2003

Generalized d-sequences and their applications to CDMA systems

Radhika Vaddiraja
Louisiana State University and Agricultural and Mechanical College

GENERALIZED d-SEQUENCES AND THEIR APPLICATION TO CDMA SYSTEMS

A Thesis

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The Department of Electrical and Computer Engineering

by
Radhika Vaddiraja
B.E., Osmania University, Hyderabad, India, 2000
August, 2003

Acknowledgements

I take this opportunity to express my deepest gratitude to Dr. Subhash Kak, my advisor, for all the support and guidance he has given me throughout my graduate study and thesis work. His suggestions and constant encouragement helped me a lot.

I would also like to thank Dr. Suresh Rai for his guidance in all the courses I took with him. I would like to thank him and Dr.Hsiao-Chun Wu for being a part of my committee.

I am grateful to my parents, Mr. and Mrs. Gopalkrishna Rao, my brother and my sister, for the tremendous amount of inspiration and moral support they have given me from my childhood without which I would not have reached this position. I would like to express thanks to my husband, Sridhar, for the love and support he has given me at times I needed the most.

I also thank Sameer for his help in my work and all my other friends at LSU who helped me indirectly in my thesis.

Table of Contents

List of Tables

Table

List of Figures

Figure

Figure

Abstract

Code Division Multiple Access (CDMA), a form of spread spectrum communications is used widely in cellular telephony. CDMA systems employ Walsh-Hadamard orthogonal codes, jointly with Pseudo-Noise (PN) sequences, Gold sequences and Kasami sequences to achieve spreading. This thesis investigates properties of generalized d-sequences and their applications as spreading sequences in CDMA systems. The correlation properties of these sequences are studied. The autocorrelation function of these sequences is not exactly two-valued but the cross correlation values are zero for certain class of these sequences. The zero cross correlation property can be useful in solving the near-far problem in CDMA communication systems, thus obviating the need for power control. The performance of these sequences is analyzed and their application to CDMA systems is investigated.

Chapter 1

Introduction

At the beginning of 2001, more than one out of 10 people in the world had a mobile telephone. The end-user equipment size, weight, and costs have dropped over 20% per year over the past 15 years. This incredible growth in the industry is due to the development of wireless communication technologies [8].

The first generation wireless communication system was the analog advanced mobile phone system (AMPS), developed primarily by AT & T. This system used a 30 kHz channel spacing while narrowband AMPS (N-AMPS), which was developed by Motorola, worked within a 10 kHz channel spacing thus increasing the AMPS capacity. The frequency division multiple access (FDMA) systems divide a wide frequency band into smaller frequency bands that are assigned to specific users allowing different users to communicate at the same time.

These first generation systems had capacity limitations since each spectral channel could be allocated to only one user. Because of the capacity limitations of the FDMA based analog cellular systems, the first digital cellular systems were based on time division multiple access (TDMA). TDMA systems divide their signals into shorter time slots thus allowing several mobile telephones to communicate on a single radio carrier frequency. The digital AMPS (D-AMPS) was developed in the late 1980s which was followed by the first Groupe Special Mobile (GSM) deployments. Today, it is estimated that there are over 800 million GSM subscribers across the 190 countries of the

world. These TDMA systems come under the second generation cellular systems. Figure 1.1 shows the evolution of wireless technologies in various stages [9].

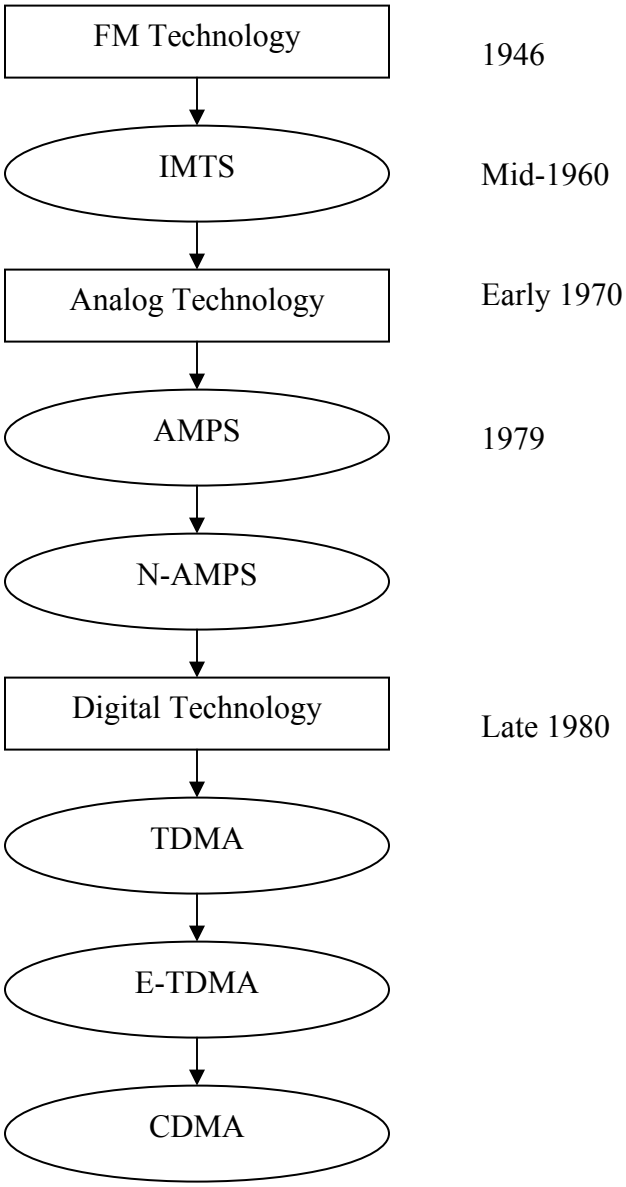

Figure 1.1: Evolution of wireless technologies

Spread spectrum technology, which was initially used in military applications, is another approach to achieve multiple access. In it, a narrowband signal is spread over a wide frequency band for transmission using code division multiple access (CDMA); it is

also called spread spectrum multiple access (SSMA). CDMA was pioneered and commercially developed by QUALCOMM in 1995. In it, multiple users can share the radio channel at the same time. The frequency reuse limitations in FDMA and TDMA are less in CDMA and so CDMA is an attractive alternative to GSM.

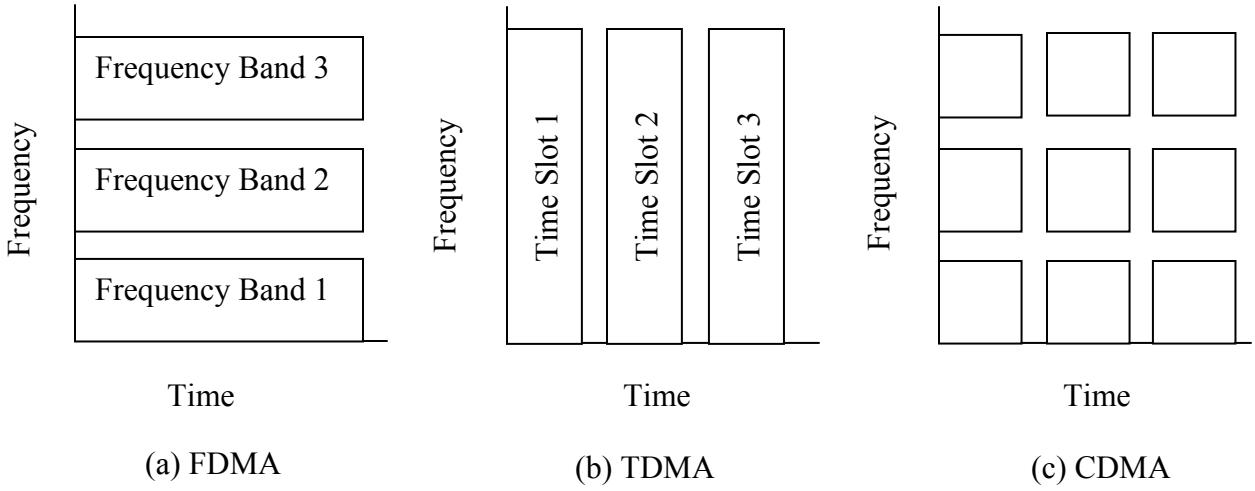

Figure 1.2: Various multiple access technologies

The international telecommunications union (ITU) undertook the international mobile telephony-2000 (IMT-2000) project and developed the third generation systems. The primary third generation technologies which were approved by ITU in 1998 were [1]:

- Wideband CDMA (W-CDMA), developed by the European telecommunication standardization institute (ETSI).
- Cdma2000, developed by the telecommunications industry association (TIA).
- EDGE (Enhanced Data Rates for GSM Evolution) which was co-sponsored by ETSI and the TIA.

The next section gives a background on spread spectrum systems and the sequences used in CDMA systems.

1.1 Background

Spread spectrum system spreads the transmitted signal over a wide frequency band, much wider, than the minimum bandwidth required to transmit the information being sent. For example, a base band signal with a bandwidth of only few kilohertz is distributed by a spread spectrum system over a bandwidth of many megahertz which is done by modulating with the information to be sent with the wideband encoding signal. Figure 1.3 shows that spreading is achieved when multiplying the signal with the spreading sequence.

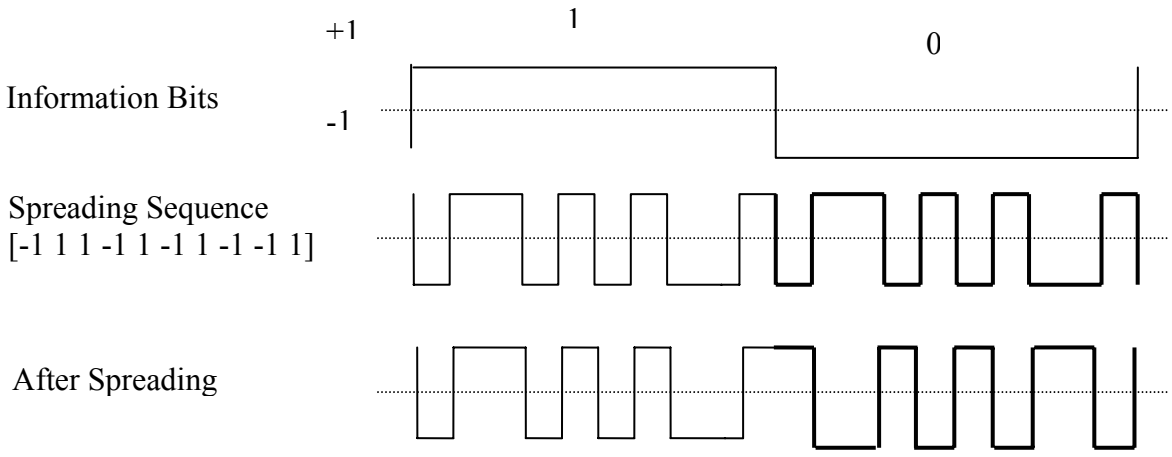

Figure 1.3: Spreading waveforms

Some of the properties of spread spectrum systems are [2]:

- Low density power spectra.
- Code division multiplexing which is possible for multiple access
- Selective addressing capability

- Interference rejection

The important forms of spread spectrum modulation are frequency hopping, direct sequence, time hopping, chirping and various hybrid combinations of the above forms though only the first two are the most important ones.

Frequency hopping spread spectrum, which is also called multiple frequency, code selected, frequency-shift keying, is one in which a signal is spread by causing it to hop rapidly from one frequency to another according to a predetermined pseudorandom sequence. A frequency hopper occupies only the bandwidth required by its information content instead of spreading the signal over a wideband channel. There are two kinds of frequency hopping systems: fast hopping and slow hopping systems. Fast hopping systems use multiple hops for each bit of end user data whereas slow hopping systems send more than one bit of end user information per hop. The slow hopping systems are less complex and therefore less expensive to build [10].

Direct sequence spread spectrum systems, which are the most widely used systems, are those in which the signal is spread over a continuous range of frequencies. Code division multiple access (CDMA) is a form of direct sequence spread spectrum which allows multiple simultaneous users on the same wideband channel. The advantages of CDMA are good signal quality, excellent system reliability, and soft hand off capability, high information security, high transmission power efficiency and high frequency reuse efficiency.

1.2 Sequences Used in CDMA Systems

The sequences which are used in CDMA systems are maximal length sequences (m-sequences) or shift register sequences, gold sequences, kasami sequences and pseudo

noise sequences (PN sequences). The sequences which are used in CDMA should have the following properties:

- There should be a balance in the number of ones and zeroes.
- The autocorrelation must be a sharp two-valued function
- The cross correlation must be as low as possible.

M-sequences:

Maximal length sequences are generated by shift register and therefore they are also called shift register sequences. These are the longest codes that can be generated by a given shift register or a delay element of given length. Figure 1.4 shows an L-stage shift register with linear feedback [12].

