Paper: ASAT-13-CM-41

13th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT- 13, May 26 – 28, 2009, E-Mail: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel : +(202) 24025292 – 24036138, Fax: +(202) 22621908

Code Detection and Acquisition Techniques in the DS/CDMA Communications

K. A. El-Barbary*, E. A. ElWaniss*, A.O. Abd El Azziz**

Abstract: In the direct sequence- code division multiple access (DS/CDMA) communications, one of the primary functions of the receiver is to despread the received PN code. This is accomplished by generating a local replica of the PN code in the receiver and then synchronizing it to the one superimposed on the received waveform. In general, this synchronization process is accomplished in two steps are; *code acquisition,* which is a coarse alignment process bringing the two PN sequences within one chip interval, and *code tracking*, which is a fine tuning and synchronization-maintaining process. However, in many situations, such as communications intelligence, the PN code utilized to spread the received signal is unknown to the intercepting receiver. In this paper, we focus on the fundamental concepts of both code estimation and code acquisition techniques. An algorithm based on the higher order statistics (HOS) for code estimation is provided. This HOS algorithm is complex and requires high signal to noise ratio, SNR for operating correctly. For that reason a much simpler algorithm based on the structure of the PN code itself and short observation of the received signal is proposed. The proposed algorithm, based on short observation, performs faster and better than the HOS algorithm, especially in dense environments. Finally we compare the serial search, the parallel search and the Z- search methods, in terms of the average delay time to acquire code acquisition for different spreading code lengths.

Keywords: Direct Sequence- Code division Multiple Access (DS/CDMA) Communications, Higher order statistics and Short observation, Algorithms for code Detection, Code acquisition Techniques, Serial vs. Parallel and Z- Search Strategies

I. Introduction

For all the code division multiple access (CDMA) protocols, it is important that a distinguish codes are assigned to the different users. Thus it is possible to separate between the signal of a desired user and the signals of other interfering users. Usually the separation is made by correlating the received signal with a locally generated code of the desired user. The auto correlation of the code is also a very important aspect because this decides how well we are able to synchronize and lock the locally generated code signal to the received signal. An ideal auto correlation function of a binary sequence would be an impulse function centered on zero time delay. However there are no code posses such impulse correlation function. The maximum length sequence (m-sequence) which is generated by linear feedback shift registers (LFSR) is a good approximation for such codes that is why it generally employed in CDMA systems. The most common realization of linear FSRs is shown in Fig.1. [1].

* Egyptian Armed Forces
** National defense council

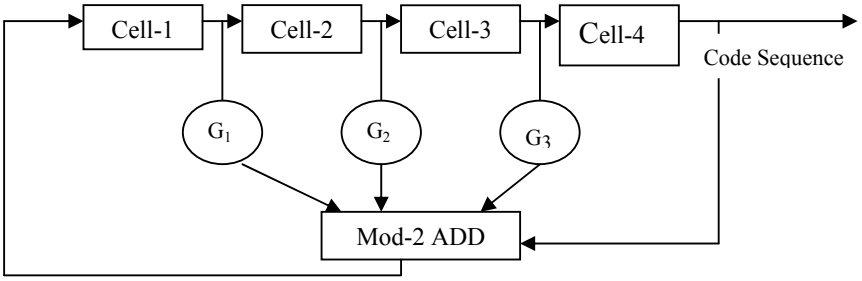


Fig. 1 Linear Feed Back shift register of order n=4

The FSRs consists of n-storage cells. Under the control of a clock pulse each cell moves its content to its output while reading its new content from its input. The input to the first cell in a non linear function (mod-2 addition) of the outputs of other cells weighted by the generator polynomial coefficients g_i , $1 \leq i \leq n$. The output of the n^{th} cell forms the desired code sequence $\{a_k\}$. A LFSR with n storage elements has a maximum length if it produces the longest possible sequence of length ($L = 2^n - 1$) before repeating itself.

A maximum length sequence (ML), usually called m-sequence is obtained by using a primitive polynomial *g(x)* as the generator polynomial for the code, where

$$g(x) = 1 + \sum_{i=1}^{n} g_i \, x^i \tag{1}$$

Where, g_i is a Binary coefficient equal *0* or *1* with $g_n = 1$.

