A spread-spectrum signal is one with an extra modulation that expands the signal bandwidth greatly beyond what is required by the underlying coded-data modulation. Spread-spectrum communication systems are useful for suppressing interference, making secure communications difficult to detect and process, accommodating fading and multipath channels, and providing a multiple-access capability. Spread-spectrum signals cause relatively minor interference to other systems operating in the same spectral band. The most practical and dominant spread-spectrum systems are direct-sequence and frequency-hopping systems.

There is no fundamental theoretical barrier to the effectiveness of spread-spectrum communications. That remarkable fact is not immediately apparent since the increased bandwidth of a spread-spectrum signal might require a receive filter that passes more noise power than necessary to the demodulator. However, when any signal and white Gaussian noise are applied to a filter matched to the signal, the sampled filter output has a signal-to-noise ratio that depends solely on the energy-to-noise-density ratio. Thus, the bandwidth of the input signal is irrelevant, and spread-spectrum signals have no inherent limitations.

Direct-sequence modulation entails the direct addition of a high-rate spreading sequence with a lower-rate data sequence, resulting in a transmitted signal with a relatively wide bandwidth. The removal of the spreading sequence in the receiver causes a contraction of the bandwidth that can be exploited by appropriate filtering to remove a large portion of the interference. This chapter describes basic spreading sequences and waveforms and provides a detailed analysis of how the direct-sequence receiver suppresses various forms of interference.

2.1 Definitions and Concepts

A direct-sequence signal is a spread-spectrum signal generated by the direct mixing of the data with a spreading waveform before the final signal modulation. Ideally, a direct-sequence signal with binary phase-shift keying (BPSK) or differential PSK
(DPSK) data modulation can be represented by

\[ s(t) = Ad(t)p(t)\cos(2\pi f_c t + \theta) \]  

(2.1)

where \( A \) is the signal amplitude, \( d(t) \) is the data modulation, \( p(t) \) is the spreading waveform, \( f_c \) is the carrier frequency, and \( \theta \) is the phase at \( t = 0 \). The data modulation is a sequence of nonoverlapping rectangular pulses of duration \( T_s \), each of which has an amplitude \( d_i = +1 \) if the associated data symbol is a 1 and \( d_i = -1 \) if it is a 0 (alternatively, the mapping could be 1 \( \rightarrow \) -1 and 0 \( \rightarrow \) +1). The spreading waveform has the form

\[ p(t) = \sum_{i=-\infty}^{\infty} p_i \psi(t - iT_c) \]  

(2.2)

where each \( p_i \) equals +1 or -1 and represents one chip of the spreading sequence. The chip waveform \( \psi(t) \) is designed to limit interchip interference in the receiver and ideally is confined to the time interval \([0, T_c]\). A rectangular chip waveform has \( \psi(t) = w(t, T_c) \), where

\[ w(t, T) = \begin{cases} 
1, & 0 \leq t < T \\
0, & \text{otherwise.} 
\end{cases} \]  

(2.3)

Figure 2.1 depicts an example of \( d(t) \) and \( p(t) \) for a rectangular chip waveform.

Message privacy is provided by a direct-sequence system if a transmitted message cannot be recovered without knowledge of the spreading sequence. Although
message secrecy can be protected by cryptography, message privacy provides protection even if cryptography is not used. If the data-symbol and chip transitions do not coincide, then it is theoretically possible to separate the data symbols from the chips by detecting and analyzing the transitions. To ensure message privacy, which is assumed henceforth, the data-symbol transitions must coincide with the chip transitions. Another reason for common transitions is the simplification of the receiver implementation. Since the transitions coincide, the spreading factor $G = T_s/T_c$ is a positive integer equal to the number of chips in a symbol interval. If $W$ is the bandwidth of $p(t)$ and $B$ is the bandwidth of $d(t)$, the spreading due to $p(t)$ ensures that $s(t)$ has a bandwidth $W >> B$.

