

ECE 729

Introduction to Channel Coding

Contents

1	Fundamental Concepts and Techniques	1
1.1	Channels	1
1.2	Encoders	1
1.2.1	Code Rates	2
1.3	Decoders	2
1.4	Probabilistic Model	2
1.5	The Probability of Error	2
1.6	New Codes from Old Codes by Throwing Away Codewords	3
1.7	The Random Coding Argument	3
1.8	The Codebook Reduction Argument	3
1.8.1	An Underlying Observation	3
1.8.2	Putting It All Together	3
1.9	Construction of Decoders	3
1.10	Bounds on the Probability of Error	4
1.11	Codeword Constraints	5
2	Achievable Rates	5
2.1	Deterministic Codes	5
2.2	Random Codes	6
2.3	Connecting Random Codes and Deterministic Codes	6
2.4	Capacity Regions	6
2.4.1	Capacity-Cost Functions	7
2.5	Cost per Bit	7
2.6	Waveform Channels and Spectral Efficiency	7

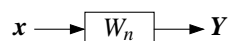
1. Fundamental Concepts and Techniques

1.1. Channels

Given a set X of **channel input symbols**, a set Y of **channel output symbols**, and a positive integer n , a **channel** W_n is a transition probability from X^n into Y^n . In other words, if $X = (X_1, \dots, X_n)$ is an X^n -valued random variable and $Y = (Y_1, \dots, Y_n)$ is a Y^n -valued random variable, then

$$W_n(B|\mathbf{x}) = P(Y \in B | X = \mathbf{x}), \quad B \subset Y^n,$$

is the conditional probability that the random sequence Y of channel output symbols lies in B given that the channel input sequence is $X = \mathbf{x}$.



If Y is a finite set, then so is Y^n , and W_n is given by a conditional probability mass function, which we also denote by W_n , and we have

$$W_n(B|\mathbf{x}) = \sum_{y \in B} W_n(\mathbf{y}|\mathbf{x}).$$

In most applications, W_n is not explicitly given, but is defined implicitly.

Example 1. Let $X = Y$ denote the integers $\{0, \dots, m-1\}$ under mod- m addition. Let the components of $Z := (Z_1, \dots, Z_n)$ be i.i.d. X -valued random variables with common pmf $p_Z(z) = P(Z = z)$ for $z \in X$. Let X be independent of Z , and put $Y := X + Z$, where the componentwise addition is mod- m . Then

$$\begin{aligned} W_n(\mathbf{y}|\mathbf{x}) &:= P(Y = \mathbf{y} | X = \mathbf{x}) \\ &= P(X + Z = \mathbf{y} | X = \mathbf{x}) \\ &= P(Z = \mathbf{y} - \mathbf{x}) \\ &= \prod_{k=1}^n p_Z(y_k - x_k). \end{aligned}$$

If $Y = \mathbb{R}$, then we take W_n to be given by a conditional probability density function, which we denote by w_n , and we have

$$W_n(B|\mathbf{x}) = \int_B w_n(\mathbf{y}|\mathbf{x}) d\mathbf{y}.$$

Here too, w_n is usually not given explicitly.

Example 2. Let $X = Y = \mathbb{R}$. Let the components of $Z := (Z_1, \dots, Z_n)$ be i.i.d. real-valued random variables with common probability density $p_Z(z)$. Let X be independent of Z , and put $Y := X + Z$. Then

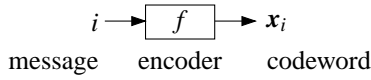
$$\begin{aligned} P(Y \leq y | X = \mathbf{x}) &= P(X + Z \leq y | X = \mathbf{x}) \\ &= P(Z \leq \mathbf{y} - \mathbf{x}) \\ &= \prod_{k=1}^n P(Z_k \leq y_k - x_k) \\ &= \prod_{k=1}^n \int_{-\infty}^{y_k - x_k} p_Z(z_k) dz_k. \end{aligned}$$

Differentiating with respect to the y_k , we have

$$w_n(\mathbf{y}|\mathbf{x}) = \prod_{k=1}^n p_Z(y_k - x_k).$$

1.2. Encoders

A mapping $f: \{1, \dots, N\} \rightarrow X^n$ is called an **encoder**. The integers $1, \dots, N$ are called **messages**. The corresponding **codewords** are denoted by $\mathbf{x}_i := f(i)$. Thus, each $\mathbf{x}_i \in X^n$. The collection $(\mathbf{x}_1, \dots, \mathbf{x}_N)$ is the corresponding **codebook**. Knowing the codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N)$ is the same as knowing the encoder f , and we sometimes just write $f = (\mathbf{x}_1, \dots, \mathbf{x}_N)$, which is an element of $(X^n)^N$.



1.2.1. Code Rates

If there are $N = 2^k$ messages, then each message can be thought of as a k -bit word. Even for N not a power of 2, we think of each message as consisting of $\log_2 N$ bits. If we use natural logarithms, we say that each message consists of $\ln N$ **nats**. We often do not specify the base of the logarithm and just write \log . In this case, we use \exp for the inverse of \log . Hence, if it is understood that the logarithm base is b , then $\exp(x) = b^x$. In particular, if the logarithm base is 2, then $\exp(x) = 2^x$, and if the logarithm base is e , then $\exp(x) = e^x$.

