PRINCIPLES OF SPREAD-SPECTRUM COMMUNICATION SYSTEMS

PRINCIPLES OF SPREAD-SPECTRUM COMMUNICATION SYSTEMS

By

DON TORRIERI

Springer

eBook ISBN: 0-387-22783-0
Print ISBN: 0-387-22782-2

Created in the United States of America

Visit Springer's eBookstore at: http://ebooks.springerlink.com
and the Springer Global Website Online at: http://www.springeronline.com

To My Family

Contents

Preface

The goal of this book is to provide a concise but lucid explanation and derivation of the fundamentals of spread-spectrum communication systems. Although spread-spectrum communication is a staple topic in textbooks on digital communication, its treatment is usually cursory, and the subject warrants a more intensive exposition. Originally adopted in military networks as a means of ensuring secure communication when confronted with the threats of jamming and interception, spread-spectrum systems are now the core of commercial applications such as mobile cellular and satellite communication. The level of presentation in this book is suitable for graduate students with a prior graduate-level course in digital communication and for practicing engineers with a solid background in the theory of digital communication. As the title indicates, this book stresses principles rather than specific current or planned systems, which are described in many other books. Although the exposition emphasizes theoretical principles, the choice of specific topics is tempered by my judgment of their practical significance and interest to both researchers and system designers. Throughout the book, learning is facilitated by many new or streamlined derivations of the classical theory. Problems at the end of each chapter are intended to assist readers in consolidating their knowledge and to provide practice in analytical techniques. The book is largely self-contained mathematically because of the four appendices, which give detailed derivations of mathematical results used in the main text.

In writing this book, I have relied heavily on notes and documents prepared and the perspectives gained during my work at the US Army Research Laboratory. Many colleagues contributed indirectly to this effort. I am grateful to my wife, Nancy, who provided me not only with her usual unwavering support but also with extensive editorial assistance.

Chapter 1

Channel Codes

Channel codes are vital in fully exploiting the potential capabilities of spread-spectrum communication systems. Although direct-sequence systems greatly suppress interference, practical systems require channel codes to deal with the residual interference and channel impairments such as fading. Frequency-hopping systems are designed to avoid interference, but the hopping into an unfavorable spectral region usually requires a channel code to maintain adequate performance. In this chapter, some of the fundamental results of coding theory [1], [2], [3], [4] are reviewed and then used to derive the corresponding receiver computations and the error probabilities of the decoded information bits.

1.1 Block Codes

A *channel code* for forward error control or error correction is a set of *codewords* that are used to improve communication reliability. An (n, k) *block code* uses a codeword of n code symbols to represent k information symbols. Each symbol is selected from an alphabet of q symbols, and there are q^k codewords. If $q = 2^m$, then an (n, k) code of q-ary symbols is equivalent to an (mn, mk) binary code. A block encoder can be implemented by using logic elements or memory to map a k-symbol information word into an n-symbol codeword. After the waveform representing a codeword is received and demodulated, the decoder uses the demodulator output to determine the information symbols corresponding to the codeword. If the demodulator produces a sequence of discrete symbols and the decoding is based on these symbols, the demodulator is said to make *hard decisions.* Conversely, if the demodulator produces analog or multilevel quantized samples of the waveform, the demodulator is said to make *soft decisions.* The advantage of soft decisions is that reliability or quality information is provided to the decoder, which can use this information to improve its performance.

The number of symbol positions in which the symbol of one sequence differs from the corresponding symbol of another equal-length sequence is called the *Hamming distance* between the sequences. The minimum Hamming distance

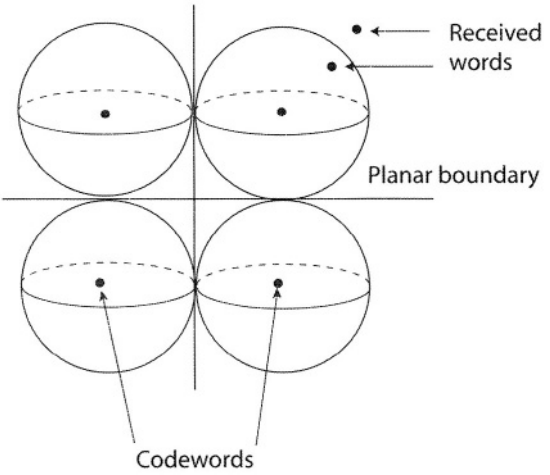

Figure 1.1: Conceptual representation of n-dimensional vector space of sequences.

between any two codewords is called the *minimum distance* of the code. When hard decisions are made, the demodulator output sequence is called the *received sequence* or the *received word.* Hard decisions imply that the overall channel between the output and the decoder input is the classical binary symmetric channel. If the channel symbol error probability is less than one-half, then the maximum-likelihood criterion implies that the correct codeword is the one that is the smallest Hamming distance from the received word. A *complete decoder* is a device that implements the maximum-likelihood criterion. An *incomplete decoder* does not attempt to correct all received words.

The n-dimensional vector space of sequences is conceptually represented as a three-dimensional space in Figure 1.1. Each codeword occupies the center of a *decoding sphere* with radius t in Hamming distance, where t is a positive integer. A complete decoder has decision regions defined by planar boundaries surrounding each codeword. A received word is assumed to be a corrupted version of the codeword enclosed by the boundaries. A *bounded-distance decoder* is an incomplete decoder that attempts to correct symbol errors in a received word if it lies within one of the decoding spheres. Since unambiguous decoding requires that none of the spheres may intersect, the maximum number of random errors that can be corrected by a bounded-distance decoder is

$$t = \lfloor (d_m - 1)/2 \rfloor \tag{1-1}$$

where d_m is the minimum Hamming distance between codewords and $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. When more than t errors occur, the received word may lie within a decoding sphere surrounding an incorrect codeword or it may lie in the interstices (regions) outside the decoding spheres. If the received word lies within a decoding sphere, the decoder selects the in-

correct codeword at the center of the sphere and produces an output word of information symbols with undetected errors. If the received word lies in the interstices, the decoder cannot correct the errors, but recognizes their existence. Thus, the decoder fails to decode the received word.

Since there are $\binom{n}{i}(q-1)^i$ words at exactly distance i from the center of the sphere, the number of words in a decoding sphere of radius t is determined from elementary combinatorics to be

$$V = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \tag{1-2}$$

Since a block code has q^k codewords, $q^k V$ words are enclosed in some sphere. The number of possible received words is $q^n \geq q^k V$, which yields

$$q^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \tag{1-3}$$

This inequality implies an upper bound on t and, hence, d_m. The upper bound on d_m is called the *Hamming bound.*

A block code is called a *linear block code* if its codewords form a k-dimensional subspace of the vector space of sequences with n symbols. Thus, the vector sum of two codewords or the vector difference between them is a codeword. If a binary block code is linear, the symbols of a codeword are modulo-two sums of information bits. Since a linear block code is a subspace of a vector space, it must contain the additive identity. Thus, the all-zero sequence is always a codeword in any linear block code. Since nearly all practical block codes are linear, henceforth block codes are assumed to be linear.

