Computation and Information

Before quantum computers

Contents

I Computation

II Information

1 Measures of information 9
1.1 Surprising information 9
1.2 Refresher on probability theory 10
1.3 Axiomatic derivation of entropy 11
1.4 Entropy 13
1.5 Joint entropy, conditional entropy and mutual information 14
1.6 Exercises 16
1.7 Solutions to selected exercises 17
1.8 Further reading 19

2 Data compression 21
2.1 Codes 21
2.2 Code length and fundamental limits 23
2.3 Huffman codes and their optimality 26
2.4 Exercises 29
2.5 Solutions to selected exercises 30
2.6 Further reading 30

3 Data transmission 31
3.1 The communications problem 31
3.2 Detection, correction and minimum distance 32
3.3 Refresher on linear algebra 35
3.4 Bounds on codes 36
3.5 Binary linear codes 37
3.6 Hamming codes 40
3.7 Channel capacity 41
3.7.1 Converse theorem for noisy channel coding 42
3.7.2 Achievability of the channel capacity 43
3.7.3 The capacity of some basic channels 43
3.8 Exercises 44
3.9 Solutions to selected exercises 44
3.10 Further reading 48
Bibliography 49
Index 51

Computation

Information

1 Measures of information 9

1.1 Surprising information
1.2 Refresher on probability theory
1.3 Axiomatic derivation of entropy
1.4 Entropy
1.5 Joint entropy, conditional entropy and mutual information
1.6 Exercises
1.7 Solutions to selected exercises
1.8 Further reading

2 Data compression 21

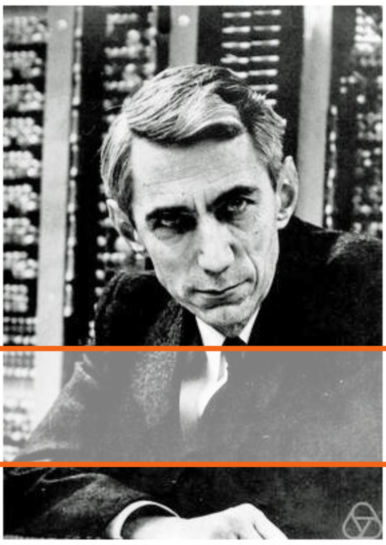
2.1 Codes
2.2 Code length and fundamental limits
2.3 Huffman codes and their optimality
2.4 Exercises
2.5 Solutions to selected exercises
2.6 Further reading

3 Data transmission 31

3.1 The communications problem
3.2 Detection, correction and minimum distance
3.3 Refresher on linear algebra
3.4 Bounds on codes
3.5 Binary linear codes
3.6 Hamming codes
3.7 Channel capacity
3.8 Exercises
3.9 Solutions to selected exercises
3.10 Further reading

Bibliography 49

Index 51



1. Measures of information

This is the age of information. We open documents, consume media, exchange text messages, perform videoconferences or watch the weather forecast to name a few examples. But what is exactly information? Can we quantify it? Is it possible to say that one weather forecast contains more information than another? In this chapter, we will learn that this is indeed possible.

1.1 Surprising information

Let us warm up with a series of questions. The premise of all of them is the following: For some reason you want to know the weather forecast for tomorrow, but don't want to watch it or read it yourself. However, in order to get some information that allows you to choose appropriately your clothing for the next day, you ask a friend to send you a message to your phone every night with a summary of the forecast. You agree on a very simple encoding for the message, your friend will send a 1 if the forecast predicts precipitations and 0 otherwise. Think about these questions and come back to them after reading the whole chapter.

Location	**Days with no rain**	**Days with rain**
Rotterdam	212	153
Atacama desert	360	5

Table 1.1: Summary of precipitations in the year 2018.

Exercise 1.1 Let us assume that you are living in the Atacama desert where it rarely rains. You receive a 0. How much information does this message carry? ■

Exercise 1.2 Now let us assume that you live in the Netherlands where it does rain quite often, but certainly not every day. You receive a 0. Does the message contain information? What about if you receive a 1? Does the 1 message contain more or less information than the message 0? ■

Exercise 1.3 Finally, let us assume that you live in the Netherlands but (boldly) also that you are aware of the current season. You receive a 0. Does the message 0 carry the same information in summer and in winter? ■

Before you continue reading, pause for a moment and think what is common in your answers.

We have posed these questions to suggest a relation between the amount of information a message provides and how surprising it is. We will make this connection stronger in the rest of these chapter.

1.2 Refresher on probability theory

A basic understanding of probability theory is essential for the material that follows. Let us review the fundamental concepts and definitions together with the notation that we will use here. As we will only deal with discrete probability distributions, the definitions that follow are not fully general but sufficient for our purposes. If you have troubles following this section and doing the exercises please go back to your undergraduate text on the topic.

Given a finite set $\mathscr{X}$, we call a probability distribution a function $p : \mathscr{X} \to [0,1]$, that is a function from the elements of $\mathscr{X}$ to the closed interval in the real line between zero and one, with the condition that $\sum_{x\in\mathscr{X}} p(x) = 1$. Note that it follows automatically from our definition that for all $x \in \mathscr{X}$ $p(x) \geq 0$.

