Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

7th International Conference
on Electrical Engineering
ICEENG 2010

Joint Demodulation and Detection of Covert Modulated M-sequence

By

Dr. Ahmed S. Badawy*

Dr. Ahmed K. Sadek**

Abstract:

The paper Present a new receiver for detection of covert M.sequence regardless the chip code sequences and the type of modulation. A Higher Order Statistics (HOS) based on the Kurtosis of the received signal is used to classify the type of the modulation, and so decide the modulator. The Triple Correlations Function (TCF) of M. sequence of the demodulated which differs from sequence to another according to the feedback connection is used to decide the generation function g (x) from the peak position of this M-sequence. This paper is classified into four sections the first section, we introduce some property of modulation and how the (TCF) of the M.sequence generated. Secondly, the digital modulation classification is classified and tabulated using theoretical cumulants Statistics C_{40}, C_{42}. The Triple Correlation function (TCF) of M.sequence is showed in section three. Computer simulation of determination of feedback polynomial y(x) at section four. Finally, the conclusion is presented in at the rest of this paper.

Keywords:

Digital Communication, Higher Order Statistics (HOS) and M-Sequence.

* Egyptian Armed Forces
** Alexandria University, Faculty of Engineering, Alexandria, Egypt.

1. Introduction:

There has been separate work in the problems of modulation classification [1,2] and detection of covert M-seq. In [3,4] a method for detecting the M-seq. and finding its code generating function g (x) was presented[5]. Its was shown that even if we receive a truncated copy of the signal we can still (to a limit) be able to find the feedback polynomial. The method presented in the paper assumed that the kind of modulation is known and assumed BPSK.

In [6,7] a simple method based on elementary fourth-order cumulants, is proposed for the classification of digital modulation schemes. These statistics are natural in this setting as they characterize the shape of the distribution of the noisy baseband I and Q samples. It is shown that cumulant-based classification is particularly effective when used in a hierarchical scheme, enabling separation into subclasses at low signal-to-noise ratio with small sample size.

In our paper presents receiver for detecting M-seq. if the chip code sequences are unavailable and the type of modulation is unknown, A simple method based on the kurtosis of the received

signal is used to classify the type of demodulated signal. Then the Triple correlation function is used to decide the generating function g (x)[5].

2. Digital modulation classification:

This method uses the zeroth lags of the 4th order cumulated as follows:

For a complex-valued stationary random process y(n), second-order moments can be defined in two different ways depending on placement of conjugation.

$$C_{20} = E\left[y^2(n)\right] \quad \text{And} \quad C_{21} = E\left[\left|y(n)\right|^2\right] \qquad (1)$$

Similarly, fourth-order moments and cumulants can be written in three ways. Thus, fourth-order cumulants can be defined as

$$C_{40}=\mathrm{cum}(y(n), y(n), y(n), y(n))$$

$$C_{41}= \mathrm{cum}(y(n), y(n), y(n), y^*(n))$$

$$C_{41}= \mathrm{cum}(y(n), y(n), y^*(n), y^*(n)) \qquad (2)$$

The statistics in (1) and (2) are the zeroth lags of the correlations and fourth-order cumulants of y(n). For zero-mean r.v.'s , w,x,y, and z, the fourth-order cumulant can be written as

cum(w,x,y,z)=E(wxyz) – E(wx)E(yz) – E(wy)E(xz) – E(wz)E(xy) (3)

We can use (2) to express C_{40}, C_{41} , or C_{42} in terms of the fourth-and second-order moments of y(n), with the appropriate conjugations. See [7] for further details.