Figure 2.2 is a functional or conceptual block diagram of the basic operation of a direct-sequence system with BPSK or DPSK. To provide common transitions, data symbols and chips, which are represented by digital sequences of 0’s and 1’s, are synchronized by the same clock and then modulo-2 added in the transmitter. The adder output is converted according to 0 $\rightarrow -1$ and 1 $\rightarrow +1$ before the chip-waveform modulation shown in Fig. 2.2a. After upconversion, the modulated signal is transmitted. As indicated in Fig. 2.2b, the received signal is filtered and then
multiplied by a synchronized local replica of $p(t)$. If $\psi(t)$ is rectangular with unit amplitude, then $p(t) = \pm 1$ and $p^2(t) = 1$. Therefore, if the filtered signal is given by (2.1), the multiplication yields the despread signal

$$s_1(t) = p(t)s(t) = Ad(t)\cos(2\pi f_c t + \theta) \quad (2.4)$$

at the input of the BPSK or DPSK demodulator. A standard demodulator extracts the data symbols or provides symbol metrics to the decoder.

Figure 2.3a is a qualitative depiction of the relative spectra of the desired signal and narrowband interference at the output of the wideband filter. Multiplication of the received signal by the spreading waveform, which is called despreading, produces the spectra of Fig. 2.3b at the demodulator input. The signal bandwidth is reduced to $B$, while the interference energy is spread over a bandwidth exceeding $W$. Since the filtering action of the demodulator then removes most of the interference spectrum that does not overlap the signal spectrum, most of the original interference energy is eliminated. An approximate measure of the interference suppression capability is given by the ratio $W/B$. Whatever the precise definition of a bandwidth, $W$ and $B$ are proportional to $1/T_c$ and $1/T_s$, respectively, with the same proportionality constant. Therefore,

$$G = \frac{T_s}{T_c} = \frac{W}{B} \quad (2.5)$$

which links the spreading factor with the interference suppression illustrated in the figure. Since its spectrum is unchanged by the despreading, white Gaussian noise is not suppressed by a direct-sequence system.

In practical systems, the wideband filter in the transmitter is used to limit the out-of-band radiation. This filter and the propagation channel disperse the chip waveform so that it is no longer confined to $[0, T_c]$. To prevent significant interchip interference in the receiver, the filtered chip waveform must be designed so that the Nyquist criterion for no interchip interference is approximately satisfied. A convenient representation of a direct-sequence signal when the chip waveform may extend beyond...
2.2 Spreading Sequences and Waveforms

Fig. 2.4 Sample function of a random binary sequence

\[ s(t) = A \sum_{i=-\infty}^{\infty} d_{[i/G]} p_i \psi (t - iT_c) \cos (2\pi f_c t + \theta) \]  

(2.6)

where \([x]\) denotes the integer part of \(x\). When the chip waveform is assumed to be confined to \([0, T_c]\), then (2.6) can be expressed by (2.1) and (2.2).

2.2 Spreading Sequences and Waveforms

A direct-sequence receiver computes the correlation between the received spreading sequence and a stored replica of the spreading sequence it is expecting. The correlation should be high when the receiver is synchronized with the received sequence, and low when it is not. Thus, it is critical that the spreading sequence have suitable autocorrelation properties. More is required for multiple-access communications when many different spreading sequences might be received, and this topic is addressed in Chap. 7. Synchronization issues are explained in Chap. 4.

Random Binary Sequence

A random binary sequence \(x(t)\) is a stochastic process that consists of independent, identically distributed symbols, each of duration \(T\). Each symbol takes the value \(+1\) with probability 1/2 or the value \(-1\) with probability 1/2. Therefore, \(E[x(t)] = 0\) for all \(t\), and

\[ P \left[ x(t) = i \right] = \frac{1}{2}, \quad i = +1, -1. \]  

(2.7)

A sample function of a random binary sequence \(x(t)\) is illustrated in Fig. 2.4. A symbol boundary does not necessarily occur at \(t = 0\).