■ **Example 1.1** Let $\mathscr{X} = \{\text{tails}, \text{heads}\}$ we could define a probability distribution function p such that $p(\text{heads}) = 0.3$ and $p(\text{tails}) = 0.7$. ■

■ **Example 1.2** An important example is the uniform distribution. Given a finite set $\mathscr{X}$, a uniform distribution on the set $\mathscr{X}$ is a function p that for all $x \in \mathscr{X}$ assigns the value

$$p(x) = \frac{1}{|\mathscr{X}|} .$$

where, we denote by $|\cdot|$ the number of elements in the set. ■

We define an ensemble X as the tuple of a probability distribution p_X together with its domain $\mathscr{A}_X$. Generally, we will refer to $\mathscr{A}_X$ as the sample space of X and to its elements as events. In information theory, X typically models an object in a communications setup (see 3.1), in this context it is common to call $\mathscr{A}_X$ the alphabet of X and refer to its elements as letters.

Note that we can extend the definition of p_X to any subset $\mathscr{S} \subseteq \mathscr{A}_X$:

$$p_X(\mathscr{S}) = \sum_{x\in\mathscr{S}} p_X(x) \tag{1.1}$$

■ **Example 1.3** Let X be an ensemble with alphabet $\mathscr{A}_X = \{1,2,3\}$ and with p_X the uniform distribution. Then if $\mathscr{S} = \{1,2\}$, $p(\mathscr{S}) = 1/3 + 1/3 = 2/3$ ■

Abusing notation, we will also call event any subset of the alphabet of an ensemble. For this particular case of set we will drop the calligraphic notation for sets. Let a and b be two events in $\mathscr{X}$, we define $a \cup b$ and $a \cap b$ as the union and intersection of a and b. $a \cup b$ is the event that contains all outcomes belonging to a, to b and to both, we will also denote the event $a \cup b$ by a or b. $a \cap b$ is the event that contains all outcomes belonging to both a and b, we will also denote the event $a \cap b$ by a and b. Two events are disjoint if their intersection is null.

Given an ensemble X and two events a, b we say that they are independent if:

$$p_X(a \text{ and } b) = p_X(a)p_X(b) \tag{1.2}$$

Let a and b be two events with non zero probability. We call $p_X(a|b) = p_X(a \text{ and } b)/p_X(b)$ the conditional probability of a given that b occurs. It follows that if and only if a and b are independent $p_X(a|b) = p_X(a)$.

In the following, we will use the explicit notation $p_X, \mathscr{A}_X$ for the probability distribution of ensemble X and its alphabet whenever confusion can arise but we will drop the subscript whenever possible.

Exercise 1.4 Let X be an ensemble modelling two fair coins. Identify two events a, b that are independent and verify that $p_X(a|b) = p_X(a)$ ■

Given two alphabets $\mathscr{A}_X, \mathscr{A}_Y$ we can define a joint ensemble on them with sample space or alphabet the direct product: $\mathscr{A}_{XY} = \mathscr{A}_X \times \mathscr{A}_Y$. We can associate, as well, a probability distribution function to map all tuples (x,y) to $[0,1]$.

The probability of an event in the joint ensemble is equally defined as the sum of the probability of the individual events. In particular, we can define for every $x \in \mathscr{X}$ the probability of $p_X(x)$ as the sum of $p_{XY}(x,y)$ for all $y \in \mathscr{Y}$:

$$p_X(x) = \sum_y p_{XY}(x,y) \tag{1.3}$$

and equivalently $p_Y(y)$:

$$p_Y(y) = \sum_x p_{XY}(x,y) \tag{1.4}$$

■ **Example 1.4** Consider n repetitions of an experiment, each repetition can be modelled by ensemble X and events in different experiments are independent. We can model the set of n repetitions via the joint ensemble $X_1 \dots X_N$, where X_i is the ensemble associated with the i-th experiment, and joint the probability distribution is given by:

$$p_{X_1 \dots X_N}(x_1, x_2, \dots, x_n) = \prod_{i=1}^{n} p_X(x_i) \tag{1.5}$$

■

A random variable V on the ensemble X is a numerical function from the elements of $\mathscr{A}_X$ to (typically) the real line. That is, a function $V : \mathscr{A}_X \to \mathscr{A}_V$, where $\mathscr{A}_V$ is a finite subset of the reals. The random variable V induces an ensemble with alphabet $\mathscr{A}_V$ and probability distribution p_V where p_V is given by:

$$p_V(v) = \sum_{x \in \mathscr{A}_X : V(x) = v} p_X(x) \tag{1.6}$$

for all $v \in \mathscr{A}_V$.

The mean or expectation of a random variable is given by:

$$\mathbb{E}[V] = \sum_{x \in \mathscr{A}_X} p_X(x) V(x) = \sum_{v \in \mathscr{A}_V} p_V v \tag{1.7}$$

1.3 Axiomatic derivation of entropy

Let us now try to understand what type of functions can quantify information in a satisfactory way. Let us make this investigation more precise. In particular, suppose that given some ensemble X we observe the occurrence of an event $x \in \mathscr{A}_X$. As we informally argued in the introduction, the information we gain seems to be related to the likelihood of the event we observed. But how can we make this intuition quantitative?

