When $t = 0$ and $\beta = 0$, the three moduli $m_1 = 4$, $m_2 = 5$, $m_3 = 7$ are all information moduli corresponding to a non-redundant or to a

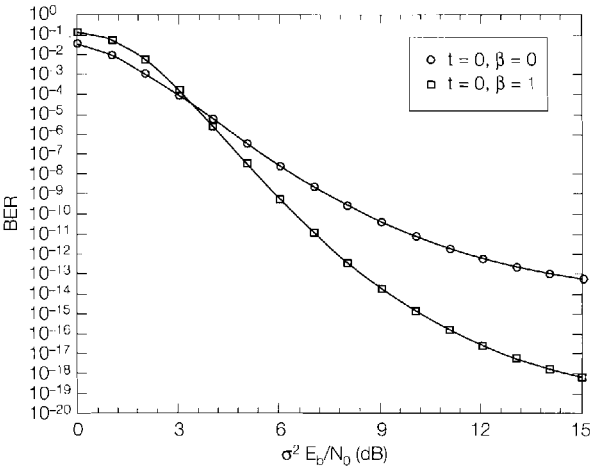

Fig. 6 - Bit error probability of RNS-based DS-CDMA system with RS (128, 99), $u = 3$ moduli, $L = 3$ diversity paths, $N = 256$ chips per bit and $Q = 50$.

"no residue error detection" RNS-based DS-CDMA system. The symbol errors are corrected by RS (128, 99) errors-correction only decoding. When $t = 0$ and $\beta = 1$, moduli $m_1 = 11$, $m_2 = 12$ are the information moduli, and $m_3 = 13$ is the redundant modulus for residue error detection. When using RNS-PC decoding, symbol erasure information is generated, which can be filled in by the RS decoding. Specifically, the symbol errors and erasures are corrected and filled by RS (128, 99) errors-and-erasures decoding. The *BER* of the RNS-based DS-CDMA system with the redundant modulus improved by more than three orders of magnitude in comparison to that of the RNS-based DS-CDMA system without redundant moduli around $\sigma^2 E_b/N_0 = 10$ dB.

In Fig. 7 and Fig. 8, we plotted the bit error probabilities versus $\sigma^2 E_b/N_0$ after RS (128, 99) decoding for a range of other schemes. The inner RNS-PC codes with $u = 5$ moduli (Fig. 7) and $u = 6$ moduli (Fig. 8) are used to correct and/or to detect the residue errors. In Fig. 7 a $u = 5$ moduli inner code, $Q = 50$ users, $N = 256$ chips

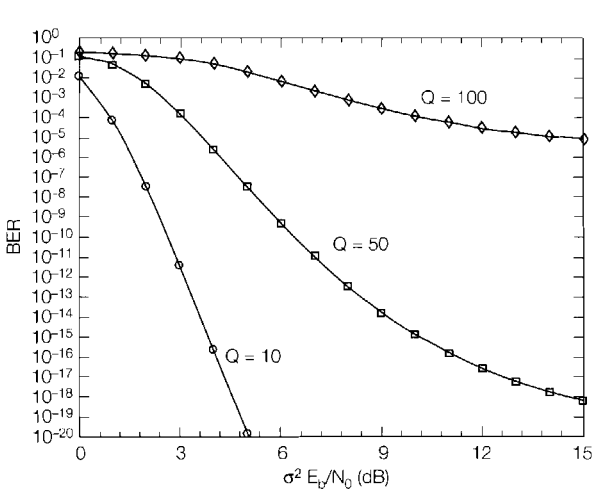

Fig. 5 - Bit error probability of RNS-based DS-CDMA system with RNS (3, 2), RS (128, 99), $L = 3$ diversity paths and $N = 256$ chips per bit for $Q = 10,50$ and 100.