Given a code $f: \{1, \dots, N\} \rightarrow \mathcal{X}^n$, or equivalently a codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N)$, the **rate** of the code is

$$R = \frac{\log N}{n}. \quad (1)$$

In this expression, n is the number of channel uses or channel symbols transmitted for each message. If the logarithm base is 2, then the numerator has units of bits, and the quotient R has units of **bits per channel use** or **bits per channel symbol**. If the channel transmits R_c channel symbols per second, then

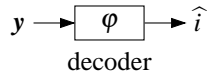
$$R_b := R_c \frac{\log_2 N}{n} \quad (2)$$

has units of bits per second. Combining this with (1) yields

$$R_b = R_c R. \quad (3)$$

1.3. Decoders

A mapping $\varphi: \mathcal{Y}^n \rightarrow \{1, \dots, N\}$ is called a **decoder**. If for $i = 1, \dots, N$ we put $D_i := \{\mathbf{y} : \varphi(\mathbf{y}) = i\}$, then the D_i form a **partition** of \mathcal{Y}^n since they are disjoint and their union is \mathcal{Y}^n . We call the D_i **decoding sets**.



1.4. Probabilistic Model

If we apply the output of the encoder to the channel, and we apply the output of the channel to the decoder, then we obtain the **channel coding system** shown in Fig. 1. Notice that the

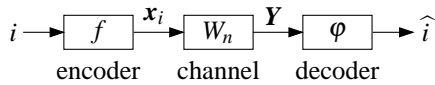


Figure 1. A channel coding system.

input to the system is i and the output is \hat{i} . We hope that most of the time $\hat{i} = i$. To make this more precise, we assume that the input to the encoder is a $\{1, \dots, N\}$ -valued random variable M , and we are interested in the probability of error $P(\varphi(\mathbf{Y}) \neq M)$.

However, this problem is not well defined unless we specify the joint distribution of M and \mathbf{Y} . We take

$$P(M = i, \mathbf{Y} \in B) := \frac{1}{N} \cdot W_n(B|\mathbf{x}_i), \quad i = 1, \dots, N, B \subset \mathcal{Y}^n. \quad (4)$$

Notice that since $W_n(\mathcal{Y}^n|\mathbf{x}_i) = 1$, (4) implies that $P(M = i) = 1/N$; i.e., the random message to be sent is chosen uniformly from the message set $\{1, \dots, N\}$. It then follows that

$$P(\mathbf{Y} \in B|M = i) = \frac{P(M = i, \mathbf{Y} \in B)}{P(M = i)} = W_n(B|\mathbf{x}_i). \quad (5)$$

We also point out that the definition of P in (4) depends on the codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N)$. Hence, $P(\varphi(\mathbf{Y}) \neq M)$ depends on the codebook and on the decoder φ .

1.5. The Probability of Error

It is now convenient to derive a somewhat explicit formula for $P(\varphi(\mathbf{Y}) \neq M)$. We use the law of total probability and substitution to write

$$\begin{aligned}
 P(\varphi(\mathbf{Y}) \neq M) &= \sum_{i=1}^N P(\varphi(\mathbf{Y}) \neq M|M = i)P(M = i) \\
 &= \frac{1}{N} \sum_{i=1}^N P(\varphi(\mathbf{Y}) \neq i|M = i) \\
 &= \frac{1}{N} \sum_{i=1}^N P(\mathbf{Y} \in \{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}|M = i) \\
 &= \frac{1}{N} \sum_{i=1}^N W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}|\mathbf{x}_i), \quad \text{by (5)}. \quad (6)
 \end{aligned}$$

Although the reader may have reservations about our choosing to have M be uniformly distributed, in many cases, we will be able to obtain a bound on the terms in (6) that does not depend on i , say

$$W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}|\mathbf{x}_i) < \lambda, \quad i = 1, \dots, N. \quad (7)$$

If we can establish such a bound, then for any probability mass function $q(i)$ on $\{1, \dots, N\}$, if we replace (4) with

$$P(M = i, \mathbf{Y} \in B) := q(i)W_n(B|\mathbf{x}_i), \quad i = 1, \dots, N, B \subset \mathcal{Y}^n,$$

it will follow that

$$\begin{aligned}
 P(\varphi(\mathbf{Y}) \neq M) &= \sum_{i=1}^N P(\varphi(\mathbf{Y}) \neq M|M = i)P(M = i) \\
 &= \sum_{i=1}^N P(\varphi(\mathbf{Y}) \neq i|M = i)q(i) \\
 &= \sum_{i=1}^N W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}|\mathbf{x}_i)q(i) \\
 &< \sum_{i=1}^N \lambda q(i) = \lambda.
 \end{aligned}$$

1.6. New Codes from Old Codes by Throwing Away Codewords

Let $f: \{1, \dots, N\} \rightarrow \mathcal{X}^n$ be any encoder, and let $\varphi: \mathcal{Y}^n \rightarrow \{1, \dots, N\}$ be any decoder. Then

$$D_i := \{\mathbf{y} : \varphi(\mathbf{y}) = i\}$$

contains exactly those outputs \mathbf{y} that are decoded to message i .

