Residue Number System Arithmetic Assisted M-ary Modulation

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

***Abstract*— A residue number system based M-ary modem is proposed and its performance is evaluated over Gaussian channels. When one or two redundant moduli are employed, a signal-to-noise ratio gain of 1.2–2 dB was achieved for a 16-ary, 32-ary and 37-ary modem, respectively, at a bit error rate of 10^{-6}.**

I. Introduction

THE SO-CALLED residue number system (RNS) [1]–[3] has two inherent features that render the RNS attractive in comparison to conventional weighted number systems, such as for example the binary representation. These two features are [2]: 1) the carry-free arithmetic and 2) the lack of ordered significance amongst the residue digits. The first property implies that the operations related to the individual residue digits of different moduli are mutually independent because of the absence of carry information. The second property of the RNS arithmetic implies that some of the residue digits can be discarded without affecting the result, provided that a sufficiently "high dynamic range" is retained in the "reduced" system in order to unambiguously contain the result, as argumented below.

In this letter, a RNS-based M-ary signaling scheme is proposed and analyzed, when the RNS is designed with or without redundant moduli and the channel is assumed to inflict additive white Gaussian noise (AWGN). A new ratio statistic test (RST) technique is proposed for dropping a number of the M-ary redundant outputs. Numerical results show that, when the RNS is designed using a moderate number of redundant moduli, we can improve the bit error rate (BER) performance of the proposed system.

II. System Model

A residue number system is defined [1] by the choice of v positive integers m_i, $(i = 1, 2, \cdots, v)$ referred to as moduli. If all the moduli are pairwise relative primes, any integer N, describing a nonbinary message in this letter, can be uniquely and unambiguously represented by the so-called residue sequence $(r_1, r_2, \cdots, r_v)$ in the range $0 \leq N < M_I$, where $r_i = N(\mathrm{mod} m_i)$ 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) [3], for any given v-tuple $(r_1, r_2, \cdots, r_v)$, where $0 \leq r_i < m_i$, there exists one and only one integer N such that $0 \leq N < M_I$ and $r_i = N(\mathrm{mod} m_i)$, which allows us to recover the message N from the received residue digits.

Manuscript received May 22, 1998. The associate editor coordinating the review of this letter and approving it for publication was Prof. E. Biglieri.

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

Publisher Item Identifier S 1089-7798(99)01262-4.

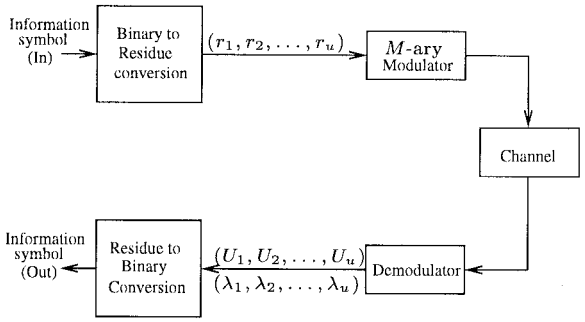

Fig. 1. The system block diagram.

For incorporating error control [2], [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 $m_{v+1}, m_{v+2}, \cdots, m_u$, where $m_{v+j} \geq \max\{m_1, m_2, \cdots, m_v\}$ 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, $(r_1, r_2, \cdots, r_u)$ with respect to the u moduli. In RRNS, the integer N can be recovered by any v out of u residue digits using their related moduli due to the second inherent property of the RNS arithmetic.

The block diagram of the proposed RNS-based orthogonal communication system is shown in Fig. 1. In the transmitter, a multibit information symbol is first transformed to a residue sequence $(r_1, r_2, \cdots, r_u)$ with respect to the moduli $(m_1, m_2, \cdots, m_u)$ of the RNS. Then u residue digits are transmitted using an M-ary scheme one by one serially, where $M \geq \max\{m_1, m_2, \cdots, m_u\}$. It is worth noting at this stage that no limitations apply to the M-ary scheme used. Hence, phase-shift keying (PSK), frequency-shift keying (FSK), and quadrature amplitude modulation (QAM) are equally applicable. In the receiver, the signal is first coherently demodulated using the correlation receiver technique of [4, pp. 260–263] for M-ary orthogonal signals over AWGN channels. After a full residue sequence was received, the estimation of the transmitted data symbol finally can be obtained by transforming the residue sequence to its binary representation. Furthermore, if the RNS-based orthogonal system is designed

with redundant moduli, metrics of λ_i for $i = 1, 2, \cdots, u$ in Fig. 1 are produced in the process of the demodulation and used for making decision of which demodulator outputs will be dropped before the residue to binary conversion, which will be discussed in Section III