A function that quantifies information will be a function from a subset of $\mathscr{A}_X$ to the reals. Let us call this function h. Then given some event x, $h(x)$ will be some number that will quantify the information we learn. Let us discuss what properties an ideal information quantifier should have.

- The measure should be non-negative, that is, an event gives either none or some information, but it can not give negative information. That is, for all events $x \in \mathscr{A}_X$ we require:

$$h(x) \geq 0 \tag{1.8}$$

- Suppose that we buy two lottery tickets in two different lottery games, event x is: "our first ticket wins a prize", event y is: "our second ticket does not win a prize". We expect these two events to be independent and the information content of knowing both events should be the sum of the information of the individual events. The occurrence of two independent events should yield the same information that the occurrence of the single events would provide an observer. If we let h be an information measuring function

$$p_X(x \text{ and } y) = p_X(x)p_X(y) \Rightarrow h(x \text{ and } y) = h(x) + h(y) \tag{1.9}$$

- Following our discussion about information and surprise, we want h to quantify less probable events with a larger value than more probable events. For any two ensembles X, Y and events $x \in \mathscr{A}_X$ and $y \in \mathscr{A}_Y$, we require:

$$p_X(x) < p_Y(y) \Rightarrow h(x) > h(y) \tag{1.10}$$

- The final condition is that we don't want that arbitrarily small changes in probability lead to a change in the information quantity, i.e. h should be a continuous function.

It turns out that there is a very limited set of functions that verify these properties. Given some ensemble X, the unique family of functions is of the form:

$$h(x) = -\log_\lambda p_X(x) \tag{1.11}$$

where $x \in \mathscr{A}_X$ and with $\lambda > 1$ for the measure to be positive. Choosing different values of λ allows us to measure information with different units.

There are some common choices of λ that give rise to well known units of information: if we let $\lambda = 2$, the unit of information is called bit. When $\lambda = 3$ information is measured in trits, for $\lambda = 10$ the unit is called a digit and when $\lambda = e$ nat. Unless stated otherwise, in the following we will assume that $\lambda = 2$ and will let $\log = \log_2$.

Definition 1.3.1 Given an ensemble X the information measured in bits of an event $S \subset \mathscr{A}_X$ is given by:

$$h(\mathscr{S}) = -\log p_X(\mathscr{S}) \tag{1.12}$$

Exercise 1.5 Let X be an ensemble modelling a fair coin, that is with alphabet $\mathscr{A}_X = \{\text{heads}, \text{tails}\}$ and with p_X the uniform distribution. What is the information of the event heads and of the event tails? ■

Let us end this section by checking that all our desired conditions hold. First since the log function is continuous and monotonically increasing in the range $(0, 1]$ it holds that h is also continuous and monotonically decreasing in the range. Finally, if two events a, b are independent,

$p(a \text{ and } b) = p(a)p(b)$ and in consequence

$$\begin{aligned} h(a \text{ and } b) &= -\log\left(p(a \text{ and } b)\right) && (1.13)\\ &= -\log\left(p(a)p(b)\right) && (1.14)\\ &= -\log(p(a)) - \log(p(b)) && (1.15)\\ &= h(a) + h(b) && (1.16) \end{aligned}$$

1.4 Entropy

We define the entropy of an ensemble as the average information content it provides:

Definition 1.4.1 Let X be an ensemble, the entropy of the ensemble is defined as:

$$H(X) = -\sum_x p(x)\log p(x) \tag{1.17}$$

where we take the convention that $0\log 0 = 0$, i.e. adding a zero-probability event to a probability distribution does not affect its entropy.

We can rewrite the definition of entropy as the expectation of the random variable $h(X)$. That is a random variable that associated each event with the negative logarithm of its probability:

$$H(X) = -\sum_x p(x)\log p(x) = E(-\log p(X)) \tag{1.18}$$

Note that entropy only depends on the values of the probabilities. In the following we will sometimes be interested in the entropy a probability distribution independently of an ensemble. We will use the notation $H(p_1,\ldots,p_n)$ to indicate the probability distribution. Let us now investigate some basic properties of entropy that we will use through this course.

Exercise 1.6 Show that entropy can not be negative.

$$H(X) \geq 0$$

■

Definition 1.4.2 A function $f(x) : (a,b) \mapsto \mathbb{R}$ is concave if any two points $x_1, x_2 \in (a,b)$ and any $p \in [0,1]$ verify:

$$f(px_1 + (1-p)x_2) \geq pf(x_1) + (1-p)f(x_2) \tag{1.19}$$

■ **Example 1.5** Some examples of concave functions are $-x^2$, $-x^4$, cosine is concave in the interval $[-\pi/2, \pi/2]$ and the logarithm function. To prove the concavity of these functions, you might recall from your calculus course that if a function is twice differentiable in the interval of interest, then it is concave if and only if the second derivative is non-negative. ■

The following is known as Jensen's inequality and will be of use in the following.

