Analysis of Residue Number System based PN sequence in AWGN channel

Kalpesh G. jadav[1] Khyati P. Vachhani[2]
[1]PG Student, Electronics & Communication Engg. Department
[2]Assistant Professor, Electronics & Communication Engg. Department
[1,2]Kalol Institute of Technology & Research Centre, Kalol, Gujarat

Abstract— The successful use of CDMA technology is based on the construction of large families of encoding sequences with good correlation properties. This paper discusses PN sequence generation based on Residue Arithmetic with an effort to improve the performance of existing interference-limited CDMA technology for mobile cellular systems. All spreading codes with residual number system proposed earlier did not consider external interferences, multipath propagation, Doppler effect etc. In literature the use of residual arithmetic in DS-CDMA was restricted to encoding of already spread sequence; where spreading of sequence is done by some existing techniques. The novelty of this paper is the use of residual number system in generation of the PN sequences which is used to spread the message signal. The significance of cross-correlation factor in alleviating multi-access interference is also discussed. The RNS based PN sequence has superior performance than most of the existing codes that are widely used in DS-CDMA applications. Simulation results suggest that the performance of the proposed system is superior to many existing systems.

Keywords—Direct-Sequence Code Division Multiple Access (DS-CDMA), Multiple-Access Interference (MAI), PN Sequence, Residue Number System (RNS).

I. INTRODUCTION

CODE-DIVISION MULTIPLE-ACCESS (CDMA) based on Spread Spectrum (SS) has emerged as one of the most important multiple access technologies for the second and third generations (2G-3G) wireless communication systems. IS-95, CDMA2000, UMTS-UTRA, WCDMA, and TD-SCDMA [1] are few of the important mobile cellular standards among many where they find applications. But the current CDMA systems are still far from perfect. The CDMA system is always considered as an interference-limited system mainly due to the existence of multiple-access interference (MAI) and multipath interference (MI). Many problems of a communication system based on CDMA technology stem from the unitary spreading codes/sequences, which includes two sub-categories, one being the orthogonal codes, such as Walsh-Hadamard codes and orthogonal variable spreading factor (OVSF) codes, and the other being pseudo-random or pseudo-noise (PN) sequences, such as Gold sequences, Kasami sequences, m-sequences, etc [1], [2].

Pseudo-Random CDMA codes have been found to be more suitable for their use in many wireless applications since orthogonal CDMA codes usually perform extremely bad if they are used for asynchronous channel transmissions where as other category of CDMA codes offer relatively uniform performance for their operation in both synchronous and asynchronous channels. But PN sequences are statistically uncorrelated, and the sum of a large number of PN sequences results in MAI [2]. Pseudo Noise (PN) sequence genera-tors generate PN codes which appear random yet they are completely deterministic in nature with a small set of initial conditions. The security of the concerned system is hence undesirably compromised at times. Practically the quality of transmission takes a toll as the number of users increases for a given code length. In this context this paper presents a PN sequence generator based on Residue Arithmetic which counters the said limitations.

RNS were introduced in field of DS-CDMA by many researchers as early as late 90s [3], [4]. In conventional systems, due to the carry forward required by the weighted number system, a bit error may affect all the bits of the result. In [3], [5] a parallel communication scheme based on RNS, which is a non-weighted carry-free number system, was proposed. The symbol to be transmitted is transformed to RNS representation, mapped into a set of orthogonal sequences and are transmitted in parallel. Error control was also incorporated in this paper using redundant RNS (RRNS) code. For bandwidth efficiency a modulation technique by combining RNS representation, PSK/QAM modulation and orthogonal modulation was proposed in [6]. The error control properties of RRNS were exploited in [7] to be used as channel codes for protecting the speech bits. In [8] residue arithmetic is used for representing the symbol to be transmitted. Redundant residue arithmetic system based multi-carrier DS-CDMA (MC/DS - CDMA) dynamic multiple access scheme has been proposed in [9] for dynamically accessing the frequency spectrum available for Cognitive Radio communication. All references basically points to a parallel communication scheme where the symbol to be transmitted by each user is represented in residue arithmetic and an inverse RNS transform block is used at the receiver to get back the symbol. But generation of PN sequences and use of these to spread message signals for multiple user transmission has never been investigated.

