Theory of Spread-Spectrum Communications—A Tutorial

RAYMOND L. PICKHOLTZ, FELLOW, IEEE, DONALD L. SCHILLING, FELLOW, IEEE, AND LAURENCE B. MILSTEIN, SENIOR MEMBER, IEEE

Abstract—**Spread-spectrum communications, with its inherent interference attenuation capability, has over the years become an increasingly popular technique for use in many different systems. Applications range from antijam systems, to code division multiple access systems, to systems designed to combat multipath. It is the intention of this paper to provide a tutorial treatment of the theory of spread-spectrum communications, including a discussion on the applications referred to above, on the properties of common spreading sequences, and on techniques that can be used for acquisition and tracking.**

I. INTRODUCTION

SPREAD-spectrum systems have been developed since about the mid-1950's. The initial applications have been to military antijamming tactical communications, to guidance systems, to experimental antimultipath systems, and to other applications [1]. A definition of spread spectrum that adequately reflects the characteristics of this technique is as follows:

> "Spread spectrum is a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by means of a code which is independent of the data, and a synchronized reception with the code at the receiver is used for despreading and subsequent data recovery."

Under this definition, standard modulation schemes such as FM and PCM which also spread the spectrum of an information signal do not qualify as spread spectrum.

There are many reasons for spreading the spectrum, and if done properly, a multiplicity of benefits can accrue simultaneously. Some of these are

- Antijamming
- Antiinterference
- Low probability of intercept
- Multiple user random access communications with selective addressing capability
- High resolution ranging
- Accurate universal timing.

Manuscript received December 22, 1981; revised February 16, 1982

R. L. Pickholtz is with the Department of Electrical Engineering and Computer Science, George Washington University, Washington, DC 20052.

D. L. Schilling is with the Department of Electrical Engineering City College of New York, New York, NY 10031.

L. B. Milstein is with the Department of Electrical Engineering and Computer Science, University of California at San Diego, La Jolla CA 92093.

The means by which the spectrum is spread is crucial. Several of the techniques are "direct-sequence" modulation in which a fast pseudorandomly generated sequence causes phase transitions in the carrier containing data, "frequency hopping," in which the carrier is caused to shift frequency in a pseudorandom way, and "time hopping," wherein bursts of signal are initiated at pseudorandom times. Hybrid combinations of these techniques are frequently used.

Although the current applications for spread spectrum continue to be primarily for military communications, there is a growing interest in the use of this technique for mobile radio networks (radio telephony, packet radio, and amateur radio), timing and positioning systems, some specialized applications in satellites, etc. While the use of spread spectrum naturally means that each transmission utilizes a large amount of spectrum, this may be compensated for by the interference reduction capability inherent in the use of spread-spectrum techniques, so that a considerable number of users might share the same spectral band. There are no easy answers to the question of whether spread spectrum is better or worse than conventional methods for such multiuser channels. However, the one issue that is clear is that spread spectrum affords an opportunity to give a desired signal a power advantage over many types of interference, including most intentional interference (i.e., jamming). In this paper, we confine ourselves to principles related to the design and analysis of various important aspects of a spread-spectrum communications system. The emphasis will be on direct-sequence techniques and frequency-hopping techniques.

The major systems questions associated with the design of a spread-spectrum system are: How is performance measured? What kind of coded sequences are used and what are their properties? How much jamming/interference protection is achievable? What is the performance of any user pair in an environment where there are many spread spectrum users (code division multiple access)? To what extent does spread spectrum reduce the effects of multipath? How is the relative timing of the transmitter-receiver codes established (acquisition) and retained (tracking)?

It is the aim of this tutorial paper to answer some of these questions succinctly, and in the process, offer some insights into this important communications technique. A glossary of the symbols used is provided at the end of the paper.

II. SPREADING AND DIMENSIONALITY—PROCESSING GAIN

A fundamental issue in spread spectrum is how this technique affords protection against interfering signals with

0090-6778/82/0500-0355$00.75

finite power. The underlying principle is that of distributing a relatively low dimensional (defined below) data signal in a high dimensional environment so that a jammer with a fixed amount of total power (intent on maximum disruption of communications) is obliged to either spread that fixed power over all the coordinates, thereby inducing just a little interference in each coordinate, or else place all of the power into a small subspace, leaving the remainder of the space interference free.

A brief discussion of a classical problem of signal detection in noise should clarify the emphasis on finite interference power. The "standard" problem of digital transmission in the presence of thermal noise is one where both transmitter and receiver know the set of M signaling waveforms $\{S_i(t), 0 \leqslant t \leqslant T;\ 1 \leqslant i \leqslant M\}$. The transmitter selects one of the waveforms every T seconds to provide a data rate of $\log_2 M/T$ bits/s. If, for example, $S_j(t)$ is sent, the receiver observes $r(t) = S_j(t) + n_w(t)$ over $[0, T]$ where $n_w(t)$ is additive, white Gaussian noise (AWGN) with (two-sided) power spectral density $\eta_0/2$ W/Hz.

It is well known [3] that the signal set can be completely specified by a linear combination of no more than $D \leqslant M$ orthonormal basis functions (see below), and that although the white noise, similarly expanded, requires an infinite number of terms, only those within the signal space are "relevant" [3]. We say that the signal set defined above is D-dimensional if the minimum number of orthonormal basis functions required to define all the signals is D. D can be shown to be [3] approximately $2B_DT$ where B_D is the total (approximate) bandwidth occupancy of the signal set. The optimum (minimum probability of error) detector in AWGN consists of a bank of correlators or filters matched to each signal, and the decision as to which was the transmitted signal corresponds to the largest output of the correlators.

Given a specific signal design, the performance of such a system is well known to be a function only of the ratio of the energy per bit to the noise spectral density. Hence, against white noise (which has infinite power and constant energy in every direction), the use of spreading (large $2B_DT$) offers no help. The situation is quite different, however, when the "noise" is a jammer with a fixed *finite* power. In this case, the effect of spreading the signal bandwidth so that the jammer is uncertain as to where in the large space the components are is often to force the jammer to distribute its finite power over many different coordinates of the signal space.

Since the desired signal can be "collapsed" by correlating the signal at the receiver with the known code, the desired signal is protected against a jammer in the sense that it has an effective power advantage relative to the jammer. This power advantage is often proportional to the ratio of the dimensionality of the space of code sequences to that of the data signal. It is necessary, of course, to "hide" the pattern by which the data are spread. This is usually done with a pseudonoise (PN) sequence which has desired randomness properties and which is available to the cooperating transmitter and receiver, but denied to other undesirable users of the common spectrum.

A general model which conveys these ideas, but which uses random (rather than pseudorandom) sequences, is as follows. Suppose we consider transmission by means of D equiprobable and equienergy orthogonal signals imbedded in an n-dimensional space so that

$$S_i(t) = \sum_{k=1}^{n} S_{ik}\phi_k(t); \qquad 1 \leqslant i \leqslant D; \qquad 0 \leqslant t \leqslant T$$

where

$$S_{ik} = \int_0^T S_i(t)\phi_k(t)\,dt$$

and where $\{\phi_k(t);\ 1 \leqslant k \leqslant n\}$ is an orthonormal basis spanning the space, i.e.,

$$\int_0^T \phi_l(t)\phi_m(t)\,dt = \delta_{lm} \triangleq \begin{cases} 1 & l = m \\ 0 & l \neq m. \end{cases}$$

The average energy of each signal is

$$\int_0^T \overline{S_i^2(t)}\,dt = \sum_{k=1}^{n} \overline{S_{ik}^2} \triangleq E_s; \qquad 1 \leqslant i \leqslant D \tag{1}$$

(the overbar is the expected value over the ensemble).

In order to hide this D-dimensional signal set in the larger n-dimensional space, choose the sequence of coefficients S_{ik} independently (say, by flipping a fair coin if a binary alphabet is used) such that they have zero mean and correlation

$$\overline{S_{ik}S_{il}} \triangleq \frac{E_s}{n}\delta_{kl}; \qquad 1 \leqslant i \leqslant D. \tag{2}$$

Thus, the signals, which are also assumed to be known to the receiver (i.e., we assume the receiver had been supplied the sequences S_{ik} before transmission) but denied to the jammer, have their respective energies uniformly distributed over the n basis directions as far as the jammer is concerned.

Consider next a jammer

$$J(t) = \sum_{k=1}^{n} J_k\phi_k(t); \qquad 0 \leqslant t \leqslant T \tag{3}$$

with total energy

$$\int_0^T J^2(t)\,dt = \sum_{k=1}^{n} J_k^2 \triangleq E_J \tag{4}$$

which is added to the signal with the intent to disrupt communications. Assume that the jammer's signal is independent of the desired signal. One of the jammer's objectives is to devise a strategy for selecting the components J_k^2 of his fixed total energy E_J so as to minimize the postprocessing signal-to-noise ratio (SNR) at the receiver.

The received signal

$$r(t) = S_i(t) + J(t) \tag{5}$$

is correlated with the (known) signals so that the output of the ith correlator is

$$U_i \triangleq \int_0^T r(t)S_i(t)\,dt = \sum_{k=1}^{n} (S_{ik}^2 + J_k S_{ik}). \tag{6}$$

Hence,

$$E(U_i \mid S_i) = \sum_{k=1}^{n} \overline{S_{ik}^2} = E_s \tag{7}$$

since the second term averages to zero. Then, since the signals are equiprobable,

$$E(U_i) = \frac{E_s}{D}. \tag{8}$$

Similarly, using (1) and (2),

$$\begin{aligned} \text{var}\,(U_i \mid S_i) &= \sum_{k,l} J_k J_l \overline{S_{ik} S_{il}} \\ &= \sum_{k=1}^{n} J_k^2 \overline{S_{ik}^2} \\ &= \frac{E_s}{n} E_J \end{aligned} \tag{9}$$

and

$$\text{var}\, U_i = \frac{E_s}{nD} E_J. \tag{10}$$

A measure of performance is the signal-to-noise ratio defined as

$$\text{SNR} = \frac{E^2(U)}{\text{var}\,(U)} = \frac{E_s}{E_J} \cdot \frac{n}{D}. \tag{11}$$

This result is *independent of the way that the jammer distributes his energy*, i.e., regardless of how J_k is chosen subject to the constraint that $\Sigma_k J_k^2 = E_J$, the postprocessing SNR (11) gives the signal an advantage of n/D over the jammer. This factor n/D is the *processing gain* and it is exactly equal to the ratio of the dimensionality of the *possible* signal space (and therefore the space in which the jammer must seek to operate) to the dimensions needed to actually transmit the signals. Using the result that the (approximate) dimensionality of a signal of duration T and of approximate bandwidth B_D is $2B_DT$, we see the processing gain can be written as

$$G_P = \frac{n}{D} \cong \frac{2B_{ss}T}{2B_DT} = \frac{B_{ss}}{B_D} \tag{12}$$

where B_{ss} is the bandwidth in hertz of the (spread-spectrum) signals $S_i(t)$ and B_D is the minimum bandwidth that would be required to send the information if we did not need to imbed it in the larger bandwidth for protection.

A simple illustration of these ideas using random binary sequences will be used to bring out some of these points. Consider the transmission of a single bit $\pm\sqrt{E_b/T}$ with energy E_b of duration T seconds. This signal is one-dimensional. As shown in Figs. 1 and 2, the transmitter multiplies the data bit $d(t)$ by a binary ± 1 "chipping" sequence $p(t)$ chosen randomly at rate f_c chips/s for a total of f_cT chips/bit. The dimensionality of the signal $d(t)p(t)$ is then $n = f_cT$. The received signal is

$$r(t) = d(t)p(t) + J(t), \qquad 0 \leqslant t \leqslant T, \tag{13}$$

ignoring, for the time being, thermal noise.

The receiver, as shown in Fig. 1, performs the correlation

$$U \triangleq \sqrt{\frac{E_b}{T}} \int_0^T r(t)p(t)\,dt \tag{14}$$

and makes a decision as to whether $\pm\sqrt{E_b/T}$ was sent depending upon $U \gtrless 0$. The integrand can be expanded as

$$r(t)p(t) = d(t)p^2(t) + J(t)p(t) = d(t) + J(t)p(t), \tag{15}$$

and hence the data bit appears in the presence of a code-modulated jammer.

If, for example, $J(t)$ is additive white Gaussian noise with power spectral density $\eta_{0J}/2$ (two-sided), so is $J(t)\,p(t)$, and U is then a Gaussian random variable. Since $d(t) = \pm\sqrt{E_b/T}$, the conditional mean and variance of U, assuming that $\pm\sqrt{E_b/T}$ is transmitted, is given by E_b and $E_b(\eta_{0J}/2)$, respectively, and the probability of error is [3] $Q(\sqrt{2E_b/\eta_{0J}})$ where $Q(x) \triangleq \int_x^\infty (1/\sqrt{2\pi})e^{-y^2/2}\,dy$. Against white noise of unlimited power, spread spectrum serves no useful purpose, and the probability of error is $Q(\sqrt{2E_b/\eta_{0J}})$ regardless of the modulation by the code sequence. White noise occupies all dimensions with power $\eta_{0J}/2$. The situation is different, however, if the jammer power is limited. Then, not having access to the random sequence $p(t)$, the jammer with available energy E_J (power E_J/T) can do better than to apply this energy to one dimension. For example, if $J(t) = \sqrt{E_J/T}$, $0 \leqslant t \leqslant T$, then the receiver output is

$$U = E_b + \sqrt{E_bE_J}\,\frac{1}{n}\sum_{i=1}^{n} X_i \tag{16}$$

where the X_i's are i.i.d.[1] random variables with $P(X_i = +1) = P(X_i = -1) = \frac{1}{2}$. The signal-to-noise ratio (SNR) is

$$\frac{E^2(U)}{\text{var}\,(U)} = \frac{E_b}{E_J} n. \tag{17}$$

Thus, the SNR may be increased by increasing n, the process-

[1] Independent identically distributed.

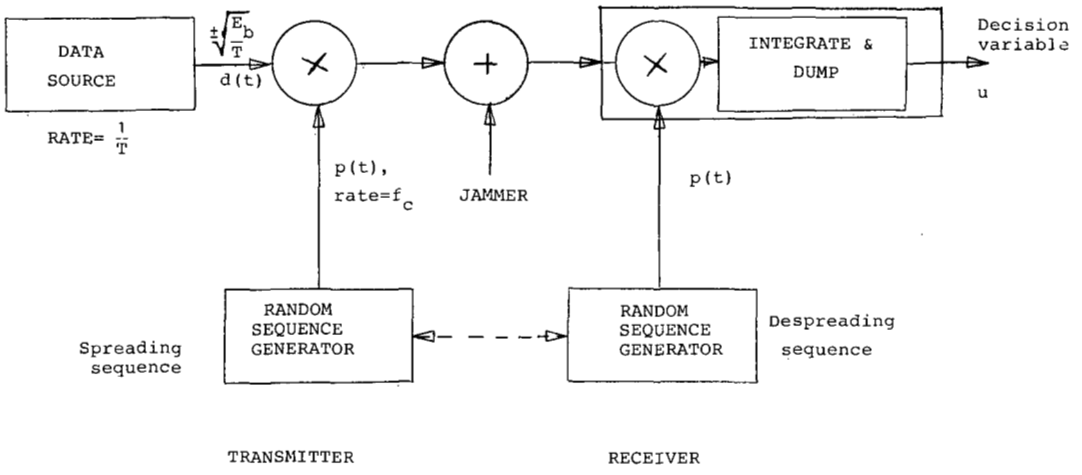


Fig. 1. Direct-sequence spread-spectrum system for transmitting a single binary digit (baseband).

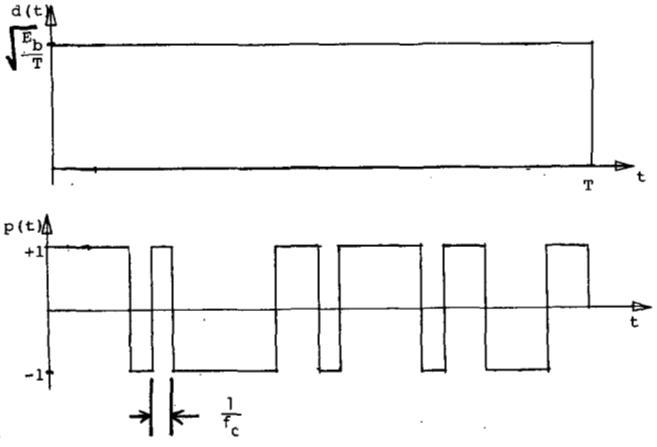


Fig. 2. Data bit and chipping sequence.

ing gain, and it has the form of (11). As a further indication of this parameter, we may compute the probability P_e that the bit is in error from (16). Assuming that a "minus" is transmitted, we have

$$P_e = P(U > 0) = P(Z_n > \alpha n) = \begin{cases} \dfrac{1}{2^n} \displaystyle\sum_{[\alpha n]}^{n} \binom{n}{k}; & \dfrac{E_b}{E_J} < 1 \\ 0; & \dfrac{E_b}{E_J} \geqslant 1 \end{cases} \tag{18}$$

where

$Z_n \triangleq \dfrac{1}{2} \displaystyle\sum_{i=1}^{n} (1 + X_i)$ is a Bernoulli random variable with mean $\dfrac{n}{2}$ and variance $\dfrac{n}{4}$,

$\alpha \triangleq \dfrac{1}{2}\left(1 + \sqrt{\dfrac{E_b}{E_J}}\right)$,

and $[X]$ is defined as the integer portion of X. The partial binomial sum on the right-hand side of (18) may be upper bounded [2] by

$$P_e \leqslant \frac{1}{2^n}\left(\frac{1}{1-\alpha}\right)^{n}\left(\frac{1-\alpha}{\alpha}\right)^{\alpha n}; \qquad \tfrac{1}{2} < \alpha \leqslant 1$$

or

$$P_e \leqslant 2^{-n[1-H(\alpha)]}; \qquad \tfrac{1}{2} < \alpha \leqslant 1 \tag{19}$$

where $H(\alpha) \triangleq -\alpha \log_2 \alpha - (1-\alpha)\log_2 (1-\alpha)$ is the binary entropy function. Therefore, for any $\alpha > \frac{1}{2}$ (or $E_b \neq 0$), P_e may be made vanishingly small by increasing n, the processing gain. (The same result is valid even if the jammer uses a chip pattern other than the constant, all-ones used in the example above.) As an example, if $E_J = 9E_b$ (jammer energy 9.5 dB larger than that of the data), then $\alpha = 2/3$ and $P_e \leqslant 2^{-0.085n}$ If $n = 200$ (23 dB processing gain), $P_e < 7.6 \times 10^{-6}$.

An approximation to the same result may be obtained by utilizing a central limit type of argument that says, for large n, U in (16) may be treated as if it were Gaussian. Then

$$P_e = P(U < 0) \cong Q\left(\sqrt{\frac{E_b}{E_J}\, n}\right) \tag{20}$$

and, if $E_b/E_J = -9.5$ dB and $n = 200$ (23 dB), $P_e \cong Q(\sqrt{22}) \simeq 1.5 \times 10^{-6}$. The processing gain can be seen to be a multiplier of the "signal-to-jamming" ratio E_b/E_J.