The popularity of m-sequence is a result of the good auto-correlation and cross-correlation behaviors. For a two random variables *x* and *y*, the auto-correlation function and the cross correlation function are defined in equation (2) and (3) respectively as [3].

$$R_{xx}(\tau) = E\{x(t)\, x^*(t-\tau)\} \tag{2}$$

$$R_{xy}(\tau) = E\{x(t)\, y^*(t-\tau)\} \tag{3}$$

It is easy to show that the auto-correlation function of an m-sequence of length L is given by [3]

$$R_{aa}(\tau) = \begin{cases} 1 & \tau = 0, L, 2L \\ \frac{-1}{L} & otherwise \end{cases} \tag{4}$$

The auto correlation function for m-sequence of length 31 generated by either one of the primitive polynomials

$$g_1(x) = 1 + x^3 + x^5 \tag{5}$$

$$g_2(x) = 1 + x^2 + x^3 + x^4 + x^5 \tag{6}$$

is plotted in Fig. 2. The cross-correlation between the two codes is also plotted as dashed lines on the same figure. A good measure of the rejection of the signals of interfering users is the ratio *R* of the maximum cross correlation coefficient and the auto correlation coefficient. The smaller this ratio is the better the interfering users' rejection [4]. It is worth to note that the second order properties of two different sequences are exactly the same. Thus we can not utilize the second order properties to estimate the m-sequence at the receiver side. Consequently the higher order statistics are applied to distinguish the generating polynomial of the desired user. After estimation of the generator polynomial of the code the receiver starts to locally generate the dispreading code and synchronize and lock the locally generated code signal to the received signal.

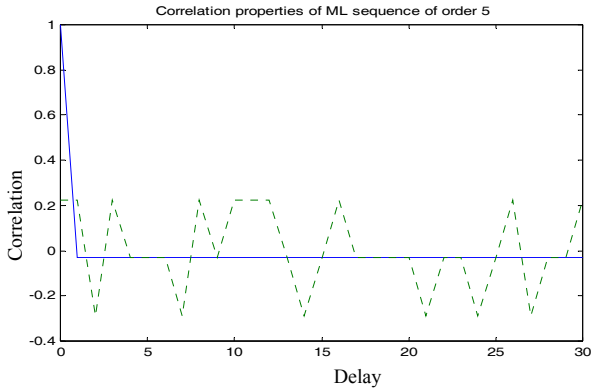


Fig. 2 Correlation properties of ML- sequence of length=31

$$g_1(x)=1+x^3+x^5 \;\;\&\;\; g_2(x)=1+x^2+x^3+x^4+x^5$$

In the active correlator system, the received signal *r(t)*, which is composed of the PN signal *s(t)* and noise *n(t)*, is first multiplied by the local PN code reference, and subsequently band pass-filtered (BPF) and square-law envelope detected, thereby dropping off the unknown modulated information and unknown carrier phase. The output is then integrated for the duration of τ_d seconds, sampled at interval τ_d, and finally used in making acquisition decision through comparison with threshold. This process is depicted in Fig. 3.

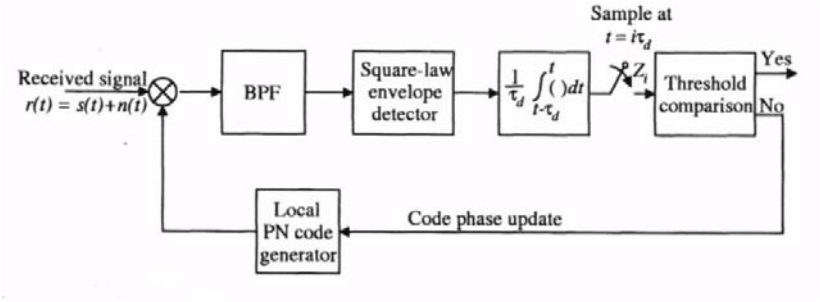


Fig. 3. Active correlator acquisition system

The rest of the paper is organized as follows; Section II provides an algorithm which utilizes the higher order statistics (HOS) for detection of m-sequence along illustration example and with simulation results. This HOS algorithm is complex and requires high signal to noise ratio, SNR for operating correctly. For that reason a much simpler algorithm based on the structure of the PN code itself and short observation of the received signal is provided in section III. Section IV provides comparison for code acquisition techniques as the serial search, the parallel search and the Z-search for the average time delay of each of the methods from the computer simulations for different code lengths. Finally section V provides the conclusion.

II- Higher order statistics for Detection tion of ML sequences.