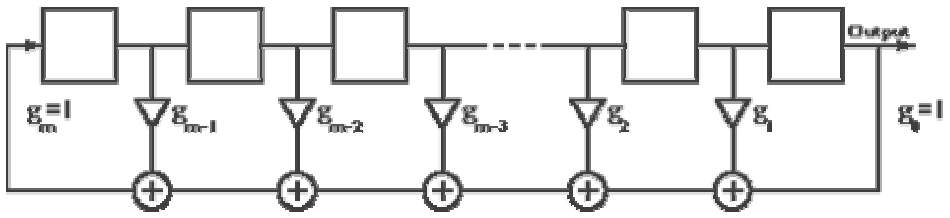

Figure 1.4: L-stage shift register with feedback

The maximum possible period of the above L-stage shift register is $2^L - 1$. Some of the properties of these m-sequences are [2]:

- The number of ones and zeros are equal in a sequence. For example, a 1023-chip code, the number of ones is 512 and the number of zeros is 511. This property is important in communications since the DC component in the code is neglected. If the number of stages in the generator is L, then the number of ones is $2^L - 1$ and the number of zeros is one less than the number of ones and is $2^{L-1} - 1$.

- The statistical distribution of ones and zeros is well defined and always the same.
- The autocorrelation of a periodic m-sequence is two valued. Autocorrelation is a measure of the number of agreements minus the number of disagreements for the overall length of the two codes being compared.
- A modulo-2 addition of a maximal linear code with a phase shifted replica results in another replica but with a different phase shift from the original. When two m-sequences of different length, $2^m - 1$ and $2^n - 1$ are linearly (modulo-2) added, it results in a composite sequence of length $(2^m - 1)(2^n - 1)$. This composite sequence is not maximal. These sequences have applications in Global Positioning Systems (GPS).

Gold Sequences

The cross correlation properties are as important in communication systems as autocorrelation properties. Cross correlation is a measure of agreement between the two different codes. The periodic cross correlation between any pair of m-sequences is very high. Such high values of cross correlation are undesirable in CDMA communications. Gold [13] developed new sequences with better cross correlation properties called Gold sequences.

Gold sequences are defined using a pair of preferred sequences; say $\{a_k\}$ and $\{b_k\}$. A modulo-2 addition of $\{a_k\}$ with cyclic shifted versions of $\{b_k\}$ is performed. The result is a new period sequences with the period $N = 2^n - 1$. By including the original sequences $\{a_k\}$ and $\{b_k\}$, the set of sequences $N + 2$ are obtained. The $N + 2$ sequences constructed in this manner are called Gold sequences. The cross correlation of gold sequences is a three-valued function with three values $\{-1, t(n), t(n) - 2\}$, where [14]

$$t(n) = 1 + 2^{(n+1)/2}, \text{ for odd } n$$

$$1 + 2^{(n+2)/2}, \text{ for even } n$$

where n is the number of stages of the shift register generator.

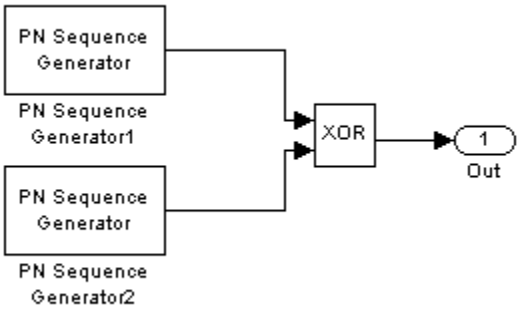

Figure 1.5: Gold sequence generator

A Gold sequence generator uses two PN sequence generators (which use a shift register to generate sequences) blocks to generate the preferred pair of sequences [14]. An XOR operation of these sequences is done to produce the output sequence. So, gold sequences are a family of codes with good cross correlation properties. The period of these sequences is N, which is same as the period of the m-sequences.

Kasami Sequences

There are two classes of Kasami Sequences: the small set and the large set. The number of sequences for the small set is $2^{n/2}$, and for the large set is $2^{n/2}(2^n + 1)$, where n is the number of stages of the shift register. The procedure for generating Kasami sequences is similar to that used for generating Gold sequences. Let $\{a_k\}$ be a m-sequence. A binary sequence $\{b_k\}$ is derived by decimating $\{a_k\}$ by $2^{n/2} + 1$. The resulting sequence $\{b_k\}$ is periodic with the period $2^{n/2} - 1$. These $N = 2^{n/2} - 1$

consecutive bits of the sequences $\{a_k\}$ and $\{b_k\}$ are taken to form a new set of sequences by adding, in modulo-2, the bits of $\{a_k\}$ to the bits of $\{b_k\}$ and its $2^{n/2}-2$ cyclic shifts. The resulting sequences obtained are called small set of Kasami sequences [15].

The maximum cross correlation value for any pair of Kasami sequences is $2^{n/2}+1$. These small set of Kasami sequences contains a relatively smaller number of sequences. When the number of users in communications is large, it is difficult to apply these small set of sequences. So, a new method to produce a large number of short-period sequences with good cross correlation properties is devised. This method combines three sequences instead of two. The obtained sequences are called large set of Kasami sequences. The maximum correlation value of the large set of Kasami sequences is same as that of the Gold sequences.

Pseudo Noise Sequences

Pseudo noise sequences are binary-valued, noise like sequences. They are generated by feedback shift registers with feedback. They are similar to a sequence of coin tossing where +1 represents a head and -1 represents a tail. The following characteristics are associated with randomness [16]:

R-1. In every period, the number of +1's is nearly equal to the number of -1's.

R-2. In every period, half the runs have length one, one-fourth have length two, one-eighth have length three as long as the number of runs exceeds 1.

R-3. The autocorrelation function is two valued.

Any sequence with the above properties is called a pseudo noise sequence.

Example: The sequence 1 1 1 -1 1 -1 -1 has length p = 7. There are four +1's and three -1's which is adequate to satisfy *R-1*. Out of the four runs, half have length one and one-

fourth have length two. So, *R-2* is satisfied too. The autocorrelation function is 1 in phase and -1/7 out of phase which satisfies the property *R-3* too.

Fig 1.7 shows the generation of a PN sequence by using a 3 stage shift register with feedback. The length of the sequence is $2^3 - 1$ which is 7.

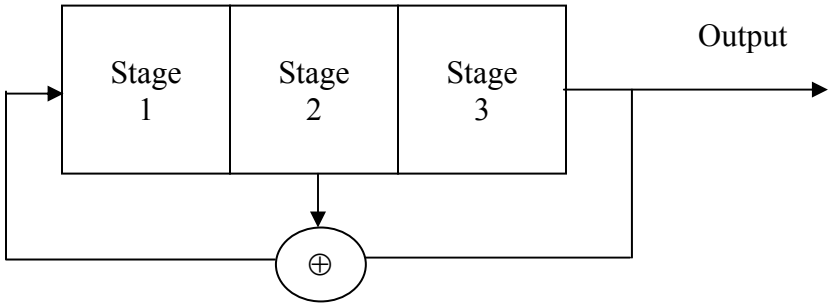

Figure 1.6: Generation of a 7-bit PN sequence

The contents of the shift register shift to the right and after each such shift, the contents of the second and third stages are used to produce an input to the first stage through an XOR operation. The contents of the shift register are shown in Table 1.1.

Table 1.1: Contents of a 3-Stage Shift Register

1	1	1
0	1	1
0	0	1
1	0	0
0	1	0
1	0	1
1	1	0
1	1	1

The initial contents of the shift register are 1 1 1. The contents are again 1 1 1 after $2^3 - 1 = 7$ more shifts, which is also the length of the output sequence at the third stage. Every possible state except 0 0 0 will occur.

1.3 Formulation of the Problem

The pervious section gave an insight to the different spreading sequences used in CDMA systems. K. Yang, Y. Kim, and P. Kumar proposed a notion of quasi orthogonal sequences (QoS) for CDMA systems which increased the number of channels [7]. They increase the system capacity and also minimize the interference. These QOS sequences are constructed from Kasami sequences and Gold sequences as well as from the binary Kerdock code. The method used to modulate the signal is binary phase shift keying.

Chen proposed a new multicarrier CDMA architecture based on orthogonal complementary codes [8]. This new architecture has several advantages when compared to the conventional CDMA systems which are used in 2G and 3G standards. First, the spreading efficiency (defined as the amount of information bit(s) conveyed by each chip) is close to one whereas the spreading efficiency of conventional CDMA systems is equal to $1/N$, where N is the length of the spreading code. Secondly, the proposed CDMA system has high bandwidth efficiency due to the use of unique spreading modulation scheme and orthogonal carriers.

CDMA systems use Walsh codes jointly with PN sequences to maintain orthogonality. Walsh codes are defined using a Hadamard matrix of order N. There are 64 possible Walsh codes, each 64 bits long. The autocorrelation and cross correlation of traditional CDMA systems are not that ideal because of which there is a deviation of the

spreading sequences from perfect orthogonality. This deviation causes multiple access interference (MAI) in CDMA systems.

Another critical problem in these systems is near-far problem. This problem occurs when the received signals from the mobile units do not have equal power at the base station and when the cross-correlation values are large around the origin. If one transmitter is relatively closer to the receiver than all others, its signal may swamp out users further away from the receiver. To overcome the near-far problem, power control is used at the base station. Power control is needed for the forward link (base station to mobile units) as well as for the reverse link (mobile units to the base station) to regulate the performance of CDMA systems. The key criterion in evaluating the performance of a communication system is its system capacity, which is defined as the largest possible number of users that can be reliably served by the system [19]. If there is no proper power control, then the transmitted power will be more for users which are away from the base station. This, in turn, increases the multiple access interference. Therefore, correlation properties are important in the performance of CDMA systems. Recently, it was proposed that a large area synchronous (LAS) CDMA system has ideal autocorrelation function and zero cross correlation zone in their cross correlation functions. The system capacity of these LAS CDMA systems can be much higher than traditional CDMA systems and therefore could be used in fourth-generation mobile radio [24].

In this thesis, we present generalized d-sequences which could be used as spreading sequences. The cross correlation properties are interesting for certain class of

these sequences. This property could be used in attaining orthogonality between sequences and thus the near-far problem could be solved in a way.

1.4 Organization of the Thesis

The remaining thesis is organized as follows. Chapter 2 explains the properties of decimal sequences and the application of these sequences to encryption and error correction. Chapter 3 introduces the proposed generalized d-sequences and gives the autocorrelation and cross correlation graphs of these sequences. Chapter 4 analyzes the performance of the generalized d-sequences and proposes a system which is similar to the IS-95 CDMA system. Chapter 5 concludes the thesis and suggests future scope for study.

Chapter 2

Decimal Sequences – Properties and Applications

In this chapter, we present the properties of Decimal sequences (d-sequences) and discuss some application of these sequences to encryption and error correction coding [4].

2.1 Introduction to Decimal Sequences

Decimal sequences are obtained when a number is represented in a decimal form in a base r and they may terminate, repeat or be aperiodic. For a certain class of decimal sequences of $1/q$, q prime, the digits spaced half a period apart add up to $r-1$, where r is the base in which the sequence is expressed. These sequences are periodic and their randomness properties are checked only in one period. Decimal sequences are known to have good cross correlation properties and they can be used in applications involving pseudorandom sequences. The following section describes the properties of decimal sequences.

2.2 Properties of Decimal Sequences

Frequency Characteristics

The following theorems are certain well known results from number theory regarding decimal sequences [6].

Theorem 1: Any positive number x may be expressed as a decimal in the scale of r

$$A_1 A_2 \cdots A_{s+1} . a_1 a_2 \cdots$$

Where $0 \le A_i < r, 0 \le a_i < r$, not all A and a are zero, and an infinity of the a_i are less than $(r-1)$. There is a one to one correspondence between the numbers and the decimals, and

$$x = A_1 r^s + A_2 r^{s-1} + \cdots + A_{s+1} + a_1 / r + a_2 / r^2$$

For example, ¼ can be represented as 0.25 in the scale of 10 and .01 in the scale of 2. Also, 1/8 can be represented as 0.125 in the scale of 10 and .001 in the scale of 2. The decimal sequences of rational and irrational numbers may be possibly used to generate pseudorandom sequences and this is suggested by the following properties of decimals of real numbers.

Theorem 2: Almost all decimals, in any scale, contain all possible digits which mean that the property applies everywhere except to a set of measure zero.

Theorem 3: Almost all decimals, in any base, contain all possible sequences of any number of digits.

Theorems 2 and 3 guarantee that a decimal sequence missing any digit is exceptional; to know the behavior of the digits for any particular decimal sequence, the following terms are introduced to characterize the frequency behavior of digits and their combinations.

Definition: A number x is said to be simply normal in base r if in the decimal of x each of the r possible digits occur with a frequency $1/r$, i.e.,

$$\lim_{n \to \infty} n_b / n \to 1/r$$

for all b, where the digit b occurs n_b times in the first n places.

Definition: A number x is said to be normal in the scale of r if all the numbers $x, rx, r^2x, \cdots$ are simply normal in all of bases $r, r^2, r^3, \cdots$. If x is expressed as a decimal in the scale of r, every combination $b_1, b_2, \cdots b_k$ of digits occurs with the proper frequencies. Thus the property that a number is normal in the scale of r may be repeated by saying that all the digits $0-(r-1)$ occur with equal likelihood and each digit of the sequence is independent of every other digit.

Theorem 4: Almost all numbers are normal in any base.