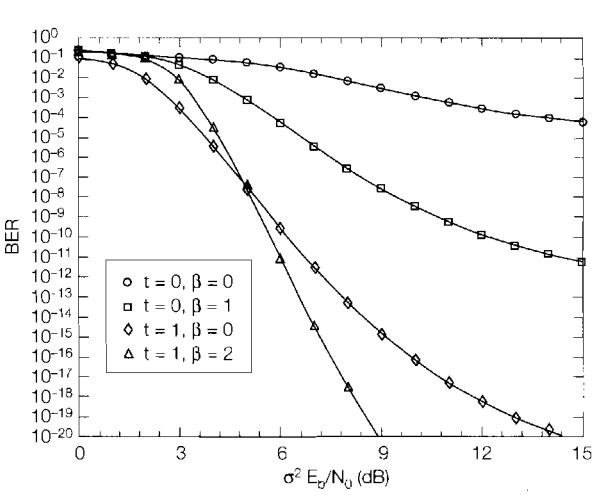

Fig. 7 - Bit error probability of RNS-based DS-CDMA system with RS (128, 99), $u = 5$ moduli, $L = 3$ diversity paths, $N = 256$ chips per bit and $Q = 50$.

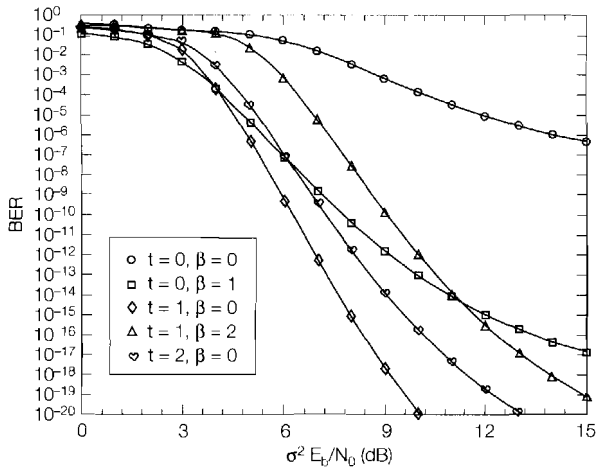

Fig. 8 - Bit error probability of RNS-based DS-CDMA system with RS (128, 99), u = 3 moduli, L = 3 diversity paths, N = 256 chips per bit and Q = 50.

per bit, L = 3 diversity paths are assumed and the other parameters are given by Table 1. In Fig. 8 a u = 6 moduli inner code, Q = 50, N = 256, L = 3 diversity paths are assumed and the other parameters are given by Table 2. Note that the moduli used in Fig. 7 and Fig. 8 were chosen according to the same selection criteria, which were used in of Fig. 3 and Fig. 4. For a given number of moduli, one set of moduli sometimes can be used for the different inner codes as shown in Table 2.

The results show that, for a given total number of total moduli, the system performance can be optimized by varying the relative number of information moduli v and redundant moduli $(u - v)$, as well as by appropriately choosing the values of each modulus. For example, given u = 6 in Fig. 8, the results show that the system with the inner RNS (6, 3) code, for which the information moduli are m_1 = 5, m_2 = 6, m_3 = 7, and the redundant moduli are m_4 = 11, m_5 = 13, m_6 = 17, and t = 1, β = 2, i.e. scenario "diamond" achieves the best performance.

Table 1 - *Parameters for 5 moduli inner code*

No.	RNS-PC Code	Capability of Correction and Detection	Values of Moduli m_1, m_2, m_3, m_4, m_5
(1)	RNS (5, 5)	$t = 0, \beta = 0$	2, 3, 5, 7, 11
(2)	RRNS (5, 4)	$t = 0, \beta = 1$	3, 5, 7, 8, 11
(3)	RRNS (5, 3)	$t = 1, \beta = 0$	5, 6, 7, 11, 13
(4)	RRNS (5, 2)	$t = 1, \beta = 2$	11, 12, 13, 17, 19

Table 2 - *Parameters for 6 moduli inner code*

No.	RNS-PC Code	Capability of Correction and Detection	Values of Moduli $m_1, m_2, m_3, m_4, m_5, m_6$
(1)	RRNS (6, 4)	$t = 0, \beta = 2$	2, 3, 5, 7, 11, 13
(2)	RRNS (6, 2)	$t = 1, \beta = 3$	11, 12, 13, 17, 19, 23
(3)	RRNS (6, 4)	$t = 1, \beta = 0$	2, 3, 5, 7, 11, 13
(4)	RRNS (6, 2)	$t = 2, \beta = 0$	11, 12, 13, 17, 19, 23
5)	RRNS (6, 3)	$t = 1, \beta = 2$	5, 6, 7, 11, 13, 17