The autocorrelation of a stochastic process \(x(t)\) is defined as

\[ R_x(t, \tau) = E \left[ x(t)x(t + \tau) \right]. \]  

(2.8)
A stochastic process is wide-sense stationary (App. C.2, Section “Stationary Stochastic Processes”) if its mean is constant and $R_x(t, \tau)$ is a function of $\tau$ alone so that the autocorrelation may be denoted by $R_x(\tau)$. As shown subsequently, a random binary sequence is wide-sense stationary if the location of the first symbol transition or start of a new symbol after $t = 0$ is a random variable uniformly distributed over the half-open interval $(0, T]$.

From (2.7) and the definitions of an expected value and a conditional probability, it follows that the autocorrelation of a random binary sequence is

$$R_x(t, \tau) = \frac{1}{2} P[x(t + \tau) = 1|x(t) = 1] - \frac{1}{2} P[x(t + \tau) = -1|x(t) = 1]$$

$$+ \frac{1}{2} P[x(t + \tau) = -1|x(t) = -1] - \frac{1}{2} P[x(t + \tau) = 1|x(t) = -1]$$

(2.9)

where $P[A|B]$ denotes the conditional probability of event $A$ given the occurrence of event $B$. From the theorem of total probability, it follows that

$$P[x(t + \tau) = i|x(t) = i] + P[x(t + \tau) = -i|x(t) = i] = 1, \ i = +1, -1.$$  

(2.10)

Since both of the following probabilities are equal to the probability that $x(t)$ and $x(t + \tau)$ differ,

$$P[x(t + \tau) = 1|x(t) = -1] = P[x(t + \tau) = -1|x(t) = 1].$$  

(2.11)

Substitution of (2.10) and (2.11) into (2.9) yields

$$R_x(t, \tau) = 1 - 2P[x(t + \tau) = 1|x(t) = -1].$$  

(2.12)

If $|\tau| \geq T$, then $x(t)$ and $x(t + \tau)$ are independent random variables because $t$ and $t + \tau$ are in different symbol intervals. Therefore,

$$P[x(t + \tau) = 1|x(t) = -1] = P[x(t + \tau) = 1] = \frac{1}{2}$$  

(2.13)

and (2.6) implies that $R_x(t, \tau) = 0$ for $|\tau| \geq T$. If $|\tau| < T$, then $x(t)$ and $x(t + \tau)$ are independent only if a symbol transition occurs in the half-open interval $I_0 = (t, t+\tau]$. Thus, the random binary sequence is not wide-sense stationary without an additional assumption.

To ensure wide-sense stationarity, we assume that the location of the first symbol transition after $t = 0$ is a random variable uniformly distributed over the half-open interval $(0, T]$. Consider any half-open interval $I_1$ of length $T$ that includes $I_0$. Exactly one transition occurs in $I_1$. Since the first transition for $t > 0$ is assumed to be uniformly distributed over $(0, T]$, the probability that a transition in $I_1$ occurs in $I_0$ is $|\tau|/T$. If a transition occurs in $I_0$, then $x(t)$ and $x(t + \tau)$ are independent, and hence differ with probability $1/2$; otherwise, $x(t) = x(t + \tau)$. Consequently, $P[x(t + \tau) = 1|x(t) = -1] = |\tau|/2T$ if $|\tau| < T$. Substitution of the preceding results into (2.12)
confirms the wide-sense stationarity of $x(t)$ and gives the *autocorrelation of the random binary sequence*:

$$R_x(\tau) = \Lambda \left( \frac{\tau}{T} \right)$$

(2.14)

where the *triangular function* is defined by

$$\Lambda(t) = \begin{cases} 1 - |t|, & |t| \leq 1 \\ 0, & |t| > 1. \end{cases}$$

(2.15)

The *power spectral density of the random binary sequence* is the Fourier transform of the autocorrelation. An elementary integration gives the power spectral density:

$$S_x(f) = \int_{-\infty}^{\infty} \Lambda \left( \frac{t}{T} \right) \exp(-j2\pi ft) dt$$

$$= T \text{sinc}^2 fT$$

(2.16)

where $j = \sqrt{-1}$ and sinc $x = (\sin \pi x)/\pi x$.