Theorem 1.4.1 — Jensen's inequality. Let $f(x) : (a,b) \mapsto \mathbb{R}$ be a concave function. Then for any set of points $\{x_i\}_{i=1}^n \in (a,b)$ and for any set of positive real numbers $\{p_i\}_{i=1}^n$ such that

$\sum_{i=1}^{n} p_i = 1$:

$$f\left(\sum_{i=1}^{n} p_i x_i\right) \geq \sum_{i=1}^{n} p_i f(x_i)$$

Proof. If $n = 2$, the proof follows by the definition of concavity. We will complete the proof by induction. Let us suppose that it holds for $n = m$:

$$f\left(\sum_{i=1}^{m} p_i x_i\right) \geq \sum_{i=1}^{m} p_i f(x_i) \tag{1.20}$$

and let us show that it implies that it also holds for $n = m+1$. Let

$$x' = \sum_{i=1}^{m} \frac{p_i}{1-p_{m+1}} x_i \tag{1.21}$$

Then we have from the definition of concavity that:

$$f\left(\sum_{i=1}^{m+1} p_i x_i\right) = f((1-p_{m+1}x' + p_{m+1}x_{m+1}) \tag{1.22}$$

$$\geq (1-p_{m+1})f(x') + p_{m+1}f(x_{m+1}) \tag{1.23}$$

Finally from the induction hypothesis (1.20) we have that:

$$f(x') = f\left(\sum_{i=1}^{m} \frac{p_i}{1-p_{m+1}} x_i\right) \tag{1.24}$$

$$\geq \sum_{i=1}^{m} \frac{p_i}{1-p_{m+1}} f(x_i) \tag{1.25}$$

which we can plug in back in (1.23) to complete the proof. ■

Exercise 1.7 The distribution that maximizes entropy for any alphabet is the uniform distribution.

$$H(p_1, ..., p_n) \leq \log n$$

■

1.5 Joint entropy, conditional entropy and mutual information

We will now explore three information measures that derive from entropy as we defined it in the previous section. The first measure is joint entropy, which is a direct application of the definition of entropy to a joint source.

Definition 1.5.1 Given two ensembles X and Y the entropy of the joint ensemble XY is given by:

$$H(XY) = -\sum_{x,y} p(x,y) \log p(x,y) \tag{1.26}$$

Exercise 1.3 suggests that the information content depends on the context. The second information measure that we introduce is conditional entropy. First, we can extend in a straightforward way the reasoning in Sec. 1.3 to define an information measure conditional on the knowledge of some event y. It can analogously be proved that a conditional information measure is of the form:

$$h(a|b) = -\log p(a|b) \tag{1.27}$$

Let XY be a joint ensemble, we can define the conditional entropy of X given the event y as the average conditional information:

$$H(X|y) = \sum_x p(x|y)h(x|y) \tag{1.28}$$

and the conditional entropy of X given ensemble Y:

$$H(X|Y) = \sum_y H(X|y) \tag{1.29}$$

Exercise 1.8 Show that $H(X|Y) = H(XY) - H(Y)$. ■

Let us investigate some basic properties of the conditional entropy.

Exercise 1.9 Show that the conditional entropy is non-negative.

$$H(X|Y) \geq 0$$

■

Exercise 1.10 Let X, Y be two random variables. Show that:

$$H(X|Y) \leq H(X)$$

■

Exercise 1.11 Given random variables X and Y if $X = f(Y)$:

$$H(X|Y) = 0$$

■

Exercise 1.12 Show that the following relation holds for any two ensembles XY:

$$H(XY) = H(X) + H(Y|X)$$

■

The third information measure that we introduce is the mutual information:

Definition 1.5.2 Given a joint ensemble XY, we define the mutual information between X and Y by:

$$I(X;Y) = H(X) + H(Y) - H(XY)$$

The mutual information $I(X;Y)$ is a measure of the information shared between the two variables X and Y. Let us make this intuition more precise:

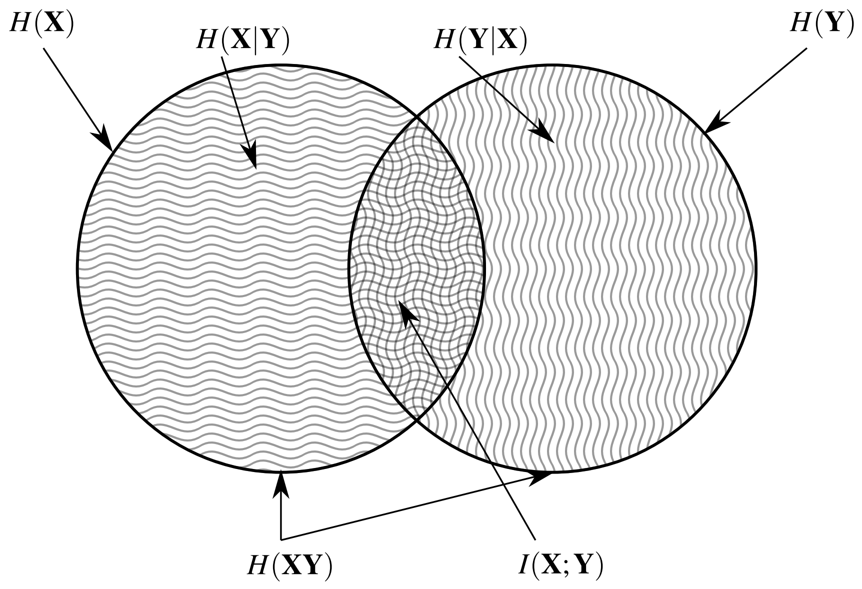

$H(\mathbf{X})$
$H(\mathbf{X}|\mathbf{Y})$
$H(\mathbf{Y}|\mathbf{X})$
$H(\mathbf{Y})$
$H(\mathbf{XY})$
$I(\mathbf{X};\mathbf{Y})$

Figure 1.1: Graphical representation of the information measures.

Exercise 1.13 Show that for any ensemble X: $I(X;X) = H(X)$. ■

Exercise 1.14 Show that $I(X;Y) = 0$ if and only if X and Y are independent. ■

Exercise 1.15 Show that $I(X;Y) \geq 0$ ■

Fig. 1.1 shows the relationship between the four measures that we have defined: entropy, joint entropy, conditional entropy and mutual information.

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H(X) - H(X|Y) \\ &= I(Y;X) \end{aligned} \tag{1.30}$$

1.6 Exercises

Exercise 1.16 Let X be a random variable with $H(X) > 0$ and let $Y = f(X)$.

1. Give one function such that $H(Y) = H(X)$
2. Give one function such that $0 < H(Y) < H(X)$
3. Give one function such that $H(Y) = 0$

■

Exercise 1.17 A classic logical problem (also classic in information theory texts!) states that you receive 12 coins one of which is a counterfeit. The counterfeit is either lighter or heavier than the normal coins, you do not know which is the case. Fortunately, you have access to a two-plate scale that can compare weights.

1. Give a non-trivial bound on the minimum number of weighings that could give the answer.

2. Give an strategy that solves the problem if you know tha the counterfeit coin is heavier than normal coins.
3. Give an strategy that solves the general problem. (difficult)

■

Exercise 1.18 Let X_1, X_2 be two independent random variables modelling two different but otherwise indistinguishable bent coins. Let Y be a binary random variable that models a process where we throw X_1 with probability t and X_2 with probability $1-t$. Show that $H(Y) \geq tH(X_1) + (1-t)H(X_2)$. ■

Exercise 1.19 Let X_1, X_2 be two independent random variables modelling two different bent coins from two different countries, i.e. the outcomes can be clearly distinguished. Let Y be a binary random variable that models a process where we throw X_1 with probability t and X_2 with probability $1-t$. Show that $H(Y) = H(t, 1-t) + tH(X_1) + (1-t)H(X_2)$. ■

1.7 Solutions to selected exercises

Solution. [Exercise 1.5] As p_X is uniform, we have that $p(\text{heads}) = p(\text{tails}) = 1/2$. Hence:

$$h(\text{heads}) = -\log(1/2) = 1 \text{ bit}$$

and

$$h(\text{heads}) = -\log(1/2) = 1 \text{ bit} .$$

■

Solution. [Exercise 1.6]

$$0 \leq p(x) \leq 1 \Rightarrow -\log p(x) \geq 0 \Rightarrow H(X) \geq 0 \tag{1.31}$$

■

Solution. [Exercise 1.7]

$$\begin{aligned}
H(p_1, \dots, p_n) - \log n &= \sum_{i=1}^{n} p_i \log \frac{1}{p_i} - \sum_{i=1}^{n} \frac{1}{n} \log n \\
&= \sum_{i=1}^{n} p_i \log \frac{1}{p_i} - \log n \sum_{i=1}^{n} \frac{1}{n} \\
&= \sum_{i=1}^{n} p_i \log \frac{1}{p_i} - \log n \sum_{i=1}^{n} p_i \\
&= \sum_{i=1}^{n} p_i \log \frac{1}{p_i} - \sum_{i=1}^{n} p_i \log n \\
&= \sum_{i=1}^{n} p_i \log \frac{1}{n p_i} \\
&\leq \log \sum_{i=1}^{n} \frac{1}{n} = 0
\end{aligned} \tag{1.32}$$

where the second equality follows from the fact that a probability distribution adds up to one and the last inequality holds from log being a concave function and applying Jensen's inequality. ■

Solution. [Exercise 1.9] $H(X|Y)$ is a sum of entropies, which are positive as we proved in Exercise 1.6, weighed by the probabilities of each event which are also positive. ■

Solution. [Exercise 1.10]

$$\begin{aligned}
H(X|Y)-H(X) &= \sum_y p(y)\sum_x p(x|y)\log\frac{1}{p(x|y)} - \sum_x p(x)\log\frac{1}{p(x)} \\
&= \sum_y\sum_x p(x,y)\log\frac{1}{p(x|y)} + \sum_{x,y} p(x,y)\log p(x) \\
&= \sum_{x,y} p(x,y)\log\frac{p(x)}{p(x|y)} \\
&= \sum_{x,y} p(x,y)\log\frac{p(x)p(y)}{p(x,y)} \\
&\leq \log\sum_{x,y} p(x)p(y) = 0 \qquad (1.33)
\end{aligned}$$