III. Performance Estimation

In this section we evaluate the performance of the RNS-based orthogonal signaling system, when the RNS is designed without redundant moduli or with $d = (u - v)$ number of redundant moduli, over an AWGN channel. With an M-ary orthogonal signaling scheme, the probability that a residue digit is decided correctly by selecting the branch exhibiting the largest correlator output is expressed as [4]:

$$P_r(C) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} [1 - Q(y)]^{M-1} e^{-(y-\sqrt{2\gamma})^2/2}\, dy \quad (1)$$

where $Q(y)$ is defined as [4]$Q(y) = 1/\sqrt{2\pi}\int_y^{\infty} e^{-t^2/2}dt$, $\gamma = \xi/uN_0$ is the signal-to-noise ratio (SNR) at the demodulator output. Furthermore, N_0 represents the variance of the noise, ξ is the energy of the transmitted information symbol, which can be computed by $\xi = E_b \cdot \lfloor \log_2 \prod_{i=1}^{v} m_i \rfloor$, since $k_b = \lfloor \log_2 \prod_{i=1}^{v} m_i \rfloor$ bit symbols can be represented by the residue sequences $(r_1, r_2, \cdots, r_u)$, where $\lfloor x \rfloor$ represents an integer not exceeding x, and E_b is the energy per bit.

Consequently, for an RNS-based orthogonal signaling scheme without redundant moduli, that is for $u = v$, the estimation of the transmitted k_b-bit symbol after residue to binary conversion is correct, if and only if, all the u number of residue digits are received correctly. Hence, the average correct symbol probability after residue-to-binary conversion can be written as

$$P_s(C) = [P_r(C)]^v \quad (2)$$

and the average BER can be approximated by [4]

$$P_b(\epsilon) \approx \tfrac{1}{2}\,(1 - P_s(C)). \quad (3)$$

If an RNS-based M-ary signaling system is designed with $d = u - v > 0$ number of redundant moduli, then, as discussed previously, up to d number of demodulator outputs can be dropped before residue to binary conversion, while still recovering the transmitted symbol using the retained demodulator outputs, provided that the retained demodulator outputs are those matched to the related residue digits, i.e., there were no residue digit errors. Conventionally, this kind of dropping is referred to as "erasure." An example of this is known in the context of Reed–Solomon (RS) [5] codes where the low-reliability symbols are erasured and error-and-erasure correction decoding is employed. Since the error-and-erasure correction decoding of RS codes should correct random errors and also fill erasures, the decoding complexity and energy cannot be decreased by dropping the erasured symbols. However, for a RNS designed with d redundant moduli, up to d residue digits having a low-reliability metric λ_i can be discarded, and the discarded residue digits are not required to be considered during the residue to binary conversion, and consequently simplify the symbol recovery procedure. We refer to our decision rule as the RST for deciding which demodulator outputs will be dropped, which we defined as

$$\lambda_i = \frac{^1\max_i\{X_0, X_1, \cdots, X_{M-1}\}}{^2\max_i\{X_0, X_1, \cdots, X_{M-1}\}} \quad (4)$$

where $^1\max_i\{\cdot\}$ and $^2\max_i\{\cdot\}$ represent the maximum and the second maximum of the correlator outputs, say $\{X_0, X_1, \cdots, X_{M-1}\}$, respectively, for receiving residue digit r_i. Our RST is based on the fact that a unreliable received signal is likely to have nearly equal energy in both the correlation branch matched to the correct signal and the correlation branches mismatched to the transmitted signal. Hence, we can argue that the correlator outputs with low absolute value of $|\lambda_i|$ are the low-reliability outputs and can be discarded before residue-to-binary conversion. Consequently, if we assume that the received residue digits are independent, the probability that a symbol is recovered correctly by the residue to binary conversion can be expressed as

$$P_s(C) = \sum_{k=0}^{d} \binom{u}{k} [1 - P_r(C)]^k\, [P_r(C)]^{u-k} P(d, k) \quad (5)$$

where $P_r(C)$ is given by (1), while $P(d,k)$ is the probability of the event that there are k demodulator outputs which are decided erroneously, but the k number of erroneously decided de modulator outputs happen to be discarded by dropping those d number of the demodulator outputs, which have the lowest value of $|\lambda_i|$. Accordingly, we have $P(d,0) = 1$, but $P(d,k)$ for $k \neq 0$ depends on the distribution of $|\lambda_i|$.

