Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.8, 2015

Design and Analysis of Ternary m-sequences with Interleaved Structure by d-Transform

Hieu Le Minh PhD.[1] Truong Dang Van[1,2] Binh Nguyen Thanh[1,3] Quynh Le Chi PhD. [1,4]

1. VNPT Vietnam 57 Huynh thuc Khang Hanoi
2. Academy of Cryptology Technology, Vietnam 105 Nguyen chi Thanh Hanoi
3. Vietnam Government Information Security Committee ,105 Nguyen chi Thanh Hanoi
4. VANLANG UNIVERSITY, 45 Nguyen Khac Nhu TP HCM Vietnam

Abstract:

Multilevel sequences find more and more applications in modern modulation schemes [4QPSK, 8QPSK,16QAM..] for the 3G ,4G system air interface [1,2].Furthermore, in modern cryptography they are also widerly used. It is also interesting to point out that the length L of these sequences are composite numbers(L=NS),that means the sequence can be easily implemented by interleaving S subsequences, each of length S.Therefore, the methods to develop multilevel sequence with interleaved structure draw a lot of attentions [3, 4]. In this contribution, a method for design and analysis of ternary m-sequences with interleaved structure is presented, based on the d-transform, Which turns out to be a very effective and versal tool for this purpose. Simulations have been made to verify the theory.

We first introduce d-transform and its properties and then work out the procedure to design an interleaving sequence in d-transform.

Keywords: d-transform,q-ary sequences, interleaved sequence.

1. Introduction

For 3G,4G telecommunication the benefit of emplyoing the multilevel sequences in high order modulation scheme is obvious:It increase the system throughput[1,2].However,In such applications like network security and cryptography, multilevel (q-ary) sequences with good static properties ,high-linear complexity and of long periods L are required[5,6,7].Understanding,presenting and generating these sequences require extensive mathematical knowledges like:Galois field arithmetic,time and frequency domain signal transformations..and so on, which are very abstact and therefore not easily to master.Hence ,we see the need to apply some simpler and more intutive approach,namely d-Transform. In this paper, for the sake of simplicity ,we first represent the new method for designing the ternary m-sequences with interleaved structure by means of d-transform.D-transformation is choosen because it is nothing but time multiplexing of bits,which is already quite familiar with telecommunication engineers in digital transmission.It is therefore easily transformed into hardware implementation. Based on that procedure the the designing of another q-ary sequeces can be followed esealy.(To complete this complicated problem,we will extend this procedure for desinging the most useful sequences:the nonlinear and cascarded interleaved sequences in the next contributions).The paper is organized as follows.

In the session II, we introduce the concept of d-Transform and its application to interleaved sequences. Next, in the session III, the case of ternary interleaved sequence is investigated in details. It is show in 3.1 how to represent ternary interleaved sequence in d-Domain. In 3.2 the procedure for construction of these sequences is explained.

Furthermore, for better understanding and wider view,a comparison with the well known Trace function is given.

To complete this paper, some statistic properties of the constructed sequence are investigated in session 4.

2. D-Transform and Interleaved sequences

In the literature, the Trace function representation based on α, a primitive element of the finite field

GF(qn) ,q being a primitive integer, has been widely used to investigate the interleaving structure [4,5,7]. In this contribution we will show that, the D-transform representation(simple mathematical tool to convert the sequences into polynomials) is not only effective but some time advantageous. As an evidence, we take the case when the length of the sequence L # q^n-1, with q being a primitive integer where the trace function is not defined

and therefore cannot be applied [8,9]. However, the polynomial representation is still applicable [10,11].Futhermore,this approach(d-transform) is quite convenient to present the time multiplexed structure like interleaved sequences. In fact, the interleaved sequences (both linear and nonlinear) with good statistic properties have been investigated and published as early as 1985 by IIT DELHI fellows [12].Q.GONG et al[5] have given a systematic treatment of interleaved structure in 1995!In 2005 a more generalized method to analyze the interleaving structure of nonlinear binary sequence in d-domain is presented[13] In 2013 a rigorous mathematical analysis of interleaved sequences over finite field is given by Jing He[14] .