$$c_{20} = \frac{1}{N}\sum_{n=1}^{N} y^2(n) \tag{4}$$

$$c_{21} = \frac{1}{N}\sum_{n=1}^{N} |y(n)|^2 \tag{5}$$

Where the superscript ^ denotes a sample average. This leads to the following estimates:

$$\hat{c}_{40} = \frac{1}{N}\sum_{n=1}^{N} y^4(n) - 3\hat{c}_{20}c_{21} \tag{6}$$

$$\hat{c}_{41} = \frac{1}{N}\sum_{n=1}^{N} y^3(n)y'(n) - 3\hat{c}_{20}c_{21} \tag{7}$$

$$\hat{c}_{42} = \frac{1}{N}\sum_{n=1}^{N} |y(n)|^4 - |\hat{c}_{20}| - 2\hat{c}_{21}{}^2 \tag{8}$$

We will assume, without loss of generality (wlog), that the constellations are normalized to have unit energy, implying that C_{21} =1 . In practice, we estimate the normalized cumulants

$$\tilde{c}_{4k} = \frac{\hat{c}_{4k}}{\hat{c}_{21}{}^2} \qquad k = 0,1,2 \tag{9}$$

This self-normalizes the cumulant estimates and removes an scale problems in the data. The complexity of (8) and (9) is of order N , requiring only about 2N and 4N complex multiples for $\hat{c}_{40}$ and $\hat{c}_{42}$, respectively. In the case of noisy data, $\hat{c}_{21}$ in (9) must be replaced by $\hat{c}_{21} - \hat{c}_{21,g}$, where $\hat{c}_{21}$ is still given by (2) and $\hat{c}_{21,g}$ is an estimate of the variance of the additive noise g(n); an estimate of $\hat{c}_{21,g}$ is usually available in practice. Theoretical values of the 4th order Cumulants for various signal constellation of integers are computed for noise free signals, these value are used for the detection procedure [6].

Table 1:

Theoretical Cumulant Statistics C_{40} and C_{42} For Various Constellation Types, And Variance of Their Sample Estimates

Constellation	C_{40}	C_{42}	N var ($\hat{C}_{40}$)	N var ($\hat{C}_{42}$)	N var1 ($\hat{C}_{42}$)
BPSK	-2.0000	-2.0000	0.00	0.00	36.00
PAM(4)	-1.3600	-1.3600	2.56	2.56	34.72
PAM(8)	-1.2381	-1.2381	4.82	4.82	32.27
PAM(16)	-1. 2094	-1.2094	5.52	5.52	31.67
PAM(32)	-1.2024	-1.2024	5.70	5.70	31.52
PAM(64)	-1.2006	-1.2006	5.74	5.74	31.49
PAM(∞)	-1.2000	-1.2000	5.76	5.76	31.47
PSK(4)	1.0000	-1.0000	0.00	0.00	12.00
PSK(>4)	0.0000	-1.0000	1.00	0.00	12.00
V32	0.1900	-0.6900	2.86	1.18	9.70
V29	0.5185	-0.5816	3.51	1.77	8.75
QAM(∞)	-0.6000	-0.6000	3.91	2.31	8.59
QAM(32,32)	-0.6012	-0.6012	3.89	2.29	8.61
QAM(16,16)	-0.6047	-0.6047	3.83	2.24	8.65
QAM(8,8)	-0.6191	-0.6191	3.58	2.06	8.82
QAM(4,4)	-0.6800	-0.6800	2.66	1.38	9.54
V29c	-1.2000	-0.6400	1.85	1.44	9.12
8AMPM	-0.5600	-0.7200	2.66	1.38	9.54

The constellations in Table 1 naturally divide into the following four subclasses: binary PSK (BPSK) (binary real-valued), PAM (real-valued), PSK (constant-modulus), and QAM-V29-V32 (general complex-valued). We therefore propose a hierarchical classification structure which is shown in Fig. 1. We use C_{42} first to decide whether the constellation is real-valued (BPSK/PAM), circular (PSK), or rectangular (QAM). Then, if the unknown phase rotation can be assumed to be small, C40 may be used to help differentiate within each subclass. If the unknown phase rotation cannot be ignored, then must be used rather than C40. As we see from Table 1, when using, there is a potential performance loss in some cases, e.g., V29 versus QAM (8,8). If the initial decision is PSK, we use to decide whether it is PSK (4) [QAM (2, 2)] or PSK (>4). Similarly, if the initial decision is QAM, we use C40 or to decide whether it is V32, V29, QAM (8, 8), QAM (4, 4), or V29c. If the unknown phase rotation can be assumed to be small, we can distinguish between PSK (2), PSK (4), and their rotated versions.