If G is any subset of $\{1, \dots, N\}$, we define the **modified encoder** $f_G: G \rightarrow \mathcal{X}^n$ by $f_G(i) := f(i) = \mathbf{x}_i$, $i \in G$, and we define the **modified decoder** $\varphi_G: \mathcal{Y}^n \rightarrow G$ by

$$\varphi_G(\mathbf{y}) := \begin{cases} \varphi(\mathbf{y}), & \mathbf{y} \in \bigcup_{i \in G} D_i \\ i_0, & \text{otherwise,} \end{cases}$$

where i_0 can be any fixed element of G . Hence, for $i \in G$ with $i \neq i_0$, $\varphi_G(\mathbf{y}) = i \Leftrightarrow \mathbf{y} \in D_i$, and we can write

$$\boxed{\{\mathbf{y} : \varphi_G(\mathbf{y}) \neq i\} = \{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}, \quad \text{for } i \in G, i \neq i_0.} \quad (8)$$

Furthermore, if we put

$$H := \left(\bigcup_{i \in G} D_i \right)^c,$$

then $\varphi_G(\mathbf{y}) = i_0 \Leftrightarrow \mathbf{y} \in D_{i_0} \cup H$. We can therefore write

$$\boxed{\{\mathbf{y} : \varphi_G(\mathbf{y}) \neq i\} \subset D_i^c = \{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}, \quad \text{for all } i \in G.} \quad (9)$$

Suppose that instead of (7), we have only

$$W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) < \lambda, \quad i \in G,$$

where G is a proper subset of $\{1, \dots, N\}$. Let f_G and φ_G be the encoder and decoder just described. Then by (9), we can write

$$W_n(\{\mathbf{y} : \varphi_G(\mathbf{y}) \neq i\} | \mathbf{x}_i) \leq W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) < \lambda, \quad i \in G.$$

1.7. The Random Coding Argument

Let g be a nonnegative function defined on some set Z , and let Z be a Z -valued random variable such that $\mathbb{E}[g(Z)] < \lambda$. Then there is at least one $z \in Z$ with $g(z) < \lambda$. To see this, suppose otherwise that $g(z) \geq \lambda$ for all z . Then we would have $\mathbb{E}[g(Z)] \geq \lambda$, which contradicts the hypothesis that $\mathbb{E}[g(Z)] < \lambda$.

We employ the **random coding argument** as follows. Looking back at (6), we put

$$e_n(\mathbf{x}_1, \dots, \mathbf{x}_N) := \frac{1}{N} \sum_{i=1}^N W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i).$$

If we can find a *random* codebook $(\mathbf{X}_1, \dots, \mathbf{X}_N)$ such that $\mathbb{E}[e_n(\mathbf{X}_1, \dots, \mathbf{X}_N)] < \lambda$, then there must be at least one codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N) \in (\mathcal{X}^n)^N$ with $e_n(\mathbf{x}_1, \dots, \mathbf{x}_N) < \lambda$.

1.8. The Codebook Reduction Argument

1.8.1. An Underlying Observation

Suppose $\theta_1, \dots, \theta_N$ are nonnegative numbers such that

$$\frac{1}{N} \sum_{i=1}^N \theta_i < \lambda.$$

Put $G := \{i : \theta_i < 2\lambda\}$. We claim that $|G| > N/2$. To see this, write

$$\begin{aligned} \lambda &> \frac{1}{N} \sum_{i=1}^N \theta_i = \frac{1}{N} \left(\sum_{i \in G^c} \theta_i + \sum_{i \in G} \theta_i \right) \\ &\geq \frac{1}{N} \sum_{i \in G^c} \theta_i \\ &\geq \frac{1}{N} \sum_{i \in G^c} 2\lambda \\ &= \frac{2\lambda}{N} |G^c|. \end{aligned}$$

It follows that $|G^c| < N/2$, and then

$$|G| = N - |G^c| > N - N/2 = N/2.$$

1.8.2. Putting It All Together

Suppose we can find a random codebook $(\mathbf{X}_1, \dots, \mathbf{X}_N)$ such that $\mathbb{E}[e_n(\mathbf{X}_1, \dots, \mathbf{X}_N)] < \lambda$. Then by the random coding argument, there is a codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N)$ such that

$$e_n(\mathbf{x}_1, \dots, \mathbf{x}_N) = \frac{1}{N} \sum_{i=1}^N W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) < \lambda.$$

By the observation above, there is a subset G of $\{1, \dots, N\}$ such that

$$W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) < 2\lambda, \quad i \in G.$$

By the throwing away the codewords \mathbf{x}_i for $i \notin G$, and using the construction in Section 1.6, we have an encoder f_G and decoder φ_G such that

$$W_n(\{\mathbf{y} : \varphi_G(\mathbf{y}) \neq i\} | \mathbf{x}_i) < 2\lambda, \quad i \in G. \quad (10)$$

Note that the rate of this modified code satisfies

$$\frac{\log |G|}{n} > \frac{\log N/2}{n} = \frac{\log N}{n} - \frac{\log 2}{n}.$$

Hence, even though we discard half of the original codewords, the rate of the modified code is nearly $(\log N)/n$ for large n .

1.9. Construction of Decoders

Let B_1, \dots, B_N be subsets of \mathcal{Y}^n , and suppose we want to have a decoder that announces message i when it observes a channel output sequence $\mathbf{y} \in B_i$. There are two difficulties with this description. First, if the B_i are not disjoint and $\mathbf{y} \in B_i \cap B_j$, does the decoder announce message i or message j ? Second, if the decoder observes a \mathbf{y} that does not belong to any of the B_i , what should the decoder do?