Spreading codes with good cross correlation properties have great significance in multi-user DS-CDMA. RNS has received wide attention due to its robust signal processing properties, however this paper discusses on the design of spreading sequence based on residue arithmetic. RNS number is represented by remainders when invariably divided by a set of numbers or divisors. According to the

Chinese Remainder Theorem (CRT), if this set of divisors is all co-primes to each other, then the residue representation of any number is unique provided the number is within the range R, where R is product of all the numbers in the set of divisors [10]. Since the divisor set is not limited, extension of the set of divisors leads to increase in the number bits in the bit representation of residue number. This property of Residue Arithmetic is exploited here to generate the PN Sequence. It provides a large family of spreading codes with a specific cross-correlation threshold for the system under consideration. Sequences can be generated with different spread factor, and for various cross-correlation threshold values to take care of MAI. The generated sequences can then be put into DS-CDMA system for performance analysis under different loading scenarios. Hence the system has been evaluated in AWGN channel.

RNS were introduced in field of DS-CDMA by many researchers as early as late 90s by Lie Liang Yang and Lajos Hanzo. In conventional systems, due to the carry forward required by the weighted number system, a bit error may affect all the bits of the result. In the proposed a parallel communication scheme based on RNS, which is a non-weighted carry-free number system. The symbol to be transmitted is transformed to RNS representation, mapped into a set of orthogonal sequences and are transmitted in parallel. Error control was also incorporated in this paper using redundant RNS (RRNS) code. Performance of the same system over busty communication channels is done by Madhukumar and Chin.

II. LITERATURE SURVEY

The WCDMA downlink transmission is prone to self-interference caused by the loss of orthogonally between spreading codes due to multipath propagation There are several techniques for interference cancellation and multiuser detection that improves the performance and capacity of the downlink WCDMA system]. Most of these techniques are designed at the expense of higher receiver complexity and with OVSF codes derived from Walsh Hadamard code. Construction methods of OVSF-ZCZ sequences have been proposed to mitigate interference due to multipath propagation. Since the number of OVSF-ZCZ sequences is limited, various assignment algorithms are required to meet the demand of large number of users. The use of Orthogonal Variable Spreading Code (OVSF) code requires that a dedicated rate matching algorithm to be used in the transceivers. This algorithm consumes a great amount of hardware and software resources and increases computation load and processing latency. In the OVSF code generation tree structure, the codes in the upper layer with lower spreading factor blocks the codes in the lower layer with higher spreading factor. i.e., fewer users can be accommodated in a cell. These issues indeed demand for the existing code replacement. In this context this theses presents a Channelization code based on Residue Arithmetic which counter the said limitations. RNS is already used in the design of decimation filters for WCDMA receivers.

III. BASICS OF RNS

Residue number systems are based on the congruence relation as: two integers, a and b are said to be congruent modulo m if m divides exactly the difference of a and b; it is common, especially in mathematics tests, to write $a \equiv b \pmod{m}$ to denote this. Thus, for example, $10 \equiv 7 \pmod 3$, $10 \equiv 4 \pmod 3$, $10 \equiv 1 \pmod 3$ and $10 \equiv -2 \pmod 3$. The number m is a modulus or base, and its values exclude unity produces only trivial congruence. If q and r are the quotient and remainder, respectively, of the integer division of a by m, that is, $a = q * m + r$ then, by definition, $a \equiv r \pmod m$. The number r is said to be the residue of a with respect to m, and is denoted by $r = |a|_m$. The set of m smallest values, {0, 1, 2, 3... (m − 1)} That the residue may assume is called the set of least positive residues modulo m. Consider a set $\{m_1, m_2...m_n\}$, of n positive and pair wise relatively prime moduli. Let R be the product of the moduli. Then every number X < R has a unique representation in the residue number system. A partial proof of this is as follows. Suppose X_1 and X_2 are two different numbers with the same residue set, then

$$|X_1|mi = |X_2|_{mi} \Rightarrow |X_1 - X_2|_{mi} = 0 \ldots\ldots\ldots\ldots (1)$$

Therefore X1 and X2 are the Least Common Multiple (LCM) of mi. But if the mi are relatively prime, then their LCM is R, and it must be that X_1 and X_2 is a multiple of R. So it cannot be that X1 < R and X_2 < R. Therefore, the set $\{|X|mi : 1 \le i \le n\}$ is unique and may be taken as the representation of X and such a representation can be written in the form $<x_1,x_2 \ldots x_n>$ where $x_i = |X|m_i$, and relationship between X and its residues can be indicated by writing $X=<x_1,x_2 \ldots x_n>$. The number R is called the dynamic range of the RNS because the number of numbers that can be represented is R.

