Memo of J. G. Proakis and M Salehi, "Digital Communications", 5th ed. New York: McGraw-Hill, 2007

Chenggao HAN

Contents

Chapter 1

Introduction

In this book, we present the basic principles that underlie the analysis and design of digital communication systems. The subject of digital communications involves the transmission of information in digital form from a source that generates the information to one or more destinations. Of particular importance in the analysis and design of communication systems are the characteristics of the physical channels through which the information is transmitted. The characteristics of the channel generally affect the design of the basic building blocks of the communication system. Below, we describe the elements of a communication system and their functions.

1.1 Elements of a Digital Communication System

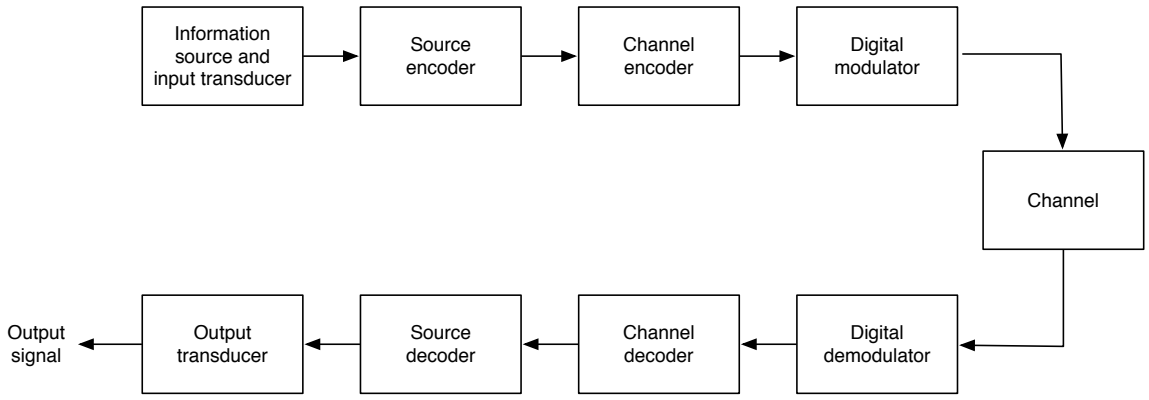

Figure 1-1: Basic elements of a digital communication system.

Figure 1-1 illustrates the functional diagram and the basic elements of a digital communication system.

- The source output may be either an analog signal, such an audio or video signal, or a digital signal, such as the output of a computer, that is discrete in time and has a finite number of output characters. In a digital communication system, the messages produced by the source are converted into a sequence of binary digits. Ideally, we should like to represent the source output (message) by as few binary digits as possible. In other words we seek an efficient of the source that results in little or no redundancy. The process of efficiently

converting the output of either an analog or digital source into a sequence of binary digits is called *source encoding* or *data compression*.

- The sequence of binary digits from the source encoder, which we call the *information sequence*, is passed to the channel encoder. The purpose of the channel encoder is to introduce, in a controlled manner, some redundancy in the binary information sequence that can be used at the receiver to overcome the effects of noise and interference encountered in the transmission of the signal through the channel. Thus the added redundancy serves to increase the reliability of the received data and improves the fidelity of the received signal. In effect, redundancy in the information sequence aids the receiver in decoding the desired information sequence. For example, a (trivial) form of encoding or the binary information sequence is simply to repeat each binary digit m times, where m is some positive integer. More sophisticated (nontrivial) encoding involves taking k information bits at time and mapping each k-bit sequence into a unique n-bit sequence, called a *code word*. The amount of redundancy introduced by encoding the data in this manner is measured by the ratio n/k. The reciprocal of this ratio, namely k/n, is called the rate of the code or, simply, the *code rate*.

- The binary sequence at the output of the channel encoder is passed to the *digital modulator*, which serves as the interface to the communication channel. Since nearly all the communication channels encountered in practice are capable or transmitting electrical signals (waveforms), the primary purpose of the digital modulator is to map the binary information sequence into signal waveforms. To elaborate on this point, let us suppose that the coded information is to be transmitted one bit at a time at some uniform rate R bits per second (bits/s). The digital modulator may simply map the binary digit 0 into a waveform $s_0(t)$ and the binary digit 1 into a waveform $s_1(t)$. In this manner, each bit from the channel encoder is transmitted separately. We call this *binary modulation*. Alternatively, the modulator may transmit b coded information bits at a time by using $M = 2^b$ distinct waveforms $s_i(t), i = 0, 1, \cdots, .M-1$, one waveform for each of the 2^b possible b-bit sequences. We call this *M-ary modulation* ($M > 2$). Note that a new b-bit sequence enters the modulator every b/R seconds. Hence, when the channel bit rate R is fixed, the amount or time available to transmit one of the M waveforms corresponding to a b-bit sequence is b times the time period in a system that uses binary modulation.

- The *communication channel* is the physical medium that is used to send the signal from the transmitter to the receiver. In wireless the channel may be the atmosphere (free space). On the other hand, telephone channels usually employ a variety of physical media, including wire lines, optical fiber cables, and wireless (microwave radio). Whatever the physical medium used for transmission of the information, the essential feature is that the transmitted signal is corrupted in a random manner by a variety of possible mechanisms, such as additive thermal noise generated by electronic devices; man-made noise, *e.g.*, automobile ignition noise; and atmospheric noise, *e.g.*, electrical lightning discharges during thunderstorms.

- At the receiving end of a digital communication system, the *digital demodulator* processes the channel-corrupted transmitted waveform and reduces the waveforms to a sequence of numbers that represent estimates of the transmitted data symbols (binary or M-ary). This sequence of numbers is passed to the channel decoder, which attempts to reconstruct the original information sequence from knowledge of the code used by the channel encoder and the redundancy contained in the received data.

A measure of how well the demodulator and decoder perform is the frequency with which errors occur in the decoded sequence. More precisely, the average probability of a bit-error at the output of the decoder is a measure of the performance of the demodulator-decoder combination. In general, the probability of error is a function of the code characteristics, the types of waveforms used to transmit the information over the channel, the transmitter power, the characteristics of the channel (*i.e.*, the amount of noise, the nature of the interference), and the method of demodulation and decoding. These items and their effect on performance will be discussed in detail in subsequent chapters.

- As a final step, when an analog output is desired, the source decoder accepts the output sequence from the channel decoder and, from knowledge of the source encoding method used, attempts to reconstruct the original signal from the source. Because of channel decoding errors and possible distortion introduced by the source encoder, and perhaps, the source decoder, the signal at the output of the source decoder is an approximation to the original source output. The difference or some function of the difference between the original signal and the reconstructed signal is a measure of the distortion introduced by the digital communication system.

1.2 Mathematical Models for Communication Channels

In the design of communication systems for transmitting information through physical channels, we find it convenient to construct mathematical models that reflect the most important characteristics of the transmission medium. Then, the mathematical model for the channel is used in the design of the channel encoder and modulator at the transmitter and the demodulator and channel decoder at the receiver. Below, we provide a brief description of the channel models that are frequently used to characterize many of the physical channels that we encounter in practice.

The Additive Noise Channel

The simplest mathematical model for a communication channel is the additive noise channel, illustrated in Figure 1-2. In this model. the transmitted signal $s(t)$ is corrupted an additive random noise process $n(t)$. Physically, the additive noise process may arise from electronic components and amplifiers at the receiver of the communication system or from interference encountered in transmission (as in the case of radio signal transmission).

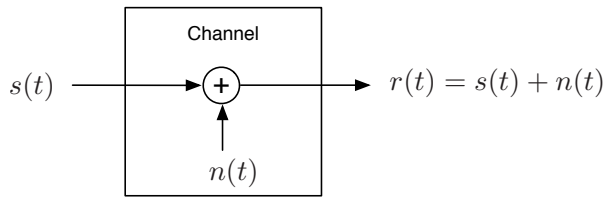

Figure 1-2: The additive noise channel.

If the noise is introduced primarily by electronic components and amplifiers at the receiver, it may be characterized as thermal noise. This type of noise is characterized statistically as a *Gaussian noise process*. Hence, the resulting mathematical model for the channel is usually called the *additive Gaussian noise channel*. Because this channel model applies to a broad class of physical communication channels and because of its mathematical tractability, this is the predominant channel model used in our communication system analysis and design. Channel attenuation is easily incorporated into the model. When the signal undergoes attenuation in transmission through the channel, the received signal is

$$r(t) = \alpha s(t) + n(t) \tag{1-1}$$

where α is the attenuation factor.

The Linear Filter Channel

In some physical channels, such as wireline telephone channels, filters are used to ensure that the transmitted signals do not exceed specified bandwidth limitations and thus do not interfere with one another. Such channels are generally characterized mathematically as linear filter channels with additive noise, as illustrated in Figure 1-3. Hence, if the channel input is the signal $s(t)$, the channel output is the signal

$$\begin{aligned} r(t) &= s(t) * c(t) + n(t) \\ &= \int_{-\infty}^{\infty} c(\tau) s(t-\tau) d\tau + n(t) \end{aligned} \tag{1-2}$$

where $c(t)$ is the impulse response of the linear filter and $*$ denotes convolution.

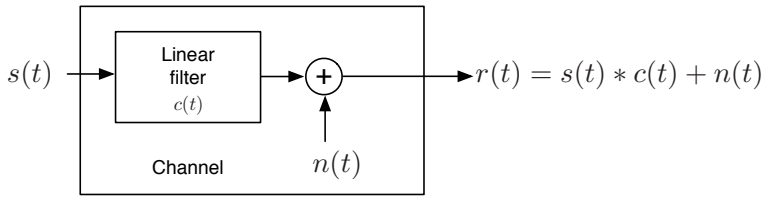

Figure 1-3: The linear filter channel with additive noise.

The Linear Time-Variant Filter Channel

Physical channels such as underwater acoustic channels and ionospheric radio channels that result in time-variant multipath propagation of the transmitted signal may be characterized mathematically as time-variant linear filters. Such linear filters are characterized by a time-variant channel impulse response $c(\tau;t)$, where $c(\tau;t)$ is the response of the channel at time t due to an impulse applied at time $t-\tau$. Thus, τ represents the "age" (elapsed-time) variable. The linear time-variant filter channel with additive noise is illustrated in Figure 1-4. For an input signal $s(t)$, the channel output signal is

$$\begin{aligned} r(t) &= s(t) * c(\tau;t) + n(t) \\ &= \int_{-\infty}^{\infty} c(\tau;t)s(t-\tau)d\tau + n(t) \end{aligned} \tag{1-3}$$

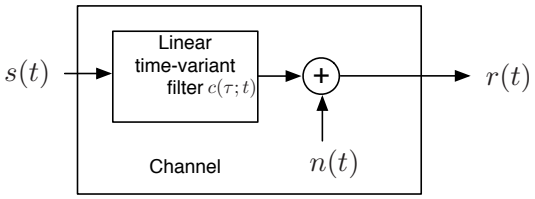

Figure 1-4: Linear time-variant filter channel with additive noise.

A good model for multipath signal propagation through physical channels, such as the ionosphere (at frequencies below 30MHz) and mobile cellular radio channels, is a special case of (1-3) in which the time-variant impulse response has the form

$$c(\tau;t) = \sum_{k=1}^{L} a_k(t)\delta(\tau - \tau_k) \tag{1-4}$$

where the $\{a_k(t)\}$ represents the possibly time-variant attenuation factors for the L multipath propagation paths and $\{\tau_k\}$ are the corresponding time delays. If (1-4) is substituted into (1-3), the received signal has the form

$$r(t) = \sum_{k=1}^{L} a_k(t)s(t-\tau_k) + n(t) \tag{1-5}$$

Hence, the received signals of L multipath components, where the kth component is attenuated by $a_k(t)$ and delayed by τ_k.

The three mathematical models described above adequately characterize the great majority of the physical channels encountered in practice. These three channel models are used in this text for the analysis and design of communication systems.

Chapter 2

Matrices and Random Processes

2.1 Matrices

A matrix is a rectangular array of real or complex numbers called the *elements of the matrix*. An $n \times m$ matrix has n rows and m columns. If $m = n$, the matrix is called a *square matrix*. An vector may be viewed as an $n \times 1$ matrix. An $n \times m$ matrix may be viewed as having m n-dimensional vectors as its rows or m n-dimensional vectors as its columns.

The complex *conjugate* and the *transpose* of a matrix $\boldsymbol{A}$ are denoted as $\boldsymbol{A}^*$ and $\boldsymbol{A}^T$, respectively. The *conjugate transpose* of a matrix with complex elements is denoted as $\boldsymbol{A}^H$; that is, $\boldsymbol{A}^H = [\boldsymbol{A}^*]^T = \left[\boldsymbol{A}^T\right]^*$.

A square matrix $\boldsymbol{A}$ is said to be *symmetric* if $\boldsymbol{A}^T = \boldsymbol{A}$. A square matrix $\boldsymbol{A}$ with complex elements is said to be *Hermitian* if $\boldsymbol{A}^H = \boldsymbol{A}$. If $\boldsymbol{A}$ is a square matrix, then $\boldsymbol{A}^{-1}$ designates the *inverse* of $\boldsymbol{A}$ (if one exists), having the property that

$$\boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{I}_n \tag{2-1}$$

where $\boldsymbol{I}_n$ is the $n \times n$ *identity* matrix, *i.e.*, a square matrix whose diagonal elements are unity and off-diagonal elements are zero. If $\boldsymbol{A}$ has no inverse, it is said to be *singular*.

The *trace* of a square matrix $\boldsymbol{A}$ is denoted as $\mathrm{tr}(\boldsymbol{A})$ and is defined as the sum of the diagonal elements, *i.e.*,

$$\mathrm{tr}(\boldsymbol{A}) = \sum_{i=1}^{n} a_{ii} \tag{2-2}$$

The *rank* of an $n \times m$ matrix $\boldsymbol{A}$ is the maximum number of linearly independent columns or rows in the matrix (it makes no difference whether we take rows or columns). A matrix is said to be of *full rank* if its rank is equal to the number of rows or columns, whichever is smaller.

