RESIDUE NUMBER SYSTEM BASED MULTIPLE CODE DS-CDMA SYSTEMS

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 novel multi-code direct-sequence code division multiple-access (DS-CDMA) system based on the so-called residue number system (RNS) or the redundant residue number system (RRNS) is proposed. Concatenated codes employing RNS product codes (RNS-PC) as the inner codes and non-binary Reed-Solomon (RS) codes as the outer codes are adopted to improve the system performance. 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, as well as by appropriately choosing the moduli's values.

1. SYSTEM DESCRIPTION

The background of M-ary Residual Number System (RNS) and Redundant RNS based parallel transmission techniques was documented in [1, 2]. *In contrast to the equal-gain combining (EGC) and selection combining (SC) schemes of [2], the results of this paper are based on maximal ratio combining (MRC) assisted, RNS product-code (RNS-PC) protected direct sequence code division multiple access (DS-CDMA).* More explicitly, the class of specific concatenated codes that employ an RNS-PC [3] as inner code and a non-binary Reed-Solomon (RS) code as outer code was adopted for error correction and detection. The inner code is used to detect or correct the residue errors, and the non-binary RS code with errors-only decoding or errors-and-erasures decoding is used to correct the symbol errors or to fill the symbol erasures.

A residue number system is defined[3] 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 an arbitrary non-binary message in this paper, can be uniquely and unambiguously represented by the so-called residue sequence $(r_1, \ldots, r_v)$ in the range $0 \leq X < M$, 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 of the system, in which quantities can be uniquely represented. According to the so-called Chinese reminder theorem[3] (CRT), for any given v-tuple $(r_1, r_2, \ldots, r_v)$, where $0 \leq r_i < m_i$, $i = 1, 2, \ldots, v$ there exists one and only one integer X such that $0 \leq X < M$ and $r_i = X \pmod{m_i}$.

It can be shown that, if orthogonal sequences are employed for transmitting each of the residues in parallel, $\sum_{i=1}^{v} m_i$ sequences are required, in order to transmit k bits of information in one symbol period, provided that $M = \prod_{i=1}^{v} m_i \geq 2^k$. Consequently, $\sum_{i=1}^{v} m_i$ correlators are required in the receiver. In contrast to our proposed parallel structure, a conventional M-ary orthogonal CDMA system[4] can be adopted to transmit a k-bit symbol, requiring 2^k orthogonal sequences per transmitter. Hence, 2^k correlators are required in the receiver in order to detect a k-bit symbol, which is much higher than in case of the proposed RNS-based system. Explicitly, the conventional approach is unacceptable in complexity terms for large values of k.

By contrast, since the proposed RNS-based communication system needs a low number of orthogonal sequences for a relatively high value of v, it is possible for our RNS-based DS-CDMA system to achieve a high-bit-rate capability by using a relatively low number of orthogonal sequences. For example, for $v = 5$ and using the relative prime integers of $m_1 = 7, m_2 = 11, m_3 = 13, m_4 = 15, m_5 = 16$, the dynamic range given by their product is larger than 2^{17} and hence can accommodate a 17-bit symbol. This symbol can be transmitted in parallel during one symbol period by using 64 orthogonal Walsh codes. Moreover, by controlling the number of transmitted residues, ie by adjusting the dynamic range of the transmitted message, the transmission bit-rate can be varied, in order to support multi- and/or variable-rate communications without increasing the hardware complexity of the receiver.

For incorporating error control, we are concerned

THE FINANCIAL SUPPORT OF THE FOLLOWING ORGANISATIONS IS ACKNOWLEDGED: MOTOROLA ECID, SWINDON, UK; EUROPEAN COMMISSION; EPSRC, UK; VIRTUAL CENTRE OF EXCELLENCE IN MOBILE COMMUNICATIONS, UK; ROYAL SOCIETY, UK.