■

Solution. [Exercise 1.11]

If $X=f(Y)$, then given Y we know X with absolute certainty, in other words, given Y there is just one possible outcome.

$$\begin{aligned}
H(X|Y) &= \sum_y p(y)H(X|y) \\
&= 0 \qquad (1.34)
\end{aligned}$$

■

Solution. [Exercise 1.12]

$$\begin{aligned}
H(XY) &= -\sum_{x,y} p(x,y)\log p(x,y) \\
&= -\sum_x p(x)\sum_y p(y|x)\log p(x)p(y|x) \\
&= -\sum_x p(x)\log p(x)\sum_y p(y|x) \\
&\quad -\sum_x p(x)\sum_y p(y|x)\log p(y|x) \\
&= H(X)+H(Y|X) \qquad (1.35)
\end{aligned}$$

■

Solution. [Exercise 1.19] Since X_1 is chosen with probability t we have that for a symbol $x_1\in\mathscr{X}_1$, the probability $p_Y(x_1)=tp_{X_1}(x_1)$. Similarly for X_2, we have that for a symbol $x_2\in\mathscr{X}_2$ the probability $p_Y(x_2)=(1-t)p_{X_2}(x_2)$. With this observation, let us expand $H(Y)$:

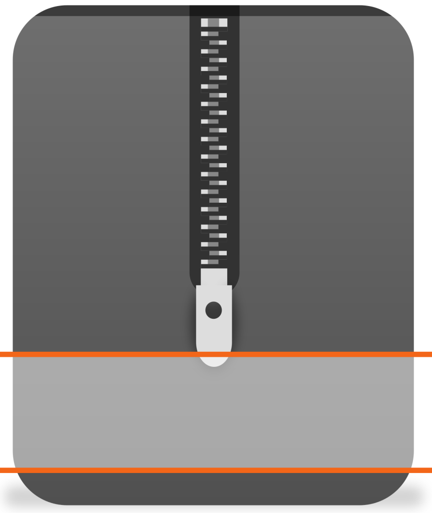
$$\begin{aligned}
H(Y) &= -\sum_y p_Y(y)\log p_Y(y) \\
&= -\sum_{x_1\in\mathscr{X}_1} tp_{X_1}(x_1)\log(tp_{X_1}(x_1)) - \sum_{x_2\in\mathscr{X}_2} tp_{X_2}(x_2)\log(tp_{X_2}(x_2)) \\
&= -t\sum_{x_1\in\mathscr{X}_1} p_{X_1}(x_1)\left(\log(t)+\log(p_{X_1}(x_1))\right) - (1-t)\sum_{x_2\in\mathscr{X}_2} p_{X_2}(x_2)\left(\log(1-t)+\log(p_{X_2}(x_2))\right) \\
&= -t\log t + tH(X_1) - (1-t)\log(1-t) + (1-t)H(X_2) \\
&= H(t,1-t) + tH(X_1) + (1-t)H(X_2)
\end{aligned}$$

■

1.8 Further reading

The mathematical foundations of information theory were to a certain extent developped single handedly by Claude Shannon. His original paper [16] developped the framework and also solved some of the most important problems. The text has not aged with time and remains a greatly written and accessible introduction to the field. A second excellent source for digging deeper into the material is the book of Cover and Thomas [3], it is the reference of the field and widely used in most introductory courses on information theory. Similar to Cover and Thomas but with a more informal treatment, the book of MacKay [12] is also a recommended source. Chapter 2 in both [3] and [12] develop in depth the material of this chapter.

In section 1.3 we sketched an axiomatic derivation of entropy. For a complete discussion on axiomatic derivations of entropy and information please refer to [1, 2, 4, 7].



2. Data compression

In the previous chapter we posed a series of conditions that information measures should possess. We built on top of those conditions and found a series of information measures satisfying them.

In this chapter we will begin a journey to show that not only entropy is a good measure for information according to our desired properties, but also that it carries a strong operational meaning. In fact, we will show that matching our intuition, if an ensemble has a certain entropy, then the length of a message that can communicate the content of the ensemble can not be smaller the entropy of then ensemble.

2.1 Codes

Definition 2.1.1 A symbol code is a map $C : \mathscr{A} \mapsto \mathscr{C}^*$. We associate every symbol a from the alphabet $\mathscr{A}$ with $C(a)$ a sequence of symbols from the code alphabet $\mathscr{C}$. We call $C(a)$ the codeword of a and denote by $|C(a)|$ its length.

■ **Example 2.1** Let X be an ensemble modelling a fair coin. We can consider the codes C_1, C_2 on the ensemble with:
$C_1(\text{tails}) = 00$ and $C_1(\text{heads}) = 111$ $C_2(\text{tails}) = 0$ and $C_2(\text{heads}) = 0$ $C_3(\text{tails}) = 00$ and $C_2(\text{heads}) = 0$ ■

You have probably noticed that the code C_2 in the previous example is not very useful. This consideration motivates the following definitions.