The triple correlation function (*TCF*) of a random process, *a(t)*, is defined as [5]

$$C_{aaa}(\tau_1,\tau_2)=E\{a(t)\,a(t+\tau_1)a(t+\tau_2)\} \tag{7}$$

The shift and add property of the ML sequences shows that; for a specific shift, $\tau_1=\tau_k$ there is a unique shift $\tau_2=\tau_j$ which recreates the original m-sequence when the two delayed versions are multiplied. Thus for only one pair (τ_k , τ_j) the following equation holds

$$a(t+\tau_k)\,a(t+\tau_j)=a(t) \tag{8}$$

For Any other pair (τ_k, τ_l) ; $l \neq j$ then the product $a(t+\tau_k)\,a(t+\tau_l)$ produces a differently shifted version of the original signal, that

$$a(t+\tau_k)\,a(t+\tau_l)=a(t+\tau) \tag{9}$$

From equations (8) & (9) we can deduce that for a given first shift $\tau_1 = k$; $k= 1, 2,3,\ldots\ldots L$. The *TCF* $C_{aaa}(k,\tau_2)$ is

$$C_{aaa}(k,\tau_2)=\begin{cases}E\{a(t)a(t)\} & \tau_2=\tau_j \\ E\{a(t)a(t+\tau)\} & \tau_2\neq\tau_j\end{cases} \tag{10}$$

Remember the properties of the ML sequence equation (7) can be rewritten as

$$C_{aaa}(k,\tau_2)=\begin{cases}1 & \tau_2=\tau_j \\ \frac{-1}{L} & \tau_2\neq\tau_j\end{cases} \tag{11}$$

Where τ_j is the unique second shift corresponds to the first shift k which satisfies equation (8). To avoid ambiguity of the reader the principle of using *HOS* can be rewritten in a discrete format that the *TCF* is evaluated as [4], [5]:

$$C(r,s)=\frac{1}{L}\sum_{i=1}^{L} a(i)\,a_r(i)a_s(i) \tag{12}$$

where

$$a_r(i)=a(i+r) \qquad \& \qquad a_s(i)=a(i+s) \tag{13}$$

By the shift and add property of the m- sequence there is one and only one shift $s=s'$ corresponding to predetermined shift $r=r'$ such that

$$a_{s'}(i)\,a_{r'}(i)=a(i) \qquad for\, i=1,2,\ldots,L \tag{14}$$

$$a_s(i)\,a_{r'}(i)=a(i+k) \qquad for\ i=1,2,\ldots,\ L\,;s\neq s' \tag{15}$$

Hence we can deduce that the discrete TCF of the m-sequence is given by

$$C_{aaa}(r,s)=\begin{cases}1 & (r,s)=(r',s') \\ \frac{-1}{L} & otherwise\end{cases} \tag{16}$$

It is shown in that the peak locations (r', s') for the m–sequence depends on the generator polynomial $g(x)$ of the code. This fact is employed to detect the generator polynomial of the ML code from an intercepted observation as shown in the following subsection.

II-1 Determination of m-sequence using HOS algorithm

Consider the m-sequence is generated by a primitive polynomial $g(x)$ of order m. The primitive element α of the Galios field $GF(2^m)$ satisfies the relation [5]

$$g(\alpha)=0 \tag{17}$$

It is shown that if the shift pair (i,j) represents a peak location then

$$\alpha^i+\alpha^j=1 \tag{18}$$

Where + indicates the modulo-2 addition in Galois field. Furthermore it is proved that if (i , j) is a peak location then the pairs (i_0 , j_0) are also peak locations, where

$$i_0=2^k\,i \quad \text{mod}(\ L);\quad k=1,2,\ldots.. \tag{19}$$

$$j_0=2^k\,j \quad \text{mod}\ (L);\quad k=1,2,\ldots.. \tag{20}$$

As an example for the generator polynomial

$$g_a(x)=1+x^2+x^3+x^4+x^5 \tag{21}$$

The triple correlation function of the generated code with this primitive generator polynomial is plotted in Fig. 4.