VTC'99, Houston, USA

0-7803-5565-2/99/$10.00 © 1999 IEEE

with the so-called RRNS [3], which is obtained by appending an additional $(u - v)$ number of moduli, ie $m_{v+1}, m_{v+2}, \ldots, m_u$, referred to as redundant moduli, to the previously introduced RNS. This system constitutes 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 the integer X in the range $[0, M)$ is represented as a u-tuple,$(r_1, r_2, \ldots, r_u)$, corresponding to u moduli. Let us now focus our attention more closely on the analysis of the proposed RNS-based multi-code DS-CDMA communication system.

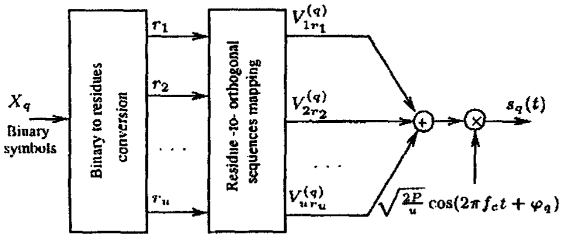
X_q
Binary symbols
Binary to residues conversion
r_1
r_2
...
r_u
Residue -to- orthogonal sequences mapping
$V^{(q)}_{1r_1}$
$V^{(q)}_{2r_2}$
...
$V^{(q)}_{ur_u}$
$s_q(t)$
$\sqrt{\frac{2P}{u}}\cos(2\pi f_c t + \varphi_q)$

Figure 1: The transmitter's block diagram for user q.

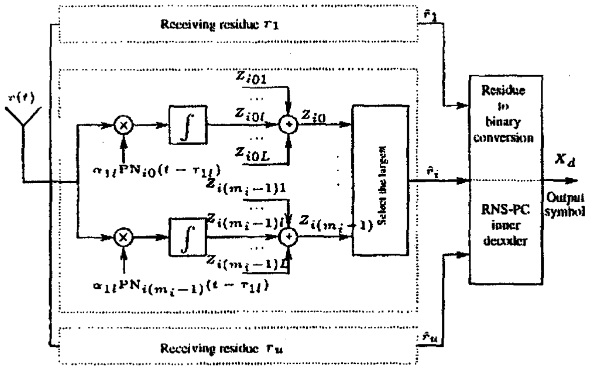

Figure 2: RAKE receiver for the reference signals.

1.1. Transmitted Signal

The block diagram of the proposed RNS based multi-code DS-CDMA communication system is shown in Fig.1. As seen in the Figure, the information to be transmitted is first transformed to a residue sequence, namely $(r_1, r_2, \ldots, r_u)$. We initially assume that all the u moduli are used for information transmission, that is $(v = u)$ and hence no redundant moduli are assigned. The residue digits are then mapped to the 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, where the subset of m_i orthogonal sequences is used for the transmission of residue r_i. Furthermore, $N_s = T_s/T_c$, where T_s is the symbol duration and T_c is the spreading sequence chip duration. The symbol duration T_s is given by $T\lfloor \log_2 \prod_{i=1}^{u} m_i \rfloor$, where $\lfloor x \rfloor$ represents the largest integer less than or equal to x. Let the integer message X_q be represented by a residue sequence of $(r_1, r_2, \ldots, r_u)$ with respect to the moduli $m_1, m_2, \ldots, m_u$, where $r_i = X_q \pmod{m_i}$, $(i = 1, 2, \ldots, u)$. Then u specific PN sequences $(V^{(q)}_{1r_1}, V^{(q)}_{2r_2}, \ldots, V^{(q)}_{ur_u})$ can be selected from the $\sum_{i=1}^{u} m_i$ sequences of the q-th user. After modulating the carrier by the baseband signal, the composite signal transmitted by user q in the period $[dT_s, (d+1)T_s]$ can be expressed as:

$$s_q(t) = \sqrt{\frac{2P}{u}} \sum_{i=1}^{u} \mathrm{PN}^{(q)}_{ir_i}(t) \cos(2\pi f_c t + \varphi_q), \qquad (1)$$