It may be noted, however, that while finite periodic decimal sequences may be simply normal in a given scale, they will not be simply normal in all scales. For example, consider

$$x = \cdot 0123456789$$

which is simply normal in the scale of 10. In the scale of 10^{10} the same number is $x = \cdot b$ where b is 123456789, which is not simply normal, 10^{10}-1 digits being missing. So, a normal number cannot be rational. Theorem 4 guarantees the existence of an uncountably infinity of irrational numbers, whose decimal representation would perfectly exhibit all randomness properties. Generating a periodic sequence from its rational number representation is computationally less complex than generating it from an irrational number.

Theorem 5: The decimal for a rational number p/q between 0 and 1 is terminating or recurring, and any terminating or recurring decimal in the scale of 10 is equal to a rational number. If $(p,q) = 1, q = 2^{\alpha}5^{\beta}$, and $\max(\alpha, \beta) = \mu$, then the decimal terminates after μ digits. If $(p,q) = 1, q = 2^{\alpha}5^{\beta}Q$, where $Q > 1, (Q,10) = 1$, and ν is the order of $10 (\mathrm{mod}\, q)$, then the decimal contains μ non-recurring and ν recurring digits.

Example of recurring decimals is 1/3 which is equivalent to 0.3333…., also 1/7 which is equal to 0.14285714285714. These are examples of pure recurring decimals in which the period reaches back to the beginning. On the other hand, 1/6 = 0.1666 …. is an example of mixed recurring decimal in which the period is preceded by one non- recurrent digit.

Theorem 6: Suppose $0 < x < 1, x = p/q, (p,q) = 1$. If $q = s^{\alpha} t^{\beta} \ldots u^{\gamma}$, where $s, t \ldots u$ are the prime factors of r, and $\mu = \max(\alpha, \beta, \cdots \gamma)$, then the decimal for x terminates at the μ th digit. If q is prime to r and ν is the order of $r (\mathrm{mod}\, q)$, then the decimal is pure recurring and has a period of ν digits. If $q = s^{\alpha} t^{\beta} \ldots u^{\gamma} Q$, (Q>1), Q is prime to r, and ν is the order of $r (\mathrm{mod}\, Q)$, then the decimal is mixed recurring, and has μ non-recurring and ν recurring digits.

Remark 1: It is clear that if $(q,r) = 1, (p,q) = 1$, the maximum length of the decimal sequence for p/q will be $\phi(q)$, the Euler's ϕ-function of q. This follows from Euler's theorem that if (r, q) = 1, then $r^{\phi(q)} \equiv 1 (\mathrm{mod}\, q)$. The period would be $\phi(q)$ or a divisor of $\phi(q)$ depending on what the order of r (mod q) is.

Remark 2: For every prime q, there exist $\phi(q-1)$ primitive roots incongruent modulo q. This is one of the results of Gauss. The evaluation of primitive roots is done by trial and error.

Definition: If q is a prime, and r is a primitive root of q, then the decimal sequence for $1/q$ has a period of $q-1$ in the scale of r. Such a sequence is called a maximum-length decimal sequence in the scale of r. Maximum length sequences are often represented by the string of its first $q-1$ digits without showing the decimal or as $(1/q)$. For each prime q, there would exist $\phi(q-1)$ maximum length sequences in different scales.

Theorem 7: A maximum length decimal sequence when multiplied by $p, p < q$, is a cyclic permutation of itself.

Proof: The remainders $1,2,\cdots q-1$ obtained during the division of $1/q$ have a one-way correspondence with the coefficients $0,1,\cdots r-1$. Since p/q starts off with a remainder $rp(\text{mod}\, q)$ instead of $r(\text{mod}\, q)$, there would be a corresponding shift of the decimal sequence.

Example: Consider x = {1/7}. The decimal sequence for x in the scale of 10 is maximum length sequence because $10^2 \equiv 1(\text{mod}\, 7)$ but $10^6 \equiv 1(\text{mod}\, 7)$. The decimal sequence is 1 4 2 8 5 7, which corresponds to the remainder sequence 3 2 6 4 5 1. The remainder sequence has considerable structure. Thus 3, 3^2, 3^3, 3^4, 3^5, 3^6 all computed modulo 7 yield the successive digits of the sequence. If x = {3/7} the remainder sequence starts with 30 ≡ 2 (modulo 7) and in fact is now 2 6 4 5 1 3, and therefore the decimal sequence for 3/7 is 4 2 8 5 7 1. This example suggests that the structure of the remainder sequence must also show up in the decimal sequence.

Theorem 8: If the decimal sequence, in the scale of r, of p/q; $(p,q) = 1, p < q, and (r,p) = 1$ is shifted to the left in a cyclic manner, l times, the resulting sequence corresponds to the number $p'/q, (p',q) = 1, p' < q$ where $p' \equiv r^l \times p(\text{mod}\, q)$.

Theorem 9: For a maximum length decimal sequence $1/q = a_1 a_2 \cdots a_k, k = q-1$, in the scale of r:

$$a_i + a_{k/2+i} = r - 1$$

Example 1: x = {1/17} in r =10

$$x \Leftrightarrow 0\,5\,8\,8\,2\,5\,5\,2\,9\,4\,1\,1\,7\,5\,4\,7$$

So, $a_i + a_{8+i} = r - 1 = 9$

Example 2: $x = \{1/19\}$ in base $r = 2$

$$x \Leftrightarrow 0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1$$

Here, $a_i + a_{9+i} = r - 1 = 1$

The extension to the above theorem is stated below.

Theorem 10: If the period k of the decimal sequence of $1/q$, q prime, is even in the scale r:

$$a_i + a_{k/2+i} = r - 1$$

Some additional structural properties of the remainder and the decimal sequence digits are presented below.

Theorem 11: For a maximal length decimal sequence the remainder sequence $m_1 m_2 \cdots m_k, k = q - 1$, satisfies the relations

$$m_i m_{q-i} = m_1 (\mathrm{mod}\, q)$$

$$m_i m_{l-i} - 2m_j m_{l-j} + m_l \equiv 0 (\mathrm{mod}\, q) \text{ for all } i, j, l .$$

Theorem 12: The decimal sequence of $1/q$, where q is of the form $r^N + 1$ when expressed in the scale of r would be N consecutive zeros followed by N consecutive $(r-1)$'s.

Distance Properties

Let the ith remainder in the division of $1/q$ be represented by m_i, where $m_0 = 1, m_i = rm_{i-1} - qa_i$. So, the following is obtained.

$$m_{i+j} = r^{j+1} m_{i-1} - q l_i (j+1)$$

where $l_i(j+1) = r^j a_i + r^{j-1} a_{i+1} + \cdots + r a_{i+j-1} + a_{i+j}$.

Example: Considering {1/13} in base 2: 0 0 0 1 0 0 1 1 1 0 1 1. The remainder and the $l_i(4)$ sequences are:

[m]: 2 4 8 3 6 12 11 9 5 10 7 1

[l] : 1 2 4 9 3 7 14 13 11 6 12 8

$m_7 = 2^4 \times m_3 - 13 \times l_4(4) = 16 * 8 - 13 * 9 = 11$

Theorem 13: For a binary decimal sequence $1/q$, if $2^m > q$, then all $l_i(m)$ are different. For such a sequence, all subsequences of length m are different.

Proof: We can write

$$-q l_i(j+1) = m_{i+j} - r^{j+1} m_{i-1}$$

$$= m_{i+j} - 2^{j+1} m_{i-1}$$

For a maximum length decimal sequence:

$$m_{i+j} = m_l^{\,i+j}$$

$$m_{i-1} = m_l^{\,i-1}$$

Now if $l_i = l_k$, then

$$m_{i+j} - 2^{j+1} m_{i-1} = m_{k+j} - 2^{j+1} m_{k-1}$$

$$\text{or } m_{i+j} \equiv m_{k+j} (\text{mod}\, 2^{j+1})$$

Theorem 14: The Hamming Distance d_j between the binary maximum length sequence $\{1/q\}$ and its jth cyclic shift satisfies

$$d_j \geq k/m, j \neq 0, j < k,$$

where $2^m > q, k = q - 1$.

At least one of each m consecutive digits is different from Theorem13. Hence, the minimum distance between each set of m digits is one. For a total of k such group of digits, the distance is k, and since the sequence considered is m times over, the distance is k/m.

Corollary: The autocorrelation $C_1(j)$ of the binary maximum length decimal sequence in the symmetric form (1,-1) satisfies $C_i(j) \le 1-2/m, j \ne 0, j < k$. Since a lower bound exists on the distance between a sequence and its cyclic shifts, these sequences can be used for error detection and correction.

Definition: A decimal (D) code for a message expressed as integer u is defined as $x = \{u/q\}$ where $u \le q-1$ and $\{1/q\}$ is a maximum length sequence. For a D code, the lower bound on errors detected is $(k/m-1)$ and likewise the lower bound on errors corrected is $(k/2m-1/2)$. Since d_j is often larger than its minimum value, the actual error detection and correction ability will be much higher. It appears that D codes do not compare favorably with the commonly used error correction codes, since the ratio m/q for large q becomes progressively smaller.

Cross Correlation Properties

Let $C_{12}(\tau) = (1/N)\sum_{i=1}^{N} a_i b_{i+\tau}$ represent the cross-correlation function of two maximum length decimal sequences $a_1 \cdots a_{k1}$, and $b_1 \cdots b_{k2}$. The period of the product sequence $a_i b_{i+\tau}$ is $N = LCM(k_1, k_2)$, where LCM is the least common multiple.

Randomness Properties

The randomness of a periodic binary sequence of +1's and -1's can be checked by comparing the run characteristics of +1's and -1's as well as its autocorrelation function to that obtained for a normal number where the digits are independent.

For a normal number, the autocorrelation function is:

$$C_1(\tau) = E(a_n a_{n+\tau})$$

where the nth digit of the sequence $a_n \in \{0,1,2,\cdots r-1\}$. The autocorrelation function is two-valued.

Generation of d-sequences

D-sequences are generated using feedback shift registers that allow carry and the hardware used for this is no more complex than for the generation of m-sequences [5]. The algorithm used in this generation is called Tirtha algorithm which is used whenever the prime number q is given in terms of the radix r as $q = tr - 1$, where t is an integer. The number of stages of the shift register required to generate the binary d-sequence $1/q$ is about $\log_2 q$. If t is written as:

$$t_{n-1}2^{n-1} + t_{n-2}2^{n-2} + \cdots + t_1 2 + t_0$$

the shift register will have n stages and the digits of t represent the feedback connections of the shift register. Figure 2.1 shows the generation of d-sequences.

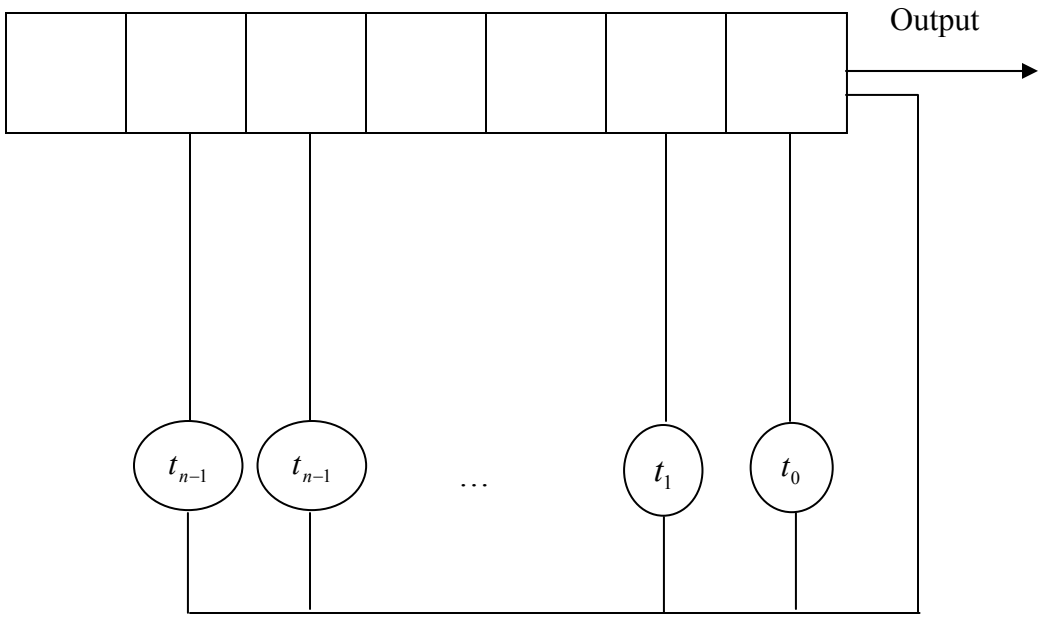

Figure 2.1: Generation of d-sequences

2.3 Encryption and Error Correction Coding Using d-sequences

D-sequences can be applied to encryption and error correction coding by a method in which the encrypted block digits generate a sequence and the digits are generated recursively [17]. This method is called joint encryption and error-correction coding because both these operations are in the group of digits modulo an appropriate number. A new approach to the discrete logarithmic problem is devised and it is called the autocorrelation function method.

Hamming Distance

For a binary maximal length decimal sequence (MLDS) $\{1/q\}_2 : a_1 a_2 \cdots a_k$, where $k = q - 1$,

$$a_i = (2^i \bmod q) \bmod 2$$

If $(2^i \bmod q)$ is odd, then a_i is 1, else a_i is 0. For $2^i < q$, a_i is 0.