The d-transform of a sequence$\{b_n\}$ over GF(q) is denoted by $D[b_n]$ or F and defined by:

$$D[b_n]= F = \sum_{i=0}^{m} b_i d^i \ , \ b_i \in \{GF(q)\} \qquad (l)$$

Example l: Lets $\{b_n\}=\{2\ 2\ 0\ 2\ 1\ 1\ 0\ 1\}$, d-transform of {b,} is $D[b_n] = 2 + 2d + 2d^3 + d^4 + d^5 + d^7$. The inverse transform of D is $D^{-1} = \{b_n\}$.

Thus, the d-transform of the sequence will have the form of a polynomial in d over GF(q) and has been conveniently used in signal and system analysis in data transmission and processing [10.11].

Some properties of polynomial over GF(q) (where q is a prime number) are now summarized.

The exponent of the polynomial Q(d) is the minimum value of *l* such that Q(d) divided $1-d^l$, i.e., $(1-d^l)/Q(d)$ is a polynomial of finite degree. An irreducible polynomial of degree m is primitive or of maximum exponent if its exponent is $q^m- 1$. Given a polynomial Q(d) of order m, its reciprocal polynomial is $d^mQ(1/d)$ and it is known that reciprocal polynomials of irreducible polynomials are themselves irreducible and that reciprocal polynomials of primitive polynomials are themselves primitive.

The d-transform of a periodic sequence is of the form $R(1)/(1-d^l)$, where *l* is the period of the sequence and R(d) is a polynomial of degree less than *l* in d over GF(q). In general, it can be show that, the d-transform of a periodic time series is of the form p(d)/Q(d) where both p(d) and Q(d) are polynomials over Galois Field. If p(d) and Q(d) are relative prime, the period of the time series represented by p(d)/Q(d) is the exponent of Q(d).

The d-transform of the generator sequence $\{b_n\}$ of a linear feedback shift register (LFSR) is then given by:

$$b(d) = S(d)/g(d) \qquad (2)$$

where g(d) of degree n is the generating polynomial of a LFSR and S(d) of degree ≤ n–1 specifies the initial condition corresponding to a particular shifted version of $\{b_n\}$. When g(d) is primitive, the LFSR sequence is an m-sequence and there are p^n-l polynomials S(d) corresponding to p^n-1 values of the initial states of that LFSR.

The d-transform pairs are given in [10,11]. The construction procedure based on d-transform for creating the non linear binary interleaved sequences is given in [12,13,].This contribution extends the result of [13]l for the case of ternary sequences. Here we show how to apply procedures for ternary cases and will discuss the two procedures:

- Procedure l: Expanding the subsequence.
- Procedure 2: Decomposition of m-sequences through decimation.

These procedures are applicable for ternary sequences, provided that the corresponding ternary d-transform is used.[10,11].

3. The procedures to construct the q-ary interleaved sequences [12,13]

- 1st step: find out the Interleaving order I_P^S .

- 2nd step: Generating the interleaved sequences.

3.1 First step: I_P^S determination. This can be carried out by two algorithms: Expanding and

Decomposition.

3.1.1 Expanding

Let $\{b_n\}$ be an m-sequence generate by g(d) of degree n, length L(composite integer) with:

$$L = 3^n - 1 = 3^{l*m} - 1 = S.(3^m - 1) = S.N,\ n = l.m,\ S = (3^n - 1)/(3^m-1)$$

Let b(d) be d-transform of $\{b_n\}$ given by (2)

we always can express b(d) as:

$$b(d) = \sum_{i=0}^{S-1} d_i F_i(d^S) \qquad (3)$$

with $F_i(d)$ is a subsequence generated by $g_l(d)$ of degree m, length N and be represented by d-transform:

$$F_i(d) = \frac{S_i(d)}{g_l(d)},\ i = 0, 1, \ldots, S-1 \qquad (4)$$

With $S_i(d)$ specifies the initial state of the subsequence and $g_l(d)$ be the generating polynomial of that subsequence respectively.