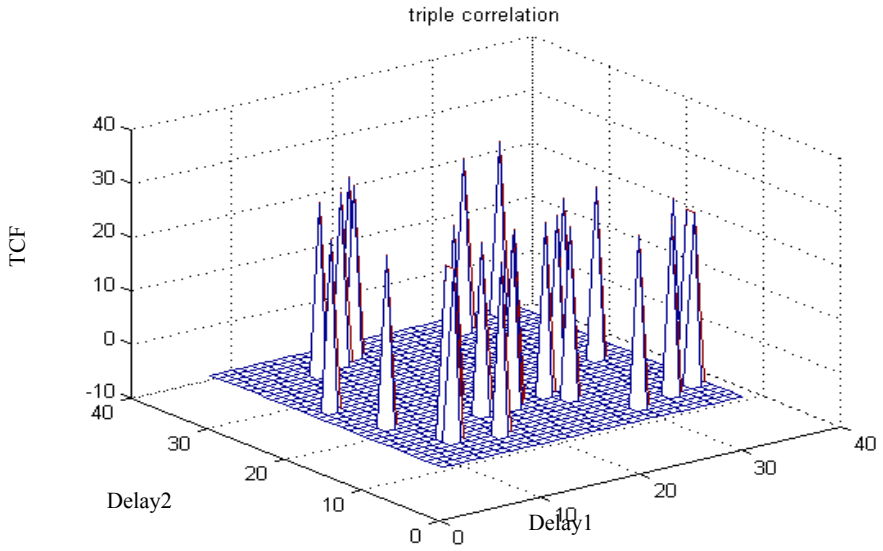


Fig.4. Triple correlation function for $g_a(x) = 1 + x^2 + x^3 + x^4 + x^5$

For the codes generated by the primitive polynomials;

$$g_b(x) = 1 + x^2 + x^5 \tag{22}$$

$$g_c(x) = 1 + x^3 + x^2 + x^4 + x^5 \tag{23}$$

Moreover the *TCFs* are computed using the equation (12).

A contour plots for the result of TCFs of the codes generated by $g_a(x)$, $g_b(x)$ and $g_c(x)$ are presented in Fig. 4. Clearly, the peaks location depends on the generator polynomials. Also we note the absence of any common peaks in the three plots. The interest results in [5] and [6] the proving that the observing of any 2 peaks location is sufficient to determine the generator polynomial.
To illustrate this result assume that only the two peaks (2,9) and (8,5) are observed then

$$\alpha^2 + \alpha^9 = 1 \quad \Rightarrow \quad \alpha^9 = \alpha^2 + 1 \tag{24}$$

$$\alpha^8 + \alpha^5 = 1 \quad \Rightarrow \quad \alpha^8 = \alpha^5 + 1 \tag{25}$$

Multiply both sides of (25) by α and substitute in (25) we get

$$\alpha^6 + \alpha^3 = \alpha^2 + 1 \quad \rightarrow \quad \alpha^6 = \alpha^2 + \alpha + 1$$

$$\alpha^5 = \alpha^8 + 1 = \alpha^2 \alpha^6 + 1 = \alpha^2(1 + \alpha + \alpha^2) + 1$$

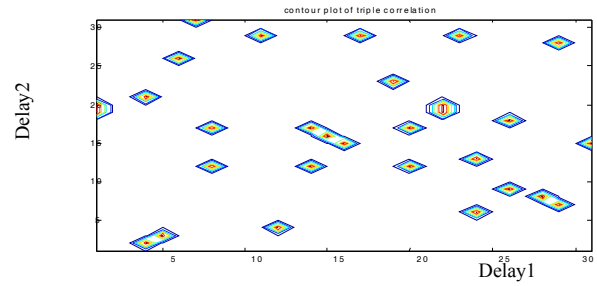
$$1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 = 0 \tag{26}$$

Since $g(\alpha) = 0$, the estimated generator polynomial is that one in equations (21). Two main reasons relies on the HOS is applied for estimation of the m-sequence generator polynomial namely [7] are;

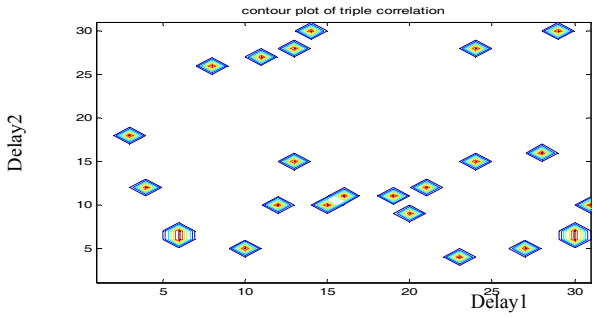
1- The one to one correspondence between the peaks location of the *TCF* and the generator polynomial of the code.
2- The HOS reduces the effects of additive white noise on the *TCF* of the observed signal. The authors [7] indicates that the method works satisfactory up to *3dB SNR*.

However the main disadvantages of this method could be summarized as follows.

