RATIO STATISTIC TEST ASSISTED RESIDUE NUMBER SYSTEM BASED PARALLEL COMMUNICATION SCHEMES

Lie-Liang Yang and Lajos Hanzo

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

ABSTRACT

A residue number system (RNS) based parallel communication system is proposed and its performance is evaluated using non-coherent demodulation. Diversity reception techniques with equal gain combining (EGC) or selection combining (SC) are considered and the related performance is evaluated *using both a non-redundant and redundant residue* number system based orthogonal signalling scheme. The so-called ratio statistic test (RST) is introduced for enhancing the system's bit error rate (BER) performance. The BER performance for the above mentioned scenarios is evaluated numerically with respect to specific system parameters. Coding gains up to 8.5dB or 11dB are achieved at a BER of 10^{-6} using one or two redundant moduli, respectively.

1. INTRODUCTION

Flexible, high-bit-rate, low bit error rate 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 binary, octal or hexadecimal number system with a base of 2, 8, 16, etc. for implementation. Often the naturally weighted binary system is favoured. In a binary system, due to the carry forward property of the weighted number system a bit error may affect all the bits of the result. By contrast, the so-called residue number system (RNS) [1] is a non-weighted number system. Due to its carry-free property, the RNS can be advantageously introduced in communication and computation systems, in order to protect the information processed or transmitted. In recent years, RNS based arithmetics have received wide attention due to their robust self-checking, error-detection, error-correction and fault-tolerant signal processing properties [1]-[3].

In this paper, a residue number system (RNS) based parallel communication system is proposed and its bit-error-rate (BER) performance is evaluated over indoor multipath fading channels using a receiver with non-coherent demodulation and equal gain combining [4](EGC) or selection combining [7](SC) diversity. The inherent properties of the RNS arithmetic on the bit-error-rate (BER) of the RNS-based orthogonal signaling system are presented and the so-called ratio statistic test (RST) is introduced for dropping some

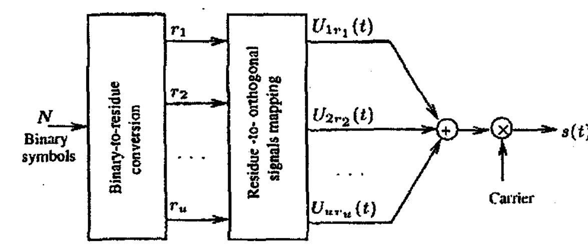

Figure 1: The transmitter block diagram.

low-reliability demodulation outputs and consequently for enhancing the system's BER performance [5, 6].

2. SYSTEM DESCRIPTION

2.1. Transmitter model

A residue number system is defined [1] by the choice of v positive integers m_i, $(i = 1, 2, \ldots, v)$ referred to as moduli. If all the moduli are pairwise relative primes, any integer N, describing a non-binary message, can be uniquely and unambiguously represented by the so-called residue sequence $(r_1, r_2, \ldots, r_v)$ in the range $0 \leq N < M_I$, where $r_i = N \pmod{m_i}$ represents the residue digit of N upon division by m_i, and $M_I = \prod_{i=1}^{v} m_i$ is the information symbols' dynamic range. Conversely, according to the so-called Chinese reminder theorem (CRT) [2], for any given v-tuple $(r_1, r_2, \ldots, r_v)$, 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 recover the message N from the received residue digits.

For incorporating error control [1]-[3], the RNS has to be designed with redundant moduli, which is referred to as a redundant residue number system (RRNS). A RRNS is obtained by appending an additional $(u-v)$ number of moduli $m_{v+1}, m_{v+2}, \ldots, m_u$, where $m_{v+j} \geq max\{m_1, m_2, \ldots, m_v\}$ is referred to as a redundant modulus, to the previously introduced RNS, in order to form an RRNS of u positive, pairwise relative prime moduli. Now an integer N in the range $[0, M_I)$ is represented as a u-tuple residue sequence, $(r_1, r_2, \ldots, r_u)$ with respect to the u moduli. In the RRNS, the integer N can be recovered by any v out of u residue digits using their related moduli due to the inherent properties of the RNS arithmetic. The transmitter block diagram of the proposed RNS-based parallel communication