Note that the value of C40 for QAM (8, 8) and QAM (4, 4) are close to one another; may be a better statistic. The hierarchical approach attempts to first classify the data using “macro” characteristics as shown in figure(1); it then refines the membership using “micro” characteristics, in the spirit of which considered the three-class BPSK/quaternary PSK (QPSK)/offset QPSK problem.

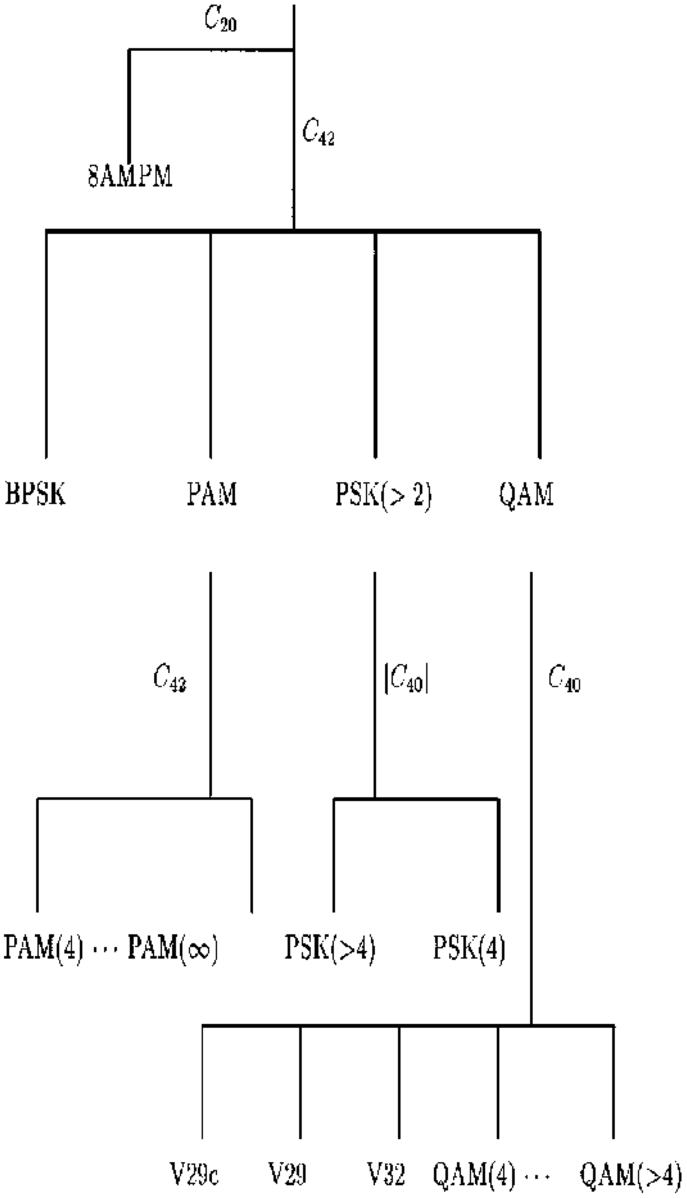


Figure 1. *Hierarchical classification scheme based on HOS.*

Form the table it is obvious that the variances of $\hat{c}_{40}$ are approximately the same, justifying the use of threshold detector.

