University of
Waterloo Research Institute

Rapid Acquisition Techniques and the Sequence Design Problem for CDMA Spread Spectrum Communication Systems

Final Report
Project No. 808-02

Prepared for
The Department of Communications
under DSS Contract No. OSU 79-00082

by
Jon W. Mark and Ian F. Blake
Department of Electrical Engineering
University of Waterloo

Scientific Authority
J.L. Pearce R. Campbell
Communications Research Centre
Ottawa

March 1980

RAPID ACQUISITION TECHNIQUES AND THE SEQUENCE DESIGN PROBLEM FOR CDMA SPREAD SPECTRUM COMMUNICATION SYSTEMS

Final Report

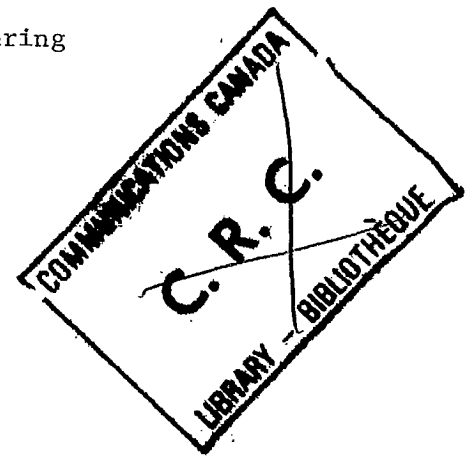
Prepared for

The Department of Communications

under DSS Contract No. OSU 79-00082

by

Jon W. Mark and Ian F. Blake
Department of Electrical Engineering
University of Waterloo



Scientific Authority

J. L. Pearce R. Campbell

Communications Research Centre
Ottawa

Project No. 808-02

March 1980

ABSTRACT

Three aspects of spread spectrum communication systems for code division multiple access application are considered in this report.

In the first part of the report a particular rapid acquisition scheme for CDMA spread spectrum systems which utilizes partial correlation of maximum length sequences is investigated. An extensive computer study of these partial correlations of a segment of our maximum length sequence with a sum of randomly phase shifted versions of distinct maximum length sequences was done. As a result of this study a model for these partial correlations was postulated and found acceptable under various statistical tests. The model was then applied to the analysis of a direct sequence and a hybrid frequency hopping/direct sequence system. Expressions were derived on such system parameters as false alarm probability and the probability of miss hit as functions of the detector threshold and compared to those values found by a detailed simulation of the system.

The problem of designing sequences for use in CDMA systems is considered in the second part of the report. Results available in the literature are collected under a common terminology and discussed in sufficient detail to allow easy generation of the sequences for those interested. This work concentrated mainly on the fundamental weight enumeration work of Kasami but includes also some recent work on the application of bent functions to the design of such sequences.

The final part of the report considers the maximum likelihood estimation of the state of a shift register generated sequence received in noise. A Viterbi algorithm approach is being taken to this problem and it has already been observed that there are possibilities to trade off the complexity of the decoder/state estimator with memory and table look up techniques. It is felt that this approach is promising, not only for the single shift register problem of concern

here, but also for the more general problem of the decoding of convolutional codes. It is hoped that the trade-offs observed will allow decoding for longer constraint lengths than is presently possible.

Table of Contents

I. Rapid Acquisition Techniques in CDMA Spread Spectrum Systems

1.1 Introduction

In many communication systems a common transmission medium is to be shared by several users. The satellite channel with large bandwidth and wide geographical coverage is a natural environment for multiple access communications. Conventional methods to accommodate multiple users are frequency division multiple access (FDMA) and time division multiple access (TDMA) in which fixed frequency bands or time slots are allocated to the users. When the number of users is large or when the data generation is random and bursty, inefficiencies appear in these conventional systems, and many other methods have been considered for various applications.

One of these methods is spread spectrum multiple access (SSMA) which allows all the users to use all the available bandwidth in a controlled overlay fashion. These systems were first proposed over twenty five years ago and have been receiving increased attention in the last decade. They are particularly effective for interference suppression in high noise environments due to channel conditions, other user signalling, or intentional attempts to jam communications.

By far the most widely discussed spread spectrum systems are direct sequence (DS)SS and frequency hopped (FH)SS. In these systems a code sequence is used both to identify the user and to create a very wideband signal from the relatively narrowband information signal. When the code sequence has certain properties, it is possible at the receiver to separate out the various signals sharing the common bandwidth. We will thus refer to both the DS and FH as code division multiple access (CDMA) SS systems. A brief exposition of these systems is presented.

A typical DSSS system is shown in Figure 1.1, where the baseband information $m_1(t)$ is first modulated in some manner to produce a signal $s_1(t)$ which

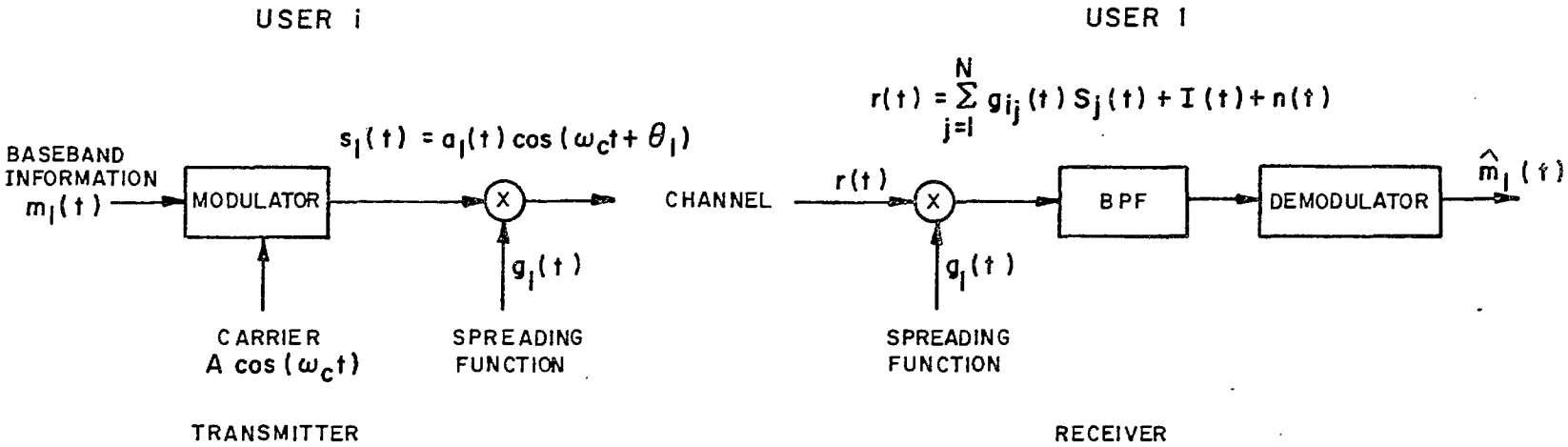


Fig. 1.1 Basic Spread Spectrum System

typically has a bandwidth on the order of that of $m_1(t)$. The wideband spreading function $a_1(t)$, derived from the code sequence, is then superimposed to produce the wideband transmitted signal $a_1(t)s_1(t)$. It is assumed there are N users in the system, each with its own spreading function, and that if user i is to transmit to user j, the spreading function $g_j(t)$ is used. The received signal for user i, r(t), is then composed of a wanted signal $a_1(t)s_1(t)$, unwanted signals $\sum_{j=2}^{N} a_{ij}(t)s_j(t)$ (where we ignore for the moment the possibility that more than one user may be transmitting to user 1 at any given time), channel noise n(t) and other noise such as an intentional jamming signal I(t). If we suppose for the moment that the spreading function $a_i(t)$, i=1,...,N, form an orthonormal set and that the receiver generated spreading function $a_1(t)$ is in synchronism with the spreading function of the incoming signal component intended for user 1, then the combination of the multiplier and bandpass filter will act as a correlator and the combination of all unwanted signals at the filter output will be diminished relative to that of the desired component.

The efficiency of this system depends in large measure on the spreading function design and a considerable effort has been expended on this problem. It is unnecessarily restrictive to use an orthonormal set and in practice a set of time functions is sought which have low cross-correlation values and low off peak autocorrelation values, with a very peaked autocorrelation function, implying wide bandwidth. Although certain gains can be realized by using multi-phase or even continuous time functions, it is most common to restrict attention to binary waveform spreading functions of the form

$$a(t) = \sum_j a_j \, p_{T_c}(t - jT_c)$$

where $\{a_j\}$ is binary (± 1) sequence and $p_{T_c}(t)$ is a unit amplitude pulse of

duration T_c, the so-called "chip time." The spreading function a(t) is often phase shift keyed (psk) onto the signal $s_i(t)$, an operation in this case equivalent to multiplication. Such signals are relatively easy to generate and maximize the transmitted power. The code removal at the receiver is often accomplished by using a heterodyne correlator where the despreading signal is generated as a psk signal, modulated by the code sequence, with a carrier frequency of $f_c + f_{IF}$. This signal is then bandpass filtered at IF before demodulation and the frequency offset is to prevent narrow band interference from appearing at the correlator output.

The most common type of code sequences in use are the pseudo-random noise (pn) sequences which are simple to generate and have excellent correlation properties. These are in fact the sequences that will be used in this investigation. However, much effort has been spent on the construction and analysis of other sets of sequences and a survey of these is given in Blake and Mark (1978).

The principle behind a frequency hopping SS system is the same as that of the DSSS system, differing only in the manner in which the spectrum spreading is achieved. A basic FHSS system is shown in Figure 1.2. As with DS there is no restriction on the type of modulation to be used. In an FH system however the code sequence is used to select the carrier frequency instead of directly modulating the carrier. The carrier frequency thus randomly hops over a set of frequencies $f_1, f_2, \ldots, f_n$ in a manner controlled by the code sequence generator. Each frequency is used for a preset time interval and it is, in fact, desirable that the frequency hopping rate be the same as the input data rate. The frequency hopping then spreads the input signal bandwith. It should be noted that with the frequency hopping method it is very difficult to maintain carrier coherence across the total bandwidth. Each time the system hops to a new frequency, the signal presented to the demodulator may

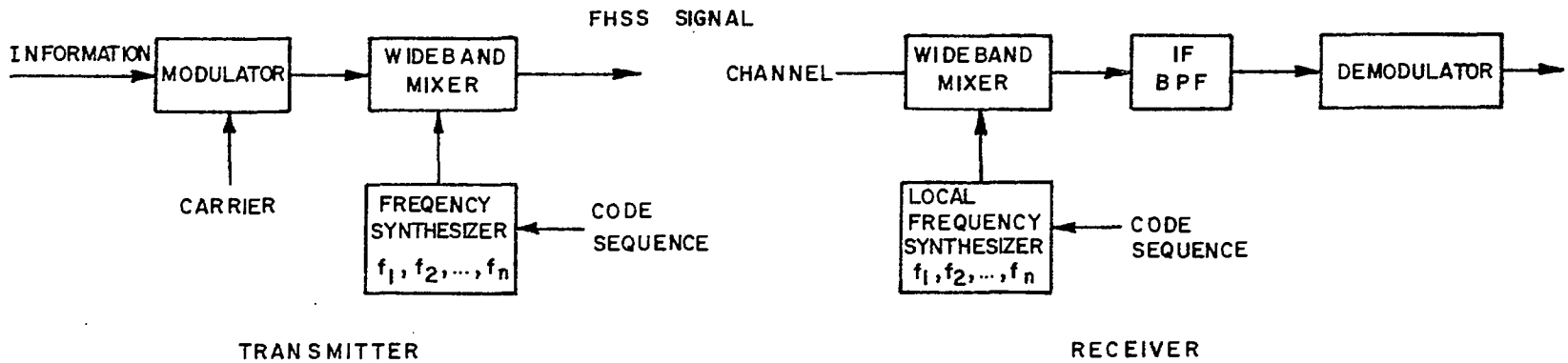


Fig. 1.2 Frequency Hopping Spread Spectrum System

change phase. Thus coherent demodulation methods are not suitable for FHSS systems and non-coherent methods such as envelope detection are most often used.

A common performance measure for SS systems is the processing gain [Dixon (1976)], defined as the ratio of output signal-to-noise ratio to input signal-to-noise ratio:

$$G_p = (S/N)_o \; / \; (S/N)_{in}.$$

In SS systems this quantity is often approximated by

$$G_p = B_{RF} \; / \; R_d$$

where B_{RF} is the RF bandwidth of the system and R_d is the baseband information data rate. In a DS system, B_{RF} is twice the code sequence rate R_c and it is seen that a high code rate, relative to the data rate, is required to achieve a high processing gain. In an FH system with n discrete frequencies, it can be shown [Dixon (1976)] that the processing gain is approximately n. Thus to achieve a high processing gain in an FH SS system, the number of frequencies must be large.

It is possible however to combine the concepts of DS and FH signalling into a hybrid FH/DS system which can achieve larger bandwidths than those attainable by either DS or FH alone. Such a hybrid system is shown in Figure 1.3. The DS code rate is normally much faster than the rate of frequency hopping and so many bits of the DS code sequence will occur in a single frequency channel. Also the number of frequency channels available is usually much smaller than the number of code bits, so that in the course of one period of the code sequence, all the frequency channels will have been used many times. As in DS systems, removal of the code in a hybrid system also employs heterodyne correlation, the difference being that the reference signal is also hybrid FH/DS.

It can be shown [Dixon (1976)] that the processing gain in dB of the

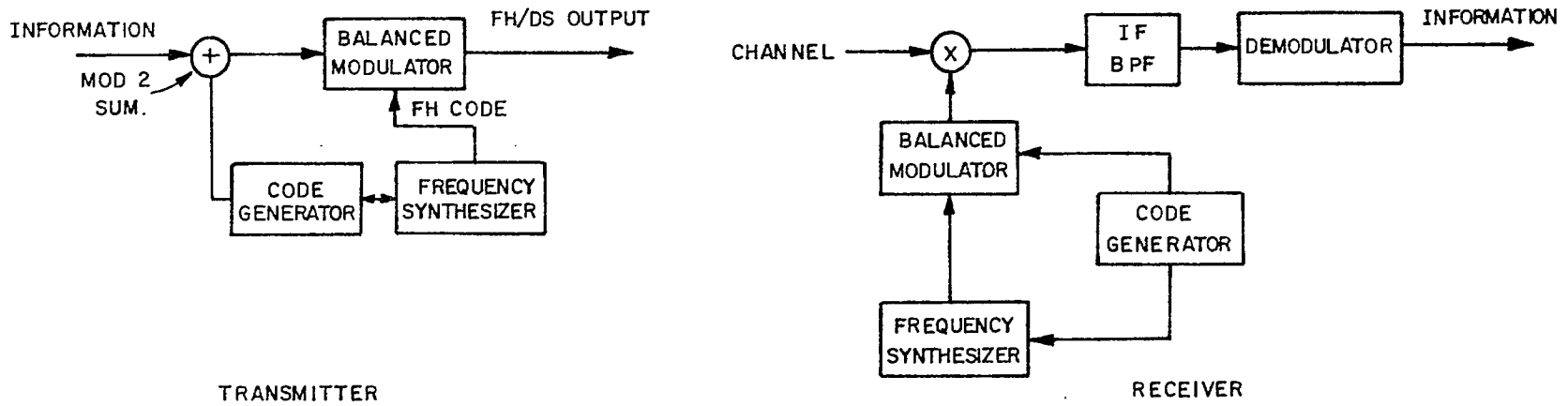


Fig. 1.3 Hybrid FH/DS Spread Spectrum System

hybrid FH/DS system is the sum of the processing gain of the FH and the DS systems, i.e.

$$G_p(\text{FH/DS}) = G_p(\text{FH}) + G_p(\text{DS})$$

$$= 10 \log_{10}(n) + 10 \log_{10} \left(\frac{2R_c}{R_d}\right).$$

With this relationship it is easy to appreciate the advantage that a hybrid system can offer over a pure DS or pure FH system to achieve a given processing gain.

For the successful operation of the above CDMA systems it is necessary that the receiver be able to both acquire and maintain synchronization of the locally generated code sequence with the same sequence contained in the incoming signal. Moreover, it is important in many applications that acquisition takes place well within the first data bit so as not to lose any information. Once acquired there are several well known techniques to track the code sequence and these appear to be well understood. This work is concerned entirely with acquisition which is generally regarded to be the harder of the two problems.

The optimum method of acquiring synchronism with the code sequence is to employ a bank of correlators or matched filters. The lengths of the sequences contemplated in this work however would make such an implementation impracticable since correlation is usually over an entire period of the sequence. In this paper a rapid acquisition technique is suggested and applied to both a DS and a hybrid FH/DS system. These systems are introduced in the next section where other attempts to solve this problem are also briefly mentioned. The acquisition systems proposed are based on partial correlations of pn sequences. As these are not well understood mathematically, an extensive experimental investigation of them was undertaken and the results are discussed in section 1.3. The results are used in section 1.4 to analyze the acquisition systems proposed and this performance is compared to that observed in simulation.

1.2. Subsequence Correlation Acquisition Methods for Spread Spectrum Systems

The acquisition problem for the DS CDMA SS system is first considered. It is assumed that each of the K users in the system is furnished with a unique pn sequence of length $N = 2^n-1$. The i^{th} user's sequence is denoted by $\{c_j^{(i)}\}$, a binary (0,1) sequence, and is generated by the primitive polynomial $f_i(x)$, $i=1,2,\ldots,K$. The correlation properties of these sequences is well understood when correlation is over an entire period. For this work the code sequences of interest will be binary (± 1) and the transformation from the (0,1) sequences $\{c_j^{(i)}\}$ to binary (± 1) sequences $\{a_j^{(i)}\}$ is $a_j^{(i)} = 1 - 2c_j^{(i)}$. If user j transmits to user k, he uses the code sequence generated by $f_k(x)$ and it is assumed for the moment that only one user transmits to user k at any given time. Without loss of generality, assume that k = 1. From the discussion of the previous section the signal received by user 1 is assumed to be of the form

$$r(t) = \sum_{k=1}^{K} \alpha_k \, a_k(t-\tau_k) \, b(t-\tau_k) \, \text{Cos} \, (\omega c t + \phi_k) + n(t) + I(t) \qquad (1.1)$$

where α_k is either 0 or 1 depending on whether a signal intended for user k is present or not, τ_k and ϕ_k are random time and phase delays respectively, n(t) is white Gaussian noise of double sided spectral density $N_o/2$ and I(t) represents other types of interference such as intentional jamming. In later analysis this last type of interference will be ignored. This model and some of the notation used is essentially that of Pursley [1977].

Notice that all transmitted signals are received with equal attenuation. On some channels, such as satellite channels perhaps, this may be an appropriate assumption. Assume there is a signal intended for user 1 present in the received signal (i.e. $\alpha_1=1$). At the receiver a locally generated version of the spreading function $a_1(t)$ must be generated in synchronism with that

contained in the received signal before it can be removed. The effect of a transition from a data +1 to a data -1, which multiplies the code sequence by -1, is ignored and a justification for this is given in the next section.

An obvious method to acquire synchronization is to use a correlator or matched filter and note the time delay to observe a peak at the output. The amount of computation required in such a system for sequences of length 2^{16} to 2^{20}, as are intended for use here, is prohibitive. A more sophisticated approach in the single user case depends on the fact that any n consecutive error free bits of the sequence completely determine the state of the code generator. This fact was used by Pearce and Rishenbatt (1971) and Kilgus (1973) who treated the pn sequence as a code and derived a set of orthogonal partiy checks on n consecutive bits to form a majority logic estimate of the pn sequence generator state. Another method, RASE (rapid acquistion by sequentical estimation) was introduced by Ward (1965). It uses sequential estimation techniques to form an estimate of the generator state. This method was later improved by introducing a recursion aided version of it which uses only simple logic elements to determine whether it is likely that n given bits in the sequence are without error [Ward and Yui (197.7a), (1977b)].