### Shift-Register Sequences

Ideally, one would prefer a random binary sequence as the spreading sequence. However, practical synchronization requirements in the receiver force one to use periodic binary sequences. A *shift-register sequence* is a periodic binary sequence generated by the output of a feedback shift register or by combining the outputs of feedback shift registers. A *feedback shift register*, which is diagrammed in Fig. 2.5, consists of consecutive two-state memory or storage stages and feedback logic. Binary sequences drawn from the alphabet \{0,1\} are shifted through the shift register in response to clock pulses. The *contents* of the stages, which are identical to their outputs, are logically combined to produce the input to the first stage. The initial contents of the stages and the feedback logic determine the successive contents of the stages. If the feedback logic consists entirely of modulo-2 adders (exclusive-OR gates), a feedback shift register and its generated sequence are called *linear*. 
Figure 2.6a illustrates a linear feedback shift register with three stages and an output sequence extracted from the final stage. The input to the first stage is the modulo-2 sum of the contents of the second and third stages. After each clock pulse, the contents of the first two stages are shifted to the right, and the input to the first stage becomes its content. If the initial contents of the shift-register stages are 0 0 1, the subsequent contents after successive shifts are listed in Fig. 2.6b. Since the shift register returns to its initial state after 7 shifts, the shift-register sequence extracted from the final stage has a period of 7 bits.

The state of an m-stage shift register after clock pulse $i$ is the vector

$$S(i) = [s_1(i) \; s_2(i) \ldots s_m(i)], \quad i \geq 0$$

where $s_l(i)$ denotes the content of stage $l$ after clock pulse $i$, and $S(0)$ is the initial state. The definition of a shift register implies that

$$s_l(i) = s_{l-k}(i-k), \quad i \geq k \geq 0, \quad k \leq l \leq m$$

where $s_0(i)$ denotes the input to stage 1 after clock pulse $i$. If $a_i$ denotes the state of bit $i$ of the shift-register sequence, then $a_i = s_m(i)$. The state of a feedback shift register uniquely determines the subsequent sequence of states and the shift-register sequence.

The period of a shift-register sequence $\{a_i\}$ is defined as the smallest positive integer $N$ for which $a_{i+N} = a_i, \; i \geq 0$. Since the number of distinct states of an m-stage nonlinear feedback shift register is $2^m$, the sequence of states and the shift-register sequence have period $N \leq 2^m$. 
The input to stage 1 of a linear feedback shift register is

\[ s_0(i) = \sum_{k=1}^{m} c_k s_k(i), \quad i \geq 0 \]  \hspace{1cm} (2.19)

where the operations are modulo-2, and the feedback coefficient \( c_k \) equals either 0 or 1, depending on whether the output of stage \( k \) feeds a modulo-2 adder. An \( m \)-stage shift register is defined to have \( c_m = 1 \); otherwise, the final state would not contribute to the generation of the output sequence, but would only provide a one-shift delay. For example, Fig. 2.6 gives \( c_1 = 0, c_2 = c_3 = 1 \), and \( s_0(i) = s_2(i) \oplus s_3(i) \), where \( \oplus \) denotes modulo-2 addition. A general representation of a linear feedback shift register is shown in Fig. 2.7a. If \( c_k = 1 \), the corresponding switch is closed; if \( c_k = 0 \), it is open.