3-Triple correlation of M-sequences:

Previous work [3,4] showed that each feedback connection [m-sequence] have a certain peak locations, which differ from sequence to another. This property was used to detect covert signals through finding the locations of the peaks.
If we have an m-sequence, u = {u (1), u (2), u (L)}, u (i) ∈ 0 , 1
We can define the vector, v = {v (1), v (2), v (L)},
such that v(i) =1 If u(i) =0 and v(i) = 0 if u(i) = 1.
The Triple correlation of complete m-sequences is evaluated as follows,

$$C_U(p,q) = \frac{1}{L}\sum_{i=1}^{L} v(i)v_p(i)v_q(i) \qquad (10)$$

The shift and add property states that for certain delays (p', q'), $u_{p'} \oplus u_{q'} = u$

It follows that for all i , $v_{p'}(i)v_{q'}(i) = v(i)$. For these delays the triple correlation has the following value,

$$C(p',q') = \frac{1}{L}\sum_{i=1}^{L}\left(v(i)\right)^2 = 1 \qquad (11)$$

For other (p,q) pairs, vp* vq= Vs where Vs closure, in such case

$$C(p',q') = \frac{1}{L}\sum_{i=1}^{L} v(i)v_s(i) = \frac{-1}{L} \qquad (12)$$

The location of the peaks differs from a feedback connection to another as shown in figure(2) and figure(3) for connection-1[1 1 1 1 0 1] and connection-2[1 0 1 1 1 1] respectively, and so they represent a deterministic feature for each sequence. Figures (2,3) show also the mesh and peaks locations for each m-sequences without noise and have the complete length used in our analysis.

Our propose at first find the kind of the modulation ,in this case ,the kind of modulation is BPSK (m-sequence) as shown in figure (2). The second we calculate the triple correlation function (TCF), C (p, q), using equations (8)and(9) of the received signal which figured in figures (3,4) . The final step used to find the determination of feedback polynomial g(x) from the triple correlation peak location using computer simulation.

4- Determination of feedback polynomial g(x) from Triple Correlation Peak Location:

In this section we will show a reconstruction method, which is, in general much easier than aforementioned direct-decomposition approach [4].

Let (r_1,s_l), (r_2,s_2,…..,L-1,sL-1) be all the peak positions of the triple correlation of some m-sequence. From the number L-1 of peaks as shown in figure (4), the length or equivalently the degree of the feedback connection of the m-sequence can be recovered by the equation L= 2n- 1 , m- sequences are L-periodic. In particular, L must be known to evaluate the TCF C (p , q).

However, there is evidence that sufficiently long partial m- sequence produce good estimation of peak locations.

L may me derived from the peak locations (i,j), (2j,2j),... ,(2k j,r) for i <j , r < 2k j mode(L) , or L = 2k .

For an example the pairs (1,20) , (2,9) would produce L as L= 2 x 20 - 9 = 40 - 9 = 31.

Every peak position (ri,si) corresponds to a polynomial satisfying $f_i(\alpha) = 0$

$$f_i(x) = x^{r_i} + x^{s_i} + 1 \tag{13}$$

Assume that f(x) is the feedback connection of the m-sequence, then f (α)=0 and f(x) divides gcd$\{f_i(x), f_j(x), f_z(x)\}$ for all possible $\subseteq$ {1,2,1}, where gcd [a(x) ,b(x)] is the popular greatest- common-divisor, which has a smaller degree and can which has a smaller degree and can be easily calculated. Because of the identity gcd[a(x),b(x), c(x)]= gcd{[a(x),b(x)], c(x)}, the gcd $\{f_i(x), f_j(x), f_z(x)\}$

can be easily determined in recursion. If we are lucky to find
h(x) = gcd$\{f_i(x), f_j(x), f_z(x)\}$

of degree n, then this polynomial h(x) is just the wanted feedback connection of the m-sequence. If, unfortunately, every possible gcd$\{f_i(x), f_j(x), f_z(x)\}$ has its degree larger than n, we now choose, among such polynomials, one of the smallest degree [5] to this polynomial of such smaller degree.