These techniques were derived for the single user case. It is clear however that the other users in a CDMA system may be regarded as simply increasing the level of interference. Thus any single user SS system designed to operate in a low noise environment may not work well when adapted to the multi-user situation.

Having observed the received signal for some period of time, the optimum acquisition method using only the information in this time interval is the maximum likelihood estimate of the pn code sequence generator state. Deriving such an estimate for shift registers of lengths 16 to 20 would

doubtless involve a computationally infeasible trellis search unless backtrack methods are employed. These approaches are not discussed here. Instead, we introduce another approach which, while suboptimal, appears to be effective in the multiple user environment and leads to rapid acquisition.

A block diagram of the system under consideration is shown in Figure 1.4. The received signal r(t) of equation (2.1) is multiplied by the output of a local oscillator and the result is low-pass filtered. In spread spectrum systems it is typical that the carrier frequency ω_c exceeds the chip rate T_c^{-1}, $\omega_c >> 1/T_c$ and the bandwidth of the information part in the received signal is less than ω_c. The code sequence of user 1 is denoted by $\{a_j^{(1)}\}$, $j=0,1,\ldots,2^n-2$, a (± 1) binary sequence. Let ℓ be some positive integer, $\ell | (2^n-1)$ and define k such that $\ell.k = 2^n-1 = N$. The sequence of user 1 is divided up into ℓ segments each of length k. Choose some subsequence length m, small with respect to the segment length k, and denote by $S_i^{(1)}$ the first m code sequence digits of segment i, i.e.,

$$S_i^{(1)} = (a_{ik}, a_{ik+1}^{(1)}, \ldots, a_{ik+m-1}^{(1)}) \quad i = 0, 1, \ldots, \ell - 1 .$$

The situation is shown graphically in Figure 1.5. The i^{th} subsequence matched filter is matched to the signal corresponding to the subsequence $S_i^{(1)}$. At a given instant of time the incoming register contains a segment of the received signal of length $m\ T_c$ and is a sum of (± 1) code sequences with random phases and noise. The number of users on the channel at any given time is also assumed to be a random variable and in practice a subsidiary function of the acquisition loop is to determine if a signal intended for user 1 is present in the received signal. This is determined automatically by the system under consideration.

At a given instant of time the output of the i^{th} matched filter,

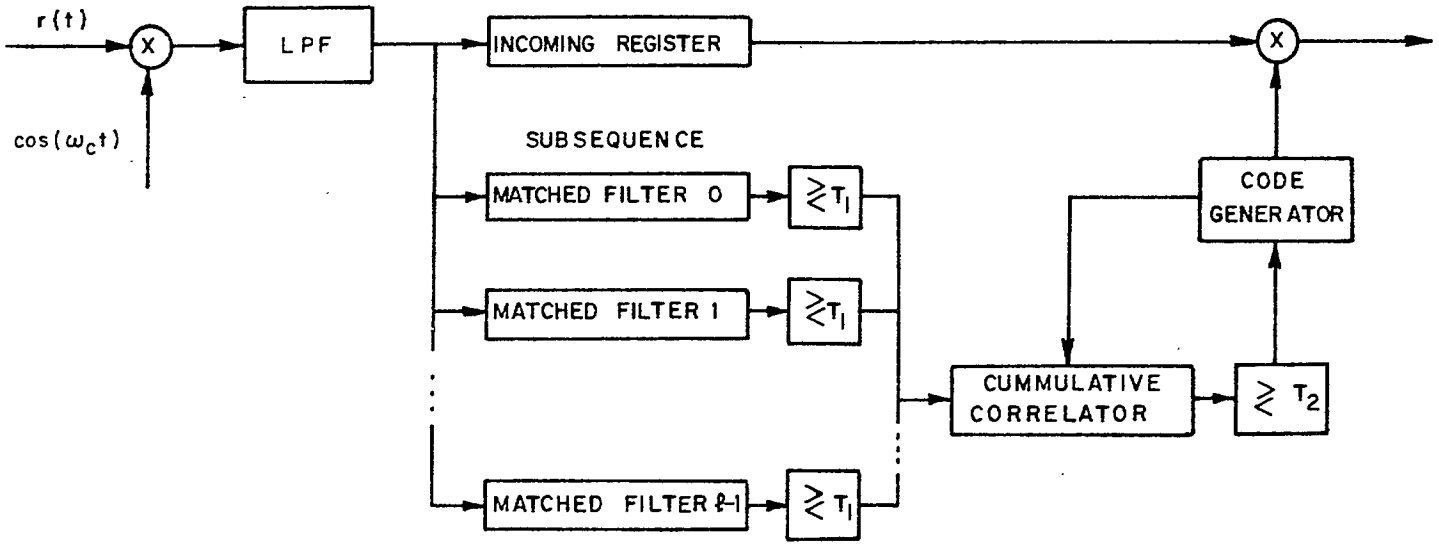


Fig. 1.4 Baseband Equivalent Model for Acquisition by Subsequence Correlation

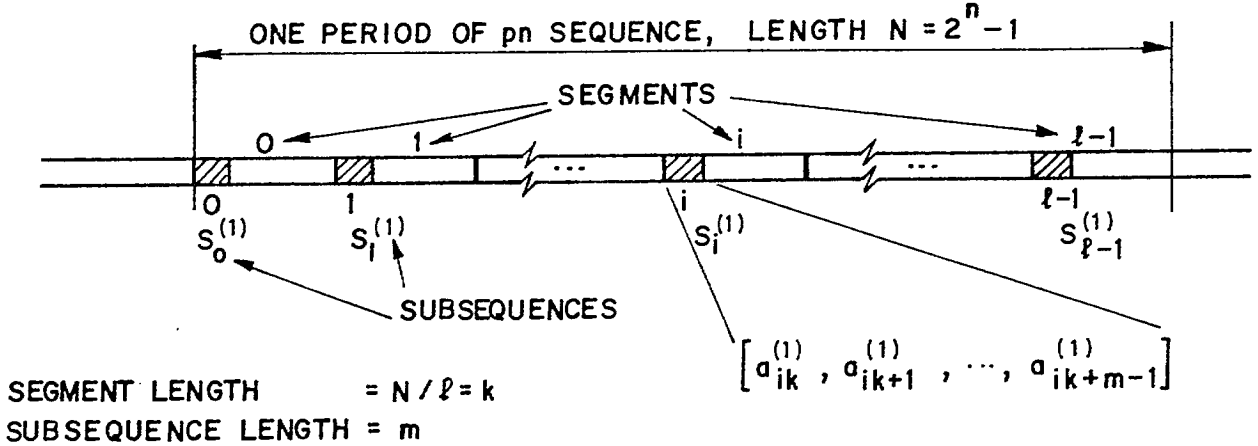


Fig. 1.5 The pn Sequence and Subsequence Relationships

denoted by U_i, with input the contents of the incoming register, is determined. If U_i exceeds the threshold T_1, the sequence generator of the cumulative correlator is initiated in a phase corresponding to that of the subsequence $S_i^{(1)}$. The cumulative correlator runs for some predetermined number of chip intervals, MT_c, $M > m$, and if the output V at the end of this interval exceeds the threshold T_2, it is assumed the incoming register contains a signal for user 1 and that the code sequence generator of the cumulative correlator is in synchronism with the code sequence of the signal intended for user 1 in the received signal. If no threshold is exceeded, the contents of the incoming register are shifted by T_c seconds and the procedure is repeated.

The operation of this system depends upon the observed properties of subsequence correlations of pn sequences. These properties are discussed in the next section. For the present we note that it will be established there that cross correlation of a subsequence of length m of a pn sequence of length $N = 2^n-1$, $m << N$, with either a distinct subsequence of length m of the same pn sequence or a subsequence of length m of another pn sequence, can be modelled as a normal random variable with mean $-m/N$ and variance approximately m. As such, fewer than .27% of such subsequence cross correlations will lie outside the $3\sigma = 3\sqrt{m}$ level about the mean. If K_a users are active on the channel and the subsequence to which the i^{th} matched filter is matched is not present in the incoming register, the output of the i^{th} matched filter U_i will be the sum of two random variables $X_i + U_i$, where X_i is the output due to the code sequences present in r(t), and U_i is due to the white noise on the channel. If it is assumed that subsequence correlations from distinct pn sequences are independent normal random variables, an assumption that is discussed in the next section, then if $S_i^{(1)}$ is not in synchronism with any subsequence of r(t) presently in the incoming register, X_i will be approximately a normal random

variable with mean $-k_a m/N$ and variance $k_a m$. If the subsequence is in synchronism, X_i will have mean $m - (k_a-1)m/N$ and variance $(k_a-k)m$. The noise random variable n_i is

$$n_i = \int_o^{mT_c} n(t)\ a_i(t)\ \mathrm{Cos}(\omega_c t)\ dt$$

which is a normal random variable with mean zero and variance $mT_c N_o/4$, regardless of synchronism considerations. It is assumed that the bandwidth of the matched filters is on the order of $1/T_c$ which is very much less than the bandwidths of the low-pass filter. Thus, the noise at the input to the matched filters can be still regarded as white. Thus, at any given instant of time the normal random variable U_i will be a normal random variable with mean and variance:

$$\begin{aligned} &S_i^{(1)} \text{ in synchronism :} && \mu_o = m\left(1-\frac{K_a-1}{N}\right);\ \sigma_o = (K_a-1)\ m + mT_c N_o/4 \\ &S_i^{(1)} \text{ not in synchronism:} && \mu_1 = -K_a\ m/N\ ;\ \sigma_1 = K_a\ m + mT_c N_o/4 \end{aligned} \tag{1.2}$$

By similar reasoning, if the cumulative correlator code sequence generator is initiated in the phase corresponding to the subsequence $S_i^{(1)}$, after MT_c seconds the cumulative correlator output will be a normal random variable with mean and variance -

$$\begin{aligned} &S_i^{(1)} \text{ in synchronism :} && \mu_o^1 = M\left(1-\frac{K_a-1}{N}\right);\ \sigma_o^1 = (K_a-1)\ M + MT_c N_o/4 \\ &S_i^{(1)} \text{ not in synchronism:} && \mu_i = -K_a\ M/N\ ;\ \sigma_1^1 = K_a\ M + MT_c N_o/4 \end{aligned} \tag{1.3}$$

It is possible, of course, that the output of the i^{th} matched filter exceeds T_1 when in fact $S_i^{(1)}$ is not in synchronism and thus the cumulative correlator will be initiated in an incorrect state.

The thresholds T_1 and T_2 must be set in relationship to the anticipated number of users, the subsequence length m and the noise level on the channel.

Once set, expressions for performance parameters of the system such as the probability of false alarm, probability of a false dismissal and probability distribution of the time to acquisition can be determined. These will use the results of the next section in which the assumptions regarding the subsequence correlations, mentioned above, are carefully examined. Expressions for the performance parameters of the system are derived in section 1.4, where they will be compared to results achieved by simulation.

There are certain design considerations for this system which should be mentioned. It is possible that more than one subsequence matched filter output exceed the threshold T_1 simultaneously. To accommodate this possibility either one of the filters may, at random, be assumed to be the correct indication of synchronism and the cumulative correlator initiated accordingly. It would also be possible to have more than one cumulative correlator initiate both of them and at the end of the MT_c seconds decide on the correct one. Similarly, in most systems it is likely that there may be more than one signal intended for user 1 present in the received signal. If more than one cumulative correlator is used, with the addition of some simple logic it would be possible to recover the data sequences from more than one source; one cumulative correlator required for each of the signals to be acquired, assuming their code sequences are not in synchronism (in which case the sum of the data signals would be given at the final output with no way of separating them).

At the transition from a +1 data bit to a -1 data bit the cross-correlation properties of the subsequences have not been investigated; i.e., the cross-correlation between a given subsequence of length m with a distinct subsequence of either the same or another pn sequence which is multiplied by -1 in its last p bits have not been considered. It is argued however that these cross-correlations would behave, on the average, as the ordinary

cross-correlations and hence are not considered further.

Finally, it is noted that it is not necessary that the entire pn sequence be divided into ℓ sequences each of length $k = N/\ell$. For certain values of N and ℓ desired, this would be inconvenient. All that is necessary is that the cumulative matched filter code sequence generator is initiated in the same state as the subsequence of the subsequence matched filter when its output exceeds the threshold T_1. This has nothing to do with the divisibility properties of the integers involved. In the simulations of the DS system the parameters chosen were $n = 16$, $N = 2^{16}-1$, $\ell = 20$ and m chosen as a (variable) multiple of 200. As $20 \times (2^{16}-1)$, the first 19 segments were chosen of length 3270 and the last segment of length 3285. The parameter m is chosen by the requirement that acquistion should normally be accomplished within $(1/m)^{th}$ of a data bit.

1.3. Subsequence Correlation Properties of Pseudonoise Sequences

To analyze the systems proposed in the previous section it is necessary to gain some insight into the correlation between a subsequence of a given pn sequence and a sum of a set of subsequences of other pn sequences of which the given pn sequence may or may not be a member. This problem is not well understood mathematically. To date, investigations have been carried out on the correlation function between two distinct pn sequences and on the correlations between a subsequence of a given pn sequence and another subsequence of the same pn sequence. Subsequence correlations between two distinct pn sequences appear not to have been considered in the literature and the problem seems beyond our capabilities with our present mathematical understanding of these sequences. We therefore take an experimental (computer simulation) approach to analyze this subsequence correlation problem and first review the known results for a single sequence.

Let $\{c_j\}$ be a binary (0,1) pn sequence of length $N = 2^n-1$ and $\{a_j\}$, $a_j = 1-2c_j$, the corresponding (±1) sequence. The cyclic autocorrelation function of such a sequence, with period N, is defined as

$$C(k) = \sum_{i=0}^{N-1} a_i\, a_{i+k} = \sum_{i=0}^{N-1} (-1)^{c_i - c_{i+k}}$$

where all subscripts are taken modulo N and $C(0) = N$, and $C(k) = -1$, $0 < k < N$. Now any other pn sequence of the same length can be obtained by decimation; i.e., taking every d^n bit of the pn sequence $\{c_j\}$ to give the sequence $\{c_{dj}\}$. Thus, if $\{e_j\}$ is a binary (0,1) pn sequence of length N, then $e_j = c_{dj+\ell}$ for some d, $0 < d < N$, $(d, N-1) = 1$ and for some suitable phase shift ℓ. If the sequence $\{c_j\}$ is generated by the polynomial $m_1(x)$, the minimal polynomial of the primitive element $\alpha \in GF(2^n)$, then the sequence $\{c_{dj}\}$ is generated

by $m_d(x)$ the minimal polynomial of α^d. The cyclic or periodic cross-correlation function between the two binary (±1) sequences corresponding to the sequences $\{c_j\}$ and $\{c_{dj}\}$ is given by

$$C_d(k) = \sum_{j=0}^{N-1} (-1)^{c_j - c_{dj}}$$

This function is known only for certain values of n and d, and Helleseth (1978) contains a summary of the known results. It is observed there that the problem is equivalent to determining the weight distribution of the $(2^n-1, 2n)$ code with generator polynomial $(x^N-1) / m_1(x)\, m_d(x)$. In light of the few results known on this problem of cross-correlating two entirely distinct pn sequences, it is not surprising how little is known on the subsequence correlation problem.

Consider the pn sequence $\{c_j\}$ of length $N = 2^n-1$ and denote by S_ℓ the subsequence of length m, $(c_\ell, c_{\ell+1}, \ldots c_{\ell+m-1})$ starting at the ℓ^{th} bit, all subscripts taken modulo N. Denote by w_ℓ the weight of S_ℓ and by a_w the number of the N possible subsequences of length m that are of weight w. Similarly, for the corresponding (±1) sequence $\{a_j\}$ denote by S_ℓ the subsequence $\{a_\ell, a_{\ell+1}, \ldots, a_{\ell+m-1}\}$ and by $W_\ell = \sum_{j=0}^{m-1} a_j$ and note that $W_\ell = m-2\, w_\ell$. Define the quantities

$$\underline{w}^p = \frac{1}{N} \sum_{i=0}^{N-1} w_i^{\,p} = \frac{1}{N} \sum_{i=0}^{N-1} i^p A_i \qquad \underline{W}^p = \frac{1}{N} \sum_{i=0}^{N-1} W_i^{\,p} = \frac{1}{N} \sum_{i=0}^{N-1} (N-2i)^p A_i .$$

The pn sequence $\{c_j\}$, together with all of its 2^n-1 cyclic shifts and the all zero sequence of length 2^n-1 forms a maximum length code and from this fact the quantities $\underline{W}^1$ and $\underline{W}^2$ are easily determined as

$$\underline{W}^1 = -\frac{m}{N} \tag{1.4 a}$$

and

$$\underline{W}^2 = m\left(1 - \frac{(m-1)}{N}\right) \tag{1.4 b}$$

It has been shown by Wainberg and Wolf [1970] and Lindholm [1968] that higher moments depend on the particular polynomials generating the pn sequences and considerable skewness in the third moments, for example, of sequences generated by certain polynomials can be found. Denote by $(S_\ell, S_k) = \sum_{i=0}^{m-1} a_{\ell+i}\, a_{k+i}$ the correlation between the two subsequences S_ℓ and S_k. By an argument similar to that used above, the average value of this correlation for $\ell \neq k$ is $-m/N$ and the average value of the square is $m(1-(m-1)/N)$. We will later interpret this subsequence correlation as a random variable and adopt the notation

$$\mu(m,n) = -m/N; \qquad \sigma^2(m,n) = m(1-\frac{(m-1)}{N}) - \frac{m^2}{N^2} \quad , \qquad N = 2^n-1$$

$$= m^2(\frac{1}{m} - \frac{1}{N})\ (1+\frac{1}{N})$$

It appears to be an intractable problem to determine the subsequence cross-correlation (S_ℓ, S'_k) for arbitrary m, when $S'_k = \{a'_k, a'_{k+1}, \ldots, a'_{k+m-1}\}$ is derived from a distinct pn sequence $\{c'_j\}$. It is reasonable to conjecture however that for subsequences S_k, S_ℓ and S'_k (S_k, S_ℓ derived from one sequence, S'_k from a distinct sequence) chosen at random, the statistical behaviour of (S_ℓ, S_k) will be similar to that of (S_ℓ, S'_k).

Now consider a set of K distinct binary (±1) pn sequences $\{a_j^{(k)}\}$, $k = 1,2, \ldots, K$ and denote by $S_\ell^{(k)}$ a subsequence of length m of $\{a_j^{(k)}\}$ starting at $a_\ell^{(k)}$, $S_\ell^{(k)} = \{a_\ell^{(k)}, a_\ell^{(k)}, a_{\ell+1}^{(k)}, \ldots, a_{\ell+m-1}^{(k)}\}$. Consider a subset of K_a integers $\{k_1, k_2, \ldots, k_{K_a}\}$, $1 \leq k_1 < k_2 < \ldots < k_{K_a} \leq K$. We are interested in correlations of the form $(S_\ell^{(1)}, \sum_{i=1}^{K_a} S_{\ell_i+k}^{(k_i)})$. In the communication context the set of a integers corresponds to the set of users to whom messages are currently being transmitted and the subscripts ℓ_i the random phases of the sequences relative to each other. If $k_1=1$ there is a message being transmitted

to user 1 and if, in addition, $\ell_1 = \ell$, the subsequence in the summation is in synchronism with $S_\ell^{(1)}$. Denote by

$$X_{K_a}(k) = (S_\ell^{(1)}, \sum_{i=1}^{K_a} S_{\ell_i+k}^{(k_i)})$$

and from the above comments for a fixed integer ℓ, this correlation is treated as a random variable. In the remainder of this section we justify modelling this discrete-time random process as an uncorrelated normal random process.