Since the shift-register sequence bit \( a_i = s_m(i) \), (2.18) and (2.19) imply that for \( i \geq m \),

\[ a_i = s_0(i - m) = \sum_{k=1}^{m} c_k s_k(i - m) = \sum_{k=1}^{m} c_k s_m(i - k) \]  \hspace{1cm} (2.20)

which indicates that each bit satisfies the linear recurrence relation:

\[ a_i = \sum_{k=1}^{m} c_k a_{i-k}, \quad i \geq m. \]  \hspace{1cm} (2.21)

The first \( m \) bits of the shift-register sequence are determined solely by the initial state:

\[ a_i = s_{m-i}(0), \quad 0 \leq i \leq m - 1. \]  \hspace{1cm} (2.22)

Figure 2.7a is not necessarily the best way to generate a particular shift-register sequence. Figure 2.7b illustrates an implementation that allows higher-speed operation. The diagram indicates that

\[ s_l(i) = s_{l-1}(i - 1) \oplus c_{m-l+1} s_m(i - 1), \quad i \geq 1, \quad 2 \leq l \leq m \]  \hspace{1cm} (2.23)
\[ s_1(i) = s_m(i - 1) \quad i \geq 1. \quad (2.24) \]

Repeated application of (2.23) implies that
\[
\begin{align*}
  s_m(i) &= s_{m-1}(i - 1) \oplus c_1 s_m(i - 1), \quad i \geq 1 \\
  s_{m-1}(i - 1) &= s_{m-2}(i - 2) \oplus c_2 s_m(i - 2), \quad i \geq 2 \\
  &\vdots \\
  s_2(i - m + 2) &= s_1(i - m + 1) \oplus c_{m-1} s_m(i - m + 1), \quad i \geq m - 1.
\end{align*}
\]  

(2.25)

Addition of these \( m \) equations yields
\[ s_m(i) = s_1(i - m + 1) \oplus \sum_{k=1}^{m-1} c_k s_m(i - k), \quad i \geq m - 1. \quad (2.26) \]

Substituting (2.24) and then \( a_i = s_m(i) \) into (2.26), we obtain
\[ a_i = a_{i-m} \oplus \sum_{k=1}^{m-1} c_k a_{i-k}, \quad i \geq m. \quad (2.27) \]

Since \( c_m = 1 \), (2.27) is the same as (2.20). Thus, the two implementations can produce the same shift-register sequence indefinitely if the first \( m \) bits coincide. However, they require different initial states and have different sequences of states.

Successive substitutions into the first equation of sequence (2.25) yields
\[ s_m(i) = s_{m-i}(0) \oplus \sum_{k=1}^{i} c_k s_m(i - k), \quad 1 \leq i \leq m - 1. \quad (2.28) \]

Substituting \( a_i = s_m(i), a_{i-k} = s_m(i - k) \), and \( j = m - i \) into (2.28) and then using binary arithmetic, we obtain
\[ s_j(0) = a_{m-j} \oplus \sum_{k=1}^{m-j} c_k a_{m-j-k}, \quad 1 \leq l \leq m. \quad (2.29) \]

If \( a_0, a_1, \ldots a_{m-1} \) are specified, then (2.29) gives the corresponding initial state of the high-speed shift register.

The sum of binary sequence \( \mathbf{a} = (a_0, a_1, \ldots) \) and binary sequence \( \mathbf{b} = (b_0, b_1, \ldots) \) is defined to be the binary sequence \( \mathbf{d} = \mathbf{a} \oplus \mathbf{b} \), each bit of which is
\[ d_i = a_i \oplus b_i, \quad i \geq 0. \quad (2.30) \]

Consider sequences \( \mathbf{a} \) and \( \mathbf{b} \) that are generated by the same linear feedback shift register but may differ because the initial states may be different. For the sequence
Principles of Spread-Spectrum Communication Systems
Torrieri, D.
2015, XVIII, 641 p. 237 illus., 37 illus. in color.,
Hardcover
ISBN: 978-3-319-14095-7