A more traditional way of describing the processing gain, which brings in the relative bandwidth of the data signal and that of the spread-spectrum modulation, is to examine the power spectrum of an *infinite sequence* of data, modulated by the rapidly varying random sequence. The spectrum of the random data sequence with rate $R = 1/T$ bits/s is given by

$$S_D(f) = T\left(\frac{\sin \pi f T}{\pi f T}\right)^2 \tag{21}$$

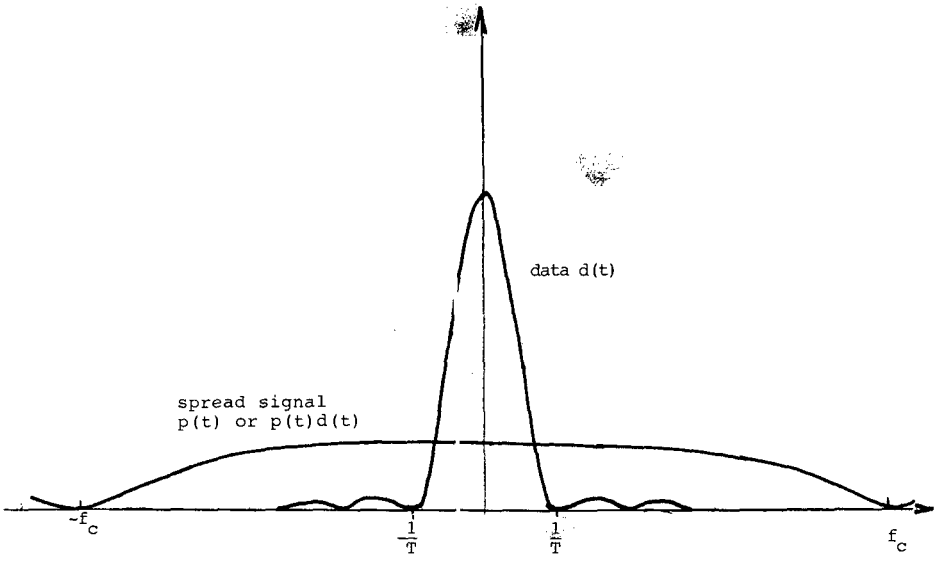


Fig. 3. Power spectrum of data and of spread signal.

and that of the spreading sequence [and also that of the product $d(t)\,p\,(t)$] is given by

$$S_{ss}(f) = \frac{1}{f_c}\left(\frac{\sin \pi f/f_c}{\pi f/f_c}\right)^2. \tag{22}$$

Both are sketched in Fig. 3. It is clear that if the receiver multiplies the received signal $d(t)p(t) + J(t)$ by $p(t)$ giving $d(t) + J(t)p(t)$, the first term may be extracted virtually intact with a filter of bandwidth $1/T \triangleq B_D$ Hz. The second term will be spread over at least f_c Hz as shown in Fig. 3. The fraction of power due to the jammer which can pass through the filter is then roughly $1/f_cT$. Thus, the data have a power advantage of $n = f_cT$, the processing gain. As in (12) the processing gain is frequently expressed as the ratio of the bandwidth of the spread-spectrum waveform to that of the data, i.e.,

$$G_p \triangleq \frac{B_{ss}}{B_D} = f_cT = n. \tag{23}$$

The notion of processing gain as expressed in (23) is simply a power improvement factor which a receiver, possessing a replica of the spreading signal, can achieve by a correlation operation. It must not be automatically extrapolated to anything else. For example, if we use frequency hopping for spread spectrum employing one of N frequencies every T_H seconds, the total bandwidth must be approximately N/T_H (since keeping the frequencies orthogonal requires frequency spacing $\approx 1/T_H$). Then, according to (12), $G_p = (N/T_H)/B_D$. Now if we transmit 1 bit/hop, $T_HB_D \simeq 1$ and $G_P = N$, the number of frequencies used. If $N = 100$, $G_p = 20$ dB, which seems fairly good. But a single spot frequency jammer can cause an average error rate of about 10^{-2}, which is not acceptable. (A more detailed analysis follows in Section IV below.) This effectiveness of "partial band jamming" can be reduced by the use of coding and interleaving. Coding typically precludes the possibility of a small number of frequency slots (e.g., one slot) being jammed causing an unacceptable error rate (i.e., even if the jammer wipes out a few of the code symbols, depending upon the error-correction capability of the code, the data may still be recovered). Interleaving has the effect of randomizing the errors due to the jammer. Finally, an analogous situation occurs in direct sequence spreading when a pulse jammer is present.

In the design of a practical system, the processing gain G_p is not, by itself, a measure of how well the system is capable of performing in a jamming environment. For this purpose, we usually introduce the *jamming margin* in decibels defined as

$$M_J = G_P - \left(\frac{E_b}{\eta_{0J}}\right)_{\min} - L. \tag{24}$$

This is the residual advantage that the system has against a jammer after we subtract both the minimum required energy/bit-to-jamming "noise" power spectral density ratio $(E_b/\eta_{0J})_{\min}$ and implementation and other losses L. The jamming margin can be increased by reducing the $(E_b/\eta_{0J})_{\min}$ through the use of coding gain.

We conclude this section by showing that regardless of the technique used, spectral spreading provides protection against a broad-band jammer with a finite power P_J. Consider a system that transmits R_0 bits/s designed to operate over a bandwidth B_{ss} Hz in white noise with power density η_0 W/Hz. For any bit rate R,

$$\left(\frac{E_b}{\eta_0}\right)_{\text{actual}} = \frac{P_s}{\eta_0 R} = \frac{P_s}{P_N}\,\frac{B_{ss}}{R} \tag{25}$$

where

$P_s \triangleq E_bR$ = signal power

$P_N \triangleq \eta_0 B_{ss}$ = noise power.

Then for a specified $(E_b/\eta_0)_{\min}$ necessary to achieve mini-

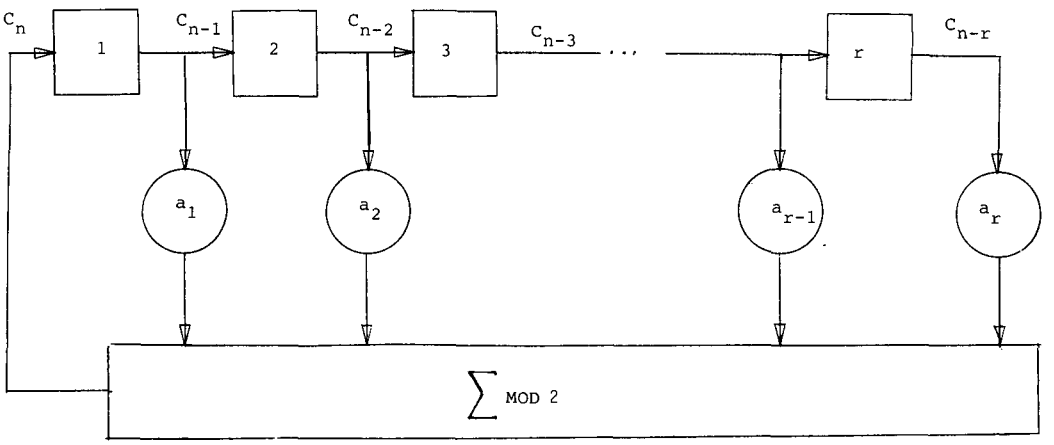


Fig. 4. Simple shift register generator (SSRG).

mum acceptable performance,

$$R \leqslant \frac{P_s}{P_N} \frac{B_{ss}}{(E_b/\eta_0)_{\min}} \triangleq R_0. \tag{26}$$

If a jammer with power P_J now appears, and if we are already transmitting at the maximum rate R_0, then (25) becomes

$$\left(\frac{E_b}{\eta_0}\right)_{\text{actual}} = \frac{P_s}{P_N + P_J} \frac{B_{ss}}{R_0} = \left(\frac{E_b}{\eta_0}\right)_{\min} \frac{P_N}{P_N + P_J}$$

or

$$\left(\frac{E_b}{\eta_0}\right)_{\text{actual}} = \left(\frac{E_b}{\eta_0}\right)_{\min} \frac{\eta_0}{\eta_0 + P_J/B_{ss}}. \tag{27}$$

Thus, if we wish to recover from the effects of the jammer, the right-hand side of (27) should be not much less than $(E_b/\eta_0)_{\min}$. This clearly requires that we increase B_{ss}, since for any finite P_J, it is then possible to make the factor $\eta_0/(\eta_0 + P_J/B_{ss})$ approach unity, and thereby retain the performance we had before the jammer appeared.

III. PSEUDORANDOM SEQUENCE GENERATORS

In Section II, we examined how a purely random sequence can be used to spread the signal spectrum. Unfortunately, in order to despread the signal, the receiver needs a replica of the transmitted sequence (in almost perfect time synchronism). In practice, therefore, we generate pseudorandom or pseudonoise (PN) sequences so that the following properties are satisfied. They

1) are easy to generate
2) have randomness properties
3) have long periods
4) are difficult to reconstruct from a short segment.

Linear feedback shift register (LFSR) sequences [4] possess properties 1) and 3), most of property 2), but not property 4). One canonical form of a binary LFSR known as a simple shift register generator (SSRG) is shown in Fig. 4. The shift register consists of binary storage elements (boxes) which transfer their contents to the right after each clock pulse (not shown). The contents of the register are linearly combined with the binary (0, 1) coefficients a_k and are fed back to the first stage. The binary (code) sequence C_n then clearly satisfies the recursion

$$C_n = \sum_{k=1}^{r} a_k C_{n-k} \pmod 2; \qquad a_r = 1. \tag{28}$$

The periodic cycle of the states depends on the initial state and on the coefficients (feedback taps) a_k. For example, the four-stage LFSR generator shown in Fig. 5 has four possible cycles as shown. The all-zeros is always a cycle for any LFSR. For spread spectrum, we are looking for *maximal length* cycles, that is, cycles of period $2^r - 1$ (all binary r-tuples except all-zeros). An example is shown for a four-state register in Fig. 6. The sequence output is $1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,0\,0 \cdots$ (period $2^4 - 1 = 15$) if the initial contents of the register (from right to left) are 1000. It is always possible to choose the feedback coefficients so as to achieve maximal length, as will be discussed below.

If we do have a maximal length sequence, then this sequence will have the following pseudorandomness properties [4].

1) There is an approximate balance of zeros and ones (2^{r-1} ones and $2^{r-1} - 1$ zeros).

2) In any period, half of the runs of consecutive zeros or ones are of length one, one-fourth are of length two, one-eighth are of length three, etc.

3) If we define the ±1 sequence $C_n' = 1 - 2C_n$, $C_n = 0, 1$, then the autocorrelation function $R_{C'}(\tau) \triangleq 1/L \sum_{k=1}^{L} C_k' C_{k+\tau}'$ is given by

$$R_{C'}(\tau) = \begin{cases} 1, & \tau = 0, L, 2L \cdots \\ -\dfrac{1}{L}, & \text{otherwise} \end{cases} \tag{29}$$

where $L = 2^r - 1$. If the code *waveform* $p(t)$ is the "square-wave" equivalent of the sequences C_n', if $L \gg 1$, and if we

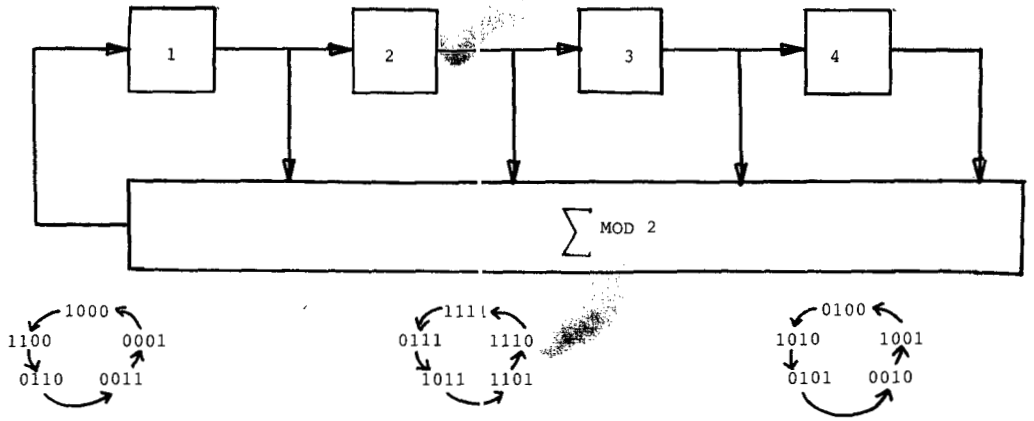


Fig. 5. Four-stage LFSR and its state cycles.

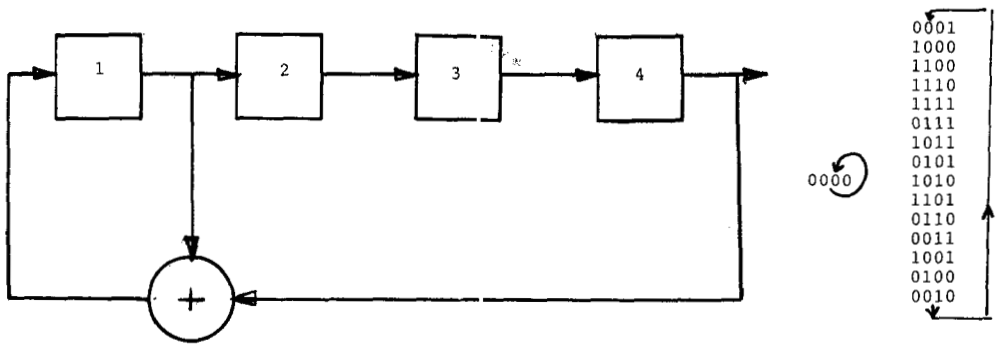


Fig. 6. Four-stage maximal length LFSR and its state cycles.

define

$$q(\tau) \triangleq \begin{cases} 1 - |\tau| f_c; & |\tau| \leq \dfrac{1}{f_c} \\ 0; & \text{otherwise} \end{cases}$$

then

$$R_p(\tau) \simeq \sum_i q\left(\tau - \frac{iL}{f_c}\right). \tag{30}$$

Equation (29), and therefore (30), follow directly from the "shift-and-add" property of maximal length (ML) LFSR sequences. This property is that the chip-by-chip sum of an MLLFSR sequence C_k and any shift of itself $C_{k+\tau}$, $\tau \neq 0$ is the *same* sequence (except for some shift). This follows directly from (28), since

$$(C_n + C_{n+\tau}) = \sum_{k=1}^{L} a_k (C_{n-k} + C_{n+\tau-k}) \pmod 2. \tag{31}$$

The shift-and-add sequence $C_n + C_{n+\tau}$ is seen to satisfy the same recursion as C_n, and if the coefficients a_k yield maximal length, then it must be the same sequence regardless of the initial (nonzero) state. The autocorrelation property (29) then follows from the following isomorphism:

$$(\{0, 1\}, +) \leftrightarrow (\{1, -1\}, \times).$$

Therefore,

$$C_k + C_{k+\tau} \leftrightarrow C_k' C_{k+\tau}'$$

and if C_k' is an MLLFSR ± 1 sequence, so is $C_k' C_{k+\tau}'$, $\tau \neq 0$. Thus, there are 2^{r-1} 1's and $(2^{r-1} - 1)$ -1's in the product and (29) follows. The autocorrelation function is shown in Fig. 7(a).

Property 3) is a most important one for spread spectrum since the autocorrelation function of the code sequence *waveform* $p(t)$ determines the spectrum. Note that because $p(t)$ is *pseudorandom*, it is periodic with period $(2^r - 1) \cdot 1/f_c$, and hence so is $R_p(\tau)$. The spectrum shown in Fig. 7(b) is therefore the line spectrum

$$S_p(f) = \left[\sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} \delta(f - mf_0)\right] \frac{L+1}{L^2} \left(\frac{\sin \pi f/f_c}{\pi f/f_c}\right)^2 + \frac{1}{L^2}\delta(f) \tag{32}$$

where

$$f_0 = \frac{f_c}{2^r - 1}.$$

If $L = 2^r - 1$ is very large, the spectral lines get closer together, and for practical purposes, the spectrum may be viewed as being continuous and similar to that of a purely random binary waveform as shown in Fig. 3. A different, but commonly used implementation of a linear feedback shift register is the modular shift register generator (MSRG) shown in Fig. 8. Additional details on the properties of linear feedback shift registers are provided in the Appendix.

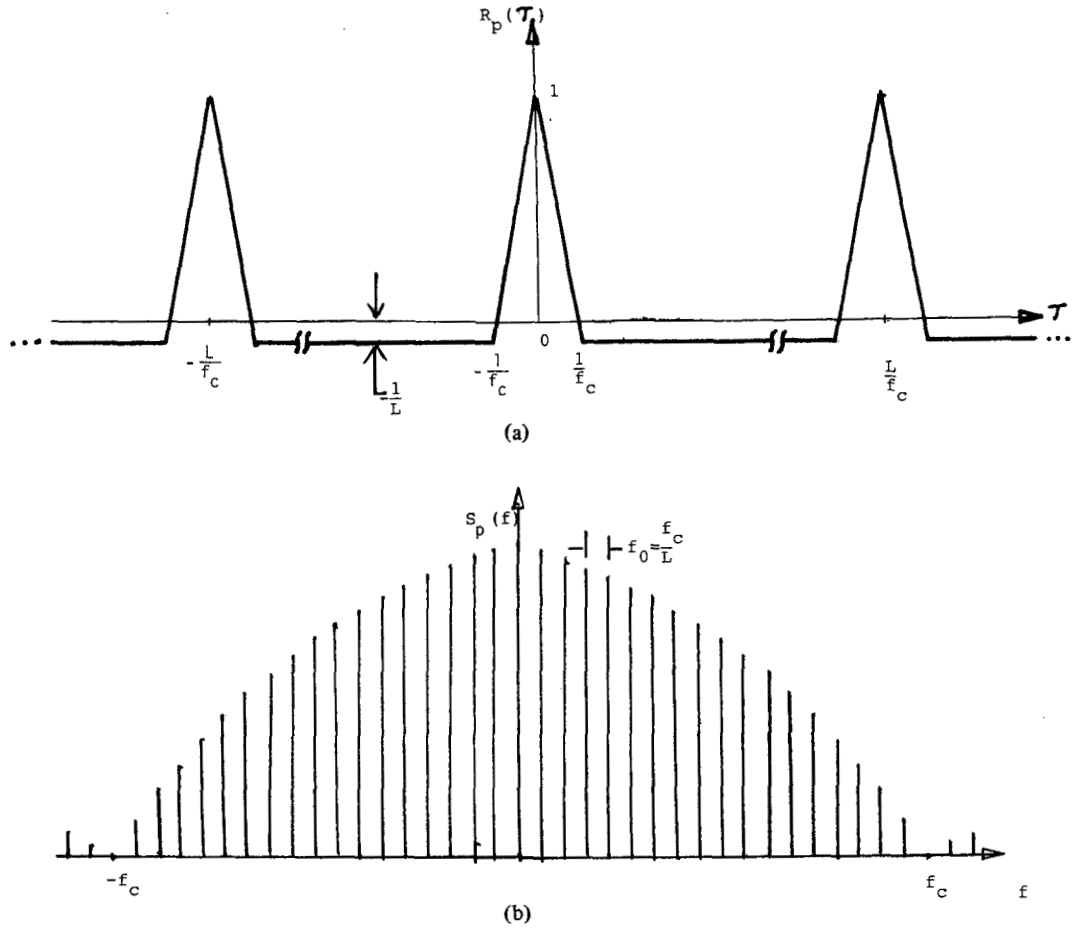


Fig. 7. Autocorrelation function $R_p(\tau)$ and power spectral density of MLLFSR sequence waveform $p(t)$. (a) Autocorrelation function of $p(t)$. (b) Power spectral density of $p(t)$.