VTC'99, Houston, USA

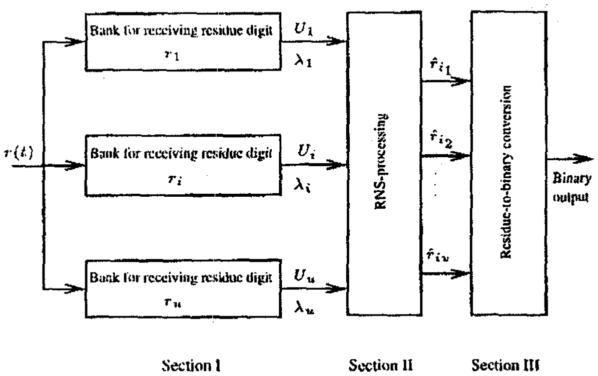

Figure 2: The receiver block diagram with RNS-processing.

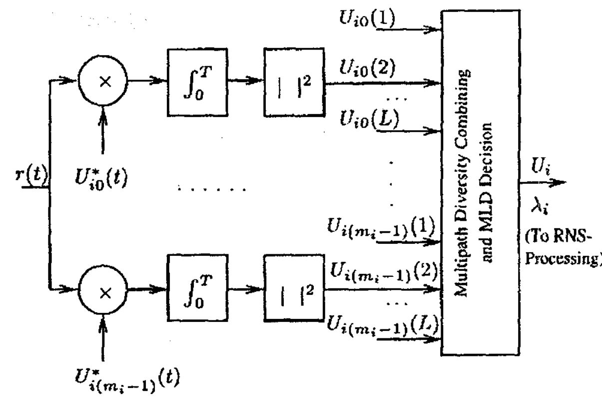

Figure 3: The non-coherent demodulation bank for receiving residue digit r_i.

system using orthogonal signalling is shown in Fig.1. According to the principles of the RNS, the binary information to be transmitted is first transformed to the residues $(r_1, r_2, \ldots, r_u)$, which are then mapped in Fig.1 to the orthogonal sequences $(U_{1r_1}, U_{2r_2}, \ldots, U_{ur_u})$ and multiplexed for transmission. The transmitted signal can be expressed as:

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

for $0 \leq t < T$, where f_c is the carrier frequency.

2.2. Channel Model

Multipath measurements of the indoor radio channel at about 1GHz in and around office buildings [8] showed that it can be characterized by slowly varying, multipath Rayleigh fading. The complex lowpass equivalent impulse response is expressed as [9]:

$$h(t) = \sum_{l=1}^{L_p} \beta_l e^{j\phi_l} \delta(t - \tau_l), \tag{2}$$

where $\delta(\cdot)$ is the Dirac function, while β_l, ϕ_l, and τ_l are the l-th path gain, phase shift and time delay of the transmitted signal, respectively, and L_p represents the number of resolvable paths at the receiver. Hence, for any input signal $s(t)$ expressed in the form of Eq.(1), the channel output signal $r(t)$ produced by the composite multipath fading channel consists of a sum of delayed, phase shifted, attenuated replicas of the input signal, and the lowpass equivalent received signal can be written as:

$$r(t) = \sum_{l=1}^{L_p} \sum_{i=1}^{u} \beta_l e^{j\varphi_l} U_{ir_i}(t - \tau_l) + N(t), \tag{3}$$

where $\varphi_l = \phi_l - 2\pi f_c \tau_l$ is uniformly distributed in $[0, 2\pi)$ and $N(t)$ represents a zero-mean Gaussian stationary random process with single-sided power spectral density of N_0.

2.3. Receiver Model

Fig.2 portrays the proposed non-coherent receiver for receiving the RNS-based orthogonal signals in the form of Eq.(3). Section I of the Figure consists of u number of banks of correlators, square-law detectors, multipath diversity reception combining and maximum likelihood detection (MLD) units, where each bank is dedicated to receiving one residue digit. The ith bank of Fig.2 is shown in Fig.3. The receiver has a diversity reception structure, consequently, L multipath components will be tracked, where $L = 1, 2, 3, \ldots$ and $L \leq L_p$ depends on the design of the receiver, although there are L_p number of signal replicas at the receiver.