A *cyclic code* is a linear block code in which a cyclic shift of the symbols of a codeword produces another codeword. This characteristic allows the implementation of encoders and decoders that use linear feedback shift registers. Relatively simple encoding and hard-decision decoding techniques are known for cyclic codes belonging to the class of *Bose-Chaudhuri-Hocquenghem* (BCH) *codes,* which may be binary or nonbinary. A BCH code has a length that is a divisor of $q^m - 1$, where $m \geq 2$, and is designed to have an error-correction capability of $t = \lfloor (\delta - 1)/2 \rfloor$, where δ is the *design distance.* Although the minimum distance may exceed the design distance, the standard BCH decoding algorithms cannot correct more than t errors. The parameters (n, k, t) for binary BCH codes with $7 \leq n \leq 127$ are listed in Table 1.1.

A *perfect code* is a block code such that every n-symbol sequence is at a distance of at most t from some n-symbol codeword, and the sets of all sequences at distance t or less from each codeword are disjoint. Thus, the Hamming bound is satisfied with equality, and a complete decoder is also a bounded-distance decoder. The only perfect codes are the binary repetition codes of odd length, the Hamming codes, the binary Golay (23,12) code, and the ternary Golay (11,6) code. *Repetition codes* represent each information bit by n binary code symbols. When n is odd, the $(n, 1)$ repetition code is a perfect code with

Table 1.1: Binary BCH codes.

n	k	t	D_p	n	k	t	D_p	n	k	t	D_p
7	4	1	1	63	45	3	0.1592	127	92	5	0.0077
7	1	3	1	63	39	4	0.0380	127	85	6	0.0012
15	11	1	1	63	36	5	0.0571	127	78	7	$1.68 \cdot 10^{-4}$
15	7	2	0.4727	63	30	6	0.0088	127	71	9	$2.66 \cdot 10^{-4}$
15	5	3	0.5625	63	24	7	0.0011	127	64	10	$2.48 \cdot 10^{-5}$
15	1	7	1	63	18	10	0.0044	127	57	11	$2.08 \cdot 10^{-6}$
31	26	1	1	63	16	11	0.0055	127	50	13	$1.42 \cdot 10^{-6}$
31	21	2	0.4854	63	10	13	0.0015	127	43	14	$9.11 \cdot 10^{-8}$
31	16	3	0.1523	63	7	15	0.0024	127	36	15	$5.42 \cdot 10^{-9}$
31	11	5	0.1968	63	1	31	1	127	29	21	$2.01 \cdot 10^{-6}$
31	6	7	0.1065	127	120	1	1	127	22	23	$3.56 \cdot 10^{-7}$
31	1	15	1	127	113	2	0.4962	127	15	27	$7.75 \cdot 10^{-7}$
63	57	1	1	127	106	3	0.1628	127	8	31	$8.10 \cdot 10^{-7}$
63	51	2	0.4924	127	99	4	0.0398	127	1	63	1

Table 1.2: Code words of Hamming (7,4) code.

0000000	0001011	0010110	0011101
0100111	0101100	0110001	0111010
1000101	1001110	1010011	1011000
1100010	1101001	1110100	1111111

$d_m = n$ and $t = (n-1)/2$. A hard-decision decoder makes a decision based on the state of the majority of the demodulated symbols. Although repetition codes are not efficient for the additive-white-Gaussian-noise (AWGN) channel, they can improve the system performance for fading channels if the number of repetitions is properly chosen. A *Hamming* (n, k) *code* is a perfect BCH code with $d_m = 3$ and

$$n = \frac{q^{n-k} - 1}{q - 1} \tag{1-4}$$

Since $t = 1$, a Hamming code is capable of correcting all single errors. Binary Hamming codes with $n \leq 127$ are found in Table 1.1. The 16 codewords of a Hamming (7,4) code are listed in Table 1.2. The first four bits of each codeword are the information bits. The *Golay* (23,12) *code* is a binary cyclic code that is a perfect code with $d_m = 7$ and $t = 3$.

Any (n, k) linear block code with an odd value of d_m can be converted into an $(n+1, k)$ *extended code* by adding a parity symbol. The advantage of the extended code stems from the fact that the minimum distance of the block code is increased by one, which improves the performance, but the decoding complexity and code rate are usually changed insignificantly. The *extended Golay* (24,12) *code* is formed by adding an overall parity symbol to the Golay (23,12) code, thereby increasing the minimum distance to $d_m = 8$. As a result, some received sequences with four errors can be corrected with a complete decoder. The (24,12) code is often preferable to the (23,12) code because the *code rate,* which is defined as the ratio k/n, is exactly one-half, which simplifies

the system timing.

The *Hamming weight* of a codeword is the number of nonzero symbols in a codeword. For a linear block code, the vector difference between two codewords is another codeword with weight equal to the distance between the two original codewords. By subtracting the codeword **c** to all the codewords, we find that the set of Hamming distances from any codeword **c** is the same as the set of codeword weights. Consequently, in evaluating decoding error probabilities, one can assume without loss of generality that the all-zero codeword was transmitted, and the minimum Hamming distance is equal to the minimum weight of the nonzero codewords. For binary block codes, the Hamming weight is the number of 1's in a codeword.

A *systematic block code* is a code in which the information symbols appear unchanged in the codeword, which also has additional parity symbols. In terms of the word error probability for hard-decision decoding, every linear code is equivalent to a systematic linear code [1]. Therefore, systematic block codes are the standard choice and are assumed henceforth. Some systematic codewords have only one nonzero information symbol. Since there are at most $n-k$ parity symbols, these codewords have Hamming weights that cannot exceed $n-k+1$. Since the minimum distance of the code is equal to the minimum codeword weight,

$$d_m \leq n - k + 1 \tag{1-5}$$

This upper bound is called the *Singleton bound.* A linear block code with a minimum distance equal to the Singleton bound is called a *maximum-distance-separable code*

Nonbinary block codes can accommodate high data rates efficiently because decoding operations are performed at the symbol rate rather than the higher information-bit rate. *Reed-Solomon codes* are nonbinary BCH codes with $n = q-1$ and are maximum-distance-separable codes with $d_m = n-k+1$. For convenience in implementation, q is usually chosen so that $q = 2^m$, where m is the number of bits per symbol. Thus, $n = 2^m - 1$ and the code provides correction of 2^m-ary symbols. Most Reed-Solomon decoders are bounded-distance decoders with $t = \lfloor (d_m - 1)/2 \rfloor$.

The most important single determinant of the code performance is its *weight distribution,* which is a list or function that gives the number of codewords with each possible weight. The weight distributions of the Golay codes are listed in Table 1.3. Analytical expressions for the weight distribution are known in a few cases. Let A_l denote the number of codewords with weight l. For a binary Hamming code, each A_l can be determined from the weight-enumerator polynomial

$$A(x) = \sum_{l=0}^{n} A_l x^l = \frac{1}{n+1}[(1+x)^n + n(1+x)^{(n-1)/2}(1-x)^{(n+1)/2}] \tag{1-6}$$

For example,the Hamming (7,4) code gives $A(x) = \frac{1}{8}[(1+x)^7 + 7(1+x)^3(1-x)^4] = 1 + 7x^3 + 7x^4 + x^7$, which yields A_0=1, A_3=7, A_4=7, A_7=1, and A_l=0,

Table 1.3: Weight distributions of Golay codes.

	Number of Codewords	
Weight	(23,12)	(24,12)
0	1	1
7	253	0
8	506	759
11	1288	0
12	1288	2576
15	506	0
16	253	759
23	1	0
24	0	1

otherwise. For a maximum-distance-separable code, $A_0=1$ and [2]

$$A_l = \binom{n}{l}(q-1)\sum_{i=0}^{l-d_m}(-1)^i\binom{l-1}{i}q^{l-i-d_m}, \quad d_m \le l \le n \tag{1-7}$$

The weight distribution of other codes can be determined by examining all valid codewords if the number of codewords is not too large for a computation.