$$\mathrm{PN}^{(q)}_{ir_i}(t) = \sum_{n=-\infty}^{\infty} V^{(q)}_{ir_i,\rho} P_{T_c}(t - nT_c), \qquad (2)$$

where f_c is the carrier frequency, $\rho = n - [n/N_s] * N_s$, $P_{T_c}(t)$ represents the rectangular chip waveform with chip-duration of T_c, while $P_\tau(t) = 1$ for $0 \leq t < \tau$ and $P_\tau(t) = 0$ otherwise. Lastly, φ_q represents the phase angle introduced by the qth user's carrier modulation. Since it can be shown that the average power of $\sum_{i=1}^{u} PN^{(q)}_{ir_i}(t)$ is u, when random signature sequences are assumed [5], hence, the average transmitted power of the signal represented by Eq.(1) is P.

1.2. Receiver Model

In order to combat the multipath distortion and to achieve an improved performance, diversity combining is employed. For 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}. The coherent correlator RAKE receiver using maximal ratio combining (MRC) is shown in Fig.2 for the reference user or user-of-interest, ie for user $q = 1$, where the user-index superscript has been omitted for convenience. The receiver uses the maximum likelihood decision rule for the detection of residue r_i. For an M-ary orthogonal signalling 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 estimate of the transmitted residue r_i.

Using the same method, the estimates of all other transmitted residues of the residue sequence $(r_1, \ldots, r_u)$ 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 as $(\hat{r}_1, \hat{r}_2, \ldots, \hat{r}_u)$, then, the transmitted data symbol can be recovered by transforming this residue sequence into its corresponding binary representation.

2. SYSTEM PERFORMANCE AND DISCUSSION

Due to the assumptions that $\{\alpha_{ql}\}$, $\{\phi_{ql}\}$ and $\{\tau_{ql}\}$ are modelled as independent random variables for different users q and/or for different diversity paths l, and since random signature sequences are assumed, the multipath-induced self-interference and the multiple access interference can be modelled as additive Gaussian noise, and consequently Gaussian approximation can be employed to estimate the BER performance. The average bit error probability of our RNS-based system was evaluated analytically, but the details are omitted here due to lack of space.

It is well known that the performance of a digital communication system can be improved by using error correction coding. Concatenated coding is a technique of combining relatively simple codes to form a powerful coding system for achieving high performance and large coding gain with reduced decoding complexity.

RNS-PCs constitute a class of maximum minimum distance separable codes [3], akin to RS codes. The RNS-PC can provide a powerful error-correction and error-detection capability, which is very similar to that of RS codes, but the inherent parallel structure of the RNS arithmetic and their flexibility in design render RNS-PCs an attractive alternative for using as inner codes. Short RNS-PCs used as inner codes can be conveniently combined with longer outer RS codes, constituting one RS-coded symbol, in order to form the concatenated RS-RNS code. Using an RS-RNS concatenated code, after RNS-PC inner decoding, the symbol error probability is typically decreased to a degree, which may maximize the external RS coding gain, and hence the average symbol error probability is further decreased to the required degree using RS decoding. In addition, since RNS-PCs constitute a class of codes providing a powerful error-detection capability using a low number of redundant moduli, using RNS-PC error-detection decoding, symbol error information can be provided for the RS outer decoding. Consequently, the effectiveness of the RS code utilizing 'error-and-erasure correction' decoding can be enhanced upon exploiting the explicit error detection capability of the inner code, since in this case the error positions are known by the RS decoder.