According to the properties of the RNS arithmetic [1], if an RNS is designed with redundant moduli using the RRNS, then some residue digits can be discarded without affecting the result, provided that a sufficiently high dynamic range is retained in the reduced-range system, in order to contain the result. The above statement can be augmented as follows. Let $\{m_1, m_2, \ldots, m_u\}$ be a set of u moduli of an RRNS, where $m_1 < m_2 < \ldots < m_u$. Let N be the value of an information symbol, which is expressed as $(r_1, r_2, \ldots, r_u)$ with respect to the above moduli. If the dynamic range of N is $[0, \prod_{i=1}^{v} m_i)$, where $v \leq u$, then N can be recovered from any v out of the u number of residue digits and their relevant moduli. This property implies that, after the MLD of the u banks, d, $(d \leq u-v)$ number of MLD outputs can be dropped before the residue-to-binary conversion, 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, or the residue digit errors in the retained MLD outputs can be corrected using the so-called residue number system product codes (RNS-PC) invoked in our system. The variables λ_i for $i = 1, 2, \ldots, u$ in Fig.2 are computed in the process of demodulating the residue digits and they are used as the metrics for making decisions as to which MLD outputs will be dropped before the RNS-PC decoding, an issue that will be discussed in Section 3.

Given the properties of the RNS arithmetic, RNS-PCs are usually suggested for error-control. RNS-PCs constitute a class of codes constructed according to the characteristics of the RNS arithmetic [2]. They are maximum minimum distance separable codes. A RNS(u, v) code, where the information dynamic range is $[0, \prod_{i=1}^{v} m_i)$ and the code dynamic range is $[0, \prod_{i=1}^{u} m_i)$, has a minimum distance of $(u - v + 1)$. It is capable of detecting $(u - v)$ or less residue digit errors and correct up to $[(u-v)/2]$ residue digit errors. Furthermore, a RNS(u,v) code is capable of correcting a maximum of t_{max} residue errors and simultaneously to detect a maximum of $\beta > t_{max}$ residue errors, if and only if $t_{max} + \beta \leq u - v$.

Moreover, let d be the number of discarded residue digits, where $d \leq u - v$. Then, a RNS(u,v) is changed to a RNS$(u-d,v)$ after d out of the u residue digits and related moduli are discarded. Obviously, the reduced RNS$(u-d,v)$ 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 RNS(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 RNS$(u-d,v)$ decoding. Since the discarded outputs do not have to be considered in the RNS$(u-d,v)$ decoding, the decoding procedure is simplified.

Accordingly, as seen in Fig.2, the RNS-processing unit of Section II in the receiver is used to implement the above algorithms, such as 'error-correction only', 'error-dropping only' as well as 'error-dropping-and-correction'. The performance of the system using these algorithms will be evaluated in the forthcoming Sections.

After the RNS-processing, the set of v retained residue digits of the RNS-processing outputs are input to the residue-to-binary conversion block of Fig.2 (Section III), and the estimation of the information symbol value N ensues according to known RNS decoding algorithms.

3. DIVERSITY COMBINING TECHNIQUES AND RATIO STATISTIC TEST

Let an information symbol of $N = 0$, which is represented by a residue sequence $\{0, 0, \ldots, 0\}$ with respect to moduli $\{m_1, m_2, \ldots, m_u\}$ of a RNS be transmitted. Furthermore, let $U_{ij}(l)$, $i = 1, 2, \ldots, u$; $j = 0, 1, \ldots, m_i - 1$ be the output of the square-law detector for the ith residue digit on the l-th diversity channel. Then, $U_{ij}(l)$ can be expressed as:

$$U_{i0}(l) = |\frac{2\xi}{u}\beta_l e^{j\varphi_l} + N_{k0}|^2, \; i = 1, 2, \ldots, u, \quad (4)$$

$$U_{ij}(l) = |N_{ij}|^2, \; i = 1, 2, \ldots, u; \; j \neq 0, \quad (5)$$

when each residue digit is transmitted using equal energy, where N_{ij} is a zero-mean complex Gaussian random variable with variance $4\xi N_0/u$, and the channel gain coefficient $\beta_l e^{j\varphi_l}$ is also a zero-mean complex Gaussian random variable with variance $E[\beta_l^2]$. Here, $E[\,]$ represents the expected value of the argument.