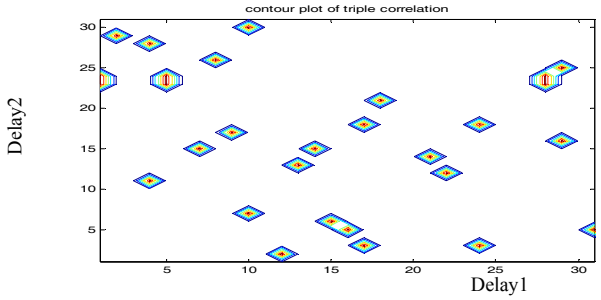
1- The complexity of computations is of order L^3
2- The peaks location detection is limited to positive values of *SNR* . In practices, specially in case of *DS/CDMA* there is multiple sources of interference such as other users, multipath, narrow-band signals and white noise. These interferences will reduce the overall signal-to-interference ratio *(SIR*) to extremely negative values where the algorithm based on *TCF* will not work. Fig. 6 shows the *TCF* of *ML*- sequence of *(L=31)* distorted by multipath interference (2 equal gain paths) and white noise. Evidently the peak location is complete distorted relative to that one in Fig. 5 for nopise absent case.



(a) $g_a(x)=1+x^2+x^3+x^4+x^5$



(b) $g_b(x)=1+x^2+x^5$



(c) $g_c(x)=1+x+x^2+x^4+x^5$

Fig. 5. Contour plot of the triple correlation functions

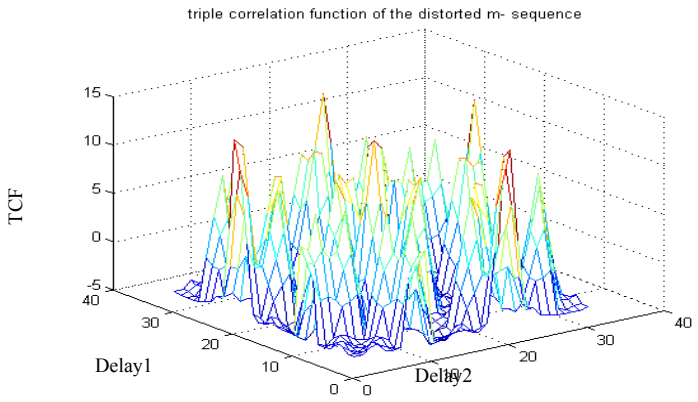


Fig. 6 Triple correlation function of distorted ML-sequence

III- Estimation of m- sequence using short observation

For the scheme of ML-code generation is discussed in section II, any outgoing code bit is dependent on the contents of the shift register cells and the generator polynomial coefficients g_i , $i= 1,2,....,n$. In other words the k[th] outgoing code bit "a_k" is a modulo- 2 linear combinations of the previous n-outgoing code bits $(a_{k-1}, a_{k-2}, \ldots\ldots a_{k-n})$ and the generator polynomial coefficients $(g_1 , g_2 , \ldots\ldots\ldots g_n)$. We can write that:

$$a_k = a_{k-1}g_1 + a_{k-2}g_2 + \ldots\ldots + a_{k-n}g_n \qquad (27)$$

where + indicates the module-2 addition and ai,gi have only the values zero or one. Equation (27) could be rewritten in decimal format as

$$a_k = rem\left(\sum_{i=1}^{n} g_i\, a_{k-i}\ ,2\right) \qquad (28)$$

This inter property between the ML sequence bits encourage us to provide a simple algorithm to estimate the generator polynomial of the ML-code based on a short observation contains only ***2n*** successive code bits. The proposed algorithm is summarized as follows.

1- Assuming that ***2n*** successive code bits are received correctly.

2- Construct the system of n- equations in the n- unknowns p_i ,$i=1,2,\ldots n$ which is given by;

$$a_k = \sum_{i=1}^{n} p_i\, a_{k-i} \qquad k = n+1, n+2, \ldots\ldots 2n \qquad (29)$$

In equations (29) the sum is binary and the resulting n- equations are solved using *matrix simple row operations with module-2 addition and multiplication.*

3- The system of equations (29) has one and only one solution which is $p_i = g_i$; $i=1,2,\ldots.n$ since the LHS of equations (27) and (29) have the same values and the RHS is a direct replacement of gi by p_i.

Clearly we utilizes the later part of the observation (last observed n-bits) as a function of the first observed n-bits to determine the generator polynomial.

III-1 Effect of interference on the behavior of proposed algorithm.