The performance of the proposed RNS-based multicode 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 [4], 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 $u = 3$ and that of M-ary orthogonal DS-CDMA, ie when $u = 1$ were evaluated and compared. In Fig.3, we let the number of users $Q = 1$, hence, there is no multiple-access interference inflicted upon the reference signal. However, in Fig.4, we let $Q = 50$. We adopted an extended RS$(128, 99)$ outer code for error correction and erasure-filling and a 7-bit Reed-Solomon code symbol was transmitted per symbol period, which corresponds to operating over the Galois Field $GF(128)$. Hence, the average symbol energy is $7E_b$ 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 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 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, ie for 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 the curve corresponding to the 'square' legends. When comparing the non-redundant RNS$(4, 5, 7)$ scheme corresponding to the curve associated with the 'circle' legends 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 1dB, 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 3dB, 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 multipath interference, the cross-over points of the curves denoted by the 'circle' and 'diamond' legends 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 modulus used 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-PCs 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 'no residue error detection' RNS-based DS-CDMA system. The symbol errors are corrected by RS$(128,99)$ 'error-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 per bit, $L = 3$ diversity paths were used and the other parameters were given by Table 1. In Fig.8 a $u = 6$ moduli inner code, $Q = 50$, $N = 256$, $L = 3$ diversity paths were used and the other parameters were 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. Furthermore, given a number of moduli, this set of moduli sometimes can be used for a variety of inner codes, as exemplified in Table 2.

The results show that, for a given total number of 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 $t = 1, \beta = 2$, i.e. the curve identified by the 'diamonds' achieves the best performance.

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 1: Parameters for 5-moduli inner code

NO.	RNS-PC code	Capability of correction 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

Table 2: Parameters for 6-moduli inner code

3. REFERENCES

[1] 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

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

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

[4] P. K. Enge, D. V. Sarwate, "Spread-spectrum multiple-access performance of orthogonal codes: Linear receivers," *IEEE Trans. on commun.*, Vol. COM-35, pp. 1309-1319, Dec. 1987.

[5] V, M. Jovanovic and E. S. Sousa, "Analysis of non-coherent correlation in DS/BPSK spread spectrum acquisition," *IEEE Trans. on Commun.*, Vol.43, No.2/3/4, pp.565-573, Feb./Mar./Apr. 1995.

[6] J. G. Proakis: *Digital communications*. McGraw-Hill, 2nd, New York, 1989.

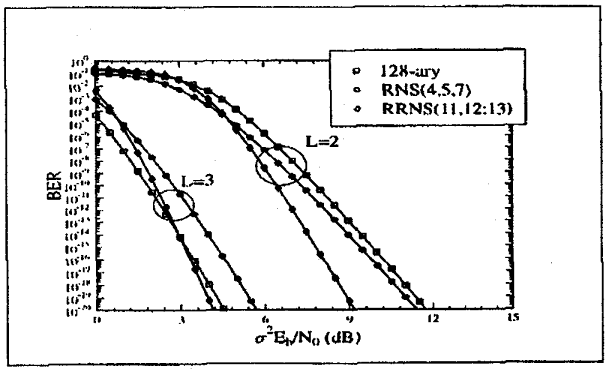

Figure 3: Performance comparison of RNS-based (u = 3) and M-ary orthogonal (u = 1) DS-CDMA system with $Q = 1$ user, $N = 256$ chips per bit, $L = 2$ and 3 diversity paths and RS(128,99) coding.

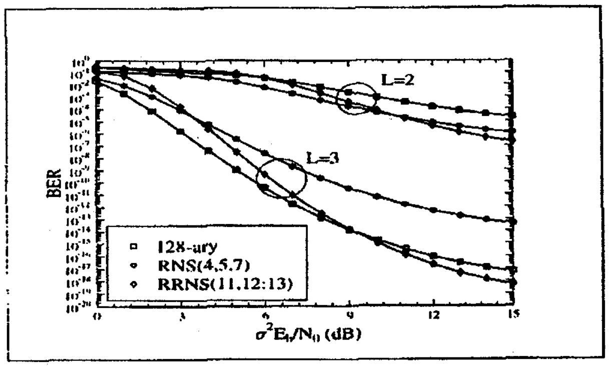

Figure 4: Performance comparison of RNS-based (u = 3) and M-ary orthogonal (u = 1) DS-CDMA system with $Q = 50$ user, $N = 256$ chips per bit, $L = 2$ and 3 diversity paths and RS(128,99) coding.