3.1. Equal Gain Combining

For a receiver with L-th order $(L \leq L_P)$ diversity reception and Equal Gain Combining (EGC), the L paths are equally weighted and then added to form the decision variables of:

$$U_{ij} = \sum_{l=1}^{L} U_{ij}(l) \quad (6)$$

for $i = 1, 2, \ldots, u$ and $j = 0, 1, \ldots, m_i - 1$. The decision rule is that for each value of i we select the largest value from the set $\left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}$ and map it to the estimation of r_i. Correspondingly, the RST is defined as [10]:

$$\lambda_i = \frac{{}^1\max_i \left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}}{{}^2\max_i \left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}}, \quad (7)$$

where ${}^1\max_i\{\cdot\}$ and ${}^2\max_i\{\cdot\}$ represent the maximum and the 'second maximum' - ie the second largest - of the correlator outputs of $\left\{U_{i0}, U_{i1}, \ldots, U_{i(m_i-1)}\right\}$, respectively, which are used for receiving residue digit r_i. It is plausible that when the first maximum is significantly higher, than the second highest correlator output, then the decision is a high-reliability one and vice-versa. Hence the outputs associated with the lowest values of λ_i are the lowest-reliability outputs, which can be dropped in the RNS-processing process.

3.2. Selection Combining

For an L-branch Selection Combining (SC) receiver, in which the branch signal with the largest amplitude is selected for demodulation, the decision variables are given by Eq.(4) and Eq.(5) for the l-th multipath component, when the residue sequence $(0, 0, \ldots, 0)$ is transmitted. Here we introduce a two-stage maximum selection, in order to invoke the RST. In the first-stage maximum selection, the maximum of the L diversity components $\{U_{ij}(1), U_{ij}(2), \ldots, U_{ij}(L)\}$ for each specific given i and j is selected, since only one output is matched to the transmitted signal and $(m_i - 1)$ outputs are mismatched after this selection. Hence, the first-stage L-branch diversity selection outputs are expressed as:

$$U_{ij} = \max\{U_{ij}(1), U_{ij}(2), \ldots, U_{ij}(L)\}, \quad (8)$$

for $i = 1, 2, \ldots, u$ and $j = 0, 1, \ldots, m_i - 1$.

In the second-stage maximum selection of the schematic, the maximum of the first-stage outputs, namely that of $\{U_{ij}\}$ for each i is selected for demodulation, i.e:

$$U_i = \max\left\{U_{i1}, U_{i2}, \ldots, U_{i(m_i-1)}\right\}, \quad (9)$$

for $i = 1, 2, \ldots, u$ and we map these maxima to the estimates of the residues r_i $i = 1, 2, \ldots, u$. Simultaneously, the ratio of the maximum to the 'second maximum' is computed in this processing stage, which is defined in Eq.(7).

4. PERFORMANCE RESULTS

In this Section, the average bit error rate (BER) is evaluated as a function of the average signal-to-noise (SNR) per bit, which is computed by $\overline{\gamma}_b = \frac{L_p u \overline{\gamma}_0}{\log_2 \prod_{i=1}^{v} m_i}$ for all systems described above.

Fig.4 shows the bit error probability for the EGC and SC schemes with $L = 1, 2, 3$. In the computations, we assume that there were $L_p = 3$ number of resolvable multipaths components at the receiver, and a non-redundant RNS-based system with its moduli assuming values of $m_1 = 7$, $m_2 = 8$, $m_3 = 9$ was considered. As expected, both the EGC and SC schemes provide dramatic BER improvements for moderate to high average SNRs per bit, when the number of combined diversity paths, L, increases. Furthermore, the results show that the EGC scheme has a lower BER than the SC scheme. This is because that EGC is the optimal diversity combining scheme for non-coherent demodulation.