The following are some additional matrix properties (lowercase letters denote vectors):

$$\begin{array}{rclcrcl} (\boldsymbol{A}\boldsymbol{v})^T &=& \boldsymbol{v}^T\boldsymbol{A}^T & & (\boldsymbol{A}\boldsymbol{B})^{-1} &=& \boldsymbol{B}^{-1}\boldsymbol{A}^{-1} \\ (\boldsymbol{A}\boldsymbol{B})^T &=& \boldsymbol{B}^T\boldsymbol{A}^T & & (\boldsymbol{A}^T)^{-1} &=& \left(\boldsymbol{A}^{-1}\right)^T \end{array} \tag{2-3}$$

Linear dependence and independence

A set of vectors $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_K\}$ in a vector space is said to be *linearly dependent* if there exist coefficients $\{a_1, \cdots, a_K\}$, not all 0, in the underlying scalar field $\mathbb{F}$ such that

$$a_1\boldsymbol{x}_1 + a_2\boldsymbol{x}_2 + \cdots + a_K\boldsymbol{x}_K = 0$$

Equivalently, one of the $\boldsymbol{x}_i$ terms is a *linear combination*, with coefficients from $\mathbb{F}$, of the others. For example

$$\left\{[1,2,3]^T, [1,0,-1]^T, [2,2,2]^T\right\}$$

is a linearly dependent set in $\mathbb{R}^3$. A subset of $\mathcal{V}$ that is not linearly dependent over $\mathbb{F}$ is said to be *linearly independent*. For example,

$$\left\{[1,2,3]^T, [1,0,-1]^T\right\}$$

is a linearly independent set in $\mathbb{R}^3$. It is important to note that both concepts intrinsically pertain to *sets* of vectors. Any subset of a linearly independent set is linearly independent; $\{\mathbf{0}\}$ is a linearly dependent set; and hence any set which includes the $\mathbf{0}$ vector is linearly dependent. It can happen that a set of vectors is linearly dependent, while any proper subset of it is linearly independent.

2.2 Eigenvalues and Eigenvectors of a Matrix

Constrained extrema and eigenvalues

Nonzero vectors $\boldsymbol{v}$ such that $\boldsymbol{A}\boldsymbol{v}$ is a multiple of $\boldsymbol{v}$ play a major role in analyzing the structure of a general matrix or linear transformation, but such vectors arise in the more elementary context of maximizing (or minimizing) a real symmetric quadratic form subject to a geometric constraint:

$$\text{Maximize } \boldsymbol{v}^T\boldsymbol{A}\boldsymbol{v},\ s.t.\ \boldsymbol{v} \in \mathbb{R}^n, \boldsymbol{v}^T\boldsymbol{v} = 1$$

in which $\boldsymbol{A}^T = \boldsymbol{A}$ is given. A conventional approach to such a constrained optimization problem is to introduce the Lagrangian

$$L = \boldsymbol{v}^T\boldsymbol{A}\boldsymbol{v} - \lambda\boldsymbol{v}^T\boldsymbol{v}$$

Necessary conditions for an extremum then are

$$\Delta L = 2(\boldsymbol{A}\boldsymbol{v} - \lambda\boldsymbol{v}) = 0$$

Thus, if a vector $\boldsymbol{v} \in \mathbb{R}^n$ with $\boldsymbol{v}^T\boldsymbol{v} = 1$ is to be an extremum of $\boldsymbol{v}^T\boldsymbol{A}\boldsymbol{v}$, it must necessarily satisfy the equation $\boldsymbol{A}\boldsymbol{v} = \lambda\boldsymbol{v}$, and hence $\boldsymbol{A}\boldsymbol{v}$ is a multiple of $\boldsymbol{v}$.

Let $\boldsymbol{A}$ be an $n \times n$ square matrix. A nonzero vector $\boldsymbol{v}$ is called an *eigenvector* of $\boldsymbol{A}$ and λ is the associated *eigenvalue* if

$$\boldsymbol{A}\boldsymbol{v} = \lambda\boldsymbol{v} \tag{2-4}$$

If $\boldsymbol{A}$ is a Hermitian $n \times n$ matrix, then there exist n mutually orthogonal eigenvectors $\boldsymbol{v}_i, i = 1, 2, \cdots, n$. Usually, we normalize each eigenvector to unit length, so that

$$\boldsymbol{v}_i^H\boldsymbol{v}_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \tag{2-5}$$

In such a case, the eigenvectors are orthonormal.

We define an $n \times n$ matrix $\boldsymbol{Q}$ whose ith column is the eigenvector $\boldsymbol{v}_i$. Then

$$\boldsymbol{Q}^H \boldsymbol{Q} = \boldsymbol{Q}\boldsymbol{Q}^H = \boldsymbol{I}_n \tag{2-6}$$

Furthermore, $\boldsymbol{A}$ may be represented (decomposed) as

$$\boldsymbol{A} = \boldsymbol{Q}\boldsymbol{\Lambda}\boldsymbol{Q}^H \tag{2-7}$$

where $\boldsymbol{\Lambda}$ is an $n \times n$ diagonal matrix with elements equal to the eigenvalues of $\boldsymbol{A}$. This decomposition is called a *spectral decomposition* of a Hermitian matrix.

If $\boldsymbol{u}$ is an $n \times 1$ nonzero vector for which $\boldsymbol{A}\boldsymbol{u} = \boldsymbol{0}$, then $\boldsymbol{u}$ is called a *null vector* of $\boldsymbol{A}$. When $\boldsymbol{A}$ is Hermitian and $\boldsymbol{A}\boldsymbol{u} = \boldsymbol{0}$ for some vector $\boldsymbol{u}$, then $\boldsymbol{A}$ is singular. A singular Hermitian matrix has at least one zero eigenvalue.

Now, consider the scalar quadratic form $\boldsymbol{u}^H \boldsymbol{A}\boldsymbol{u}$ associate with the Hermitian matrix $\boldsymbol{A}$. If $\boldsymbol{u}^H \boldsymbol{A}\boldsymbol{u} > 0$, the matrix $\boldsymbol{A}$ is said to be *positive definite*. In such a case all the eigenvalues of $\boldsymbol{A}$ are positive. On the other hand, if $\boldsymbol{u}^H \boldsymbol{A}\boldsymbol{u} \geq 0$, matrix $\boldsymbol{A}$ is said to be *positive semidefinite*. In such a case, all the eigenvalues of $\boldsymbol{A}$ are nonnegative.

The following properties involving the eigenvalues of an arbitrary $n \times n$ matrix $\boldsymbol{A} = (a_{ij})_n$ hold:

$$\sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} a_{ii} = \operatorname{tr}(\boldsymbol{A}) \tag{2-8}$$

$$\prod_{i=1}^{n} \lambda_i = \det(\boldsymbol{A}) \tag{2-9}$$

$$\sum_{i=1}^{n} \lambda_i^k = \operatorname{tr}\left(\boldsymbol{A}^k\right) \tag{2-10}$$

$$\operatorname{tr}\left(\boldsymbol{A}^T \boldsymbol{A}\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2 \geq \sum_{i=1}^{n} \lambda_i^2, \ \boldsymbol{A} \text{ real} \tag{2-11}$$

2.3 Singular-valued Decomposition

The singular-valued decomposition (SVD) is another orthogonal decomposition of a matrix. Let us assume that $\boldsymbol{A}$ is an $n \times m$ matrix of rank r. Then there exist an $n \times r$ matrix $\boldsymbol{U}$, an $m \times r$ matrix $\boldsymbol{V}$, and an $r \times r$ diagonal matrix $\boldsymbol{\Sigma}$ such that $\boldsymbol{U}^H \boldsymbol{U} = \boldsymbol{V}^H \boldsymbol{V} = \boldsymbol{I}_r$, and

$$\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H \tag{2-12}$$

where $\boldsymbol{\Sigma} = \operatorname{diag}(\sigma_1, \sigma_2, \cdots, \sigma_r)$. The r diagonal elements of $\boldsymbol{\Sigma}$ are strictly positive and are called the *singular values* of matrix $\boldsymbol{A}$. For convenience, we assume that $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r$.

The SVD of matrix $\boldsymbol{A}$ may be expressed as

$$\boldsymbol{A} = \sum_{i=1}^{r} \sigma_i \boldsymbol{u}_i \boldsymbol{v}_i^H \tag{2-13}$$

where $\boldsymbol{u}_i$ are the column vectors of $\boldsymbol{U}$, which are called the *left singular vectors* of $\boldsymbol{A}$, and $\boldsymbol{v}_i$ are the column vectors of $\boldsymbol{V}$, which are called the *right singular vectors* of $\boldsymbol{A}$.

The singular values $\{\sigma_i\}$ are the nonnegative square roots of the eigenvalues of matrix $\boldsymbol{A}^H\boldsymbol{A}$. To demonstrate this, we postmultiply Equation 2-12 by $\boldsymbol{V}$. Thus, we obtain

$$\boldsymbol{A}\boldsymbol{V} = \boldsymbol{U}\boldsymbol{\Sigma} \tag{2-14}$$

or, equivalently,

$$\boldsymbol{A}\boldsymbol{v}_i = \sigma_i\boldsymbol{u}_i,\ i = 1, 2, \cdots, r \tag{2-15}$$

Similarly, we postmultiply $\boldsymbol{A}^H = \boldsymbol{V}\boldsymbol{\Sigma}\boldsymbol{U}^H$ by $\boldsymbol{U}$. Thus, we obtain

$$\boldsymbol{A}^H\boldsymbol{U} = \boldsymbol{V}\boldsymbol{\Sigma} \tag{2-16}$$

or equivalently,

$$\boldsymbol{A}^H\boldsymbol{u}_i = \sigma\boldsymbol{u}_i,\ i = 1, 2, \cdots, r \tag{2-17}$$

Then, by premultiplying both sides of Equation 2-15 with $\boldsymbol{A}^H$ and using Equation 2-17, we obtain

$$\boldsymbol{A}^H\boldsymbol{A}\boldsymbol{v}_i = \sigma_i^2\boldsymbol{v}_i,\ i = 1, 2, \cdots, r \tag{2-18}$$

This demonstrates that the r nonzero eigenvalues of $\boldsymbol{A}^H\boldsymbol{A}$ are the squares of the singular values of $\boldsymbol{A}$, and the corresponding r eigenvectors $\boldsymbol{v}_i$ are the right singular vectors of $\boldsymbol{A}$. The remaining $m - r$ eigenvalues of $\boldsymbol{A}^H\boldsymbol{A}$ are zero. On the other hand, if we premultiply both sides of Equation 2-17 by $\boldsymbol{A}$ and use Equation 2-15, we obtain

$$\boldsymbol{A}\boldsymbol{A}^H\boldsymbol{u}_i = \sigma_i^2\boldsymbol{v}_i,\ i = 1, 2, \cdots, r \tag{2-19}$$

This demonstrates that the r nonzero eigenvalues of $\boldsymbol{A}\boldsymbol{A}^H$ are the squares of the singular values of $\boldsymbol{A}$, and the corresponding r eigenvectors $\boldsymbol{u}_i$ are the left singular vectors of $\boldsymbol{A}$. The remaining $n-r$ eigenvalues of $\boldsymbol{A}\boldsymbol{A}^H$ are zero. Hence, $\boldsymbol{A}\boldsymbol{A}^H$ and $\boldsymbol{A}^H\boldsymbol{A}$ have the same set of nonzero eigenvalues.

2.4 Matrix Norm and Condition Number

Recall that the Euclidean norm (L_2 norm) of a vector $\boldsymbol{v}$, denoted as $\|\boldsymbol{v}\|$, is defined as

$$\|\boldsymbol{v}\| = \left(\boldsymbol{v}^H\boldsymbol{v}\right)^{1/2} \tag{2-20}$$

The Euclidean norm of a matrix $\boldsymbol{A}$, denoted as $\|\boldsymbol{A}\|$, is defined as

$$\|\boldsymbol{A}\| = \max \frac{\|\boldsymbol{A}\boldsymbol{v}\|}{\|\boldsymbol{v}\|} \tag{2-21}$$

for any vector $\boldsymbol{v}$. It is easy to verify that the norm of a Hermitian matrix is equal to the largest eigenvalue.

Another useful quantity associated with a matrix $\boldsymbol{A}$ is the nonzero minimum value of $\|\boldsymbol{A}\boldsymbol{v}\|/\|\boldsymbol{v}\|$. When $\boldsymbol{A}$ is a nonsingular Hermitian matrix, this minimum value is equal to the smallest eigenvalue.

The squared Frobenius norm of an $n \times m$ matrix $\boldsymbol{A}$ is defined as

$$\|\boldsymbol{A}\|_F^2 = \mathrm{tr}\left(\boldsymbol{A}\boldsymbol{A}^H\right) = \sum_{i=1}^{n}\sum_{j=1}^{n}|a_{ij}|^2 \tag{2-22}$$

From the SVD of the matrix $\boldsymbol{A}$, it follows that

$$\|\boldsymbol{A}\|_F^2 = \sum_{i=1}^{n} \lambda_i \tag{2-23}$$

where $\{\lambda_i\}$ are the eigenvalues of $\boldsymbol{A}\boldsymbol{A}^H$.

The following are bounds on matrix norms:

$$\begin{array}{rcl} \|\boldsymbol{A}\| & > & 0,\ \boldsymbol{A} \neq \boldsymbol{0} \\ \|\boldsymbol{A}+\boldsymbol{B}\| & \leq & \|\boldsymbol{A}\| + \|\boldsymbol{B}\| \\ \|\boldsymbol{A}\boldsymbol{B}\| & \leq & \|\boldsymbol{A}\|\|\boldsymbol{B}\| \end{array} \tag{2-24}$$

The condition number of a matrix $\boldsymbol{A}$ is defined as the ratio of the maximum value to the minimum value of $\|\boldsymbol{A}\boldsymbol{v}\|/\|\boldsymbol{v}\|$. When $\boldsymbol{A}$ is Hermitian, the condition number is $\lambda_{\max}/\lambda_{\min}$, where $\lambda_{\max}$ is the largest eigenvalue and $\lambda_{\min}$ is the smallest eigenvalue of $\boldsymbol{A}$.