IV. STANDARD PN SEQUENCES

A. Maximal Length Sequence: Pseudo Random Binary Sequences (PRBSs), also known as pseudo noise, Linear Feedback Shift Register (LFSR) sequences or maximal length bi- nary sequences (m sequences), are widely used in digital communications. This sequence is generated using a shift register and modulo-2 adders. Certain outputs of the shift register are modulo-2 added and the adder output is fed back to the register. An m-stage shift register can generate a maximal length sequence of 2m -1 bits. Only certain outputs, or taps, can generate maximal length sequences [13].

For CDMA spreading code, we need a random sequence that passes certain "quality" criterion for randomness. These criterions are

1. The number of runs of 0's and 1's is equal. We want equal number of two 0's and 1's, a length of three 0's and 1's and four 0's and 1's etc. This property gives us a perfectly random sequence.
2. There are equal number of runs of 0's and 1's. This ensures that the sequence is balanced.
3. The periodic autocorrelation function (ACF) is nearly two valued with peaks at 0 shifts and is zero elsewhere. This allows us to encrypt the signal effectively

B. Gold Sequence: Gold Sequence was proposed by Robert Gold. These are constructed by modulo-2 addition of two m-sequences of the same length generated from Shift

Register Generator (SRG) with each other. These code sequences are added chip by chip through synchronous clocking. Thus, for a Gold sequence of length m = $2^l - 1$, one uses two linear feedback shift register (LFSR), each of length m = $2^l - 1$. Choosing LFSRs appropriately, Gold sequences give better cross correlation properties than maximum length LSFR sequences [14].

C. Kasami Sequence: Kasami sequence sets are one of the important types of binary sequence sets because of their very low cross-correlation. For sequence generation, a sequence A0 is formed from an m-sequence A by decimating A by $2^{n/2} + 1$. It can be verified that the resulting A_0 is an m-sequence with period $2^{n/2} - 1$. Now, by taking $N = 2^n - 1$ bits of sequences A and A_0, a new set of sequences is formed by adding, modulo-2, the bits from A and the bits from A_0 and all $2^{n/2} - 2$ cyclic shifts of the bits from A_0. By including A in the set, a set of 2n/2 binary sequences of length $N = 2^n - 1$ is obtained [15].

V. RNS SEQUENCE GENERATION PROCESS.

To generate RNS based PN sequence first we have to generate Moduli set for given Spreading factor β. Here we take Spending factors multiple of 8 to be compatible with binary arithmetic. There are two methods for selection of moduli one is Consecutive and other is expontial here we use consecutive moduli selection. Once we generate moduli set next step is to calculate range which is relatively large and computation is large for each member in range so we randomly select some members and generate RNS representation of that members. Then we convert those into Binary Sequences of eight bit for each residue of two digits. In this way we generate pn sequences based on RNS arithmetic.

Now Next task is to select those sequences which satisfy required cross correlation threshold for given application. For this we have to calculate CF for Each other for all generated sequences and only consider those sequences which satisfy our criteria and discard other put selected sequences into primal pool for online use during real operation.

VI. RESULTS AND DISCUSSION

We design RNS PN sequence generator based on above discussion in matlab and Generate Some RNS PN sequences for Different value of cross correlation (CF) and spending factor also compared with other existing Sequences like gold ML. For simulation We considered spreading factors β=8 and Generate RNS and Other Sequences and generate cross correlation matrix for RNS, ML sequence and Gold Sequence and Found that RNS based PN sequences Having Better Cross correlation as shown In Figures(Results) see fig 1-3