If $k_1 \neq 1$ (sequence $\{a_j^{(1)}\}$ not present in the summation), it would appear reasonable to assume that

$$E(X_{K_a}(k)) = -K_a m/N \tag{1.5 a}$$

and

$$V(X_{K_a}(k)) = \sum_{i=1}^{K_a} V\left\{(S_\ell^{(1)}, S_{\ell_i+k}^{(k_i)})\right\}$$

$$= K_a m^2 (\frac{1}{m} - \frac{1}{N})(1 + \frac{1}{N}) \tag{1.5 b}$$

where it has been assumed that correlations $(S_i^{(1)}, S_{\ell_i}^{(k_1)})$ and $(S_\ell^{(1)}, S_{\ell_j}^{(k_j)})$ are uncorrelated. If $k_1 = 1$ but $\ell_1 \neq \ell$, the same expressions will hold. If $k_1 = 1$ and $\ell_1 = \ell$ then the correlation $(S_\ell^{(1)}, S_\ell^{(1)}) = m$ introduces a "d.c. offset" term into the summation and essentially reduces the number of terms in the sequence by 1, thus

$$E(X_{K_a}(0)) = m - \frac{(K_a - 1)m}{N} \tag{1.6 a}$$

and

$$V(X_{K_a}(0)) = (K_a - 1)m^2(\frac{1}{m} - \frac{1}{N})(1 + \frac{1}{N}) \tag{1.6 b}$$

There are two aspects to the above computations which must be verified; namely, it is necessary to verify that $X_{K_a}(k)$ can be viewed as a normal random

variable and that $X_{K_a}(k)$ and $X_{K_a}(k')$ are uncorrelated, $k \neq k'$. Extensive simulations were performed on these questions and the results are now discussed.

To determine whether $X_{K_a}(k)$ can be modelled as a normal random variable, correlations for subsequences of length m = 200, 400, 600, 800 and 1000 were performed for the numbers of users K_a = 5, 10, 15, 20, 25, 30, 35, 40, 45 and 50. In each case 8192-m correlations were obtained by generating k_{K_a} distinct pn sequences by choosing every $100/K_a^{th}$ of the generating polynomials of Table 1.1 and generating a sum of subsequence of length 200 of the first sequence, sequentially, i.e., $(S_\ell^{(1)}, \sum_{i=1}^{(K_a)} S_{\ell_i+k}^{(k_i)})$, $k_1 = 1$, is determined for k = 0, 1,..., 8192 = m for the five values of m. The distribution of these 8192 - m subsequence correlations was considered and goodness of fit tests applied in the cases m = 200, 400, 600, 800 and 1,000 for K_a = 25, and for K_a = 5, 10, 15, ..., 50 for m = 200. For all computations n = 16, i.e., only sequences of length $2^{16} - 1$ were considered. The results of the chi-square goodness of fit tests are reported in Table 1.2. It is seen that for the hypotheses

H_o: data obeys a normal distribution

H_1: data does not obey a normal distribution

The hypothesis H_o is never rejected at the 1% level of significance while it is rejected only three times at the 4% level of significance. The test is to reject H_o if

$$\sum_{i=1}^{k} \frac{(u_i - \ell_i)^2}{\ell_i} > X^2_{1-\alpha;\, k-3}$$

where $X^2_{1-\alpha;\, k-3}$ is the $(1-\alpha)$-percentage point of a chi-square random variable with k-3 degrees of freedom. (The mean and standard deviation of the distribution were estimated from the data, hence the (k-3) degrees of freedom rather than (k-1) degrees of freedom if these parameters were assumed known). In this expression k is the number of intervals on the real line used for the test,

TABLE 1.1 - OCTAL REPRESENTATION OF PRIMITIVE POLYNOMIAL OF ORDER 16

202277 *	246515	306227	337027
203603	251447	306235	337457
205745	255505	311203	337521
206173	257253	311427	341337
210435	261163	313437	343011
211213	263641	314013	344153
213253	263737	315o57	344513
213523	264001	315713	346173
214157	264111	316505	346243
216313	267205	320317	346467
216607	271341	321433	351021
216777	271655	322111	352363
217527	272425	323113	352653
222535	273235	324523	354047
224671	275247	326317	354175
231265	276241	326423	355513
232045	277053	326571	363657
232233	277461	326715	366057
232435	277505	330o23	366171
232561	300025	330177	366345
232643	303045	30523	367033
234111	303417	331333	370467
237337	303435	331577	371253
240675	303463	332017	373237
245057	304655	335717	377755

TABLE 1.2 - GOODNESS OF FIT TEST RESULTS

Degree of Polynomial	Subseq. Length	Number of Users	Mean	Standard Deviation	Number of Samples	Number of Intervals	$\sum_{i=1}^{k} \frac{(n_i - e_i)^2}{e_i}$	$X^2_{.95;k-3}$	$X^2_{.99;k-3}$
16	200	5	-.276	31.64	7992	21	19.582	28.87	34.81
16	200	10	.004	45.25	7992	30	25.863	40.11	46.96
16	200	15	-.058	54.58	7992	21	18.651	28.87	34.81
16	200	20	-2.670	63.64	7992	21	23.517	28.87	34.81
16	200	25	-1.400	71.05	7992	25	36.448	33.92*	40.29
16	200	30	-2.180	77.15	7992	26	15.747	35.17	41.64
16	200	35	-2.150	83.04	7992	28	17.963	37.65	44.31
16	200	40	-1.270	88.55	7992	31	39.841	41.34	48.28
16	200	45	-2.570	94.01	7992	32	40.736	42.56	49.59
16	200	50	-2.520	100.17	7992	33	37.636	43.77	50.89
16	400	25	-1.900	100.66	7792	32	43.139	42.56*	49.59
16	600	25	-2.06	122.42	7592	16	23.427	22.36*	27.69
16	800	25	-1.420	141.78	7392	20	21.754	27.59	33.41

ℓ_i is the expected number of the 8192-m correlations in the i^{th} interval and n_i is the observed number of correlations in this interval. From the results contained in Table 1.2, it would seem reasonable for the purpose of this work to model the correlations as normal random variables.

The simulation data on the behaviour of the variance of the subsequence correlations is given in Figs 1.6 and 1.7. From equation (1) it is seen that theoretically the variance is given as

$$V(X_{K_a}(k)) = K_a m^2 (\frac{1}{m} - \frac{1}{N}) \ (1 + \frac{1}{N}).$$

Since $m << N$ in cases of interest here, this expression can be well approximated by $K_a m$. The data of Figs. 1.6 and 1.7 indicate good agreement with this result for the smaller subsequence lengths and the smaller number of users. As either the number of users increases or the subsequence length increases there is some falling off of the observed data from the theoretical value and the reasons for this are unknown. As the subsequence length inreases however, one might intuitively argue that the "degree of randomness" in the method of obtaining the correlations is diminished. Similarly, one might argue that as the number of users increases, there is more of a relationship between the generating polynomials being used, leading to some deficiencies of the model used to derive the formulae for the mean and variance. Nonetheless, in the sequel it will be assumed that $X_{K_a}(k)$ is a normal random variable with mean and variance given by either equation (1.5) or (1.6).

Tests were also performed to examine the correlation between $X_{K_a}(k)$ and $X_{K_a}(k)$ and $X_{K_a}(k+1)$. For a subsequence of length m the sample correlation function was determined by

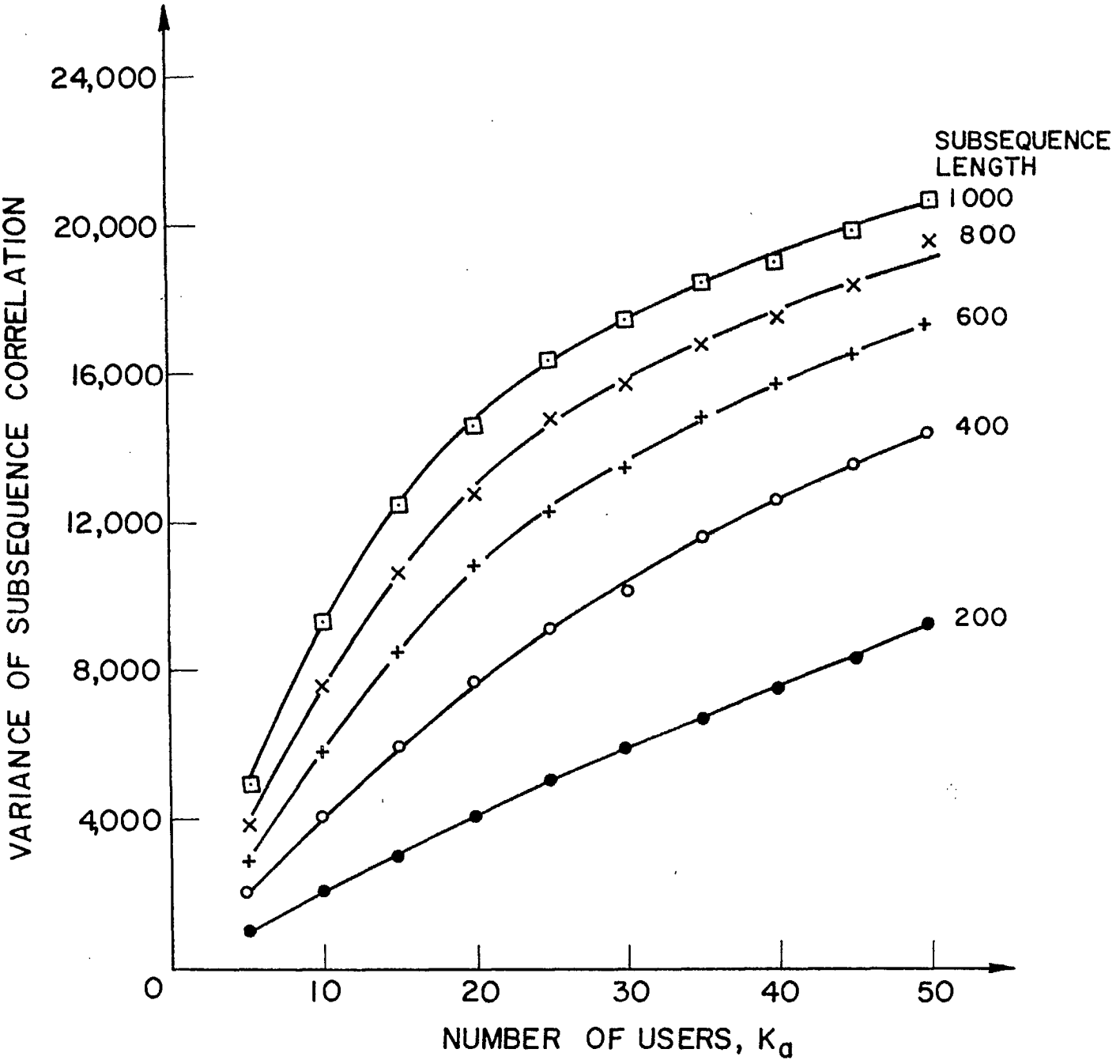


Fig. 1.6 Subsequence Correlation Variance

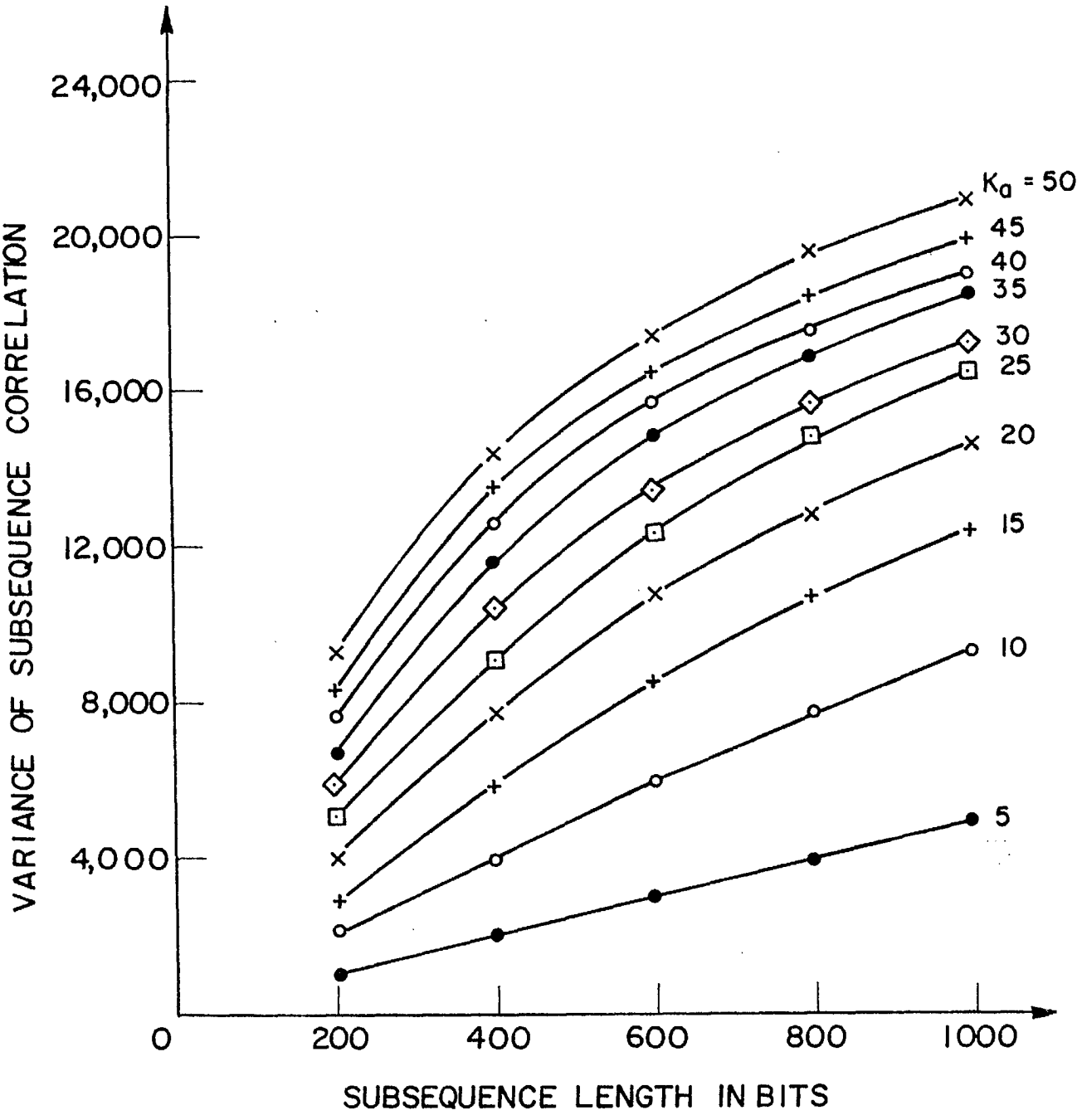


Fig. 1.7 Subsequence Correlation Variance

$$\hat{\rho} = \frac{J \sum_{j=1}^{J} X_{K_a}(j) X_{K_a}(j+1) - \left[\sum_{j=1}^{J} X_{K_a}(j)\right]\left[\sum_{j=1}^{J} X_{K_a}(j+1)\right]}{\left[J \sum_{j=1}^{J} X_{K_a}^2(j) - \left(\sum_{j=1}^{J} X_{K_a}(j)\right)^2\right]\left[J \sum_{j=1}^{J} X_{K_a}^2(j)) - \left(\sum_{j=1}^{J} X_{K_a}(j)\right)^2\right]}, \quad J = 819.2\text{-}m\text{-}1$$

Sample correlation functions were determined for subsequence lengths m = 200, 400, 600, 800 and 1000 and for K_a = 5, 10, 15, 20, 25, 30, 35, 40, 45 and 50, and the results are given in Table 1.3. To test the hypotheses

$$H_o: \quad \rho = 0$$

$$H_1: \quad \rho \neq 0$$

the appropriate test is to reject H_o if

$$\frac{|\hat{\rho}|(J-2)^{1/2}}{(1-\hat{\rho}^2)^{1/2}} > t_{1-\frac{\alpha}{2};\,J-2}$$

where $t_{1-\alpha;\,J-2}$ is the $(1-\alpha)$ percentage point of students t-distribution with J-2 degrees of freedom. At the 1% level of significance, for large J, $t_{1-\frac{\alpha}{2};J-2} = 2.576$ and since all measured correlations are close to zero the test reduces to rejecting H_o if $|\hat{\rho}| > t_{1-\frac{\alpha}{2};J-2}/(J-2)^{1/2}$, a quantity which varies from 0.0288 to 0.0304 as m varies from 200 to 1,000. From the data of Table 3 it would appear that most samples would lead to H_o not being rejected.

It would have been interesting to compute sample correlations between $X_{K_a}(k)$ and $X_{K_a}(k+\tau)$, $\tau > 1$ but as the amount of computation becomes excessive and it is not clear that the additional evidence would have been any more conclusive than that for the case $\tau = 1$, this was not done.

The results on the correlation properties of the sequence $X_{K_a}(k)$ are perhaps inconclusive. Nonetheless, they generally support the assumption that the sequence $\{X_{K_a}(k)\}$ is a normally distributed independent process, each point having the mean and variance of either equation (1.5) or (1.6). Under the

TABLE 1.3 - SAMPLE CORRELATION COEFFICIENT RESULTS

SUBS. LENGTH \ NO. OF USERS K_a	5	10	15	20	25	30	35	40	45	50
200	.0094	.0305	.0372	.0258	.0274	.0297	.0395	.0283	.0172	.0133
400	-.0083	-.0027	-.0041	-.0093	-.0066	-.0004	.0088	-.0170	-.0134	-.0099
600	.0348	.0448	.0457	.0345	.0438	.0428	.0448	.0263	.0234	.0225
800	.0131	.0148	.0063	.0048	.0125	.0092	.0144	.0065	-.0017	-.0018
1,000	.0248	.0319	.0237	.0145	.0150	.0072	.0107	.0102	.0010	.0041

conditions stated this seems reasonable although on the limited amount of evidence presented it must be viewed with some discretion. These assumptions are, however, a useful approximation, and allow progress to be made on the analysis of the systems under consideration.

To conclude this section, it is interesting to compare the results of this section with those obtained for truly random sequences. Specifically, let S_1 and S_2 be two binary (± 1) sequences of length m where each digit of each sequence is chosen independently and the probability of each digit being +1 is 1/2. The correlation (S_1, S_2) is a random variable and its behaviour is identical to the correlation of S_1 with the sequence of m 1's. Assume for the moment that m is an even integer, $m = 2m'$. The probability that X is k is the probability that the sequence S_1 contains $(m+k)/2$ 1's and $(m-k)/2$ (-1)'s and

$$P(X=k) = \left[\binom{m}{\frac{m+k}{2}}\right] \left(\frac{1}{2}\right)^m$$

and it follows that if m is even, k must be even also. Letting $m = 2m'$ and $k = 2k'$,

$$P(X=k) = \left[\binom{2m'}{m'+k'}\right] \left(\frac{1}{2}\right)^m, \quad k' = -m', -(m'-1), \ldots, -1, 0, 1, \ldots, m'.$$

The random variable $Y = (X + m')/2$ is a binomial random variable with mean m/2 and variance m/4. Consequently, K is a random variable with mean 0 and variance m, a result which is to be compared with the results of equation (1.5) for $K_a=1$, for the pn sequences. Applying the Central Limit Theorem to the random variable A shows that $Z = (X/\sqrt{m}$ tends to a standard normal random variable. This line of reasoning would further support the argument that the difference between the observed variances of the subsequence correlations and those anticipated by equation (1.5) is due to the sequences involved becoming "less random" in appearance.