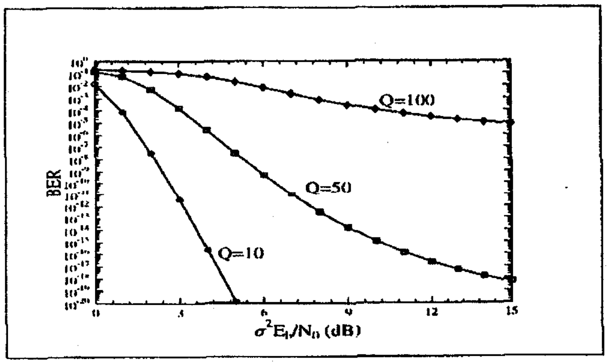

Figure 5: Bit error probability of RNS-based DS-CDMA system with RNS(3,2), RS(128,99), $L = 3$ diversity paths and $N = 256$ chips per bit for $Q = 10, 50$ and 100.

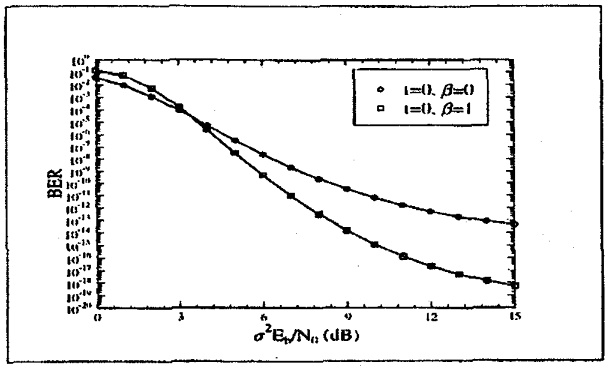

Figure 6: Bit error probability of RNS-based DS-CDMA system with RS(128,99), $u = 3$ moduli, $L = 3$ diversity paths, $N = 256$ chips per bit and $Q = 50$.

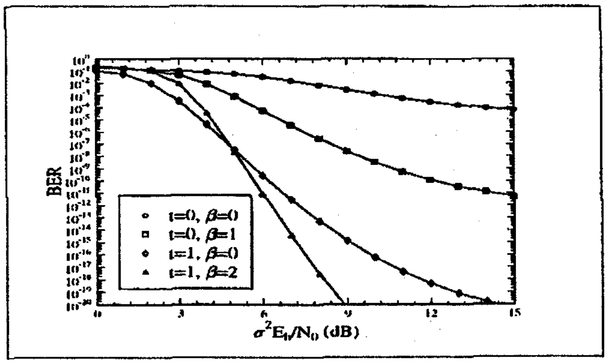

Figure 7: Bit error probability of RNS-based DS-CDMA system with RS(128,99), $u = 5$ moduli, $L = 3$ diversity paths, $N = 256$ chips per bit and $Q = 50$.

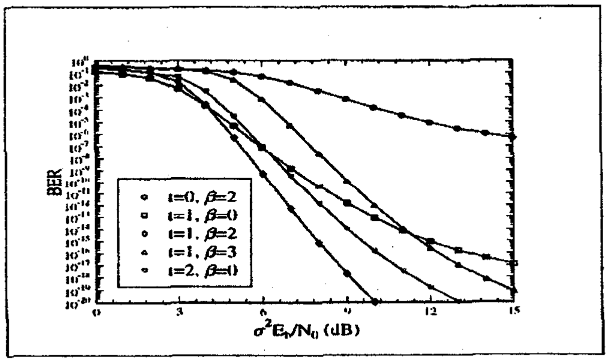

Figure 8: Bit error probability of RNS-based DS-CDMA system with RS(128,99), $u = 3$ moduli, $L = 3$ diversity paths, $N = 256$ chips per bit and $Q = 50$.