In Fig.5, which is related to the EGC scheme and in Fig.6 characterising the SC scheme, we evaluated the BER

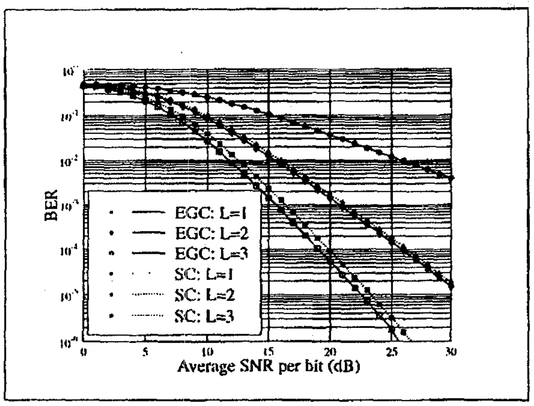

Figure 4: **EGC, SC:** BER versus average SNR per bit for the RNS-based system with 3 moduli, $m_1 = 7$, $m_2 = 8$, $m_3 = 9$ and $L_p = 3$.

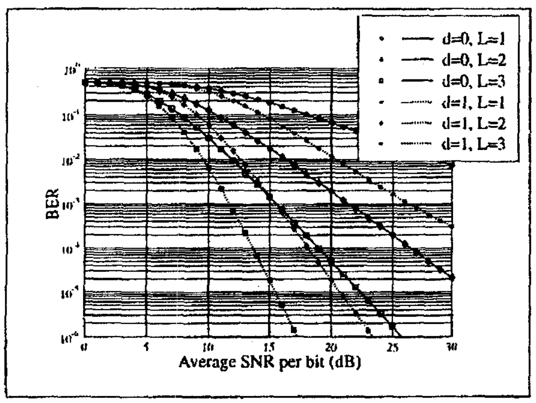

Figure 5: **EGC:** BER versus average SNR per bit for the RNS-based system with 7 moduli, $m_1 = 29, m_2 = 31, m_3 = 32, m_4 = 33, m_5 = 35, m_6 = 37, m_7 = 41$, and $L_p = 3$, where d is the number of lowest-reliability inputs of RNS-processing dropped.

performance of a RRNS-based system employing RNS-processing without redundancy, or using one redundant modulus with one lowest-reliability input of the RNS-processing being discarded, which we denote as $d = 0$ and $d = 1$. In the related computations, moduli of 29, 31, 32, 33, 35, 37, 41, as well as $L_p = 3$ total resolvable paths were used, and $L = 1$, 2 or 3 paths were combined in the receiver using an EGC or SC scheme. The results show that when the RNS is designed with redundant moduli, the BER performance of both the EGC and the SC scheme is substantially improved. Taking $L = 2$, 3 paths as examples, the EGC scheme can achieve an error rate of 10^{-4} at SNRs per bit of 18dB or 13.5dB, when one lowest-reliability input of the RNS-processing is dropped, which are shown by the $d = 1$, $L = 2$ and $d = 1$, $L = 3$ curves. However, if the RNS-based system is designed without redundancy, an average of 26dB or 19dB SNR per bit is required for the EGC scheme using $L = 2$ or $L = 3$ to achieve the bit error

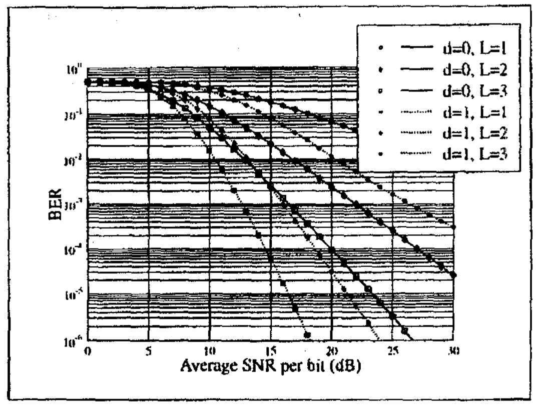

Figure 6: **SC:** BER versus average SNR per bit for the RNS-based system with 7 moduli, $m_1 = 29, m_2 = 31, m_3 = 32, m_4 = 33, m_5 = 35, m_6 = 37, m_7 = 41$, and $L_p = 3$, where d is the number of lowest-reliability inputs of RNS-processing dropped.