Property: The minimum hamming distance d_j between the maximum-length binary sequence $\{1/q\}_2$ and its cyclic shifts equals to the integer closest to $q/3$ or $[2q/3]-[q/3]$. Also, the hamming distance between $\{1/q\}_2$ and $\{u/q\}_2$ is given by:

a) Odd numbers in $(1, q2^{-t})$ + even numbers in $(q2^{-t}, q2^{-t+1})$ + odd numbers in $(q2^{-t+1}, q2^{-t+2})$ + … when $u = 2^t < q$.

b) $[2q/u]-[q/u]+[4q/u]-[3q/u]+\cdots+[(u-1)q/u-(u-2)q/u]$, when u is an odd number.

c) Odd numbers in $(1, q/u)$ + even numbers in $(q/u, 2q/u)$ + odd numbers in $(2q/u, 3q/u)+\cdots$ otherwise.

The proof of the above property is found in [17]. The autocorrelation function $C(j)$ for a binary MLDS in the symmetric (1, -1) form is given by:

$$C(j) \le 1/3, \quad j \ne 0, j < q.$$

The autocorrelation function of $\{1/q\}$ in the symmetric form is 1 for $j = 0$ and -1 for $j = (q-1)/2$. It is generally small and close to zero for even value of j. The autocorrelation function is symmetric about both $j = 0$ and $j = (q-1)/2$ and elsewhere it is spiky. The magnitude of the spikes is between $(-1/\sqrt{q}, 1/\sqrt{q})$. The autocorrelation properties of d sequences are not as good as shift register sequences but their performance improves as the period increases.

Error-correction Coding

Decimal sequences can be used as error-correcting code words because there exists a minimum hamming distance between a maximal length decimal sequence (MLDS) and its cyclic shifts. For such a sequence, the cyclic code obtained is a binary

maximum length D (MLD) code. Non maximum length sequences can also be used for error correction coding and the code corresponding to non maximum length sequences is called a non maximum length D (NMLD) code.

Example for MLD code:

For q = 11, the sequence obtained according to the definition of a decimal sequence is 0 0 0 1 0 1 1 1 0 1. The mapping between the information word to the code word is:

$$0\ 0\ 0\ 1 \rightarrow 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1$$

$$0\ 0\ 1\ 0 \rightarrow 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0$$

$$0\ 0\ 1\ 1 \rightarrow 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1$$

It can be observed that the code words are linear in terms of ordinary addition.

Example for NMLD code

Let q = 23, k =11. The code words for this case are

$$0\ 0\ 0\ 0\ 1 \rightarrow 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1$$

$$0\ 0\ 1\ 1\ 1 \rightarrow 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1$$

The remaining code words are cyclic shifts of the above two code words.

Encryption

D-sequences can be applied to encryption and in order to transmit encrypted blocks of data over a noisy channel, an additional step of error-correction coding is required. A method is described where the cipher block generates a continuing D-sequence and the sequence digits are generated recursively. The algorithm used to form the basis of the cryptographic system is the Diffie–Hellman key distribution scheme which assumes that all users, including the cryptanalyst, can access the prime number q and the primitive root r. If A and B are two users and $k1$ and $k2$ are the random

numbers generated by them, then A transmits to B the number $r^{k1} \bmod q$, and B transmits to A the number $r^{k2} \bmod q$. The transmission of $r^k \bmod q$ numbers must be error free in the Diffie – Hellman method. The steps involved in this method are:

Step 1: Generate $r^k \bmod q$.

Step 2: Find the first j digits of the expansion

$$(r^k \bmod q)/q \text{ in base r}$$

Let the digits be represented by $a_{k1}a_{k2}\cdots a_{kj}$

Step 3: Transmit $a_{k1}a_{k2}\cdots a_{kj}$.

2.4 Summary

In this chapter, an introduction to decimal sequences is given. Some of the properties and theorems are presented. It is also seen that these sequences can be generated easily using feedback shift register with carry. The application of these sequences to encryption and error-correction coding is discussed.

Chapter 3

Generalized d-Sequences

In this chapter, we introduce the proposed generalized d-sequences and list some of their properties. The autocorrelation and cross correlation graphs are shown for several prime numbers.

3.1 Introduction

D-sequences are thought to have greater performance over PN sequences with their excellent cross correlation properties. In order to further extend this study, sequences with non-binary base are studied and experimented. We call these sequences as generalized d-sequences because these are a more general form of d-sequences. If q is a prime number and r is the base of the sequence, then these generalized d-sequences are generated according to the rule [18]:

$$q \bmod r \equiv -k \equiv -1/l$$

$$a_i = l[r^i \bmod q] \bmod r$$

where k and l are integers, and $i = 1,2,\cdots$

'≡' is the congruence notation, first introduced by Gauss which is a convenient way of expressing that two integers differ by a multiple of a positive integer. If,

$$a \equiv b (\bmod m)$$

we say that a is congruent to b modulo m or m is a divisor of $a-b$. It can also be written as $a = b + km$ for a positive integer k.

These sequences are categorized into two types based on their definition:

Type I: The expansion of $\{1/q\}$ in base r (non-binary) in this case is given by:

$$a_i = [r^i \bmod q] \bmod r$$

where q is the prime number and r is the base.

Example 1: Consider the sequence of $\{1/11\}$ in base 3,

So, the sequence $a_i = [3^i \bmod 11] \bmod 3$

$= [3\ 9\ 5\ 4\ 1] \bmod 3$

$= [0\ 0\ 2\ 1\ 1]$

Since the base is 3, the digits in the expansion of the sequence are 0, 1, and 2. The period of this sequence is 5 after which the digits repeat.

Example 2: The sequence of $\{1/27\}$ in base 5

$a_i = [5^i \bmod 27] \bmod 5$

$= [5\ 25\ 17\ 4\ 20\ 19\ 14\ 16\ 26\ 22\ 2\ 10\ 23\ 7\ 8\ 13\ 11\ 21] \bmod 5$

$= [0\ 0\ 2\ 4\ 0\ 4\ 4\ 1\ 1\ 2\ 2\ 0\ 3\ 2\ 3\ 3\ 1\ 1]$

Here since the sequence is of base 5, the digits in the sequence are 0, 1, 2, 3 and 4.

Type II: This is a case in which the expansion of $\{1/q\}$ in base r is given by:

$$a_i = [r^i \bmod q] \bmod s$$

where r is the non-binary base and $s = 3$.

Example 1: Consider the sequence of $\{1/13\}$ base 7.

According to the above definition, this sequence can be expanded as:

$a_i = [7^i \bmod 13] \bmod 3$

$= [7\ 10\ 5\ 9\ 11\ 12\ 6\ 3\ 8\ 4\ 2\ 1\ ] \bmod 3$

$= [1\ 1\ 2\ 0\ 2\ 0\ 0\ 0\ 2\ 1\ 2\ 1]$

Example 2: The sequence of $\{1/19\}$ base 5.

The expansion can be written as:

a_i = [5^i mod 19] mod 3

= [5 6 11 17 9 7 16 4 1] mod 3

= [2 0 2 2 0 1 1 1 1]

The following two sections give the autocorrelation and cross correlation graphs for some examples of the generalized d-sequences.

3.2 Autocorrelation Graphs

Autocorrelation is defined as the correlation of a function with itself over successive time intervals. The autocorrelation function $C(j)$ of a periodic sequence a_i is given by:

$$C(j) = (1/N)\sum_{i=1}^{N} a_i a_{i+j}$$

where the sequence a_i here is given by: $a_i = [r^i \bmod q] \bmod r$

Here, N is the period of the generalized d-sequence. Consider a sequence consisting of five digits in each period and the autocorrelation function for a shift of one digit is desired. This is illustrated as follows:

$$a_1 a_2 a_3 a_4 a_5 a_1 \cdots$$

$$a_2 a_3 a_4 a_5 a_1 a_2 \cdots$$

The autocorrelation function for one shift will be then,

$$C(1) = a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_1$$

The autocorrelation function is calculated using MATLAB and in order to achieve symmetry about X axis in the graphs, certain assumptions are made. Figures 3.1 to 3.8 show the autocorrelation graphs.