2.5 The Moore-Penrose Pseudoinverse

Let us consider a rectangular $n \times m$ matrix $\boldsymbol{A}$ of rank r, having an SVD as $\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H$. The Moore-Penrose pseudoinverse, denoted by $\boldsymbol{A}^+$, is an $m \times n$ matrix defined as

$$\boldsymbol{A}^+ = \boldsymbol{V}\boldsymbol{\Sigma}^{-1}\boldsymbol{U}^H \tag{2-25}$$

where $\boldsymbol{\Sigma}^{-1}$ is an $r \times r$ diagonal matrix with diagonal elements $1/\sigma_i$, $i = 1, 2, \cdots, r$. We may also express $\boldsymbol{A}^+$ as

$$\boldsymbol{A}^+ = \sum_{i=1}^{r} \frac{1}{\sigma_i} \boldsymbol{v}_i \boldsymbol{u}_i^H \tag{2-26}$$

We observe that the rank of $\boldsymbol{A}^+$ is equal to the rank of $\boldsymbol{A}$.

When the rank $r = m$ or $r = n$, the pseudoinverse $\boldsymbol{A}^+$ can be expressed as

$$\begin{array}{rcll} \boldsymbol{A}^+ & = & \boldsymbol{A}^H \left(\boldsymbol{A}\boldsymbol{A}^H\right)^{-1} & r = n \\ \boldsymbol{A}^+ & = & \left(\boldsymbol{A}^H\boldsymbol{A}\right)^{-1} \boldsymbol{A}^H & r = m \\ \boldsymbol{A}^+ & = & \boldsymbol{A}^{-1} & r = m = n \end{array} \tag{2-27}$$

These relations are equivalent to $\boldsymbol{A}\boldsymbol{A}^+ = \boldsymbol{I}_n$ and $\boldsymbol{A}^+\boldsymbol{A} = \boldsymbol{I}_m$.

2.6 Some Useful Random Variables

In subsequent chapters, we shall encounter several different types of random variables. In section we list these frequently encountered random variables, their probability density functions (PDFs), their cumulative distribution functions (CDFs), and their moments. Our main emphasis will be on the Gaussian random variable and many random variables that are derived from the Gaussian random variable.

2.6.1 The Bernoulli Random Variable

The Bernoulli random variable is a discrete binary-valued random variable taking values 1 and 0 with probabilities p and $1-p$, respectively. Therefore the probability mass function (PMF) for this random variable is given by

$$\begin{cases} \Pr\{X=1\} &= p \\ \Pr\{X=0\} &= 1-p \end{cases} \tag{2-28}$$

The mean and variance of this random variable are given by

$$\begin{cases} E\{X\} &= p \\ \mathrm{Var}\{X\} &= p(1-p) \end{cases} \tag{2-29}$$

2.6.2 The Binomial Random Variable

The binomial random variable models the sum of n independent Bernoulli random variables with common parameter p. The PMF of this random variable is given by

$$\Pr\{X=k\} = {}_kC_n p^k (1-p)^{n-k}, \quad k=0,1,\cdots,n \tag{2-30}$$

For this random variable we have

$$\begin{cases} E\{X\} &= np \\ \mathrm{Var}\{X\} &= np(1-p) \end{cases} \tag{2-31}$$

This random variable models, for instance, the number of errors when n bits are transmitted over a communication channel and the probability of error for each bit is p.

2.6.3 The Uniform Random Variable

The uniform random variable is a continuous random variable with PDF

$$p(x) = \begin{cases} \frac{1}{b-a} &= a \le x \le b \\ 0 &= \text{otherwise} \end{cases} \tag{2-32}$$

where $b > a$ and the interval $[a,b]$ is the range of the random variable. Here we have

$$\begin{cases} E\{X\} &= \frac{b-a}{2} \\ \mathrm{Var}\{X\} &= \frac{(b-a)^2}{12} \end{cases} \tag{2-33}$$

2.6.4 The Gaussian (Normal) Random Variable

The Gaussian random variable is described in terms of two parameters $\mu \in \mathbb{R}$ and $\sigma > 0$ by the PDF

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{2-34}$$

We usually use the shorthand form $\mathcal{N}(\mu, \sigma^2)$ to denote the PDF of Gaussian random variables and write $X \sim \mathcal{N}(\mu, \sigma^2)$. For this random variable

$$\begin{cases} E\{X\} &= \mu \\ \text{Var}\{X\} &= \sigma^2 \end{cases} \tag{2-35}$$

A Gaussian random variable with $\mu = 0$ and $\sigma = 1$ is called a *standard normal*. A function closely related to the Gaussian random variable is the Q function defined as

$$Q(x) = \Pr\{\mathcal{N}(0,1) > x\} = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt \tag{2-36}$$

The CDF of a Gaussian random variable is given by

$$\begin{aligned} F(x) &= \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(t-\mu)^2}{2\sigma^2}} dt \\ &= 1 - \int_{x}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(t-\mu)^2}{2\sigma^2}} dt \\ &= 1 - \int_{\frac{x-\mu}{\sigma}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}} du \\ &= 1 - Q\left(\frac{x-\mu}{\sigma}\right) \end{aligned} \tag{2-37}$$

where we have introduced the change of variable $u = (t - \mu)/\sigma$. The PDF and the CDF of a Gaussian random variable are shown in Figure 2-1.

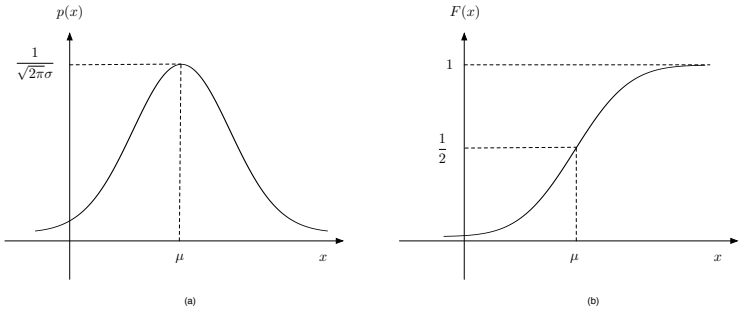

Figure 2-1: PDF and CDF of a Gaussian random variable.

In general if $X \sim \mathcal{N}(\mu, \sigma^2)$, then

$$\begin{aligned} \Pr\{X > \alpha\} &= Q\left(\frac{\alpha - \mu}{\sigma}\right) \\ \Pr\{X < \alpha\} &= Q\left(\frac{\mu - \alpha}{\sigma}\right) \end{aligned} \tag{2-38}$$

Following are some of the important properties of the Q function:

$$\begin{array}{rcl} Q(0) & = & \frac{1}{2} \\ Q(\infty) & = & 0 \\ Q(-\infty) & = & 1 \\ Q(-x) & = & 1 - Q(x) \end{array} \tag{2-39}$$

Some useful bounds for the Q function for $x > 0$ are

$$\begin{array}{rcl} Q(x) & \leq & \frac{1}{2}e^{-\frac{x^2}{2}} \\ Q(x) & \leq & \frac{1}{x\sqrt{2\pi}}e^{-\frac{x^2}{2}} \\ Q(x) & \leq & \frac{x}{(1+x^2)\sqrt{2\pi}}e^{-\frac{x^2}{2}} \end{array} \tag{2-40}$$

From the last two bounds we conclude that for large x we have

$$Q(x) \approx \frac{1}{x\sqrt{2\pi}}e^{-\frac{x^2}{2}} \tag{2-41}$$

A plot of the Q function bounds is given in Figure 2-2.

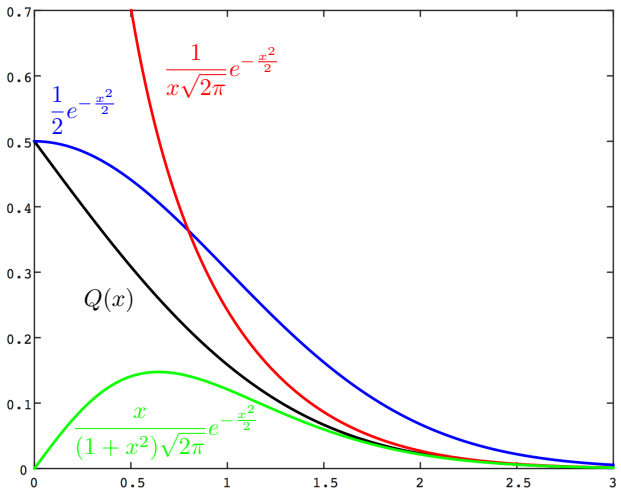

Figure 2-2: Plot of $Q(x)$ and its upper and lower bounds.

Tables 2.1 and 2.2 give values of the Q function.

Another function closely related to the Q function is the *complementary error function*, defined as

$$\text{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt \tag{2-42}$$

The complementary error function is related to the Q function as follows:

$$Q(x) = \frac{1}{2}\text{erfc}\left(\frac{x}{\sqrt{2}}\right)$$

Table 2.1: Table of Q Function Values

x	$Q(x)$	x	$Q(x)$	x	$Q(x)$	x	$Q(x)$
0	5.0000×10^{-1}	1.8	3.5930×10^{-2}	3.6	1.59×10^{-4}	5.4	3.3320×10^{-8}
0.1	4.6017×10^{-1}	1.9	2.8717×10^{-2}	3.7	1.08×10^{-4}	5.5	1.8990×10^{-8}
0.2	4.2074×10^{-1}	2	2.2750×10^{-2}	3.8	7.2348×10^{-5}	5.6	1.0718×10^{-8}
0.3	3.8209×10^{-1}	2.1	1.7864×10^{-2}	3.9	4.8096×10^{-5}	5.7	5.9904×10^{-9}
0.4	3.4458×10^{-1}	2.2	1.3903×10^{-2}	4	3.1671×10^{-5}	5.8	3.3157×10^{-9}
0.5	3.0854×10^{-1}	2.3	1.0724×10^{-2}	4.1	2.0658×10^{-5}	5.9	1.8175×10^{-9}
0.6	2.7425×10^{-1}	2.4	8.198×10^{-3}	4.2	1.3346×10^{-5}	6.0	9.8659×10^{-10}
0.7	2.4196×10^{-1}	2.5	6.210×10^{-3}	4.3	8.5399×10^{-6}	6.1	5.3034×10^{-10}
0.8	2.1186×10^{-1}	2.6	4.661×10^{-3}	4.4	5.4125×10^{-6}	6.2	2.8232×10^{-10}
0.9	1.8406×10^{-1}	2.7	3.467×10^{-3}	4.5	3.3977×10^{-6}	6.3	1.4882×10^{-10}
1.0	1.5866×10^{-1}	2.8	2.555×10^{-3}	4.6	2.1125×10^{-6}	6.4	7.7689×10^{-11}
1.1	1.3567×10^{-1}	2.9	1.866×10^{-3}	4.7	1.3008×10^{-6}	6.5	4.0160×10^{-11}
1.2	1.1507×10^{-1}	3.0	1.350×10^{-3}	4.8	7.9333×10^{-7}	6.6	2.0558×10^{-11}
1.3	9.6800×10^{-2}	3.1	9.68×10^{-4}	4.9	4.7918×10^{-7}	6.7	1.0421×10^{-11}
1.4	8.0757×10^{-2}	3.2	6.87×10^{-4}	5.0	2.8665×10^{-7}	6.8	5.2309×10^{-12}
1.5	6.6807×10^{-2}	3.3	4.83×10^{-4}	5.1	1.6983×10^{-7}	6.9	2.6001×10^{-12}
1.6	5.4799×10^{-2}	3.4	3.37×10^{-4}	5.2	9.9644×10^{-8}	7.0	1.2799×10^{-12}
1.7	4.4565×10^{-2}	3.5	2.33×10^{-4}	5.3	5.7901×10^{-8}	7.1	6.2378×10^{-13}

Table 2.2: Selected Q Function Values

$Q(x)$	x
10^{-1}	1.2816
10^{-2}	2.3263
10^{-3}	3.0902
10^{-4}	3.7190
10^{-5}	4.2649
10^{-6}	4.7534
10^{-7}	5.1993
0.5×10^{-5}	4.4172
0.25×10^{-5}	4.5648
0.667×10^{-5}	4.3545

$$\text{erfc}(x) = 2Q\left(\sqrt{2}x\right) \tag{2-43}$$

The characteristic function[1] of a Gaussian random variable is given by

$$\Phi_X(\omega) = e^{j\omega\mu - \frac{1}{2}\omega^2\sigma^2} \tag{2-44}$$

For an $\mathcal{N}(\mu, \sigma^2)$ random variable we have

$$E\left\{(X-\mu)^n\right\} = \begin{cases} 1 \times 3 \times 5 \times \cdots \times (2k-1)\sigma^{2k} = \frac{(2k)!\sigma^{2k}}{2^k k!} & \text{for } n = 2k \\ 0 & \text{for } n = 2k+1 \end{cases} \tag{2-45}$$

from which we can obtain moments of the Gaussian random variable.

The sum of n independent Gaussian random variables is a Gaussian random variable whose mean and variance are the sum of the means and the sum of the variances of the random variables, respectively.

2.6.5 The Rayleigh Random Variable

If X_1 and X_2 are two i.i.d. random variables each distributed according to $\mathcal{N}(0, \sigma^2)$, then

$$X = \sqrt{X_1^2 + X_2^2} \tag{2-46}$$

is a *Rayleigh random variable*. From our discussion of the χ^2 random variables, it is readily seen that a Rayleigh random variable the square root of a χ^2 random variable with two degrees of freedom. We can also conclude that the Rayleigh random variable is the square root of an exponential random variable as given by Equation 2.3-27. The PDF of a Rayleigh random variable is given by

$$p(x) = \begin{cases} \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}} & x > 0 \\ 0 & \text{otherwise} \end{cases} \tag{2-47}$$

and its mean and variance are

$$\begin{cases} E\{X\} = \sigma\sqrt{\frac{\pi}{2}} \\ \text{Var}\{X\} = \left(2 - \frac{\pi}{2}\right)\sigma^2 \end{cases} \tag{2-48}$$

2.6.6 Jointly Gaussian Random Variables

An $n \times 1$ column random vector $\boldsymbol{X}$ with components $\{X_i, 1 \le i \le n$ is called a *Gaussian vector*, and its components are called *jointly Gaussian random variables* or *multivariate Gaussian random variables* if the joint PDF of X_i's can be written as

$$p(\boldsymbol{x}) = \frac{1}{(2\pi)^{n/2}\left(\det \boldsymbol{C}\right)^{1/2}} e^{-\frac{1}{2}(\boldsymbol{x}-\boldsymbol{\mu})^T \boldsymbol{C}^{-1}(\boldsymbol{x}-\boldsymbol{\mu})} \tag{2-49}$$

where $\boldsymbol{\mu}$ and $\boldsymbol{C}$ are the mean vector and covariance matrix, respectively, of $\boldsymbol{X}$ and are given by

$$\begin{cases} \boldsymbol{\mu} = E\{\boldsymbol{X}\} \\ \boldsymbol{C} = E\left\{(\boldsymbol{X}-\boldsymbol{\mu})(\boldsymbol{X}-\boldsymbol{\mu})^T\right\} \end{cases} \tag{2-50}$$

[1]Recall that for any random variable X, the *characterisric function* is defined by $\Phi_X(\omega) = E\{e^{j\omega X}\}$. The *moment generating function* (MGF) is defined by $\Theta_X(t) = E\{e^{tX}\}$. Obviously, $\Theta(t) = \Phi(-jt)$ and $\Phi(\omega) = \Theta(j\omega)$.