8. Conclusions

A communication system based on the combination of RNS or RRNS and spread-spectrum modulation has been presented. The performances of the uncoded and coded systems with coherent RAKE receiver have been studied, when considering a combination of AWGN and multiple-access interference besides multipath fading. From the results, we draw the following conclusions:

1) The performance of the proposed RNS-based DS-CDMA system was significantly improved with an increasing number of diversity paths, when the channel was the multipath fading channel. However, in the RNS-based DS-CDMA communication system, since each user activates multiple spreading PN sequences, the system performance is seriously affected by both multiple-access interference and multipath interference. The interference inflicted to a reference signal comes from each PN sequence of the interfering users, consequently, the performance is more sensitive to these interference sources than that of the M-ary orthogonal DS-CDMA system, which was proposed and studied in [1].
2) Systems with the same length inner RNS-PC codes, equal number of active users and equal-length spreading PN sequences have been compared. The results show that the RNS-PC codes are a class of powerful residue error-detection codes. By using RNS error-detection codes to find residue errors and to provide erasure information for RS decoding, the error control performance of the non-binary RS code with errors-and-erasures decoding is effectively improved and hence the system performance is also enhanced.
3) Given a constant-length inner RNS-PC code, the performance of RNS-based DS-CDMA systems can be optimized by varying the relative number of information moduli and redundant moduli as well as by optimizing the moduli values.

Appendix A
Average power of a random sequence

In this Appendix, we will derive the average power

of the random sequence which is represented by

$$V = \sum_{i=1}^{u} \sum_{n=-\infty}^{\infty} V_{i,n} P_{T_c}(t - nT_c) \quad (A.1)$$

where $V_{i,n}$ are independent random variables assuming values of {+1, −1} with equal probability and $P_{T_c}(t)$ is the rectangular chip waveform over the interval defined as $[0, T_c)$. We write eq. (A.1) in the following form,

$$V = \sum_{n=-\infty}^{\infty} \lambda P_{T_c}(t - nT_c) \quad (A.2)$$

where

$$\lambda = \sum_{i=1}^{u} V_{i,n} \quad (A.3)$$

for $-\infty < n < \infty$. As the quantities of $V_{i,n}$ are independent random variables and take values of +1 or −1, respectively, with equal probability, hence, the distribution function of λ can be directly derived and represented as

$$f_u(\lambda) = 2^{-u} \sum_{i=0}^{u} \binom{u}{i} \delta[\lambda - (2i - u)] \quad (A.4)$$

where $\binom{u}{i} = u!/i!\,(u-i)!$ and $\delta(\cdot)$ is the dirac-Delta function, while λ is a discrete random variable, assuming values in $\{-u, -u+2, \ldots, u-2, u\}$ with probability $f_u(\lambda)$.

For a rectangular pulse having amplitude λ, which is defined in $[\tau_1, \tau_2)$, the average power over $[\tau_1, \tau_2)$ can be computed by

$$\bar{P}_{\text{pulse}} = \lambda^2, \quad \text{for} \quad \tau_1 \le t < \tau_2 \quad (A.5)$$

Hence the average power of the sequence of eq. (A.1) having amplitude distribution given by eq. (A.4), can be computed as

$$\bar{P}(V) = \sum_{i=0}^{u} \lambda^2 f(\lambda) \quad (A.6)$$

Finally, upon simplifying eq. (A.6) using $\sum_{i=0}^{u} \binom{u}{i} = 2^u$, $\sum_{i=1}^{u} i \binom{u}{i} = u2^{u-1}$ and $\sum_{i=1}^{u} i^2 \binom{u}{i} = u(u+1)2^{u-2}$. The average power of eq. (A.1) is derived as

$$\bar{P}(V) = u \quad (A.7)$$

Acknowledgment

The authors wish to thank the anonymous reviewers for thier helpful suggestions.

Manuscript received on July 1, 1997.

REFERENCES

[1] P. K. Enge, D. V. Sarwate: *Spread-spectrum multiple-access performance of orthogonal codes: Linear receivers.* "IEEE Transactions on Communications", Vol. COM-35, December 1987, p. 1309-1319.