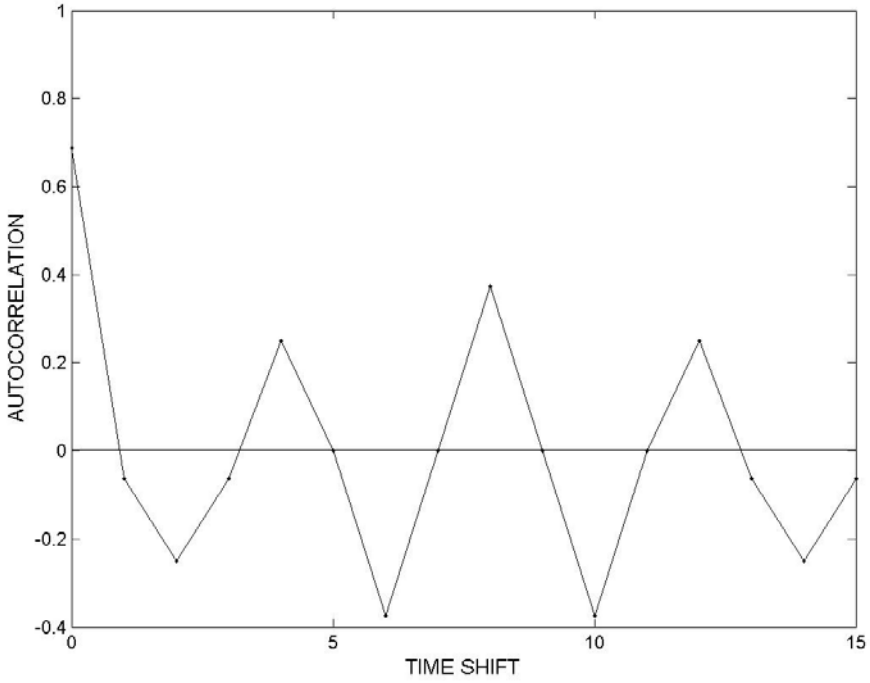

Figure 3.1: Autocorrelation for q = 17, r = 3

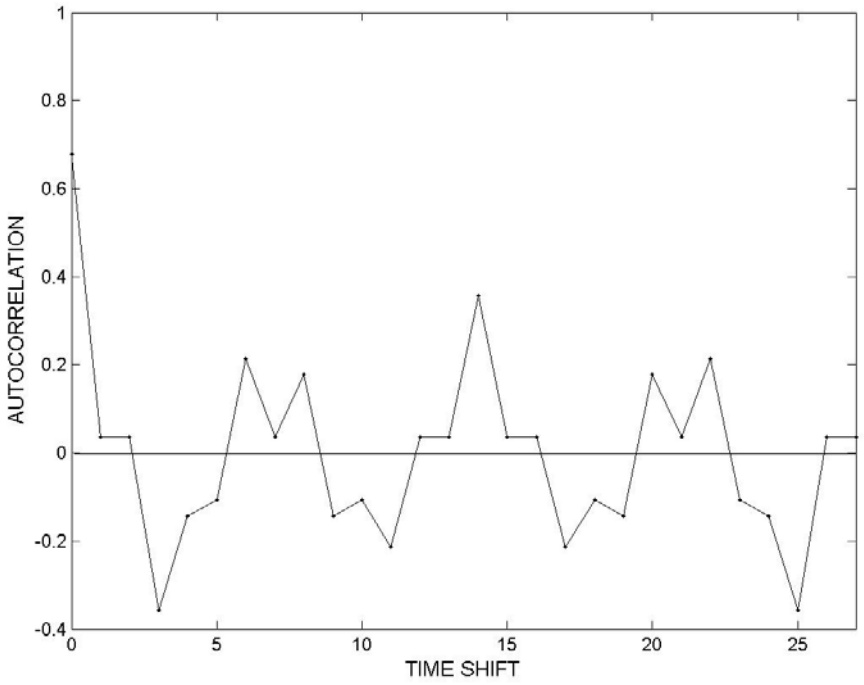

Figure 3.2: Autocorrelation for q = 29, r = 3

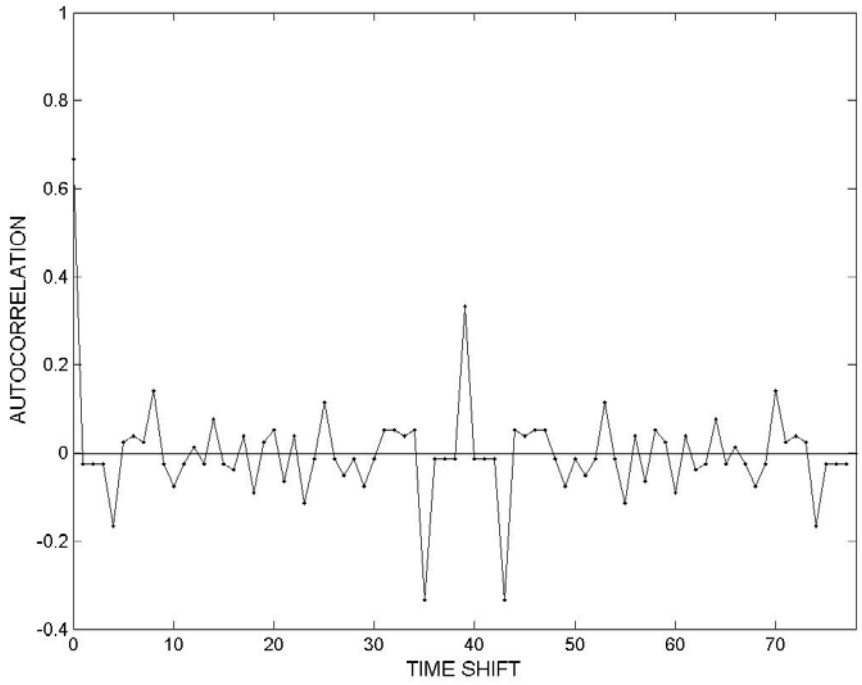

Figure 3.3: Autocorrelation for q = 79, r = 3

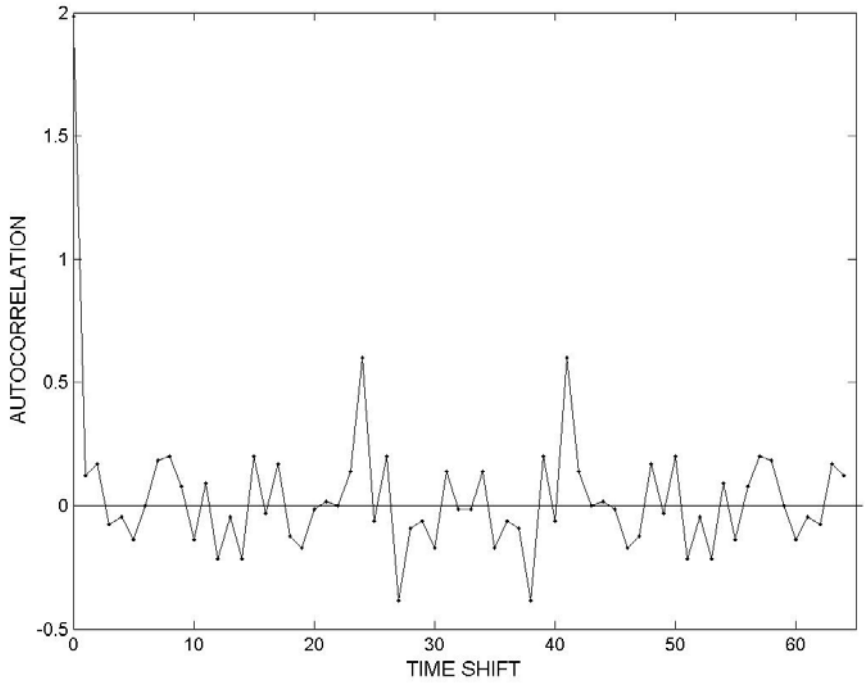

Figure 3.4: Autocorrelation for q = 131, r = 5

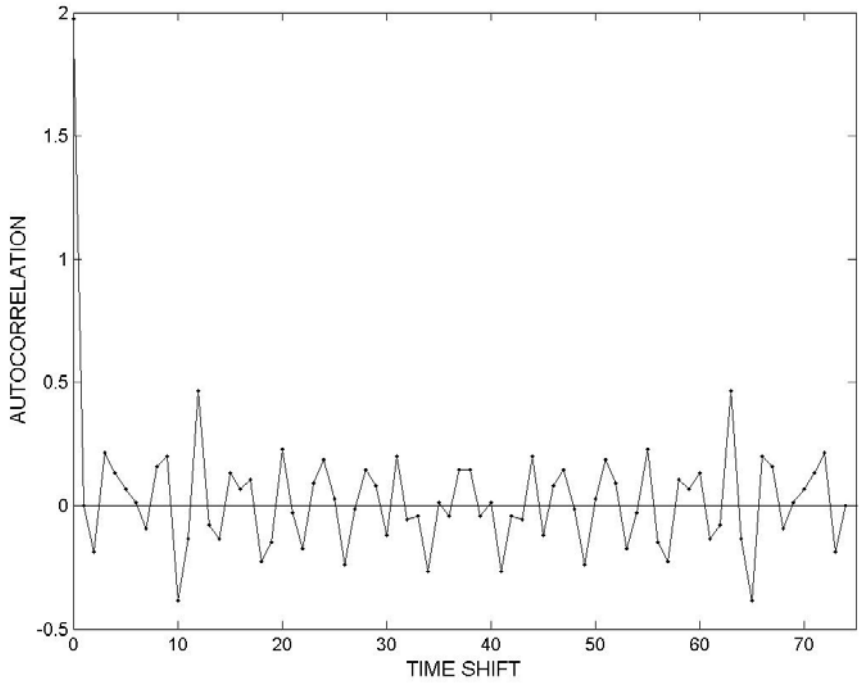

Figure 3.5: Autocorrelation for q = 151, r = 5

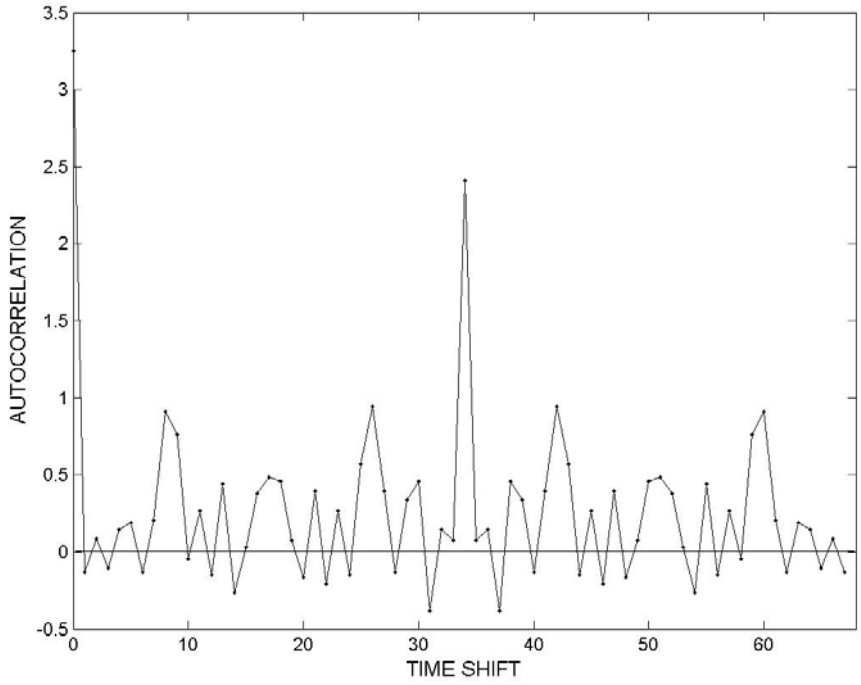

Figure 3.6: Autocorrelation for q = 137, r = 7

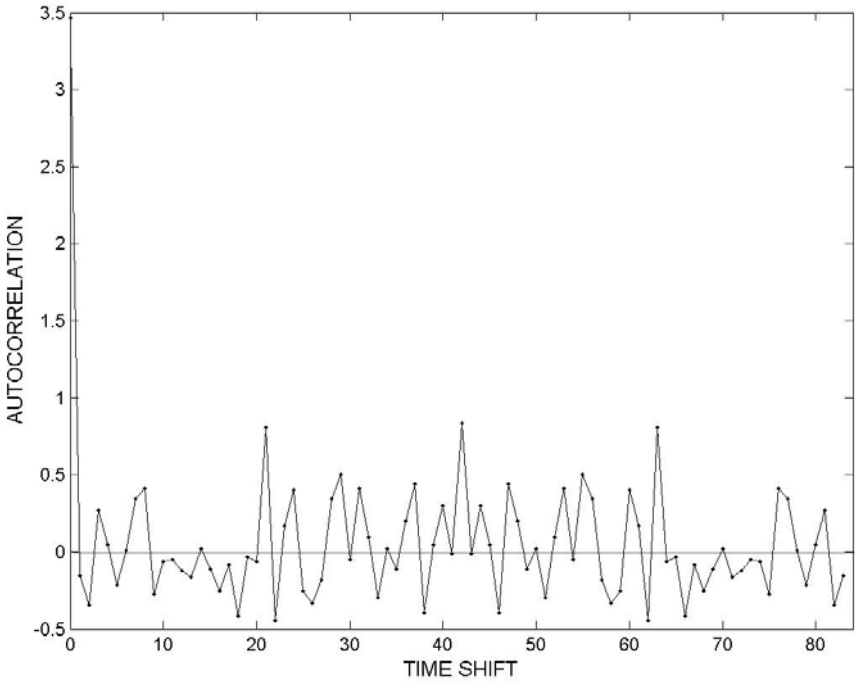

Figure 3.7: Autocorrelation for q = 167, r = 7

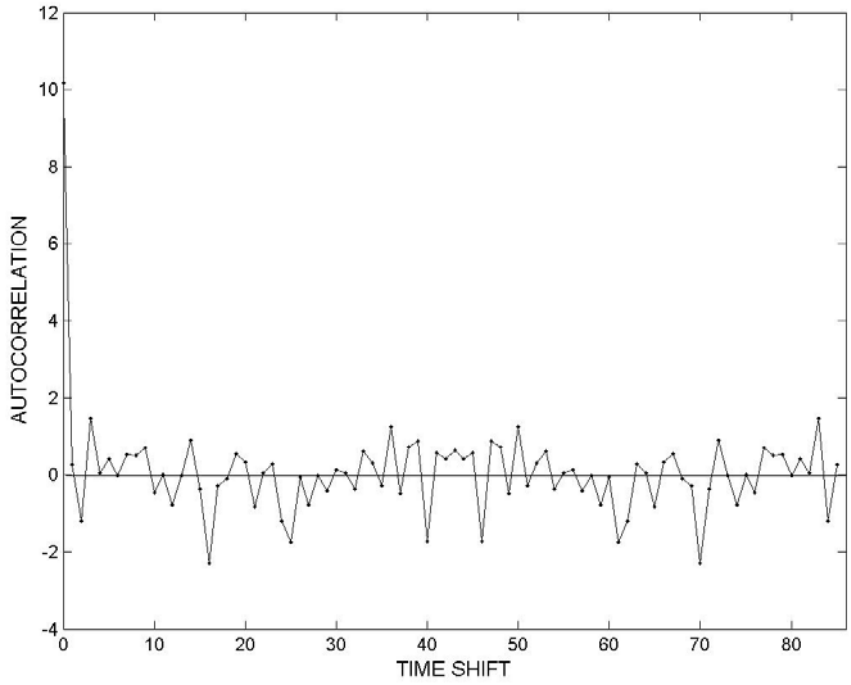

Figure 3.8: Autocorrelation for q = 173, r = 11

The following table shows the period for the above examples:

Table 3.1 Periods for the Autocorrelation graphs

Prime Number (q)	Base (r)	Period
17	3	16
29	3	28
79	3	78
131	5	65
151	5	75
137	7	68
167	7	83
173	11	86

Definition: If q is a prime number, and r is the base, the generalized d-sequence is called a maximum length generalized decimal sequence in the scale of r if it has a period of $q-1$.

Example: From the above table, the generalized d-sequence for $q=17$ with base $r=3$ is of maximum length.

It is also been found that some of the generalized d-sequences which are not of maximum length have a period of $(q-1)/2$. The autocorrelation of the generalized d-sequences in not exactly two-valued.

3.3 Cross Correlation Graphs

The cross-correlation $R(\tau)$ between two sequences a_k and b_k of period N is given by:

$$R(\tau) = (1/N)\sum_{k=1}^{N} a_k b_{k+\tau}$$

The sequences a_k and b_k are given by:

$$a_k = [r^k \bmod q] \bmod r$$

$$b_k = [r^k \bmod t] \bmod r$$

where q and t are the respective prime numbers for the two sequences and r is their base, and τ is the time shift. In calculating the cross correlation, the period N is taken as the LCM of the periods of the first and second sequence.