Error Probabilities for Hard-Decision Decoding

There are two types of bounded-distance decoders: erasing decoders and reproducing decoders. They differ only in their actions following the detection of uncorrectable errors in a received word. An *erasing decoder* discards the received word and may initiate an automatic retransmission request. For a systematic block code, a *reproducing decoder* reproduces the information symbols of the received word as its output.

Let P_s denote the *channel-symbol error probability,* which is the probability of error in a demodulated code symbol. It is assumed that the channel-symbol errors are statistically independent and identically distributed, which is usually an accurate model for systems with appropriate symbol interleaving (Section 1.3). Let P_w denote the *word error probability,* which is the probability that a received word is not decoded correctly due to both undetected errors and decoding failures. There are $\binom{n}{i}$ distinct ways in which i errors may occur among n symbols. Since a received sequence may have more than t errors but no information-symbol errors,

$$P_w \le \sum_{i=t+1}^{n}\binom{n}{i}P_s^i(1-P_s)^{n-i} \tag{1-8}$$

for a reproducing decoder that corrects t or few errors. For an erasing decoder, (1-8) becomes an equality. For reproducing decoders, t is given by (1-1) because

it is pointless to make the decoding spheres smaller than the maximum allowed by the code. However, if a block code is used for both error correction and error detection, an erasing decoder is often designed with t less than the maximum. If a block code is used exclusively for error detection, then $t = 0$.

Conceptually, a complete decoder correctly decodes when the number of symbol errors exceeds t if the received sequence lies within the planar boundaries associated with the correct codeword, as depicted in Figure 1.1. When a received sequence is equidistant from two or more codewords, a complete decoder selects one of them according to some arbitrary rule. Thus, the word error probability for a complete decoder satisfies (1-8). If $P_s \leq 1/2$, a complete decoder is a maximum-likelihood decoder.

Let P_{ud} denote the probability of an *undetected error,* and let P_{df} denote the probability of a *decoding failure.* For a bounded-distance decoder

$$P_{ud} + P_{df} = \sum_{i=t+1}^{n} \binom{n}{i} P_s^i (1 - P_s)^{n-i} \tag{1-9}$$

Thus, it is easy to calculate P_{df} once P_{ud} is determined. Since the set of Hamming distances from a given codeword to the other codewords is the same for all given codewords of a linear block code, it is legitimate to assume for convenience in evaluating P_{ud} that the all-zero codeword was transmitted. If channel-symbol errors in a received word are statistically independent and occur with the same probability P_s, then the probability of an error in a specific set of i positions that results in a specific set of i erroneous symbols is

$$P_e(i) = \left(\frac{P_s}{q-1}\right)^i (1 - P_s)^{n-i} \tag{1-10}$$

For an undetected error to occur at the output of a bounded-distance decoder, the number of erroneous symbols must exceed t and the received word must lie within an incorrect decoding sphere of radius t. Let $N(l, i)$ is the number of sequences of Hamming weight i that lie within a decoding sphere of radius t associated with a particular codeword of weight l. Then

$$\begin{aligned} P_{ud} &= \sum_{i=t+1}^{n} P_e(i) \sum_{l=\max(i-t,d_m)}^{\min(i+t,n)} A_l N(l,i) \\ &= \sum_{i=t+1}^{n} \left(\frac{P_s}{q-1}\right)^i (1 - P_s)^{n-i} \sum_{l=\max(i-t,d_m)}^{\min(i+t,n)} A_l N(l,i) \end{aligned} \tag{1-11}$$

Consider sequences of weight i that are at distance s from a particular codeword of weight l, where $|l - i| \leq s \leq t$ so that the sequences are within the decoding sphere of the codeword. By counting these sequences and then summing over the allowed values of s, we can determine $N(l, i)$. The counting is done by considering changes in the components of this codeword that can produce one of these sequences. Let j denote the number of nonzero codeword symbols that

are changed to zeros, α the number of codeword zeros that are changed to any of the $(q-1)$ nonzero symbols in the alphabet, and β the number of nonzero codeword symbols that are changed to any of the other $(q-2)$ nonzero symbols. For a sequence at distance s to result, it is necessary that $0 \leq j \leq s$. The number of sequences that can be obtained by changing any j of the l nonzero symbols to zeros is $\binom{l}{j}$, where $\binom{b}{a} = 0$ if $a > b$. For a specified value of j, it is necessary that $\alpha = j + i - l$ to ensure a sequence of weight i. The number of sequences that result from changing any α of the $n-l$ zeros to nonzero symbols is $\binom{n-l}{\alpha}$ $(q-1)^{\alpha}$. For a specified value of j and hence α, it is necessary that $\beta = s - j - \alpha = s + l - i - 2j$ to ensure a sequence at distance s. The number of sequences that result from changing β of the $l-j$ remaining nonzero components is $\binom{l-j}{\beta}$ $(q-2)^{\beta}$, where $0^x = 0$ if $x \neq 0$ and $0^0 = 1$. Summing over the allowed values of s and j, we obtain

$$N(l,i) = \sum_{s=|l-i|}^{t} \sum_{j=0}^{s} \binom{l}{j} \binom{n-l}{j+i-l} \binom{l-j}{s+l-i-2j} \times (q-1)^{j+i-l}(q-2)^{s+l-i-2j} \tag{1-12}$$

Equations (1-11) and (1-12) allow the exact calculation of P_{ud}.

When $q = 2$, the only term in the inner summation of (1-12) that is nonzero has the index $j = (s+l-i)/2$ provided that this index is an integer and $0 \leq (s+l-i)/2 \leq s$. Using this result, we find that for binary codes,

$$N(l,i) = \sum_{s=|l-i|}^{t} \binom{n-l}{\frac{s+i-l}{2}} \binom{l}{\frac{s+l-i}{2}}, \quad q = 2 \tag{1-13}$$

where $\binom{m}{\frac{1}{2}} = 0$ for any nonnegative integer m. Thus, $N(l,l) = 1$ and $N(l,i) = 0$ for $|l-i| \geq t+1$.

The word error probability is a performance measure that is important primarily in applications for which only a decoded word completely without symbol errors is acceptable. When the utility of a decoded word degrades in proportion to the number of information bits that are in error, the *information-bit error probability* is frequently used as a performance measure. To evaluate it for block codes that may be nonbinary, we first examine the information-symbol error probability.

Let $P_{is}(j)$ denote the probability of an error in information symbol j at the decoder output. In general, it cannot be assumed that $P_{is}(j)$ is independent of j. The *information-symbol error probability,* which is defined as the unconditional error probability without regard to the symbol position, is

$$P_{is} = \frac{1}{k} \sum_{j=1}^{k} P_{is}(j) \tag{1-14}$$

The random variables Z_j, $j = 1, 2, \ldots, k$, are defined so that $Z_j = 1$ if information symbol j is in error and $Z_j = 0$ if it is correct. The expected number

of information-symbol errors is

$$E[I] = E\left[\sum_{j=1}^{k} Z_j\right] = \sum_{j=1}^{k} E[Z_j] = \sum_{j=1}^{k} P_{is}(j) \tag{1-15}$$

where $E[\ ]$ denotes the expected value. The *information-symbol error rate* is defined as $E[I]/k$. Equations (1-14) and (1-15) imply that

$$P_{is} = \frac{E[I]}{k} \tag{1-16}$$

which indicates that the information-symbol error probability is equal to the information-symbol error rate.