This follows immediately from the properties of d-transform since $\{b_n\}$ can be constructed by interleaving S phases of $\{F_n\}$. The particular phases of $\{F_n\}$ in that interleaving can be determined through 3-steps.

1st step: expanding the subsequence $F_i(d)$ by S times (inserting S-1 zeros between two consecutive bits of $F_i(d)$), in d-transform, it is equivalent to replace d with d^S.

$$F_i(d^S) = \frac{S_i(d^S)}{g_l(d^S)} \qquad (5)$$

2nd step: Express d-transform of b_n in term of interleaving of $F_i(d)$.

or (inserting S different phases of $F_i(d)$ to create b(d))

$$b(d) = \sum_{i=0}^{S-1} d_i F_i(d^S) = \sum_{i=0}^{S-1} d^i \frac{S_i(d^S)}{g_l(d^S)} \qquad (6)$$

Then, put the numerator of (6) as:

$$G(d) = \sum_{i=0}^{S-1} d^i S_i(d^S) \qquad (7)$$

Substituting (6) into (2) we obtain:

$$G(d) = \frac{S(d) \cdot g_1(d^S)}{g(d^{\ })} \qquad (8)$$

3rd step: - put $d^S = D$

- Finding out the phase shifts $\frac{S_i(D)}{g_l(D)} = F_i(D)$

And regrouping b(d) as:

$$b(d) = \sum_{i=0}^{S-1} d^i F_i(D) \qquad (9)$$

Comparing $d^i F(D)$ with d-transform table for example: table l, we can easily find out the interleaving order I_P^S

This procedure is best illustrated by the following example.

Example 2: Let $g(d) = 1 + d^3 + 2d^4$. n = 4, m = 2, L = 80, N = 8, S = 80/8 = 10

$g_1(d) = 1 + d + 2d^2$.

$$F_l(d^S) = \frac{S_i(d^S)}{g_l(d^S)} = \frac{S_i(d^{10})}{g_l(d^{10})} \qquad (10)$$

$$G(d) = \frac{S(d) \cdot g_1(d^{10})}{g(d)} \qquad (11)$$

If no particular phase of b(d) is interested, we can put: S(d) = 1 for simplicity without loss of generality. Then:

$$G(d) = \frac{g_1(d^{10})}{g(d)} = \frac{1 + d^{10} + 2d^{20}}{1 + d^3 + 2d^4} \qquad (12)$$

$$G(d) = d^{16} + d^{15} + d^{14} + d^{13} + 2d^{12} + d^{10} + 2d^{9} + d^{8} + d^{7} + d^{6} + d^{4} + 2d^{3} + 1$$

$$b(d) = \frac{G(d)}{g_1(d^{10})} = \frac{d^{16} + d^{15} + d^{14} + d^{13} + d^{12} + d^{10} + d^{9} + d^{8} + d^{7} + d^{6} + d^{4} + 2d^{3} + 1}{1 + d^{10} + 2d^{20}} \quad (14)$$

put $d^{10} = D$ and rearrange b(d) as follow:

$$b(d) = \frac{(1+D) + (2D)d^2 + (2+D)d^3 + (1+D)d^4 + (D)d^5 + (1+D)d^6 + (1)d^7 + (1)\,d^8 + (2)d^9}{1 + D + 2D^2} \quad (15)$$

Comparing (it) with table 1, we can see that (15) is d-transform{b_n}:an interleaving of 10 component sequences {a_n}generated by $g_1(d)=1 + d + 2d^2$. The interleaving order (shift sequence[7,15]) is :