From this definition it is clear that

$$C_{ij} = \text{Cov}\{X_i, X_j\} \tag{2-51}$$

and therefore $\boldsymbol{C}$ is a symmetric matrix. From elementary probability it is also well known that $\boldsymbol{C}$ is nonnegative definite.

In the special case of $n = 2$, we have

$$\begin{cases} \boldsymbol{\mu} &= \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix} \\ \boldsymbol{C} &= \begin{bmatrix} \sigma_1^2 & \rho\sigma_1\sigma_2 \\ \rho\sigma_1\sigma_2 & \sigma_2^2 \end{bmatrix} \end{cases} \tag{2-52}$$

where

$$\rho = \frac{\text{Cov}\{X_1, X_2\}}{\sigma_1\sigma_2}$$

is the correlation coefficient of the two random variables. In this case the PDF reduces to

$$p(x_1, x_2) = \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}} e^{-\frac{\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2 + \left(\frac{x_2-\mu_2}{\sigma_2}\right)^2 - 2\rho\left(\frac{x_1-\mu_1}{\sigma_1}\right)\left(\frac{x_2-\mu_2}{\sigma_2}\right)}{2(1-\rho^2)}} \tag{2-53}$$

where μ_1, μ_2, σ_1^2 and, σ_2^2 are means and variances of the two random variables and ρ is their correlation coefficient. Note that in the special case when $\rho = 0$ (*i.e.*, when the two random variables are uncorrelated), we have

$$p(x_1, x_2) = \mathcal{N}(\mu_1, \sigma_1^2) \times \mathcal{N}(\mu_2, \sigma_2^2)$$

This means that the two random variables are independent, and therefore for this case independence and uncorrelatedness are equivalent. This property is true for general jointly Gaussian random variables.

Another important property of jointly Gaussian random variables is that linear combinations of jointly Gaussian random variables are also jointly Gaussian. In other words, if $\boldsymbol{X}$ is a Gaussian vector, the random vector $\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{X}$, where the invertible matrix $\boldsymbol{A}$ represents a linear transformation, is also a Gaussian vector whose mean and covariance matrix are given by

$$\begin{cases} \boldsymbol{\mu}_Y &= \boldsymbol{A}\boldsymbol{\mu}_X \\ \boldsymbol{C}_Y &= \boldsymbol{A}\boldsymbol{C}_X\boldsymbol{A}^T \end{cases} \tag{2-54}$$

In summary, jointly Gaussian random variables, have the following important properties:

1. For jointly Gaussian random variables, *uncorrelated* is equivalent to *independent*.
2. Linear combinations or jointly random variables are themselves jointly Gaussian.
3. The random variables in any subset of jointly Gaussian random variables are jointly Gaussian, and any subset of random variables conditioned on random variables in any other subset is also jointly Gaussian (all joint subsets and all conditional subsets are Gaussian).

We also emphasize that any set of independent Gaussian random variables is jointly Gaussian, but this is not necessarily true for a set of dependent Gaussian random variables.

2.7 Complex Random Variables

A complex random variable $Z = X + jY$ can be considered as a pair of real random variables X and Y. Therefore, we treat a complex random variable as a two-dimensional random vector with components X and Y. The PDF of a complex random variable is defined to be the joint PDF of its real and complex parts. If X and Y are jointly Gaussian random variables, then Z is a complex Gaussian random variable. The PDF of a zero-mean complex Gaussian random variable Z with i.i.d. real and imaginary parts is given by

$$p(z) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{2-55}$$

$$= \frac{1}{2\pi\sigma^2} e^{-\frac{|z|^2}{2\sigma^2}} \tag{2-56}$$

For a complex random variable Z the mean and variance are defined by

$$E\{Z\} = E\{X\} + jE\{Y\} \tag{2-57}$$

$$\mathrm{Var}\{Z\} = E\left\{|Z|^2\right\} - |E\{Z\}|^2 = \mathrm{Var}\{X\} + \mathrm{Var}\{Y\} \tag{2-58}$$

2.7.1 Complex Random Vectors

A complex random vector is defined as $\boldsymbol{Z} = \boldsymbol{X} + j\boldsymbol{Y}$, where $\boldsymbol{X}$ and $\boldsymbol{Y}$ are real-valued random vectors of size n. We define the following real-valued matrices for a complex random vector $\boldsymbol{Z}$.

$$\boldsymbol{C_X} = E\left\{(\boldsymbol{X} - E\{\boldsymbol{X}\})(\boldsymbol{X} - E\{\boldsymbol{X}\})^T\right\} \tag{2-59}$$

$$\boldsymbol{C_Y} = E\left\{(\boldsymbol{Y} - E\{\boldsymbol{Y}\})(\boldsymbol{Y} - E\{\boldsymbol{Y}\})^T\right\} \tag{2-60}$$

$$\boldsymbol{C_{XY}} = E\left\{(\boldsymbol{X} - E\{\boldsymbol{X}\})(\boldsymbol{Y} - E\{\boldsymbol{Y}\})^T\right\} \tag{2-61}$$

$$\boldsymbol{C_{YX}} = E\left\{(\boldsymbol{Y} - E\{\boldsymbol{Y}\})(\boldsymbol{X} - E\{\boldsymbol{X}\})^T\right\} \tag{2-62}$$

Matrices $\boldsymbol{C_X}$ and $\boldsymbol{C_Y}$ are the *covariance matrices* of real random vectors $\boldsymbol{X}$ and $\boldsymbol{Y}$, respectively, and hence they are symmetric and nonnegative definite. It is clear from above that $\boldsymbol{C_{YX}} = \boldsymbol{C_{XY}^T}$.

The PDF of $\boldsymbol{Z}$ is the joint PDF of its real and imaginary parts. If we define the $2n$-dimensional real vector

$$\tilde{\boldsymbol{Z}} = \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix} \tag{2-63}$$

then the PDF of the complex vector $\boldsymbol{X}$ is the PDF of the real vector $\tilde{\boldsymbol{Z}}$. It is clear that $\boldsymbol{C}_{\tilde{\boldsymbol{Z}}}$, the covariance matrix of $\tilde{\boldsymbol{Z}}$, can be written as

$$\boldsymbol{C}_{\tilde{\boldsymbol{Z}}} = \begin{bmatrix} \boldsymbol{C_X} & \boldsymbol{C_{XY}} \\ \boldsymbol{C_{YX}} & \boldsymbol{C_Y} \end{bmatrix} \tag{2-64}$$

We also define the following two, in general complex-valued, matrices

$$\boldsymbol{C_Z} = E\left\{(\boldsymbol{Z} - E\{\boldsymbol{Z}\})(\boldsymbol{Z} - E\{\boldsymbol{Z}\})^H\right\} \tag{2-65}$$

$$\tilde{\boldsymbol{C}}_{\boldsymbol{Z}} = E\left\{(\boldsymbol{Z} - E\{\boldsymbol{Z}\})(\boldsymbol{Z} - E\{\boldsymbol{Z}\})^T\right\} \tag{2-66}$$

where $\boldsymbol{A}^T$ denotes the transpose and $\boldsymbol{A}^H$ denotes the Hermitian transpose of $\boldsymbol{A}$ ($\boldsymbol{A}$ is transposed and each element of it is conjugated). $\boldsymbol{C_Z}$ and $\tilde{\boldsymbol{C}}_{\boldsymbol{Z}}$ are called the *covariance* and the

pseudocovariance of the complex random vector $\boldsymbol{Z}$, respectively. It is easy to verify that for any $\boldsymbol{Z}$, the covariance matrix is Hermitian[2] and nonnegative definite. The pseudocovariance is skew-Hermitian.

From these definitions it is easy to verify the following relations.

$$\begin{aligned}
\boldsymbol{C_Z} &= \boldsymbol{C_X} + \boldsymbol{C_Y} + j(\boldsymbol{C_{YX}} - \boldsymbol{C_{XY}}) && (2\text{-}67)\\
\tilde{\boldsymbol{C}}_{\boldsymbol{Z}} &= \boldsymbol{C_X} - \boldsymbol{C_Y} + j(\boldsymbol{C_{YX}} + \boldsymbol{C_{XY}}) && (2\text{-}68)\\
\boldsymbol{C_X} &= \frac{1}{2}\Re\left\{\boldsymbol{C_Z} + \tilde{\boldsymbol{C}}_{\boldsymbol{Z}}\right\} && (2\text{-}69)\\
\boldsymbol{C_Y} &= \frac{1}{2}\Re\left\{\boldsymbol{C_Z} - \tilde{\boldsymbol{C}}_{\boldsymbol{Z}}\right\} && (2\text{-}70)\\
\boldsymbol{C_{YX}} &= \frac{1}{2}\Im\left\{\boldsymbol{C_Z} + \tilde{\boldsymbol{C}}_{\boldsymbol{Z}}\right\} && (2\text{-}71)\\
\boldsymbol{C_{XY}} &= \frac{1}{2}\Im\left\{\tilde{\boldsymbol{C}}_{\boldsymbol{Z}} - \boldsymbol{C_Z}\right\} && (2\text{-}72)
\end{aligned}$$

2.7.2 Proper and Circularly Symmetric Random Vectors

A complex random vector $\boldsymbol{Z}$ is called *proper* if its pseudocovariance is zero, *i.e.*, if $\tilde{\boldsymbol{C}}_{\boldsymbol{Z}} = 0$. From Equation 2-68 it is clear that for a proper random vector we have

$$\begin{aligned}
\boldsymbol{C_X} &= \boldsymbol{C_Y} && (2\text{-}73)\\
\boldsymbol{C_{XY}} &= -\boldsymbol{C_{YX}} && (2\text{-}74)
\end{aligned}$$

Substituting these results into Equations 2-67 to 2-72 and 2-64, we conclude that for proper random vectors

$$\begin{aligned}
\boldsymbol{C_Z} &= 2\boldsymbol{C_X} + 2j\boldsymbol{C_{YX}} && (2\text{-}75)\\
\boldsymbol{C_X} &= \boldsymbol{C_Y} = \frac{1}{2}\Re\{\boldsymbol{C_Z}\} && (2\text{-}76)\\
\boldsymbol{C_{YX}} &= -\boldsymbol{C_{XY}} = \frac{1}{2}\Im\{\boldsymbol{C_Z}\} && (2\text{-}77)\\
\boldsymbol{C}_{\tilde{\boldsymbol{Z}}} &= \begin{bmatrix} \boldsymbol{C_X} & \boldsymbol{C_{XY}} \\ -\boldsymbol{C_{XY}} & \boldsymbol{C_X} \end{bmatrix} && (2\text{-}78)
\end{aligned}$$

For the special case of $n = 1$, *i.e.*, when we are dealing with a single complex random variable $Z = X + jY$, the conditions for being proper become

$$\begin{aligned}
\mathrm{Var}\{X\} &= \mathrm{Var}\{Y\} && (2\text{-}79)\\
\mathrm{Cov}\{X, Y\} &= -\mathrm{Cov}\{Y, X\} && (2\text{-}80)
\end{aligned}$$

which means that Z is proper if X and Y have equal variances and are uncorrelated. In this case $\mathrm{Var}\{Z\} = 2\mathrm{Var}\{X\}$. Since in the case of jointly Gaussian random variables uncorrelated is equivalent to independent, we conclude that a complex Gaussian random variable Z is proper if and only if its real and complex parts independent with equal variance. For a zero-mean proper complex Gaussian random variable, the PDF is given by Equation 2-56.

If the complex random vector $\boldsymbol{Z} = \boldsymbol{X} + j\boldsymbol{Y}$ is Gaussian, meaning that $\boldsymbol{X}$ and $\boldsymbol{Y}$ are jointly Gaussian, then we have

$$p(\boldsymbol{z}) = p(\tilde{\boldsymbol{z}}) = \frac{1}{(2\pi)^n (\det \boldsymbol{C}_{\tilde{\boldsymbol{Z}}})^{\frac{1}{2}}} e^{-\frac{1}{2}(\tilde{\boldsymbol{z}} - \tilde{\boldsymbol{\mu}})^T \boldsymbol{C}_{\tilde{\boldsymbol{Z}}}^{-1} (\tilde{\boldsymbol{z}} - \tilde{\boldsymbol{\mu}})} \qquad (2\text{-}81)$$

[2]Matrix $\boldsymbol{A}$ is Hermitian if $\boldsymbol{A} = \boldsymbol{A}^H$. It is skew-Hermitian if $\boldsymbol{A}^H = -\boldsymbol{A}$.

where

$$\tilde{\boldsymbol{\mu}} = E\left\{\tilde{\boldsymbol{Z}}\right\} \tag{2-82}$$

It can be shown that in the special case where $\boldsymbol{Z}$ is a proper n-dimensional complex Gaussian random vector, with mean $\boldsymbol{\mu} = E\{\boldsymbol{Z}\}$ and nonsingular covariance matrix $\boldsymbol{C}_{\boldsymbol{Z}}$, its PDF can be written as

$$p(\boldsymbol{z}) = \frac{1}{\pi^n \det \boldsymbol{C}_{\tilde{\boldsymbol{Z}}}} e^{-\frac{1}{2}(\boldsymbol{z}-\boldsymbol{\mu})^T \boldsymbol{C}_{\boldsymbol{Z}}^{-1}(\boldsymbol{z}-\boldsymbol{\mu})} \tag{2-83}$$

A complex random vector $\boldsymbol{Z}$ is called *circularly symmetric* or *circular* if rotating the vector by any angle does not change its PDF. In other words, a complex random vector $\boldsymbol{Z}$ is circularly symmetric if $\boldsymbol{Z}$ and $e^{j\theta}\boldsymbol{Z}$ have the same PDF for all θ. If $\boldsymbol{Z}$ is circular, then it is zero-mean and proper, *i.e.*, $E\{\boldsymbol{Z}\} = \boldsymbol{0}$ and $E\left\{\boldsymbol{Z}\boldsymbol{Z}^T\right\} = \boldsymbol{0}$. If $\boldsymbol{Z}$ is a zero-mean proper Gaussian complex vector, then $\boldsymbol{Z}$ is circular. In other words, *for complex Gaussian random vectors being zero-mean and proper is equivalent to being circular.*

If $\boldsymbol{Z}$ is a proper complex vector, then any *affine transformation* of it, *i.e.*, any transform of the form $\boldsymbol{W} = \boldsymbol{A}\boldsymbol{Z} + \boldsymbol{b}$, is also a proper complex vector. Since we know that if $\boldsymbol{Z}$ is Gaussian, so is $\boldsymbol{W}$, we conclude that if $\boldsymbol{Z}$ is a proper Gaussian vector, so is $\boldsymbol{W}$.

