A PN Sequence Generator based on Residue Arithmetic for Multi-User DS-CDMA Applications

Chithra R, Pallab Maji, Sarat Kumar Patra and Girija Sankar Rath

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 generators 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 counter 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 are 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 lead 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, \( \beta \) 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, Rayleigh Fading channel and different Stationary Multipath Channels. The enhanced performance of RNS based PN sequence is established by comparing the bit error probability to that of other PN sequences in a multi-user environment.

The paper is organized as follows. Following this, Section II deals with introduction to Spread Spectrum techniques and standard PN sequence generation techniques. Section III deals with generation of RNS based PN Sequence. Simulation results with performance analysis for different channel environments is presented in Section IV. Finally, the paper concludes with Section V.

II. BACKGROUND MATERIAL

A. Spread Spectrum Communication

Shannon stated that the stationary Gaussian noise process which maximizes capacity is the one that spreads its available power uniformly across the given bandwidth [11]. Thus the capacity \( C \) for a given bandwidth \( B \) of a jamming channel is derived from the well known equation \( C = B \log_2 (1 + SNR) \) where SNR is the signal to noise ratio defined as

\[
SNR = \frac{P}{BN_0 + N_f}
\]

where \( P \) is the signal power, \( N_0 \) the thermal noise density and \( N_f \) the jamming power. The motivation is then to expand (spread) \( B \) in jamming situations until the total received noise power \( BN_0 \) dominates \( N_f \). The spreading leads to a reduction in required SNR which is very advantageous for communications.

There are three primarily different types of CDMA technologies: Direct Sequence (DS) CDMA, Frequency Hopping (FH) CDMA and Time Hopping (TH) CDMA. This paper deals only with DS-CDMA system, which is the simplest and the most popular CDMA scheme. Fig I shows the block diagram of the DS-CDMA system. The transmitted signal at time \( T \) is constructed by summing the spread sequence of each user. The signal is then passed through the channel. A CDMA receiver processes the received signal with either a bank of matched filters (MFs) or RAKEs. To recover the data, the received signal is multiplied by the required sequence, which is generated locally by the receiver. For a multipath scenario, the spreading codes \( C_i \) where \( i = 1 \) to \( U \) is replaced by the convolution between \( C_i \otimes H_{ch} \) where \( \otimes \) represents construction operation. The spreading sequences used for the system under consideration are generated based on residue arithmetic. The transmitter generates \( U \) number of RNS based PN sequences for \( U \) users.

B. Standard PN Sequences

1) Maximal Length Sequence: Maximal length binary sequences (m-sequences), also known as linear feedback shift register (LFSR), 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 \( N \)-stage shift register can generate a maximal length sequence of \( 2^N - 1 \) bits. Only certain outputs, or taps, can generate a maximal length sequence [13].

2) Gold Sequence: Gold Sequence was proposed by Robert Gold [14]. These are constructed by modulo-2 addition of two m-sequences of the same length 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 LFSR sequences.

3) 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 \( A' \) is formed from an m-sequence \( A \) by decimating \( A \) by \( 2^n + 1 \). It can be verified that the resulting \( A' \) is an m-sequence with period \( 2^n - 2 \). Now, by taking \( N = 2^n - 1 \) bits of sequences \( A \) and \( A' \), a new set of sequences is formed by adding, modulo-2, the bits from \( A \) and the bits from \( A' \) and all \( 2^n - 2 \) cyclic shifts of the bits from \( A' \). By including \( A \) in the set, a set of \( 2^{n/2} \) binary sequences of length \( N = 2^n - 1 \) is obtained [15].