Example: The cross correlation between (7, 13) base 3, the sequences a_k and b_k are:

$a_k = [0 \quad -1 \quad 0 \quad 1 \quad -1 \quad 1]$

$b_k = [0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1]$

The cross correlation for a time shift of 0 is given by:

$$R(0) = (1/6)\{(0*0)+(-1*0)+(0*1)+(1*0)+(-1*0)+(1*1)\} = 0.1667.$$

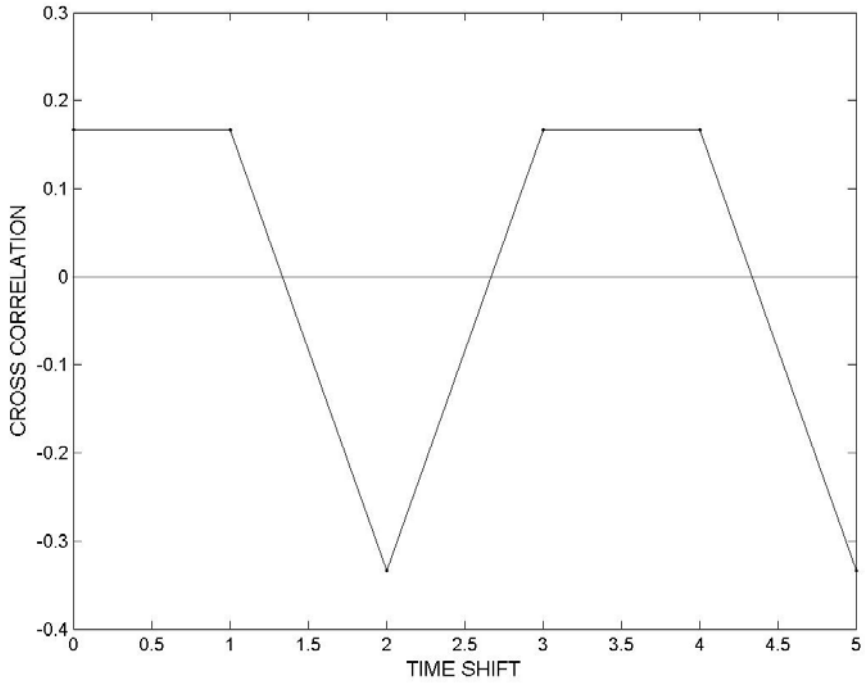

Figure 3.9: Cross correlation of (7, 13) base 3

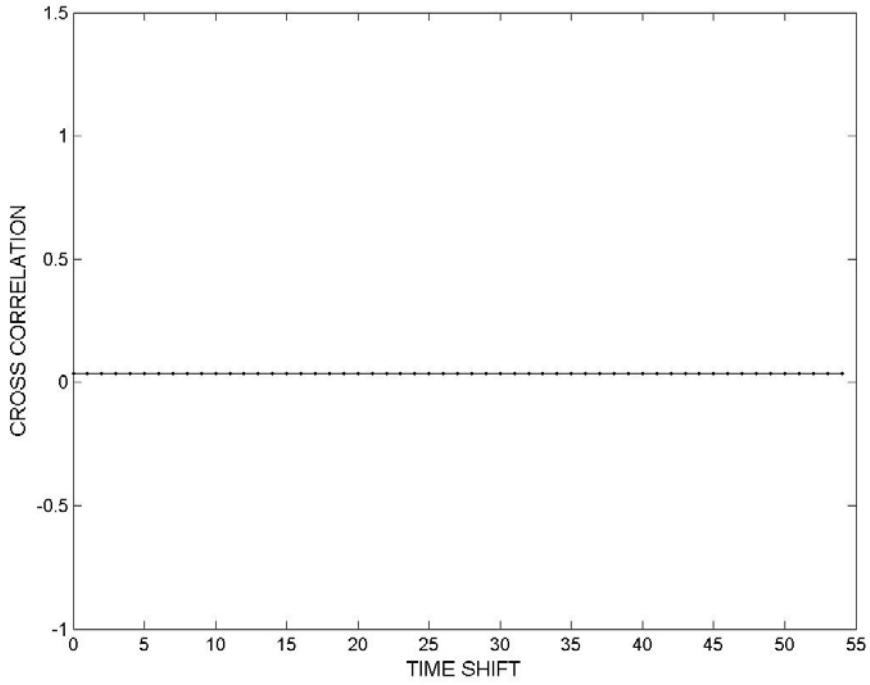

Figure 3.10: Cross correlation of (11, 23) base 3

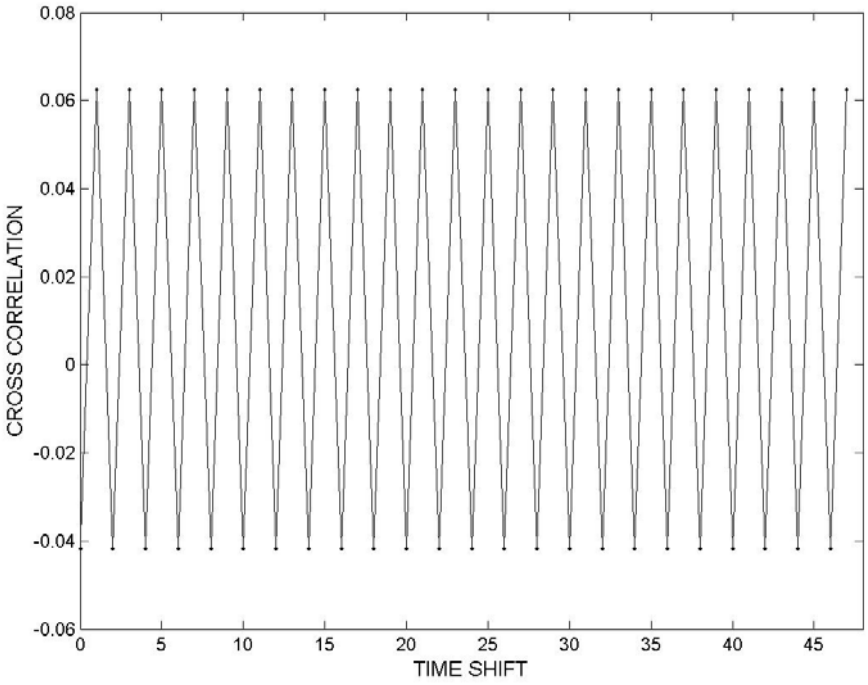

Figure 3.11: Cross correlation of (7, 17) base 5

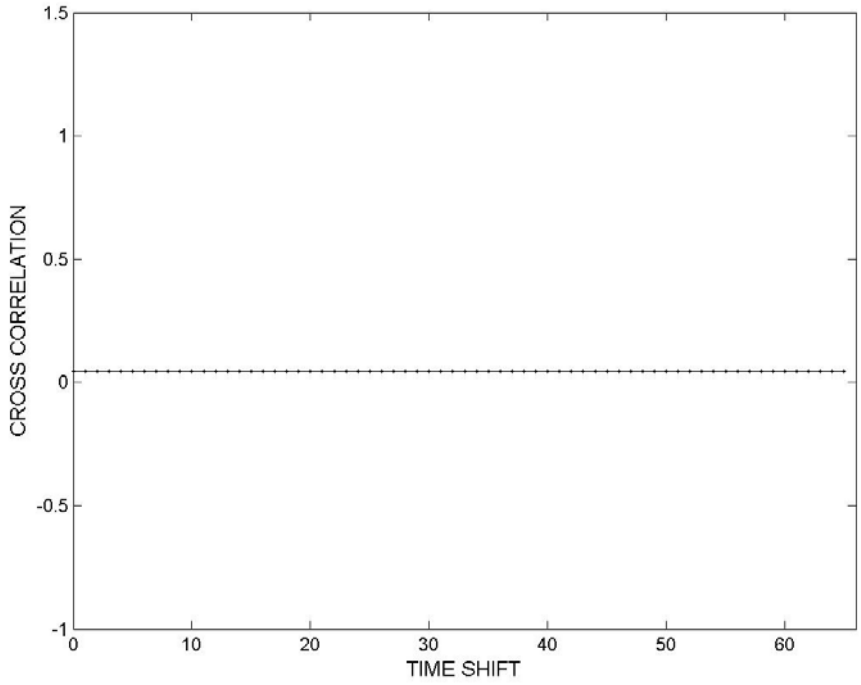

Figure 3.12: Cross correlation of (23, 31) base 5

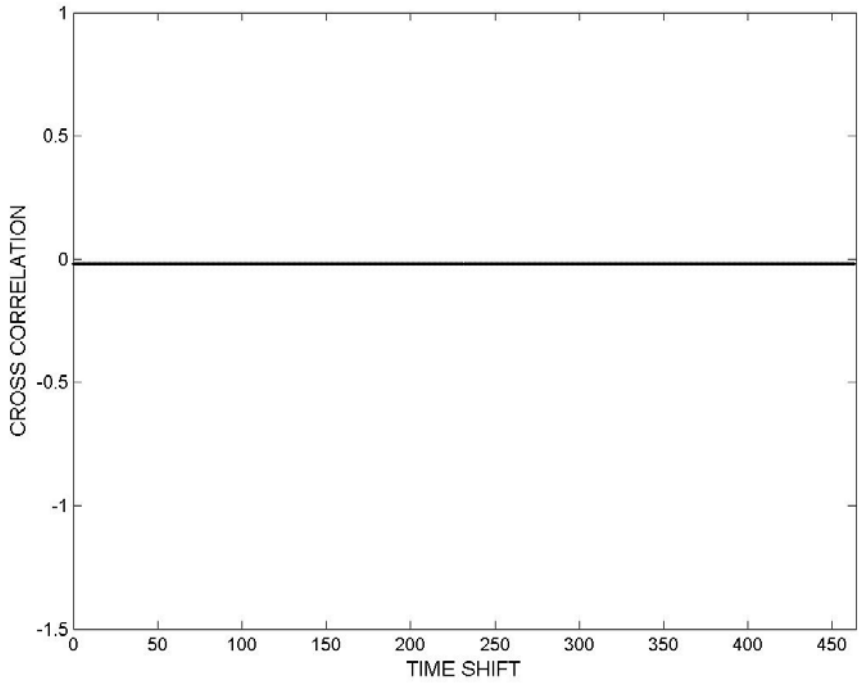

Figure 3.13: Cross correlation of (17, 59) base 7

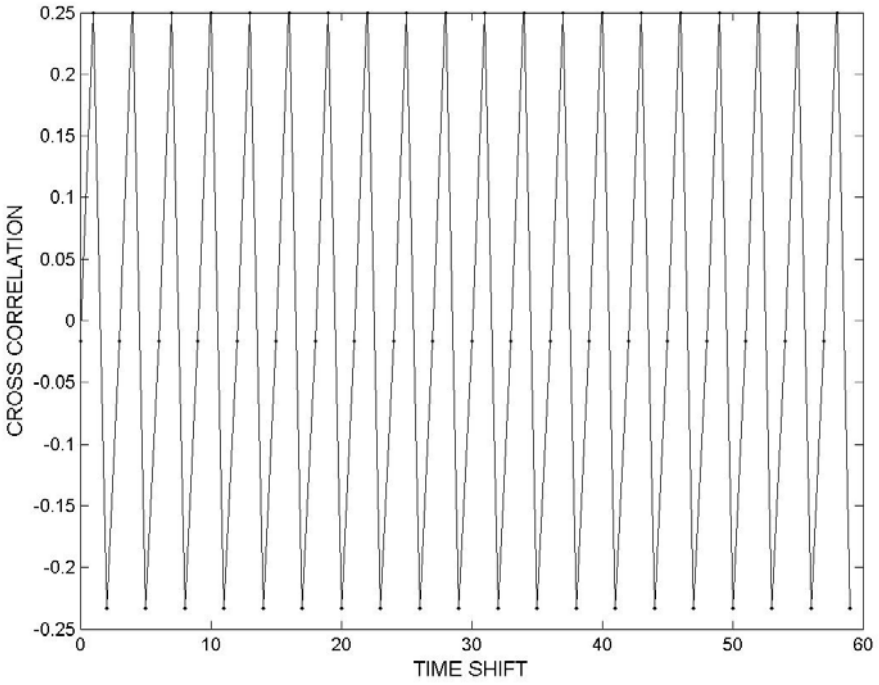

Figure 3.14: Cross correlation of (19, 61) base 7

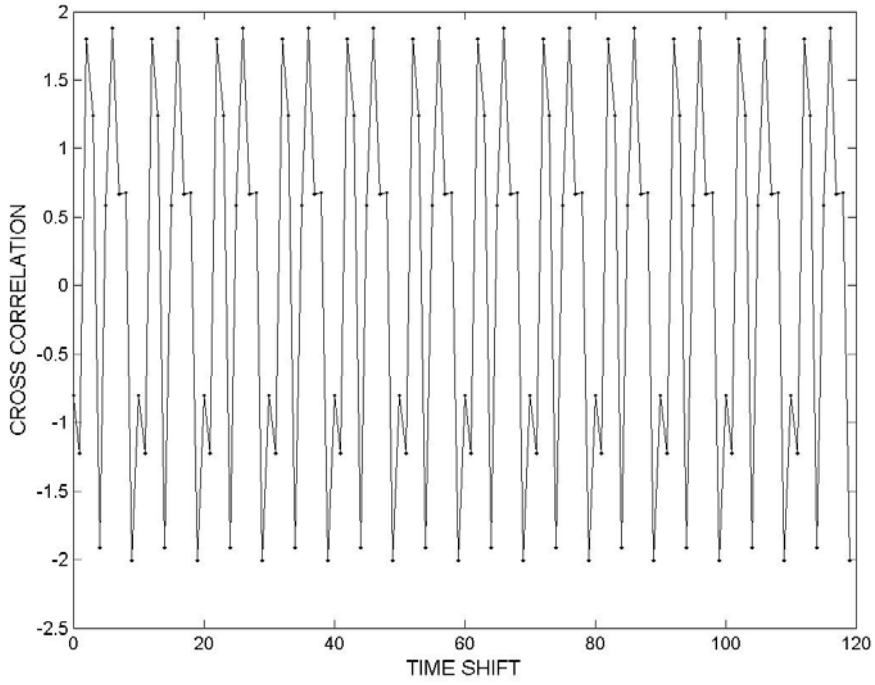

Figure 3.15: Cross correlation of (31, 41) base 11

The table below shows the period for the above graphs. The period in the calculation of cross correlation function is the LCM of the period of the first sequence and the period of the second sequence.