5- Computer Simulation:

In order to show the superiority of our new approach, we consider an example. Let { b(i), $0 \leq i \leq 30$} be the m-sequence with feedback f(x)=1+x+ x2+ x3+ x5 . After running the program of m-sequence the output gives the peak positions of this m-sequence are (1,12),(12,1), (2,24), (24,2), (3,8), (8,3), (4,17), (17,4), (5,28), (28,5), (6,16), (16,6), (7,9), (9,7), (10,25), (25,10), (11,30), (30,11), (13,27), (27,13) ,(14,18), (18,14), (15,21), (21,15), (19,20), (20,19), (22,29), (29,22), (23,26), (26,23) as shown in figure (6). Now we will use the new approach to reconstruct the feedback connection f(x) based only on these 30 peak positions.

At first from the number 30, we get the length L-1 = 30, we get L=31 of the m-sequence, or equivalently deg f(x) = 5. On the other hand, among the 30 polynomials, $0 \leq i \leq 30$, corresponding to the peak positions {(ri,si): $0 \leq i \leq 30$}, the polynomials a(x) = $1+ x^3+ x^8$ and b(x) = $1+ x^7 + x^9$, corresponding to the peak positions (3,8) and (7,9) respectively, are of the smallest degree degrees.

$$f_i(x) = x^{r_i} + x^{s_i} + 1 \tag{14}$$

It is lucky that gcd [a(x), b(x)]= $1 +x+ x^2+ x^3+ x^5$ is of degree 5, the expected degree of f(x), thus this polynomial is exactly the feedback connection of the given m-sequence. By the same way, if another peak location is known the primitive g(x) can be solved. Moreover, as previously explained, it is possible to derive the actual polynomial generator function from the positions (p,q) of a very limited number of peaks.

Conclusion:

We have shown that Higher Order Statistics are useful for classification and detection of digitally modulated signals. They are practically effective when use in hierarchically scheme, allowing broad classification at low SNR. Also we have shown that Triple correlation function in generally much easier method to find the original feedback polynomial g(x).

Reference:

[1] John G. Proakis Digital Communications 4th edition, McGraw-Hill, 2001.

[2] G.R. Cooper & C.D. Mc Gillen. “Modern Communication and Spread Spectrum”, MC Graw – Hill, 2nd printing 1988.

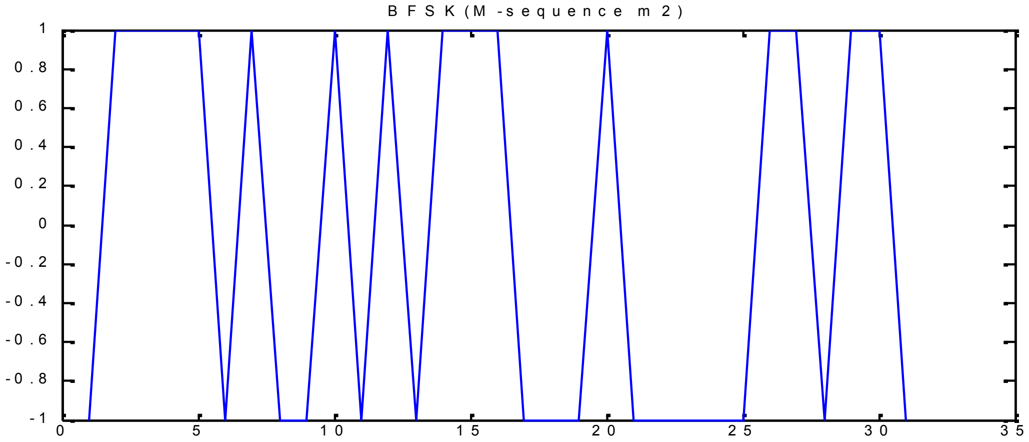
[3] J. M. Mendel, “Tutorial on Higher – Order Statistics (Spectra) in Signal Processing and System Theory: Theoretical and some Applications,” Proc. of IEEE, Vol. 79, No.3 March 1991.