IP = {5, "∞", 2, 0, 5, 6, 5, 7, 7, 3} (16)

where ∞ represents the all zero sequence position

$g_1(d)$	Subsequences	Binary form	Phase index	$S_i(d)$	S(D)
$1 + d + 2d^2$	T^0W	2 2 0 2 1 1 0 1	0	2 + d	2 + D
	T^1W	2 0 2 1 1 0 1 2	1	2 + 2 d	2 + 2D
	T^2W	0 2 1 1 0 1 2 2	2	2d	2D
	T^3W	2 1 1 0 1 2 2 0	3	2	2
	T^4W	1 1 0 1 2 2 0 2	4	1 + 2d	1 + 2D
	T^5W	1 0 1 2 2 0 2 1	5	1 + d	1 + D
	T^6W	0 1 2 2 0 2 1 1	6	d	D
	T^7W	1 2 2 0 2 1 1 0	7	1	1
$1 + 2d + 2d^2$	T^0Z	2 1 0 1 1 2 0 2	0	2 + 2d	2 + 2D
	T^1Z	1 0 1 1 2 0 2 2	1	1 + 2d	1 + 2D
	T^2Z	0 1 1 2 0 2 2 1	2	d	D
	T^3Z	1 1 2 0 2 2 1 0	3	1	1
	T^4Z	1 2 0 2 2 1 0 1	4	1 + d	1 + D
	T^5Z	2 0 2 2 1 0 1 1	5	2 + d	2 + D
	T^6Z	0 2 2 1 0 1 1 2	6	2d	2D
	T^7Z	2 2 1 0 1 1 2 0	7	2	2

Table 1: d-transform of component m-sequences

3.1.2 Decomposition of ternary interleaved m-sequence {b_n} :This decomposition based on the decimation of {b_n} by S to find out the way in which the subsequences are time multiplexed(interleaved)

The decomposition can be carried out by two methods:

The d-transform method, the trace function method .

3.1.2.1 The d-transform method

Let consider the ternary m-sequence {b_n} of length L: q^n-1 with q: a primitive integer like {0,1,2,5,7,...} and n = m.k. Then L = N.S : $q^{m.k}$-1.

It has been show [12.13] that in this case, {b_n} can be constructed by interleaving (N-l) component subsequences each of length N: q^m-l and one Null sequence. The subsequences can be obtained by decimation of {b_n} by S.

When the decimation starts at the first bit, we will obtain the subsequence:

$$\{a_0, a_S, \ldots, a_{(3^m-2)S}\} \quad (17)$$

Similarly, we'll obtain the subsequence $\{a_1, a_{S+1}, ..., a_{(3^m-2)S+1}\}$ when the decimation start at the $(t+1)^{th}$ bit. Thus, on the time-domain, these subsequences (arrange in column) can be considered as S time-multiplexed sequences: $\{a_{nS}\}\{a_{nS+1}\}...\{a_{n(3^m-2)S-1}\}$ into S time slots (fig 1):

$$M = \begin{vmatrix} a_0 & a_1 & \cdots & a_{S-1} \\ a_S & a_{S+1} & \cdots & a_{2S-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{(3^m-2)S} & a_{(3^m-2)S+1} & \cdots & a_{(3^m-1)S-1} \end{vmatrix}$$

$$= \{a_{nS}\}\{a_{nS+1}\}...\{a_{n(3^m-2)S-1}\} \qquad (18)$$

T time slots

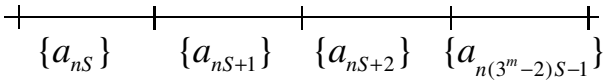

Fig l: Time multiplexed sequences.

The order into which the subsequences are multiplexed is in fact the Interleaving order I_P^S.

Now we can just look up at *table 1* and find out the corresponding $S_i(d^S)$ for the subsequences (in column) and then obtain I_P^S.

Example 3

2: Let n = 4, m = 2 and let α be a primitive element of GF(3^4) with primitive polynomial.