Here is a standard approach to address these difficulties. First, if \mathbf{y} belongs to more than one B_i , announce the smallest corresponding value of i . Second, if \mathbf{y} does not belong to any B_i , announce some fixed message, say N . To state this approach mathematically, let

$$F_1 := B_1$$

$$F_i := B_i \cap B_{i-1}^c \cap \dots \cap B_1^c, \quad i = 2, \dots, N,$$

and put

$$F := \left(\bigcup_{i=1}^N F_i \right)^c = F_1^c \cap \dots \cap F_N^c.$$

Then $F \cap F_i = \emptyset$ for $i = 1, \dots, N$, and

$$F_1 \cup \dots \cup F_N \cup F = \mathcal{Y}^n.$$

In other words, F_1, \dots, F_N and F constitute a **partition** of \mathcal{Y}^n . If we put

$$\varphi(\mathbf{y}) := \sum_{i=1}^N i I_{F_i}(\mathbf{y}) + N I_F(\mathbf{y}),$$

then for $i = 1, \dots, N-1$, $\varphi(\mathbf{y}) = i \Leftrightarrow \mathbf{y} \in F_i$, and thus

$$\varphi(\mathbf{y}) \neq i \Leftrightarrow \mathbf{y} \in F_i^c, \quad i = 1, \dots, N-1. \quad (11)$$

Furthermore, since $\varphi(\mathbf{y}) = N \Leftrightarrow \mathbf{y} \in F_N \cup F$, we have

$$\varphi(\mathbf{y}) \neq N \Leftrightarrow \mathbf{y} \in F_N^c \cap F^c,$$

where it is important to note that

$$F_N^c \cap F^c \subset F_N^c.$$

Hence,

$$\varphi(\mathbf{y}) \neq i \Rightarrow \mathbf{y} \in F_i^c, \quad i = 1, \dots, N. \quad (12)$$

To conclude, observe that

$$F_i^c = \begin{cases} B_1^c, & i = 1, \\ B_i^c \cup \left(\bigcup_{j < i} B_j \right), & i = 2, \dots, N. \end{cases} \quad (13)$$

We can now write

$$F_i^c \subset B_i^c \cup \left(\bigcup_{j \neq i} B_j \right), \quad i = 1, \dots, N. \quad (14)$$

From (12) and (14), we have

$$\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} \subset B_i^c \cup \left(\bigcup_{j \neq i} B_j \right), \quad \underline{\underline{i = 1, \dots, N}}. \quad (15)$$

and from (11) and (13) we have

$$\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} = F_i^c \supset B_i^c, \quad \underline{\underline{i = 1, \dots, N-1}}. \quad (16)$$

There are two special cases to be mentioned. First, if the B_i are disjoint, then $F_i = B_i$, and we have from (12) that

$$\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} \subset B_i^c, \quad i = 1, \dots, N.$$

Second, if the union of the B_i is equal to \mathcal{Y}^n , then

$$B_i^c \subset \bigcup_{j \neq i} B_j.$$

It then follows from (15) that

$$\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} \subset \bigcup_{j \neq i} B_j, \quad i = 1, \dots, N. \quad (17)$$

1.10. Bounds on the Probability of Error

We can use (15) to get a bound on a typical term in (6). We have

$$W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) \leq W_n(B_i^c | \mathbf{x}_i) + \sum_{j \neq i} W_n(B_j | \mathbf{x}_i). \quad (18)$$

By appealing to the two special cases above, we see that if the B_i are disjoint, then we can omit the sum on the right-hand side. If the union of the B_i is equal to \mathcal{Y}^n , then we can omit the term $W_n(B_i^c | \mathbf{x}_i)$.

Example 3 (Maximum-Likelihood Decoding). In **maximum-likelihood decoding**, we take

$$B_i = \{\mathbf{y} : W_n(\mathbf{y} | \mathbf{x}_i) \geq W_n(\mathbf{y} | \mathbf{x}_j) \text{ for all } j\}.$$

Since every \mathbf{y} must belong to at least one of these sets, their union is \mathcal{Y}^n . Letting

$$D_i := \{\mathbf{y} : \varphi(\mathbf{y}) = i\},$$

we have

$$W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) = \sum_{\mathbf{y}} I_{D_i^c}(\mathbf{y}) W_n(\mathbf{y} | \mathbf{x}_i). \quad (19)$$

Now, D_i depends on $\mathbf{x}_1, \dots, \mathbf{x}_N$. Let $\mathbf{X}_1, \dots, \mathbf{X}_N$ be i.i.d. with common pmf $p_n(\mathbf{x})$ on \mathcal{X}^n . Then for any $0 < \rho \leq 1$,

$$\begin{aligned} \mathbb{E}[I_{D_i^c}(\mathbf{y}) | \mathbf{X}_i = \mathbf{x}] &\leq \mathbb{P}\left(\bigcup_{j \neq i} B_j \mid \mathbf{X}_i = \mathbf{x}\right), \quad \text{by (17),} \\ &\leq \left[\sum_{j \neq i} \mathbb{P}(B_j | \mathbf{X}_i = \mathbf{x}) \right]^\rho, \quad \text{by [1, p. 136].} \end{aligned}$$

We next observe that for any $s > 0$,

$$\begin{aligned} \mathbb{P}(B_j | \mathbf{X}_i = \mathbf{x}) &\leq \mathbb{P}\left(W_n(\mathbf{y} | \mathbf{X}_j) \geq W_n(\mathbf{y} | \mathbf{x}) \mid \mathbf{X}_i = \mathbf{x}\right) \\ &= \mathbb{P}\left(W_n(\mathbf{y} | \mathbf{X}_j) \geq W_n(\mathbf{y} | \mathbf{x})\right) \\ &= \sum_{\mathbf{x}'} p_n(\mathbf{x}') I_{\{W_n(\mathbf{y} | \mathbf{x}') \geq W_n(\mathbf{y} | \mathbf{x})\}} \\ &\leq \sum_{\mathbf{x}'} p_n(\mathbf{x}') \left[\frac{W_n(\mathbf{y} | \mathbf{x}')}{W_n(\mathbf{y} | \mathbf{x})} \right]^s. \end{aligned}$$