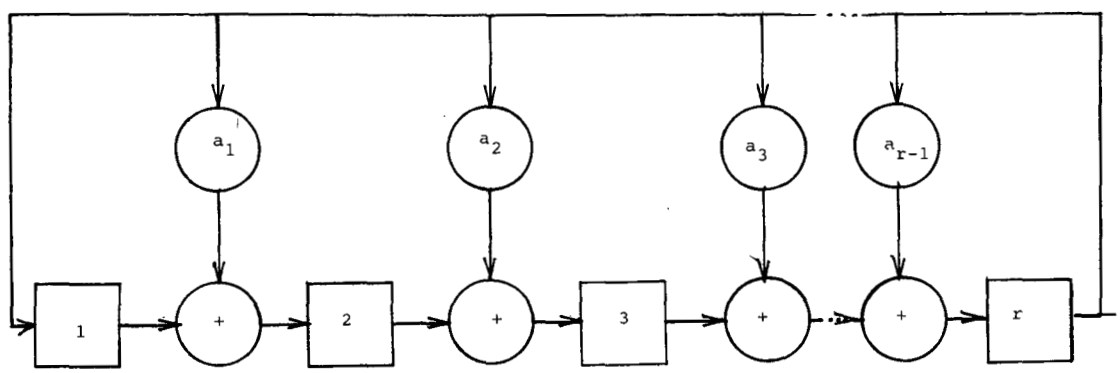


Fig. 8. Implementation as a modular shift register generator (MSRG).

For spread spectrum and other secure communications (cryptography) where one expects an adversary to attempt to recover the code in order to penetrate the system, property 4) cited in the beginning of this section is extremely important. Unfortunately, LFSR sequences do not possess that property. Indeed, using the recursion (28) or (A8) and observing only $2r-2$ consecutive bits in the sequence C_n allows us to solve for the $r-2$ middle coefficients and the r initial bits in the register by linear simultaneous equations. Thus, even if $r = 100$ so that the length of the sequence is $2^{100}-1 \simeq 10^{30}$, we would be able to construct the entire sequence from 198 bits by solving 198 linear equations (mod 2), which is neither difficult nor that time consuming for a large computer. Moreover, because the sequence C_n satisfies a recursion, a very efficient algorithm is known [7], [8] which solves the equations or which equivalently synthesizes the shortest LFSR which generates a given sequence.

In order to avoid this pitfall, several modifications of the LFSR have been proposed. In Fig. 9(a) the feedback function is replaced by an arbitrary Boolean function of the contents of the register. The Boolean function may be implemented by ROM or random logic, and there are an enormous number of these functions (2^{2^r}). Unfortunately, very little is known [4] in the open literature about the properties of such non-

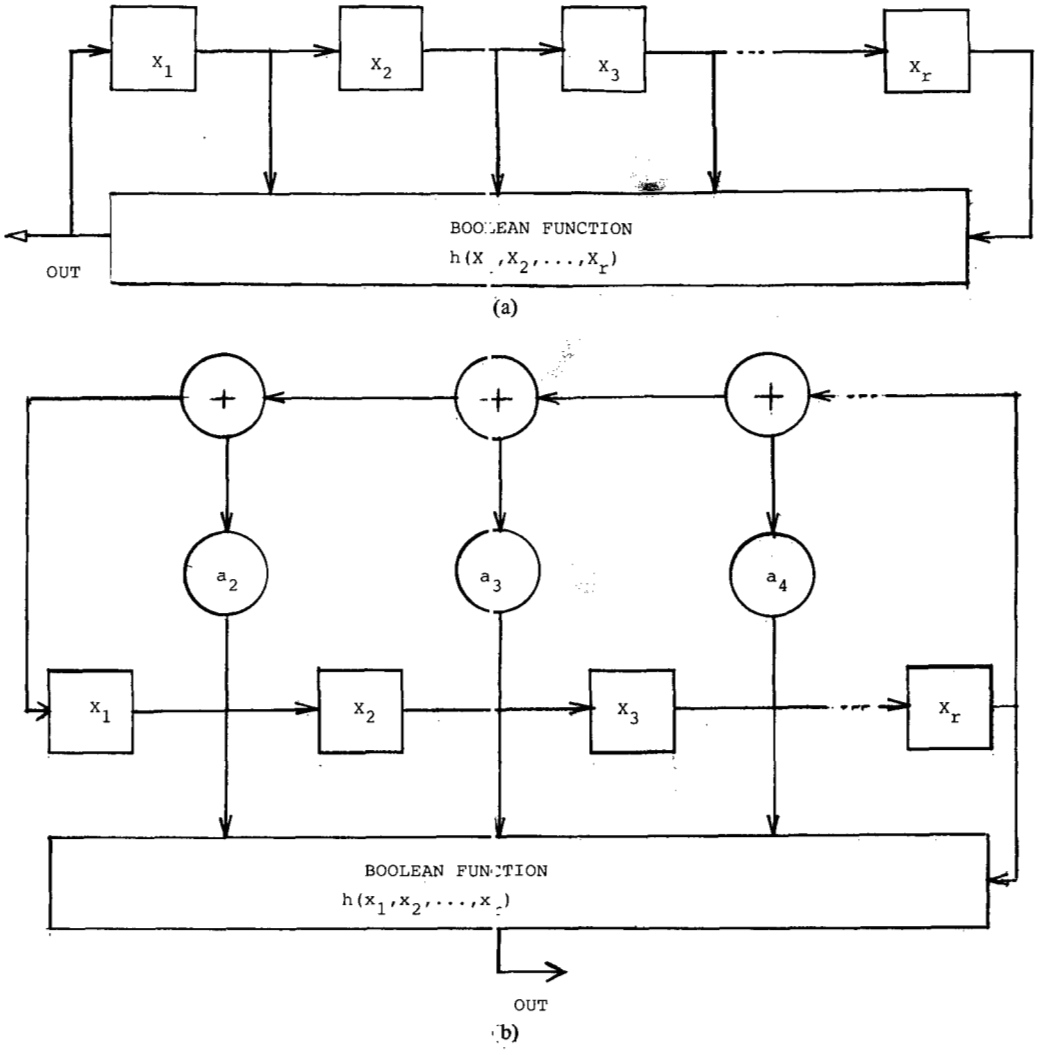


Fig. 9. Nonlinear feedback shift registers. (a) Nonlinear FDBK. Number of Boolean functions = 2^{2^r}. (b) Linear FSR, nonlinear function of state, i.e., nonlinear output logic (NOL).

linear feedback shift registers. Furthermore, some nonlinear FSR's may have no cycles or length > 1 (e.g., they may have only a *transient* that "homes" towards the all-ones state after any initial state). Are there feedback functions that generate only *one* cycle of length 2^r? The answer is yes, and there are exactly $2^{2^{r-1}-r}$ of them [9]. How do we find them? Better yet, how do we find a subset of them with all the "good" randomness properties? These are, and have been, good research problems for quite some time, and unfortunately no general theory on this topic currently exists.

A second, more manageable approach is to use an MLLFSR with nonlinear output logic (NOL) as shown in Fig. 9(b). Some clues about designing the NOL while still retaining "good" randomness properties are available [10]-[12], and a measure for judging how well condition 4) is fulfilled is to ask: What is the degree of the shortest LFSR that would generate the same sequence? A simple example of an LFSR with NOL having three stages is shown in Fig. 10(a). The shortest LFSR which generates the same sequence (of period 7) is shown in Fig. 10(b) and requires six stages.

When using PN sequences in spread-spectrum systems, several additonal requirements must be met.

1) The "partial correlation" of the sequence C_n' over a window w smaller than the full period should be as small as possible, i.e., if

$$\rho(w;j,\tau) \triangleq \sum_{n=j}^{j+w-1} C_n' C_{n+\tau}',$$

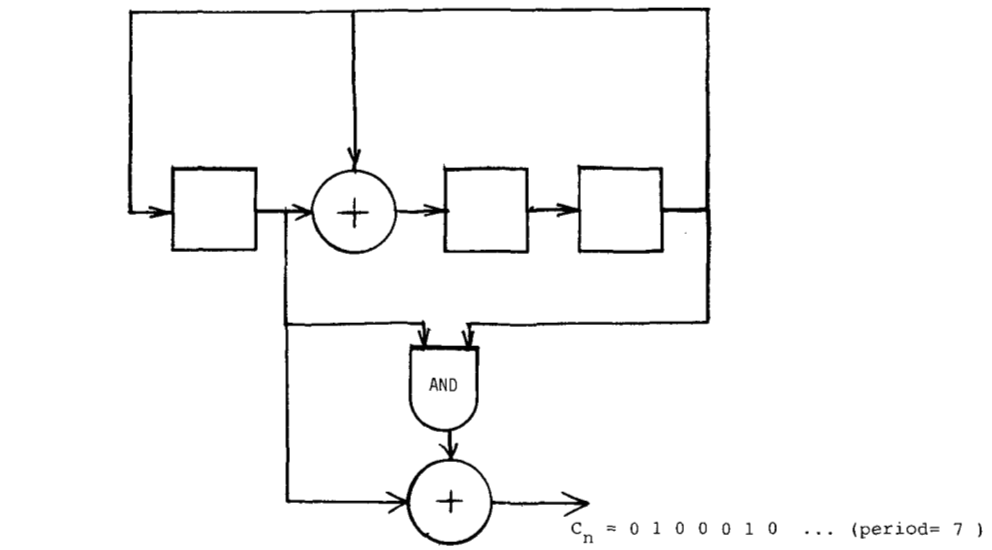
$$\rho(w) = \max_{j,\tau} |\rho(w;j,\tau)| \tag{33}$$

should be $\ll L = 2^r - 1$.

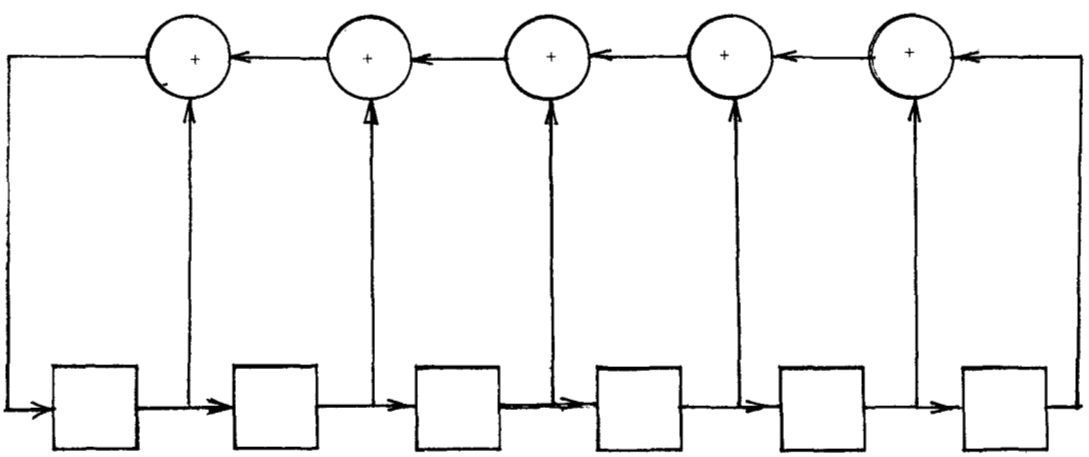
2) Different code pairs should have uniformly low cross correlation, i.e.,

$$R_{C'C''}(\tau) \triangleq \frac{1}{L} \sum_{k=1}^{L} C_k' C_{k+\tau}'' \tag{34}$$

should be $\ll 1$ for all values of τ.



(a)



(b)

Fig. 10. LFSR with NOL and its shortest linear equivalent. (a) Three-stage LFSR with NOL. (b) LFSR with $f(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ which generates the same sequence as that of (a) under the initial state 1 0 0 0 1 0.

3) Since the code sequences are periodic with period L, there are two correlation functions (depending on the relative polarity of one of the sequences in the transition over an initial point τ on the other). If we define the finite-cross-correlation function [13] as

$$f_{C'C''}(\tau) \triangleq \frac{1}{L} \sum_{k=1}^{\tau} C_k' C_{k+\tau}'', \tag{35}$$

then the so-called even and odd cross-correlation functions are, respectively,

$$R_{C'C''}^{(e)}(\tau) = f_{C'C''}(\tau) + f_{C'C''}(L-\tau)$$

and

$$R_{C'C''}^{(o)}(\tau) = f_{C'C''}(\tau) - f_{C'C''}(L-\tau)$$

and we want

$$\max_{\tau} |R_{C'C''}^{e}(\tau)| \quad \text{and} \quad \max_{\tau} |R_{C'C''}^{(o)}(\tau)|$$

to be $\ll 1$.

The reason for 1) is to keep the "self noise" of the system as low as possible since, in practice, the period is very long compared to the integration time per symbol and there will be fluctuation in the sum of any filtered (weighted) subsequence. This is especially worrisome during acquisition where these fluctuations can cause false locking. Bounds on $\rho(w)$ [14] and averages over j of $\rho(w; j, \tau)$ are available in the literature.

Properties 2) and 3) are both of direct interest when using PN sequences for code division multiple access (CDMA) as will be discussed in Section V below. This is to ensure minimal cross interference between any pair of users of the common spectrum. The most commonly used collection of

sequences which exhibit property 2) are the Gold codes [15]. These are sequences derived from an MLLFSR, but are *not* of maximal length. A detailed procedure for their construction is given in the Appendix.

Virtually all of the known results about the cross-correlation properties of useful PN sequences are summarized in [16].

As a final comment on the generation of PN sequences for spread spectrum, it is not at all necessary that feedback shift registers be used. *Any* technique which can generate "good" pseudorandom sequences will do. Other techniques are described in [4], [16], [17], for example. Indeed, the generation of good pseudorandom sequences is fundamental to other fields, and in particular, to cryptography [18]. A "good" cryptographic system can be used to generate "good" PN sequences, and vice versa. A possible problem is that the specific additional "good" properties required for an operational spread-spectrum system may not always match those required for secure cryptographic communications.

IV. ANTIJAM CONSIDERATIONS

Probably the single most important application of spread-spectrum techniques is that of resistance to intentional interference or jamming. Both direct-sequence (DS) and frequency-hopping (FH) systems exhibit this tolerance to jamming, although one might perform better than the other given a specific type of jammer.

The two most common types of jamming signals analyzed are single frequency sine waves (tones) and broad-band noise. References [19] and [20] provide performance analyses of DS systems operating in the presence of both tone and noise interference, and [21]-[26] provide analogous results for FH systems.

The simplest case to analyze is that of broad-band noise jamming. If the jamming signal is modeled as a zero-mean wide sense stationary Gaussian noise process with a flat power spectral density over the bandwidth of interest, then for a given fixed power P_J available to the jamming signal, the power spectral density of the jamming signal must be reduced as the bandwidth that the jammer occupies is increased.

For a DS system, if we assume that the jamming signal occupies the total RF bandwidth, typically taken to be twice the chip rate, then the despread jammer will occupy an even greater bandwidth and will appear to the final integrate-and-dump detection filter as approximately a white noise process. If, for example, binary PSK is used as the modulation format, then the average probability of error will be approximately given by

$$P_e = Q\left(\sqrt{\frac{2E_b}{\eta_0 + \eta_{0J}}}\right). \tag{36}$$

Equation (36) is just the classical result for the performance of a coherent binary communication system in additive white Gaussian noise. It differs from the conventional result because an extra term in the denominator of the argument of the $Q(\cdot)$ function has been added to account for the jammer. If P_e from (36) is plotted versus E_b/η_0 for a given value of P_J/P_S, where P_S is the average signal power, curves such as the ones shown in Fig. 11 result.

Expressions similar to (36) are easily derived for other modulation formats (e.g., QPSK), and curves showing the performance for several different formats are presented, for example, in [19]. The interesting thing to note about Fig. 11 is that for a given η_{0J}, the curve "bottoms out" as E_b/η_0 gets larger and larger. That is, the presence of the jammer will cause an irreducible error rate for a given P_J and a given f_c. Keeping P_J fixed, the only way to reduce the error rate is to increase f_c (i.e., increase the amount of spreading in the system). This was also noted at the end of Section II.

For FH systems, it is not always advantageous for a noise jammer to jam the entire RF bandwidth. That is, for a given P_J, the jammer can often increase its effectiveness by jamming only a fraction of the total bandwidth. This is termed *partial-band jamming*. If it is assumed that the jammer divides its power uniformly among K slots, where a slot is the region in frequency that the FH signal occupies on one of its hops, and if there is a total of N slots over which the signal can hop, we have the following possible situations. Assuming that the underlying modulation format is binary FSK (with noncoherent detection at the receiver), and using the terminology MARK and SPACE to represent the two binary data symbols, on any given hop, if

1) $K = 1$, the jammer might jam the MARK only, jam the SPACE only, or jam neither the MARK nor the SPACE;

2) $1 < K < N$, the jammer might jam the MARK only, jam the SPACE only, jam neither the MARK nor the SPACE, or jam both the MARK and the SPACE;

3) $K = N$, the jammer will always jam both the MARK and the SPACE.

To determine the average probability of error of this system, each of the possibilities alluded to above has to be accounted for. If it is assumed that the N slots are disjoint in frequency and that the MARK and SPACE tones are orthogonal (i.e., if a MARK is transmitted, it produces no output from the SPACE bandpass filter (BPF) and vice versa), then the average probability of error of the system can be shown to be given by [23], [24]

$$\begin{aligned} P_e = {} & \frac{(N-K)(N-K-1)}{N(N-1)} \frac{1}{2} \exp\left(-\tfrac{1}{2}\,\mathrm{SNR}\right) \\ & + \frac{K(N-K)}{N(N-1)} \exp\left[-\frac{1}{\frac{2}{\mathrm{SNR}} + \frac{1}{\mathrm{SJR}}}\right] + \frac{K(K-1)}{N(N-1)} \frac{1}{2} \\ & \cdot \exp\left[-\frac{1}{2} \frac{1}{\frac{1}{\mathrm{SNR}} + \frac{1}{\mathrm{SJR}}}\right] \end{aligned} \tag{37}$$

where SNR is the ratio of signal power to thermal noise power at the output of the MARK BPF (assuming that a MARK has been transmitted) and SJR is the ratio of signal

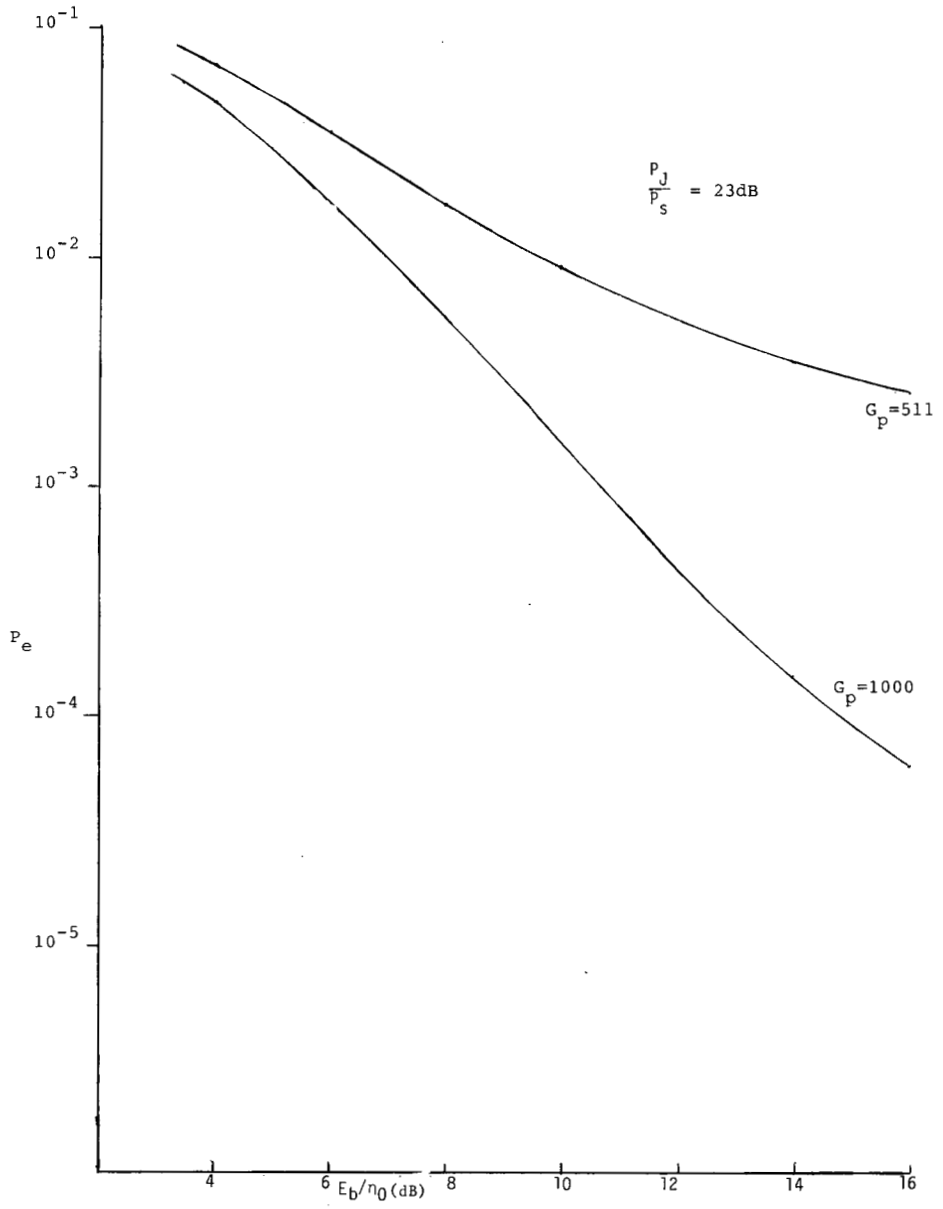


Fig. 11. Probability of error versus E_b/η_0.

power to *jammer power per slot* at the output of the MARK BPF. By jammer power per slot, we mean the total jammer power divided by the number of slots being jammed (i.e., SJR = $P_s/(P_J/K)$).