III. RNS BASED PN SEQUENCE GENERATION

A. RNS Basics for PN Code Generation

Let \( x_i = |A|p_i \) denote remainder of primal, \( A \) when divided by \( p_i \), \( i = 1, 2, \ldots, n \). Given a moduli set, \( P = \{ p_1, p_2, p_3, \ldots, p_n \} \), then every integer \( A \) in a range

\[
R = \prod_{i=1}^{n} p_i
\]

will have unique representation \( \{ x_1, x_2, x_3, \ldots, x_n \} \) [16]. The rules for their one to one assignment is given by CRT. If b is...
the no. of bits of individual elements of set $P$, then spreading factor
\[ \beta = n \times b \] (3)

B. PN Sequence Generation based on Residue Arithmetic

RNS based PN sequence generation for multi-user scenario consists of an off-line process for the generation of Initial Primal Vector and finally the generation of the required PN sequence which is done on-line. The off-line process is summarized in Fig 2. The external inputs to these blocks include spread factor, $\beta$ and the cross-correlation threshold, $T$. Moduli set, $P$, for a given $\beta$ are selected either by consecutive method or exponential method [16]. Consecutive method of moduli selection is used here. Table I shows the generated moduli set and dynamic range, R for various spreading factors using Consecutive moduli selection method. For a given spread factor, the number of users that can be accommodated is huge in comparison to other spreading codes. A primal, $J_1$ is randomly selected from the range, R in eq. 2. The corresponding residue set, $R_s(J_1)$
\[ R_s(J_1) = \{ |J_1|_{p_1}, |J_1|_{p_2}, \ldots, |J_1|_{p_n} \} \] (4)
is the output of Decimal to Residue Arithmetic Converter. The generated residue numbers are concatenated and converted into 8 bit (since $b = 8$ in eq. 3) binary sequence of 1 and 0. This sequence is passed through the NRZ encoder to get the sequence $C_1$ corresponding to primal $J_1$. This procedure is repeated for every primals in range, R. The generated sequences are tested for correlation amongst themselves such that
- correlation between $C_i$ and $C_j$, $i \neq j$ has to be unity.
- correlation between $C_i$ and $C_j$, $i = j$ has to be preferably less than a threshold $T$. This threshold can vary for different applications based on the channel properties and error tolerance.

<table>
<thead>
<tr>
<th>$\beta$</th>
<th>MODULI SET $P = {p_1, p_2, \ldots, p_m}$</th>
<th>RANGE, R</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>[255]</td>
<td>255</td>
</tr>
<tr>
<td>16</td>
<td>64770</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>[255 254 253 251]</td>
<td>4113089310</td>
</tr>
<tr>
<td>64</td>
<td>[255 254 253 251 247 241 239 233]</td>
<td>$\geq 10^{19}$</td>
</tr>
<tr>
<td>128</td>
<td>[255 254 253 251 247 241 239 233]</td>
<td>$\geq 10^{40}$</td>
</tr>
</tbody>
</table>

IV. RESULTS AND DISCUSSION

For the analysis of the cross-correlation properties of RNS based PN sequence in comparison with other standard PN sequences, spreading codes have been generated with a spreading factor, $\beta = 8$, and moduli set $P = [255]$. The primal vector, $J = [10 39 60 77 86 25 140]$, is generated by varying the threshold value from 0 to 0.25. The correlation matrix of RNS based PN sequence, Gold sequence and Maximal Length sequence are tabulated in Table II, Table III and Table IV respectively. The data shows that the maximum cross correlation between any two sequences is limited to 0.25 for RNS based PN sequence whereas it come up to 0.41 and 0.73 for gold sequences and maximal length sequences, while the auto correlation reaches to 1.

In order to validate the improved performance with decrease in cross correlation factor, the generated sequence is used in DS-CDMA system. The difference in the cross correlation factor is directly reflected in the system performance, which is shown in Fig 4.

Detailed study of the behaviour of RNS based PN Sequence under different channel environment and with different loading
TABLE III
CORRELATION MATRIX FOR GOLD SEQUENCE, $\beta = 8$