In presence of interference such as noise, multiple access and multipath the received signal is represented as

$$r_k = a_k + n_k \qquad (30)$$

where n_k is a Gaussian random variable with zero- mean and variance σ_n^2. Since the useful signal is a ML-sequence ($a_k = \pm 1$). The signal to noise ratio (SNR) is simply calculated as

$$SNR = 10\log\left(\frac{1}{\sigma_n^2}\right) = -10\log(\sigma_n^2) \qquad (31)$$

In order to operate the proposed algorithm a pre-decision must be taken on the observed signal r_k. It is well kwon that the maximum likelihood decision rule is applied to minimize the probability of decision error[3],[7]. The received signal model could be consider as an antipodal signaling scheme. Thus the Maximum likelihood decision rule will be;

$$\hat{s}_k = \begin{cases} 1 & r_k \geq 0 \\ -1 & r_k < 0 \end{cases} \tag{32}$$

The resultant bit error probability pe for the antipodal signaling scheme is given by [7];

$$p_e = Q\left(\sqrt{SNR}\right) \tag{33}$$

where the Q function is defined as;

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp(-\frac{x^2}{2}) dx \tag{34}$$

The probability of correct decision for any bit is;

$$p_c = 1 - p_e \tag{35}$$

In order to run the proposed algorithm correctly we need ***2n*** successive correctly decided bits, thus the probability of correct estimation of the generator polynomial of order ***n*** is given by;

$$p_{c-est} = p_c^{2n} = \left[1 - Q(\sqrt{SNR})\right]^{2n} \tag{36}$$

Fig. 7 shows $P_{c\text{-}est}$ versus the SNR with n as a parameter. It is clear that for certain order, *n* the $P_{c\text{-}est}$ increases as the SNR increase. Also the Pc-est is much greater for smaller values of ***n*** for the same SNR . This result does not disturb us since if a failure occurs during choise of data frame of length ***2n*** we can repeat the trial with another frame and the proposed algorithm is still much simpler than that one based on the HOS. The figure also shows the probability of correct estimate versus the SNR for both cases of single trial and 5 repeated trials. One can see that the estimate of the generating code polynomial is *100% correct* for *SNR* greater than *10 dB* in case of sigle trial while it is sufficient to have *SNR* greater than *5 dB* in case of 5 trials.

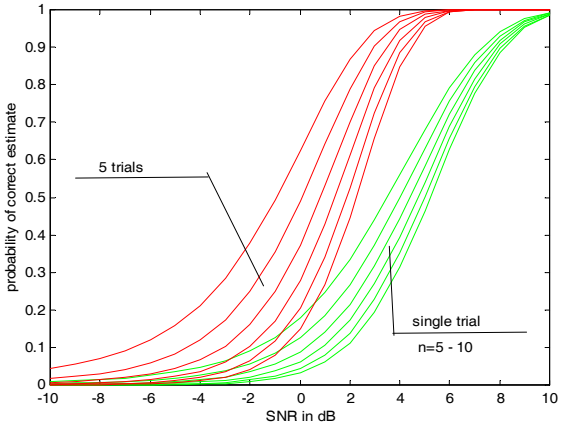


Fig. 7 Probability of Correct Estimation of code generating polynomials

Finally it is worth to mention that the complexity of the proposed algorithm is of order n^2 compared to order of L^3 in case of HOS. Clearly the comparison is quite fair for our proposed algorithm. Moreover in case of poor signal-to noise ratio, both the proposed algorithm and that one based on HOS (triple correlation function) suffers of erroneous bits. This problem is solved in the proposed algorithm by repeated trials which enhances the probability of capturing a non-distorted frame and consequence a correct estimate of the generator polynomial. Of course this enhancement is obtained on the expanse of increasing the computational complexity.

IV- Serial vs. Parallel and Z- Search Strategies

The serial search is the widely used technique for initial synchronization. All the potential code phases and frequencies are serially until the correct phase and frequency are identified. Correctness of phase/frequency is determined by attempting to despread the received signal: If the estimated code phase and frequency are both correct, dispreading will be properly done and thus a high energy output will be sensed. Otherwise, dispreading will not be done properly and the resulting energy will be low. Fig. 8 depicts a realization of the maximum-likelihood serial search technique: First, the correlation between the local PN code and the received PN sequence is calculated and stored. Then, the local PN code phase shifts to the next code phase and the same operation is conducted. This process is repeated until all the q cell uncertainty region is examined, or, equivalently, for all $t = i\tau_d$, $i = 1, 2, ..., q$. Finally, the code phase that yields the maximum correlation value is selected as the correct one.

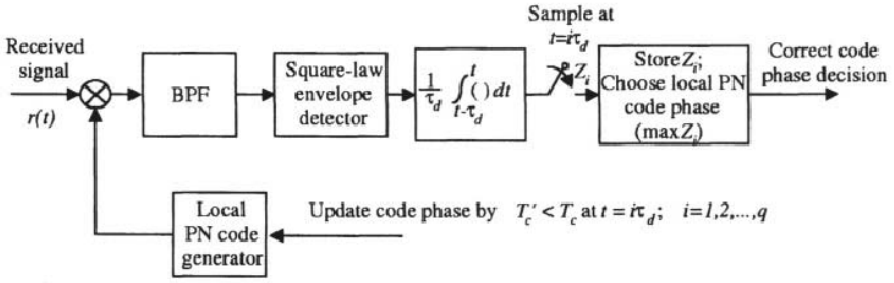


Fig. 8 Serial search realization of the maximum lihelihood search technique.