1.4. Performance of a Direct Sequence Spread Spectrum Code Division Multiple Access System

With the model developed in section 2 and the results on subsequence correlations discussed in the previous section, certain performance parameters of a DS/SS CDMA system can be evaluated. Specifically, expressions for the following parameters are obtained in this section: (i) the probability of acquiring the signal when in fact the signal is in synchronism with one of the matched filter subsequences; ii) the probability of missing acquisition when in fact the signal is in synchronism (a false dismissal); (iii) the probability of deciding on synchronism when there is none (a false alarm); (iv) the probability distribution of the time to acquisition.

From section 2 the output of matched filter i is modelled as a normal random variable with the means and variances of equations (1.2), depending on whether or not a matched filter subsequence is in synchronism or not, where approximate expressions are used for the variances. The problem is perhaps best viewed as an hypothesis testing situation. The following hypotheses on the output of the i^{th} matched filter are considered, when the number of active users is K_a:

H_o: i^{th} matched filter subsequence is in synchronism

U_i has mean $\mu_o = m(1 - \frac{(K_a-1)}{N})$ and variance $\sigma_o^2 = (K_a-1)m^2(\frac{1}{m} - \frac{1}{N})(1+\frac{1}{N})$

$$+ mT_cN_o/4$$

$$\cong (K_a-1)m + mT_cN_o/4$$

H_1: i^{th} matched filter subsequence is not in synchronism

U_i has mean $\mu_1 = -K_a\, m/N$ and variance $\sigma_1^2 = K_am^2(\frac{1}{m} - \frac{1}{N})(1+\frac{1}{N}) + mT_cN_o/4$

$$\cong K_am + mT_cN_o/4$$

Similarly, the hypotheses H_o' and H_1' are defined for V, the output of the cumulative correlator

H_o': the cumulative correlator is in synchronism

V has mean $\mu_o' = M(1 - \frac{(K_a-1)}{N})$, variance $\sigma_o'^2 = (K_a-1)M^2(\frac{1}{M}-\frac{1}{N})(1+\frac{1}{N}) + MT_cN_o/4$

H_1': the cumulative matched filter is not in synchronism

V has mean $\mu_1' = -K_aM/N$, variance $\sigma_1'^2 = K_aM^2(\frac{1}{M} - \frac{1}{N})(1+\frac{1}{N})+MT_cN_o/4$

where M is the length of cumulative correlation.

As discussed in section 1.2 it is assumed the cumulative correlator is initiated only when one of the subsequence matched filter outputs exceeds the threshold T, and that the cumulative correlator is initiated in a state subsequent to the m bits of the subsequence matched filter exceeding a threshold. The implication of this assumption is that the computations for threshold exceedance of the cumulative correlator can be performed independently of the computations for the subsequence matched filters.

The probability of acquiring the signal, when in fact the signal is in synchronism with the i^{th} matched filter, is simply the probability that the threshold T_1 is exceeded under hypothesis H_o, times the probability threshold T_2 is exceeded by the output of the cumulative correlator:

$$p_s = P(\text{synch. acquired/synch. present}) = (1-\Phi(\frac{T_1-\mu_o}{\sigma_o}))(1-\Phi(\frac{T_2-\mu_o'}{\sigma_o'})) \quad (1.7)$$

where $\Phi(.)$ is the cumulative distribution function of the standard normal density function.

The probability of missing synchronism, when in fact synchronism exists, is the sum of two probabilities, the probability that the subsequence matched filter misses the synchronism, plus the product of the probabilities that the

subsequence matched filter catches synchronism and the possibility the cumulative correlator misses it:

$$p_m = P(\text{false dismissal}) = \Phi\left(\frac{T_1-\mu_o}{\sigma_o}\right) + \left(1-\Phi\left(\frac{T_1-\mu_o}{\sigma_o}\right)\right)\Phi\left(\frac{T_2-\mu_o'}{\sigma_o'}\right) \tag{1.8}$$

A false alarm is an indication of synchronism when none exists and is determined as

$$P(\text{false alarm}) = P(\text{synch. indicated / no synch. present})$$
$$= \left(1 - \Phi\left(\frac{T_1-\mu_1}{\sigma_1}\right)\right)\left(1 - \Phi\left(\frac{T_2-\mu_1'}{\mu_1'}\right)\right). \tag{1.9}$$

The probability distribution of the time to acquisition is determined as follows. The present time instant is assumed to be uniformly distributed among the k digits of a segment. Let t be a positive integer such that $t = q.k + r$, $0 \leq r < k$, $q > 0$. The probability it takes t chip times to acquire the signal is

$$P(T_a = t) = \frac{1}{M} \cdot p_m^{\,q} \cdot p_s \tag{1.10}$$

and is independent of r, the residue of t after division by q.

1.5. Subsequence Correlation Acquisition Methods for FH/DS Hybrid Systems

The direct sequence (DS) approach to CDMA/SS derives its spectrum spreading characteristic from the orthogonality property inherent in the time code. In a DSSS system all users in a K-user environment employ the same carrier frequency. Orthogonality amongst the K potential users may be enhanced by a superposition of spatial orthogonality, which can be accomplished by assigning a different carrier frequency to each of the K-users. This mode of signaling is termed fixed frequency diversity. From the anti-jamming point of view, i.e., not just multiple access, varying or hopping the carrier frequency over the time code by each user can impregnate the signal with jamming immunity, since an intentional jammer must be able to hop his frequencies synchronously with those of the transmitting user. The composite system is a hybrid frequency hopping/direct sequence (FH/DS) system depicted in Fig. 1.3.

The principle of frequency hopping and its usage as a spectrum spreading mechanism is well known [Dixon 1976]. A tacit assumption associated with an FH system is that the intended receiver knows the code generator polynomial, the initial state of the code generator and the frequency hopping code. The intended receiver thus possesses an innate ability to hop with the desired transmitter. As in the preceding sections, user 1 will be assumed to be the receiver. The number of actively transmitting users is $K_a \leq K - 1$. On the assumption that only one user, say the i^{th}, is transmitting to user 1, the number of unwanted sources is K_a-1. Arrivals from some of these K_a-1 unwanted transmitters, or any intentional jammers, may be at carrier frequencies different from the receiver's reference frequency so that the receiver's response to these undesired signals will be small.

The signal acquisition method for an FH/DS hybrid system is an extension of that described in section 1.2 for the DS system; the difference

lies in that the hybrid system possesses orthogonality (since finite length sequences are being considered here, the subsequences are only approximately orthogonal) in frequency as well as in time. Approximate time and frequency orthogonality is achieved by assigning each subsequence in the DS code its own frequency. The frequency assignment can be made by a separate code generator or by a selection of bits from the DS code to form a frequency selection code. In the present study the frequency selection code is derived from the DS code in the following manner: Suppose a β-bit codeword is used to select from a set of 2^{β} frequencies. As depicted in Fig. 1.8b the first bit of β consecutive subsequences is used as the frequency selection code. Since the generator polynomial and the initial state are known, the receiver has prior knowledge of the frequency assignment procedure. Each of the subsequence matched filters of Fig. 1.8a has its own center frequency. For a subsequence matched filter to have a coherent accumulation, m consecutive bits of the incoming sequence must be the same as the m-bit subsequence stored in the matched filter and at the same frequency as the matched filter's center frequency. If either the frequency or the m-bit subsequence differs from that of the matched filter, the output response will be low, i.e., incoherent accumulation.

Let $\{\omega_{\alpha_j}\}$, $j = 1, 2, \ldots, 2^{\beta}$ be the frequency set and let $S_{\ell}^{(\alpha_i)} \equiv \{a_{\ell}, a_{\ell+1}, \ldots, a_{\ell+m-1}\}$, $a_{\ell} \in \{1, -1\}$, be a subsequence. The corresponding signal is written as $S_{\ell}^{(\alpha_j)} \cos \omega_{\alpha_j} t$. Let the subsequence stored in the subsequence matched filter be $S_{\ell}^{(1)}$, so that the bandpass signal representation is $S_{\ell}^{(1)} \cos \omega_1 t$. Neglecting for the time being any carrier phase uncertainty, the inner product has the form

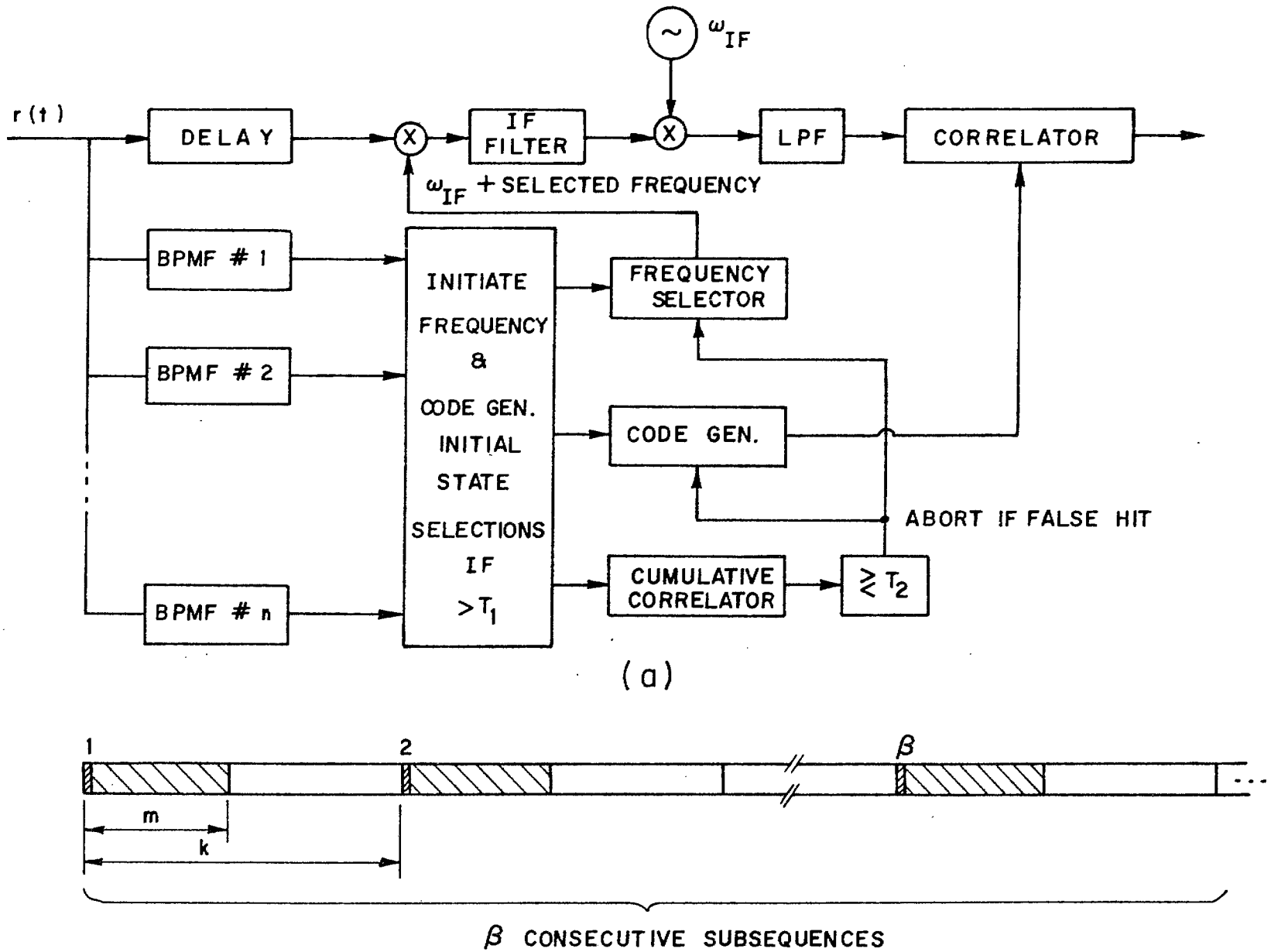


Fig. 1.8 Acquisition by Bandpass Subsequence Matched Filtering (Each at its own frequency)

$$p(t) = \frac{1}{2}\,(S_{\ell}^{(1)},\ S_{\ell_j+k}^{(\alpha_j)}\ [\cos\,(\omega_{\alpha_j} - \omega_1)\ t + \cos\,(\omega_{\alpha_j} + \omega_1)])$$

The filtered signal is

$$q(t) = LP\ [p(t)]$$

where LP[.] denotes a low-pass filtering operator. On the assumption that $|\omega_{\alpha_j} - \omega_1| > \omega_c$ for all $\omega_{\alpha_j} \neq \omega_1$, where ω_c is the cut-off frequency of the low-pass filter, the following cases prevail:

i) $S_{\ell+k}^{(\alpha_j)} = S_{\ell_i}^{(1)}$ and $\omega_{\alpha_j} = \omega_1$, i.e., k=0, $\ell_j = \ell_i$ and $\alpha_j = 1$

$$q(t) = \frac{1}{2}\,(S_{\ell_j}^{(1)}\ ,\ S_{\ell_i}^{(1)}) = \frac{1}{2}\,m$$

ii) $S_{\ell_j+k}^{(\alpha_j)} \neq S_{\ell_i}^{(1)}$ and $\omega_{\alpha_j} = \omega_1$

$$q(t) = \frac{1}{2}\,(S_{\ell_i}^{(1)},\ S_{\ell_j+k}^{(1)}) = \frac{1}{2}\,X_{\alpha_j}(k)$$

iii) $S_{\ell_j+k}^{(\alpha_j)} = S_{\ell_i}^{(1)}$ and $\omega_{\alpha_j} \neq \omega_1$

$$q(t) = \epsilon_{\alpha_j}\ (\frac{1}{2}\,m)$$

iv) $S_{\ell_j+k}^{(\alpha_j)} \neq S_{\ell_j}^{(1)}$ and $\omega_{\alpha_j} \neq \omega_1$

$$q(t) = \epsilon_{\alpha_j}\ (\frac{1}{2}\,X_{\alpha_j}(k))$$

where $X_{\alpha_j}(k) \triangleq (S_{\ell}^{(1)},\ S_{\ell_j+k}^{(\alpha_j)})$, $X_1(0) \triangleq (S_{\ell}^{(1)},\ S_{\ell_i}^{(1)}) = \sum_{p=1}^{m-1} a_{\ell+p}^2 = m$,

and ϵ_{α_j} is a small quantity to account for the low-pass filter's inability to

completely reject the difference frequency component. Cases (i) and (ii) above in which the carrier frequency of the incoming subsequence is the same as that of the subsequence matched filter's center frequency correspond to the DSSS mode.

In a multi-user environment an FH/DS hybrid system, with approximate orhtogonality in time and in frequency, is expected to perform better compared to the DS system. Suppose there are K_a active users, of which K_Ω are at the same carrier frequency as the subsequence $S^{(1)}_{\ell_i} = \{a_{\ell_i}, a_{\ell_i+1}, a_{\ell_i+2}, \ldots, a_{\ell_i+m-1}\}$ over the space $[\ell_i, \ell_i + m-1]$, where it is assumed that only user i is transmitting to user 1. Ω is the set of hopping frequencies, which in the present study, equal $\{\omega_1, \omega_2, \ldots, \omega_{2^\beta}\}$. Consider for the moment an interference-free and noise-free situation so that the corrupting influence comes purely from the K_a-1 unwanted transmitters. Let $\alpha_i = 1$ so that the i^{th} user's subsequence is denoted by $S^{(1)}_{\ell_i}$. Let $S^{(\alpha_j)}_{\ell_j + k}$ be the $(\ell_j+k)^{th}$ subsequence of the $\alpha_j{}^{th}$ active transmitter. Since the transmitters have random starting time, the composite signal presented to the receiver, in an m-bit interval starting with ℓ_j, is characterizable as

$$z(t) = \sum_{j=1}^{K_a} S^{(\alpha_j)}_{\ell_j+k} \cos(\omega_{\alpha_j} t + \theta_{\alpha_j})$$

where α_j denotes the number of the intended receiver with transmission coming from the j^{th} active user. Thus, if user i is transmitting to user 1, then $\alpha_i = 1$ and

$$z(t) = \begin{cases} S^{(1)}_{\ell_i} \cos(\omega_1 t + \theta_1) + \sum_{\substack{j=1 \\ \alpha_i \neq 1}}^{K_a} S^{(\alpha_j)}_{\ell_i + k} \cos(\omega_{\alpha_i} t + \theta_{\alpha_i}, & \\ \qquad \text{if } S^{(1)}_{\ell_i} \text{ is in the signal.} & \\ \sum_{\substack{j=1 \\ \alpha_i \neq 1}}^{K_a} S^{(\alpha_j)}_{\ell_j + k} \cos(\omega_{\alpha_j} t + \theta_{\alpha_j}), \text{ if } S^{(1)}_{\ell_i} \text{ is not in the signal.} \end{cases}$$

Because of the carrier phase uncertainties, θ_{α_j}, the subsequence matched filters assume a quadrature configuration as depicted in Fig. 1.9. Assuming that the LPF cuts off the difference as well as the sum frequency components; i.e., $e_{\alpha_j} \to 0$, the outputs at the LPFs are:

i) In-phase channel:

$$x(t) = \begin{cases} (S_{\ell_i}^{(1)}, S_{\ell_i}^{(1)} \cos\theta_1) + (S_{\ell_i}^{(1)}, \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega} S_{\ell_j+k}^{(\alpha_j)} \cos\theta_{\alpha_j}) \\ \qquad \text{if } S_{\ell_i}^{(1)} \text{ is in the signal.} \\ (S_{\ell_i}^{(1)}, \sum_{\substack{j=1 \\ \alpha_i\neq 1}}^{K_\Omega} S_{\ell_j+k}^{(\alpha_j)} \cos\theta_{\alpha_j}), \quad \text{if } S_{\ell_i}^{(1)} \text{ is not in the signal.} \end{cases}$$

ii) Quadrature Channel:

$$y(t) = \begin{cases} (S_{\ell_i}^{(1)}, S_{\ell_i}^{(1)} \sin\theta_1) + (S_{\ell_i}^{(1)}, \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega} S_{\ell_j+k}^{(\alpha_j)} \sin\theta_{\alpha_j}), \text{ if } S_{\ell_i}^{(1)} \text{ is in the signal} \\ (S_{\ell_i}^{(1)}, \sum_{\substack{j=1 \\ \alpha_i\neq 1}}^{K_\Omega} S_{\ell_j+k}^{(\alpha_j)} \sin\theta_{\alpha_j}), \text{ if } S_{\ell_i}^{(1)} \text{ is not in the signal,} \end{cases}$$

where $K_\Omega \leq K_a$ is the set of transmitting users whose carrier frequencies over the subsequence length equal ω_1. The quantity presented to the threshold detector is

$$R(t) = \sqrt{x^2(t) + y^2(t)}$$

For the general case in which all or some of the θ_{α_j}'s are different, the function R(t) is quite complex. For the special case where $\theta_{\alpha_j} = \theta_1 \ \forall j$, R(t)

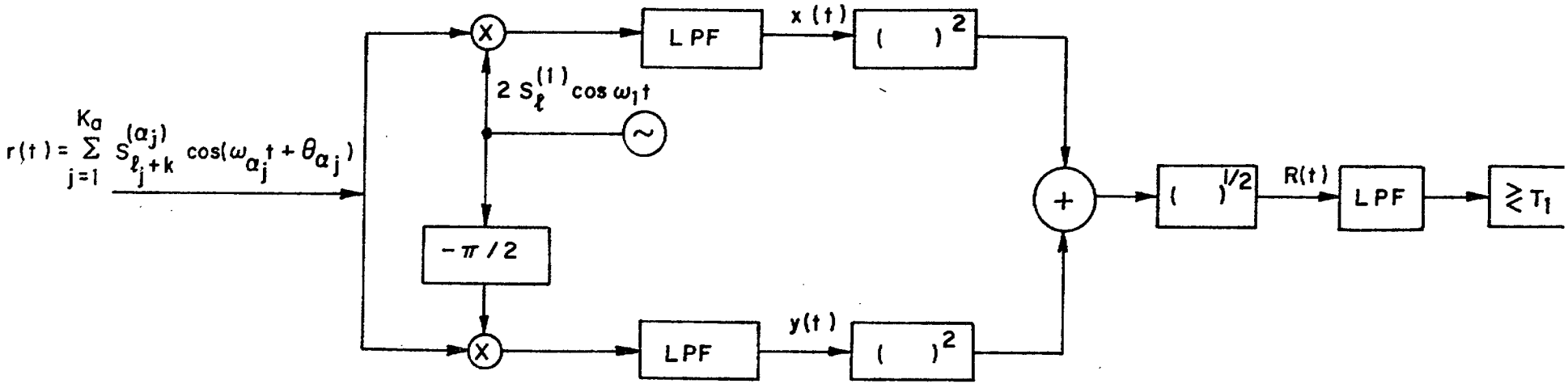


Fig. 1.9 Detection of Bandpass Signals at Complex Low-pass

simplifies to

$$R(t) = (S_{\ell_i}^{(1)}, S_{\ell_i}^{(1)}) + (S_{\ell_i}^{(1)}, \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega} S_{\ell_j + k}^{(\alpha_j)}), S_{\ell_i}^{(1)} \text{ in the signal}$$

This special case has a direct correspondence to the low-pass equivalent model used in sections 1.2 and 1.3 in the DSS case. While the $P[\theta_{\alpha_j} = \theta_1, j = 1, 2, \ldots, K_a]$ may be small, the above special case nevertheless offers an insight into the comparative performance between a FH/DS and a DS system, which would otherwise be buried in a set of unwieldy algebras.