<table>
<thead>
<tr>
<th></th>
<th>PN1</th>
<th>PN2</th>
<th>PN3</th>
<th>PN4</th>
<th>PN5</th>
<th>PN6</th>
<th>PN7</th>
</tr>
</thead>
<tbody>
<tr>
<td>PN1</td>
<td>1</td>
<td>0.41</td>
<td>-0.09</td>
<td>-0.16</td>
<td>-0.09</td>
<td>-0.09</td>
<td>-0.35</td>
</tr>
<tr>
<td>PN2</td>
<td>0.41</td>
<td>1</td>
<td>-0.09</td>
<td>0.41</td>
<td>-0.09</td>
<td>-0.09</td>
<td>-0.35</td>
</tr>
<tr>
<td>PN3</td>
<td>-0.09</td>
<td>-0.09</td>
<td>1</td>
<td>-0.09</td>
<td>-0.40</td>
<td>-0.40</td>
<td>0.25</td>
</tr>
<tr>
<td>PN4</td>
<td>-0.16</td>
<td>0.41</td>
<td>-0.09</td>
<td>1</td>
<td>-0.09</td>
<td>-0.09</td>
<td>-0.35</td>
</tr>
<tr>
<td>PN5</td>
<td>-0.09</td>
<td>-0.09</td>
<td>-0.40</td>
<td>-0.09</td>
<td>1</td>
<td>-0.40</td>
<td>0.25</td>
</tr>
<tr>
<td>PN6</td>
<td>-0.09</td>
<td>-0.09</td>
<td>-0.40</td>
<td>-0.09</td>
<td>-0.40</td>
<td>1</td>
<td>0.25</td>
</tr>
<tr>
<td>PN7</td>
<td>-0.35</td>
<td>-0.35</td>
<td>0.25</td>
<td>-0.35</td>
<td>0.25</td>
<td>0.25</td>
<td>1</td>
</tr>
</tbody>
</table>

TABLE IV
CORRELATION MATRIX FOR MAXIMAL LENGTH SEQUENCE, $\beta = 8$

<table>
<thead>
<tr>
<th></th>
<th>PN1</th>
<th>PN2</th>
<th>PN3</th>
<th>PN4</th>
<th>PN5</th>
<th>PN6</th>
<th>PN7</th>
</tr>
</thead>
<tbody>
<tr>
<td>PN1</td>
<td>1</td>
<td>0.54</td>
<td>-0.30</td>
<td>0.54</td>
<td>0.09</td>
<td>-0.30</td>
<td>0.40</td>
</tr>
<tr>
<td>PN2</td>
<td>0.54</td>
<td>1</td>
<td>0.09</td>
<td>0.41</td>
<td>-0.41</td>
<td>0.09</td>
<td>-0.54</td>
</tr>
<tr>
<td>PN3</td>
<td>-0.30</td>
<td>0.09</td>
<td>1</td>
<td>0.09</td>
<td>-0.09</td>
<td>0.30</td>
<td>-0.40</td>
</tr>
<tr>
<td>PN4</td>
<td>0.54</td>
<td>0.41</td>
<td>-0.09</td>
<td>1</td>
<td>0.16</td>
<td>-0.54</td>
<td>0.09</td>
</tr>
<tr>
<td>PN5</td>
<td>0.09</td>
<td>-0.41</td>
<td>-0.09</td>
<td>0.16</td>
<td>1</td>
<td>-0.73</td>
<td>0.54</td>
</tr>
<tr>
<td>PN6</td>
<td>-0.30</td>
<td>0.09</td>
<td>0.30</td>
<td>-0.54</td>
<td>-0.73</td>
<td>1</td>
<td>0.40</td>
</tr>
<tr>
<td>PN7</td>
<td>0.40</td>
<td>-0.54</td>
<td>-0.40</td>
<td>0.09</td>
<td>0.54</td>
<td>-0.40</td>
<td>1</td>
</tr>
</tbody>
</table>

scenarios by varying cross correlation factor is done for $\beta = 64$ and $\beta = 128$; because a DS-CDMA system using a higher spreading factor is capable of supporting a higher number of active users than that using a lower spreading factor, while maintaining the target performance. Bit error rate (BER) was considered as the performance index throughout. Monte Carlo simulation were conducted to estimate the BER performance.

A. AWGN Channel

The performance of DS-CDMA system using RNS based PN sequence over a AWGN channel for $\beta = 64$ in Fig 5 and $\beta = 128$ in Fig 6 is shown. The $E_b/N_0$ characteristics were varied from 1 to 20 dB for different loading scenarios. Here the cross correlation threshold value is chosen to be 0.20. Additional tests were also conducted by varying number of active users in the system for $E_b/N_0$ of 5 dB and 20 dB shown in Fig 7. From the results, for a given target BER for example, $10^{-3}$ and for a given $E_b/N_0$ of 12 dB, 6 users can be accommodated with $\beta = 64$ while it is doubled for $\beta = 128$.