Problems

Problem 2.7.1. State some matrix decomposition methods and the conditions to apply for each method.

Problem 2.7.2. Let X_I and X_Q be statistically independent zero-mean Gaussian random variables with identical variance. Show that a (rotational) transformation of the form

$$Y_I + jY_Q = (X_I + jX_Q)e^{j\phi}$$

results in another pair (Y_I, Y_Q) of Gaussian random variables that have the same joint PDF as the pair (X_I, X_Q).

Chapter 3

Optimum Receivers for AWGN Channels

In Chapter 1 we have seen that communication channels can suffer from a variety of impairments that contribute to errors. These impairments include noise, attenuation, distortion, fading, and interference. Characteristics of a communication channel deter mine which impairments apply to that particular channel and which are the determining factors in the performance of the channel. Noise is present in all communication channels and is the major impairment in many communication systems.

In particular, this chapter deals with the design and performance characteristics of optimum receivers for the various modulation methods when the channel corrupts the transmitted signal by the addition of white Gaussian noise.

3.1 Waveform and Vector Channel Models

The additive white Gaussian noise (AWGN) channel model is a channel whose sole esffect is addition of a white Gaussian noise process to the transmitted signal. This channel is mathematically described by the relation

$$r(t) = s_m(t) + n(t) \tag{3-1}$$

where $s_m(t)$ is the transmitted signal; $n(t)$ is a sample waveform of a zero-mean white Gaussian noise process with power spectral density of $N_0/2$; and $r(t)$ is the received waveform. This channel model is shown in Figure 3-1.

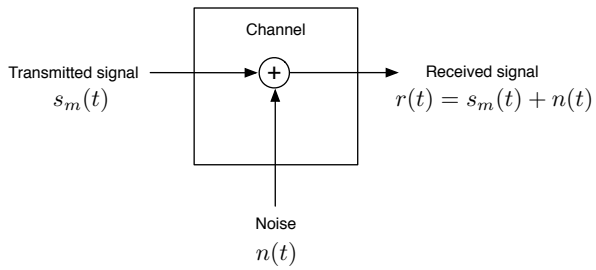

Figure 3-1: Model for received signal passed through an AWGN channel.

The receiver observes the received signal $r(t)$ and, based on this observation, makes the optimal decision about which message m, $1 \leq m \leq M$, was transmitted. By an optimal decision we mean a decision rule which results in minimum error probability, *i.e.*, the decision rule that minimizes the probability of disagreement between the transmitted message m and the detected message $\hat{m}$ given by

$$P_e = \Pr\{\hat{m} \neq m\} \tag{3-2}$$

Although the AWGN channel model seems very limiting, its study is beneficial from two points of view.

1. First, noise is the major type of corruption introduced by many channels. Therefore isolating it from other channel impairments and studying its effect results in better understanding of its effect on all communication systems.

2. Second the AWGN channel, although very simple, is a good model for studying deep space communication channels which were historically one of the first challenges encountered by communication engineers.

By using an orthonormal basis $\{\phi_j(t), 1 \leq j \leq N\}$, each signal $s_m(t)$ can be represented by a vector $\boldsymbol{s}_m \in \mathbb{R}^N$. Any orthonormal basis can be used for expansion of a zero-mean white Gaussian process, and the resulting coefficients of expansion will be *i.i.d.* zero-mean Gaussian random variables with variance $N_0/2$. Therefore, $\{\phi_j(t), 1 \leq j \leq N\}$, when extended appropriately, can be used for expansion of the noise process $n(t)$. This observation prompts us to view the waveform channel $r(t) = s_m(t) + n(t)$ in the vector form $\boldsymbol{r} = \boldsymbol{s}_m + \boldsymbol{n}$ where all vectors are N-dimensional and components of $\boldsymbol{n}$ are *i.i.d.* zero-mean Gaussian random variables with variance $N_0/2$. We will give a rigorous proof of this equivalence in Section 3.2. We continue our analysis with the study of the vector channel introduced above.

3.1.1 Optimal Detection for a General Vector Channel

The mathematical model for the AWGN vector channel is given by

$$\boldsymbol{r} = \boldsymbol{s}_m + \boldsymbol{n} \tag{3-3}$$

where all vectors are N-dimensional real vectors. The message m is chosen according to probabilities P_m, from the set of possible messages $\{1, 2, \cdots, M\}$. The noise components n_j, $1 \leq j \leq N$, are i.i.d., zero-mean, Gaussian random variables each distributed according to $\mathcal{N}(0, N_0/2)$. Therefore, the PDF of the noise vector $\boldsymbol{n}$ is given by

$$p(\boldsymbol{n}) = \left(\frac{1}{\sqrt{\pi N_0}}\right)^N e^{-\frac{\sum_{j=1}^N n_j^2}{2\sigma^2}} = \left(\frac{1}{\sqrt{\pi N_0}}\right)^N e^{-\frac{\|\boldsymbol{n}\|^2}{N_0}} \tag{3-4}$$

We, however, study a more general vector channel model in this section which is not limited to the AWGN channel model. This model will later be specialized to an AWGN channel model in Section 3.2. In our model, vectors $\boldsymbol{s}_m$ are selected from a set of possible signal vectors $\{\boldsymbol{s}_m, 1 \leq m \leq M\}$ according to prior or a priori probabilities P_m and transmitted over the channel. The received vector $\boldsymbol{r}$ depends statistically on the transmitted vector through the conditional probability density function $p(\boldsymbol{r}|\boldsymbol{s}_m)$. The channel model is shown in Figure 3-2.

The receiver observes $\boldsymbol{r}$ and based on this observation decides which message was transmitted. Let us denote the decision function employed at the receiver by $g(\boldsymbol{r})$, which is a function from $\mathbb{R}^N$ into the set of messages $\{1, 2, \cdots, M\}$. Now if $g(\boldsymbol{r}) = \hat{m}$, *i.e.*, the receiver decides that $\hat{m}$

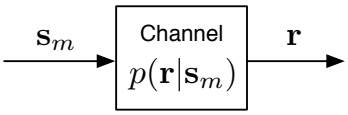

Figure 3-2: A general vector channel.

was transmitted, then the probability that this decision is correct is the probability that $\hat{m}$ was in fact the transmitted message. In other words, the probability of a correct decision, given that $\boldsymbol{r}$ is received, is given by

$$\Pr\{\text{correct decision}|\boldsymbol{r}\} = \Pr\{\hat{m} \text{ sent}|\boldsymbol{r}\} \tag{3-5}$$

and therefore the probability of a correct decision is

$$\begin{aligned} \Pr\{\text{correct decision}\} &= \int \Pr\{\text{correct decision}|\boldsymbol{r}\}\, p(\boldsymbol{r}) d\boldsymbol{r} \\ &= \int \Pr\{\hat{m} \text{ sent}|\boldsymbol{r}\}\, p(\boldsymbol{r}) d\boldsymbol{r} \end{aligned} \tag{3-6}$$

Our goal is to design an optimal detector that minimizes the error probability or, equivalently, maximizes $\Pr\{\text{correct decision}\}$. Since $p(\boldsymbol{r})$ is nonnegative for all $\boldsymbol{r}$, the right-hand side of Equation 3-6 is maximized if for each $\boldsymbol{r}$ the quantity $\Pr\{\hat{m}|\boldsymbol{r}\}$ is maximized. This means that the optimal detection rule is the one that upon observing $\boldsymbol{r}$ decides in favor of the message m that maximizes $\Pr\{m|\boldsymbol{r}\}$. In other words,

$$\hat{m} = g_{\text{opt}}(\boldsymbol{r}) = \arg\max_{1 \le m \le M} \Pr\{m|\boldsymbol{r}\} \tag{3-7}$$

The optimal detection scheme described in Equation 3-7 simply looks among all $\Pr\{m|\boldsymbol{r}\}$ for $1 \le m \le M$ and selects the m that maximizes $\Pr\{m|\boldsymbol{r}\}$. The detector then declares this maximizing m as its best decision. Note that since transmitting message m is equivalent to transmitting $\boldsymbol{s}_m$, the optimal decision rule can be written as

$$\hat{m} = g_{\text{opt}}(\boldsymbol{r}) = \arg\max_{1 \le m \le M} \Pr\{\boldsymbol{s}_m|\boldsymbol{r}\} \tag{3-8}$$

MAP and ML Receivers

The optimal decision rule given by Equations 3-7 and 3-8 is known as the maximum a posteriori probability rule, or MAP rule. Note that the MAP receiver can be simplified to

$$\hat{m} = \arg\max_{1 \le m \le M} \frac{P_m p(\boldsymbol{r}|\boldsymbol{s}_m)}{p(\boldsymbol{r})} \tag{3-9}$$

and since $p(\boldsymbol{r})$ is independent of m and for all m remains the same, this is equivalent to

$$\hat{m} = \arg\max_{1 \le m \le M} P_m p(\boldsymbol{r}|\boldsymbol{s}_m) \tag{3-10}$$

Equation 3-10 is easier to use than Equation 3-7 since it is given in terms of the prior probabilities P_m and the probabilistic description of the channel $p(\boldsymbol{r}|\boldsymbol{s}_m)$, both directly known.

In the case where the messages are equiprobable a priori, *i.e.*, when $P_m = \frac{1}{M}$ for all $1 \leq m \leq M$, the optimal detection rule reduces to

$$\hat{m} = \arg \max_{1 \leq m \leq M} p(\boldsymbol{r}|\boldsymbol{s}_m) \tag{3-11}$$

The term $p(\boldsymbol{r}|\boldsymbol{s}_m)$ is called the *likelihood of message* m, and the receiver given by Equation 3-11 is called the *maximum-likelihood receiver*, or ML receiver. It is important to note that the ML detector is not an optimal detector unless the messages are equiprobable. The ML detector, however, is a very popular detector since in many cases having exact information about message probabilities is difficult.

The Decision Regions

Any detector-including MAP and ML detectors-partitions the output space $\mathbb{R}^N$ into M regions denoted by $\mathbb{D}_1, \mathbb{D}_2, \cdots, \mathbb{D}_M$, such that if $\boldsymbol{r} \in \mathbb{D}_m$, then $\hat{m} = g(\boldsymbol{r}) = m$, *i.e.*, the detector makes a decision in favor of m. The region $\mathbb{D}_m$, $1 \leq m \leq M$ is called the decision region for message m; and $\mathbb{D}_m$ is the set of all outputs of the channel that are mapped into message m by the detector. If a MAP detector is employed, then the $\mathbb{D}_m$'s constitute the optimal decision regions resulting in the minimum possible error probability. For a MAP detector we have

$$\mathbb{D}_m = \left\{ \boldsymbol{r} \in \mathbb{R}^N | \Pr\{m|\boldsymbol{r}\} > \Pr\left\{m'|\boldsymbol{r}\right\}, \text{ for all } 1 \leq m' \leq M \text{ and } m' \neq m \right\} \tag{3-12}$$

Note that if for some given $\boldsymbol{r}$ two or more messages achieve the maximum a posteriori probability, we can arbitrarily assign $\boldsymbol{r}$ to one of the corresponding decision regions.

The Error Probability

To determine the error probability of a detection scheme, we note that when $\boldsymbol{s}_m$ is transmitted, an error occurs when the received $\boldsymbol{r}$ is not in $\mathbb{D}_m$. The symbol error probability of a receiver with decision regions $\{\mathbb{D}_m, 1 \leq m \leq M\}$ is therefore given by

$$\begin{aligned} P_e &= \sum_{m=1}^{M} P_m \Pr\{\boldsymbol{r} \notin \mathbb{D}_m | \boldsymbol{s}_m \text{ sent}\} \\ &= \sum_{m=1}^{M} P_m P_{e|m} \end{aligned} \tag{3-13}$$

where $P_{e|m}$ denotes the error probability when messege m is transmitted and is given by

$$\begin{aligned} P_{e|m} &= \int_{\mathbb{D}_m^c} p(\boldsymbol{r}|\boldsymbol{s}_m) d\boldsymbol{r} \\ &= \sum_{1 \leq m' \leq M, m' \neq m} \int_{\mathbb{D}_{m'}} p(\boldsymbol{r}|\boldsymbol{s}_m) d\boldsymbol{r} \end{aligned} \tag{3-14}$$

Using Equation 3-14 in Equation 3-13 gives

$$P_e = \sum_{m=1}^{M} P_m \sum_{1 \leq m' \leq M, m' \neq m} \int_{\mathbb{D}_{m'}} p(\boldsymbol{r}|\boldsymbol{s}_m) d\boldsymbol{r} \tag{3-15}$$

Equation 3-15 gives the probability that an error occurs in transmission of a symbol or a message and is called *symbol error probability* or *message error probability.* Another type of error

probability is the *bit error probability*. This error probability is denoted by P_b and is the error probability in transmission of a single bit. Determining the bit error probability in general requires detailed know ledge of how different bit sequences are mapped to signal points. Therefore, in general finding the bit error probabiility is not easy unless the constellation exhibits certain symmetry properties to make the derivation of the bit error probability easy. We will see later in this chapter that orthogonal signaling exhibits the required symmetry for calculation or the bit error probability. In other cases we can bound the bit error probability by noting that a symbol error occurs when at least one bit is in error, and the event of a symbol error is the union of the events of the errors in the $k = \log_2 M$ bits representing that symbol. Therefore we can write

$$P_b \leq P_e \leq kP_b \tag{3-16}$$

or

$$\frac{P_e}{\log_2 M} \leq P_e \leq P_e \tag{3-17}$$

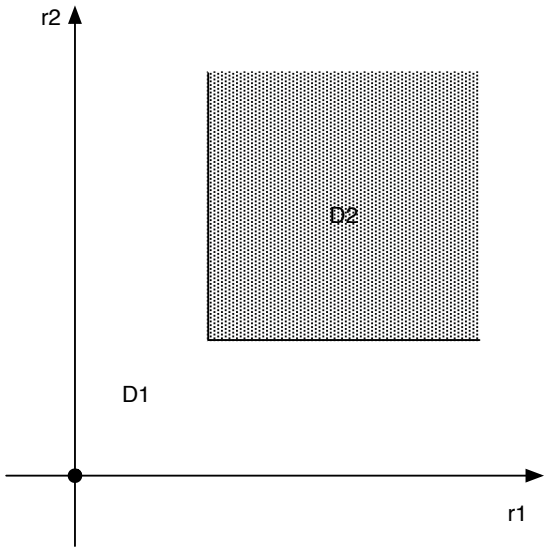

Figure 3-3: Decision regions $\mathbb{D}_1$ and $\mathbb{D}_2$.