The first two moments of R(t) are given by (for the case $S_{\ell_i}^{(1)}$ in the signal):

$$E[R(t)] = m + \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega} E[X_{\alpha_j}(k)] \tag{1.11a}$$

and

$$E[R^2(t)] = m^2 + 2m \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega} E[X_{\alpha_j}(k)] + \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega} E[X_{\alpha_j}^2(k)]$$

$$+ 2 \sum_{\substack{j=1 \\ j\neq i}}^{K_\Omega - 1} \sum_{p=j+1}^{K_\Omega} E[X_{\alpha_j}(k)]\, E[X_{\alpha_j}(r)] \tag{1.11b}$$

where $m = (S_{\ell_i}^{(1)}, S_{\ell_i}^{(1)})$ is the inner product of the subsequence $S_{\ell_i}^{(1)}$ and $X_{\alpha_i}(k) = (S_{\ell_i}^{(1)}, S_{\ell_i + k}^{(\alpha_j)})$ is the cross-correlation between the reference subsequence $S_{\ell_i}^{(1)}$ and a subsequence from one of the other $(K_\Omega - 1)$ transmitting users. Using the argument which led to equation (1.4), the first two moments of $X_{\alpha_j}(k)$ are given by

$$E[X_{\alpha_j}(k)] = -\frac{m}{N} \; ; \; E[X^2_{\alpha_j}(k)] = m\left(1 - \frac{m-1}{N}\right)$$

Using the above in equation (1.11) yields the following:

$$E[R(t)] = m\left(1 - \frac{K_\Omega - 1}{N}\right) \tag{1.12a}$$

and

$$E[R^2(t)] = m^2 + 2m\,(K_\Omega - 1)\,\left(\frac{-m}{N}\right) + (K_\Omega - 1)\,m\left(1 - \frac{m-1}{N}\right) + (K_\Omega - 1)\,(K_\Omega - 2)\,\left(-\frac{m}{N}\right)^2,$$

so that the variance of R(t) is prescribed by

$$V[R(t)] = (K_\Omega - 1)\,m^2\,\left(\frac{1}{m} - \frac{1}{N}\right)\left(1 + \frac{1}{N}\right) \tag{1.12b}$$

For the case $S^{(1)}_{\ell_i}$ not in the signal, the mean and variance of R(t) is given by (cf. equation (1.5)):

$$E[R(t) = -K_\Omega \frac{m}{N} \tag{1.13a}$$

and

$$V[R(t)] = -K_\Omega\, m^2\left(\frac{1}{m} - \frac{1}{N}\right)\left(1 + \frac{1}{N}\right) \tag{1.13b}$$

Comparing equations (3.3) and (5.2) and noting that $K_\Omega \leq K_a$, we have

$$E[R(t)]_{FH/DS} \geq E[X_{K_a}(k)]_{DS} \tag{1.14a}$$

and

$$V[R(t)]_{FH/DS} \leq V[X_{K_a}(k)]_{DS} \tag{1.14b}$$

Assuming a least favourable distribution, on the average $K_\Omega = K_a/\|\Omega\|$, where $\|\Omega\|$ is the number of frequencies, which in the present study, is 2^β. For the simulation results presented in the sequel, a 3-bit selection code is used so that $\|\Omega\| = 2^3 = 8$.

Guided by the probability of synch acquisition analysis described in section 1.4, an extensive simulation study into the probability of correct

synchronization as a function of threshold values for both the DS and FH/DS systems has been carried out. Simulation results of $P_s = P$ (synch acquired/synch present), for subsequences of length m = 1000 bits and generator polynomials of degree 16, are plotted in Fig. 1.10 as a function of threshold values, with the number of active users as parameter. In the simulation, users transmit at random initial times; i.e., θ_{α_j} is randomly chosen. The results of Figure 10 clearly show that the hybrid FH/DS system is superior to the DS system, as predicted by equation (1.14). With the FH/DS system, the subsequence matched filter output provides a clear synch indication. On the other hand, the cumulative correlator is needed, in the DS case, to ascertain synch when the number of active users exceeds 20.

Since the coherent peak of the subsequence matched filter output is clearly larger than the off-peak values in each of the FH/DS cases studied, no false dismissals were observed. With the DS system, false dismissals were observed in the $K_a = 40$ and $K_a = 50$ active users cases. Also, since the peak-to-sidelobe ratio of the FH/DS system's subsequence matched filter output is large, the threshold selection is fairly robust. The probability of synch acquisition within the first subsequence of the transmitted time code is very high, i.e., approaches unity with the proper threshold setting.

The simulation studies have been carried out with $\|\Omega\| = 8$ different frequencies. It is reasonable to expect that the performance of the FH/DS system improves with the size of the frequency selection code. Although an exhaustive simulation study of frequency selection codes has not been carried out, the analytic and simulation results obtained hitherto lead us to conjecture that the subsequence matched filter technique described in this paper, particularly the hybrid FH/DS system, represents a viable approach to rapid acquisition.

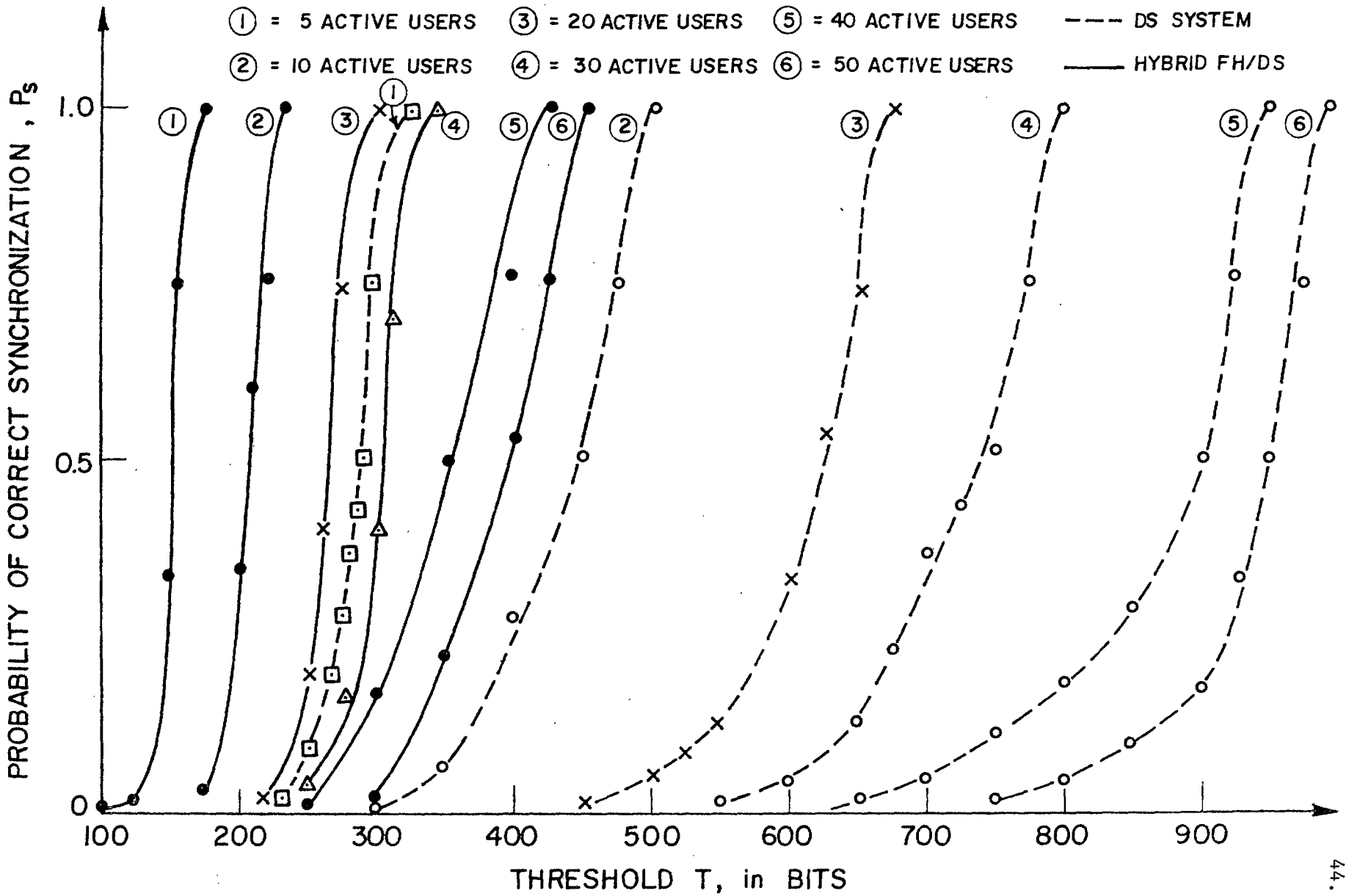


Fig. 1.10 Probability of Correct Synchronization Characteristics

1.6. Concluding Remarks

Recognizing that initial synchronization is a formidable problem in spread spectrum systems, we have proposed a subsequence matched filtering approach to rapid acquisition. We considered synch acquisition in both the the DS and FH/DS systems, where the spreading sequence is a maximum shift register, or pn, sequence. While the correlation properties of cyclic pn sequences are well known, the correlation properties of subsequences are less understood, particularly correlation between subsequences belonging to distinct pn sequences. Extensive simulations have been conducted to determine the statistical behaviour of the subsequence correlation properties. Simulation results indicate that the subsequence correlation at the matched filter output can be modelled as a Gaussian random variable. The Gaussian model permits the formulation in section 1.4 expressions for probabilities of synch acquisition, false alarm and time to acquisition. These probability expression are applicable to the FH/DS as well as the DS system, with the difference lying in the values of the mean and variance of the subsequence matched filter outputs. Simulation results reveal that subsequence matched filtering, as described in this paper, is a viable rapid acquisition scheme, particularly with the FH/DS hybrid system.

II. Construction of Sequences for Use in CDMA Systems

2.1. Introduction

The use of sequences with good auto and cross correlation properties has been discussed in the first part of this report. There, only m-sequences were used and partial auto and cross correlation parameters were of importance. For CDMA applications it is often desirable to have large sets of sequences with known correlation properties and the use of m-sequences, as m-sequences, is limited.

A previous report surveyed construction techniques for complex sequences with desirable correlation properties. The advantages of using binary {±1} sequences are significant and it is felt that further investigations of these sequences would be useful. Fortunately the construction of many such sequences has been well documented in an excellent forthcoming survey article by Sarwate and Pursley [1980]. Thus, rather than duplicate their effort we simply discuss many of these constructions from a different point of view, relating them more closely to the coding theory and weight enumeration work of Kasami [1969], from which so many of the constructions arise. Bent sequences, those derived from bent functions are discussed in section 2.5. They were not covered in the report of Sarwate and Pursley [1980]. It appears that many of the constructions using coding theory can be interpreted as special cases of bent functions. It is hoped that this report will serve as a basis for further work in the area.

Only binary {±1} sequences are considered here. Furthermore, although the odd correlation function is recognized as being a parameter of importance in CDMA systems [Massey, 1975] it is a difficult parameter to consider analytically and it will not be included in the discussion.

2.2. Preliminaries

Let $a = (a_0, a_1, \ldots, a_{N-1}) = \{a_i\}$ and $b = \{b_i\}$ be two periodic binary $\{\pm 1\}$ sequences of period N. Their cross correlation function is defined by

$$\theta_{a,b}(\ell) = \sum_{i=0}^{N-1} a_i b_{i+\ell} \qquad \ell = 0, 1, \ldots, N-1$$

where $i + \ell$ is reduced modulo N. The autocorrelation function of the sequence a is $\theta_{a,a}(\ell) = \theta_a(\ell)$ and, for a set M of binary sequences, we define the parameters

$$\theta_a = \max_{\substack{x \in M \\ \ell \neq o}} |\theta_x(\ell)| \qquad \theta_c = \max_{\substack{x,y \in M \\ x \neq y}} |\theta_{x,y}(\ell)|$$

and

$$\theta_{max} = \max \{\theta_a, \theta_c\}.$$

There have been many investigations on relationships among the various correlation functions and bounds on their parameters. We quote only two such results here. It was shown by Welch [1974] that for any set of complex sequences M, $|M| = M$, of dimension N and unit length,

$$\theta_{max}^{2k} \geq \frac{1}{MN-1} \left[\frac{MN}{\binom{N+k-1}{k}} - 1 \right]$$

where $k \geq 1$, k a positive integer. Since the bound holds for complex sequences it certainly holds for binary $\{\pm 1\}$ sequences. For $k = 1$ the inequality reduces to

$$\theta_{max} \geq \left(\frac{M-1}{MN-1} \right)^{1/2}$$

and it was observed by Welch [1974] that if $M < N$ this is the only choice giving nontrivial results. Sidelnikov [1971] also considered this problem and showed that for binary $\{\pm 1\}$ sequence sets of size $M = N^s$

$$\theta_{max} \geq (2s(N-s))^{1/2}$$

and, in particular, for $s = 1$

$$\theta_{max} \geq (2(N-1))^{1/2}.$$

2.3. Maximum Length Sequences (m-sequences)

An extraordinary amount of effort has been devoted to determining the properties of m-sequences and, in preparation for subsequent work, some of these will be reviewed here.

Following the notation of Helleseth [1976], [1978] let $a = \{a_i\}$, $a_i \varepsilon GF(2)$, $i = 0, 1, \ldots, 2^n-2$ be an m-sequence of length $N = 2^n-1$. Such a sequence can be generated by a linear feedback shift register with the feedback function determined by a primitive polynomial $m_1(x)$, the minimum polynomial of α, α a primitive element of $GF(2^n)$. The m-sequence and all its cyclic shifts can also be viewed as a cyclic code generated by $g(x) = (x^N+1)/m_i(x)$ and this code is devoted by $V(m_1)$ following the useful notation of Gold [1968]. The m-sequence can also be described by

$$a_j = Tr(\beta\alpha^j) \qquad , \qquad \beta \varepsilon GF(2^n)$$

where

$$Tr(\gamma) = \sum_{i=0}^{n-1} \gamma^{2^i} \quad .$$

In this description each choice of β gives a cyclic shift of the sequence. The decimation of the sequence $\{a_j\}$ by d gives the sequence $\{a_{dj}\}$, formed by taking every d^{th} bit of $\{a_j\}$. This decimated sequence is an m-sequence iff $(d,2^n-1)=1$. In fact all m-sequences of a given length can be realized by decimating a given m-sequence and consequently there are precisely $\phi(2^n-1)/n$ cyclically distinct m-sequences of this length. If $b = \{b_i\}$ is an m-sequence, then there exists a decimation d and phase k such that $b_i = a_{di+k}$. If $(d,2^n-1) = e$ then the period of the decimated sequence $\{a_{dj}\}$ is $(2^n-1)/e$ and is generated by $m_d(x)$, the minimal polynomial of α^d. This polynomial is not primitive if $e > 1$ but may still be of degree n and, if not of degree n, has degree which divides n.

If a and b are two binary {0,1} sequences the cross correlation function of their equivalent binary {±1} sequences (obtained by replacing 0 by +1 and 1 by

-1), which we also denote by a and b is

$$\theta_{a,b}(\ell) = \sum_{i=0}^{2^n-2} (-1)^{a_i+b_{i+\ell}} \qquad (a_i,\ b_j \text{ binary } \{0,1\}).$$

It can be shown that this cross correlation function is always an odd integer and in fact, that $8|(\theta_{a,b}(\ell)+1)$ unless a and b are reciprocal sequences (generated by reciprocal polynomials), in which case $4|(\theta_{a,b}(\ell)+1)$. It is also true that

$$\sum_{\ell=0}^{2^n-2} \theta_{a,b}(\ell) = 1 \qquad \sum_{\ell=0}^{2^n-2} \theta^2_{a,b}(\ell) = 2^{2n}-2^n-1$$

Furthermore, the cross correlation function of distinct m-sequences must assume at least three values (as opposed, for example, to the two valued autocorrelation function of an m-sequence). Gold [1969] has shown there exist pairs of distinct m-sequences which have cross correlation values -1, $-1-2^{\lfloor (n+2)/2 \rfloor}$ and $2^{\lfloor (n+2)/2 \rfloor}-1$ (where $\lfloor x \rfloor$ is the integer part of x). A pair of m-sequences which have only these cross correlation values is called a preferred pair of sequences and the pair of polynomials which generate them is called a preferred pair of polynomials. We adopt the convenient notation of Sarwate and Pursley [1980] and let

$$t(n) = 2^{\lfloor (n+2)/2 \rfloor}+1 = \begin{cases} 2^{(n+2)/2}+1 & n \text{ even} \\ 2^{(n+1)/2}+1 & n \text{ odd} \end{cases}$$

It was shown by Gold [1969] that if (k,n)=1 then the pair of polynomials $m_1(x)$ and $m_\ell(x)$, $\ell=2^k+1$ is a preferred pair of polynomials (cross correlation values of the corresponding sequences take only the values -1, $-t(n)$, $t(n)-2$) and so $\theta_{max} = t(n)$. The situation is summarized by Sarwate and Pursley [1980, Section 3] as follows: i) for $n \not\equiv 0 \pmod 4$ there exist preferred pairs of sequences of length $N = 2^n-1$ (and $\theta_c = t(n)$), ii) for n even $\theta_c = t(n)-2$ for reciprocal m-sequences iii) for $n \equiv 0 \pmod 4$ there exist sequences for which $\theta_c = t(n)-2$.