Let H_1 and H_0 represent the assumptions that a residue digit is demodulated correctly or erroneously, respectively. Then, for a given value of M and a given residue digit the pdf's of $|\lambda_i|$ under assumptions of H_1 and H_0, i.e., $f_{|\lambda_i|}(y|H_\theta)$ with $\theta \in \{1, 0\}$ can be derived using the distribution density functions of the correlator outputs matched or mismatched to the transmitted residue digit. Examples of the exact numerically evaluated pdf's of $f_{|\lambda_i|}(y|H_1)$ and $f_{|\lambda_i|}(y|H_0)$ with $M = 16$ are shown in Fig. 2 at an SNR per bit of 2 and 5 dB. As expected, under H_1, the value of $|\lambda_i|$ is distributed most probably in the area of $y > 1$, while under H_0, the value of $|\lambda_i|$ is distributed very close to $y = 1$. Moreover, when increasing the SNR per bit of the transmitted signal, the distribution of $f_{|\lambda_i|}(y|H_1)$ will shift to the right-hand side, while the peak of the distribution of $f_{|\lambda_i|}(y|H_0)$ at $y = 1$ becomes higher and higher.

However, using the exact pdf's of $f_{|\lambda_i|}(y|H_\theta)$ to compute $P(d,k)$ is an arduous task due to the quadruple integrals involved. Hence, we invoke approximations to simplify the computations. First, under H_1, the pdf's of the maximum and the second maximum of $^1\max_i\{\cdot\}$ and $^2\max_i\{\cdot\}$ can be approximated as the pdf [4] of the correlator output matched to the transmitted residue digit and the pdf [6] of the maximum amongst the other correlator outputs mismatched to the transmitted residue digit. Upon using these pdf's, we can obtain the pdf of λ_i under assumption H_1 as

$$f_{\lambda_i}(y|H_1) \approx \frac{M-1}{2\pi} \int_0^{\infty} \Big\{ [Q(x)]^{M-2} e^{-(xy+\sqrt{2\gamma})^2/2} + [1 - Q(x)]^{M-2} e^{-(xy-\sqrt{2\gamma})^2/2} \Big\} x e^{-x^2/2} dx. \quad (6)$$

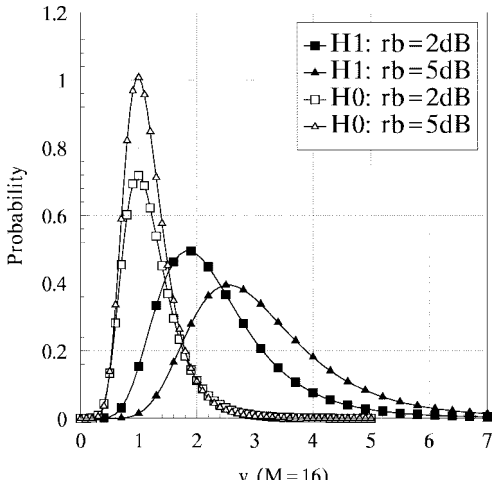

Fig. 2. Exact probability density functions of $|\lambda_i| = \left|{}^1\max_i\{\cdot\}/{}^2\max_i\{\cdot\}\right|$ under the assumptions of H_1 and H_0.

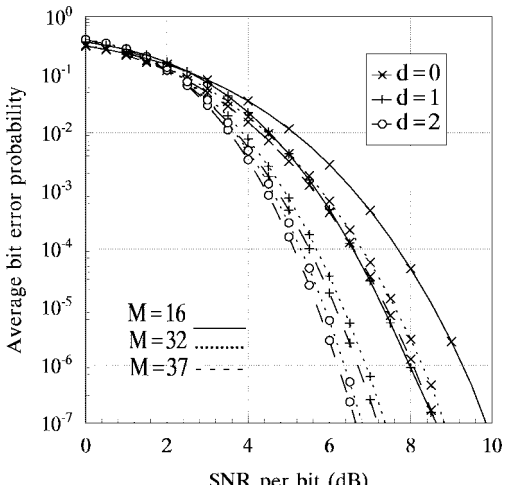

Fig. 3. BER performance of the RNS-based orthogonal system with or without redundant moduli over an AWGN channel.