Definition 2.1.2 A code $C : \mathscr{X} \mapsto \mathscr{Y}$ is non-singular if $\forall x, y \in \mathscr{X}$ with $x \neq y$ $C(x) \neq C(y)$.

If we receive a single symbol encoded with a non-singular code, correct decoding is guaranteed, all codewords are different. However, we might consider the use of a code for sending a sequence of symbols from some ensemble. Let X be an ensemble, C be a code on the ensemble and $x = (x_1, \dots, x_n) \in \mathscr{X}^*$ a sequence of elements of $\mathscr{X}$ with finite length. We can extend the definition of C and define its action on x as follows: $C(x) = C(x_1)C(x_2)\dots C(x_n)$. That is, the word associated with x is the concatenation of the codewords for x_1, x_2 until x_n. Under this extended definition, some non-singular codes can lead to erroneous decodings. For instance, consider the code C_3 in the previous example and the word 000. It can be decoded both as (tails,heads) or as (heads,tails).

Definition 2.1.3 A code $C : \mathscr{X} \mapsto \mathscr{Y}$ is uniquely decodable if $\forall x, y \in \mathscr{X}^*$ with $x \neq y$ $C(x) \neq C(y)$.

If we think in the usefulness of a code, unique decodability is a basic requirement. A more practical requirement is that it should be possible to decode symbols as one reads a word instead of waiting until the end of the transmission. A code is called instantaneous if it can be decoded symbol by symbol from left to right without regarding future symbols.

A convenient family of instantaneous codes are so called prefix codes. Before defining them, let $w_1, w_2 \in D^*$, w_1 is a prefix of w_2 if there exist $t \in D^*$ such that w_1 concatenated with t equals w_2. That is: $w_1, t = w_2$.

Definition 2.1.4 A prefix code is a code where no codeword is the prefix of any other codeword.

It is easy to see that prefix codes are instantaneous, indeed as soon as a complete codeword is seen, it is possible to decode the associated symbol. Since the codeword can not be prefix of a subsequent codeword, there is no possibility of confusion. Moreover, it turns out that all instantaneous codes are also prefix, i.e. both concepts are equivalent. In order to prove this, we can argue the contrapositive.

Let C be a non-prefix code and let's see that it implies it is not instantaneous. If C is non prefix there exist codewords w_1, w_2 and t such that $w_1, t = w_2$. Hence, if we receive w_1 we can not decode until additional symbols are received that allow to discriminate between w_1 and w_2.

Exercise 2.1 Let $w_1, w_2 \in D^*$, w_1 is a suffix of w_2 if there exist $t \in D^*$ such that t concatenated with w_1 equals w_2. We call a code a suffix code if no codeword is suffix of any other code word.

1. Are all suffix codes also prefix codes? If yes, prove it. If not, give a counterexample.
2. Are suffix codes uniquely decodable?
3. Are suffix codes instantaneous?

■

In the previous example, it was fairly easy to spot that the code was not uniquely decodable. However, for some codes it is not so simple.

Exercise 2.2 Let $C_1 = \{01, 100, 1101, 0111\}$ and $C_2 = \{01, 100, 1101, 10111, 01011\}$. Are C_1, C_2 uniquely decodable? (Hint: if you can not find the solution, continue reading and return to this exercise once you have understood the Sardinas-Patterson method) ■

Let us now investigate a method to find if a code is uniquely decodable or not. This method was proposed by Sardinas and Patterson [15] and is also known as the method of the dangling suffixes.

The method works as follows:

1. Let C_0 be the set of codewords in the code
2. Let $C_1 = \{w \in \mathscr{A}^* : uw = v, \text{ where } u, v \in C_0\}$.
3. For $n \geq 2$ do:
   (a) Let $C_n = \{w \in \mathscr{A}^* : uw = v, \text{ where } u \in C_0, v \in C_{n-1} \text{ or } u \in C_{n-1}, v \in C_0\}$.
   (b) If C_n is empty, the code is uniquely decodable
   (c) If there is $2 \leq m < n$ such that $C_m = C_n$, i.e. if C_n is a repeated set, then the code is uniquely decodable.
   (d) If the intersection between C_0 and C_n is non-empty. That is if there is some codeword in C_n. Then the code is not uniquely decodable.
   (e) Else we increase n.

This method is a little bit magical. Let us informally investigate some of its properties. One might wonder about two things. First, does the algorithm end for all codes? This first question is relatively straight forward if one observes that the sets C_n for $n \geq 2$ are always composed of suffixes of C_0. Since the number of possible suffixes is finite, the number of sets of suffixes is also finite. Hence at some point the algorithm will end. The second question is whether or not the output of the algorithm is correct. This is a little more complicated and beyond the scope of the course see [14] for more information.