[4] M.E.Gouda, E.R.Adams & P.C.Hill, “Estimation & Identification Techniques for DS/SS signals”, Proceedings of IEEE 32nd IECON 97, New Orleans, USA, Nov. 1997 pp.311-315.

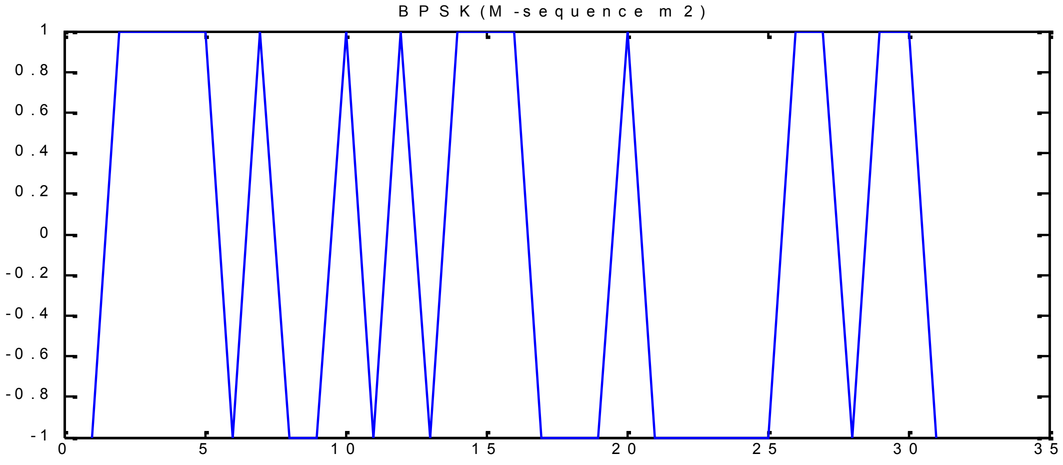
[5] M.E.Gouda, E.R. Adams & P.C. Hill, "Detection & Discrimination of Covert DS/SS Signals Using Triple Correlation,” Proceedings of IEEE 15th NRSC 98, Cairo, Egypt, Feb.1998.

[6] Walter Akmouche " Detection of multicarrier modulations using 4th-order cumulants",MILCON,1999.

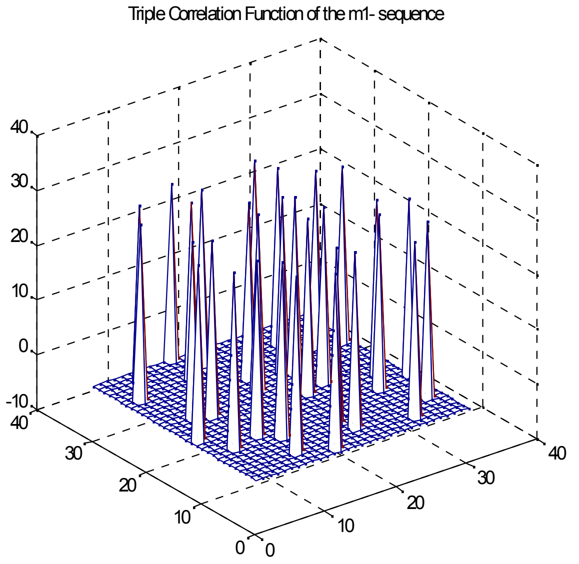
[7] A. Swami and M. Sadler, "Hierarchical Digital Modulation Classification Using Cumulants"IEEE Transaction on Communications ,Vol. 48, No. 3, March 2000.