For any two binary {±1} sequences the Sidelnikov bound states that

$$\theta_{max} > (2N-2)^{1/2} = (2^{n+1}-4)^{1/2} = 2^{(n+1)/2}\ (1-\frac{1}{2^{n-1}})^{1/2}$$

$$> 2^{(n+1)/2}\ (1-\frac{1}{2^{n-1}}) = 2^{(n+1)/2} - \frac{1}{2^{(n-3)/2}}$$

$$> 2^{(n+1)/2} - 1$$

where the middle inequality follows from the fact that $(1-x)^{1/2} > (1-x)$ for $0<x<1$. But for m-sequences, θ_{max} is an odd integer from which it follows that $\theta_{max} \geq 2^{(n+1)/2} + 1$. For n odd this implies $\theta_{max} \geq t(n)$ and preferred pairs of sequences are optimal in this sense. For n even the bound $2^{(n+1)/2} + 1$ is less than t(n) by a factor of $\sqrt{2}$.

Clearly one approach to determining sets of sequences with good correlation properties would be to search for sets of primitive polynomials such that any distinct pair of polynomials in the set is a preferred pair. Thus $\theta_c = t(n)$ for the entire set. Experimental results show however, [Sarwate and Pursley, 1980] that the number of sequences in such sets is disappointingly small. Choosing larger sets of m-sequences and not requiring any pair to be a preferred pair, results in quite severely degraded correlation properties. In the next section other approaches to the problem are described which lead to considerably better results.

2.4. Sequences from Cyclic Codes

Let C be a cyclic (n,k) code over GF(2) with minimum distance d. If two code words are in distinct cyclic equivalence classes then their cross and auto correlation functions (of the corresponding {±1} sequences) are bounded above by n-2d. Massey [1975] carried the argument one step further and was able to obtain a bound on the odd correlation function which is not to be discussed here. The problem with this approach is to determine the number of cyclic equivalence classes with period N. It turns out that this is not hard to do when the generator polynomial of the code is of a certain form.

Some preliminary results are first discussed and the following theorem will be useful.

Theorem [Blake and Mullin, 1975]

Let C_1 and C_2 be binary cyclic codes of length n with generator polynomials $g_1(x)$ and $g_2(x)$ respectively. Then

i) $C_1 \cup C_2 = \{c_1(x) + c_2(x),\ c_1(x) \varepsilon C_1,\ c_2(x) \varepsilon C_2\}$ is generated by $(g_i(x), g_2(x))$.

ii) $C_1 \cap C_2$ is generated by $[g_1(x), g_2(x)]$ (ℓcm).

iii) $C_1 C_2$ is generated by $(g_1(x)\ g_2(x), x^n+1)$.

From this it follows that the set of values that the auto and cross correlation function of a sequence from C_1 and a sequence from C_2 may take on is a subset of the set of weights of the code $C_1 \cup C_2$. Thus, for example, if a is an m-sequence in $V(m_1)$ (generator polynomial $(x^n+1)/m_1(x)$) and b is an m-sequence in $V(m_i)$ (generator polynomial $(x^n+1)/m_i(x)$, $m_i(x) \neq m_1(x)$) then the auto and cross correlation values are weights in the code $V(m_1 m_i)$ (generator polynomial $(x^n+1)/m_1(x)m_i(x) = ((x^n+1)/m_1(x), (x^n+1)/m_i(x))$. This fact is exploited repeatedly here and the sets of Gold and Kasami sequences and their derivatives, which can be obtained from such considerations, are discussed.

The treatment of these sequences given here can be viewed as an alternative to that given in Sarwate and Pursley [1980] which it follows in outline.

Consider first the following argument due to Gold [1969] and let a be a sequence in $V(m_1(x)m_t(x))$, $(t,N) = 1$. Then a is a sequence of the form a_1+a_t where $a_1 \varepsilon\ V(m_1(x))$, $a_t \varepsilon V(m_t(x))$. Suppose that the cross correlation function of any two such sequences a_1 and a_t is less than k. The period of a is ℓcm (period b, period c) = N. Then if $a,b \varepsilon\ V(m_1(x)m_t(x))$, the cross correlation of these two sequences if $N-2d(a,b) = N-2w(a+b) = N-2w(a_1+a_t+b_1+b_t) = N-2d(a_1+b_1, a_t+b_t)$ which is the cross correlation of the sequences $a_i+a_t \varepsilon\ V(m_1(x))$ and $b_1+b_t \varepsilon\ V(m_t(x))$. By assumption this is less than k. In the code $V(m_1(x)m_t(x))$ there are $2^{2n}-1$ nonzero sequences and each cyclic equivalence class has order N. Thus there are $(2^{2n}-1)/(2^n-1)=2^n+1$ such classes and a complete set of representatives of these classes can be taken as $a_1+a_t^{(i)}$, $i=0,1,\ldots,N$, where $a_t^{(i)}$ is the cyclic shift of a, i positions. Thus it is possible to construct a set of N+1 sequences, each with period N, such that the maximum cross correlation and off peak autocorrelation is at most k. If $m_1(x)$ and $m_t(x)$ is any pair of preferred polynomials then a set of 2^n+1 sequences of length $N=2^n-1$ is constructed with maximum cross correlation $\theta_c=t(n)$. Further discussion on the existence of such sequences is deferred until results of Kasami have been considered.

Kasami [1969] considered the problem of the weight enumeration of certain BCH - codes and in discussing these results we adopt his notation with the exception of using $2^n-1 = N$ for the length of the code rather than 2^m-1. It should be mentioned that some of these results were apparently known to others and some have since been rediscovered. We omit references to history and use Kasami as the most convenient and comprehensive reference.

A d-BCH code is a binary BCH code which has elements $\alpha,\alpha^2,\ldots,\alpha^{d-1}$, but not α^d, as roots of its generator polynomial. Let $g(x) = (x^N+1)/h_1(x)\ldots h_p(x)$

be the generator polynomial of a cyclic code C where $h_i(x) = m_{-(2^{\mu_i}+1)}(x)$, $i= 1,2,\ldots,P$, and $0\leq\mu_1<\mu_2<\ldots<\mu_P\leq n/2$. It is known that $h_i(x)$ is of degree n iff $\mu_i<n/2$. If $\mu_i=n/2$ then $\deg(h_i(x)) = n/2$ since in this case the cyclotomic coset containing $\alpha^{-2^{n/2}+1}$ contains precisely the m/2 elements

$$\alpha^{-(2^{n/2}+1)}, \alpha^{-2(2^{n/2}+1)}, \ldots, \alpha^{-2^{n/2-1}(2^{n/2}+1)}$$

on noting that $\alpha^{-2^{n/2}(2^{n/2}+1)} = \alpha^{-(2^{n/2}+1)}$.

Those results of Kasami which will be useful for our discussion are given in Table 2.1 and we consider certain subcases now. Notice that if n is odd and $\mu_2=1$ then the roots of $h_1(x)h_2(x)$ include $\alpha^{-1},\alpha^{-2},\alpha^{-3}$ and α^{-4} and, for c = 1, the weight distribution given in case I A is that of the dual code of a double error correcting BCH code. In case II, the dimension of the code generated is 5n/2 and it can be shown that this is a $(2^{n-1} -2^{n/2})$ - BCH code. In case III the code is of dimension 3n and is a $(2^{n-1} -2^{(n+1)/2})$ - BCH code and also the dual of a triple error correcting code.

A. Gold Sequences: Earlier in the section it was observed that if $m_i(x)$ and $m_j(x)$ is any preferred pair of polynomials then a set of $2^n+1 = N+2$ sequences with $\theta_c = t(n)$ can be obtained from $V(m_i m_j)$. The sequences in $V(m_i m_j)$ are of the form $a_i + a_j$, $a_i \varepsilon V(m_i)$, $a_j \varepsilon V(m_j)$ and each has period N. These sequences can be viewed as sums of the outputs of linear feedback shift registers with feedback polynomials $m_i(x)$ and $m_j(x)$ respectively. A set of representatives of the cyclic equivalence classes can be taken as $a_i + a_j^{(k)}$ and, for proper sums, these are not maximal length sequences.

Thus the question of the existence of Gold sequences reduces to determining when preferred pairs of polynomials exist. Consider case I A of the Table 2.1. To obtain the correct correlation function for a preferred pair of sequences, it is necessary that c = 1. If n is odd and (n,μ_2) then $(n,2\mu_2) = 1$ and a preferred

pair of sequences results and this was first shown by Gold [1969]. It is mentioned in Sarwate and Pursley [1980, Theorem 1] that $m_1(x)$ and $m_q(x)$, $q = 2^{2k}-2^k+1$ is also a preferred pair of sequences if $(n_1 k) = 1$, n odd. A similar weight enumeration result to that of part I A of Table 2.1 is available in this case. If $n \equiv 2 \pmod 4$ and $(n,\mu_2) = 2$, n/2 is odd, (for example, choose $\mu_2 = n/2-1$) then again a preferred pair of sequences arises in this case also in that the auto and cross correlation functions assume values only in the set $\{-1, -t(n), t(n)-2\}$. Thus if $n \not\equiv 0 \pmod 4$ preferred pairs of sequences exist and, from the comments of Gold quoted earlier, these will be referred to as Gold sequences. It has already been observed that for m-sequences the cross correlation value must be odd and so $\theta_c \geq t(n)$ and for n odd Gold sequences are optimal with respect to this bound.

B. Gold-like Sequences

Choosing $\mu_1 = 0$ and $\mu_2 = \frac{n}{2} - 1$ and m even, we first observe that $2^{\frac{m-2}{2}}-1$ is in the same cyclotomic coset as $\frac{m}{2} + 1$ and $t(n) = 2^{\frac{m}{2}+1} + 1$. Thus $h_2(x) = m_{t(n)}(x)$ and if $n \equiv 2 \pmod 4$ this is a primitive polynomial and the codes constructed are the Gold codes. If $n \equiv 0 \pmod 4$, say $n = 4m$, then $2(n,\mu_2) = 2(4m,2m-1) = (4m,2(2m-1)) = c < 4m$ and case I B applies. (This follows since (2m-1) is an odd integer and thus (4m,2m-1) is odd.). In this case $h_2(x)$, which is the minimal polynomial of $\alpha^{t(n)}$ is of degree n but of order N/3 i.e. the sequences in $V(h_2)$ all have period N/3 since $(2^{\frac{N}{2}-1}, 2^n-1) = 3$. The code $V(h_2)$ thus consists of three linearly independent sequences and all their cyclic shifts of order N/3 or less. Thus in the case $n \equiv 0 \pmod 4$ $V(m_{\alpha^{t(n)}})$ does not contain m-sequences and the code $V(h_1 h_2)$ has five nonzero weights (case I B). If a, b, c are cyclically inequivalent codewords in $V(h_2)$ and $u \in V(h_1)$ then a set of cyclically inequivalent sequences in $V(h_i h_2)$ is $u + a^{(i)}$, $u + b^{(i)}$ and $u + c^{(i)}$ $i = 0, 1, \ldots, \frac{N}{3}-1$. Furthermore, from Table 2.1, case I B since

$(4m,2m-1) = 1$ (as $2m-1$ is odd, any gcd greater than unity must be odd and therefore must divide m, in which case it cannot divide $2m-1$, unless it is unity) we must have $c = 2$ and so

$$\theta_{max} = 2^n-1-2(2^{n-1}-2^{n/2}) = 2^{(n+2)/2} + 1 = t(n).$$

Thus performance wise these sequences are identical to the Gold sequences, differing only in their cyclic structure.

C. Dual BCH Sequences

Choose $\mu_1 = 0$, $\mu_2 = 1$ and note that this implies that $\alpha^{-1},\alpha^{-2},\alpha^{-3}$ and α^{-4} are roots of $h_1(x)h_2(x)$ and consequently the code is the dual of a double error correcting BCH code. When n is odd we have $(m,1) = (m,2) = 1$ and case I A applies. When n is even $2(m,1) = (m,2) = 2 = c$ and case I B applies. In either case $\theta_{max} = t(n)$. When n is odd $(3,2^n-1) = 1$ and $h_2(x)$ is primitive and the resulting sequences are Gold sequences. When n is even $(3,2^n-1) = 3$, $h_2(x)$ is of degree n but order N/3.

This concept can be extended to the duals of other BCH codes. It is shown in [van Lint, 1971(P.129)] that the minimum distance of the dual of the binary t-error correcting BCH code of block length $N = 2^n-1$ is at least $2^{n-1} - 1 - (t-1)2^{n/2}$ and Welch [3] observed the implication that there must be at least 2^{nt} codewords with an inner product less than or equal to $(t-1)2^{n/2}$.

D. Kasami Sequences - Small Set

For n even choose $\mu_1=0$, $\mu_2=n/2$ and in this case the dimension of the code is $3n/2$. The sequences generated by $h_2(x)$ have period $2^{n/2}-1$ and it is possible to obtain $2^{n/2}-1$ sequences of this period. Case I C applies and $\theta_{max} = 2^{n/2} + 1 = s(n)$ (using the terminology of Sarwate and Pursley [1980] and it is shown there that this set is optimal with respect to the bound of Welch [1974]).

E. Kasami Sequences - Large Set

For n even again choose $\mu_1 = 0$, $\mu_2 = n/2-1$ and $\mu_3 = n/2$ in which case the code is of dimension $5n/2$ and case II applies. This is a $(2^{n-1}-2^{n/2})$ - BCH code. If $n \equiv 2 \pmod 4$ then sequences in $V(h_1h_2)$ are Gold sequences and the number of cyclically distinct sequences in $V(h_3) \cup V(h_1h_2)$ is $2^{n/2}(2^n+1)$. If $n \equiv 0 \pmod 4$ the number of cyclically distinct sequences is $2^{n/2}(2^n+1) - 1$. In either case $\theta_{max} = t(n)$ as can be determined from Table 2.1, case II.

2.5. Bent Sequences

Bent functions were introduced by Rothaus [1976] as Boolean functions on $V = V_n(2)$, the vector space of dimension n over GF(2). Let b(v) be a function from $V_n(2)$ to $V_1(2)$ and define the function

$$\hat{B}(\lambda) = \frac{1}{2^{n/2}} \sum_{v \in V} (-1)^{(\lambda,v)} \ (-1)^{b(v)}$$

We call b(v) a bent function if $|\hat{B}(\lambda)|=1$ for all $\lambda \in V$. The name apparently derives from an association with Boolean functions to codewords in first order Reed-Muller codes [MacWilliams and Sloane, 1977]. It can be shown that for a bent function on V to exist $\dim(V_n(2))=n$ must be even. For example if $V = V_1 \oplus 1/2$, $V_i \cong V_{n/2}(2)$, $\dim V_i = n/2 = k$, let f be an arbitrary function from V_2 to $V_1(2) = GF(2)$. Then the function $b(v) = (v_1,v_2) + f(v_2)$, $v_1 \in V_1$, $v_2 \in V_2$, $v = v_1 + v_2$, is bent. Similarly, the function $(v_1,v_2) + f(v_2) + L(v)$, where L is any linear functional on V, is bent.

Consider the sequences defined by ${}^{(i)}a = \{a_j\}$, ${}^{(i)}a_j = (-1)^{f_i(\alpha^j)}$, $j = 0,1,\ldots,2^n-2$, α a primitive element of $GF(2^n)$, where $f_i(v)$ is a bent function of the form

$$f_i(v) = b(v_1) + L_i(v_1) + Tr(v), \quad v \in V, \ v_1 \in V_1$$

where $Tr(v) = \sum_{i=0}^{n-1} v^{2^i} \in GF(2)$ and the L_i are distinct linear functionals on V_1. There are $2^{n/2}$ distinct linear functionals on V_1 which define the set of $2^{n/2}$ sequences ${}^{(i)}a$. It can be shown (Olsen, Scholz and Welch [1980]) that these sequences of length 2^n-1, have $\theta_{max} \leq 2^{n/2} + 1$.

The mechanization of these bent sequences is discussed in (Olsen et al, [1980]) where it is observed that very long period sequences can be generated with fewer memory elements (but were complicated logic control) than the same period linear shift register sequences. Other classes of bent functions are described in [Lempel and Cohn, 1980].

2.6. Comments

It is noticed from Table 2.2, where the parameters of all the sequences discussed here are summarized, that the parameters of bent sequences and the small set of Kasami sequences are identical. It would be interesting to determine if these were in fact different constructions of the same sequences.

One limitation of all the constructions presented here is that the sequence lengths are of the form 2^n-1. It would be useful and important to construct sequences of other lengths to give the system designer greater flexibility.

The generation and synchronization problems of sequences other than m-sequences has not received much attention in the literature and this another area for future investigation.

Table 2.1. Summary of the Weight Enumeration Results of Kasami

	Parameter Conditions	Nonzero Codeword Weights	Number of Codewords of Given Weight
I	$p=2, \mu_1=0$		
	A. $(n,\mu_2)=(n,2\mu_2)=c$	$2^{n-1}\pm 2^{(n+c-2)/2}$	$(2^{n-c-1}\mp 2^{(n-c-2)/2})(2^n-1)$
		2^{n-1}	$(2^n-2^{n-c}+1)(2^n-1)$
	B. $2(n,\mu_2)=(n,2\mu_2)=c\neq n$	$2^{n-1}\pm 2^{(n+c-2)/2}$	$2^{(n-c-2)/2}(2^{(n-c)/2}\mp 1)\cdot$ $(2^n-1)/(2^{c/2}+1)$
		$2^{n-1}\pm 2^{(n-2)/2}$	$2^{(n+c-2)/2}(2^{n/2}\mp 1)(2^n-1)/(2^{c/2}+1)$
		2^{n-1}	$((2^{c/2}-1)2^{n-c}+1)(2^n-1)$
	C. $2(n,\mu_2)=(n,2\mu_2)=n$	$2^{n-1}\pm 2^{n/2-1}$	$(2^{n-1}\mp 2^{n/2-1})(2^{n/2}-1)$
		2^{n-1}	2^n-1
II	$p=3$, n even,	$2^{n-1}\pm 2^{n/2}$	$2^{(n-4)/2}(2^{(n+2)/2}\mp 1)\cdot$ $(2^{(n+2)/2}-1)(2^n-1)/3$
	$\mu_1=0, \mu_2=\frac{n}{2}-1, \mu_3=\frac{n}{2}$	$2^{n-1}\pm 2^{(n-2)/2}$	$2^{(n-2)/2}(2^{n/2}\mp 1)(2^{n/2}-1)\cdot$ $(2^n+2^{(n+2)/2}+4)/3$
		2^{n-1}	$(2^{n/2}-1)(2^{2n-1}+2^{(3n-4)/2}-2^{n-2}$ $+2^{n/2}+1)$
III	$p=3$, n odd, $n\geq 5$	$2^{n-1}\pm 2^{(n+1)/2}$	$2^{(n-5)/2}(2^{(n-3)/2}\mp 1)(2^n-1)(2^{n-1}-1)/3$
	$\mu_1=0, \mu_2=(n-3)/2, \mu_3=(n-1)/2$	$2^{n-1}\pm 2^{(n-1)/2}$	$2^{(n-3)/2}(2^{(n-1)/2}\mp 1)(2^n-1)\cdot$ $(5.2^{n-1}+4)/3$
		2^{n-1}	$(2^n-1)(9.2^{2n-4}+3.2^{n-3}+1)$

Table 2.2 Summary of Correlation Properties of Sequences of Length 2^n-1

$$t(n) = \begin{cases} 2^{(n+2)/2} + 1 & n \text{ even} \\ 2^{(n+1)/2} + 1 & n \text{ odd} \end{cases} \qquad s(n) = 2^{n/2} + 1 \quad (n \text{ even only})$$

Sequence Name	Existence	Size of Sequence Set	Values Assumed by Correlation Functions	θ_{max}
Gold	$n \not\equiv 0 \pmod 4$	$2^n + 1$	$-1, -t(n), -2$	$t(n)$
Gold-like	$n \equiv 0 \pmod 4$	2^n	$-1,-t(n),t(n)-2,-s(n),s(n)-2$	$t(n)$
Dual BCH	n even	2^n	$-1,-t(n),t(n)-2,-s(n),s(n)-2$	$t(n)$
Kasami-small set	n even	$2^{n/2}$	$-1, -s(n), s(n)-2$	$s(n)$
Kasami-large set	$n \equiv 0 \pmod 4$	$2^{n/2}(2^n+1)-1$	$-1,-s(n),1-2s(n),s(n)-2,-3+2s(n)$	$t(n)$
	$n \equiv 2 \pmod 4$	$2^{n/2}(2^n+1)$	$-1,-s(n),1-2s(n),s(n)-2,-3+2s(n)$	$t(n)$
Bent	$n \equiv 0 \pmod 4$	$2^{n/2}$	?	$s(n)$

III. Maximum Likelihood State Estimation of Shift Register Generators

3.1 Evolution of System Equations

A shift register pn sequence (or m-sequence) generator is an autonomous finite state machine which has a tree representation. Consider an n-stage shift register pn sequence generator shown in Figure 3.1. Let x_k be the kth input, $\underline{S}_k$ be the state vector at the kth time instant and y_k be the kth output symbol. With all arithmetic operations in GF(2), the system equations can be represented as follows:

State equation: $$\underline{S}_{k+1} = F\,\underline{S}_k + \underline{b}\,x_k \tag{3.1}$$

Input equation: $$x_k = \underline{C}^t\,\underline{S}_k \tag{3.2}$$

Output equation: $$y_k = \underline{d}^t\,\underline{S}_k \tag{3.3}$$

where

$$F = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{nxn}, \quad \underline{b} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{nx1}, \quad \underline{S}_k = \begin{bmatrix} S_{k-1} \\ S_{k-2} \\ \vdots \\ S_{k-n} \end{bmatrix}, \quad \underline{d} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}_{nx1}$$

and

$$\underline{C} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}, \quad c_i \in \{0,1\}$$

is the shift register generator coefficient vector. If the coefficients are chosen such that the generator polynomial is primitive, the output sequence $\{y_k\}$ is a maximum length sequence with period $N = 2^n - 1$.