Let $P_{ds}(j)$ denote the probability of an error in symbol j of the codeword chosen by the decoder or symbol j of the received sequence if a decoding failure occurs. The decoded-symbol error probability is

$$P_{ds} = \frac{1}{n}\sum_{j=1}^{n} P_{ds}(j) \tag{1-17}$$

If $E[D]$ is the expected number of decoded-symbol errors, a derivation similar to the preceding one yields

$$P_{ds} = \frac{E[D]}{n} \tag{1-18}$$

which indicates that the decoded-symbol error probability is equal to the decoded-symbol error rate. It can be shown [5] that for cyclic codes, the error rate among the information symbols in the output of a bounded-distance decoder is equal to the error rate among all the decoded symbols; that is,

$$P_{is} = P_{ds} \tag{1-19}$$

This equation, which is at least approximately valid for linear block codes, significantly simplifies the calculation of P_{is} because P_{ds} can be expressed in terms of the code weight distribution, whereas an exact calculation of P_{is} requires additional information.

An erasing decoder makes an error only if it fails to detect one. Therefore, $P_{ds} = P_{ud}$ and (1-11) implies that the *decoded-symbol error rate for an erasing decoder* is

$$P_{ds} = \sum_{i=t+1}^{n} \left(\frac{P_s}{q-1}\right)^{i} (1-P_s)^{n-i} \sum_{l=\max(i-t,d_m)}^{\min(i+t,n)} A_l N(l,i)\frac{l}{n} \tag{1-20}$$

The number of sequences of weight i that lie in the interstices outside the decoding spheres is

$$L(i) = (q-1)^i \binom{n}{i} - \sum_{l=\max(i-t,d_m)}^{\min(i+t,n)} A_l N(l,i)\ , \quad i \geq t+1 \tag{1-21}$$

where the first term is the total number of sequences of weight i, and the second term is the number of sequences of weight i that lie within incorrect decoding spheres. When i symbol errors in the received word cause a decoding failure, the decoded symbols in the output of a reproducing decoder contain i errors. Therefore, the *decoded-symbol error rate for a reproducing decoder* is

$$P_{ds} = \sum_{i=t+1}^{n} \left(\frac{P_s}{q-1}\right)^i (1-P_s)^{n-i} \left[\sum_{l=\max(i-t,d_m)}^{\min(i+t,n)} A_l N(l,i)\frac{l}{n} + L(i)\frac{i}{n}\right] \quad (1\text{-}22)$$

Even if $P_{is} = P_{ds}$, two major problems still arise in calculating P_{is} from (1-20) or (1-22). The computational complexity may be prohibitive when n and q are large, and the weight distribution is unknown for many linear or cyclic block codes.

The *packing density* is defined as the ratio of the number of words in the q^k decoding spheres to the total number of sequences of length n. From (2), it follows that the packing density is

$$D_p = \frac{q^k}{q^n} \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \quad (1\text{-}23)$$

For perfect codes, $D_p = 1$. If $D_p > 0.5$, undetected errors tend to occur more often then decoding failures, and the code is considered *tightly packed.* If $D_p < 0.1$, decoding failures predominate, and the code is considered *loosely packed.* The packing densities of binary BCH codes are listed in Table 1.1. The codes are tightly packed if $n = 7$ or 15. For $k > 1$ and $n = 31$, 63, or 127, the codes are tightly packed only if $t = 1$ or 2.

To approximate P_{is} for tightly packed codes, let $A(i)$ denote the event that i errors occur in a received sequence of n symbols at the decoder input. If the symbol errors are independent, the probability of this event is

$$P[A(i)] = \binom{n}{i} P_s^i (1-P_s)^{n-i} \quad (1\text{-}24)$$

Given event $A(i)$ for i such that $d_m \leq i \leq n$, it is plausible to assume that a reproducing bounded-distance decoder usually chooses a codeword with approximately i symbol errors. For i such that $t+1 \leq i \leq d_m$, it is plausible to assume that the decoder usually selects a codeword at the minimum distance d_m. These approximations, (1-19), (1-24), and the identity $\binom{n}{i}\frac{i}{n} = \binom{n-1}{i-1}$ indicate that P_{is} for reproducing decoders is approximated by

$$P_{is} \approx \sum_{i=t+1}^{d_m} \frac{d_m}{n}\binom{n}{i} P_s^i (1-P_s)^{n-i} + \sum_{i=d_m+1}^{n} \binom{n-1}{i-1} P_s^i (1-P_s)^{n-i} \quad (1\text{-}25)$$

The virtues of this approximation are its lack of dependence on the code weight distribution and its generality. Computations for specific codes indicate that the accuracy of this approximation tends to increase with P_{ud}/P_{df}. The right-hand

side of (1-25) gives an approximate upper bound on P_{is} for erasing bounded-distance decoders, for loosely packed codes with bounded-distance decoders, and for complete decoders because some received sequences with $t+1$ or more errors can be corrected and, hence, produce no information-symbol errors.

For a loosely packed code, it is plausible that P_{is} for a reproducing bounded-distance decoder might be accurately estimated by ignoring undetected errors. Dropping the terms involving $N(l,i)$ in (1-21) and (1-22) and using (1-19) gives

$$P_{is} \geq \sum_{i=t+1}^{n} \binom{n-1}{i-1} P_s^i (1-P_s)^{n-i} \tag{1-26}$$

The virtue of this lower bound as an approximation is its independence of the code weight distribution. The bound is tight when decoding failures are the predominant error mechanism. For cyclic Reed-Solomon codes, numerical examples [5] indicate that the exact P_{is} and the approximate bound are quite close for all values of P_s when $t \geq 3$, a result that is not surprising in view of the paucity of sequences in the decoding spheres for a Reed-Solomon code with $t \geq 3$. A comparison of (1-26) with (1-25) indicates that the latter overestimates P_{is} by a factor of less than $d_m/(t+1)$.

A *q-ary symmetric channel* or *uniform discrete channel* is one in which an incorrectly decoded information symbol is equally likely to be any of the remaining $q-1$ symbols in the alphabet. Consider a linear (n,k) block code and a q-ary symmetric channel such that q is a power of 2 and the "channel" refers to the transmission channel plus the decoder. Among the $q-1$ incorrect symbols, a given bit is incorrect in $q/2$ instances. Therefore, the information-bit error probability is

$$P_b = \frac{q}{2(q-1)} P_{is} \tag{1-27}$$

Let r denote the ratio of information bits to transmitted channel symbols. For binary codes, r is the code rate. For block codes with $m = \log_2 q$ information bits per symbol, $r = mk/n$. When coding is used but the information rate is preserved, the duration of a channel symbol is changed relative to that of an information bit. Thus, the energy per received channel symbol is

$$\mathcal{E}_s = r\mathcal{E}_b = \frac{mk}{n}\mathcal{E}_b \tag{1-28}$$

where $\mathcal{E}_b$ is the energy per information bit. When $r < 1$, a code is potentially beneficial if its error-control capability is sufficient to overcome the degradation due to the reduction in the energy per received symbol. For the AWGN channel and coherent binary phase-shift keying (PSK), the classical theory indicates that the symbol error probability at the demodulator output is

$$P_s = Q\left(\sqrt{\frac{2r\mathcal{E}_b}{N_0}}\right) \tag{1-29}$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{y^2}{2}\right) dy = \frac{1}{2}\operatorname{erfc}\left(\frac{x}{\sqrt{2}}\right) \tag{1-30}$$

and erfc( ) is the complementary error function. Consider the noncoherent detection of q-ary orthogonal signals over an AWGN channel. The channel symbols for multiple frequency-shift keying (MFSK) modulation are received as orthogonal signals. It is shown subsequently that P_s at the demodulator output is

$$P_s = \sum_{i=1}^{q-1} \frac{(-1)^{i+1}}{i+1} \binom{q-1}{i} \exp\left[-\frac{imr\mathcal{E}_b}{(i+1)N_0} \right] \tag{1-31}$$

which decreases as q increases for sufficiently large values of $\mathcal{E}_b/N_0$. The orthogonality of the signals ensures that at least the transmission channel is q-ary symmetric, and, hence, (1-27) is at least approximately correct.