The coefficients in front of the exponentials in (37) are the probabilities of jamming neither the MARK nor the SPACE, jamming only the MARK or only the SPACE, or jamming both the MARK and the SPACE. For example, the probability of jamming both the MARK and the SPACE is given by $K(K-1)/N(N-1)$. In Fig. 12, the P_e predicted by (37) is plotted versus SNR for $K = 1$ and $K = 100$ for a P_J/P_s of 10 dB. These two curves are labeled "uncoded" on the figure.

Often, a somewhat different model from that used in deriving (37) is considered. This latter model is used in [26], and effectively assumes that either MARK and SPACE are simultaneously jammed or that neither of the two is jammed. For this case, a parameter ρ, where $0 < \rho \leqslant 1$, representing the fraction of the band being jammed, is defined. The resulting average probability of error is then maximized with respect to ρ (i.e., the worst case ρ is found), and it is shown in [26] that

$$P_{e_{\max}} > \frac{e^{-1}}{E_b/\eta_0}$$

where e is the base of the natural logarithm. It can be seen that partial band jamming affords the jammer a strategy whereby he can degrade the performance significantly (i.e., P_e can be forced to be inversely proportional to E_b/η_0 rather than exponential).

For tone jamming, the situation becomes somewhat more complicated than it is for noise jamming, especially for DS systems. This is because the system performance depends upon the location of the tone (or tones), and upon whether the period of the spreading sequence is equal to or greater than the duration of a data symbol. Oftentimes the effect

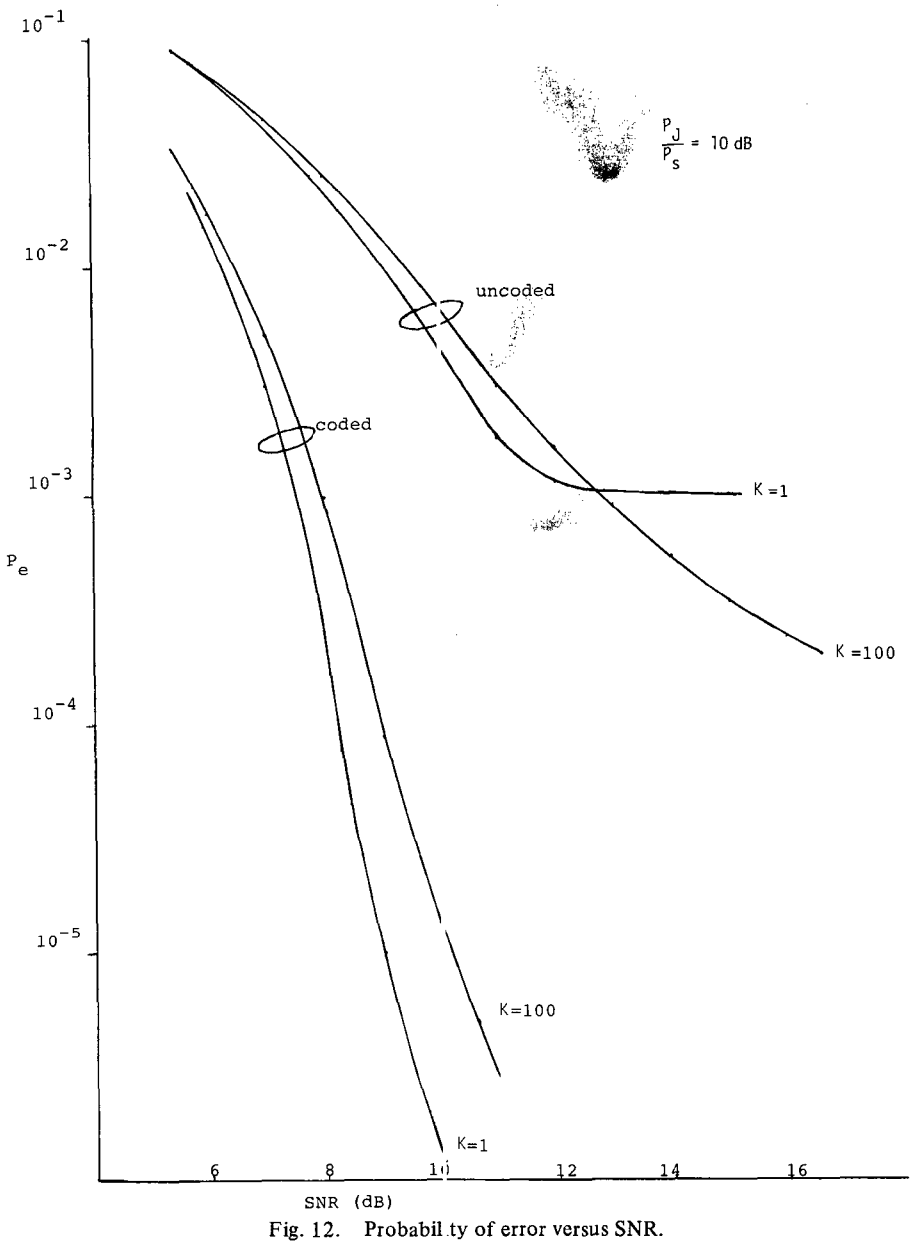


Fig. 12. Probability of error versus SNR.

of a despread tone is approximated as having arisen from an equivalent amount of Gaussian noise. In this case, the results presented above would be appropriate. However, the Gaussian approximation is not always justified, and some conditions for its usage are given in [20] and [27].

The situation is simpler in FH systems operating in the presence of partial-band tone jamming, and as shown, for example, in [24], the performance of a noncoherent FH-FSK system in partial-band tone jamming is often virtually the same as the performance in partial-band noise jamming. One important consideration in FH systems with either noise or tone jamming is the need for error-correction coding. This can be seen very simply by assuming that the jammer is much stronger than the desired signal, and that it chooses to put all of its power in a single slot (i.e., the jammer jams one out of N slots). The $K = 1$ uncoded curve of Fig. 12 corresponds to this situation. Then with no error-correction coding, the system will make an error (with high probability) every time it hops to a MARK frequency when the corresponding SPACE frequency is being jammed or vice versa. This will happen on the average one out of every N hops, so that the probability of error of the system will be approximately $1/N$, independent of signal-to-noise ratio. This is readily seen to be the case in Fig. 12. The use of coding prevents a simple error as caused by a spot jammer from degrading the system performance. To illustrate this point, an error-correcting code (specifically a Golay code [2]) was used in conjunction with the system whose uncoded performance is shown in Fig. 12, and the performance of the coded system is also shown in Fig. 12. The advantage of using error-correction coding is obvious from comparing the corresponding curves.

Finally, there are, of course, many other types of common jamming signals besides broad-band noise or single frequency tones. These include swept-frequency jammers, pulse-burst jammers, and repeat jammers. No further discussion of these

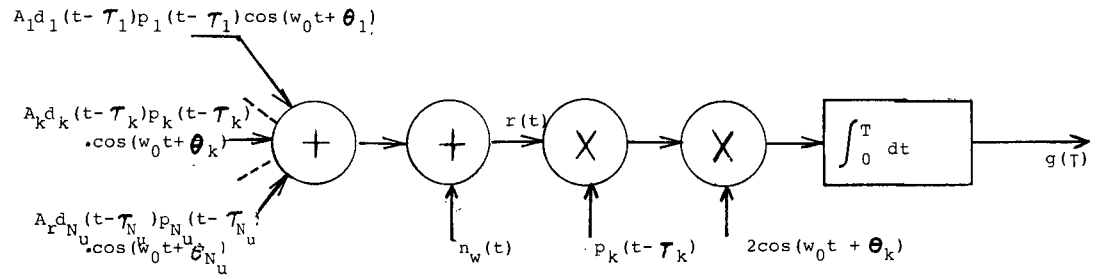


Fig. 13. DS CDMA system.

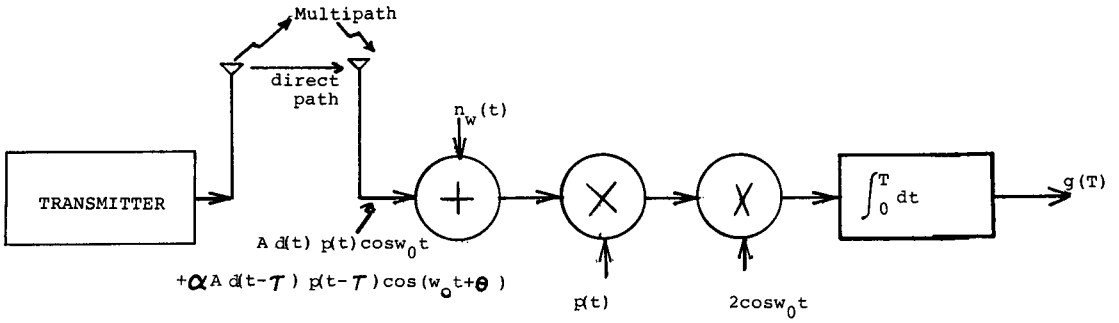


Fig. 14. DS used to combat multipath.

jammers will be presented in this paper, but references such as [28]-[30] provide a reasonable description of how these jammers affect system performance.

V. CODE DIVISION MULTIPLE ACCESS (CDMA)

As is well known, the two most common multiple access techniques are frequency division multiple access (FDMA) and time division multiple access (TDMA). In FDMA, all users transmit simultaneously, but use disjoint frequency bands. In TDMA, all users occupy the same RF bandwidth, but transmit sequentially in time. When users are allowed to transmit simultaneously in time and occupy the same RF bandwidth as well, some other means of separating the signals at the receiver must be available, and CDMA [also termed spread-spectrum multiple access (SSMA)] provides this necessary capability.

In DS CDMA [31]-[33], each user is given its own code, which is approximately orthogonal (i.e., has low cross correlation) with the codes of the other users. However, because CDMA systems typically are asynchronous (i.e., the transition times of the data symbols of the different users do not have to coincide), the design problem is much more complicated than that of having, say, N_u spreading sequences with uniformly low cross correlations such as the Gold codes discussed in Section III and in the Appendix. As will be seen below, the key parameters in a DS CDMA system are both the cross-correlation and the partial-correlation functions, and the design and optimization of code sets with good partial-correlation properties can be found in many references such as [16], [34], and [35].

The system is shown in Fig. 13. The received signal is given by

$$r(t)=\sum_{i=1}^{N_u} A_i d_i(t-\tau_i)p_i(t-\tau_i)\cos(\omega_0 t+\theta_i)+n_w(t) \quad (38)$$

where

$d_i(t)$ = message of ith user and equals ± 1
$p_i(t)$ = spreading sequence waveform of ith user
A_i = amplitude of ith carrier
θ_i = random phase of ith carrier uniformly distributed in $[0, 2\pi]$
τ_i = random time delay of ith user uniformly distributed in $[0, T]$
T = symbol duration
$n_w(t)$ = additive white Gaussian noise.

Assuming that the receiver is correctly synchronized to the kth signal, we can set both τ_k and θ_k to zero without losing any generality. The final test statistic out of the integrate-and-dump receiver of Fig. 14 is given by

$$g(T)=A_k+\frac{1}{T}\sum_{\substack{i=1\\ i\neq k}}^{N_u} A_i\int_0^T d_i(t-\tau_i)\cdot p_i(t-\tau_i)p_k(t)\cos(\theta_i)\,dt+\frac{2}{T}\int_0^T n_w(t)p_k(t)\cos(\omega_0 t)\,dt \quad (39)$$

where double frequency terms have been ignored.

Consider the second term on the RHS of (39). It is a sum of N_u-1 terms of the form

$$A_i\cos(\theta_i)\int_0^T d_i(t-\tau_i)p_i(t-\tau_i)p_k(t)\,dt.$$

Notice that, because the ith signal is not, in general, in sync with the kth signal, $d_i(t-\tau_i)$ will change signs somewhere in the interval $[0, T]$ 50 percent of the time. Hence, the above

integral will be the sum of two partial correlations of $p_i(t)$ and $p_k(t)$, rather than one total cross correlation. Therefore, (39) can be rewritten

$$g(T) = A_k + \sum_{\substack{i=1 \\ i \neq k}}^{N_u} A_i[\pm\rho_{ik}(\tau_i) \pm \hat{\rho}_{ik}(\tau_i)] \cos(\theta_i) + n(T) \quad (40)$$

where

$$\rho_{ik}(\tau_i) \triangleq \frac{1}{T}\int_0^{\tau_i} p_i(t-\tau_i)p_k(t)\,dt$$

$$\hat{\rho}_{ik}(\tau_i) \triangleq \frac{1}{T}\int_{\tau_i}^{T} p_i(t-\tau_i)p_k(t)\,dt$$

and

$$n(T) \triangleq \frac{2}{T}\int_0^T n_w(t)p_k(t)\cos\omega_0 t\,dt.$$

Notice that the coefficients in front of $\rho_{ik}(\tau_i)$ and $\hat{\rho}_{ik}(\tau_i)$ can independently have a plus or minus sign due to the data sequence of the ith signal. Also notice that $\rho_{ik}(\tau_i) + \hat{\rho}_{ik}(\tau_i)$ is the total cross correlation between the ith and kth spreading sequences. Finally, the continuous correlation functions $\rho_{ik}(\tau) \pm \hat{\rho}_{ik}(\tau)$ can be expressed in terms of the discrete even and odd cross-correlation functions, respectively, that were defined in Section III.

While the code design problem in CDMA is very crucial in determining system performance, of potentially greater importance in DS CDMA is the so-called "near-far problem." Since the N_u users are typically geographically separated, a receiver trying to detect the kth signal might be much closer physically to, say, the ith transmitter rather than the kth transmitter. Therefore, if each user transmits with equal power, the signal from the ith transmitter will arrive at the receiver in question with a larger power than that of the kth signal. This particular problem is often so severe that DS CDMA cannot be used.

An alternative to DS CDMA, of course, is FH CDMA [36]-[40]. If each user is given a different hopping pattern, and if all hopping patterns are orthogonal, the near-far problem will be solved (except for possible spectral spillover from one slot into adjacent slots). However, the hopping patterns are never truly orthogonal. In particular, any time more than one signal uses the same frequency at a given instant of time, interference will result. Events of this type are sometimes referred to as "hits," and these hits become more and more of a problem as the number of users hopping over a fixed bandwidth increases. As is the case when FH is employed as an antijam technique, error-correction coding can be used to significant advantage when combined with FH CDMA.

FH CDMA systems have been considered using one hop per bit, multiple hops per bit (referred to as fast frequency hopping or FFH), and multiple bits per hop (referred to as slow frequency hopping or SFH). Oftentimes the characteristics of the channel over which the multiple users transmit play a significant role in influencing which type of hopping one employs. An example of this is the multipath channel, which is discussed in the next section.

It is clearly of interest to consider the relative capacity of a CDMA system compared to FDMA or TDMA. In a perfectly linear, perfectly synchronous system, the number of orthogonal users for all three systems is the same, since this number only depends upon the dimensionality of the overall signal space. In particular, if a given time-bandwidth product G_P is divided up into, say, G_P disjoint time intervals for TDMA, it can also be "divided" into N binary orthogonal codes (assume that $G_P = 2^m$ for some positive integer m).

The differences between the three multiple-accessing techniques become apparent when various real-world constraints are imposed upon the ideal situation described above. For example, one attractive feature of CDMA is that it does not *require* the network synchronization that TDMA requires (i.e., if one is willing to give up something in performance, CDMA can be (and usually is) operated in an asynchronous manner). Another advantage of CDMA is that it is relatively easy to add additional users to the system. However, probably the dominant reason for considering CDMA is the need, in addition, for some type of external interference rejection capability such as multipath rejection or resistance to intentional jamming.

For an asynchronous system, even ignoring any near-far problem effects, the number of users the system can accommodate is markedly less than G_P. From [31] and [35], a rough rule-of-thumb appears to be that a system with processing gain G_P can support approximately $G_P/10$ users. Indeed, from [31, eq. (17)], the peak signal voltage to rms noise voltage ratio, averaged over all phase shifts, time delays, and data symbols of the multiple users, is approximately given by

$$\overline{\text{SNR}} \simeq \left[\frac{N_u - 1}{3G_P} + \frac{\eta_0}{2E_b}\right]^{-1/2}$$

where the overbar indicates an ensemble average. From this equation, it can be seen that, given a value of E_b/η_0, $(N_u - 1)/G_P$ should be in the vicinity of 0.1 in order not to have a noticeable effect on system performance.

Finally, other factors such as nonlinear receivers influence the performance of a multiple access system, and, for example, the effect of a hard limiter on a CDMA system is treated in [45].

VI. MULTIPATH CHANNELS

Consider a DS binary PSK communication system operating over a channel which has more than one path linking the transmitter to the receiver. These different paths might consist of several discrete paths, each one with a different attenuation and time delay relative to the others, or it might consist of a continuum of paths. The RAKE system described in [1] is an example of a DS system designed to operate effectively in a multipath environment.

For simplicity, assume initially there are just two paths, a direct path and a single multipath. If we assume the time delay the signal incurs in propagating over the direct path is smaller than that incurred in propagating over the single

multipath, and if it is assumed that the receiver is synchronized to the time delay and RF phase associated with the direct path, then the system is as shown in Fig. 14. The received signal is given by

$$r(t) = Ad(t)p(t)\cos\omega_0 t + \alpha Ad(t-\tau)p(t-\tau) \cdot \cos(\omega_0 t + \theta) + n_w(t) \quad (41)$$

where τ is the differential time delay associated with the two paths and is assumed to be in the interval $0 \leqslant \tau \leqslant T$, θ is a random phase uniformly distributed in $[0, 2\pi]$, and α is the relative attenuation of the multipath relative to the direct path. The output of the integrate-and-dump detection filter is given by

$$g(T) = A + [\pm\alpha A\rho(\tau) + \alpha A\hat{\rho}(\tau)]\cos\theta \quad (42)$$

where $\rho(\tau)$ and $\hat{\rho}(\tau)$ are partial correlation functions of the spreading sequence $p(t)$ and are given by

$$\rho(\tau) \triangleq \frac{1}{T}\int_0^\tau p(t)p(t-\tau)\,dt \quad (43)$$

and

$$\hat{\rho}(\tau) \triangleq \frac{1}{T}\int_\tau^T p(t)p(t-\tau)\,dt. \quad (44)$$

Notice that the sign in front of the second term on the RHS of (42) can be plus or minus with equal probability because this term arises from the pulse preceding the pulse of interest (i.e., if the ith pulse is being detected, this term arises from the $i-1$th pulse), and this latter pulse will be of the same polarity as the current pulse only 50 percent of the time. If the signs of these two pulses happen to be the same, and if $\tau > T_c$ where T_c is the chip duration, then $\rho(\tau) + \hat{\rho}(\tau)$ equals the autocorrelation function of $p(t)$ (assuming that a full period of $p(t)$ is contained in each T second symbol), and this latter quantity equals $-(1/L)$, where L is the period of $p(t)$. In other words, the power in the undesired component of the received signal has been attenuated by a factor of L^2.