There are 2^n possible states of which the $\underline{0}$ state is an

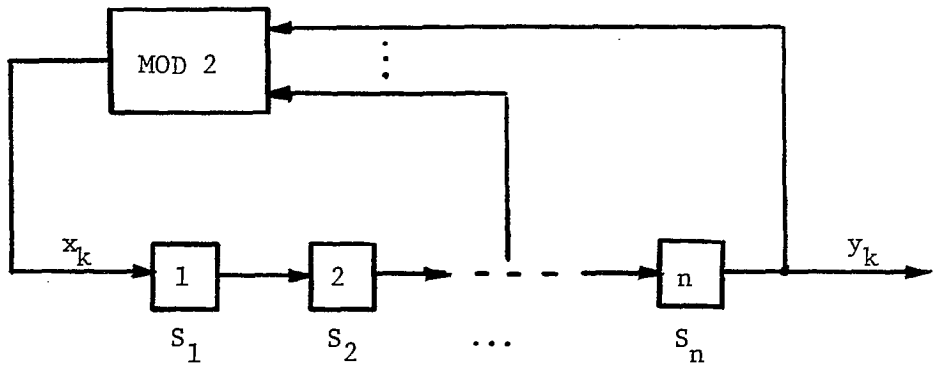


Fig. 3.1 n-Stage Shift Register m-Sequence Generator with Primitive Polynomial F(x).

absorbing state. An n-stage shift register generator has a trellis representation. The case of n = 3 is illustrated in Figure 3.2 where the contents of the boxes denote the states and the edge values $x_k(y_k)$ denote input (output). The thick (heavy) path in Figure 3.2 represents the output $\underline{y}$ of a pn shift register generator with primitive polynomial $F(x) = 1+x+x^3$ and initial state 101. Since $\underline{0}$ is an absorbing state, $\underline{0}$ cannot be a node in any path of a pn sequence. It follows that the all-zeros state path cannot be a valid path and is therefore a "forbidden" path. In fact any path having $\underline{0}$ as a node is a forbidden path.

The input/output relationship of a binary shift register generator is depicted in Figure 3.3 where the input x_k and the output y_k are prescribed, respectively, by (3.2) and (3.3).

3.2 Maximum Likelihood Trellis Search

Under the assumption that the digits $\{y_k\}$ are statistically independent and equally likely to be 0's or 1's (this is a consistent assumption since $\{y_k\}$ is a pn sequence) all paths through the trellis are equally likely. Thus, for optimal state estimation we seek that path $\hat{\underline{z}}$ through the trellis such that

$$P[\underline{r} = \underline{\rho}|\underline{y} = \underline{y}(\hat{\underline{z}})] = \prod_{i=1}^{L} P[r = \rho_i | y = y_1(\hat{\underline{z}})]$$

is maximum, where $\underline{\rho}$ is the actual received sequence, $\underline{y}(\hat{\underline{z}})$ is the pn sequence along the path specified by $\hat{\underline{z}}$, $y_i(\hat{\underline{z}})$ is the ith digit of $\underline{y}(\hat{\underline{z}})$, and L is the depth searched.

Let the superscript m on a vector denote its first m components. A function $L_\rho[\underline{y}^m]$ which satisfies

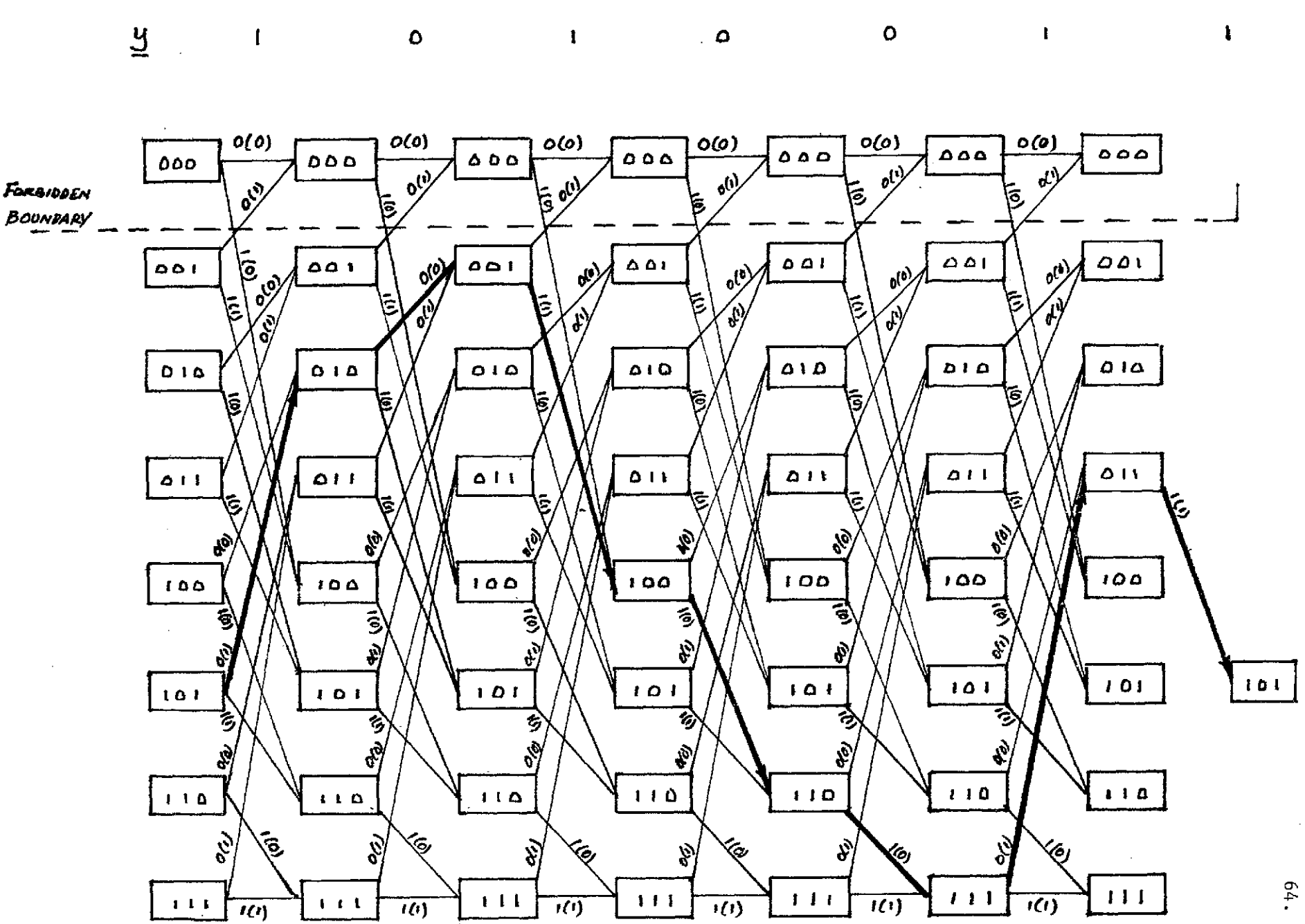


Fig. 3.2 Trellis Diagram for m-sequence Generator with Primitive polynomial $F(x) = 1 + x + x^3$

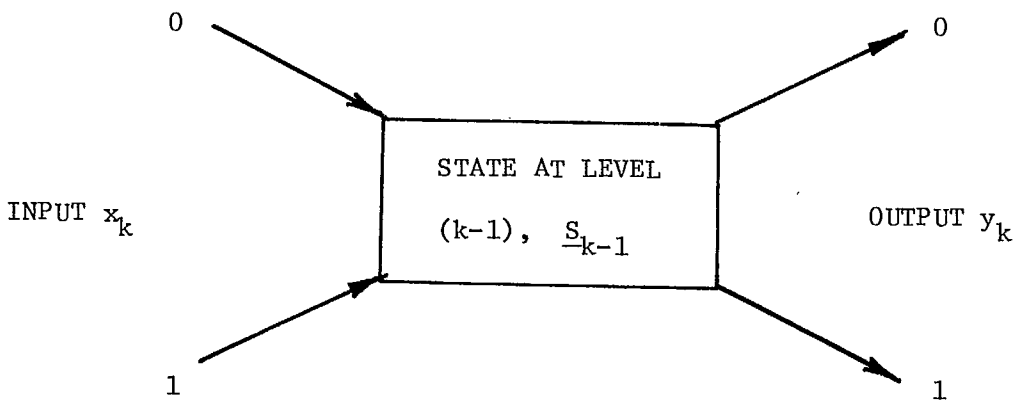


Fig. 3.3 Input/Output Relationship at the kth Time Instant.

$$L_\rho[\underline{y}^m] = \sum_{i=1}^{m} L_\rho[y_i] \tag{3.4}$$

and

$$L_\rho[\underline{y}_1^m] > L_\rho[\underline{y}_2^m]$$

if and only if $P[\underline{r} = \underline{\rho}^m | \underline{y} = \underline{y}_1^m] > P[\underline{r} = \underline{\rho}^m | \underline{y} = \underline{y}_2^m]$ is called a path likelihood function. Optimum state estimation reduces to finding the path $\hat{\underline{z}}$ which maximizes $L_\rho[\underline{y}(\hat{\underline{z}})]$. A nature choice for $L_\rho[y_i]$ is

$$L_\rho[y_i] = \log P[r = \rho_i | y = y_i]. \tag{3.5}$$

On a binary symmetric channel (BSC), $L_p[y_i]$ can take the form

$$L_\rho[y_i] = \begin{cases} 0 & \text{if } \rho_i = y_i \\ -1 & \text{if } \rho_i \neq y_i \end{cases} \tag{3.6}$$

Equation (3.6) is a Hamming metric. Thus, $L_\rho[\underline{y}^m]$ is just the negative of the apparent number of errors between $\underline{\rho}^m$ and $\underline{y}^m$. The optimium path is that path for which $L_\rho[\underline{y}^m]$ is a maximum. In the absence of noise max $L_\rho[\underline{y}^m] = 0$. A maximum likelihood search of the trellis will thus yield the most likely state of the shift register generator. In a noisy environment a decision taken at a depth of approximately 5 times the constraint length of the shift register generator (n in the present case) would yield a "good" decision [Forney, 1973].

3.3 Properties of m-Sequence Generator

The fact that the output symbol of an m-sequence generator corresponds to the nth state variable offers a desirable property which we state in the following theorem:

Theorem 3.1

Any n component vector in a trellis path, excluding the "forbidden" path, represents a state of an antonomous pn sequence generator.

Proof: Since the output symbol is identical to the nth state variable and since a new state is generated by a linear shift of the old state, as in (3.1), n consecutive branch output symbols of a trellis path defines a state vector of the shift register generator.

In the absence of noise and under a single user environment, with probability 1 an exhaustive search of the trellis will yield a correct identification of the generator state. Once the state vector has been correctly identified a local shift register generator can then be initiated to perform the despreading function. It is thus conceivable that a trellis search as a means of identifying the state of the shift register generator offers a possibility for rapid bit synchronization.

Figure 3.4 depicts a maximum likelihood state estimation of an m-sequence generator, with primitive polynomial $F(x) = 1 + x^3 + x^4$ and initial state $\underline{S}_0 = (S_1,S_2,S_3,S_4) = (1001)$, over a length of one period. The heavy path traces out the error-free received sequence $\underline{\rho}$. By theorem 3.1 the inital state 1001 and the subsequent states can then be identified.

While it is intuitively satisfying that a maximum likelihood search of the trellis represents an optimum state estimation of shift register generators, because of the large size of shift register generators needed for CDMA applications, the state space is simply too large for a trellis search to be of practical value. Consider, for example, the 16-stage generator used in the DS and FH/DS systems in section 1, where the number of valid states or nodes (the terms state and node will be used synonymously) is $N = 2^{16}-1 = 65,535$. As there is 1 survivor per node per level searched there are 65,535 survivors per level. If a decision is to be taken only after penetrating the trellis at a depth equal to 5 times the constraint length, then, 80 x 65,535 survivors need to be stored.

In addition 65,535 values of the metric $L_\rho[\underline{y}^{80}]$ must be stored. The following theorem makes trellis search a viable method to perform maximum likelihood state estimation of shift register generators.

Theorem 3.2

An n-stage autonomous shift register generator can be represented by a transformed trellis diagram with fewer than 2^n-1 states if at least one of the state variables of the original state vector is preserved.

Proof:

Since at least one of the state variables of the original state is preserved and since the output symbol of a shift register generator is a delayed version of a state variable, the output sequences traced out in the original and transformed trellis diagrams are identical. Since, by Theorem 3.1, any n component vector of the output sequence $\underline{y}$ represents a state vector of the original trellis diagram, then any state vector of the original trellis can be identified by a search of the transformed trellis.

Theorem 3.2 permits the representation of a general n-stage pn shift register generator by a trellis with a substantially smaller number of states than that of the original trellis. Then maximum likelihood state estimation via a search of the smaller trellis can be practical. Let $\underline{S}'$ be the new state vector. The smallest viable state vector would be one of dimension 2 (dimension 1 is not admissible since a 0 or a 1 input will produce a 0 or 1 output so that an ambiguity exists which prevents a unique inverse mapping to the full state representation), i.e., $\underline{S}' = (S_1', S_2')$. For convenience let $S_2' = S_n$, i.e., preserve the nth state variable of the original state vector, and let $S_1' = f(\underline{S})$. The simplest transformation would be $S_1' = S_1$. This choice of new state assignments has the salient

feature that S_2' is identified with the output symbol y_k and S_1' is identified with the autonomously generated input x_k. For illustrative purposes we again consider the 4-stage example whose full trellis is shown in Figure 3.4. The new trellis diagram with $S_1' = S_1$ and $S_2' = S_4$ has a total of $2^2 = 4$ states, as shown in Figure 3.5. The state transitions in the new trellis is obtained from the original shift register state transitions as shown in Figure 3.6, where 1001 has again been taken to the initial state. The state transitions of the new states are shown in Figure 3.6b, where the edge values $x_k(y_k)$ represent the input x_k generated from the state vector $\underline{S}_k$ in accordance with the primitive polynomial $F(x) = 1 + x^3 + x^4$ and the output y_k which equals the nth state variable. Simply stated, y_k equals S_2' in the present state and x_k equals S_1' in the next state.

The complete new trellis diagram for one period of the output sequence $\underline{y}$ is shown in Figure 3.5. The heavy path again traces out the output sequence $\underline{y}$. The edge label on the trellis is of the form $x_k(y_k)(L_\rho[\underline{y}^k])$ where $L_\rho[\underline{y}^k]$ is the likelihood function given by equations (3.4) and (3.6). If the received sequence is noise-free, i.e., $\underline{\rho} = \underline{y}$, which is the case shown in Figure 3.5, then any 4 consecutive received symbols along the heavy path represent a state of the original shift register generator, with initial state 1001.

Maximum likelihood trellis search amounts to comparing the kth received symbol ρ_k with each possible branch output symbol at the kth level, as k takes on the integer values 1,2,... . Since x_k and y_k are computed from the same state vector, there is only one value of y_k at any one time instant whether x_k is a 0 or a 1 as dictated by the value of S_1' in the next state. The metric $L_\rho[y_i]$ associated with a $0(y_k)(L_\rho[y_i])$ or

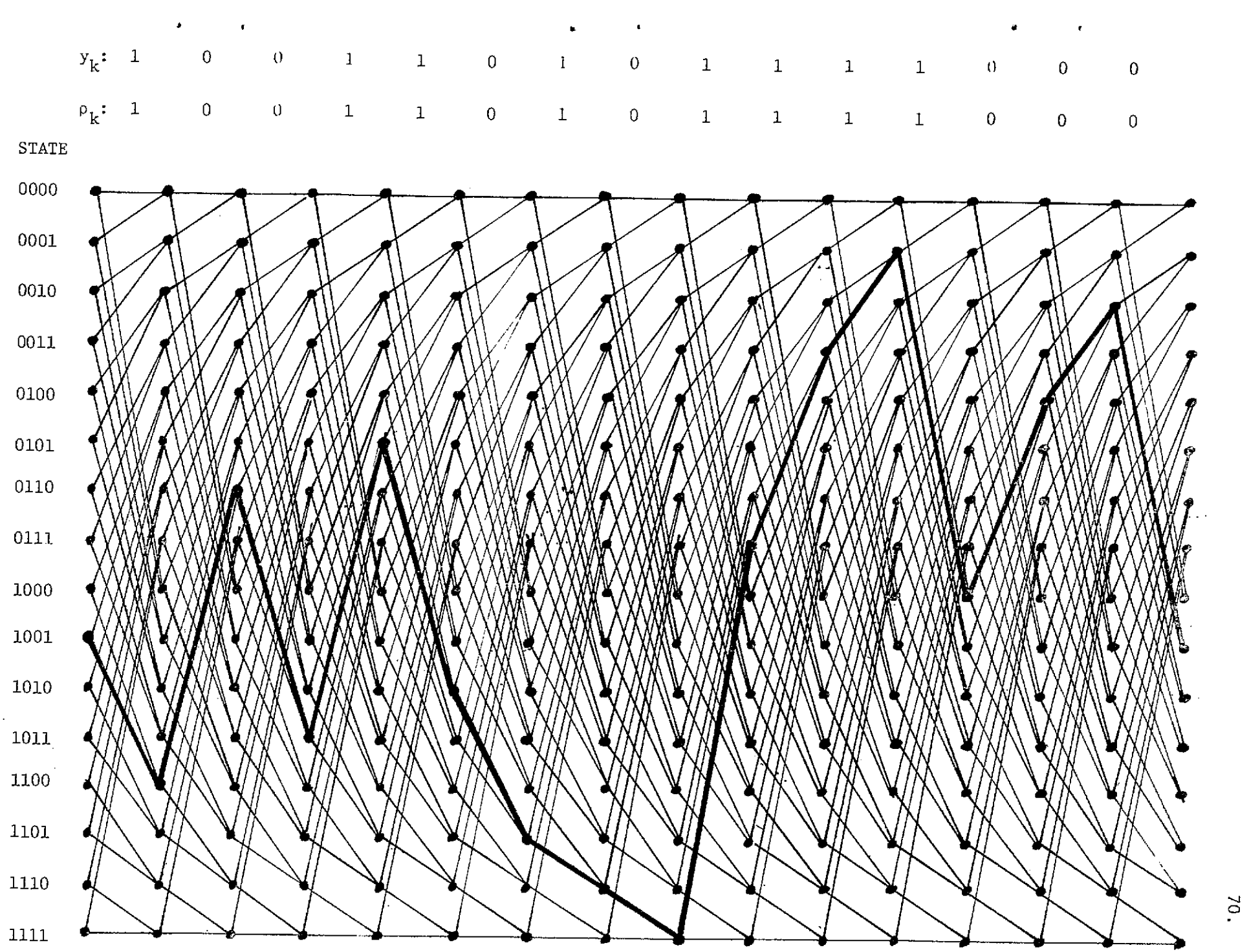


Fig. 3.4 Trellis Diagram for m-Sequence Generator with Primitive Polynomial $F(x) = 1 + x^3 + x^4$ (Error-Free Sequence Reception)