$b(d) = 1 + d^3 + 2d^4$ over GF(3). Let $\{b_n\}$ denote the m-sequence generated by b(d)

$\{b_n\}$ = {1 0 0 0 1 0 0 2 1 0 1 1 1 2 0 0 2 2 0 1 0 2 2 1 1 0 1 0 1 2 1 2 2 1 2 0 1 2 2 2
2 0 0 0 2 0 0 1 2 0 2 2 2 1 0 0 1 1 0 2 0 1 1 2 2 0 2 0 2 1 2 1 1 2 1 0 2 1 1 1}

Decimation of b_n by S = 10, we obtain:

$\{a_n\} = \{b_{n*10}\}$ and rearrange is as (18)

$$M = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 \\ 1 & 1 & 1 & 2 & 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 2 & 2 & 1 & 1 & 0 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 2 & 0 & 1 & 2 & 2 & 2 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 2 & 0 \\ 2 & 2 & 2 & 1 & 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 1 & 1 & 2 & 2 & 0 & 2 & 0 & 2 & 1 \\ 2 & 1 & 1 & 2 & 1 & 0 & 2 & 1 & 1 & 1 \end{vmatrix}$$

- Compare the column of M with *Table 1*, we have the interleaving order or (shift sequence) as below:

$$I_P^S = \{4, 6, 6, 2, 5, \text{“}\infty\text{”}, 2, 0, 5, 6\}$$

where ∞ represents the all zero sequence position

Note that I_P^S is fully identical to the result calculated by trace funtion below.

3.1.2.2 The Trace function method

In [15,] the relation between power offield element α and d-transform is again very clear explanned.

Since both representation (via power of α and d-transform) are quite equivalent ,the interleaving order (in which the component sequences are placed) can be determined by two methods.

a. Power of α (Trace function) representation

In this case, the interleaving order is determined as follows:

Which m,n are positive integer, α is a primitive element of the finite field GF(3^n) and

S = L/N = (3^n-1)/(3^m-1)

$Tr_m^n(x)$ is the trace function and with n divisible by m, maps GF(3^n) into subfield GF(3^m) [9] according to the relation:

$$Tr_m^n(x) = \sum_{k=0}^{\frac{n}{m}-1} x^{3^{mk}}$$

The interleaving order I_P is: $I_P = I_P^0, I_P^1, \ldots, I_P^{S-1}$

with:

$$I_P^j = \begin{cases} i & Tr_m^n(\alpha^j) = \alpha^{Si} \quad i = 0,1,...,3^m - 2 \\ \infty & Tr_m^n(\alpha^j) = 0 \quad j = 0,1,...,S-1 \end{cases}$$

Example 4:

Let trace function from GF(3^4) onto GF(3^2) with primitive polynomial 10012: f(x) = x4 + x + 2 with: n = 4,L = 3^4-1 = 80; m = 2, N = 3^2-1 = 8, S = L/N = 10

Calculating the trace function of x from GF(3^4) into GF(3^2) we obtained:

$$Tr_m^n(\alpha) = \sum_{k=0}^{n/m-1} \alpha^{3^{2k}} = \alpha + \alpha^9$$

α^{Si} table:

i = 0 ⇨ $\alpha^0 = 1$
i = 1 ⇨ $\alpha^{10} = 1 + 2\alpha + \alpha^2 + \alpha^3$
i = 2 ⇨ $\alpha^{20} = \alpha + 2\alpha^2 + 2\alpha^3$
i = 3 ⇨ $\alpha^{30} = 1 + \alpha + 2\alpha^2 + 2\alpha^3$
i = 4 ⇨ $\alpha^{40} = 2$
i = 5 ⇨ $\alpha^{50} = 2 + \alpha + 2\alpha^2 + 2\alpha^3$
i = 6 ⇨ $\alpha^{60} = 2\alpha + \alpha^2 + \alpha^3$
i = 7 ⇨ $\alpha^{70} = 2 + 2\alpha + \alpha^2 + \alpha^3$

- With j run from 0 to S-1 we get:

j = 0 ⇨ $Tr(\alpha^0) = Tr(1) = 1 + 1 = 2 = \alpha^{40}$ ⇨ $I_P^0 = 4$

j = 1 ⇨ $Tr(\alpha^1) = \alpha + \alpha^9 = 2\alpha + \alpha^2 + \alpha^3 = \alpha^{60}$ ⇨ $I_P^1 = 6$

j = 2 ⇨ $Tr(\alpha^2) = \alpha^2 + \alpha^{18} = 2\alpha + \alpha^2 + \alpha^3 = \alpha^{60}$ ⇨ $I_P^2 = 6$