rate of 10^{-4}. This implies that we can obtain about 8dB or 5.5dB gain at $P_b(\epsilon) = 10^{-4}$ by using one lowest-reliability RNS-processing input dropping for $L = 2$ or 3, respectively. Similarly, the SC scheme using $L = 2$ or 3 can achieve an error rate of 10^{-4} at SNRs per bit of 18.5dB or 14.5dB, and obtain about 8dB or 5.5dB gain at $P_b(\epsilon) = 10^{-4}$ by using one lowest-reliability RNS-input dropping for $L = 2$ or 3, respectively.

Similarly to Fig.5 and Fig.6, in Fig.7 and Fig.8 we evaluated the BER performance of a 10-moduli RNS-based communication system using EGC or SC schemes, when $d = 2$ lowest-reliability inputs of the RNS-processing were dropped or $t_{max} = 1$ residue digit error-correction RNS-processing was considered. Obviously, these two RNS-based systems used the same number of redundant moduli and had the same information rate. The parameters related to the computations were $m_1 = 29$, $m_2 = 31$, $m_3 = 35$, $m_4 = 36$, $m_5 = 37$, $m_6 = 41$, $m_7 = 43$, $m_8 = 47$, $m_9 = 53$, $m_{10} = 59$, and $L_p = 5$. Observe that the BER of the RNS-based system with the two lowest-reliability inputs of the RNS-processing discarded is lower than that of the system with one residue digit error-correction RNS-processing, when the same number of multipath components are combined in the receiver. Specifically, the EGC scheme with two lowest-reliability inputs dropped requires 2dB or 1.5dB less bit-SNR, than that of the system with one residue digit error-correction, in order to achieve the BER of 10^{-4}, when $L = 2$ or $L = 3$ multipath components is combined in the receiver, respectively. The results imply that, for a ten-moduli RNS-based system, RNS-processing using lowest-reliability dropping is a highly-effective RNS-processing method for improving the system's BER performance. Furthermore, the complexity of the RNS(10,8) decoding of dropping two of the lowest-reliability inputs of the RNS-processing is much lower than that of the RNS(10,8) one residue digit error-correction decoding.

Finally, the coding gains achieved in Fig.5 to Fig.8 were summarized in Table 1, where $k = \lfloor \log_2 \prod_{i=1}^{v} m_i \rfloor$ is the number of bits of the transmitted symbol represented by

Table 1: Summary of Coding Gain Achieved in Fig.5-Fig.8.

RNS-processing Mode	k (bits)	Values of Moduli	EGC or SC	L_p	L	Coding gain (dB) 1×10^{-3}	Coding gain (dB) 1×10^{-6}
One redundant		$m_1=29, m_2=31, m_3=32,$		3	2	6	>10
modulus and	30	$m_4=33, m_5=35, m_6=37,$	EGC	3	3	3.5	8.5
lowest-reliability		$m_7=41$		3	2	6	>10
input dropping			SC	3	3	3.5	8.5
Two redundant		$m_1=29, m_2=31, m_3=35,$		5	2	8	>11
moduli and	41	$m_4=36, m_5=37, m_6=41,$	EGC	5	3	6	11
lowest-reliability		$m_7=43, m_8=47, m_9=53$		5	2	8	>11
input dropping		$m_{10}=59$	SC	5	3	6	11
Two redundant		$m_1=29, m_2=31, m_3=35,$		5	2	6.5	>9
moduli and	41	$m_4=36, m_5=37, m_6=41,$	EGC	5	3	4.5	9
one residue digit		$m_7=43, m_8=47, m_9=53$		5	2	6.5	>9
error correction		$m_{10}=59$	SC	5	3	4.5	9