If the alphabets of the code symbols and the transmitted channel symbols are the same, then the channel-symbol error probability P_{cs} equals the code-symbol error probability P_s. If not, then the q-ary code symbols may be mapped into q_1-ary channel symbols. If $q = 2^m$ and $q_1 = 2^{m_1}$, then choosing m/m_1 to be an integer is strongly preferred for implementation simplicity. Since any of the channel-symbol errors can cause an error in the corresponding code symbol, the independence of channel-symbol errors implies that

$$P_s = 1 - (1 - P_{cs})^{m/m_1} \tag{1-32}$$

A common application is to map nonbinary code symbols into binary channel symbols ($m_1 = 1$). In this case, (1-27) is no longer valid because the transmission channel plus the decoder is not necessarily q-ary symmetric. Since there is at least one bit error for every symbol error,

$$\frac{P_{is}}{m} \le P_b \le \frac{qP_{is}}{2(q-1)} \tag{1-33}$$

This lower bound is tight when P_{cs} is low because then there tends to be a single bit error per code-symbol error before decoding, and the decoder is unlikely to change an information symbol. For coherent binary PSK, (1-29) and (1-32) imply that

$$P_s = 1 - \left[1 - Q\left(\sqrt{\frac{2r\mathcal{E}_b}{N_0}} \right) \right]^m \tag{1-34}$$

Error Probabilities for Soft-Decision Decoding

A symbol is said to be erased when the demodulator, after deciding that a symbol is unreliable, instructs the decoder to ignore that symbol during the decoding. The simplest practical soft-decision decoding uses *erasures* to supplement hard-decision decoding. If a code has a minimum distance d_m and a received word is assigned ϵ erasures, then all codewords differ in at least $d_m - \epsilon$ of the unerased symbols. Hence, ν errors can be corrected if $2\nu + 1 \le d_m - \epsilon$. If d_m or more erasures are assigned, a decoding failure occurs. Let P_ϵ denote the probability of an erasure. For independent symbol errors and erasures, the probability

that a received sequence has i errors and j erasures is $P_s^i P_\epsilon^j (1 - P_s - P_\epsilon)^{n-i-j}$. Therefore, for a bounded-distance decoder,

$$P_w \leq \sum_{j=0}^{n} \sum_{i=i_0}^{n-j} \binom{n}{j} \binom{n-j}{i} P_s^i P_\epsilon^j (1 - P_s - P_\epsilon)^{n-i-j} ,$$

$$i_0 = \max(0, \lceil (d_m - j)/2 \rceil) \tag{1-35}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. This inequality becomes an equality for an erasing decoder. For the AWGN channel, decoding with optimal erasures provides an insignificant performance improvement relative to hard-decision decoding, but erasures are often effective against fading or sporadic interference. Codes for which *errors-and-erasures decoding* is most attractive are those with relatively large minimum distances such as Reed-Solomon codes.

Soft decisions are made by associating a number called the *metric* with each possible codeword. The metric is a function of both the codeword and the demodulator output samples. A soft-decision decoder selects the codeword with the largest metric and then produces the corresponding information bits as its output. Let $\mathbf{y}$ denote the n-dimensional vector of noisy output samples $y_i, i = 1, 2, \ldots, n$, produced by a demodulator that receives a sequence of n symbols. Let $\mathbf{x}_l$ denote the lth codeword vector with symbols $x_{li}, i = 1, 2, \ldots, n$. Let $f(\mathbf{y}|\mathbf{x}_l)$ denote the *likelihood function,* which is the conditional probability density function of $\mathbf{y}$ given that $\mathbf{x}_l$ was transmitted. The maximum-likelihood decoder finds the value of l, $1 \leq l \leq q^k$, for which the likelihood function is largest. If this value is l_0, the decoder decides that codeword l_0 was transmitted. Any monotonically increasing function of $f(\mathbf{y}|\mathbf{x}_l)$ may serve as the metric of a maximum-likelihood decoder. A convenient choice is often proportional to the logarithm of $f(\mathbf{y}|\mathbf{x}_l)$, which is called the *log-likelihood function.* For statistically independent demodulator outputs, the log-likelihood function for each of the q^k possible codewords is

$$\ln f(\mathbf{y}|\mathbf{x}_l) = \sum_{i=1}^{n} \ln f(y_i|x_{li}) , \qquad l = 1, 2, \ldots, q^k \tag{1-36}$$

where $f(y_i|x_{li})$ is the conditional probability density function of y_i given the value of x_{li}.

For coherent binary PSK communication over the AWGN channel, if codeword l is transmitted, then the received signal representing symbol i is

$$r_i(t) = \sqrt{2\mathcal{E}_s} x_{li} \psi(t) \cos 2\pi f_c t + n_i(t) , \quad 0 \leq t \leq T_s, \quad i = 1, 2, \ldots, n \tag{1-37}$$

where $\mathcal{E}_s$ is the symbol energy, T_s is the symbol duration, f_c is the carrier frequency, $x_{li} = +1$ when binary symbol i is a 1 and $x_{li} = -1$ when binary symbol i is a 0, $\psi(t)$ is the unit-energy symbol waveform, and $n_i(t)$ is independent, zero-mean, white Gaussian noise. Since $\psi(t)$ has unit energy and vanishes outside $[0, T_s]$,

$$\int_0^{T_s} |\psi(t)|^2 dt = 1 \tag{1-38}$$

For coherent demodulation, a frequency translation to baseband is provided by multiplying $r_i(t)$ by $\cos 2\pi f_c t$. After discarding a negligible integral, we find that the matched-filter demodulator, which is matched to $\psi(t)$, produces the output samples

$$y_i = \sqrt{\mathcal{E}_s/2}x_{li} + \int_0^{T_s} n_i(t)\psi(t)\cos 2\pi f_c t \, dt \ , \quad i = 1, 2, \ldots, n \tag{1-39}$$

These outputs provide sufficient statistics because $\psi(t)\cos 2\pi f_c t$ is the sole basis function for the signal space. Since $n_i(t)$ is statistically independent of $n_k(t)$ when $i \neq k$, the $\{y_i\}$ are statistically independent.