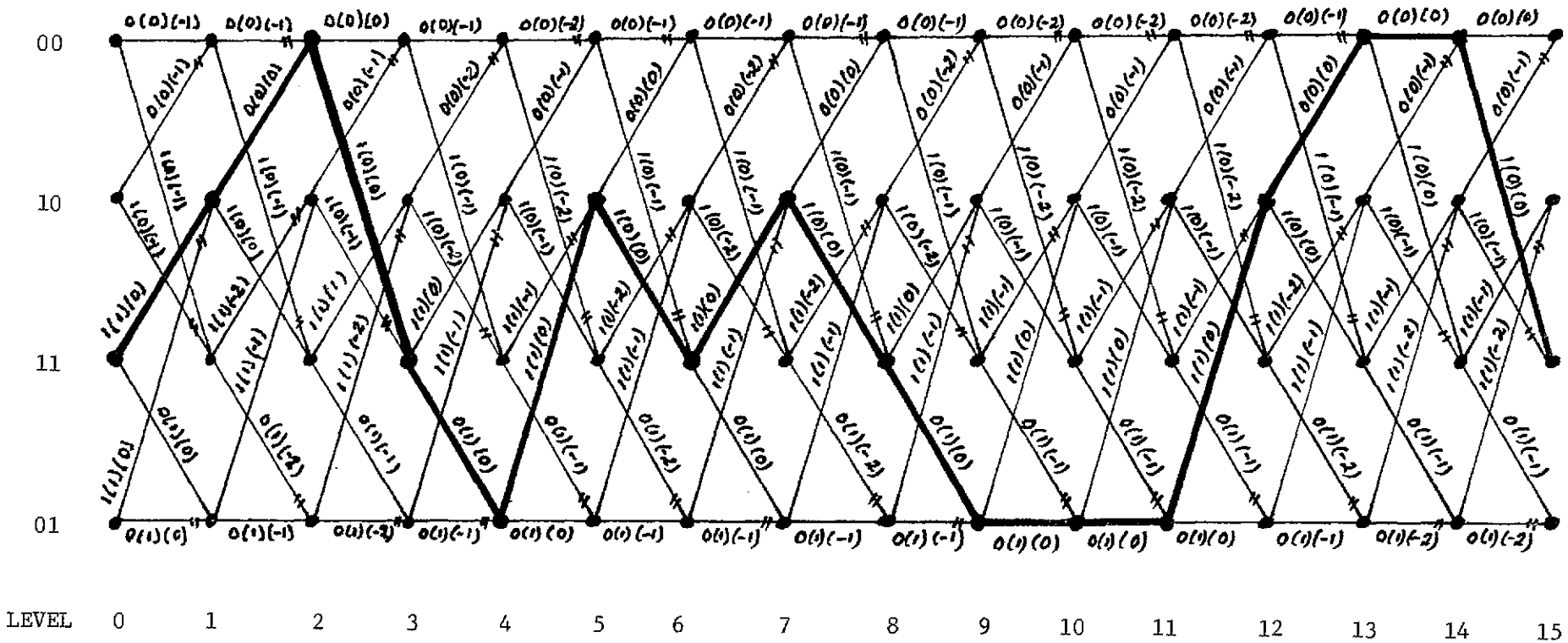
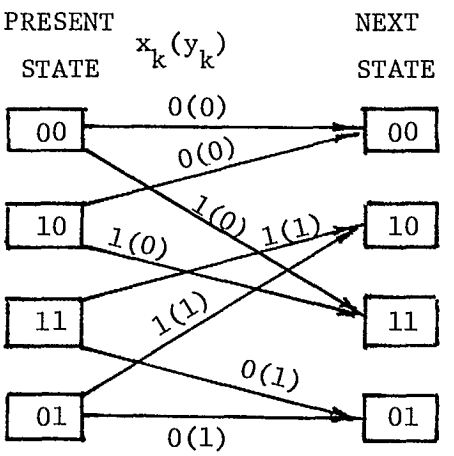


Fig. 3.5 "Reduced" Trellis Search for Detection of Error-Free m-Sequence Generated by Primitive Polynomial

$F(x) = 1 + x^3 + x^4$

OLD STATES S	NEW STATES S'
1001	11
1100	10
0110	00
1011	11
0101	01
1010	10
1101	11
1110	10
1111	11
0111	01
0011	01
0001	01
1000	10
0100	00
0010	00
1001	11

(a) STATE TRANSITIONS FOR $F(x) = 1 + x^3 + x^4$



(b) STATE TRANSITION DIAGRAM

Fig. 3.6 State Transitions for "Reduced" Trellis

a $1(y_k)(L_\rho[y_i])$ edge value that emanates from the same node are thus identical. Thus, at level 14 in Figure 3.5, we have a transition from state 00 to state 00 with edge value 0(0)(0) and a transition from the same state to state 11 with edge value 1(0)(0). The 00 - 11 transition is chosen because 00 - 00 is not a valid transition in which the heavy path leading to node 00 at level 14 is a prefix. It is noted also that there are two branches merging into node 10 at level 1 with a branch metric $L_\rho[y_1] = 0$. These branches emanate from nodes 11 and 01 at level 0. Since 11 corresponds to one of the original states 1001, 1011, 1101 or 1111, and since the initial 4-tuple in the estimated sequence is 1001, the state 11 at level 0 is chosen as the root node. It also identifies 1001 as the initial state of the m-sequence generator.

In the pruning of the trellis branches entering any one node, the one with a larger metric (likelihood function) survives. Whenever there is a tie, the lower branch is arbitrarily cut, except when it concerns the seeking of the root node at level 0 (in the present example it is only by coincidence that the branch from the root node 11 at level 0 is also an upper branch, which survives the cut).

The output from a binary symmetric channel has an effect similar to that of a hard decision. An error will change the binary digit to its complement. The effect of one error on the "reduced" trellis search is illustrated in Figure 3.7. The error, although occurring at a depth between the level 5 and level 6 nodes, exerts an effect which permeates to the immediately preceding and following branches. As illustrated in Figure 3.7 the dashed heavy subpath lying between the 4th level node and the 7th level node represents the correct subpath. However, the error causes the solid

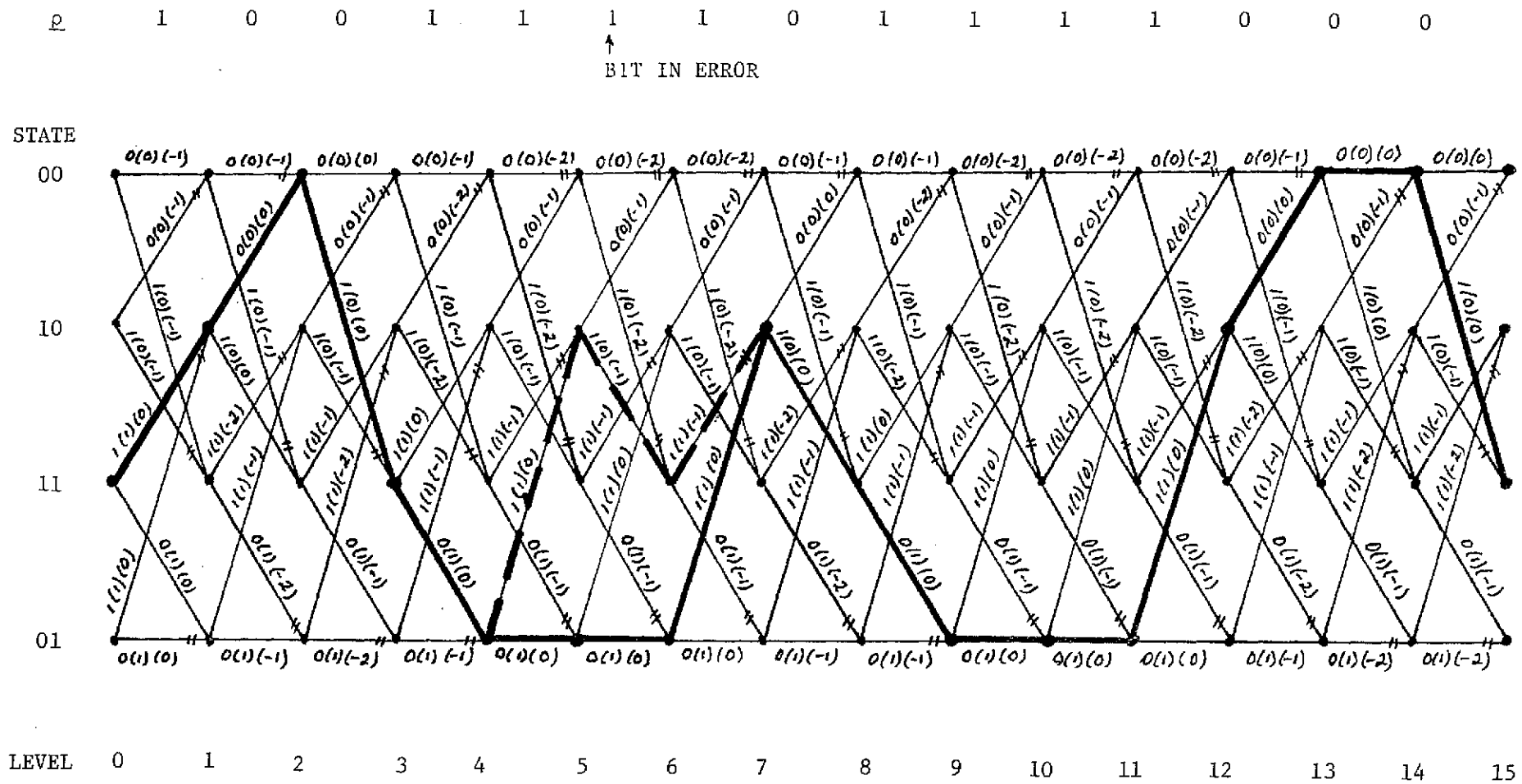


Fig. 3.7 "Reduced" Trellis Search for Reception of m-Sequence Generated by Primitive Polynomial $F(x) = 1 + x^3 + x^4$ (One Bit in Error)

heavy subpath over the same span to be selected as the optimum estimate. It is noted that the correct (dashed) and the apparent (solid) subpath depart at the level 4 node and re-merge at the level 7 node. A knowledge of the generator polynomial together with the information about the states before and after the error event permit the making of a decision that the dashed subpath is the correct perfix and suffix to the error-free heavy subpaths. This error correction capability is an inherent property of the shift register generator, which we state in the following theorem:

Theorem 3.3

A knowledge of the generator polynomial is sufficient to correct random errors in the maximum likelihood searched reduced trellis.

3.4 Comments

Although a maximum likelihood search of the trellis offers a means of performing state estimation, the state space of a shift register generator needed in CDMA applications is simply too large for a search of the full trellis to be of practical use. The fact that the generator output sequence is a delayed version of any one of the generator state variables permits the representation of a shift register generator by an equivalent but "reduced" trellis. By preserving at least one of the variables of the original state vector, a general n-stage shift register generator can be represented by a 4-state trellis to make maximum likelihood state estimation a practical scheme.

A random error such as that introduced in Figure 3.7 would have been corrected by a maximum likelihood search of the full trellis. As illustrated in Figure 3.7 a maximum likelihood search of the "reduced" trellis alone cannot correct the error. In this case knowledge of the

generator structure is needed to correct the error. Here then lies the trade-off between maximum likelihood state estimation using the full trellis or the reduced trellis.

IV. Conclusions

Three aspects of CDMA spread spectrum communication have been studied and reported. Section I presents a thorough investigation of a subsequence matched filtering approach to rapid acquisition in a DS or FH/DS system. The investigations have been carried out analytically and by means of computer simulations. Simulation results enabled the modelling of the subsequence matched filter outputs (the subsequence correlations) as a Gaussian sequence. The Gaussian model permits the formulation of expressions for probabilities of synch acquisition, false alarm, false dismissal, and time to acquisition. For the case studied in which one data digit corresponds to one period of a pn sequence, it is shown that subsequence matched filtering is indeed a viable method for rapid acquisition for either the DS or the FH/DS system. In the FH/DS case, discrimination against interference from unwanted transmitters manifests itself in the approximate orthogonal properties of the time and frequency codes. The added spatial orthogonality in an FH/DS system, through frequency hopping, renders subsequence matched filtering a suitable technique for rapid acquisition, as revealed by the simulation results shown in Fig. 1.10.

Section II describes different sequence design strategies, which may serve as alternatives to the m-sequence, for CDMA purposes. The impact of these sequences, for example the bent sequence, as candidates for CDMA applications, particularly the rapid acquisition mode, need further investigation.

Section III focuses attention on maximum likelihood state estimation via a search of a "reduced" trellis. The properties of shift register sequences, which enable their representation by a reduced trellis, are discussed. The main idea behind the study of "reduced" state trellis representations and the associated maximum likelihood estimation is the introduction of an easily implementable state estimation scheme for synchronization purposes. This appears to be a fruitful approach and further investigation in this direction will be carried out.

References

T. Helleseth, A Note on the Cross Correlation Function Between Two Binary Maximal Length Linear Sequence, Discrete Mathematics, 23 (1978), 301-307.

R. C. Dixon, Spread Spectrum Systems, John Wiley and Sons (Wiley-Interscience), New York (1976).

J. W. Mark and I. F. Blake, Rapid Acquisition Using Subsequences, Final Report (Part II), Project No. 808-01, Department of Supply and Services, Ottawa, Canada (1979).

J. H. Lindholm, An Analysis of the Pseudo-Randomness Properties of Subsequences of Long m-Sequences, IEEE Trans. Inf. Th., 14 (1968), 569-576.

D. E. Cartier, Partial Correlation Properties of Pseudonoise (PN) Codes in Noncoherent Synchronization/Detection Schemes, IEEE Trans. Comm., 24 (1976), 898-903.

S. Wainberg and J. K. Wolf, Subsequences of Pseudorandom Sequences, IEEE Trans. Comm. Tech., 18 (1970), 606-612.

M. B. Pursley, Performance Evaluation for Phase-Coded Spread-Spectrum Multiple-Access Communication - Part I: System Analaysis, IEEE Trans. Comm., 25 (1977), 795-799.

W. F. Utlaut, Spread Spectrum, IEEE Communications Magazine (1978), September 21-30.

M. B. Pursley and D. V. Sarwate, Performance Evaluation for Phase-Coded Spread-Spectrum Multiple-Access Communication - Part II: Code Sequence Analysis, IEEE Trans. Comm., 25 (1977), 800-803.

A. J. Viterbi, Spread Spectrum Communications - Myths and Realities, IEEE Communications Magazine, (1979) May, 11-18.

R. B. Ward and K. P. Yui, Acquisition of Pseudonoise Signals by Recursion-Aided Sequential Estimation, IEEE Trans. Comm., 25 (1977), 784-794.

R. B. Ward and K. P. Yui, Acquisition of Pseudonoise Signals by Recursions-Aided Sequential Estimation, National Telecommunication Conference (1977), 35:1-1 - 35:1-13.

R. B. Ward, Acquisition of Pseudonoise Signals by Sequential Estimation, IEEE Trans. Comm. Tech., 13 (1965), 475-483.

H. M. Pearce and M. P. Ristenbatt, The Threshold Decoding Estimator for Synchronization with Binary Linear Recursive Sequences, International Communications Conference (1971), 43.25 - 43.30.

T. Helleseth, Some Results About the Cross-correlation Function Between Two Maximal Linear Sequences, Discrete Mathematics, 16 (1976), 209-232.

H. P. Hartmann, Analysis of a Dithering Loop for PN Code Tracking, IEEE Trans. Aerosp. Elec. Sys., 10 (1974), 2-9.

M. K. Simon, Noncoherent Pseudonoise Code Tracking Performance of Spread Spectrum Receivers, IEEE Trans. Comm., 25 (1977), 327-345.

C. C. Kilgus, Pseudonoise Code Acquisition Using Majority Logic Decoding, IEEE Trans. Comm., 21 (1973), 772-774.

J. K. Holmes, Acquisition Time Performance of PN Spread-Spectrum Systems, IEEE Trans. Comm., 25 (1977), 778-783.

P. M. Hopkins, A Unified Analysis of Pseudonoise Synchronization by Envelope Correlation, IEEE Trans. Comm., 25 (1977), 770-777.

G. F. Sage, Serial Synchronization of Pseudonoise Systems, IEEE Trans. Comm. Tech., (1964), 123-127.

I. F. Blake and J. W. Mark, CDMA Sequences and Techniques, Technical Report for Project No. 808-01, Department of Supply and Services of Canada. Department of Electrical Engineering, University of Waterloo (1978).

D. V. Sarwate and M. B. Pursley, Crosscorrelation Properties of Pseudorandom and Related Sequences, Proc. IEEE (to appear 1980).

J. L. Massey and J. J. Uhran, Sub-Band Coding, Proceedings 13th Annual Allerton Conference on Circuit and System Theory, October, 1975.

L. R. Welch, Lower Bounds on the Maximum Cross Correlation of Signals, IEEE Trans. Inf. Th., vol. IT-20, 397-399 (1974).

V. M. Sidelinkov, On Mutual Correlation of Sequences, Soviet Math. Dokl., vol. 12, 197-201 (1971).

R. Gold, Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions, IEEE Trans. Inf. Th., vol. IT-14, 154-156 (1968).

I. F. Blake and R.C. Mullin, The Mathematical Theory of Coding, Academic Press, New York, 1975.

T. Kasami, Weight Distribution of Bose - Chaudhuri - Holguenghem Codes, in Combinatorial Mathematics and its Applications, Univ. North Carolina Press, Chapel Hill, 1969.

J. H. van Lint, Coding Theory, Springer-Verlag, Berlin, volume 201, Lecture Notes in Mathematics, 1971.

O. S. Rothaus, On "Bent" Functions, Jour. Comb. Th. (A), vol. 201, 300-305 (1976).

F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland Publishing Company, Amsterdam, 1977.

J. D. Olsen, R. A. Scholz and L. R. Welch, Bent-function Sequences, to appear, (1980).

L. R. Welch, personal correspondence, 1980.

A. Lempel and M. Cohn, Maximal Families of Bent Sequences, to appear, 1980.

G. D. Forney, Jr., The Viterbi Algorithm, Proc. IEEE, 61 (1973), 268-278.

J. L. Massey, Coding Technique for Digital Communications, ICC'73 Tutorial Notes, 1973.