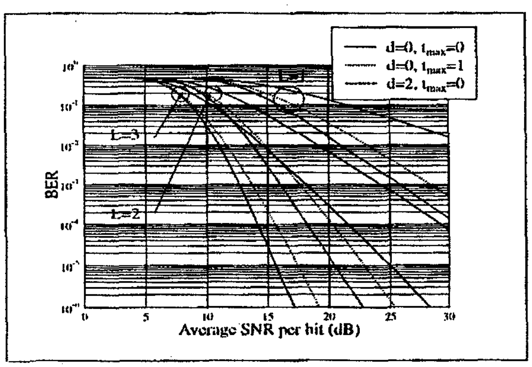

Figure 7: **EGC:** BER versus average SNR per bit for the RNS-based system with 10 moduli, $m_1=29, m_2=31, m_3=35, m_4=36, m_5=37, m_6=41, m_7=43, m_8=47, m_9=53, m_{10}=59$, and $L_p=5$, where t_{max} is the number of errors corrected by RNS$(u-d, v)$ and d is the number of lowest-reliability inputs of RNS-processing dropped.

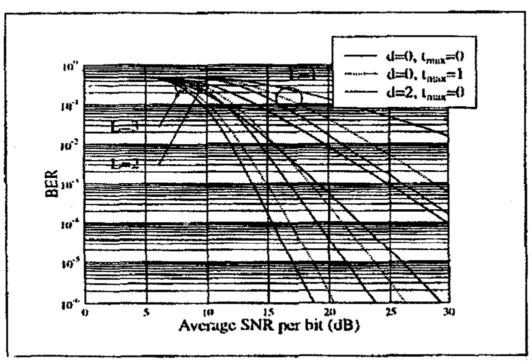

Figure 8: **SC:** BER versus average SNR per bit for the RNS-based system with 10 moduli, $m_1=29, m_2=31, m_3=35, m_4=36, m_5=37, m_6=41, m_7=43, m_8=47, m_9=53, m_{10}=59$, and $L_p=5$, where t_{max} is the number of errors corrected by RNS$(u-d, v)$ and d is the number of lowest-reliability inputs of RNS-processing dropped.

the related RRNS.

5. ACKNOWLEDGEMENT

The financial support of Motorola ECID, Swindon, UK and that of the European Commission in the framework of the First and Median projects is gratefully acknowledged. Sincere thanks are also due to the EPSRC, UK and to the Virtual Centre of Excellence in Mobile Communications as well as to the Royal Society.

6. REFERENCES

[1] K. W. Watson, "Self-checking computations using residue arithmetic," *Proc. of the IEEE*, Vol. 54, No. 12, pp. 1920-1931, Dec. 1966.

[2] H. Krishna and J. D. Sun,"On theory and fast algorithms for error correction in residue number system product codes,"*IEEE Trans. on Computers* Vol. C-42, No. 7, pp. 840-852, July 1993.

[3] W. K. Jenkins and E. J. Altman, "Self-checking properties of residue number error checkers based on mixed radix conversion," *IEEE Trans. on Circuits and Systems*, Vol. 35, No. 2, pp. 159-167, Feb. 1988.

[4] 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. SAC-12, No. 5, pp.862-870, June 1994.

[5] L-L. Yang, L. Hanzo: Performance of Residue Number System Based DS-CDMA over Multipath Channels Using Orthogonal Sequences, European Tr. on Comms., Vol.9, No.6, Nov.-Dec. 1998, pp 525-535

[6] L-L. Yang, L. Hanzo: Ratio Statistic Test Assisted Residue Number System Based Parallel Communication Schemes, Proc. of VTC'99, Houston, USA, May, 1999

[7] G. Chyi, J. G. Proakis, and C. M. Keller, " On the symbol error probability of maximum-selection diversity reception schemes over a Rayleigh fading channel," *IEEE TCOM*, Vol. COM-37, No. 1, pp. 79-83, Jan. 1989.

[8] A. A. M. Saleh and A. Valenzuela, "A statistical model for indoor multipath propagation," *IEEE J. Select. Areas Commun.*, Vil.5, pp.138-146, Feb. 1987.

[9] J. G. Proakis, *Digital Communications*, (2nd Ed.) McGraw-Hill, New York, 1989.

[10] 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.