The autocorrelation of each white noise process is

$$E[n_i(t)n_i(t+\tau)] = \frac{N_{0i}}{2}\delta(\tau) \ , \quad i = 1, 2, \ldots, n \tag{1-40}$$

where $N_{0i}/2$ is the two-sided power spectral density of $n_i(t)$ and $\delta(\tau)$ is the Dirac delta function. A straightforward calculation using (1-40) and assuming that the spectrum of $\psi(t)$ is confined to $|f| < f_c$ indicates that the variance of the noise term of (1-39) is $N_{0i}/4$. Therefore, the conditional probability density function of y_i given that x_{li} was transmitted is

$$f(y_i|x_{li}) = \frac{1}{\sqrt{\pi N_{0i}/2}} \exp\left[- \frac{(y_i - \sqrt{\mathcal{E}_s/2}x_{li})^2}{N_{0i}/2} \right] , \quad i = 1, 2, \ldots, n \tag{1-41}$$

Since y_i^2 and $x_{li}^2 = 1$ are independent of the codeword l, terms involving these quantities may be discarded in the log-likelihood function of (1-36). Therefore, the maximum-likelihood metric is

$$U(l) = \sum_{i=1}^{n} \frac{x_{li}y_i}{N_{0i}} \ , \quad l = 1, 2, \ldots, 2^k \tag{1-42}$$

which requires knowledge of $N_{0i}, i = 1, 2, \ldots, n$.

If each $N_{0i} = N_0$, a constant, then this constant is irrelevant, and the maximum-likelihood metric is

$$U(l) = \sum_{i=1}^{n} x_{li}y_i \ , \quad l = 1, 2, \ldots, 2^k \tag{1-43}$$

Let $P_2(\delta)$ denote the probability that the metric for an incorrect codeword at distance δ from the correct codeword exceeds the metric for the correct codeword. After reordering the samples $\{y_i\}$, the difference between the metrics for the correct codeword and the incorrect one may be expressed as

$$D(\delta) = \sum_{i=1}^{\delta} (x_{1i} - x_{2i})y_i = 2\sum_{i=1}^{\delta} x_{1i}y_i \tag{1-44}$$

where the sum includes only the δ terms that differ, x_{1i} refers to the correct codeword, x_{2i} refers to the incorrect codeword, and $x_{2i} = -x_{1i}$. Then $P_2(\delta)$

is the probability that $D(\delta) < 0$. Since each of its terms is independent, $D(\delta)$ has a Gaussian distribution. A straightforward calculation using (1-41) and $\mathcal{E}_s = r\mathcal{E}_b$ yields

$$P_2(\delta) = Q\left(\sqrt{\frac{2\delta r\mathcal{E}_b}{N_0}}\right) \tag{1-45}$$

which reduces to (1-29) when a single symbol is considered and $\delta = 1$.

A fundamental property of a probability, called *countable subadditivity,* is that the probability of a finite or countable union of events B_n, $n = 1, 2, \ldots$, satisfies

$$P[\cup_n B_n] \leq \sum_n P[B_n] \tag{1-46}$$

In communication theory, a bound obtained from this inequality is called a *union bound.* To determine P_w for linear block codes, it suffices to assume that the all-zero codeword was transmitted. The union bound and the relation between weights and distances imply that P_w for soft-decision decoding satisfies

$$P_w \leq \sum_{l=d_m}^{n} A_l P_2(l) \tag{1-47}$$

Let β_l denote the total information-symbol weight of the codewords of weight l. The union bound and (1-16) imply that

$$P_{is} \leq \sum_{l=d_m}^{n} \frac{\beta_l}{k} P_2(l) \tag{1-48}$$

To determine β_l for any cyclic (n, k) code, consider the set S_l of A_l codewords of weight l. The total weight of all the codewords in S_l is $A_T = lA_l$. Let α and β denote any two fixed positions in the codewords. By definition, any cyclic shift of a codeword produces another codeword of the same weight. Therefore, for every codeword in S_l that has a zero in α, there is some codeword in S_l that results from a cyclic shift of that codeword and has a zero in β. Thus, among the codewords of S_l, the total weight of all the symbols in a fixed position is the same regardless of the position and is equal to A_T/n. The total weight of all the information symbols in S_l is $\beta_l = kA_T/n = klA_l/n$. Therefore,

$$P_{is} \leq \sum_{l=d_m}^{n} \frac{l}{n} A_l P_2(l) \tag{1-49}$$

Optimal soft-decision decoding cannot be efficiently implemented except for very short block codes, primarily because the number of codewords for which the metrics must be computed is prohibitively large, but approximate maximum-likelihood decoding algorithms are available. The *Chase algorithm* [3] generates a small set of candidate codewords that will almost always include the codeword with the largest metric. Test patterns are generated by first making hard decisions on each of the received symbols and then altering the

least reliable symbols, which are determined from the demodulator outputs given by (1-39). Hard-decision decoding of each test pattern and the discarding of decoding failures generate the candidate codewords. The decoder selects the candidate codeword with the largest metric.

The quantization of soft-decision information to more than two levels requires analog-to-digital conversion of the demodulator output samples. Since the optimal location of the levels is a function of the signal, thermal noise, and interference powers, automatic gain control is often necessary. For the AWGN channel, it is found that an eight-level quantization represented by three bits and a uniform spacing between threshold levels cause no more than a few tenths of a decibel loss relative to what could theoretically be achieved with unquantized analog voltages or infinitely fine quantization.

The *coding gain* of one code compared with a second one is the reduction in the signal power or value of E_b/N_0 required to produce a specified information-bit or information-symbol error probability. Calculations for specific communication systems and codes operating over the AWGN channel have shown that an optimal soft-decision decoder provides a coding gain of approximately 2 dB relative to a hard-decision decoder. However, soft-decision decoders are much more complex to implement and may be too slow for the processing of high information rates. For a given level of implementation complexity, hard-decision decoders can accommodate much longer block codes, thereby at least partially overcoming the inherent advantage of soft-decision decoders. In practice, soft-decision decoding other than erasures is seldom used with block codes of length greater than 50.

Performance Examples

Figure 1.2 depicts the information-bit error probability $P_b = P_{is}$ versus $\mathcal{E}_b/N_0$ for various binary block codes with coherent PSK over the AWGN channel. Equation (1-25) is used to compute P_b for the Golay (23,12) code with hard decisions. Since the packing density D_p is small for these codes, (1-26) is used for the BCH (63,36) code, which corrects $t = 5$ errors, and the BCH (127,64) code, which corrects $t = 10$ errors. Equation (1-29) is used for P_s. Inequality (1-49) and Table 1.2 are used to compute the upper bound on $P_b = P_{is}$ for the Golay (23,12) code with optimal soft decisions. The graphs illustrate the power of the soft-decision decoding. For the Golay (23,12) code, soft-decision decoding provides an approximately 2-dB coding gain for $P_b = 10^{-5}$ relative to hard-decision decoding. Only when $P_b < 10^{-5}$ does the BCH (127,64) begin to outperform the Golay (23,12) code with soft decisions. If $\mathcal{E}_b/N_0 \leq 3$ dB, an uncoded system with coherent PSK provides a lower P_b than a similar system that uses one of the block codes of the figure.