We can now write

$$\begin{aligned} \mathbb{E}[I_{D_i^c}(\mathbf{y})|\mathbf{X}_i = \mathbf{x}] &\leq \left[\sum_{j \neq i} \sum_{\mathbf{x}'} p_n(\mathbf{x}') \left[\frac{W_n(\mathbf{y}|\mathbf{x}')}{W_n(\mathbf{y}|\mathbf{x})} \right]^s \right]^\rho \\ &= (N-1)^\rho W_n(\mathbf{y}|\mathbf{x})^{-\rho s} \\ &\quad \cdot \left[\sum_{\mathbf{x}'} p_n(\mathbf{x}') W_n(\mathbf{y}|\mathbf{x}')^s \right]^\rho. \end{aligned}$$

It now follows that if $\mathbf{x}_1, \dots, \mathbf{x}_N$ in (19) are replaced by $\mathbf{X}_1, \dots, \mathbf{X}_N$ and we take the expectation, it is upper bounded by

$$(N-1)^\rho \sum_{\mathbf{y}} \left[\sum_{\mathbf{x}} p_n(\mathbf{x}) W_n(\mathbf{y}|\mathbf{x})^{1-\rho s} \right] \left[\sum_{\mathbf{x}'} p_n(\mathbf{x}') W_n(\mathbf{y}|\mathbf{x}')^s \right]^\rho.$$

Specializing to $s = 1/(1+\rho)$, we obtain

$$(N-1)^\rho \sum_{\mathbf{y}} \left[\sum_{\mathbf{x}} p_n(\mathbf{x}) W_n(\mathbf{y}|\mathbf{x})^{1/(1+\rho)} \right]^{1+\rho}. \quad (20)$$

Note that since the expectation of (19) is at most one, (20) holds even for $\rho = 0$. In the case of a discrete memoryless channel, $W_n = W^n$. If we also take $p_n = p^n$, then the above sum over \mathbf{x} becomes

$$\prod_{k=1}^n \left(\sum_x p(x) W(y_k|x)^{1/(1+\rho)} \right).$$

Denoting this product by $\lambda(y_1) \cdots \lambda(y_n)$, (20) becomes

$$(N-1)^\rho \sum_{\mathbf{y}} \lambda(y_1)^{1+\rho} \cdots \lambda(y_n)^{1+\rho}.$$

Hence, for a DMC with $p_n = p^n$, we have

$$(N-1)^\rho \left\{ \sum_{\mathbf{y}} \left[\sum_x p(x) W(y|x)^{1/(1+\rho)} \right]^{1+\rho} \right\}^n.$$

If $N = \lfloor e^{nR} \rfloor \leq e^{nR}$, we obtain the further upper bound

$$e^{-n[E_o(\rho, p) - \rho R]},$$

where

$$E_o(\rho, p) := -\ln \sum_{\mathbf{y}} \left[\sum_x p(x) W(y|x)^{1/(1+\rho)} \right]^{1+\rho}.$$

To obtain the best bound, we optimize over ρ and p . Hence, the best bound is $e^{-nE_r(R)}$, where

$$E_r(R) := \sup_{0 \leq \rho \leq 1} \sup_p [E_o(\rho, p) - \rho R]$$

is called the **random coding exponent**.

1.11. Codeword Constraints

If a is nonnegative ‘‘cost’’ function defined on X , we may require that all codewords satisfy¹

$$a_n(\mathbf{x}) := \frac{1}{n} \sum_{k=1}^n a(x_k) \leq A$$

¹If $A_{\max} := \sup_{x \in \mathsf{X}} a(x)$ is finite, and if $A \geq A_{\max}$, then all codewords satisfy $a_n(\mathbf{x}) \leq A$, and the constraint is said to be **inactive**. If $A < A_{\min} := \inf_{x \in \mathsf{X}} a(x)$, then no codewords satisfy $a_n(\mathbf{x}) \leq A$.

for some constant A . In other words, the total cost to transmit a codeword cannot exceed nA . When $\mathsf{X} = \mathbb{R}$, we usually take $a(x) = x^2$ as a measure of the energy required to send the symbol x , and $a_n(\mathbf{x})$ is the average power used to transmit the codeword.

If we define a decoder φ as outlined in Section 1.9, we will choose the set B_i to have the form

$$B_i = \{\mathbf{y} : \text{‘‘expression involving } \mathbf{x}_i \text{ and } \mathbf{y}\text{’’ and } a_n(\mathbf{x}_i) \leq A\}.$$

This structure implies that

$$B_i^c \supset \{\mathbf{y} : a_n(\mathbf{x}_i) > A\}. \quad (21)$$

The set on the right-hand side is either Y^n the empty set in accordance with whether the condition $a_n(\mathbf{x}_i) > A$ is true or false. Hence, if we can show that

$$1 > W_n(\{\mathbf{y} : a_n(\mathbf{x}_i) > A\}|\mathbf{x}_i),$$

then the set is empty; i.e., we must have $a_n(\mathbf{x}_i) \leq A$. Now suppose that we proceed as in Section 1.8.2 with some $\lambda < 1/2$. Then

$$\begin{aligned} 1 &> W_n(\{\mathbf{y} : \varphi_G(\mathbf{y}) \neq i\}|\mathbf{x}_i), \quad i \in G, \text{ by (10),} \\ &= W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}|\mathbf{x}_i), \quad \text{by (8) if } i \neq i_0, \\ &\geq W_n(B_i^c|\mathbf{x}_i), \quad \text{by (16) if } i \neq N, \\ &\geq W_n(\{\mathbf{y} : a_n(\mathbf{x}_i) > A\}|\mathbf{x}_i), \quad \text{by (21).} \end{aligned}$$