j = 3 ⇨ $Tr(\alpha^3) = \alpha^3 + \alpha^{27} = \alpha + 2\alpha^2 + 2\alpha^3 = \alpha^{20}$ ⇨ $I_P^3 = 2$

j = 4 ⇨ $Tr(\alpha^4) = \alpha^4 + \alpha^{36} = 2 + \alpha + 2\alpha^2 + 2\alpha^3 = \alpha^{50}$ ⇨ $I_P^4 = 5$

j = 5 ⇨ $Tr(\alpha^5) = \alpha^5 + \alpha^{45} = 0$ ⇨ $I_P^5 = \infty$

j = 6 ⇨ $Tr(\alpha^6) = \alpha^6 + \alpha^{54} = \alpha + 2\alpha^2 + 2\alpha^3 = \alpha^{20}$ ⇨ $I_P^6 = 2$

j = 7 ⇨ $Tr(\alpha^7) = \alpha^7 + \alpha^{63} = 1 = \alpha^0$ ⇨ $I_P^7 = 0$

j= 8 ⇨ $Tr(\alpha^8) = \alpha^8 + \alpha^{72} = 2 + \alpha + 2\alpha^2 + 2\alpha^3 = \alpha^{50}$ ⇨ $I_P^4 = 5$

j= 9 ⇨ $Tr(\alpha^9) = \alpha^9 + \alpha^{81} = 2\alpha + \alpha^2 + \alpha^3 = \alpha^{60}$ ⇨ $I_P^1 = 6$

- The interleaving order is:

$I_P = \{4, 6, 6, 2, 5, \infty, 2, 0, 5, 6\}$

4. The properties of ternary interleaved sequence:Although The statistic properties of interleaved sequence derived from p-ary m –sequences have been thoroughly discucessed, we will show some resutls for demonstration.

4.1 Correlation function:

Cross-correlation function (CCF): For generality we discuss the CCF $R_{a,b}(\tau)$. First, If a = b, we have autocorrelation function (ACF): $R_a(\tau)$

Let a,b ∈ A be two ternary sequences of the sequence set A. Both a,b are periodic sequences of length $L = 3^n-1$. The CCF between a,b: $R_{a,b}(\tau)$ is defined as:

$$R_{a,b}(\tau) = \sum_{i=0}^{L-1} \omega^{b_{i+\tau} - a_i} \quad , 0 \le \tau < L \qquad (22)$$

With $\omega = \exp\left(j\frac{2\pi}{3}\right)$ and $(i + \tau)$ is the addition mod L.

Similar, the ACF of the sequence a is

$$R_a(\tau) = \sum_{i=0}^{L-1} \omega^{a_{i+\tau} - a_i} \quad , 0 \le \tau < L \qquad (23)$$

For the ternary sequences, we have the following remark

Remark 1 : Let $\{a_i\}$ be a PN Sequence over GF(3^n) with period $L = 3^n-1$ and N_c, the ACF is given by:

$$R_a(\tau) = \begin{cases} 3^n - 1 & \tau = 0 \bmod (3^n - 1) \\ -1 & \tau \ne 0 \bmod (3^n - 1) \end{cases} \qquad (24)$$

if and only if the number N_c of times that the symbol c∈GF(3) occurs in one period of the difference sequence $\{a_i - a_{i+\tau}\}$ of sequence $\{a_i\}$ and its time-shift sequence $\{ a_{i+\tau} \}$, is:

$$N_c = \begin{cases} 3^{n-1} - 1 & c = 0 \\ 3^{n-1} \quad if & c = 1 \\ 3^{n-1} & c = 2 \end{cases} \qquad (25)$$

Example 5: Let $b(d) = 1 + d^3 + 2d^4$,

$\{b_n\}$ = {1 0 0 0 1 0 0 2 1 0 1 1 1 2 0 0 2 2 0 1 0 2 2 1 1 0 1 0 1 2 1 2 2 1 2 0 1 2 2 2
2 0 0 0 2 0 0 1 2 0 2 2 2 1 0 0 1 1 0 2 0 1 1 2 2 0 2 0 2 1 2 1 1 2 1 0 2 1 1 1}