If the sign of the preceding pulse is opposite to that of the current pulse, the attenuation of the undesired signal will be less than L^2, and typically can be much less than L^2. This is analogous, of course, to the partial correlation problem in CDMA discussed in the previous section.

The case of more than two discrete paths (or a continuum of paths) results in qualitatively the same effects in that signals delayed by amounts outside of $\pm T_c$ seconds about a correlation peak in the autocorrelation function of $p(t)$ are attenuated by an amount determined by the processing gain of the system.

If FH is employed instead of DS spreading, improvement in system performance is again possible, but through a different mechanism. As was seen in the two previous sections, FH systems achieve their processing gain through interference avoidance, not interference attenuation (as in DS systems). This same qualitative difference is true again if the interference is multipath. As long as the signal is hopping fast enough relative to the differential time delay between the desired signal and the multipath signal (or signals), all (or most) of the multipath energy will fall in slots that are orthogonal to the slot that the desired signal currently occupies.

Finally, the problems treated in this and the previous two sections are often all present in a given system, and so the use of an appropriate spectrum-spreading technique can alleviate all three problems at once. In [41] and [42], the joint problem of multipath and CDMA is treated, and in [43] and [44], the joint problem of multipath and intentional interference is analyzed. As indicated in Section V, if only multiple accessing capability is needed, there are systems other than CDMA that can be used (e.g., TDMA). However, when multipath is also a problem, the choice of CDMA as the multiple accessing technique is especially appropriate since the same signal design allows both many simultaneous users and improved performance of each user individually relative to the multipath channel.

In the case of signals transmitted over channels degraded by both multipath and intentional interference, either factor by itself suggests the consideration of a spectrum-spreading technique (in particular, of course, the intentional interference), and when all three sources of degradation are present simultaneously, spread spectrum is a virtual necessity.

VII. ACQUISITION

As we have seen in the previous sections, pseudonoise modulation employing direct sequence, frequency hopping, and/or time hopping is used in spread-spectrum systems to achieve bandwidth spreading which is large compared to the bandwidth required by the information signal. These PN modulation techniques are typically characterized by their very low repetition-rate-to-bandwidth ratio and, as a result, synchronization of a receiver to a specified modulation constitutes a major problem in the design and operation of spread-spectrum communications systems [46]-[50].

It is possible, in principle, for spread-spectrum receivers to use matched filter or correlator structures to synchronize to the incoming waveform. Consider, for example, a direct-sequence amplitude modulation synchronization system as shown in Fig. 15(a). In this figure, the locally generated code $p(t)$ is available with delays spaced one-half of a chip ($T_c/2$) apart to ensure correlation. If the region of uncertainty of the code phase is N_c chips, $2N_c$ correlators are employed. If no information is available regarding the chip uncertainty and the PN sequence repeats every, say, 2047 chips, then 4094 correlators are employed. Each correlator is seen to examine λ chips, after which the correlator outputs V_0, V_1, $\cdots$, V_{2N_c-1} are compared and the largest output is chosen. As λ increases, the probability of making an error in synchronization decreases; however, the acquisition time increases. Thus, λ is usually chosen as a compromise between the probability of a synchronization error and the time to acquire PN phase.

A second example, in which FH synchronization is employed, is shown in Fig. 15(b). Here the spread-spectrum signal

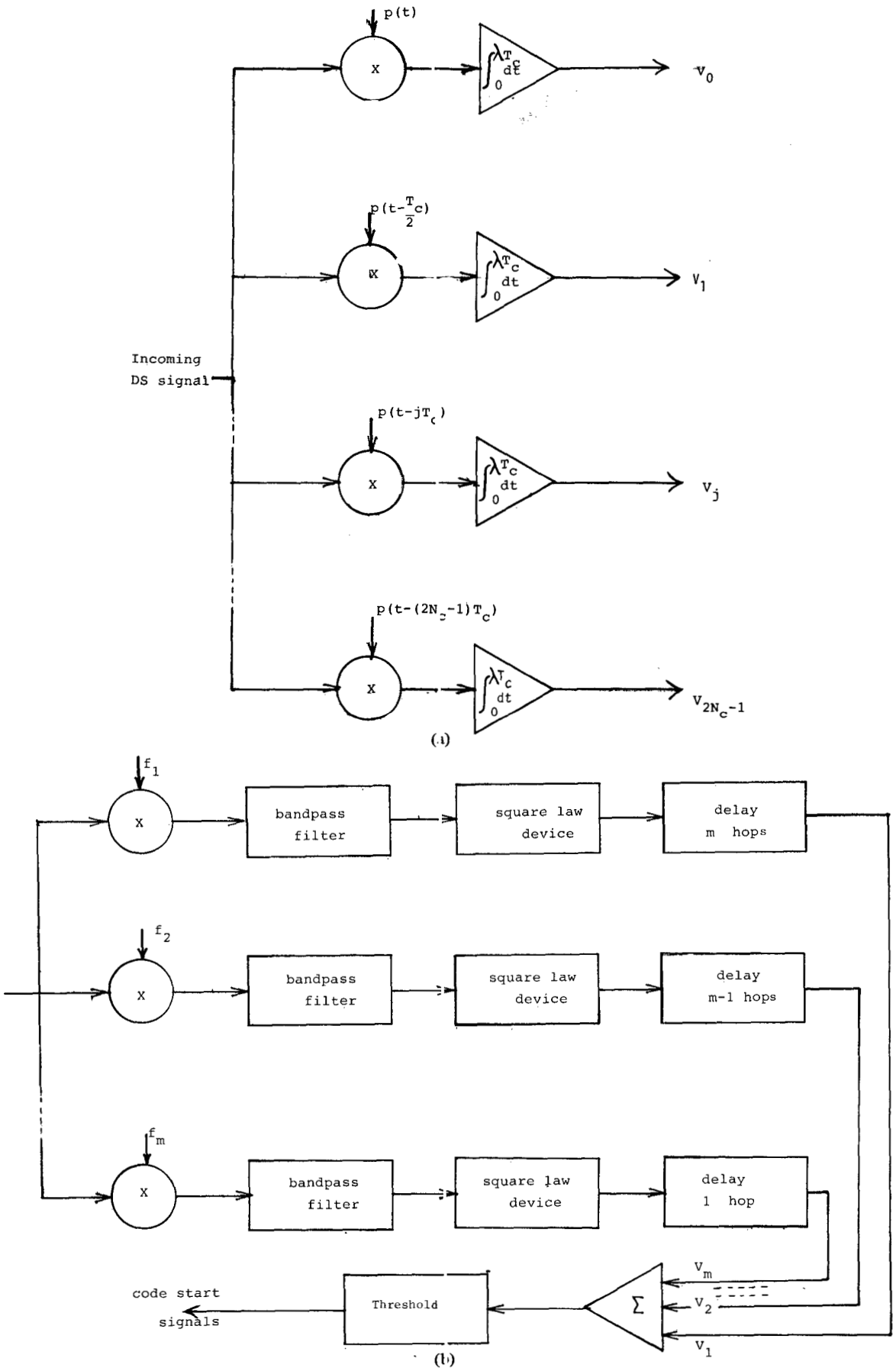


Fig. 15. (a) Direct sequence acquisition using $2N_c$ correlators. (b) Passive correlator structure for a frequency-hopping coarse acquisition scheme.

hops over, for example, $m = 500$ distinct frequencies. Assume that the frequency-hopping sequence is $f_1, f_2, \cdots, f_m$ and then repeats. The correlator then consists of $m = 500$ mixers, each followed by a bandpass filter and square law detector. The delays are inserted so that when the correct sequence appears, the voltages $V_1, V_2, \cdots, V_m$ will occur at the same instant of time at the adder and will, therefore, with high probability, exceed the threshold level indicating synchronization of the receiver to the signal.

While the above technique of using a bank of correlators or matched filters provides a means for rapid acquisition, a considerable reduction in complexity, size, and receiver cost can be achieved by using a single correlator or a single matched filter and repeating the procedure for each possible sequence shift. However, these reductions are paid for by the increased acquisition time needed when performing a serial rather than a parallel operation. One obvious question of interest is therefore the determination of the tradeoff between the number of parallel correlators (or matched filters) used and the cost and time to acquire. It is interesting to note that this tradeoff may become a moot point in several years as a result of the rapidly advancing VLSI technology.

No matter what synchronization technique is employed, the time to acquire depends on the "length" of the correlator. For example, in the system depicted in Fig. 15(a), the integration is performed over λ chips where λ depends on the desired probability of making a synchronization error (i.e., of deciding that a given sequence phase is correct when indeed it is not), the signal-to-thermal noise power ratio, and the signal-to-jammer power ratio. In addition, in the presence of fading, the fading characteristics affect the number of chips and hence the acquisition time.

The importance that one should attribute to acquisition time, complexity, and size depends upon the intended application. In tactical military communications systems, where users are mobile and push-to-talk radios are employed, rapid acquisition is needed. However, in applications where synchronization occurs once, say, each day, the time to synchronize is not a critical parameter. In either case, once acquisition has been achieved and the communication has begun, it is extremely important not to lose synchronization. Thus, while the acquisition process involves a search through the region of time-frequency uncertainty and a determination that the locally generated code and the incoming code are sufficiently aligned, the next step, called *tracking*, is needed to ensure that the close alignment is maintained. Fig. 16 shows the basic synchronization system. In this system, the incoming signal is first locked into the local PN signal generator using the acquisition circuit, and then kept in synchronism using the tracking circuit. Finally, the data are demodulated.

One popular method of acquisition is called the *sliding correlator* and is shown in Fig. 17. In this system, a single correlator is used rather than L correlators. Initially, the output phase k of the local PN generator is set to $k = 0$ and a partial correlation is performed by examining λ chips. If the integrator output falls below the threshold and therefore is deemed too small, k is set to $k = 1$ and the procedure is repeated. The determination that acquisition has taken place

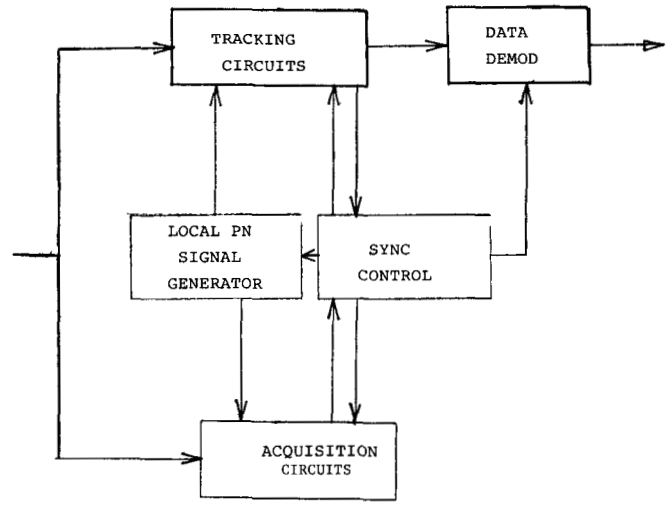


Fig. 16. Functional diagram of synchronization subsystem.

is made when the integrator output V_I exceeds the threshold voltage $V_T(\lambda)$.

It should be clear that in the worst case, we may have to set $k = 0, 1, 2, \cdots$, and $2N_c - 1$ before finding the correct value of k. If, during each correlation, λ chips are examined, the worst case acquisition time (neglecting false-alarm and detection probabilities) is

$$T_{\text{acq,max}} = 2\lambda N_c T_c. \tag{45}$$

In the $2N_c$-correlator system, $T_{\text{acq,max}} = T_c\lambda$, and so we see that there is a time-complexity tradeoff.

Another technique, proposed by Ward [46], called rapid acquisition by sequential estimation, is illustrated in Fig. 18. When switch S is in position 2, the shift register forms a PN generator and generates the same sequence as the input signal. Initially, in order to synchronize the PN generator to the incoming signal, switch S is thrown to position 1. The first N chips received at the input are loaded into the register. When the register is fully loaded, switch S is thrown to position 2. Since the PN sequence generator generates the same sequence as the incoming waveform, the sequences at positions 1 and 2 must be identical. That such is the case is readily seen from Fig. 19 which shows how the code $p(t - jT_C)$ is initially generated. Comparing this code generator to the local generator shown in Fig. 18, we see that with the switch in position 1, once the register is filled, the outputs of both mod 2 adders are *identical*. Hence, the bit stream at positions 1 and 2 are the same and switch S can be thrown to position 2. Once switch S is thrown to position 2, correlation is begun between the incoming code $p(t - jT_c)$ in white noise and the locally generated PN sequence. This correlation is performed by first multiplying the two waveforms and then examining λ chips in the integrator.

When no noise is present, the N chips are correctly loaded into the shift register, and therefore the acquisition time is $T_{\text{acq}} = NT_c$. However, when *noise is present,* one or more chips may be incorrectly loaded into the register. The resulting waveform at 2 will then not be of the same phase as the sequence generated at 1. If the correlator output after λT_c ex-

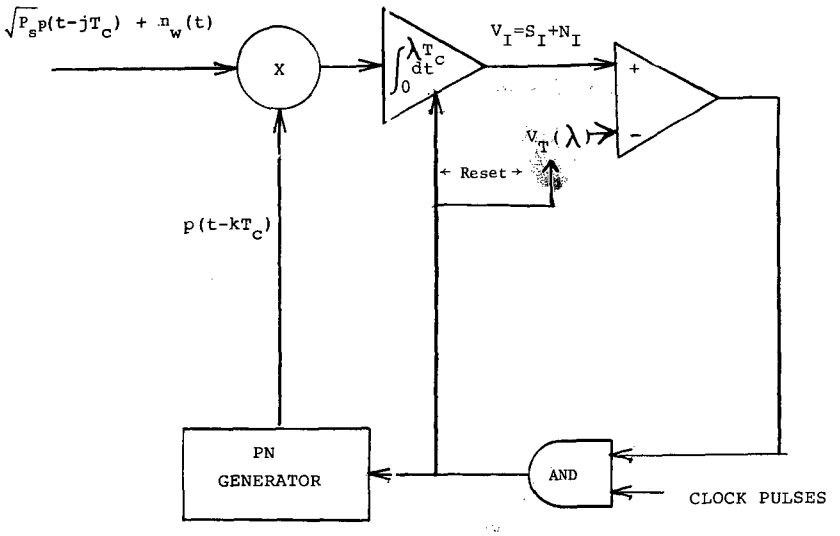


Fig. 17. The "sliding correlator."

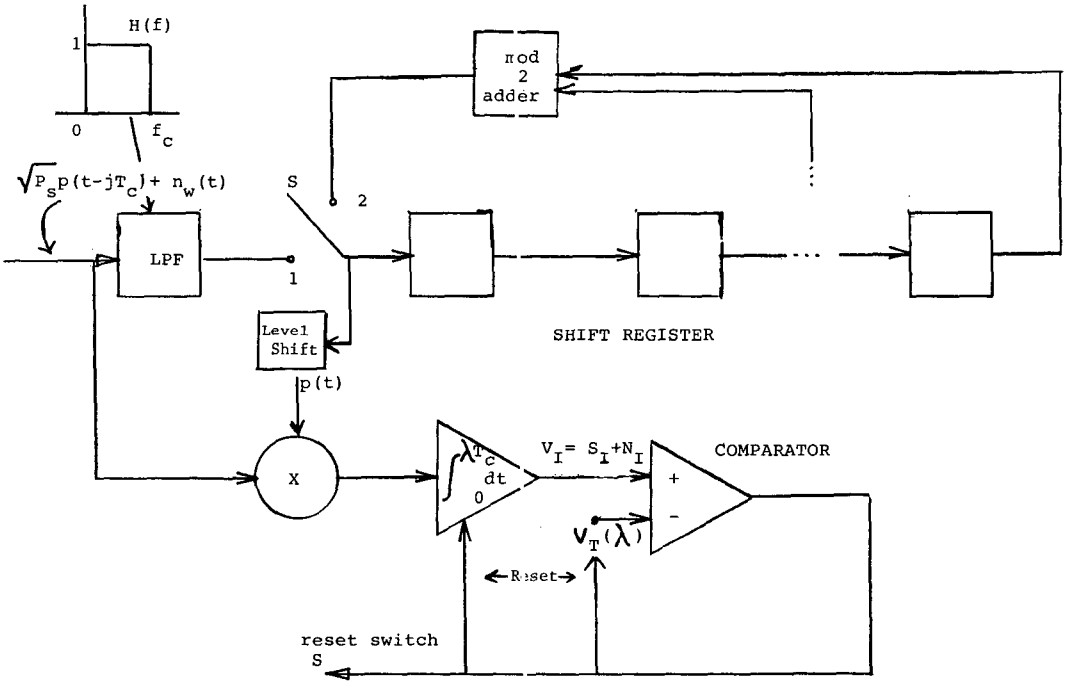


Fig. 18. Shift register acquisition circuit.

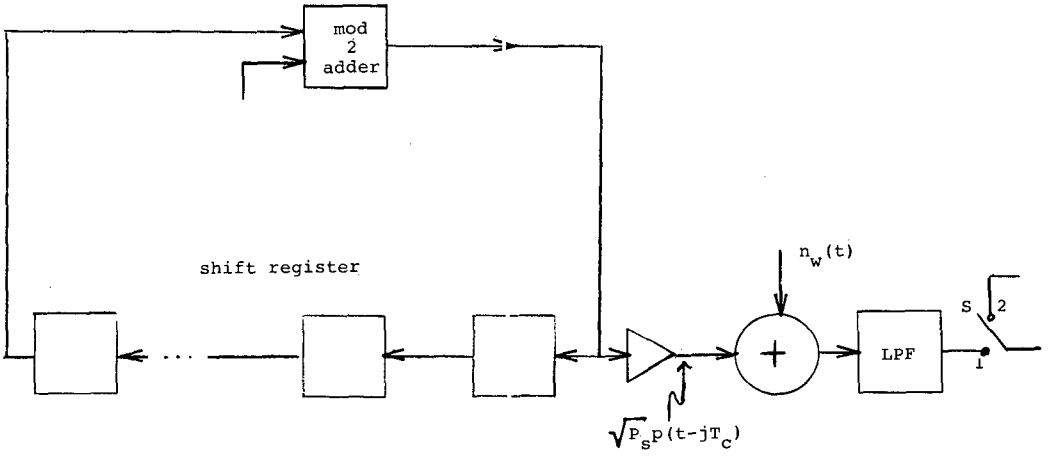


Fig. 19. The equivalent transmitter SRSG.

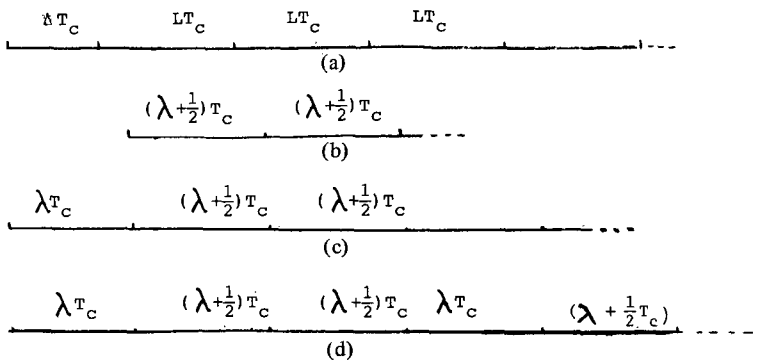


Fig. 20. Timing diagram for serial search acquisition.

ceeds the threshold voltage, we assume that synchronization has occurred. If, however, the output is less than the threshold voltage, switch S is thrown to position 1, the register is reloaded, and the procedure is repeated.