Figure 1.3 illustrates the performance of loosely packed Reed-Solomon codes with hard-decision decoding over the AWGN channel. The lower bound in (1-26) is used to compute the approximate information-bit error probabilities for binary channel symbols with coherent PSK and for nonbinary channel symbols with noncoherent MFSK. For the nonbinary channel symbols, (1-27) and (1-31)

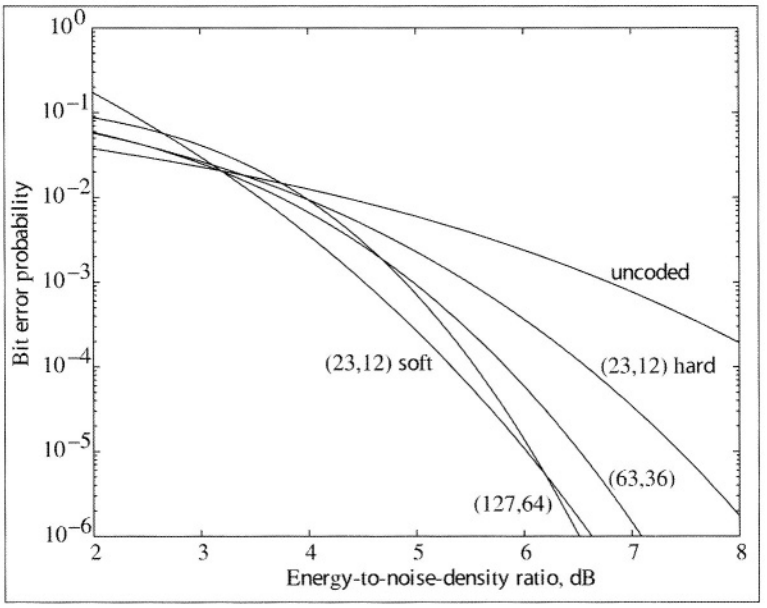

Figure 1.2: Information-bit error probability for binary block (n, k) codes and coherent PSK.

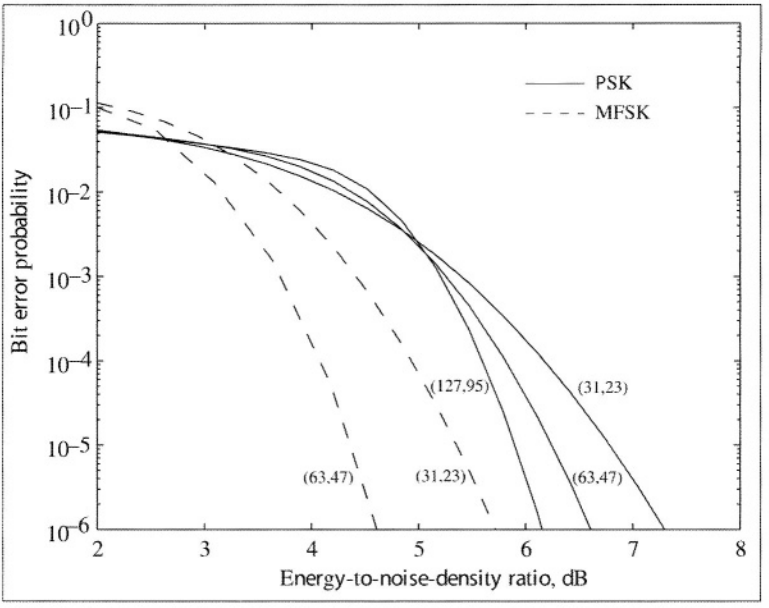

Figure 1.3: Information-bit error probability for Reed-Solomon (n, k) codes. Modulation is coherent PSK or noncoherent MFSK.

are used. For the binary channel symbols, (1-34) and the lower bound in (1-33) are used. For the chosen values of n, the best performance at $P_b = 10^{-5}$ is obtained if the code rate is $k/n \approx 3/4$. Further gains result from increasing n and hence the implementation complexity. Although the figure indicates the performance advantage of Reed-Solomon codes with MFSK, there is a major bandwidth penalty. Let B denote the bandwidth required for an uncoded binary PSK signal. If the same data rate is accommodated by using uncoded binary frequeny-shift keying (FSK), the required bandwidth for demodulation with envelope detectors is approximately $2B$. For uncoded MFSK using $q = 2^m$ frequencies, the required bandwidth is $2^m B/m$ because each symbol represents m bits. If a Reed-Solomon (n, k) code is used with MFSK, the required bandwidth becomes $2^m nB/mk$.

Code Metrics for Orthogonal Signals

For q-ary orthogonal symbol waveforms, $s_1(t)$, $s_2(t)$, ..., $s_q(t)$, q matched filters are needed, and the observation vector is $\mathbf{y} = [\mathbf{y}_1\ \mathbf{y}_2 \cdots\ \mathbf{y}_q]$, where each $\mathbf{y}_k$ is an n-dimensional row vector of matched-filter output samples for filter k with components $y_{ki}, i = 1, 2, \ldots, n$. Suppose that symbol i of codeword l uses unit-energy waveform $s_\nu(t)$, where the integer ν is a function of i and l. If codeword l is transmitted over the AWGN channel, the received signal for symbol i can be expressed in complex notation as

$$r_i(t) = \mathrm{Re}\left[\sqrt{2\mathcal{E}_s}s_\nu(t)e^{j2\pi f_c t+\theta_i}\right] + n_i(t), \quad 0 \le t \le T_s\ , \quad i = 1, 2, \ldots, n \quad (1\text{-}50)$$

where $n_i(t)$ is independent, zero-mean, white Gaussian noise with two-sided power spectral density $N_{0i}/2$, f_c is the carrier frequency, and θ_i is the phase. Since the symbol energy for all the waveforms is unity,

$$\int_0^{T_s} |s_k(t)|^2 dt = 1\ , \quad k = 1, 2, \ldots, q \quad (1\text{-}51)$$

The orthogonality of symbol waveforms implies that

$$\int_0^{T_s} s_k(t)s_m^*(t)dt = 0\ , \quad k \neq m \quad (1\text{-}52)$$

A frequency translation or *downconversion* to baseband is followed by matched filtering. Matched-filter k, which is matched to $s_k(t)$, produces the output samples

$$y_{ki} = \int_0^{T_s} r_i(t)e^{-j2\pi f_c t}s_k^*(t)dt\ , \quad i = 1, 2, \ldots, n\ , \quad k = 1, 2, \ldots, q \quad (1\text{-}53)$$

The substitution of (1-50) into (1-53), (1-52), and the assumption that each of the $\{s_k(t)\}$ has a spectrum confined to $|f| < f_c$ yields

$$y_{ki} = \sqrt{\mathcal{E}_s/2}e^{j\theta_i}\delta_{k\nu} + n_{ki} \quad (1\text{-}54)$$

where $\delta_{k\nu} = 1$ if $k = \nu$ and $\delta_{k\nu} = 0$ otherwise, and

$$n_{ki} = \int_0^{T_s} n_i(t) e^{-j2\pi f_c t} s_k^*(t) dt \tag{1-55}$$

Since the real and imaginary components of n_{ki} are jointly Gaussian, this random process is a *complex-valued Gaussian random variable.* Straightforward calculations using (1-40) and the confined spectra of the $\{s_k(t)\}$ indicates that the real and are imaginary components of n_{ki} are uncorrelated and, hence, independent and have the same variance $N_{0i}/4$. Since the density of a complex-valued random variable is defined to be the joint density of its real and imaginary parts, the conditional probability density function of y_{ki} given θ_i is

$$\begin{aligned} f(y_{ki} \mid \theta_i) &= \frac{1}{\pi N_{0i}/2} \exp\left(- \frac{\left| y_{ki} - \sqrt{\mathcal{E}_s/2} e^{j\theta_i} \delta_{k\nu} \right|^2}{N_{0i}/2} \right), \\ i &= 1, 2, \ldots, n, \quad k = 1, 2, \ldots, q \end{aligned} \tag{1-56}$$

The independence of the white Gaussian $\{n_i(t)\}$, the orthogonality condition (1-52), and the spectrally confined symbol waveforms ensure that both the real and imaginary parts of y_{ki} are independent of both the real and imaginary parts of y_{mp} unless $k{=}m$ and $i{=}p$. Thus, the likelihood function of the observation vector $\mathbf{y}$ is the product of the qn densities specified by (1-56).