A natural extension of this serial technique will be a parallel search in which two or more paths search the code phase simultaneously, expecting that by increasing the hardware complexity the acquisition time would decrease in proportion to the number of paths used.

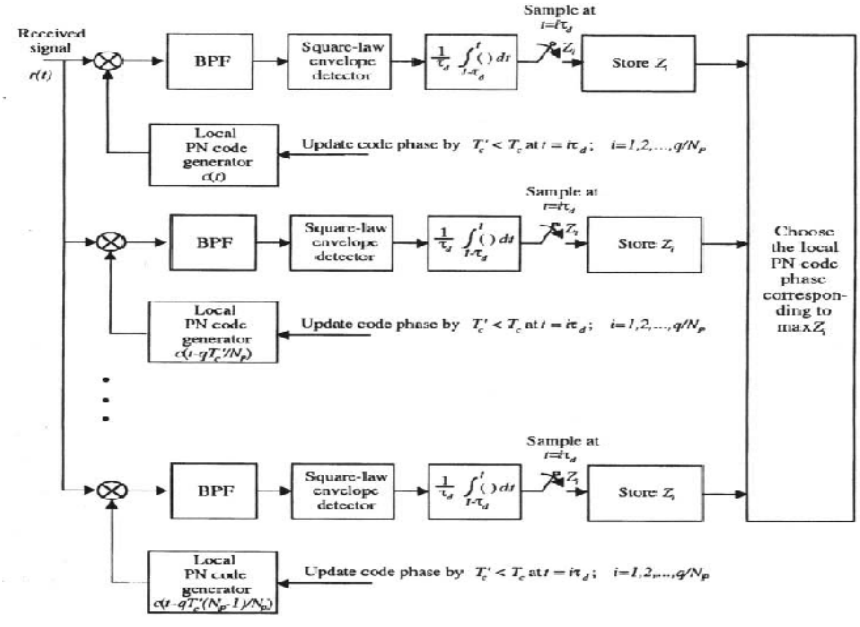


Fig.8. Parallel search realization of the maximum lihelihood search technique.

Fig. 9 shows the parallel search realization in which the entire q cell uncertainty region is subdivided into $N_p \geq 2$ identical components, with each responsible for q/N_p code phases. The code phase that yields the maximum among all those despread outputs is determined to be the right code phase in the final stage

Apparently, the serial search can be implemented with low complexity but at the expense of long acquisition time. On the contrary, the parallel search has more complex hardware, but can achieve a faster acquisition. A mid way comprise can be found practically according to the acquisition time and complexity requirement [9],[10].

The particular search procedure is adopted by the receiver through the uncertainty region is called the *search strategy*. The uncertainty is two-dimensional in nature, time and frequency, and the search can be done either *continuously* or in *discrete steps*. In the discrete-step case, the time uncertainty region is quantized into a finite number of elements called *cells*, through which the receiver is stepped.

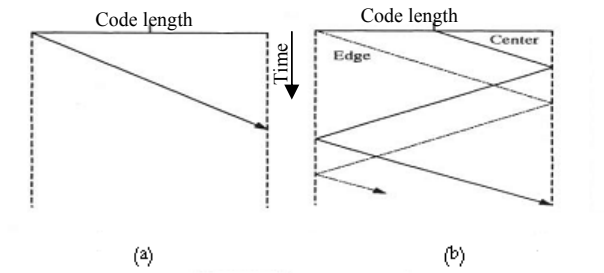
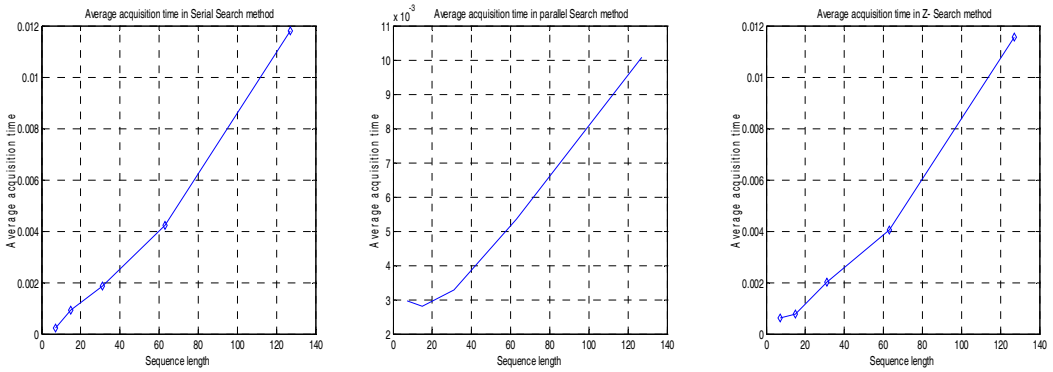