Note that in both Figs. 17 and 18, correlation occurs for a time λT_c before predicting whether or not synchronism has occurred. If, however, the correlator output is examined after a time nT_c and a decision made at each $n \leqslant \lambda$ as to whether 1) synchronism has occurred, 2) synchronism has not occurred, or 3) a decision cannot be made with sufficient confidence and therefore an additional chip should be examined, then the average acquisition time can be reduced substantially.

One can approximately calculate the mean acquisition time of a parallel search acquisition system, such as the system shown in Fig. 15, by noting that after integrating over λ chips, a correct decision will be made with probability P_D where P_D is called the probability of detection. If, however, an incorrect output is chosen, we will, after examining an additional λ chips, again make a determination of the correct output. Thus, on the average, the acquisition time is

$$\bar{T}_{\text{acq}} = \lambda T_c P_D + 2\lambda T_c P_D(1-P_D) + 3\lambda T_c P_D(1-P_D)^2 + \cdots = \frac{\lambda T_c}{P_D} \tag{46}$$

where it is assumed that we continue searching every λ chips even after a threshold has been exceeded. This is not, in general, the way an actual system would operate, but does allow a simple approximation to the true acquisition time.

Calculation of the mean acquisition time when using the "sliding correlator" shown in Fig. 17 can be accomplished in a similar manner (again making the approximation that we never stop searching) by noting that we are initially offset by a random number of chips Δ as shown in Fig. 20(a). After the correlator of Fig. 17 finally "slides" by these Δ chips, acquisition can be achieved with probability P_D. (Note that this P_D differs from the P_D of (46), since the latter P_D accounts for false synchronizations due to a correlator matched to an incorrect phase having a larger output voltage than does the correlator matched to the correct phase.) If, due to an incorrect decision, synchronization is not achieved at that time, L additional chips must then be examined before acquistion can be achieved (again with probability P_D).

We first calculate the average time needed to slide by the Δ chips. To see how this time can change, refer to Fig. 20(b) which indicates the time required if we are not synchronized. λ chips are integrated, and if the integrator output $V_I < V_T$ (the threshold voltage), a $\frac{1}{2}$ chip delay is generated, and we then process an additional λ chips, etc. We note that in order to slide Δ chips in $\frac{1}{2}$ chip intervals, this process must occur 2Δ times. Since each repetition takes a time $(\lambda + \frac{1}{2})T_c$, the total elapsed time is $2\Delta(\lambda + \frac{1}{2})T_c$.

Fig. 20(b) assumes that at the end of each examination interval, $V_I < V_T$. However, if a false alarm occurs and $V_I > V_T$, no slide of $T_c/2$ will occur until after an additional λ chips are searched. This is shown in Fig. 20(c). In this case, the total elapsed time is $2\Delta(\lambda + \frac{1}{2})T_c + \lambda T_c$. Fig. 20(d) shows the case where false alarms occurred twice. Clearly, neither the separation between these false alarms nor where they occur is relevant. The total elapsed time is now $2\Delta(\lambda + \frac{1}{2})T_c + 2\lambda T_c$.

In general, the average elapsed time to reach the correct synchronization phase is

$$\begin{aligned}\bar{T}_{s/\Delta} &= 2\Delta(\lambda + \tfrac{1}{2})T_c + \lambda T_c P_F + 2\lambda T_c P_F^2 + \cdots \\ &= 2\Delta(\lambda + \tfrac{1}{2})T_c + \lambda T_c P_F \sum_{n=1}^{\infty} n P_F^{n-1} \\ &= 2\Delta(\lambda + \tfrac{1}{2})T_c + \frac{\lambda T_c P_F}{(1-P_F)^2}\end{aligned} \tag{47}$$

where P_F is the false alarm probability. Equation (47) is for a given value of Δ. Since Δ is a random variable which is equally likely to take on any integer value from 0 to $L-1$, $\bar{T}_{s/\Delta}$ must be averaged over all Δ. Therefore,

$$\bar{T}_s \triangleq \frac{1}{L}\sum_{\Delta=0}^{L-1} \bar{T}_{s/\Delta} = L(\lambda + \tfrac{1}{2})T_c + \frac{\lambda T_c P_F}{(1-P_F)^2}. \tag{48}$$

Equation (48) is the average time needed to slide through Δ chips. If, after sliding through Δ chips, we do not detect the correct phase, we must now slide through an additional L chips. The mean time to do this is given by (47), with Δ replaced by L. We shall call this time $\bar{T}_{s/L}$:

$$\bar{T}_{s/L} = 2L(\lambda + \tfrac{1}{2})T_c + \frac{\lambda T_c P_F}{(1-P_F)^2}. \tag{49}$$

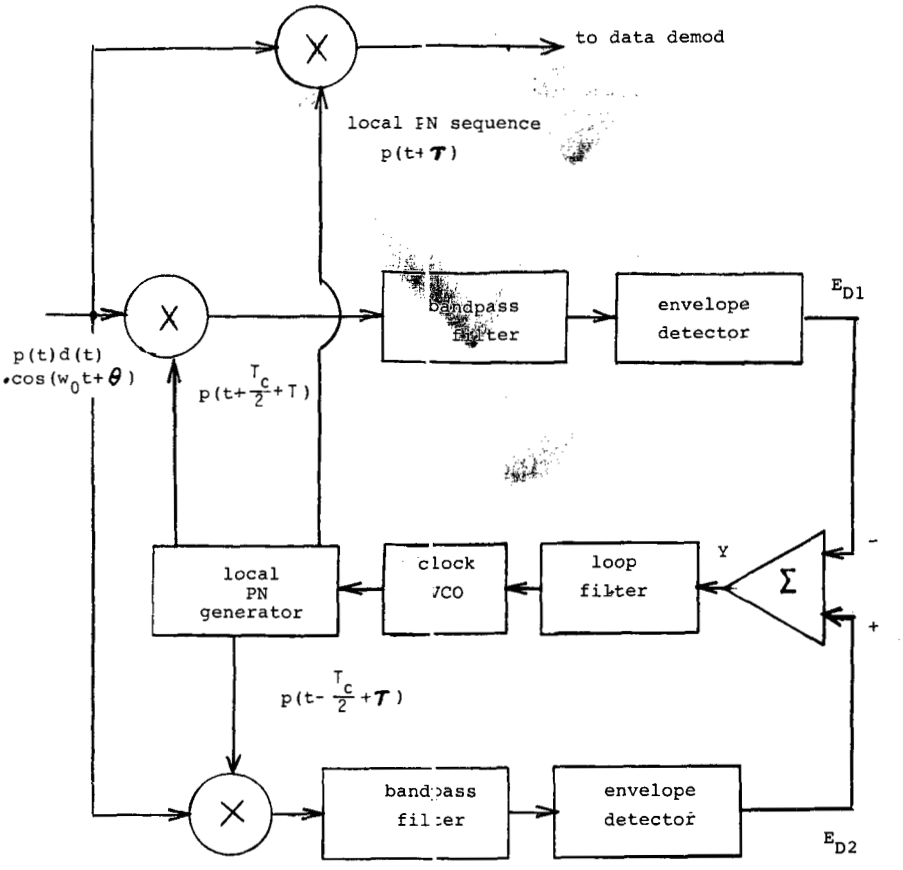


Fig. 21. Delay-locked loop for tracking direct-sequence PN signals.

The mean time to acquire a signal can now be written as

$$\bar{T}_{acq} = \bar{T}_s + \bar{T}_{s/L}[P_D(1-P_D) + 2P_D(1-P_D)^2 + \cdots]$$

$$\bar{T}_s + \frac{1-P_D}{P_D}\bar{T}_{s/L}$$

or

$$\bar{T}_{acq} = \left[L(\lambda + \tfrac{1}{2})T_c + \frac{\lambda T_c P_F}{(1-P_F)^2}\right] + \frac{1-P_D}{P_D}\left[2L(\lambda + \tfrac{1}{2})T_c + \frac{\lambda T_c P_F}{(1-P_F)^2}\right]. \quad (50)$$

VIII. TRACKING

Once acquisition, or coarse synchronization, has been accomplished, tracking, or fine synchronization, takes place. Specifically, this must include chip synchronization and, for coherent systems, carrier phase locking. In many practical systems, no data are transmitted for a specified time, sufficiently long to ensure that acquisition has occurred. During tracking, data are transmitted and detected. Typical references for tracking loops are [51]-[54].

The basic tracking loop for a direct-sequence spread-spectrum system using PSK data transmission is shown in Fig. 21. The incoming carrier at frequency f_0 is amplitude modulated by the product of the data $d(t)$ and the PN sequence $p(t)$. The tracking loop contains a local PN generator which is offset in phase from the incoming sequence $p(t)$ by a time τ which is less than one-half the chip time. To provide "fine" synchronization, the local PN generator generates two sequences, delayed from each other by one chip. The two bandpass filters are designed to have a two-sided bandwidth B equal to twice the data bit rate, i.e.,

$$B = 2R = 2/T. \quad (51)$$

In this way the data are passed, but the product of the two PN sequences $p(t)$ and $p(t \mp T_c/2 + \tau)$ is *averaged*. The envelope detector eliminates the data since $|d(t)| = 1$. As a result, the output of each envelope detector is approximately given by

$$E_{D1,2} \cong \overline{\left|p(t)p\left(t \pm \frac{T_c}{2} + \tau\right)\right|} = \left|R_p\left(\tau + \frac{T_c}{2}\right)\right| \quad (52)$$

where $R_p(x)$ is the autocorrelation function of the PN waveform as shown in Fig. 7(a). [See Section III for a discussion of the characteristics of $R_p(x)$.]

The output of the adder $Y(t)$ is shown in Fig. 22. We see from this figure that, when τ is positive, a positive voltage, proportional to Y, instructs the VCO to increase its frequency, thereby forcing τ to decrease, while when τ is negative, a

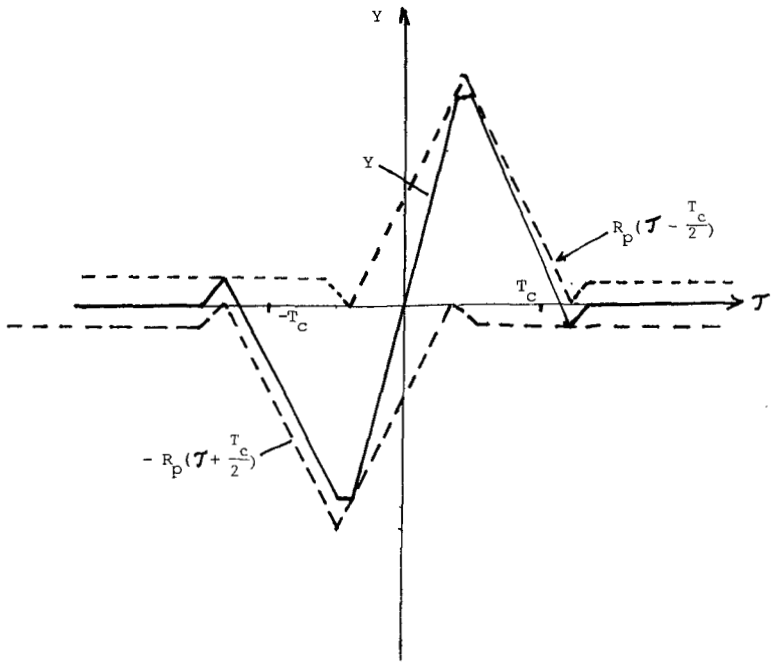


Fig. 22. Variation of Y with τ.

negative voltage instructs the VCO to reduce its frequency, thereby forcing τ to increase toward 0.

When the tracking error τ is made equal to zero, an output of the local PN generator $p(t+\tau) = p(t)$ is correlated with the input signal $p(t) \cdot d(t) \cos(\omega_0 t + \theta)$ to form

$$p^2(t)d(t)\cos(\omega_0 t + \theta) = d(t)\cos(\omega_0 t + \theta).$$

This despread PSK signal is inputted to the data demodulator where the data are detected.

An alternate technique for synchronization of a DS system is to use a tau-dither (TD) loop. This tracking loop is a delay-locked loop with only a single "arm," as shown in Fig. 23(a). The control (or gating) waveforms $g(t)$, $\bar{g}(t)$, and $g'(t)$ are shown in Fig. 23(b), and are used to generate both "arms" of the DLL even though only one arm is present. The TD loop is often used in lieu of the DLL because of its simplicity.

The operation of the loop is explained by observing that the control waveforms generate the signal

$$V_p(t) = g(t)p(t+\tau - T_c/2) + \bar{g}(t)p(t+\tau + T_c/2). \quad (53)$$

Note that either one or the other, but not both, of these waveforms occurs at each instant of time. The voltage $V_p(t)$ then multiplies the incoming signal

$$d(t)p(t)\cos(\omega_0 t + \theta).$$

The output of the bandpass filter is therefore

$$E_f(t) = d(t)g(t)\,|\,p(t)p(t+\tau+T_c/2)\,| + d(t)g(t)\,|\,p(t)p(t+\tau-T_c/2)\,| \quad (54)$$

where, as before, the average occurs because the bandpass filter is designed to pass the data and control signals, but cuts off well below the chip rate. The data are eliminated by the envelope detector, and (54) then yields

$$E_d(t) = g(t)\,|R_p(\tau + T_c/2)\,| + g(t)|R_p(\tau - T_c/2)\,|. \quad (55)$$

The input $Y(t)$ to the loop filter is

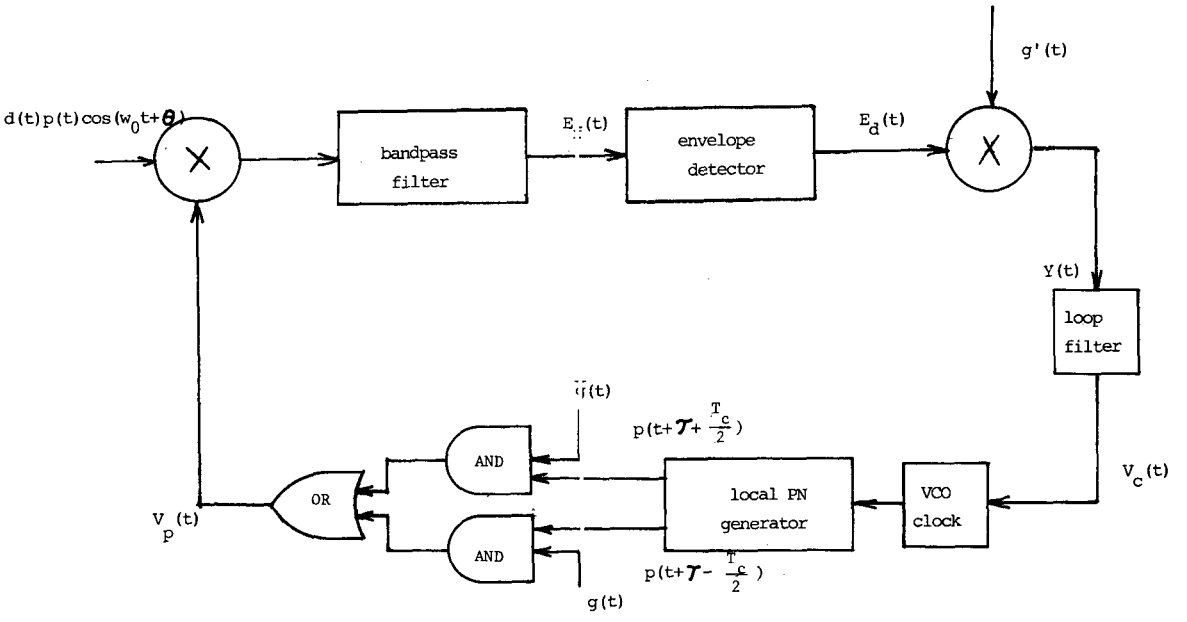
$$Y(t) = E_d(t)g'(t) = g(t)\,|R_p(\tau - T_c/2)\,| - \bar{g}(t)\,|R_p(\tau - T_c/2)\,| \quad (56)$$

where the "—" sign was introduced by the inversion caused by $g'(t)$.

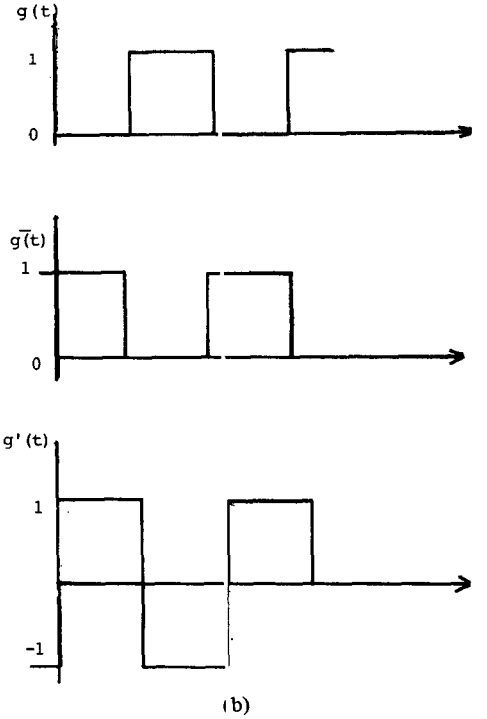
The narrow-band loop filter now "averages" $Y(t)$. Since each term is zero half of the time, the voltage into the VCO clock is, as before,

$$V_c(t) = |R_p(\tau - T_c/2)\,| - |R_p(\tau + T_c/2)\,|. \quad (57)$$

A typical tracking system for an FSK/FH spread-spectrum system is shown in Fig. 24. Waveforms are shown in Fig. 25. Once again, we have assumed that, although acquisition has occurred, there is still an error of τ seconds between transitions of the incoming signal's frequencies and the locally generated frequencies. The bandpass filter BPF is made sufficiently wide to pass the product signal $V_p(t)$ when $V_1(t)$ and $V_2(t)$ are at the same frequency f_i, but sufficiently narrow to reject $V_p(t)$ when $V_1(t)$ and $V_2(t)$ are at different frequencies f_i and f_{i+1}. Thus, the output of the envelope detector $V_d(t)$, shown in Fig. 24, is unity when $V_1(t)$ and $V_2(t)$ are at the same frequency and is zero when $V_1(t)$ and $V_2(t)$ are at different frequencies. From Fig. 25, we see that $V_g(t) = V_d(t)\ V_c(t)$ and is a three-level signal. This three-level signal is filtered to form a dc voltage which, in this case, presents a negative voltage to the VCO.



(a)



(b)

Fig. 23. The tau-dither loop. (a) Block diagram. (b) Control waveforms.