The pdf of $f_{|\lambda_i|}(y|H_1)$ then can be computed by

$$f_{|\lambda_i|}(y|H_1) = f_{\lambda_i}(y|H_1) + f_{\lambda_i}(-y|H_1). \tag{7}$$

Second, we approximate the pdf of $|\lambda_i|$ under H_0 as $f_{|\lambda_i|}(y|H_0) = \delta(y-1)$, where $\delta(\cdot)$ is a delta function. Note that, if $|\lambda_i|$ is distributed symmetrically around $y=1$, the result obtained using $\delta(y-1)$ is just the average of y over the effective area of $f_{|\lambda_i|}(y|H_0)$. However, since the distribution of $f_{|\lambda_i|}(y|H_0)$ in Fig. 2 is not symmetrical, the result obtained using $\delta(y-1)$ consequently yields an approximation. We further note that the first approximation increases the estimated BER, while the second approximation decreases the BER. However, when the SNR per bit of the transmitted signal is sufficiently high, for example >2 dB for the $M=16$-ary orthogonal system, the result is very close the exact BER.

By using the above approximations, we finally obtain $P(d,k)$ in (5) as

$$P(d,k) = \sum_{m=0}^{d-k} \binom{u-k}{m} \left[\int_0^1 f_{|\lambda_i|}(y|H_1)dy\right]^m \cdot \left[\int_1^\infty f_{|\lambda_i|}(y|H_1)\,dy\right]^{u-k-m} \tag{8}$$

where $d=u-v$ represents the number of redundant moduli. Consequently, the correct symbol probability of the proposed RRNS-based orthogonal system can be evaluated by combining (5) and (8) and the average BER can be approximated by (3).

IV. Numerical Results

Fig. 3 portrays the BER performance of the RNS-based orthogonal system using $M=16$-ary, $M=32$-ary or $M=37$-ary orthogonal signaling schemes for the transmission of the residue digits. Note that, the value of M obeys the relation of $M \geq \max\{m_1, m_2, \cdots, m_u\}$ but not necessary limited to an integer power of 2 in the RNS-based system. The parameters related to the BER computations were given in the Table I. The results of Fig. 3 show that, for the RNS-based system with 16-ary, 32-ary and 64-ary orthogonal signaling schemes, up to 1.2–2 dB of bit SNR, depending on the value of M, can be conserved by using one or two redundant moduli, respectively, at the BER of 10^{-6}.

TABLE I
The Parameters Related to the Numerical Computations

M	d	k_b	m_1	m_2	m_3	m_4	m_5	m_6	m_7
16	0	13	7	11	13	14			
	1	13	7	11	13	14	15		
32	0	22	19	23	25	27	28		
	1	22	19	22	25	27	28	29	
	2	22	19	22	25	27	28	29	31
37	0	24	23	29	31	32	33		
	1	24	23	29	31	32	33	35	
	2	24	23	29	31	32	33	35	37

V. Conclusions

We have proposed and analyzed a novel communication system, which combines the RNS arithmetic with the M-ary orthogonal signaling technique. Our approach is applicable to arbitrary QAM and PSK systems.

References

[1] K. W. Watson, "Self-checking computations using residue arithmetic," *Proc. IEEE*, vol. 54, pp. 1920–1931, Dec. 1966.
[2] E. D. D. Claudio, G. Orlandi, and F. Piazza, "A systolic redundant residue arithmetic error correction circuit," *IEEE Trans. Computers*, vol. 42, pp. 427–432, Apr. 1993.
[3] H. Krishna and J. D. Sun, "On theory and fast algorithms for error correction in residue number system product codes," *IEEE Trans. Computers*, vol. 42, pp. 840–852, July 1993.
[4] J. G. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.
[5] S. Lin and D. J. Costello, *Error Control Coding-Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.
[6] J. N. Pierce, "Theoretical diversity improvement in frequency-shift keying," *Proc. IRE*, vol. 46, pp. 903–910, May 1958.