Fig.9. Two different types of search strategies. (a) straight line search & (b) Z-search,

There are several different types of search strategies are used depending on the nature of the uncertainty region, available prior information, and other factors. Fig. 9 illustrates two different types of search strategies are; straight line search which is applied in serial method and the Z-search. In case a priori information on the correct code-phase is made available through a variety of means such as short preamble, auxiliary reference, and past synchronization history, the distribution of the correct code-phase has been modeled as triangular or truncated Gaussian. In this case, the Z-search strategy is used to achieve a rapid synchronization [11] where the sweep lengths are equal to the number of cells in the whole uncertainty region, while, in the straight line search, the sweep length expands from a fraction to the full coverage of the uncertainty region.

The starting cell position for the Z-search strategy may be specified at the most probable position (center) or the least probable position (edge) and the search path may be made continuous or broken. The edge Z-search has an intermediate level of performance but does not effectively utilize the available a priori information [12]. Three different types of search strategies are implemented using a computer simulation, and the evaluation between them are shown in Fig.10. From this figure we conclude that the parallel search is the superior one as it provides the shortest average code acquistion time where the Z-search is moderate and the simple serial search has the longest average code acquistion time.



(a) Serial search (b) Paerallel search (c) Z-search

Fig.10. Average code acquistion time for different search stratigies

V- Conclution

This paper proposed a technique for detection of m-sequence in the DS/CDMA system which is faster than the algorithm based on the HOS. Moreover, a computer simulations is presented to evaluate the both algorithms. In addition , the evaluation of the processing time for the different code acquisition techniques are presented. From the simulation resultes we conclude that the Z-search method is the optimum startegy since it is faster than traditional search and less in complexity than the parallel search strategy.

References

[1] Prasad, R ‘ CDMA for Wireless Personal Communications’ (Artech House, Boston London, 1996.)

[2] H.-R.ParkandB.-J. Kang, “On the performance of a maximum-likelihood code-acquisition technique for preamble search in a CDMA reverse link,” *IEEE Trans. Veh. Technol.,* vol. 47, no. 1, pp.65-74, Feb. 1998.

[3] Papoulis, A ‘ Probability, Random variables and Stochastic Processes’ (McGRaw-Hill, New York,1990, 4th edn)

[4] Proakis, J.G. ‘Digital Communications’(McGRaw-Hill, New York,1995, 3rd edn).

[5] E.S. Warner, B. Mulgrew & P.M. Grant, “Triple correlation analysis of binary sequences for codeword detection” IEE Proc. Im. Sig. Proc. 141, October 1994.

[6] W. Adolf & B. Wirnitzer, “ Triple correlations” Proc. IEEE, Vol. 72, No. 7, July 1987 pp. 889-901.

[7] E.R. Adams, M.E. Gouda & P.C. Hill “ Detection and characteristics of DS/SS signals using higher order correlation” Proceeding of IEEE 4th ISSTA, Mainz Germany, Sept 1996, pp 27-31.

[8] R.E. Ziemer & R.L. Peterson, “Digital communications and spread spectrum systems” MacMillan, New York, 1985.

[9] Sourour and S. C. Gupta, “Direct-sequence spread-spectrum parallel acquisition in a fading mobile channel,” IEEE Trans. Commun., vol. 38, No. 7, pp.992-998, July 1990.

[10] S.-M. Pan, D. H. Madill, and D. E. Dodds, “A unified time-domain analysis of serial search with application to spread spectrum receivers,” IEEE Trans. Commun., vol. 43, no. 12, pp.3046-3054, Dec. 1995.

[11] S.-M. Pan, H. A. Grant, D. E. Dodds, and S. Kumar, “An offset-Z search strategy for spread spectrum systems,” IEEE Trans. Commun., vol. 43, no. 12, pp.2900-2902, Dec. 1995.

[12] V. M. Jovanovic, “Analysis of strategies for serial search spread-spectrum code acquisition - direct approach,” IEEE Trans. Commun., vol. COM-36, pp. 1208-1220, Nov. 1988.