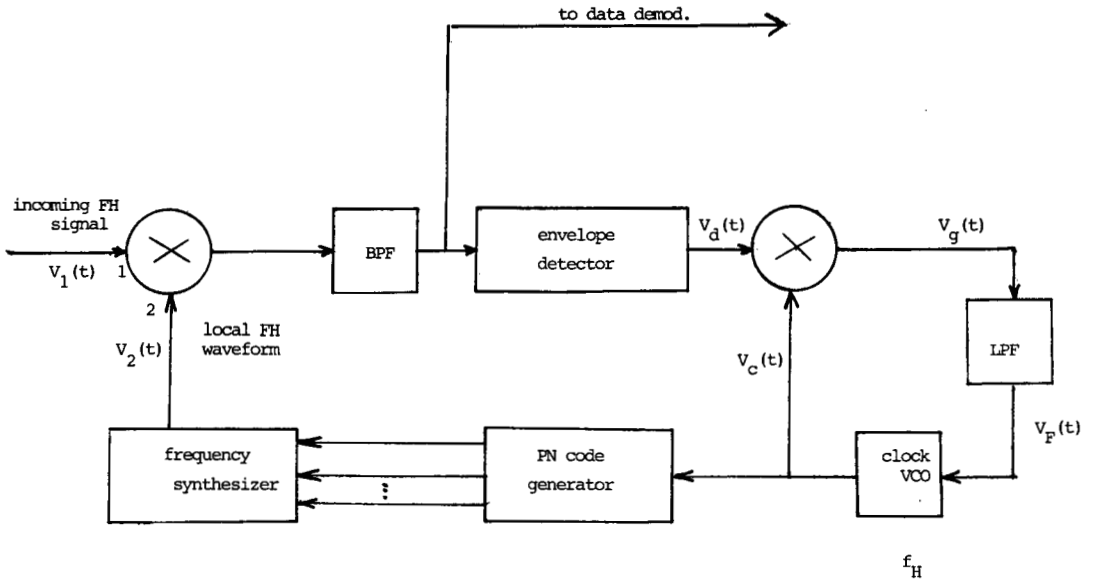


Fig. 24. Tracking loop for FH signals.

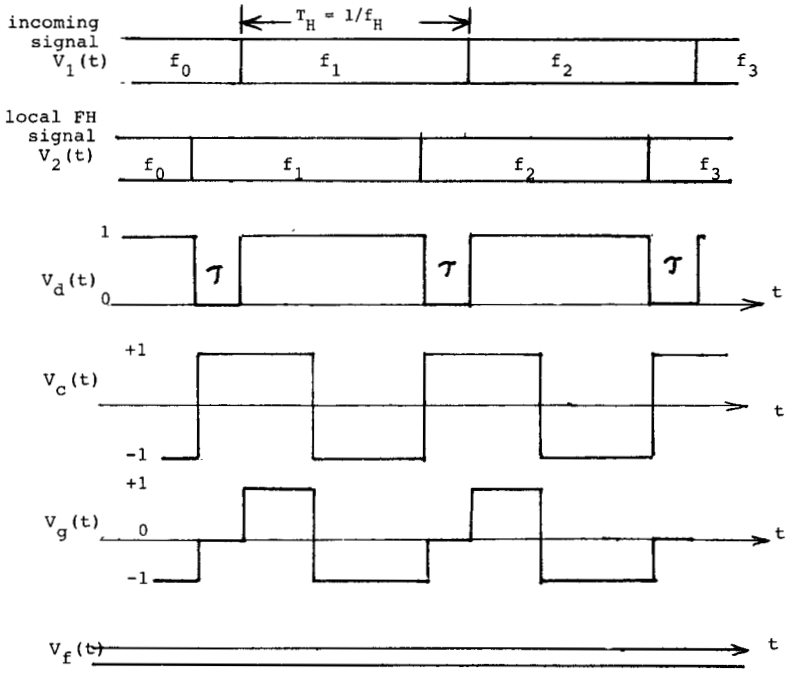


Fig. 25. Waveforms for tracking an FH signal.

It is readily seen that when $V_2(t)$ has frequency transitions which precede those of the incoming waveform $V_1(t)$, the voltage into the VCO will be negative, thereby delaying the transition, while if the local waveform frequency transitions occur after the incoming signal frequency transitions, the voltage into the VCO will be positive, thereby speeding up the transition.

The role of the tracking circuit is to keep the offset time τ small. However, even a relatively small τ can have a major impact on the probability of error of the received data. Referring to the DS system of Fig. 21, we see that if τ is not zero, the input to the data demodulator is $p(t)p(t + \tau)d(t) \cos(\omega_0 t + \theta)$ rather than $p^2(t)d(t) \cos(\omega_0 t + \theta) = d(t) \cos(\omega_0 t + \theta)$. The data demodulator removes the carrier and then averages the remaining signal, which in this case is $\overline{p(t)p(t + \tau)d(t)}$. The result is $\overline{p(t)p(t + \tau)d(t)}$. Thus, the amplitude of the data has been reduced by $\overline{p(t)p(t + \tau)} = R_p(\tau) \leq 1$. For example, if $\tau = T_c/10$, that data amplitude is reduced to 90 percent of its value, and the power is reduced to 0.81. Thus, the probability of error in correctly detecting the data is reduced from

$$P_e = Q\left(\sqrt{\frac{2E_b}{\eta_0}}\right)$$

to

$$P_e(\tau = T_c/10) = Q\left(\sqrt{\frac{1.62E_b}{\eta_0}}\right),$$

and at an E_b/η_0 of 9.6 dB, P_e is increased from 10^{-5} to 10^{-4}.

IX. CONCLUSIONS

This tutorial paper looked at some of the theoretical issues involved in the design of a spread-spectrum communication system. The topics discussed included the characteristics of PN sequences, the resulting processing gain when using either direct-sequence or frequency-hopping antijam considerations, multiple access when using spread spectrum, multipath effects, and acquisition and tracking systems.

No attempt was made to present other than fundamental concepts; indeed, to adequately cover the spread-spectrum system completely is the task for an entire text [55], [56]. Furthermore, to keep this paper reasonably concise, the authors chose to ignore both practical system considerations such as those encountered when operating at, say, HF, VHF, or UHF, and technology considerations, such as the role of surface acoustic wave devices and charge-coupled devices in the design of spread-spectrum systems.

Spread spectrum has for far too long been considered a technique with very limited applicability. Such is not the case. In addition to military applications, spread spectrum is being considered for commercial applications such as mobile telephone and microwave communications in congested areas.

The authors hope that this tutorial will result in more engineers and educators becoming aware of the potential of spread spectrum, the dissemination of this information in the classroom, and the use of spread spectrum (where appropriate) in the design of communication systems.

APPENDIX

ALGEBRAIC PROPERTIES OF LINEAR FEEDBACK SHIFT REGISTER SEQUENCES

In order to fully appreciate the study of shift register sequences, it is desirable to introduce the polynomial representation (or generating function) of a sequence

$$C(x) = \sum_{i=0}^{\infty} C_i x^i \leftrightarrow (C_0, C_1, C_2, \cdots). \tag{A1}$$

If the sequence is periodic with period L, i.e.,

$$C_0, C_1, C_2, \cdots, C_{L-1} C_0 C_1, \cdots, C_{L-1}, C_0, \cdots,$$

then since $x^L C(x) \leftrightarrow (0, 0, \cdots, 0, C_0, C_1, C_2, \cdots)$,

$$C(x)(1-x^L) = \sum_{i=0}^{L-1} C_i x^i \triangleq R(x) \tag{A2}$$

with $R(x)$ the (finite) polynomial representation of one period.

Thus, for any periodic sequence of period L,

$$C(x) = \frac{R(x)}{1-x^L}; \qquad \deg R(x) < L. \tag{A3}$$

Next consider the periodic sequence generated by the LFSR recursion. Multiplying each side by x^n and summing gives

$$\sum_{n=0}^{\infty} C_n x^n = \sum_{k=1}^{r} a_k \sum_{n=0}^{\infty} C_{n-k} x^n$$

$$= \sum_{k=1}^{r} a_k \sum_{l=0}^{k-1} C_{l-k} x^l + \sum_{k=1}^{r} a_k x^k \left(\sum_{n=0}^{\infty} C_n x^n \right).$$

The left-hand side is the generating function $C(x)$ of the sequence. The first term on the right is a polynomial of degree $<r$, call it $g(x)$, which depends only on the initial state of the register $C_{-1}, C_{-2}, C_{-3}, \cdots, C_{-r}$. Thus, the basic equation of the register sequence may be written as

$$C(x) = \frac{g(x)}{f(x)}; \qquad \deg g(x) < r \tag{A4}$$

where $f(x) \triangleq 1 - \Sigma_{k=1}^{r} a_k x^k$ is the characteristic polynomial[2] (or connection polynomial) of the register. Since $C(x)$ is the generating polynomial of a sequence of period $L = 2^r - 1$, it can be shown from (A3) and (A4) that $f(x)$ must divide $1 - x^L$. This is illustrated in the following example.

Example

The three-stage binary maximal length register with $f(x) = 1 + x + x^3$ has period 7. If the initial contents of the register are $C_{-3} = 1$, $C_{-2} = 0$, $C_{-1} = 0$, then $g(x) = a_3 = 1$ and $C(x) = 1/(1 + x + x^3)$. Long division (modulo 2) yields

$$C(x) = 1 + x + x^2 + x^4 + x^7 + x^9 + \cdots$$

which is the generating function of the periodic sequence

$$1\,1\,1\,0\,1\,0\,0 \vdots 1\,1\,1\,0\,1 \cdots,$$

and which is precisely the sequence generated by the corresponding recursion

$$C_n = C_{n-1} + C_{n-3} \pmod 2.$$

Observe that

$$(1 + x + x^3)(1 + x + x^2 + x^4) = 1 + x^7$$

so that $f(x)$ divides $1 + x^7$. Also, we may write

$$C(x) = \frac{1}{1 + x + x^3} \cdot \frac{1 + x + x^2 + x^4}{1 + x + x^2 + x^4} = \frac{1 + x + x^2 + x^4}{1 + x^7}$$

which is in the form of (A3).

[2] For binary sequences, all sums are modulo two and minus is the same as plus. The polynomials defining them have 0, 1 coefficients and are said to be polynomials over a finite field with two elements. A field is a set of elements, and two operations, say, + and •, which obey the usual rules of arithmetic. A finite field with q elements is called a Galois field and is designated as $GF(q)$.

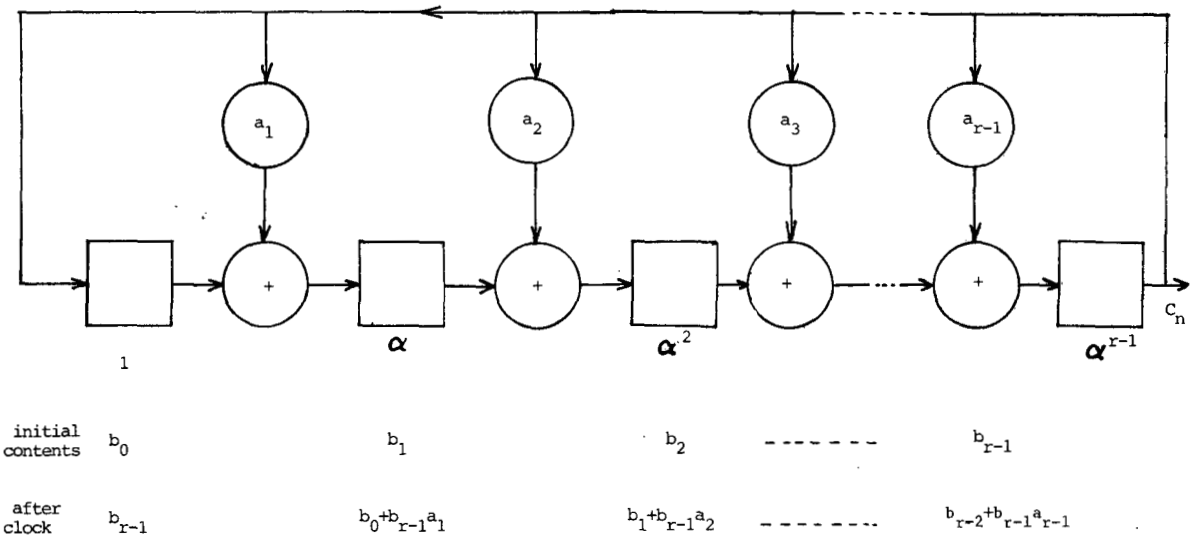


Fig. 26. Binary modular shift register generator with polynomial $f_M(x) = 1 + a_1x + a_2x^2 + \cdots + a_{r-1}x^{r-1} + x^r$.

It is easy to see (by multiplying and equating coefficients of like powers) that if

$$\frac{1}{f(x)} = \frac{1}{1 + a_1x + a_2x^2 + \cdots + a_rx^r}$$

$$= C_0 + C_1x + C_2x^2 + \cdots = C(x)$$

then

$$C_n = \sum_{k=1}^{r} a_kC_{n-k},$$

so that (except for initial conditions) $f(x)$ completely describes the maximal length sequence. Now what properties must $f(x)$ possess to ensure that the sequence is maximal length? Aside from the fact that $f(x)$ must divide $1 + x^L$, it is necessary (but not sufficient) that $f(x)$ be irreducible, i.e., $f(x) \neq f_1(x) \cdot f_2(x)$. Suppose that $f(x) = f_1(x)\, f_2(x)$ with $f_1(x)$ of degree r_1, $f_2(x)$ of degree r_2, and $r_1 + r_2 = r$. Then we can write, by partial fractions,

$$\frac{1}{f(x)} = \frac{\alpha(x)}{f_1(x)} + \frac{\beta(x)}{f_2(x)}; \qquad \deg \alpha(x) < r_1 \quad \deg \beta(x) < r_2.$$

The maximum period of the expansion of the first term is $2^{r_1}-1$ and that of the second term is $2^{r_2}-1$. Hence, the period of $1/f(x) \leq$ least common multiple of $(2^{r_1}-1, 2^{r_2}-1) < 2^r-3$. This is a contradiction, since if $f(x)$ were maximal length, the period of $1/f(x)$ would be 2^r-1. Thus, a *necessary* condition that the LFSR is maximal length is that $f(x)$ is irreducible.

A *sufficient* condition is that $f(x)$ is *primitive*. A primitive polynomial of degree r over $GF(2)$ is simply one for which the period of the coefficients of $1/f(x)$ is 2^r-1. However, additional insight can be had by examining the roots of $f(x)$. Since $f(x)$ is irreducible over $GF(2)$, we must imagine that the roots are elements of some larger (extension) field. Suppose that α is such an element and that $f(\alpha) = 0 = \alpha^r + a_{r-1}\alpha^{r-1} + \cdots + a_1\alpha + 1$ or

$$\alpha^r = a_{r-1}\alpha^{r-1} + \cdots + a_1\alpha + 1. \tag{A5}$$

We see that *all* powers of α can be expressed in terms of a linear combination of $\alpha^{r-1}, \alpha^{r-2}, \cdots, \alpha, 1$ since any powers larger than $r-1$ may be reduced using (A5). Specifically, suppose we have some power of α that we represent as

$$\beta \triangleq b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{r-1}\alpha^{r-1}. \tag{A6}$$

Then if we multiply this β by α and use (A5), we obtain

$$\beta\alpha = b_{r-1} + (b_0 + b_{r-1}a_1)\alpha + (b_1 + b_{r-1}a_2)\alpha^2 + \cdots + (b_{r-2} + b_{r-1}a_{r-1})\alpha^{r-1} \tag{A7}$$

The observations above may be expressed in another, more physical way with the introduction of an LFSR in modular form [called a modular shift register generator (MSRG)] shown in Fig. 26. The feedback, modulo 2, is between the delay elements. The binary contents of the register at any time are shown as $b_0, b, \cdots, b_{r-1}$. This vector can be identified with β as

$$\beta = b_0 + b_1\alpha + \cdots + b_{r-1}\alpha^{r-1} \leftrightarrow [b_0, b_1, \cdots b_{r-1}],$$

the contents of the first stage being identified with the coefficient of α^0, those of the second stage with the coefficient of α^1, etc. After one clock pulse, it is seen that the register contents correspond to

$$\beta\alpha = b_{r-1} + (b_0 + b_{r-1})\alpha + \cdots + (b_{r-2} + b_{r-1}a_{r-1})\alpha^{r-1} \leftrightarrow [b_{r-1}, \cdots, b_{r-2} + b_{r-1}a_{r-1}].$$

Thus, the MSRG is an α-multiplier. Now if $\alpha^0, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{L-1}$, $L = 2^r - 1$ are all *distinct*, we call α a *primitive* element of $GF(2^r)$. The register in Fig. 26 cycles through all states (starting in any nonzero state), and hence generates a maximal length sequence. Thus, another way of describing that the polynomial $f_M(x)$ is primitive (or maximal length) is that it has a primitive element in $GF(2^r)$ as a root.

There is an intimate relationship between the MSRG shown in Fig. 26 and the SSRG shown in Fig. 4. From Fig. 25 it is easily seen that the output sequence C_n satisfies the recursion

$$C_n = \sum_{k=0}^{r-1} a_k C_{n-r+k}. \tag{A8}$$

Multiplying both sides by x^n and summing yields

$$\begin{aligned} C(x) \triangleq \sum_{n=-\infty}^{\infty} C_n x^n &= \sum_{k=0}^{r-1} a_k \sum_{n=0}^{\infty} C_{n-r+k} x^n \\ &= \sum_{k=0}^{r-1} a_k x^{r-k} \sum_{l=-r+k}^{-1} C_l x^l \\ &\quad + x^r \sum_{k=0}^{r-1} a_k x^{-k} \left(\sum_{n=0}^{\infty} C_n x^n \right) \end{aligned} \tag{A9}$$

or

$$C(x) = g_M(x) + x^r \sum_{k=0}^{r-1} a_k x^{-k} C(x). \tag{A10}$$

$g_M(x)$ is the first term on the right-hand side of (A9) and is a polynomial of degree $< r$ which depends on the initial state. Then we have

$$C(x) = \frac{g_M(x)}{f_M(x)} \tag{A11}$$

where

$$f_M(x) = 1 - \{a_0 x^r + a_1 x^{r-1} + a_2 x^{r-2} + \cdots + a_{r-1} x\}$$

(recall that in $GF(2)$, minus is the same as plus) is the characteristic (or connection) polynomial of the MSRG. Since the sequence C_n [of coefficients of $C(x)$] when $f_M(x)$ is primitive depends *only* on $f_M(x)$ (discounting phase), the relationship between the SSRG and the MSRG which generates the *same* sequence is

$$f(x) = x^r f_M\left(\frac{1}{x}\right). \tag{A12}$$

$f_M(x)$ is called the *reciprocal* polynomial of $f(x)$ and is obtained from $f(x)$ by reversing the order of the coefficients.

There are several good tables of irreducible and primitive polynomials available [2], [5], [6], and although the tables do not list all the primitive polynomials, algorithms exist [7] which allow one to generate all primitive polynomials of a given degree if one of them is known. The number $\lambda(r)$ of primitive polynomials of degree r is [4]

$$\lambda(r) = \frac{\phi(2^r - 1)}{r} \tag{A13}$$

where $\phi(m)$ is the number of integers less than m which are relatively prime to m (Euler totient function). The growth of this number with r is shown in Table I.

TABLE I
THE NUMBER OF MAXIMAL LENGTH LINEAR SRG SEQUENCES OF DEGREE r = $\lambda(r) = \phi(2^r - 1)/r$

r	2^r-1	$\lambda(r)$
1	1	1
2	3	1
3	7	2
4	15	2
5	31	6
6	63	6
7	127	18
8	255	16
9	511	48
10	1,023	60
11	2,047	176
12	4,095	144
13	8,191	630
14	16,383	756
15	32,767	1,800
16	65,535	2,048
17	131,071	7,710
18	262,143	8,064
19	524,287	27,594
20	1,048,575	24,000
21	2,097,151	87,672
22	4,194,303	120,032

The algebra of LFSR's is useful in constructing codes with uniformly low cross correlation known as Gold codes. The underlying principle of these codes is based on the following *theorem* [15].