[2] P. K. Enge, D. V. Sarwate: *Spread-spectrum multiple-access performance of orthogonal codes: Impulsive noise.* "IEEE Transactions on Communications", Vol. COM-36, January 1988, p. 98-105.

[3] M. Chase, K. Pahlavan: *Performance of DS-CDMA over measured indoor radio channels using random orthogonal codes.* "IEEE Transactions on Vehicular Technology", Vol. 42, November. 1993, p. 617-624.

[4] L.Vandendorpe: *Multitone spread spectrum multiple access communications system in a multipath Rician fading channel.* "IEEE Transactions on Vehicular Technology", Vol. 44, May 1995, p. 327-337.

[5] S. Sasaki, H. Kikuchi, J. K. Zhu: *Performance of parallel combinatory SS communication systems in Rayleigh fading channel.* "IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences", Vol. E77-A, June 1994, p.1028-1032.

[6] E. D. D. Claudio, G. Orlandi, F. Piazza: *A systolic redundant residue arithmetic error correction circuit.* "IEEE Transactions on Computers", Vol. 42, April 1993, p.427-432.

[7] M. H. Etzel, W. K. Jenkins: *Redundant residue number systems for error detection and correction in digital filters.* "IEEE Transactions on Acoustic, Speech, and Signal Processing", Vol. ASSP-28, October 1980, p.538-545.

[8] B. Tseng, G. A. Jullien, W. C. Miller: *Implementation of FFT structures using the residue number system.* "IEEE Transactions on Computers", Vol. 28, November 1979, p. 831-844.

[9] D. Radhakrishnan, Y. Yuan: *Novel approaches to the design of VLSI RNS multipliers.* "IEEE Transactions on Circuits and Systems-II", Vol. 39, January 1992, p. 52-57.

[10] R. Krishnan, G. A. Jullien, W. C. Miller: *Complex digital signal processing using quadratic residue number systems.* "IEEE Transactions on Acoustic, Speech, and Signal Processing", Vol. ASSP-34, February 1986, p.166-177.

[11] R. J. Cosentino: *Fault tolerance in a systolic residue arithmetic processor array.* "IEEE Transactions on Computers", Vol. 37, July 1988, p. 886-889.

[12] R. W. Watson, C. W. Hastings: *Self-checked computation using residue arithmetic.* "Proceedings of the IEEE", Vol. 54, December 1966, p. 1920-1931.

[13] H. Krishna, K. Lin, J. Sun: *A coding theory approach to error control in redundant residue number system- Part I: Theory and single error correction.* "IEEE Transactions on Circuits and Systems-II", Vol. 39, January 1992, p. 8-17.

[14] J. Sun, H. Krishna: *A coding theory approach to error control in redundant residue number system- Part II: Multiple error detection and correction.* "IEEE Transactions on Circuits and Systems-II", Vol. 39, January 1992, p.18-34.

[15] K. Krishna, J. Sun: *On theory and fast algorithms for error correction in residue number system product codes.* "IEEE Transactions on Computers", Vol. 42, July 1993, p. 840-852.

[16] K. M. Elleithy, M. A. Bayoumi: *Fast and flexible architecture for RNS arithmetic decoding.* "IEEE Transactions on Circuits and Systems-II", Vol. 39, April 1992, p.226-235.

[17] G. Alia, E. Martinelli: *A VLSI algorithm for direct and reverse conversion from weighted binary number system to residue number system.* "IEEE Transactions on Circuits and Systems", Vol. 31, December 1984, p.1033-1039.

[18] J. G. Proakis: *Digital communications.* McGraw-Hill, New York, 1989.

[19] M. B. Pursley: *Performance evaluation for phase-coded spread-spectrum multiple-access communication-Part I: system analysis.* "IEEE Transactions on Communications", Vol. 25, August 1977, p. 795-799.

[20] J. Galambos: *Introductory probability theory.* Marcel Dekker, New York and Basel, 1984.

[21] L. B. Milstein, et al.: *Performance evaluation for cellular CDMA.* "IEEE J. on Selected Areas in Communications", Vol. 10, May 1992, p. 680-689.

[22] T. Vlachus, E. Geraniotis: *Performance study of hybrid spread-spectrum random-access communications.* "IEEE Transactions on Communications", Vol. 39; June 1991, p. 975-985.