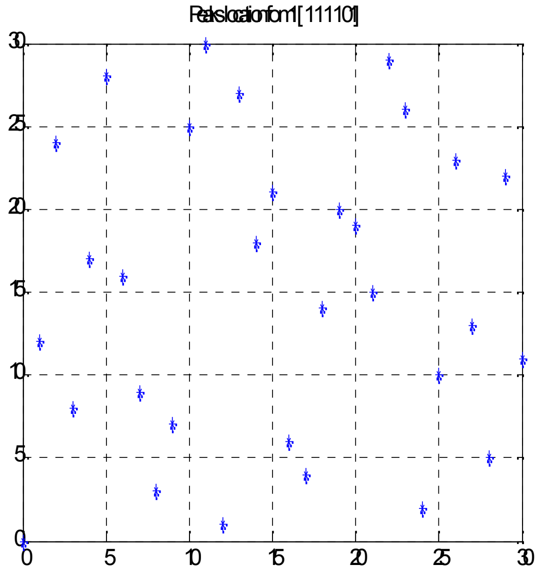
Figure(2-a) *BFSK signal (m-sequence 1 f(x)=1+x+x2+x3+x5)*



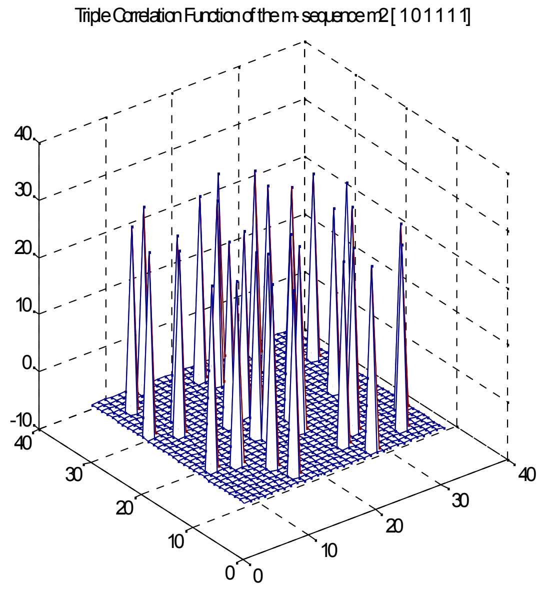
Figure(2-b) *BFSK signal (m-sequence 2 f(x)=1+x2+ x3+ x4+ x5)*



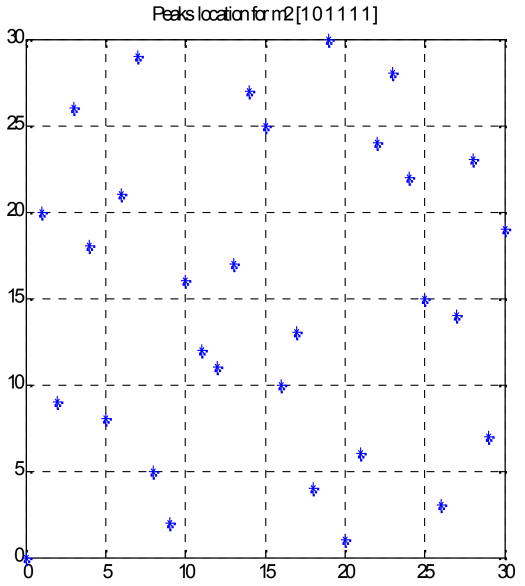
Figure(3-a) *Mesh of Tripe correlation function*
w.r.t. (m-sequence 1 f(x)=1+x+x2+x3+x5)



Figure(3-b) *Mesh of Tripe correlation function*
w.r.t. (m-sequence 1 f(x)=1+x+x2+x3+x5)



Figure(4-a) *Mesh of Tripe correlation function*
w.r.t. (m-seq. 2 f(x)=1+x+x2+x3+x4+x5)



Figure(4-b) *Mesh of Tripe correlation function*
w.r.t. (m-seq. 2 f(x)=1+ x2+ x3+x4+x5)