If $f_1(x)$ is the minimal polynomial of the primitive element $\alpha \in GF(2^r)$ and $f_t(x)$ is the minimal polynomial of α^t, where both $f_1(x)$ and $f_t(x)$ are of degree r and

$$t = \begin{cases} 2^{\frac{r+1}{2}} + 1, & r \text{ odd} \\ 2^{\frac{r+2}{2}} + 1, & r \text{ even,} \end{cases}$$

then the product $f(x) \triangleq f_1(x) f_t(x)$ determines an LFSR which generates $2^r + 1$ different sequences (corresponding to the $2^r + 1$ states in distinct cycles) of period $2^r - 1$, and such that for any pair C' and C'',

$$L\,|R_{C'C''}(\tau)| < t.$$

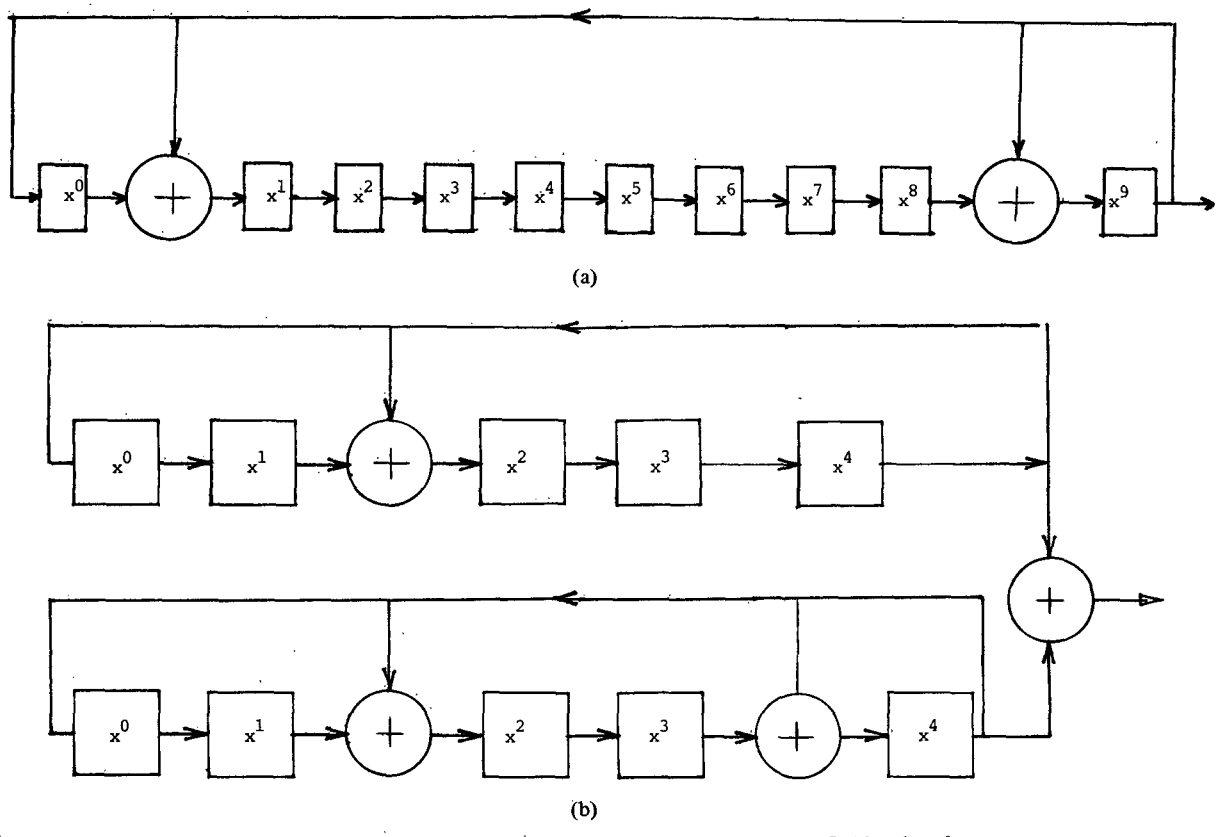


Fig. 27. Two implementations of LFSR which generate Gold codes of length $2^5 - 1 = 31$ with maximum cross correlation $t = 9$. (a) LFSR with $f(x) = 1 + x + x^3 + x^9 + x^{10}$. (b) LFSR which generates sequences corresponding to $f(x) = (1 + x^2 + x^5)\cdot(1 + x^2 + x^4 + x^5) = 1 + x + x^3 + x^9 + x^{10}$.

Futhermore, $R_{C'C''}(\tau)$ is only a three-valued function for any integer τ.

A minimal polynomial of α is simply the smallest degree monic[3] polynomial for which α is a root. With the help of a table of primitive polynomials, we can identify minimal polynomials of powers of α and easily construct Gold codes. For example, if $r = 5$ and $t = 2^3 + 1 = 9$, using [2] we find that $f_1(x) = 1 + x^2 + x^5$ and $f_9(x) = 1 + x^2 + x^4 + x^5$. Then $f(x) = 1 + x + x^3 + x^9 + x^{10}$. The two ways to represent this LFSR (in MSRG form) are shown in Fig. 27. Fig. 27(a) shows one long nonmaximal length register of degree 10 which generates sequences of period $2^5 - 1 = 31$. Since there are $2^{10} - 1$ possible nonzero initial states, the number of initial states that result in distinct cycles is $(2^{10} - 1)/(2^5 - 1) = 2^5 + 1 = 33$. Each of these initial states specifies a different Gold code of length 31. Fig. 27(b) shows how the same result can be obtained by adding the outputs of the two MLFSR's of degree 5 together modulo two. This follows simply from the observation that the sequence(s) generated by $f(x)$ are just the coefficients in the expansion of $1/f(x) = 1/f_1(x)\cdot f_9(x)$. By using partial fractions, one can see that the resulting coefficients are the (modulo two) sum of the coefficients of like powers in the expansion of $1/f_1(x)$ and $1/f_9(x)$. Naturally, the sequence resulting will depend on the relative *phases* of the two degree-5 registers. As before, there are $(2^{10} - 1)/(2^5 - 1) = 2^5 + 1 = 33$ relative phases which result in 33 different sequences satisfying the cross-correlation bound given by the theorem.

[3] A monic polynomial is one whose coefficient of its highest power is unity.

GLOSSARY OF SYMBOLS

a_n	{0, 1} feedback taps for LFSR.
B_D	One-sided bandwidth (Hz) for data signal(s).
B_{ss}	One-sided bandwidth (Hz) of baseband spread-spectrum signal.
$C(x)$	Generating function of C_n; $C(x) = \Sigma_{n=0}^{\infty} C_n x^n$.
C_n	{0, 1} LFSR sequence.
C_n' or C_n''	{1, −1} LFSR sequence.
D	Dimensionality of underlying signal space.
$d(t)$	Data sequence waveform.
Δ	Initial offset, in chips, of incoming signal and locally generated code.
DS	Direct sequence.
E_b	Energy/information bit.
E_J	Jammer energy over the correlation interval.
E_s	Energy/symbol.
$f(x)$	Characteristic (connection) polynomial of an LFSR, $f(x) = 1 + a_1 x + \cdots + a_{r-1} x^{r-1} + x^r$.
f_c	Chip rate; $T_c = 1/f_c$.
FH	Frequency hopping.
G_P	Processing gain.
$J(t)$	Jammer signal waveform.

K	Number of frequencies jammed by partial-band jammer.
$L = 2^r - 1$	Period of PN sequence.
L	Implementation losses.
λ	Number of chips examined during each search in the process of acquisition.
$\lambda(r)$	Number of binary maximal length PN codes of degree r (length $L = 2^r - 1$).
M	Signal alphabet size.
M_J	Jamming margin.
n	Number of chips/bit or number of dimensions of spread signal space.
N	Number of frequencies in FH.
N_c	Number of chips in uncertainty region at start of acquisition.
N_u	Number of users in CDMA system.
η_0	One-sided white noise power spectral density (W/Hz).
η_{0J}	$P_J/2f_c$ = power density of jammer.
$n_w(t)$	Additive white Gaussian noise (AWGN).
$p(t)$	Spreading sequence waveform.
P_D	Probability of detection.
P_e	Probability of error.
P_F	Probability of false alarm.
P_J	Jammer power.
P_N	Noise power.
P_s	Signal power.
PN	Pseudonoise sequence.
r	Number of stages of shift register.
$r(t)$	Received waveform.
R	Data rate (bits/s).
$R_p(\tau)$	Autocorrelation function.
$R_{C'C''}(\tau)$	Cross-correlation function of two (periodic) ± 1 sequences C_n', C_n''.
$\rho(\tau)$	$(1/T)\int_0^\tau p(t)\,p(t-\tau)\,dt$ (partial correlation function).
$\hat{\rho}(\tau)$	$(1/T)\int_\tau^T p(t)\,p(t-\tau)\,dt$.
$S(t)$	Transmitted signal waveform.
$S_p(f)$	Power spectral density of spreading sequence waveform [also denoted $S_{ss}(f)$].
SNR	Signal-to-noise power ratio.
SJR	Signal-to-jammer power ratio.
T	Signal or symbol duration.
T_c	Chip duration.
T_H	Time to hop one frequency; $1/T_H$ = hopping rate.
V	Correlator output voltage.

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers for their constructive suggestions in the final preparation of this paper.

REFERENCES

[1] R. A. Scholtz, "The origins of spread-spectrum communications," this issue, pp. 822–854.
[2] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd ed. Cambridge, MA: M.I.T. Press, 1972.
[3] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. New York: Wiley, 1965.
[4] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden Day, 1967.
[5] R. W. Marsh, *Table of Irreducible Polynomials over GF(2) Through Degree 19*. Washington, DC: NSA, 1957.
[6] W. Stahnke, "Primitive binary polynomials," *Math. Comput.*, vol. 27, pp. 977–980, Oct. 1973.
[7] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[8] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, Jan. 1969.
[9] N. G. deBruijn, "A combinatorial problem," in *Koninklijke Nederlands Akademie Van Wetenschappen Proc.*, 1946, pp. 758–764.
[10] E. J. Groth, "Generation of binary sequences with controllable complexity," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 288–296, May 1971.
[11] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732–736, Nov. 1976.
[12] H. Beker, "Multiplexed shift register sequences," presented at CRYPTO '81 Workshop, Santa Barbara, CA, 1981.
[13] J. L. Massey and J. J. Uhran, "Sub-baud coding," in *Proc. 13th Annu. Allerton Conf. Circuit and Syst. Theory*, Monticello, IL, Oct. 1975, pp. 539–547.
[14] J. H. Lindholm, "An analysis of the pseudo randomness properties of the subsequences of long m-sequences," *IEEE Trans. Inform. Theory*, vol. IT-14, 1968.
[15] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619–621, 1967.
[16] D. V. Sarwate and M. B. Pursley, "Cross correlation properties of pseudo-random and related sequences," *Proc. IEEE*, vol. 68, pp. 598–619, May 1980.
[17] A. Lempel, M. Cohn, and W. L. Eastman, "A new class of balanced binary sequences with optimal autocorrelation properties," IBM Res. Rep. RC 5632, Sept. 1975.
[18] A. G. Konheim, *Cryptography, A Primer*. New York: Wiley, 1981.
[19] D. L. Schilling, L. B. Milstein, R. L. Pickholtz, and R. Brown, "Optimization of the processing gain of an M-ary direct sequence spread spectrum communication system," *IEEE Trans. Commun.*, vol. COM-28, pp. 1389–1398, Aug. 1980.
[20] L. B. Milstein, S. Davidovici, and D. L. Schilling, "The effect of multiple-tone interfering signals on a direct sequence spread spectrum communication system," *IEEE Trans. Commun.*, vol. COM-30, pp. 436–446, Mar. 1982.
[21] S. W. Houston, "Tone and noise jamming performance of a spread spectrum M-ary FSK and 2, 4-ary DPSK waveforms," in *Proc. Nat. Aerosp. Electron. Conf.*, June 1975, pp. 51–58.
[22] G. K. Huth, "Optimization of coded spread spectrum systems performance," *IEEE Trans. Commun.*, vol. COM-25, pp. 763–770, Aug. 1977.
[23] R. H. Pettit, "A susceptibility analysis of frequency hopped M-ary NCPSK—Partial-band noise on CW tone jamming," presented at the Symp. Syst. Theory, May 1979.
[24] L. B. Milstein, R. L. Pickholtz, D. L. Schilling, "Optimization of the processing gain of an FSK-FH system," *IEEE Trans. Commun.*, vol. COM-28, pp. 1062–1079, July 1980.
[25] M. K. Simon and A. Polydoros, "Coherent detection of frequency-hopped quadrature modulations in the presence of jamming—Part I: QPSK and QASK; Part II: QPR class I modulation," *IEEE Trans. Commun.*, vol. COM-29, pp. 1644–1668, Nov. 1981.
[26] A. J. Viterbi and I. M. Jacobs, "Advances in coding and modulation for noncoherent channels affected by fading, partial band, and multiple access interference," in *Advances in Communication Systems*, vol. 4. New York: Academic, 1975.
[27] J. M. Aein and R. D. Turner, "Effect of co-channel interference on CPSK carriers," *IEEE Trans. Commun.*, vol. COM-21, pp. 783–790, July 1973.
[28] R. H. Pettit, "Error probability for NCFSK with linear FM jamming," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-8, pp. 609–614, Sept. 1972.
[29] A. J. Viterbi, "Spread spectrum communications—Myths and realities," *IEEE Commun. Mag.*, pp. 11–18, May 1979.
[30] D. J. Torrieri, *Principles of Military Communication Systems*. Dedham, MA: Artech House, 1981.

[31] M. B. Pursley, "Performance evaluation for phase-coded spread spectrum multiple-access communication—Part I: System analysis," *IEEE Trans. Commun.*, vol. COM-25, pp. 795–799, Aug. 1977.
[32] K. Yao, "Error probability of asynchronous spread-spectrum multiple access communication systems," *IEEE Trans. Commun.*, vol. COM-25, pp. 803–809, Aug. 1977.
[33] C. L. Weber, G. K. Huth, and B. H. Batson, "Performance considerations of code division multiple access systems," *IEEE Trans. Veh. Technol.*, vol. VT-30, pp. 3–10, Feb. 1981.
[34] M. B. Pursley and D. V. Sarwate, "Performance evaluation for phase-coded spread spectrum multiple-access communication—Part II. Code sequence analysis," *IEEE Trans. Commun.*, vol. COM-25, pp. 800–803, Aug. 1977.
[35] M. B. Pursley and H. F. A. Roefs, "Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences," *IEEE Trans. Commun.*, vol. COM-25, pp. 1597–1604, Aug. 1977.
[36] G. Solomon, "Optimal frequency hopping sequences for multiple access," in *Proc. 1973 Symp. Spread Spectrum Commun.*, vol. 1, AD915852, pp. 33–35.
[37] D. V. Sarwate and M. B. Pursley, "Hopping patterns for frequency-hopped multiple-access communication," in *Proc. 1978 IEEE Int. Conf. Commun.*, vol. 1, pp. 7.4.1–7.4.3.
[38] P. S. Henry, "Spectrum efficiency of a frequency-hopped-DPSK spread spectrum mobile radio system," *IEEE Trans. Veh. Technol.*, vol. VT-28, pp. 327–329, Nov. 1979.
[39] O. C. Yue, "Hard-limited versus linear combining for frequency-hopping multiple-access systems in a Rayleigh fading environment," *IEEE Trans. Veh. Technol.*, vol. VT-30, pp. 10–14, Feb. 1981.
[40] R. W. Nettleton and G. R. Cooper, "Performance of a frequency-hopped differentially modulated spread-spectrum receiver in a Rayleigh fading channel," *IEEE Trans. Veh. Technol.*, vol. VT-30, pp. 14–29, Feb. 1981.
[41] D. E. Borth and M. B. Pursley, "Analysis of direct-sequence spread-spectrum multiple-access communication over Rician fading channels," *IEEE Trans. Commun.*, vol. COM-27, pp. 1566–1577, Oct. 1979.
[42] E. A. Geraniotis and M. B. Pursley, "Error probability bounds for slow frequency-hopped spread-spectrum multiple access communications over fading channels," in *Proc. 1981 Int. Conf. Commun.*
[43] L. B. Milstein and D. L. Schilling, "Performance of a spread spectrum communication system operating over a frequency-selective fading channel in the presence of tone interference," *IEEE Trans. Commun.*, vol. COM-30, pp. 240–247, Jan. 1982.
[44] ——, "The effect of frequency selective fading on a noncoherent FH-FSK system operating with partial-band interference," this issue, pp. 904–912.
[45] J. M. Aein and R. L. Pickholtz, "A simple unified phasor analysis for PN multiple access to limiting repeaters," this issue, pp. 1018–1026.
[46] R. B. Ward, "Acquisition of pseudonoise signals by sequential estimation," *IEEE Trans. Commun. Technol.*, vol. COM-13, pp. 474–483, Dec. 1965.
[47] R. B. Ward and K. P. Yiu, "Acquisition of pseudonoise signals by recursion-aided sequential estimation," *IEEE Trans. Commun.*, vol. COM-25, pp. 784–794, Aug. 1977.
[48] P. M. Hopkins, "A unified analysis of pseudonoise synchronization by envelope correlation," *IEEE Trans. Commun.*, vol. COM-25, pp. 770–778, Aug. 1977.
[49] J. K. Holmes and C. C. Chen, "Acquisition time performance of PN spread-spectrum systems," *IEEE Trans. Commun.*, vol. COM-25, pp. 778–783, Aug. 1977.
[50] S. S. Rappaport, "On practical setting of detection thresholds," *Proc. IEEE*, vol. 57, pp. 1420–1421, Aug. 1969.
[51] J. J. Spilker, Jr., "Delay-lock tracking of binary signals," *IEEE Trans. Space Electron. Telem.*, vol. SET-9, pp. 1–8, Mar. 1963.
[52] P. T. Nielson, "On the acquisition behavior of delay lock loops," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-12, pp. 415–523, July 1976.
[53] ——, "On the acquisition behavior of delay lock loops," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-11, pp. 415–417, May 1975.
[54] H. P. Hartman, "Analysis of the dithering loop for PN code tracking," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-10, pp. 2–9, Jan. 1974.
[55] R. C. Dixon, *Spread Spectrum Systems*. New York: Wiley, 1976.
[56] J. K. Holmes, *Coherent Spread Spectrum Systems*. New York: Wiley, 1982.

★

Raymond L. Pickholtz (S'54–A'55–M'60–SM'77–F'82) received the B.E.E. and M.S.E.E. degrees from the City College of New York, New York, NY, and the Ph.D. degree from the Polytechnic Institute of Brooklyn, Brooklyn, NY.

He is a Professor and was Chairman of the Department of Electrical Engineering and Computer Science, George Washington University, Washington, DC. He was a Research Engineer at RCA Laboratories and at ITT Laboratories for a period of ten years, working on problems ranging from color television to secure communications and guidance before returning to academia. He was an Associate Professor at the Polytechnic Institute of Brooklyn until 1972 when he joined the faculty at George Washington University. He taught part-time at New York University, New York, and in the Department of Physics, Brooklyn College, Brooklyn. He was a Visiting Professor at the University of Quebec, Quebec, P.Q., Canada. He has been an active consultant in communications to industry and government for many years and has lectured extensivley in this country, Canada, Europe, and South America on various aspects of communications. He is President of Telecommunications Associates, a small consulting and research firm.

Dr. Pickholtz has been very active in the IEEE and in the Communications Society (ComSoc) in particular. He was the first Editor for Computer Communication of the IEEE TRANSACTIONS ON COMMUNICATIONS. He organized the Technical Committee on Computer Communication of ComSoc. He was Guest Editor of the Special TRANSACTIONS Issue on Computer Communications. He was General Chairman of the Third Data Networks Symposium and of the Workshop on Data Networks. In addition, he was Chairman of the New York Chapter of the Information Theory Group and has also contributed his efforts to the Computer Society.

★

Donald L. Schilling (S'56–M'58–SM'69–F'75), for a photograph and biography, see this issue, p. 821.

★

Laurence B. Milstein (S'66–M'68–SM'77), for a photograph and biography, see this issue, p. 820.