For *coherent* signals, the $\{\theta_i\}$ are tracked by the phase synchronization system and, thus, ideally may be set to zero. Forming the log-likelihood function with the $\{\theta_i\}$ set to zero, and eliminating irrelevant terms that are independent of l, we obtain the maximum-likelihood metric

$$U(l) = \sum_{i=1}^{n} \frac{\mathrm{Re}(V_{li})}{N_{0i}} \tag{1-57}$$

where $V_{li} = y_{\nu i}$ is the sampled output i of the filter matched to $s_\nu(t)$, the signal representing symbol i of codeword l. If each $N_{0i} = N_0$, then the maximum-likelihood metric is

$$U(l) = \sum_{i=1}^{n} \mathrm{Re}\,(V_{li}) \tag{1-58}$$

and the common value N_0 does not need to be known to apply this metric.

For *noncoherent* signals, it is assumed that each θ_i is independent and uniformly distributed over $[0, 2\pi)$, which preserves the independence of the $\{y_{ki}\}$. Expanding the argument of the exponential function in (1-56), expressing y_{ki} in polar form, and integrating over θ_i, we obtain the probability density function

$$f(y_{ki}) = \frac{1}{\pi N_{0i}/2} \exp\left[- \frac{|y_{ki}|^2 + \mathcal{E}_s \delta_{k\nu}/2}{N_{0i}/2} \right] I_0\left(\frac{\sqrt{8\mathcal{E}_s}\, |y_{ki}|\, \delta_{k\nu}}{N_{0i}} \right) \tag{1-59}$$

where $I_0(\ )$ is the modified Bessel function of the first kind and order zero, This function may be represented by

$$I_0(x) = \frac{1}{2\pi}\int_0^{2\pi} \exp(x\cos u)du$$
$$= \sum_0^{\infty} \frac{1}{i!i!}\left(\frac{x}{2}\right)^{2i} \tag{1-60}$$

Let $R_{li} = |y_{\nu i}|$ denote the sampled envelope produced by the filter matched to $s_\nu(t)$, the signal representing symbol i of codeword l. We form the log-likelihood function and eliminate terms and factors that do not depend on the codeword l, thereby obtaining the maximum-likelihood metric

$$U(l) = \sum_{i=1}^{n} \ln I_0\left(\frac{\sqrt{8\mathcal{E}_s}R_{li}}{N_{0i}}\right) \tag{1-61}$$

If each $N_{0i} = N_0$, then the maximum-likelihood metric is

$$U(l) = \sum_{i=1}^{n} \ln I_0\left(\frac{\sqrt{8\mathcal{E}_s}R_{li}}{N_0}\right) \tag{1-62}$$

and $\sqrt{\mathcal{E}_s}/N_0$ must be known to apply this metric.

From the series representation of $I_0(x)$, it follows that

$$I_0(x) \leq \exp\left(\frac{x^2}{4}\right) \tag{1-63}$$

From the integral representation, we obtain

$$I_0(x) \leq \exp(|\ x\ |) \tag{1-64}$$

The upper bound in (1-63) is tighter for $0 \leq x < 2$, while the upper bound in (1-64) is tighter for $2 < x < \infty$. If we assume that R_{li}/N_{0i} is often less than 2, then the approximation of $I_0(x)$ by $\exp(x^2/4)$ is reasonable. Substitution into (1-61) and dropping an irrelevant constant gives the metric

$$U(l) = \sum_{i=1}^{n} \frac{R_{li}^2}{N_{0i}^2} \tag{1-65}$$

If each $N_{0i} = N_0$, then the value of N_0 is irrelevant, and we obtain the *Rayleigh metric*

$$U(l) = \sum_{i=1}^{n} R_{li}^2 \tag{1-66}$$

which is suboptimal for the AWGN channel but is the maximum-likelihood metric for the Rayleigh fading channel with identical statistics for each of the symbols (Section 5.6). Similarly, (1-64) can be used to obtain suboptimal metrics suitable for large values of R_{li}/N_{0i}.

To determine the maximum-likelihood metric for making a hard decision on each symbol, we set $n = 1$ and drop the subscript i in (1-57) and (1-61). We find that the maximum-likelihood symbol metric is $Re(V_l)$ for coherent MFSK and $\ln [I_0(\sqrt{8\mathcal{E}_s}R_l/N_0)]$ for noncoherent MFSK, where the index l ranges over the symbol alphabet. Since the latter function increases monotonically and $\sqrt{8\mathcal{E}_s}/N_0$ is a constant, optimal symbol metrics or decision variables for noncoherent MFSK are R_l or R_l^2 for $l = 1, 2, \ldots, q$.

Metrics and Error Probabilities for MFSK Symbols

For noncoherent MFSK, baseband matched-filter l is matched to the unit-energy waveform $s_l(t) = A\exp(j2\pi f_l t)$, $0 \le t \le T_s$, where $A = 1/\sqrt{T_s}$. If $r(t)$ is the received signal, a downconversion to baseband and a parallel set of matched filters and envelope detectors provide the decision variables

$$R_l^2 = A^2 \left| \int_0^{T_s} r(t) e^{-j2\pi f_c t} e^{-j2\pi f_l t} dt \right|^2 \tag{1-67}$$

The orthogonality condition (1-52) is satisfied if the adjacent frequencies are separated by k/T_s, where k is a nonzero integer. Expanding (1-67), we obtain

$$R_l^2 = R_{lc}^2 + R_{ls}^2 \tag{1-68}$$

$$R_{lc} = A \int_0^{T_s} r(t) \cos [2\pi(f_c + f_l)t]\, dt \tag{1-69}$$

$$R_{ls} = A \int_0^{T_s} r(t) \sin [2\pi(f_c + f_l)t]\, dt \tag{1-70}$$

These equations imply the correlator structure depicted in Figure 1.4, where the irrelevant constant A has been omitted. The comparator decides what symbol was transmitted by observing which comparator input is the largest.

To derive an alternative implementation, we observe that when the waveform is $s_l(t) = A\cos 2\pi(f_c + f_l)t$, $0 \le t \le T_s$, the impulse response of a filter matched to it is $A\cos 2\pi(f_c + f_l)(T_s - t)$, $0 \le t \le T_s$. Therefore, the matched-filter output at time t is

$$\begin{aligned} y_l(t) &= A \int_0^t r(\tau) \cos [2\pi(f_c + f_l)(\tau - t + T_s)]\, d\tau \\ &= A \left\{ \int_0^t r(\tau) \cos [2\pi(f_c + f_l)\tau]\, d\tau \right\} \cos [2\pi(f_c + f_l)(t - T_s)] \\ &\quad + A \left\{ \int_0^t r(\tau) \sin [2\pi(f_c + f_l)\tau]\, d\tau \right\} \sin [2\pi(f_c + f_l)(t - T_s)] \\ &= AR_l(t) \cos [2\pi(f_c + f_l)(t - T_s) + \phi(t)] \ , \quad 0 \le t \le T_s \end{aligned} \tag{1-71}$$