1) Role of cross-correlation threshold in system performance: PN sequence generation based on Residue Arithmetic also accord to the tolerability and tractability of correlation factor. Fig 8 illustrates that the correlation properties can be varied as per the system requirements. For applications which require better performance, the cross-correlation threshold should be reduced further so as to mitigate the multiple access interference. For 12.5 percent loading of a system with spread factor, $\beta = 128$ and 12 users being active in the system, the bit error rate went down to $10^{-5}$ for cross-correlation threshold of 0.10 whereas it is only $4 \times 10^{-3}$ for 0.20.

2) Performance Comparison with other PN sequences: Fig 9 compares RNS based PN sequence with the most widely used quasi-orthogonal CDMA codes, which includes Gold codes, Kasami codes and Maximal Length sequence. The superior performance of residue arithmetic code even for a cross correlation threshold of 0.20 shows that it has better resilience to inter-user interference than other standard PN sequences. Simulations are done for $\beta = 64$ and 5 users are active in the DS-CDMA system.
B. Rayleigh Fading Channel

Fig 10 shows BER versus signal-to-noise ratio for a DS-CDMA system in Rayleigh Fading channel, $\beta = 128$. The analysis has been carried out under flat Rayleigh fading channels and multiple-access interference. Since the spread spectrum processing gain makes uncorrelated noise negligible after despreading, equalization is not considered. So for the required number of users in the system, the performance degradation due to fading is compensated by reducing cross correlation threshold, CF, from 0.20 to 0.10.

C. Stationary Multipath Channel

For the next phase, the channel which corrupts the transmitted signal with both MAI and MI was taken into account. Here the consideration was for different types of AWGN multipath channels with transfer functions $1 + 0.5z^{-1} + 0.2z^{-2}$, $0.5 + z^{-1}$ and $0.3482 + 0.8704z^{-1} + 0.3482z^{-2}$.

- $1 + 0.5z^{-1} + 0.2z^{-2}$, Minimum Phase Channel - with zeros located inside the unit circle.
- $0.5 + z^{-1}$, Maximum Phase Channel - with a zero located outside the unit circle.
- $0.3482 + 0.8704z^{-1} + 0.3482z^{-2}$, Mixed/Non-minimum Phase Channel - with some of its zeros inside the unit circle and the remaining zeros outside the unit circle.

The simulations were conducted for different levels of $E_b/N_0$ and varying number of users active in the cell. A minimum phase system in Fig 11 is affected only with MI. On the other hand, maximum and mixed phase channel undergoes a net phase change [17] along with MI. As a result of this, the performance of Fig 12 and Fig 13 degrades further. From the results, it is clear that sequences having cross-correlation threshold above 0.20 does not have any significance. Here the cross correlation threshold has to be 0.10 and below.
The proposed sequence offers provision to vary correlation threshold based on the channel properties and error tolerance unlike any existing techniques. It also inherits high dynamic key range such that it yields a PN sequence which has pragmatically a nether correlation. DS-CDMA performance in all of MAI-AWGN, Rayleigh flat fading and different stationary multipath channels has been evaluated. It offers MAI-resistant operation in both synchronous and asynchronous MAI-AWGN channels, reducing co-channel interference and increasing capacity in a mobile cellular system. The joint effect of ideal auto-correlation function and good cross correlation function makes RNS based PN sequence superior to all other standard PN sequences like Gold codes, Kasami codes and Maximal Length sequence.

V. Conclusion

The proposed sequence offers provision to vary correlation threshold based on the channel properties and error tolerance unlike any existing techniques. It also inherits high dynamic key range such that it yields a PN sequence which has pragmatically a nether correlation. DS-CDMA performance in all of MAI-AWGN, Rayleigh flat fading and different stationary multipath channels has been evaluated. It offers MAI-resistant operation in both synchronous and asynchronous MAI-AWGN channels, reducing co-channel interference and increasing capacity in a mobile cellular system. The joint effect of ideal auto-correlation function and good cross correlation function makes RNS based PN sequence superior to all other standard PN sequences like Gold codes, Kasami codes and Maximal Length sequence.

References