ACF of the sequence b is

$$R_b(\tau) = \sum_{i=0}^{L-1} \omega^{b_{i+\tau} - b_i} \quad , 0 \le \tau < L$$

$R_b(\tau)$ = {80, -1, -1, -1, -1, -1, -1, -1,-1,-1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -l, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1)

with $a(d) = 1 + d + 2d^2 + 2d^3 + 2d^4$,

$\{a_n\}$ = {1 0 0 0 1 2 2 1 1 1 0 0 2 2 0 1 0 0 1 0 1 0 2 2 1 0 2 1 2 1 1 0 1 1 1 1 2 1 0 1
2 1 0 1 2 1 1 2 2 2 0 0 1 1 0 2 0 0 2 0 2 0 1 1 2 1 1 2 1 2 2 0 2 2 2 2 1 2 0 1}

The CCF between a,b:

$$R_{a,b}(\tau) = \sum_{i=0}^{L-1} \omega^{b_{i+\tau} - a_i} \quad , 0 \le \tau < L$$

$R_{a,b}(\tau)$ ={-1, 8, -10, 8, 26, -19, -1, -19, 8, -10, -1, -1, -1, -19, -10, -1, 8, -1, -1, -10, -10, -10, -l,-1, 17,-1,8, 8,-1, 8,-10,-19, 8,-1,-10,-1.-10,-1, 8, 8, 8,-1, 8, -1,17,8,-1, 8,-1,-10,-1,8, -10, 8, 8, -10, -1, 8, -1, -10, -1, -1, -1, -10,17,8, -10, -1, -10, 8, 8, 8, -1, 8, 8, 8, -1, -10, -10, 8}

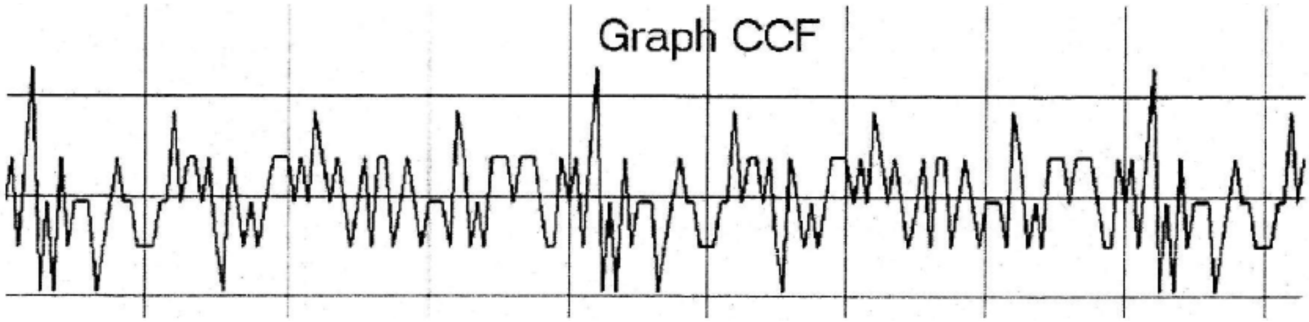

Fig 2: The CCF diagram of example 5

4.2 Distribution : the uniform allocation of q-ary digits in the sequence is another important property of q-ary m-sequence and has been discussed very clearly in [6,12,13,14...].Overall speaking, the distribution of q-ary msequences are very good.

5. Conclusion and future work

In this paper, the procedure to construct the ternary interleaved sequences having ideal ACF and good distribution is presented. This procedure is based on d-transform which is applicable for all periodical sequences with the period L being an integer. This is clearly the big advantage as compared to the trace function method, which is valid only for $L = q^n - 1$. The basic concept of this procedure is rather simple:we derive the interleaving order (shift sequence) of the component sequences $\{a_n\}$ to create the composite sequence $\{b_n\}$ based on the time multiplexed concept which is known to every engineer!