Table 3.2: Periods for the Cross correlation graphs

Prime Number 1 (q)	Prime Number 2 (t)	Base (r)	Period = LCM (q, t)
7	13	3	6
11	23	3	55
7	17	5	48
23	31	5	66
17	59	7	464
19	61	7	60
31	41	11	120

Zero Cross correlation:

It has been found that the cross correlation function of two generalized d-sequences in the symmetric form is identically equal to zero if the ratio k_1 / k_2 of their periods reduces to an irreducible fraction n_1 / n_2 where either n_1 or n_2 is an even number. This interesting property can be very useful in CDMA systems. An example of zero cross correlation is the cross correlation of the two sequences {1/19} and {1/53} base 7. The period of the first sequence is 3 and that of the second sequence is 26. Here, the ratio of their periods 3/26 is an irreducible fraction.

3.4 Summary

This chapter introduces generalized d-sequences and lists the two types of sequences. The autocorrelation and cross correlation functions are defined for these sequences and their graphs are shown. It is found that the autocorrelation function is not exactly two valued while the cross correlation is zero for certain class of these sequences and near to zero for some of them.

Chapter 4

Performance Analysis of Generalized d-Sequences

This chapter deals with analyzing the performance of generalized d-sequences and proposes a system based on these sequences. First, a little overview of binary phase shift keying (BPSK) and direct sequence spread spectrum is presented.

Binary Phase Shift Keying

Digital modulation techniques are classified as coherent and non-coherent techniques. Each of them is again subdivided into binary and M-ary techniques. Examples of coherent binary modulation techniques are amplitude-shift keying (ASK), phase-shift keying (PSK) and frequency-shift keying (FSK) which means that two-level changes are applied to the amplitude, phase and frequency of a sinusoidal carrier wave respectively. Examples of non-coherent systems are non-coherent ASK and non-coherent FSK [19].

4.1 Performance of Direct Sequence Spread Spectrum

All electrical systems have noise in some scale. Noise is defined as unwanted electrical or magnetic phenomena that corrupt a message signal. The effect of the noise depends, among many factors, on the signal level. If the signal level is low, then even a low-level noise can degrade the performance of a system. Noise is categorized into two types based on sources as internal and external noise. Internal noise is generated by components associated with the signal itself while external noise is from natural or man-made electrical or magnetic elements. Some sources of internal and external noise are radio frequency interference, leakage paths at the input terminals, arcs, high frequency

transients etc. The effect of noise on the performance of a system is measured by the ratio of the total signal power to the total noise level. This ratio called as the Signal to Noise ratio (SNR) is usually measured in decibels (dB). The probability of error of a direct sequence spread spectrum is given by [21]:

$$P_E = Q(\sqrt{2E_b / N_0})$$

where P_E is the probability of error, Q is the Gaussian function, E_b is the energy per bit, and N_0 is the single-sided power spectral density of the input noise. The signal to interference ratio (SIR) is defined as the ratio of power in a signal to the interference power in the channel. It is given by the following expression:

$$SIR = \frac{SignalPower}{NoisePower + MAI}$$

where MAI is the multiple access interference.

4.2 Performance Results

Performance Comparison of Generalized d-sequences with PN Sequences

The performance of the proposed generalized d-sequences is compared with that of PN sequences which are used in CDMA systems. This comparison is done by plotting the values of signal to interference ratio (SIR) for different values of signal to noise Ratio (SNR) where SIR is given by the above equation. The signal power is equal to the energy per bit and it is taken as 10W. The generalized d-sequences used are of base 3 and therefore the digits obtained in the expansion of the sequence are 0, 1 and 2. In order to make the digits symmetric, 2 is replaced with -1 so the digits will be 0, 1 and -1. The number of users is taken as 6 for both the PN and the generalized d-sequences. The PN sequences used are generated by feedback shift register taps. For each value of SNR

ranging from 1 to 8, the SIR of each user with every other user is computed. The value of SIR is computed over a particular length of sequences called the sequence length (seqlength) which is varied for each comparison. The programming is done in MATLAB.

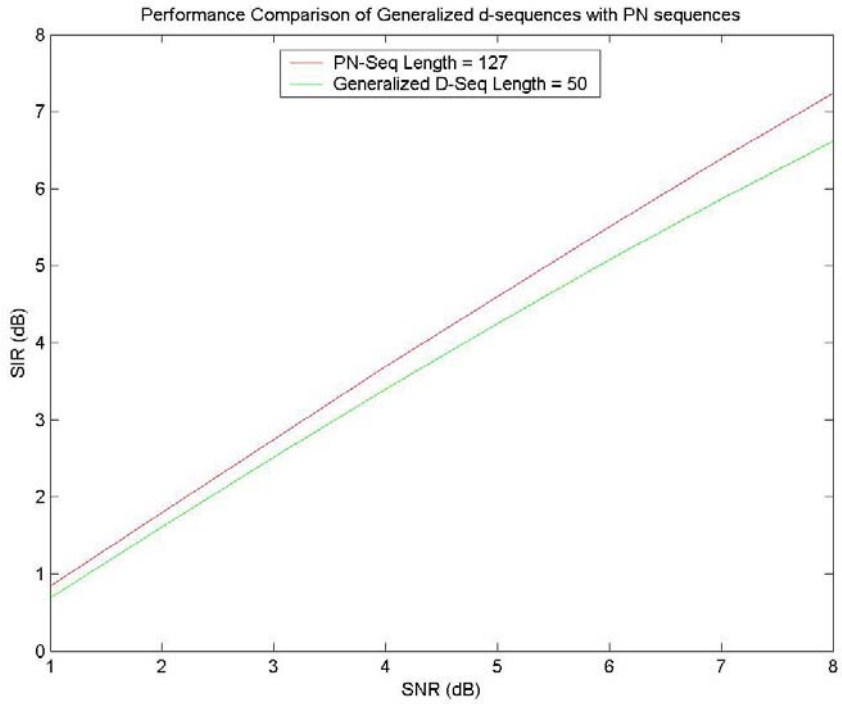

Figure 4.1: Performance of Generalized d-sequences of length 50

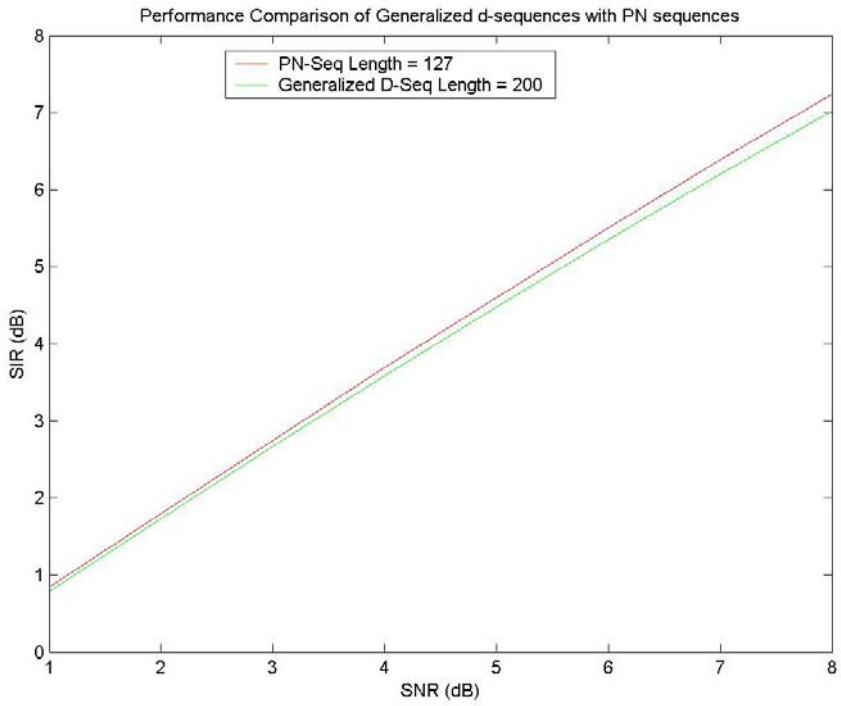

Figure 4.2: Performance of Generalized d-sequences of length 200

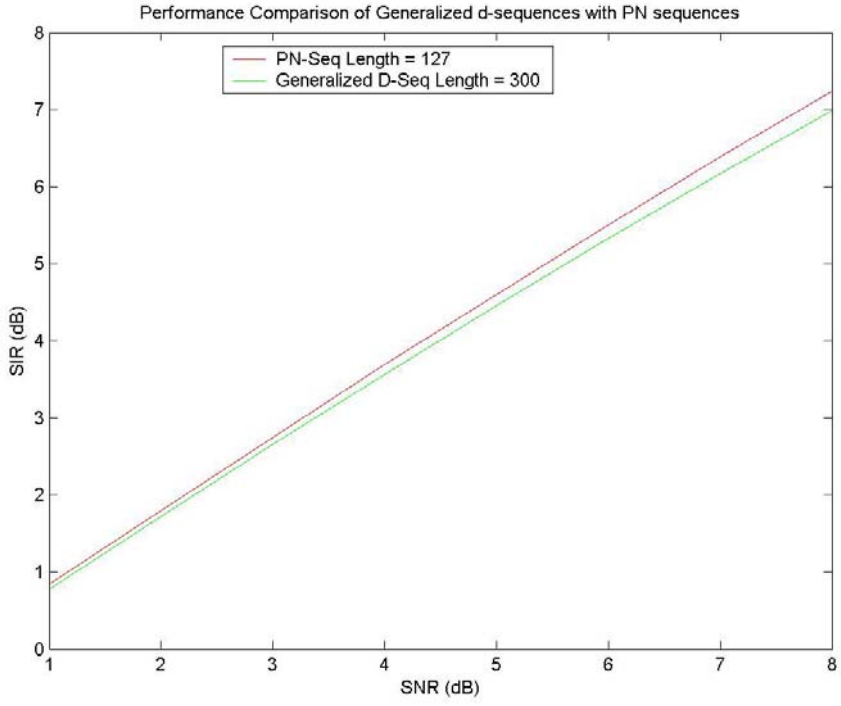

Figure 4.3: Performance of Generalized d-sequences of length 300

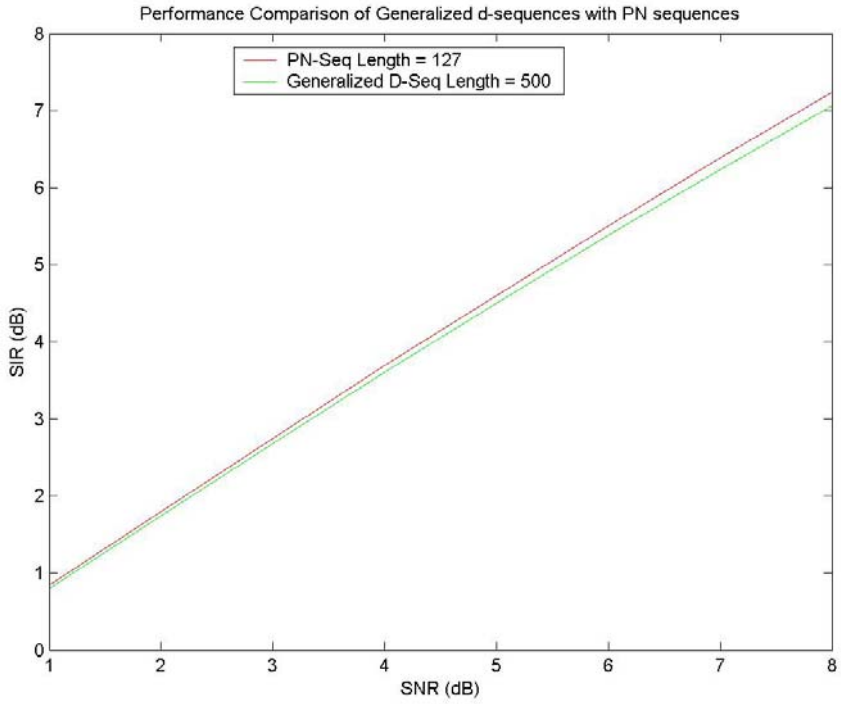

Figure 4.4: Performance of Generalized d-sequences of length 500

From the above graphs, it can be seen that the value of signal to interference ratio of the generalized d-sequences increases with the length of the sequence. For a sequence length of 500, the SIR is close to that of the PN sequences. This is illustrated by plotting the SIR of these sequences for different sequence lengths.

Generalized d-sequences with Different Sequence Lengths

The effect of sequence length on the generalized d-sequences is analyzed by plotting SIR Vs SNR for different sequence lengths. It is found that as the sequence length increases, the value of SIR for each value of SNR increases.