Hence, there are at least $|G| - 2$ codewords that satisfy both (10) and $a_n(\mathbf{x}_i) \leq A$. Throwing away one or two codewords if necessary, we obtain a modified encoder $f_{G'}$ and a modified decoder $\varphi_{G'}$ that satisfy $W_n(\{\mathbf{y} : \varphi_{G'}(\mathbf{y}) \neq i\}|\mathbf{x}_i) < 2\lambda$ for $i \in G'$ and $a_n(\mathbf{x}_i) \leq A$ for all $i \in G'$. Furthermore, the rate of this code satisfies, for large N ,

$$\begin{aligned} \frac{\log |G'|}{n} &\geq \frac{\log(|G| - 2)}{n} \geq \frac{\log |G|/2}{n} \\ &\geq \frac{\log N/4}{n} = \frac{\log N}{n} - \frac{\log 4}{n}. \end{aligned}$$

2. Achievable Rates

2.1. Deterministic Codes

Definition D-A. A number $R \geq 0$ is achievable using **deterministic codes** under the **average** probability-of-error criterion and **codeword constraint** A if for every $\lambda > 0$, for every $\Delta R > 0$, for all sufficiently large n , there is a positive integer N with

$$\frac{\log N}{n} > R - \Delta R,$$

and there is a codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N)$ and decoder φ (usually depending on the codebook) such that $a_n(\mathbf{x}_i) \leq A$ for all $i = 1, \dots, N$, and

$$\frac{1}{N} \sum_{i=1}^N W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\}|\mathbf{x}_i) < \lambda.$$

Definition D-M. A number $R \geq 0$ is achievable using **deterministic codes** under the **maximal** probability-of-error criterion and **codeword constraint** A if for every $\lambda > 0$, for every $\Delta R > 0$, for all sufficiently large n , there is a positive integer N with

$$\frac{\log N}{n} > R - \Delta R,$$

and there is a codebook $(\mathbf{x}_1, \dots, \mathbf{x}_N)$ and decoder φ (usually depending on the codebook) such that $a_n(\mathbf{x}_i) \leq A$ for all $i = 1, \dots, N$, and

$$W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{x}_i) < \lambda, \quad i = 1, \dots, N.$$

It is easy to see that if a rate satisfies Definition D-M, then it satisfies Definition D-A. In other words, if $\mathcal{C}_{D-M}(A)$ denotes the set of achievable rates under Definition D-M, and if $\mathcal{C}_{D-A}(A)$ denotes the set of achievable rates under Definition D-A, then

$$\mathcal{C}_{D-M}(A) \subset \mathcal{C}_{D-A}(A). \quad (22)$$

2.2. Random Codes

Definition R-A. A number $R \geq 0$ is achievable using **random codes** under the **average** probability-of-error criterion and **codeword constraint** A if for every $\lambda > 0$, for every $\Delta R > 0$, for all sufficiently large n , there is a positive integer N with

$$\frac{\log N}{n} > R - \Delta R,$$

and there is a *random* codebook $(\mathbf{X}_1, \dots, \mathbf{X}_N)$ and decoder φ (usually depending on the codebook) such that $E[a_n(\mathbf{X}_i)] \leq A$ for all $i = 1, \dots, N$, and

$$E \left[\frac{1}{N} \sum_{i=1}^N W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{X}_i) \right] < \lambda.$$

Definition R-M. A number $R \geq 0$ is achievable using **random codes** under the **maximal** probability-of-error criterion and **codeword constraint** A if for every $\lambda > 0$, for every $\Delta R > 0$, for all sufficiently large n , there is a positive integer N with

$$\frac{\log N}{n} > R - \Delta R,$$

and there is a *random* codebook $(\mathbf{X}_1, \dots, \mathbf{X}_N)$ and decoder φ (usually depending on the codebook) such that $E[a_n(\mathbf{X}_i)] \leq A$ for all $i = 1, \dots, N$, and

$$E[W_n(\{\mathbf{y} : \varphi(\mathbf{y}) \neq i\} | \mathbf{X}_i)] < \lambda, \quad i = 1, \dots, N.$$

It is easy to see that if a rate satisfies Definition R-M, then it satisfies Definition R-A. In other words, if $\mathcal{C}_{R-M}(A)$ denotes the set of achievable rates under Definition R-M, and if $\mathcal{C}_{R-A}(A)$ denotes the set of achievable rates under Definition R-A, then

$$\mathcal{C}_{R-M}(A) \subset \mathcal{C}_{R-A}(A). \quad (23)$$

2.3. Connecting Random Codes and Deterministic Codes

By the random coding arguments in Sections 1.8.2 and 1.11,

$$\mathcal{C}_{R-A}(A) \subset \mathcal{C}_{D-M}(A). \quad (24)$$

We next point out that since a deterministic codebook is a special case of a random codebook,

$$\mathcal{C}_{D-M}(A) \subset \mathcal{C}_{R-M}(A) \quad (25)$$

and

$$\mathcal{C}_{D-A}(A) \subset \mathcal{C}_{R-A}(A). \quad (26)$$

If we combine (23), (24), and (25), we find that

$$\mathcal{C}_{R-M}(A) = \mathcal{C}_{R-A}(A) = \mathcal{C}_{D-M}(A).$$

Furthermore, if we combine (24), (22), and (26), we find that

$$\mathcal{C}_{R-A}(A) = \mathcal{C}_{D-M}(A) = \mathcal{C}_{D-A}(A).$$

Hence,

$$\mathcal{C}_{R-M}(A) = \mathcal{C}_{R-A}(A) = \mathcal{C}_{D-M}(A) = \mathcal{C}_{D-A}(A). \quad (27)$$

2.4. Capacity Regions

The **capacity region** under a given probability-of-error criterion and under a constraint (if any) is the set of all achievable rates under the corresponding definition. As we have shown, the four capacity regions above are all the same. We just do not know what any of them is yet!