The result are fully identical with other well known methods.In order to get a clear picture of ternary interleaved m-sequence ,some statistic properties of the constructed sequence are investigated. It is shown that the statistic properties of ternary interleaved sequences are very good in term of correlation function and distribution.

Howerver,these merits are far from enough for the sequences to be used in such application like :cryptography,which requires among other the non-linearity!Therefore, many non-linear interleaved sequences,generated by different kinds of shift registers are proposed recently [3,5,6,12,16,17,18,19,20...].

In our future reseach,we will focus on the following directions:

- algorithms to generate non-linear sequences..(to make shift registers sequences non linear!)
- analysis of the characteristics of the newly generated sequences
- methods to attack these sequences...
- hardware implementation of the above mentioned sequences..

We hope to present the results in the new contributions.The authors express their deep sense of gratiude to the unknown reviewers for their encouraging comments and instructions.

Reference

[1] The LTE 10A Air Interface Ericsion 2009.

[2] Moving Forward to LTE-Advanced with Heterogeneous Networks 2013 Agilent Technologies

[3] LIM.T et al (2011) “New Construction of Quaternary Sequences with Good CorrelationUsing Binary Sequences with Good Correlation “ IEICE Trans .Fundamentals,,vol. e94-a,no8-August 2011,p 1701-1705

[4].Tang X.H, Fan F.Z.(2001): "A class of PN sequences over GF (P) with low correlation zone", *IEEE Trans. Inform. Theory*, vol.41, no.4, pp. 1644-1649, May 2001.

[5]. Gong. G (1995): "Theory and application of q-ary interleaving sequences." *IEEE Trans. Inform. Theory*, vol41, pp. 400-411, March 1995.

[6] Tasheva A. T (2011) et al "Generalization of the Self-Shrinking Generator in the Galois Field GF(p^n)" Hindawi Publishing Corporation Advances in Artificial Intelligence p1-10 2011

[7] Lin X.D. and.Chang K.H (1997): "Optimal PN sequences design for quasisynchronous CDMA communication systems", *IEEE Trans. Comm*.vol 45. pp 221-226. Feb 1997

[8]. LIDL .R &. Niedemeiter. H (2000), "Introduction to finite field and their application", Cambridge University press 2000.

[9] McEliece R. J.(1987), "Finite Field for Computer Scientists and Engineers". Boston, MA: Kluwer, 1987.

[10] Gill A (1996), Linear sequential circuits, Mc Grahill Newyork 1996.

[11] Gitlin R.G & Hayer J. F (1975), "Timming recovery and scramblers in data transmission", Bell Syst Tech Journal, vol 54, no3, pp 589-593, March 1975.

[12].Quynh L.C,Prasad. S(1985): "A class of binary cipher sequences with best possible correlation funtion." IEEE Proceeding Part F .Dec 1985. vol 132.pp.560-570

[13]. Hieu L.M &. Quynh L.C: "Design and Analysis of Sequences with Interleaved Structure by d-Transform," IETE Journal of Research, vol. 51, no. l, pp.61-67, Jan-Feb. 2005.

[14] He. . J (2013)" Interleaved Sequences Over Finite Fields "PhD thesis Carleton University Ottawa, Ontario 2013

[15] Perterson R.L, Zeemer R.E & Both D.B (1995)," Introduction to spread spectrum", Prentice Hall Int Inc 1995.

[16] Meier, W., Staffelbach, O.(1995), "The self-shrinking generator", Advances in Cryptology - EUROCRYPT '94, 1995, pp. 205-214.

[17].Krawczyk. H (1994) "LFSR based hashing and authentication" Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes In Computer Science; Vol. 839, pp. 129 – 139, 1994

[18]. Bruen A.A and. Mollin R.A (2009) "Cryptography and Shift Registers", The Open Mathematics Journal,2009, 2, 16-21

[19] Kanso, A.(2010)," Modified self-shrinking generator", Computers and Electrical Engineering, 36 (5), 2010, pp. 993-1001.

[20] Tasheva, A (2012)., "Some cryptanalysis of a p-ary Generalized Self-Shrinking Generator", ACM International Conference Proceeding Series, 2012, pp. 126-133.