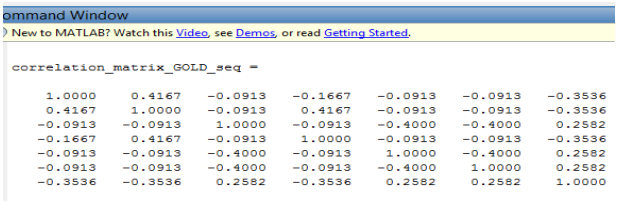

Figure 1: Correlation Matrix for GOLD sequence

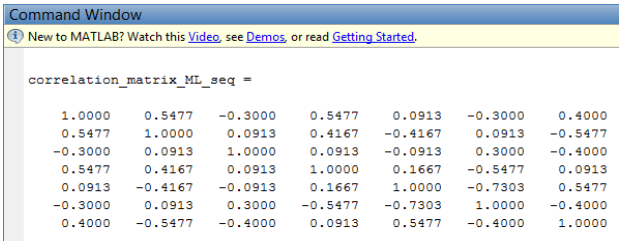

Figure 2: Correlation Matrix for ML sequence

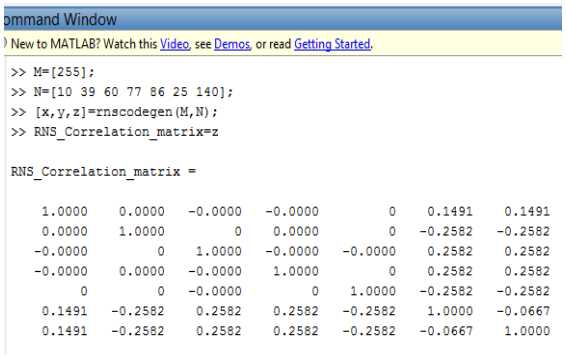

Figure 3: Correlation Matrix for RNS sequence

Our next phase is to check whether this Better cross correlation Properties will affect in System Performance to check this we use direct sequence CDMA and use RNS coed as Spreading Code in CDMA transmitter and at Receiver side same RNS code for Dispreading Data. Here we use AWGN channel as Transmission Channel Which adds a white nose into transmitted cdma signal. At receiver side we recovered transmitted signal and calculate Bit Error rate for Given Signal to noise ratio per bit (Eb/No). We Compare RNS sequence with GOLD and ML sequences for β=8 and for RNS sequence CF=0.25 which is shown in fig 4. Next we vary Cross correlation and Spreading Factor and plot BER curve of RNS sequences in CDMA AWGN channel which is shown in fig 4 and fig 5.

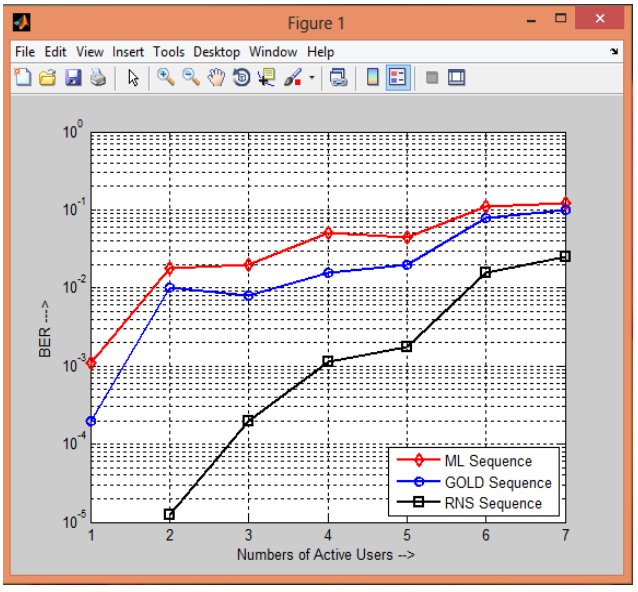

Figure 4: BER performance versus the Number of Active Users with spreading factor, β = 8 for Maximal Length Sequence, Gold Sequence and RNS based PN Sequence

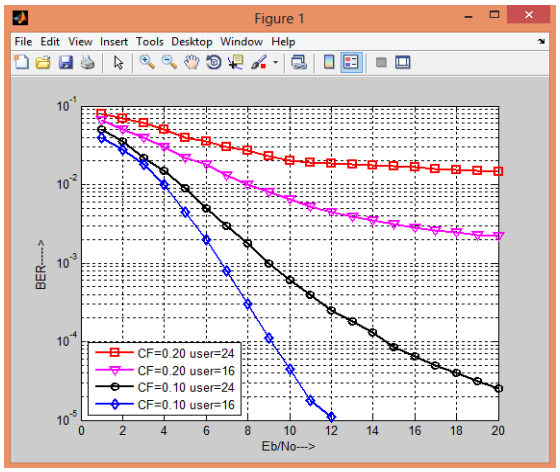

Figure 5: Performance Comparison of DS-CDMA system with cross correlation threshold, CF, 0.20 and 0.10 for β = 128