An important property of capacity regions is that they are **closed**. Suppose R_k is a sequence of achievable rates and that R_k converges to some R . We must show that the limit R is also achievable. Let $\Delta R > 0$ be given. Since $R_k \rightarrow R$, there is some k_0 such that for all $k \geq k_0$, $R_k > R - \Delta R/2$. Now, since R_{k_0} is achievable, there is a code with

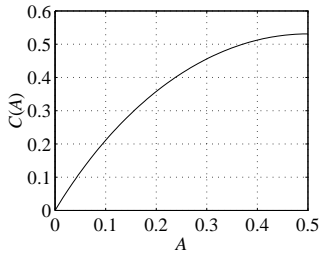
$$\frac{\log N}{n} > R_{k_0} - \Delta R/2,$$

satisfying the codeword constraint (if any), and having small probability of error. Since $R_{k_0} > R - \Delta R/2$, we also have

$$\frac{\log N}{n} > R - \Delta R.$$

Another important property of capacity regions is that if R is an achievable rate, then any $R' < R$ is also achievable. This follows from the fact that $R > R'$ implies

$$\frac{\log N}{n} > R - \Delta R > R' - \Delta R.$$

Figure 2. A typical capacity-cost function $C(A)$.

2.4.1. Capacity-Cost Functions

Let $\mathcal{C}(A)$ denote any of the four capacity regions in (27), and let $C(A)$ denote the supremum of $\mathcal{C}(A)$. Then $C(A)$ is called the **capacity under input constraint A** or it is called the **capacity-cost function**. From the foregoing observations, the capacity region is the interval

$$\mathcal{C}(A) = [0, C(A)].$$

As noted earlier (Section 1.11), for $A < A_{\min}$, no codeword can satisfy $a_n(\mathbf{x}) \leq A$. Hence, for such A there are no achievable rates, and the capacity region is empty. Although we may put $C_{\dots}(A) := -\infty$ when the capacity region is empty, we usually just restrict attention to $A \geq A_{\min}$. However, if X is an infinite set, it may happen that there is no $x \in X$ that achieves the infimum $A_{\min} := \inf_{x \in X} a(x)$. In this case, no codeword can satisfy $a_n(\mathbf{x}) \leq A_{\min}$ and the capacity region is empty. In these cases, it is understood that we would restrict attention to $A > A_{\min}$. Capacity-cost curves are always nondecreasing as shown in Fig. 2. This can be established mathematically as follows. From the definition of achievable rate, it is clear that $A_1 \leq A_2$ implies $\mathcal{C}(A_1) \subset \mathcal{C}(A_2)$, which then implies $C(A_1) \leq C(A_2)$. Hence, $C(A)$ is nondecreasing. We also point out that if $A_{\max} := \sup_{x \in X} a(x)$ is finite, then $C(A)$ becomes constant for large A ; in particular, for $A \geq A_{\max}$, $C(A) = C(A_{\max})$. This follows because, as noted in Section 1.11, if $A \geq A_{\max}$, then all codewords satisfy $a_n(\mathbf{x}) \leq A$.

2.5. Cost per Bit

If all codewords satisfy the constraint

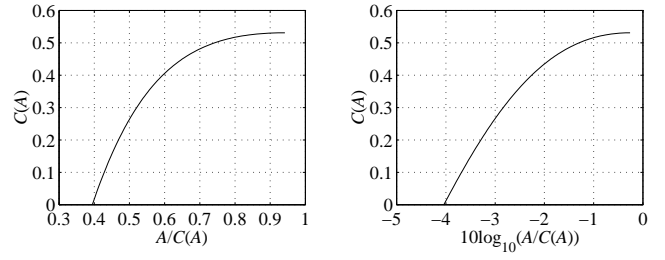
$$\frac{1}{n} \sum_{k=1}^n a(x_k) \leq A, \quad (28)$$

then the cost to send a message is at most $n \cdot A$. Since each message consists of $\log_2 N$ bits, we call

$$A_b := \frac{n \cdot A}{\log_2 N} = \frac{A}{R}, \quad \text{by (1),} \quad (29)$$

the average **cost per bit**. If $C(A)$ is the highest rate R at which we can reliably transmit messages using codewords that satisfy the constraint, then the average cost per bit is lower bounded by the **minimum average cost per bit** [4]

$$\mathcal{A}_{b,\min}(A) := \frac{A}{C(A)}. \quad (30)$$

Figure 3. Graph of parametric curve $(\mathcal{A}_{b,\min}(A), C(A))$ (left) and the parametric curve $(\mathcal{A}_{b,\min}^{\text{dB}}(A), C(A))$ (right) based on the capacity-cost function $C(A)$ in Fig. 2.

The parametric curve $(\mathcal{A}_{b,\min}(A), C(A))$ at the left in Fig. 3 shows the tradeoff between the minimum average cost per bit and the corresponding maximum reliable transmission rate using codewords that satisfy the constraint. To express the cost per bit in dB, put

$$\begin{aligned} \mathcal{A}_{b,\min}^{\text{dB}}(A) &:= 10 \log_{10} \mathcal{A}_{b,\min}(A) \\ &= 10(\log_{10} e) [\ln A - \ln C(A)]. \end{aligned}$$

We can then plot the new parametric curve $(\mathcal{A}_{b,\min}^{\text{dB}}(A), C(A))$ as shown at the right in Fig. 3. The slope of this curve at a point $(\mathcal{A}_{b,\min}^{\text{dB}}(A), C(A))$ is

$$\frac{\frac{d}{dA} C(A)}{\frac{d}{dA} \mathcal{A}_{b,\min}^{\text{dB}}(A)} = \frac{C'(A)}{10(\log_{10} e) \left[\frac{1}{A} - \frac{C'(A)}{C(A)} \right]}.$$