Example 1. Consider two equiprobable message signals $\boldsymbol{s}_1 = (0, 0)$ and $\boldsymbol{s}_2 = (1, 1)$. The channel adds *i.i.d.* noise components n_1 and n_2 to the transmitted vector each with an exponential PDF of the form

$$p(n) = \begin{cases} e^{-n} & n \geq 0 \\ 0 & n < 0 \end{cases}$$

Since the messages are equiprobable, the MAP detector is equi valent to the ML detector, and the decision region $\mathbb{D}_1$ is given by

$$\mathbb{D}_1 = \{\boldsymbol{r} \in \mathbb{R}^2 : p(\boldsymbol{r}|\boldsymbol{s}_1) > p(\boldsymbol{r}|\boldsymbol{s}_2)\}$$

Noting that $p(\boldsymbol{r}|\boldsymbol{s}=(s_1,s_2))=p(\boldsymbol{n}=\boldsymbol{r}-\boldsymbol{s})$, we have

$$\mathbb{D}_1=\{\boldsymbol{r}\in\mathbb{R}^2; p_{\boldsymbol{n}}(r_1,r_2)>p_{\boldsymbol{n}}(r_1-1,r_2-1)\}$$

where

$$p_{\boldsymbol{n}}(n_1,n_2)=\begin{cases} e^{-n_1-n_2} & n_1,n_2\geq 0 \\ 0 & n<0 \end{cases}$$

From this relation we conclude that if either r_1 or r_2 is less than 1, then the point $\boldsymbol{r}$ belongs to $\mathbb{D}_1$, and if both r_1 and r_2 are greater than 1, we have $e^{-r_1-r_2}<e^{-(r_1-1)-(r_2-1)}$ and $\boldsymbol{r}$ belongs to $\mathbb{D}_2$.

Note that in this channel neither r_1 nor r_2 can be negative, because signal and noise are always nonnegative. Therefore,

$$\mathbb{D}_2=\{\boldsymbol{r}\in\mathbb{R}^2: r_1\geq 1, r_2\geq 1\}$$

and

$$\mathbb{D}_1=\{\boldsymbol{r}\in\mathbb{R}^2: r_1,r_2\geq 0, \text{ either } 0\leq r_1\leq 1 \text{ or } 0\leq r_2<1\}$$

The decision regions are shown in Figure 3-3. For this channel, when $\boldsymbol{s}_2$ is transmitted, regardless of the value of noise components, $\boldsymbol{r}$ will always be in $\mathbb{D}_2$ and no error will occur.

Errors will occur only when $\boldsymbol{s}_1=(0,0)$ is transmitted and the received vector $\boldsymbol{r}$ belongs to $\mathbb{D}_2$, *i.e.*, when both noise components exceed 1. Therefore, the error probability is given by

$$\begin{aligned} P_e &= \frac{1}{2}\Pr\{\boldsymbol{r}\in\mathbb{D}_2|\boldsymbol{s}_1=(0,0) \text{ sent}\} \\ &= \frac{1}{2}\int_1^\infty e^{-n_1}dn_1\int_1^\infty e^{-n_2}dn_2 \\ &= \frac{1}{2}e^{-2}\approx 0.0068 \end{aligned}$$

Sufficient Statistics

Let us assume that at the receiver we have access to a vector $\boldsymbol{r}$ that can be written in terms of two vectors $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$, *i.e.*, $\boldsymbol{r}=(\boldsymbol{r}_1,\boldsymbol{r}_2)$. We further assume that $\boldsymbol{s}_m$, $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ constitute a Markov chain in the given order, *i.e.*,

$$p(\boldsymbol{r}_1,\boldsymbol{r}_2|\boldsymbol{s}_m)=p(\boldsymbol{r}_1|\boldsymbol{s}_m)p(\boldsymbol{r}_2|\boldsymbol{r}_1) \tag{3-18}$$

Under these assumptions $\boldsymbol{r}_2$ can he ignored in the dctcction of $\boldsymbol{s}_m$, and the detection can be based only on $\boldsymbol{r}_1$. The reason is that by Equation 3-10

$$\begin{aligned} \hat{m} &= \arg\max_{1\leq m\leq M} P_m p(\boldsymbol{r}|\boldsymbol{s}_m) \\ &= \arg\max_{1\leq m\leq M} P_m p(\boldsymbol{r}_1,\boldsymbol{r}_2|\boldsymbol{s}_m) \end{aligned}$$

$$\begin{aligned} &= \arg\max_{1\le m\le M} P_m p(\boldsymbol{r}_1|\boldsymbol{s}_m)p(\boldsymbol{r}_2|\boldsymbol{r}_1) \\ &= \arg\max_{1\le m\le M} P_m p(\boldsymbol{r}_1|\boldsymbol{s}_m) \end{aligned} \tag{3-19}$$

where in the last step we have ignored the positive factor $p(\boldsymbol{r}_2|\boldsymbol{r}_1)$ since it does not depend on m. This shows that the optimal detection can be based only on $\boldsymbol{r}_1$.

When the Markov chain relation among $\boldsymbol{s}_m$, $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ as given in Equation 3-18 is satisfied, it is said that $\boldsymbol{r}_1$ is a *sufficient statistic* for detection of $\boldsymbol{s}_m$. In such a case, when $\boldsymbol{r}_2$ can be ignored without sacrificing the optimality of the receiver, $\boldsymbol{r}_2$ is called *irrelevant data* or *irrelevant information*. Recognizing sufficient statistics helps to reduce the complexity of the detection process through ignoring a usually large amount of irrelevant data at the receiver.

Example 2. Let us assume that in Example 1, in addition to $\boldsymbol{r}$, the receiver can observe n_1 as well. Therefore, we can assume that $\boldsymbol{r} = (\boldsymbol{r}_1, \boldsymbol{r}_2)$ is available at the receiver, where $\boldsymbol{r}_1 = (r_1, n_1)$ and $\boldsymbol{r}_2 = r_2$. To design the optimal detector, we notice that having access to both r_1 and n_1 uniquely determines $\boldsymbol{s}_{m1}$ at the receiver; and since $s_{11} = 0$ and $s_{21} = 1$, this uniquely determines the message m, thus making $\boldsymbol{r}_2 = r_2$ irrelevant. The optimal decision rule in this case becomes

$$\hat{m} = \begin{cases} 1 & \text{if } r_1 - n_1 = 0 \\ 2 & \text{if } r_1 - n_1 = 1 \end{cases} \tag{3-20}$$

and the resulting error probability is zero.

Preprocessing at the Receiver

Let us assume that the receiver applies an invertible operation $\mathscr{G}(\cdot)$(denoted as $\boldsymbol{G}(\cdot)$ in Figure 3-4) on the received vector $\boldsymbol{r}$. In other words instead of supplying $\boldsymbol{r}$ to the detector, the receiver passes $\boldsymbol{r}$ through $\mathscr{G}$ and supplies the detector with $\boldsymbol{\rho} = \mathscr{G}(\boldsymbol{r})$, as shown in Figure 3-4.

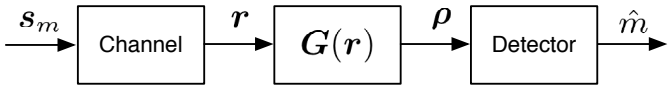

Figure 3-4: Preprocessing at the receiver.

Since $\mathscr{G}$ is invertible and the detector has access to $\boldsymbol{\rho}$, it can apply $\mathscr{G}^{-1}$ to $\boldsymbol{\rho}$ to obtain $\mathscr{G}^{-1} = \mathscr{G}^{-1}(\mathscr{G}(\boldsymbol{r})) = \boldsymbol{r}$. The detector now has access to both $\boldsymbol{\rho}$ and $\boldsymbol{r}$; therefore the optimal detection rule is

$$\begin{aligned} \hat{m} &= \arg\max_{1\le m\le M} P_m p(\boldsymbol{r}, \boldsymbol{\rho}|\boldsymbol{s}_m) \\ &= \arg\max_{1\le m\le M} P_m p(\boldsymbol{r}|\boldsymbol{s}_m)p(\boldsymbol{\rho}|\boldsymbol{r}) \\ &= \arg\max_{1\le m\le M} P_m p(\boldsymbol{r}|\boldsymbol{s}_m) \end{aligned} \tag{3-21}$$

where we have used the fact that $\boldsymbol{\rho}$ is a function of $\boldsymbol{r}$ and hence, when $\boldsymbol{r}$ is given, $\boldsymbol{\rho}$ does not depend on $\boldsymbol{s}_m$. From Equation 3-22 it is clear that the optimal detector based on the observation of $\boldsymbol{\rho}$ makes the same decision as the optimal detector based on the observation of $\boldsymbol{r}$. In other words. an invertible preprocessing of the received information does not change the optimality of the receiver.

Example 3. Let us assume the received vector is of the form

$$\boldsymbol{r} = \boldsymbol{s}_m + \boldsymbol{n}$$

where $\boldsymbol{n}$ is a nonwhite (colored) noise. Let us further assume that there exists an invertible whitening operator denoted by matrix $\boldsymbol{W}$ such that $\boldsymbol{\nu} = \boldsymbol{W}\boldsymbol{n}$ is a white vector. Then we can consider

$$\boldsymbol{\rho} = \boldsymbol{W}\boldsymbol{r} = \boldsymbol{W}\boldsymbol{s}_m + \boldsymbol{\nu}$$

which is equivalent to a channel with white noise for detection without degrading the performance. The linear operation denoted by $\boldsymbol{W}$ is called a *whitening filter*.

3.2 Waveform and Vector AWGN Channels

The waveform AWGN channel is described by the input-output relation

$$r(t) = s_m(t) + n(t) \tag{3-22}$$

where $s_m(t)$ is one of the possible M signals $\{s_1(t), s_2(t), \cdots, s_M(t)\}$, each selected with prior probability P_m and $n(t)$ is a zero-mean white Gaussian process with power spectral density $\frac{N_0}{2}$. Let us assume that using the Gram-Schmidt procedure, we have derived an orthonormal basis $\{\phi_j(t), 1 \leq j \leq N\}$ for representation of the signals and, using this set, the vector representation of the signals is given by $\{\boldsymbol{s}_m, 1 \leq m \leq M\}$. The noise process cannot be completely expanded in terms of the basis $\{\phi_j(t)\}_{j=1}^N$. We decompose the noise process $n(t)$ into two components. One component, denoted by $n_1(t)$ is part of the noise process that can be expanded in terms of $\{\phi_j(t)\}_{j=1}^N$, *i.e.*, the projection of the noise onto the space spanned by these basis functions; and the other part, denoted by $n_2(t)$, is the part that cannot be expressed in terms of this basis function. With this definition we have

$$n_1(t) = \sum_{j=1}^{N} n_j \phi_j(t), \quad n_j = \langle n(t), \phi_j(t) \rangle \tag{3-23}$$

and

$$n_2(t) = n(t) - n_1(t) \tag{3-24}$$

Noting that

$$s_m(t) = \sum_{j=1}^{N} s_{mj} \phi_j(t), \quad s_{mj} = \langle s_m(t), \phi_j(t) \rangle \tag{3-25}$$

and using Equations 3-23 and 3-24, we can write Equation 3-22 as

$$r(t) = \sum_{j=1}^{N} (s_{mj} + n_j)\phi_j(t) + n_2(t) \tag{3-26}$$

By defining

$$r_j = s_{mj} + n_j \tag{3-27}$$

where

$$r_j = \langle s_m(t), \phi_j(t) \rangle + \langle n(t), \phi_j(t) \rangle = \langle s_m(t) + n(t), \phi_j(t) \rangle = \langle r(t), \phi_j(t) \rangle \tag{3-28}$$

we have

$$r(t) = \sum_{j=1}^{N} r_j \phi_j(t) + n_2(t), \quad r_j = \langle r(t), \phi_j(t) \rangle \tag{3-29}$$

We know that n_j's are *i.i.d.* zero-mean Gaussian random variables each with variance $\frac{N_0}{2}$. This result can also be directly shown, by noting that the n_j's defined by

$$n_j = \int_{-\infty}^{\infty} n(t)\phi_j(t)dt \tag{3-30}$$

are linear combinations of the Gaussian random process $n(t)$, and therefore they are Gaussian. Their mean is given by

$$\begin{aligned} E\{n_j\} &= E\left\{\int_{-\infty}^{\infty} n(t)\phi_j(t)dt\right\} \\ &= \int_{-\infty}^{\infty} E\{n(t)\}\,\phi_j(t)dt \\ &= 0 \end{aligned} \tag{3-31}$$

where the last equality holds since $n(t)$ is zero-mean, *i.e.*, $E\{n(t)\} = 0$.