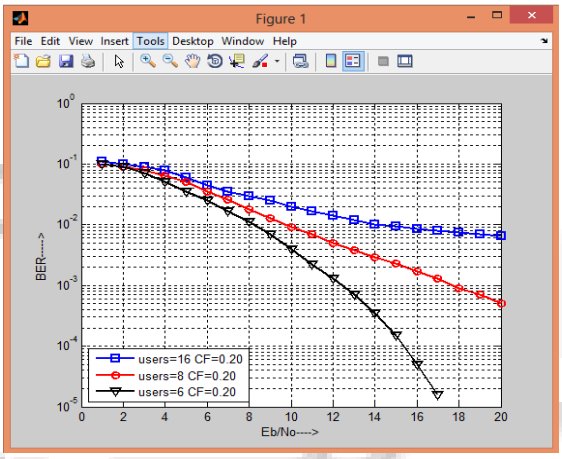

Figure 6: Performance Comparison of DS-CDMA system with cross correlation threshold, CF, 0.20 and β = 128 for varying active users

VII. CONCLUSION

RNS sequences having Better Cross correlation Properties than other existing sequences also it has very large dynamic range compared to other sequences so we can accommodate more users Using RNS sequences simulation results show RNS has less BER for given spreading factor. Simulation Results also States that as we go from CF=0.20 To CF=0.10 we get Better Performance so we can say that Cross correlation properties are reflected on System Performance

REFERENCES

[1] Juha Korhonen, Introduction to 3G Mobile Communications, 2nd ed., Artech House Mobile Communications Series, 2003.

[2] Hsiao-Hwa Chen, The Next Generation CDMA Technologies, 1st ed., John Wiley and Sons, 2007.

[3] L. Yang and L. Hanzo, 'Performance of residue number system based DS-CDMA over multipath fading channels using orthogonal sequences," European Transactions on Telecommunications, vol. 9, no. 6, pp. 525535, 1998

[4] Lie-Liang Yang; Hanzo, L., "Residue number system based multiple code DS-CDMA systems," Vehicular Technology Conference, 1999 IEEE 49th , vol.2, no., pp.1450-1454 vol.2, Jul 1999 doi: 10.1109/VETEC.1999.780587

[5] L. Yang and L. Hanzo, 'A residue number system based parallel com-munication scheme using orthogonal signaling .I. System outline," IEEE Transactions on Vehicular Technology, vol. 51, no. 6, pp. 1534 - 1546, 2002

[6] A. S. Madhukumar and F. Chin, 'Enhanced architecture for residue number system-based CDMA for high-rate data transmission," IEEE Transactions on Wireless Communications, vol. 3, no. 5, pp. : 1363 - 1368, 2004

[7] H. T. How, T. H. Liew, Ee-Lin Kuan, Lie-Liang Yang and Lajos Hanzo, 'A redundant residue number system coded burst-by-burst adaptive joint-detection based CDMA speech transceiver," IEEE Transactions on Vehic-ular Technology, vol. 55, no. 1, pp. 387 - 396, 2006

[8] M. I. Youssef,A. E. Emam and M. Abd Elghany, "Direct Sequence Spread Spectrum Technique with Residue Number System," International Journal of Electrical and Electronics, vol. 3:4, pp. 223-229, 2009

[9] Shuo Zhang, Youguang Zhang and Lie-Liang Yang, "Redundant Residue Number System Based Multicarrier DS-CDMA for Dynamic Multiple-Access in Cognitive Radios," IEEE 73rd Vehicular Technology Confer-ence (VTC Spring), pp. 1-5, 2011

[10] Amos Omundi and Benjamin Premkumar, "Residue Number System: Theory and Implementation," Imperial College Press, Vol.2, 2007.

[11] R. A. Scholtz, "The Evolution of Spread-Spectrum Multiple-Access Communications," Proceedings International Symposium on Spread Spectrum Techniques and Applications, Oulu, Finland, pp. 413, IEEE, 1994.

[12] S. Moshavi,"Multi-User Detection for DS-CDMA Communications," IEEE Communications Magazine, vol. 34, pp. 124136, October 1996.

[13] R. N. Mutagi, "Pseudo noise sequences for engineers," Electronics and Communication Engineering Journal, vol. 8, Issue. 2, pp. 79-87, 1996.

[14] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Transactions on Information Theory, vol.13, pp.619-621, 1967.

[15] Esmael H. Dinan, Bijan Jabbari, "Spreading Codes for DS-CDMA And Wideband Cellular Networks," IEEE Communications Magazine, September 1998.

[16] P.Maji and G.S.Rath, "A novel design approach for low pass finite impulse response filter based on residue number system," International Conference on Electronics Computer Technology (ICECT), IEEE, Vol.3, pp.74-78, 2011

[17] John G. Proakis, Dimitris G. Manolakis, Digital Signal Processing - Principles, Algorithms and Applications, 4th ed., Pearson Education Inc., 2007.