To compute the limiting slope as $A \rightarrow A_{\min}$ when $A_{\min} = 0$, we carefully write (cf. [2, p. 2517])

$$\begin{aligned} \lim_{A \rightarrow 0} \frac{1}{\frac{1}{A} - \frac{C'(A)}{C(A)}} &= \lim_{A \rightarrow 0} \frac{C(A)A}{C(A) - C'(A)A} \\ &= \lim_{A \rightarrow 0} \frac{C(A) + AC'(A)}{-C''(A)A}, \quad \text{by l'Hôpital's rule,} \\ &= -2 \frac{C'(0)}{C''(0)}. \end{aligned}$$

Hence,

$$\lim_{A \rightarrow 0} \frac{\frac{d}{dA} C(A)}{\frac{d}{dA} \mathcal{A}_{b,\min}^{\text{dB}}(A)} = \frac{-2C'(0)^2}{10(\log_{10} e)C''(0)}. \quad (31)$$

2.6. Waveform Channels and Spectral Efficiency

Given a set of messages $\{1, \dots, N\}$, suppose we associate corresponding signals $\xi_1(t), \dots, \xi_N(t)$ belonging to some finite-dimensional space spanned by orthonormal waveforms $\psi_1(t), \dots, \psi_n(t)$. Then every signal can be expressed in the form

$$\xi_i(t) = \sum_{k=1}^n x_{ik} \psi_k(t),$$

where

$$x_{ik} := \int \xi_i(t) \overline{\psi_k(t)} dt,$$

and the overbar denotes the complex conjugate if complex-valued waveforms are allowed. When transmitting signal $\xi_i(t)$, the receiver sees the waveform $Z(t)$; e.g., $Z(t) = \xi_i(t) + V(t)$, where $V(t)$ is additive white Gaussian noise (AWGN). In any case, we arbitrarily put $\mathbf{Y} := (Y_1, \dots, Y_n)$, where²

$$Y_k := \int Z(t) \overline{\psi_k(t)} dt, \quad k = 1, \dots, n.$$

When the waveforms ψ_i all have duration T , to transmit each message requires sending a signal ξ_i , which is equivalent to sending the n channel symbols $x_{i,1}, \dots, x_{i,n}$. Hence, we the number of channel uses per second (cf. eq. (2)) is

$$R_c = \frac{n}{T}.$$

It is convenient to *define* the **bandwidth** of the signals as [3, pp. 90–90]

$$B := n/(2T).$$

This implies

$$R_c = 2B.$$

With this substitution in (2), it follows that

$$\frac{R_b}{2B} = \frac{\log N}{n}.$$

The fraction on the left is called the **spectral efficiency**. It has units of bits per second per Hertz. From the right-hand side, we see that if there is an input constraint as in Section 2.5, then the maximum spectral efficiency of a reliable system is $C(A)$.

In waveform channels, there is usually a constraint on the average power (energy per second). For signals of duration T , this means

$$\frac{1}{T} \int_0^T |\xi_i(t)|^2 dt \leq P.$$

By Parseval's formula,

$$\int_0^T |\xi_i(t)|^2 dt = \sum_{k=1}^n |x_{ik}|^2.$$

Hence, if we take $a(x) := x^2$, then³ the power constraint says that each codeword $\mathbf{x}_i = (x_{i,1}, \dots, x_{i,n})$ must satisfy

$$a_n(\mathbf{x}_i) = \frac{1}{n} \sum_{k=1}^n a(x_{ik}) \leq \frac{PT}{n} = \frac{PT}{2BT} = \frac{P}{2B} =: A.$$

Hence, for fixed power constraint P , every operating point $(\mathcal{A}_{b,\min}^{\text{dB}}(A), C(A))$ on the parametric curve corresponds to a different bandwidth B . In particular, for large B (“the wide-band regime” [5]), the slope of the parametric curve is well approximated by (31). In fact, since the parametric curve $(\mathcal{A}_{b,\min}^{\text{dB}}(A), C(A))$ describes the capacity C as a function of the

minimum average cost per bit in dB, denoted by α , we have the linear approximation

$$C \approx \frac{-2C'(0)^2}{10(\log_{10} e)C''(0)} (\alpha - \alpha_0),$$

where

$$\alpha_0 := \lim_{A \rightarrow 0} \mathcal{A}_{b,\min}^{\text{dB}}(A) = 10 \log_{10} \frac{1}{C'(0)}.$$

References

- [1] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
- [2] K. Liu, V. Raghavan, and A. M. Sayeed, “Capacity scaling and spectral efficiency in wide-band correlated MIMO channels,” *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2504–2526, Oct. 2003.
- [3] R. J. McEliece, *The Theory of Information and Coding*. Reading, MA: Addison-Wesley, 1977.
- [4] S. Verdú, “On channel capacity per unit cost,” *IEEE Trans. Inform. Theory*, vol. 36, no. 5, pp. 1019–1030, Sept. 1990.
- [5] S. Verdú, “Spectral efficiency in the wideband regime,” *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1319–1343, June 2002.

²In the case of AWGN, there is no loss of information in performing this operation; in general, we just do it as a practical signal processing operation.

³Note that for $a(x) = x^2$, $A_{\min} = 0$. If $A = 0$, then the only codeword that satisfies $a_n(\mathbf{x}) \leq A$ is the all zeros codeword. Hence, the only achievable rate with $A = 0$ is zero; thus, $C(0) = 0$.