We can also find the covariance of n_i and n_j as

$$\begin{aligned} \mathrm{Cov}\{n_i n_j\} &= E\{n_i n_j\} - E\{n_i\}E\{n_j\} \\ &= E\left\{\int_{-\infty}^{\infty} n(t)\phi_i(t)dt \int_{-\infty}^{\infty} n(t)\phi_j(s)ds\right\} \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E\{n(t)n(s)\}\,\phi_i(t)\phi_j(s)dtds \\ &= \frac{N_0}{2}\int_{-\infty}^{\infty}\left[\int_{-\infty}^{\infty}\delta(s-t)\phi_i(t)dt\right]\phi_j(s)ds \\ &= \frac{N_0}{2}\int_{-\infty}^{\infty}\phi_i(s)\phi_j(s)ds \\ &= \begin{cases}\frac{N_0}{2} & i=j\\ 0 & i\neq j\end{cases} \end{aligned} \tag{3-32}$$

where we have used the facts that n_i and n_j are zero-mean, and since $n(t)$ is white, its autocorrelation function is $\frac{N_0}{2}\delta(\tau)$. In the last step we applied the orthonormality of $\{\phi_j(t)\}$. Equation 3-32 shows that for $i \neq j$, n_i and n_j are uncorrelated and since they are Gaussian, they are independent as well. It also shows that each n_j has a variance equal to $\frac{N_0}{2}$.

Now we study the properties of $n_2(t)$. We first observe that since the n_j's are jointly Gaussian random variables, the process $n_1(t)$ is a Gaussian process and thus $n_2(t) = n(t) - n_1(t)$, which is a linear combination of two jointly Gaussian processes, is itself a Gaussian process. At any given t we have

$$\begin{aligned} \mathrm{Cov}\{n_j n_2\} &= E\{n_j n_2\} \\ &= E\{n_j n\} - E\{n_j n_1\} \\ &= E\left\{n(t)\int_{-\infty}^{\infty} n(s)\phi_j(s)ds\right\} - E\left\{n_j\sum_{i=1}^{N} n_i\phi_i(t)\right\} \\ &= \frac{N_0}{2}\int_{-\infty}^{\infty}\delta(t-s)\phi_j(s)ds - \frac{N_0}{2}\phi_j(t) \\ &= \frac{N_0}{2}\phi_j(t) - \frac{N_0}{2}\phi_j(t) \\ &= 0 \end{aligned} \tag{3-33}$$

where we have used the fact that $E\{n_j n_i\} = 0$, except when $i = j$, in which case $E\{n_j n_j\} = \frac{N_0}{2}$.

Equation 3-33 shows that $n_2(t)$ is uncorrelated with all n_j's, and since they are jointly Gaussian, $n_2(t)$ is independent of all n_j's, and therefore it is independent of $n_1(t)$.

Since $n_2(t)$ is independent of $s_m(t)$ and $n_1(t)$, we conclude that in Equation 3-29, the two components of $r(t)$, namely, $\sum_j r_j\phi_j(t)$ and $n_2(t)$, are independent. Since the first component is the only component that carries the transmitted signal, and the second component is independent of the first component, the second component cannot provide any information about

the transmitted signal and therefore has no effect in the detection process and can be ignored without sacrificing the optimality of the detector. In other words $n_2(t)$ is irrelevant information for optimal detection.

From the above discussion it is clear that for the design of the optimal detector, the AWGN waveform channel of the form

$$r(t) = s_m(t) + n(t), \quad 1 \le m \le M \tag{3-34}$$

is equivalent to the N-dimensional vector channel

$$\boldsymbol{r} = \boldsymbol{s}_m(t) + \boldsymbol{n}, \quad 1 \le m \le M \tag{3-35}$$

3.2.1 Optimal Detection for the Vector AWGN Channel

The additive AWGN vector channel is the vector equivalent channel to the waveform AWGN channel and is described by Equation 3-1 in which the components of the noise vector are i.i.d. zero-mean Gaussian random variables with variance $N_0/2$. The joint PDF of the noise vector is given by Equation 3-4. The MAP detector for this channel is given by

$$\begin{aligned}
\hat{m} &= \underset{1\le m\le M}{\arg\max} \{P_m p(\boldsymbol{r}|\boldsymbol{s}_m)\} \\
&= \underset{1\le m\le M}{\arg\max} \{P_m p_{\boldsymbol{n}}(\boldsymbol{r} - \boldsymbol{s}_m)\} \\
&= \underset{1\le m\le M}{\arg\max} \left\{ P_m \left(\frac{1}{\sqrt{\pi N_0}}\right)^N e^{-\frac{\|\boldsymbol{r}-\boldsymbol{s}_m\|^2}{N_0}} \right\} \\
&\overset{(a)}{=} \underset{1\le m\le M}{\arg\max} \left\{ P_m e^{-\frac{\|\boldsymbol{r}-\boldsymbol{s}_m\|^2}{N_0}} \right\} \\
&\overset{(b)}{=} \underset{1\le m\le M}{\arg\max} \left\{ \ln P_m - \frac{\|\boldsymbol{r}-\boldsymbol{s}_m\|^2}{N_0} \right\} \\
&\overset{(c)}{=} \underset{1\le m\le M}{\arg\max} \left\{ \frac{N_0}{2} \ln P_m - \frac{1}{2}\|\boldsymbol{r}-\boldsymbol{s}_m\|^2 \right\} \\
&= \underset{1\le m\le M}{\arg\max} \left\{ \frac{N_0}{2} \ln P_m - \frac{1}{2}\left(\|\boldsymbol{r}\|^2 + \|\boldsymbol{s}_m\|^2 - 2\boldsymbol{r}\cdot\boldsymbol{s}_m\right) \right\} \\
&\overset{(d)}{=} \underset{1\le m\le M}{\arg\max} \left\{ \frac{N_0}{2} \ln P_m - \frac{1}{2}\mathcal{E}_m + \boldsymbol{r}\cdot\boldsymbol{s}_m) \right\} \\
&\overset{(e)}{=} \underset{1\le m\le M}{\arg\max} \{\eta_m + \boldsymbol{r}\cdot\boldsymbol{s}_m\}
\end{aligned} \tag{3-36}$$

where we have used the following steps in simplifying the expression:

(a) $\left(\frac{1}{\sqrt{\pi N_0}}\right)^N$ is a positive constant and can be dropped.

(b) $\ln(\cdot)$ is an increasing function.

(c) $N_0/2$ is positive and multiplying by a positive number docs not affect the result of arg max.

(d) $\|\boldsymbol{r}\|^2$ was dropped since it docs not depend on m and $\|\boldsymbol{s}_m\|^2 = \mathcal{E}_m$.

(e) We have defined

$$\eta_m = \frac{N_0}{2} \ln P_m - \frac{1}{2}\mathcal{E}_m \tag{3-37}$$

as the *basis term.*

From Equation 3-36, it is clear that the optimal (MAP) decision rule for an AWGN vector channel is given by

$$\begin{aligned} \hat{m} &= \arg\max_{1\le m\le M}\{\eta_m + \boldsymbol{r}\cdot\boldsymbol{s}_m\} \\ \eta_m &= \tfrac{N_0}{2}\ln P_m - \tfrac{1}{2}\mathcal{E}_m \end{aligned} \tag{3-38}$$

In the special case where the signal $\boldsymbol{s}$ are equiprobable, *i.e.*, $P_m = 1/M$ for all m, this relation becomes somewhat simpler. In this case Equation 3-15 at step (c) can be written as

$$\begin{aligned} \hat{m} &= \arg\max_{1\le m\le M}\left\{\frac{N_0}{2}\ln P_m - \frac{1}{2}\|\boldsymbol{r}-\boldsymbol{s}_m\|^2\right\} \\ &= \arg\max_{1\le m\le M}\left\{-\|\boldsymbol{r}-\boldsymbol{s}_m\|^2\right\} \\ &= \arg\min_{1\le m\le M}\{\|\boldsymbol{r}-\boldsymbol{s}_m\|\} \end{aligned} \tag{3-39}$$

where we have used the fact that maximizing $-\|\boldsymbol{r}-\boldsymbol{s}_m\|^2$ is equivalent to minimizing its negative, *i.e.*, $\|\boldsymbol{r}-\boldsymbol{s}_m\|^2$, which is equivalent to minimizing its square root $\|\boldsymbol{r}-\boldsymbol{s}_m\|$.

A geometric interpretation of Equation 3-39 is particularly convenient. The receiver receives $\boldsymbol{r}$ and looks among all $\boldsymbol{s}_m$ to find the one that is closest to $\boldsymbol{r}$ using standard Euclidean distance. Such a detector is called a *nearest-neighbor* or *minimum-distance*, detector. Also note that in this case, since the signals are equiprobable, the MAP and the ML detector coincide, and both are equivalent to the minimum-distance detector. In this case the boundaries of decisions $\mathbb{D}_m$ and $\mathbb{D}_{m'}$ are the set of points that are equidistant from $\boldsymbol{s}_m$ and $\boldsymbol{s}_{m'}$, which is the perpendicular bisector of the line connecting these two signal points. This boundary in general is a hyperplane. For the case of $N = 2$ the boundary is a line, and for $N = 3$ it is a plane. These hyperplanes completely determine the decision regions. An example of a two-dimensional constellation ($N = 2$) with four signal points ($M = 4$) is show n in Figure 3-5. The solid lines denote the boundaries of the decision regions which are the perpendicular bisectors of the dashed lines connecting the signal points.

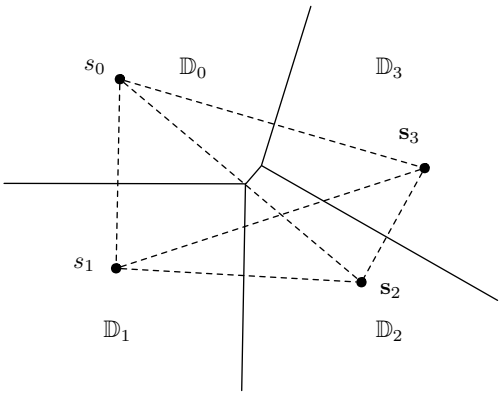

Figure 3-5: The decision regions for equiprobable signaling.

When the signals are both equiprobable and have equal energy, the bias terms defined as $\eta_m = \frac{N_0}{2}\ln P_m - \frac{1}{2}\mathcal{E}_m$ are independent of m and can be dropped from Equation 3-38. The optimal detection rule in this case reduces to

$$\hat{m} = \arg\max_{1\le m\le M}\{\boldsymbol{r}\cdot\boldsymbol{s}_m\} \tag{3-40}$$

In general, the decision region $\mathbb{D}_m$ is given as

$$\mathbb{D}_m = \left\{ \boldsymbol{r} \in \mathbb{R}^N | \boldsymbol{r} \cdot \boldsymbol{s}_m + \eta_m > \boldsymbol{r} \cdot \boldsymbol{s}_{m'} + \eta_{m'},\ \forall\ 1 \leq m' \leq M, m' \neq m \right\} \tag{3-41}$$

Note that each decision region is described in terms of at most $M-1$ inequalities. In some cases some of these inequalities are dominated by the others and are redundant. Also note that each boundary is of the general form of

$$\boldsymbol{r} \cdot (\boldsymbol{s}_m - \boldsymbol{s}_{m'}) > \eta_{m'} - \eta_m \tag{3-42}$$

which is the equation of a hyperplane. Therefore the boundaries of the decision regions in general are hyperplanes. We know that

$$\boldsymbol{r} \cdot \boldsymbol{s}_m = \int_{-\infty}^{\infty} r(t) s_m(t) dt \tag{3-43}$$

and

$$\mathcal{E}_m = \|\boldsymbol{s}\|^2 = \int_{-\infty}^{\infty} s_m^2(t) dt \tag{3-44}$$

Therefore, the optimal MAP detection rule in an AWGN channel can be written in the form

$$\hat{m} = \underset{1 \leq m \leq M}{\arg\max} \left\{ \frac{N_0}{2} \ln P_m + \int_{-\infty}^{\infty} r(t) s_m(t) dt - \frac{1}{2} \int_{-\infty}^{\infty} s_m^2(t) dt \right\} \tag{3-45}$$

and the ML Detector has the following form:

$$\hat{m} = \underset{1 \leq m \leq M}{\arg\max} \left\{ \int_{-\infty}^{\infty} r(t) s_m(t) dt - \frac{1}{2} \int_{-\infty}^{\infty} s_m^2(t) dt \right\} \tag{3-46}$$

At this point it is convenient to introduce three metrics that we will use frequently in the future. We define the *distance metric* as

$$\begin{aligned} D(\boldsymbol{r}, \boldsymbol{s}_m) &= \|\boldsymbol{r} - \boldsymbol{s}_m\|^2 \\ &= \int_{-\infty}^{\infty} \left(r(t) - s_m(t) \right)^2 dt \end{aligned} \tag{3-47}$$

denoting the square of the Euclidean distance between $\boldsymbol{r}$ and $\boldsymbol{s}_m$. The *modified distance metric* is defined as

$$D'(\boldsymbol{r}, \boldsymbol{s}_m) = -2\boldsymbol{r} \cdot \boldsymbol{s}_m + \|\boldsymbol{s}_m\|^2 \tag{3-48}$$

and is equal to the distance metric when the term $\|\boldsymbol{r}\|^2$, which does not depend on m, is removed. The *correlation metric* is defined as the negative of the modified distance metric and is given by

$$\begin{aligned} C(\boldsymbol{r}, \boldsymbol{s}_m) &= -2\boldsymbol{r} \cdot \boldsymbol{s}_m + \|\boldsymbol{s}_m\|^2 \\ &= 2 \int_{-\infty}^{\infty} r(t) s_m(t) dt - \int_{-\infty}^{\infty} s_m^2(t) dt \end{aligned} \tag{3-49}$$

It is important to note that using the term *metric* is just for convenience. In general, none of these quantities is a metric in a mathematical sense. With these definitions the optimal detection rule (MAP rule) in general can be written as

$$\begin{aligned} \hat{m} &= \underset{1 \leq m \leq M}{\arg\max} \left\{ N_0 \ln P_m - D(\boldsymbol{r}, \boldsymbol{s}_m) \right\} \\ &= \underset{1 \leq m \leq M}{\arg\max} \left\{ N_0 \ln P_m + C(\boldsymbol{r}, \boldsymbol{s}_m) \right\} \end{aligned} \tag{3-50}$$

and the ML detection rule becomes

$$\hat{m} = \underset{1 \leq m \leq M}{\arg\max} \left\{ C(\boldsymbol{r}, \boldsymbol{s}_m) \right\} \tag{3-51}$$

Optimal Detection for Binary Antipodal Signaling

In a binary antipodal signaling scheme $s_1(t) = s(t)$ and $s_2(t) = -s(t)$. The probabilities of messages 1 and 2 are p and $1-p$, respectively. This is obviously a case with $N = 1$, and the vector representations of the two signals are just scalars with $s_1 = \sqrt{\mathcal{E}_s}$ and $s_2 = -\sqrt{\mathcal{E}_s}$, where $\mathcal{E}_s$ is energy in each signal and is equal to $\mathcal{E}_b$. Following Equation 3-41, the decision region $\mathbb{D}_1$ is given as

$$\begin{aligned}\mathbb{D}_1 &= \left\{ r \,\middle|\, r\sqrt{\mathcal{E}_b} + \frac{N_0}{2}\ln p - \frac{1}{2}\mathcal{E}_b > -r\sqrt{\mathcal{E}_b} + \frac{N_0}{2}\ln(1-p) - \frac{1}{2}\mathcal{E}_b \right\} \\ &= \left\{ r \,\middle|\, r > \frac{N_0}{4\sqrt{\mathcal{E}_b}} \ln\frac{1-p}{p} \right\} \\ &= \{ r \,|\, r > r_{\text{th}} \} \end{aligned} \tag{3-52}$$

where the threshold r_{th} is defined as

$$r_{\text{th}} = \frac{N_0}{4\sqrt{\mathcal{E}_b}} \ln\frac{1-p}{p} \tag{3-53}$$

The constellation and teh decision regions are shown in Figure 3-6.