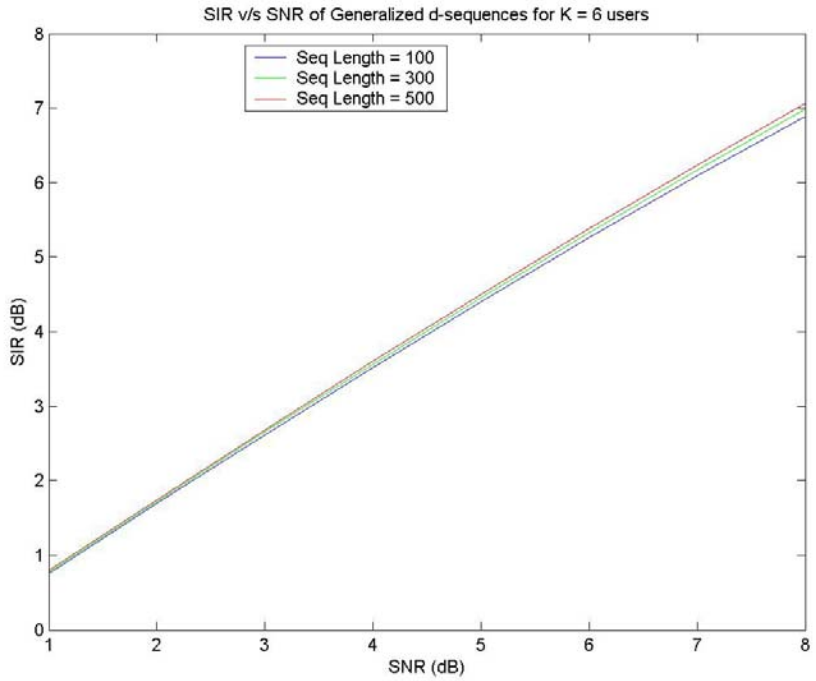

Figure 4.5: Performance of Generalized d-sequences for different sequence lengths

Comparison of Generalized d-sequences with d-sequences:

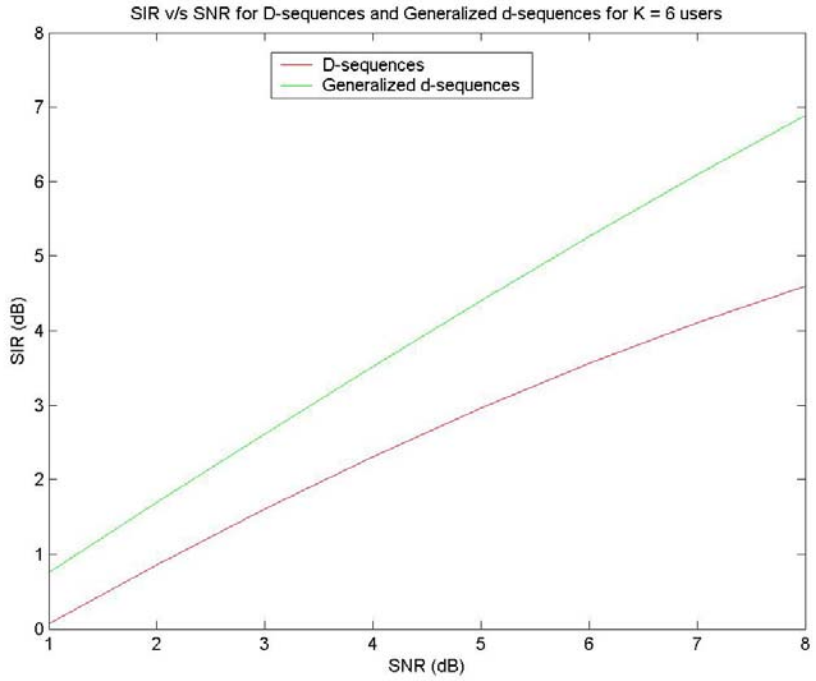

Figure 4.6: Performance Comparison with d-sequences

The performance of generalized d-sequences is compared with that of d-sequences. The generalized d-sequences are of base 3 in this case and d-sequences are of base 2. All the other parameters are kept same. It is found that the value of SIR is more for generalized d-sequences than that of d-sequences.

4.3 Application to CDMA System

This section proposes an application of generalized d-sequences to a system close to IS-95 CDMA system. The fundamentals of IS-95 CDMA system are given and then the proposed system is suggested.

IS-95 CDMA System

IS-95 CDMA is a digital cellular radio system that is used in over 35 countries around the world [22]. It uses orthogonal codes called Walsh codes which are 64 in number. It combines these orthogonal codes with two pseudorandom sequences (PN) for each communication channel. There are two types of PN codes used in IS-95 CDMA system which are short PN code of period 2^{15} and long PN codes of period $2^{42}-1$. The short code is used for quadrature spreading on both the forward and reverse links while the long code is used for separating reverse channel links and data scrambling on the forward link. Figure 4.7 shows IS-95 forward channel diagram [24].

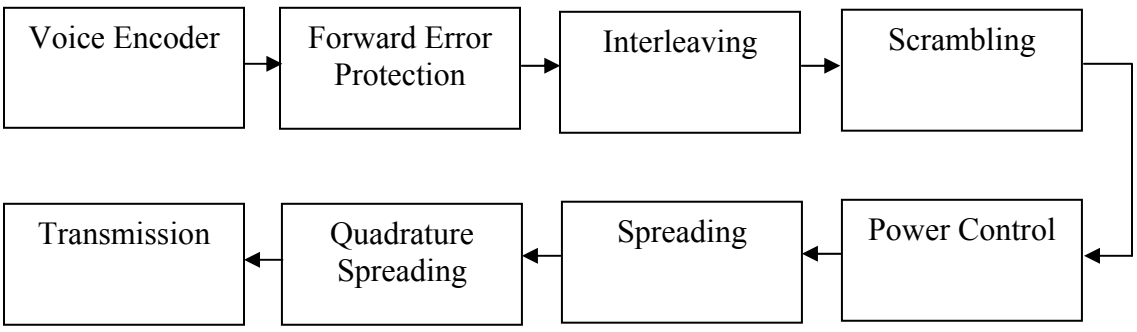

Figure 4.7: IS-95 Forward voice channel coding and modulation

First, an audio signal is supplied to the voice encoder and then error protection bits are added at the forward error protection level. These bits are alternated in time in the interleaver to avoid errors and a pseudorandom sequence is applied to randomize the data and provide privacy. Spreading is done by using orthogonal Walsh codes which increases the data rate by a factor of 64. A PN code is again applied in quadrature spreading level from where the data is sent to the modulator where it modulates the radio frequency carrier for radio transmission. The IS-95 forward link uses the following channels:

- The pilot channel which is used for estimation of the channel
- The Sync channel, used for synchronization
- The Paging channels used for control information
- The Traffic channel which carries the speech or data.

The reverse channel is similar to the forward channel except that there is a randomizer which selects the group of repeated symbols to be transmitted.

Generalized d-sequences are shown to less cross correlation values and zero cross correlation is some cases. Their comparison with PN sequences showed that their performance is closer to PN sequences. So, these sequences can be used in the applications involving PN sequences. One such application can be in a system which is similar to IS-95 CDMA system. Since the PN sequences have large cross correlation values around the origin, it results in near-far problem and power control becomes mandatory in order to keep a uniform received level at the base station. Since the generalized d-sequences have zero cross correlation for certain sets of sequences, they can be used as spreading sequences.

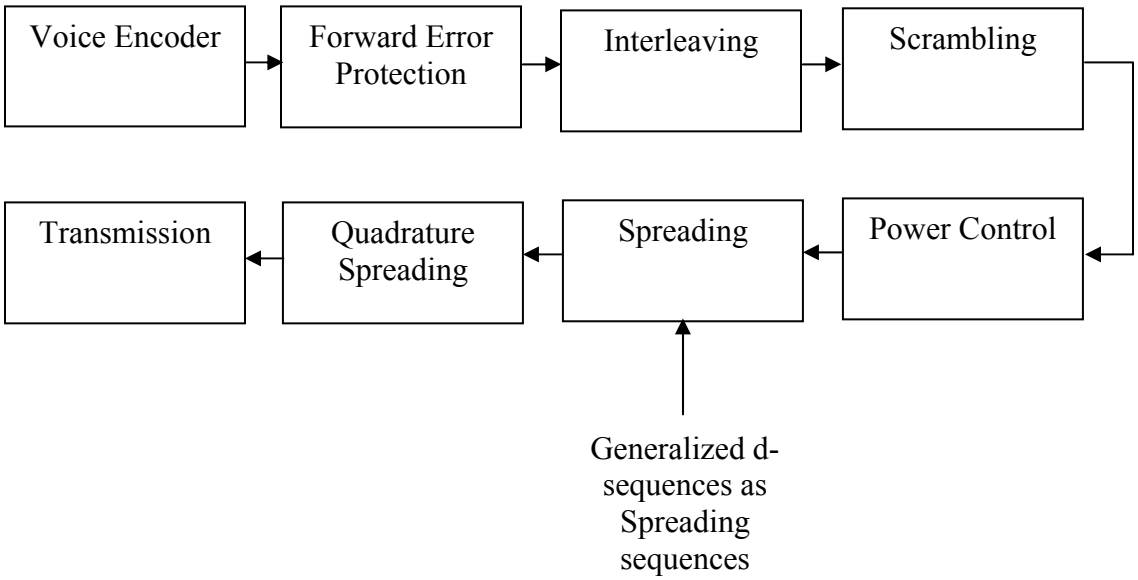

Figure 4.8: Suggested system using Generalized d-sequences

4.4 Summary

This chapter analyzed the performance of generalized d-sequences in terms of the signal to noise ratio, and compared the performance with PN sequences. They are also compared with d-sequences. The IS-95 CDMA system is explained and a system with generalized d-sequences as spreading sequences is proposed.

Chapter 5

Conclusions

This thesis presents properties of generalized d-sequences which could be used as spreading sequences in certain applications requiring multiple access. These sequences have certain desirable properties with regard to cross correlation but at the cost of certain degradation of autocorrelation characteristics. In some applications, the low autocorrelation performance may not matter. Also, the superior cross correlation performance would help in overall performance because of reduced noise. In some special cases, where these is zero cross correlation for certain class of generalized d-sequences, the power control limitation which is one of the shortcomings of the CDMA technology would not apply. These sequences would solve the near-far problem which occurs in CDMA systems when the received signals are not orthogonal.

However, the condition of zero cross correlation would be true only if each user were to use a spreading sequence equal to the least common multiple of the basic generalized d-sequences. In reality, this would place a restriction that may not be realistic with regard to accommodating multi-users. Therefore, further research is to be done to find the partial cross correlation function of the generalized d-sequences and its implication for signal design.

Bibliography

[1] G. Mandyam and J. Lai, "Third- Generation cdma systems for enhanced data services", Academic Press, 2002.

[2] R. Dixon, "Spread Spectrum Systems with Commercial Applications", Third Edition, John Wiley & Sons, Inc, 1994.

[3] S. Kak and S. Herlekar, "Performance Analysis of a D-sequence Based Direct Sequence CDMA system", 2002.

[4] S. Kak, A. Chatterjee, "On Decimal Sequences", IEEE Trans. Inform. Theory, Vol. IT-27, Sept 1981, pp.647-652.

[5] S. Kak, "Generating d-sequences", Electronics Letter, 1987.

[6] R. Gold, "Optimal binary sequences for spread spectrum multiplexing", IEEE Trans. Inform. Theory, vol.IT-13, 1967, pp.619-621.

[7] K. Yang, Y. Kim, P. Kumar, "Quasi-Orthogonal Sequences for Code-Division Multiple-Access Systems", IEEE Trans. Inform. Theory, vol.46, May 2000.

[8] GSM MoU, www.gsmworld.com, February, 2001.

[9] V. Garg, J. Wilkes, "Wireless and Personal Communications Systems", Prentice Hall, 1996, pp 5.

[10] I. Brodsky, "Wireless: The Revolution in Personal Telecommunications", 1995, pp 37-43.

[11] CDMA Concepts and Applications in Wireless PCS Networks, http://www.itv.umd.edu/webvideo/SCCDMA_Part1.pdf .

[12] B. Lee, B. Kim, "Scrambling Techniques for CDMA Communications", New York Kluwer Academic Publishers, 2002.

[13] R. Gold, "Maximal Recursive Sequences with 3-valued Recursive Cross-Correlation Functions," IEEE Trans. Inform. Theory, Jan., 1968, pp. 154-156.

[14] Gold Sequence Generator, http://www.mathworks.com.

[15] T. Kasami, "Weight distribution formula for some class of cyclic codes", Coordinated Science Lab, Univ. Illinois, Urbana. Tech. Rep. R-285 (AD 632574), 1966, pp, 268-274.

[16] S. Golomb, "Shift Register Sequences", San Francisco: Holden-Day, 1967.

[17] S. Kak, "Encryption and Error-Correction Coding Using D-sequences", IEEE Trans. on computers, Vol. c-34, No. 9, September 1985, pp 803-809.

[18] S. Kak, "New Results on D-sequences", Electronics Letters, Vol. 23, June 1987, pp 617.

[19] S. Haykin, "Communication Systems", 4th Edition,

[20] Direct Sequence Spread Spectrum, http://www.see.ed.ac.uk/~ssp/project.

[21] R. Ziemer, W. Tranter, "Principles of Communications", Fifth Edition, John Wiley & Sons, Inc.

[22] H. Lawrence, "CDMA IS-95 for Cellular and PCS", McGraw-Hill Telecommunications.

[23] D. Li, "The Perspectives of Large Area Synchronous CDMA Technology for the Fourth Generation Mobile Radio", IEEE Communications Magazine, March 2003.

[24] L. Harte, R. Levine, R. Kikta, "3G Wireless Demystified", McGraw Hill.

Vita

Radhika Vaddiraja was born in Hyderabad, India, on September 19, 1978. She received her bachelor of engineering degree in electrical and electronics engineering from Osmania University, Hyderabad, India, in 2000. After graduation, she joined the graduate program in the Department of Electrical and Computer Engineering at Louisiana State University in the fall of 2000. She expects to receive the degree of Master of Science in Electrical Engineering in August, 2003.