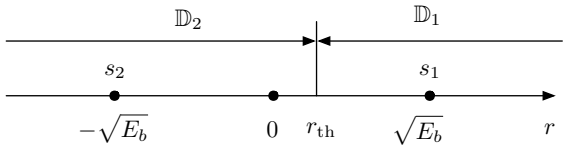

Figure 3-6: The decision regions for antipodal signaling.

Note that as $p \to 0$, we have $r_{\text{th}} \to \infty$ and the entire real line becomes $\mathbb{D}_2$; and when $p \to 1$, the entire line becomes $\mathbb{D}_1$, as expected. Also note that when $p = \frac{1}{2}$, *i.e.*, when the messages are equiprobable, $r_{\text{th}} = 0$ and the decvision rule reduces to a minimum-distance rule. To derive the error probability for this system, we use Equation 3-15. This yields

$$\begin{aligned} P_e &= \sum_{m=1}^{2} P_m \sum_{1\le m'\le 2 | m'\ne m} \int_{\mathbb{D}_{m'}} p(\boldsymbol{r}|\boldsymbol{s}_m)d\boldsymbol{r} \\ &= p\int_{\mathbb{D}_2} p\left(r \,\middle|\, s = \sqrt{\mathcal{E}_b}\right) dr + (1-p)\int_{\mathbb{D}_1} p\left(r \,\middle|\, s = -\sqrt{\mathcal{E}_b}\right) dr \\ &= p\int_{-\infty}^{r_{\text{th}}} p\left(r \,\middle|\, s = \sqrt{\mathcal{E}_b}\right) dr + (1-p)\int_{r_{\text{th}}}^{\infty} p\left(r \,\middle|\, s = -\sqrt{\mathcal{E}_b}\right) dr \\ &= p\Pr\left\{\mathcal{N}\left(\sqrt{\mathcal{E}_b}, \frac{N_0}{2}\right) < r_{\text{th}}\right\} + (1-p)\Pr\left\{\mathcal{N}\left(-\sqrt{\mathcal{E}_b}, \frac{N_0}{2}\right) > r_{\text{th}}\right\} \\ &= pQ\left(\frac{\sqrt{\mathcal{E}_b} - r_{\text{th}}}{\sqrt{\frac{N_0}{2}}}\right) + (1-p)Q\left(\frac{\sqrt{\mathcal{E}_b} + r_{\text{th}}}{\sqrt{\frac{N_0}{2}}}\right) \end{aligned} \tag{3-54}$$

where in the last step we have used Equation 2-38. In the special case where $p = \frac{1}{2}$, we have $r_{\text{th}} = 0$ and the error probability simplifies to

$$P_e = Q\left(\sqrt{\frac{2\mathcal{E}_b}{N_0}}\right) \tag{3-55}$$

Also note that since the system is binary, the error probability for each message is equal to the bit error probability, *i.e.*, $P_b = P_e$.

Error Probability for Equiprobable Binary Signaling Scheme

In this case the transmitter transmits one or the two equiprobable signals $s_1(t)$ and $s_2(t)$ over the AWGN channel. Since the signals are equiprobable, the two decision regions are separated by the perpendicular bisector of the line connecting $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$. By symmetry, error probabilities when $\boldsymbol{s}_1$ or $\boldsymbol{s}_2$ is transmitted are equal, therefore $P_b = \Pr\{\text{error}|\boldsymbol{s}_1 \text{ sent}\}$. The decision regions and the perpendicular bisector of the line connecting $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ are shown in Figure 3-7.

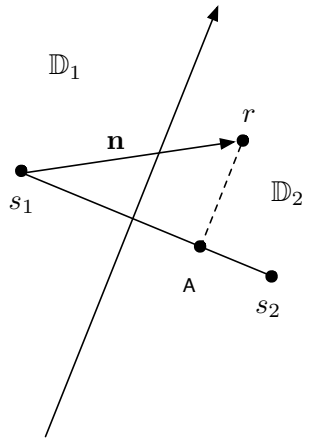

Figure 3-7: Decision regions for binary equiprobable signals.

Since we are assuming that $\boldsymbol{s}_1$ is sent, an error occurs if $\boldsymbol{r}$ is in $\mathbb{D}_2$, which means the distance between the projection of $\boldsymbol{r} - \boldsymbol{s}_1$ on $\boldsymbol{s}_2 - \boldsymbol{s}_1$, *i.e.*, point A, from $\boldsymbol{s}_1$ is larger than $\frac{d_{12}}{2}$, where $d_{12} = \|\boldsymbol{s}_2 - \boldsymbol{s}_1\|$. Note that since $\boldsymbol{s}_1$ is sent, $\boldsymbol{n} = \boldsymbol{r} - \boldsymbol{s}_1$, and the projection of $\boldsymbol{r} - \boldsymbol{s}_1$ on $\boldsymbol{s}_2 - \boldsymbol{s}_1$ becomes equal to $\frac{\boldsymbol{n}\cdot(\boldsymbol{s}_2-\boldsymbol{s}_1)}{d_{12}}$. Therefore, the error probability is given by

$$P_b = \Pr\left\{\frac{\boldsymbol{n}\cdot(\boldsymbol{s}_2-\boldsymbol{s}_1)}{d_{12}} > \frac{d_{12}}{2}\right\} \tag{3-56}$$

or

$$P_b = \Pr\left\{\boldsymbol{n}\cdot(\boldsymbol{s}_2-\boldsymbol{s}_1) > \frac{d_{12}^2}{2}\right\} \tag{3-57}$$

We note that $\boldsymbol{n}\cdot(\boldsymbol{s}_2-\boldsymbol{s}_1)$ is a zero-mean Gaussaan random variable with rariance $\frac{d_{12}^2 N_0}{2}$; therefore, using Equation 2-38, we obtain

$$\begin{aligned} P_b &= Q\left(\frac{\frac{d_{12}^2}{2}}{d_{12}\sqrt{\frac{N_0}{2}}}\right) \\ &= Q\left(\sqrt{\frac{d_{12}^2}{2N_0}}\right) \end{aligned} \tag{3-58}$$

Equation 3-58 is very general and applies to all binary equiprobable signaling systems regardless of the shape of the signals. Since $Q(\cdot)$ is a decreasing function, in order to minimize the error probability, the distance between signal points has to be maximized. The distance d_{12} is obtained from

$$d_{12}^2 = \int_{-\infty}^{\infty}(s_1(t) - s_2(t))^2 dt \tag{3-59}$$

In the special case that the binary signals are equiprobable and have equal energy, *i.e.*, when $\mathcal{E}_{s_1} = \mathcal{E}_{s_2} = \mathcal{E}$, we can expand Equation 3-59 and get

$$d_{12}^2 = \mathcal{E}_{s_1} + \mathcal{E}_{s_2} - 2\langle s_1(t), s_2(t)\rangle = 2\mathcal{E}(1-\rho) \tag{3-60}$$

where ρ is the cross-correlation coefficient between $s_1(t)$ and $s_2(t)$. Since $-1 \leq \rho \leq 1$, we observe from Equation 3-60 that the binary signals are maximally separated when $\rho = -1$, *i.e.*, when the signals are antipodal. In this case the error prohahility of the system is minimized.

Optimal Detection for Binary Orthogonal Signaling

For binary orthogonal signals we have

$$\int_{-\infty}^{\infty} s_i(t)s_j(t)dt = \begin{cases} \mathcal{E}; & i = j \\ 0; & i \neq j \end{cases} \quad 1 \leq i, j \leq 2 \tag{3-61}$$

Note that since the system is binary, $\mathcal{E}_b = E$. Here we choose $\phi_j(t) = \frac{s_j(t)}{\sqrt{\mathcal{E}_b}}$ for $j = 1, 2$, and the vector representations of the signal set become

$$\begin{aligned} \boldsymbol{s}_1 &= (\sqrt{\mathcal{E}_b}, 0) \\ \boldsymbol{s}_2 &= (0, \sqrt{\mathcal{E}_b}) \end{aligned} \tag{3-62}$$

The constellation and the optimal decision regions for the case of equiprohahlc signals are shown in Figure 3-8.

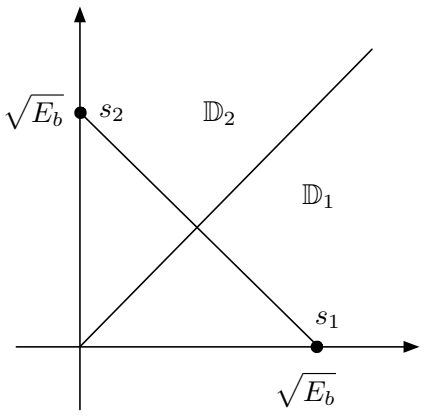

Figure 3-8: Signal constellation and decision regions for equiprobable binary orthogonal signaling.

For this signaling scheme it is clear that $d = \sqrt{2\mathcal{E}_b}$ and

$$P_b = Q\left(\sqrt{\frac{d^2}{2N_0}}\right) = Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right) \tag{3-63}$$

Comparing this result with the error probability of binary antipodal signaling given in Equation 3-55, we see that a binary orthogonal signaling requires twice the energy per bit of a binary antipodal signaling system to provide the same error probability. Therefore in terms of power efficiency, binary orthogonal signaling underperforms binary antipodal signaling by a factor of 2, or equivalently by 3 dB.

The term

$$\gamma_b = \frac{\mathcal{E}_b}{N_0} \tag{3-64}$$

which appears in the expression for error probability of many signaling systems is called the *signal-to-noise ratio per bit*, or *SNR per bit*, or simply the *SNR* of the communication system. Plots of error probability as a function of SNR/bit for binary antipodal and binary orthogonal signaling are shown in Figure 3-9. It is clear from this figure that the plot for orthogonal signaling is the result of a 3-dB shift of the plot for antipodal signaling.

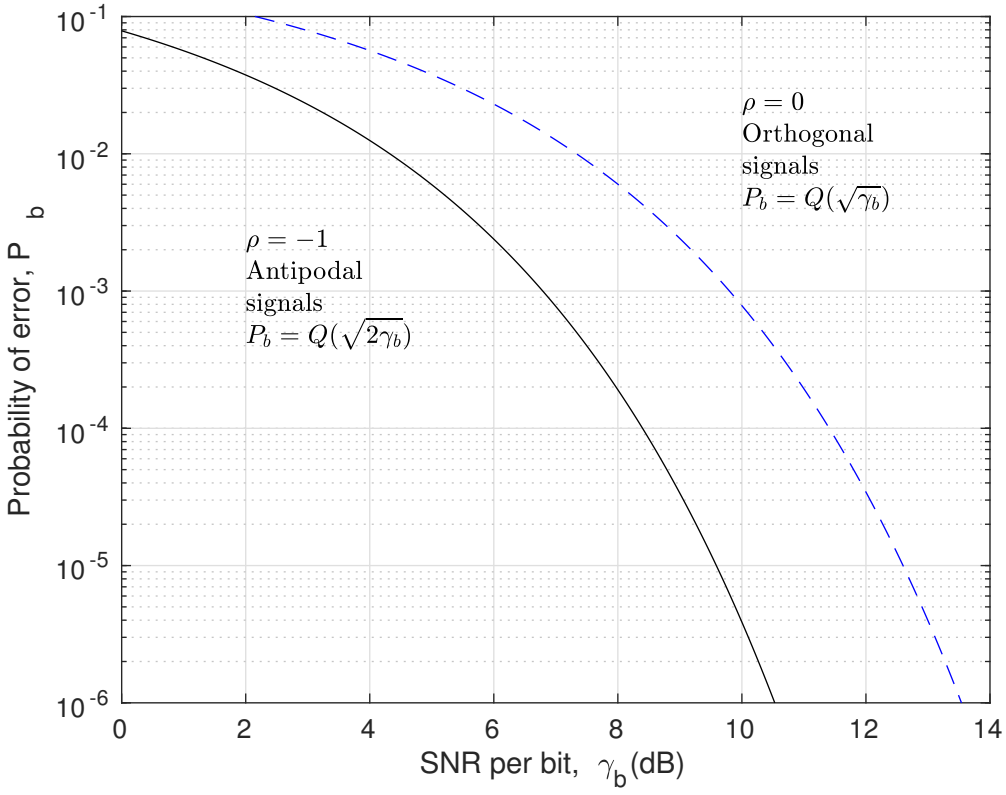

Figure 3-9: Error probability for binary antipodal and binary orthogonal signaling.