2.2 Code length and fundamental limits

Definition 2.2.1 Given an ensemble X and a code C for this ensemble, we define the average length of the code as follows:

$$l(C) = \sum_{x \in \mathscr{X}} p(x)|C(x)| \tag{2.1}$$

where $|C(x)|$ is the length of the codeword of event x.

▪ **Example 2.2** Consider the codes C_1, C_2 for a fair coin. $C_1(\text{tails}) = 0$, $C_1(\text{heads}) = 10$, $C_2(\text{tails}) = 0$, $C_2(\text{tails}) = 1$. The average length of the codes is:

$$L(C_1) = \frac{1}{2}1 + \frac{1}{2}2 = 1.5 \tag{2.2}$$

$$L(C_2) = \frac{1}{2}1 + \frac{1}{2}1 = 1 \tag{2.3}$$

▪

Intuitively, it seems that we can not do better than C_2, how do we prove it? In the following we prove a fundamental relation between the length of a code and the entropy of the associated ensemble. Previous to that we need to prove Kraft-MacMillan's inequality. This inequality was first proved by McMillan [13] however the following proof is a simpler version by Karush [3, 10].

Theorem 2.2.1 The length of a uniquely decodable code C for a random variable X taking values in alphabet $\mathscr{Y}$ verifies:

$$\sum_x \frac{1}{|\mathscr{Y}|^{l(x)}} \leq 1$$

Proof. Let $c(x_1, x_2, ..., x_k)$ be a concatenation of codewords of aggregated length $l(x_1, x_2, ..., x_k) = \sum_{i=1}^{k} l(x_i)$. Since C is uniquely decodable for any aggregated length k, no more than $|\mathscr{Y}|^k$ different concatenation of codewords can be generated.

We can consider the related expression on the aggregated length:

$$\begin{aligned}
\left(\sum_x \frac{1}{|\mathscr{Y}|^{l(x)}}\right)^n &= \sum_{x_1} \frac{1}{|\mathscr{Y}|^{l(x_1)}} \sum_{x_2} \frac{1}{|\mathscr{Y}|^{l(x_2)}} \cdots \sum_{x_n} \frac{1}{|\mathscr{Y}|^{l(x_n)}} \\
&= \sum_{x_1, x_2, ..., x_n} \frac{1}{|\mathscr{Y}|^{l(x_1)+l(x_2)+\cdots+l(x_n)}} \\
&= \sum_{x_1, x_2, ..., x_n} \frac{1}{|\mathscr{Y}|^{l(x_1+x_2+\cdots+x_n)}}
\end{aligned} \tag{2.4}$$

which can also be written as the sum for all possible lengths i of the number T_i of concatenation of n codewords:

$$\begin{aligned}\left(\sum_x \frac{1}{|\mathscr{Y}|^{l(x)}}\right)^n &= \sum_{i=1}^{nl_{max}} \frac{T_i}{|\mathscr{Y}|^i} \\ &\leq \sum_{i=1}^{nl_{max}} \frac{|\mathscr{Y}|^i}{|\mathscr{Y}|^i} \\ &\leq nl_{max} \end{aligned} \tag{2.5}$$

where $l_{max} = \max_x l(x)$. And taking the n-th root in both sides:

$$\sum_x \frac{1}{|\mathscr{Y}|^{l(x)}} \leq (nl_{max})^{1/n} \tag{2.6}$$

now since the limit $\lim_{n\to\infty}(nl_{max})^{1/n} = 1$ and the result holds for all n:

$$\sum_x \frac{1}{|\mathscr{Y}|^{l(x)}} \leq 1 \tag{2.7}$$

■

The Kraft-MacMillan inequality is in a sense an if and only if condition. Given a set of lengths satisfying the inequality, there exists a code C with the same lengths that is a prefix code. Let us see how to construct this associated prefix code.

We first observe that any prefix code can be represented by a tree with each codeword represented by a leave of the tree. For example, consider the code $C = \{0, 10, 1100, 1101, 1110, 1111\}$ and its representation in figure 2.1.

Second, consider a set of lengths $\{l_1, \dots, l_n\}$ which we assume are ordered i.e. $l_1 \leq \dots \leq l_n$ and let us assume that this set verifies the Kraft-MacMillan inequality. We will construct the code by assigning to each codeword a number of leaves from a full binary tree of depth l_n. There are then a total of 2^{l_n} leaves to be assigned. The strategy will be to assign to codeword i $2^{l_n - l_i}$ leaves. We should verify that the number of leaves assigned is not larger than the total number of leaves in the tree. That is:

$$\sum_i 2^{l_n - l_i} \leq 2^{l_n}. \tag{2.8}$$

The inequality holds since if we divide both sides by 2^{l_n} we recover Kraft-MacMillan's inequality.

Finally, we proceed to assign the leaves in the tree to each codeword consecutively and from left to right. The assignment is done in order of length from the shortest to the longest codeword.

We can now show that the length of a uniquely decodable code is lower bounded by the entropy of the random variable.

Theorem 2.2.2 The length of a uniquely decodable code taking values from finite alphabet $\mathscr{Y}$ for random variable X is lower bounded by the entropy of X.

$$L \geq H_{|\mathscr{Y}|}(X)$$

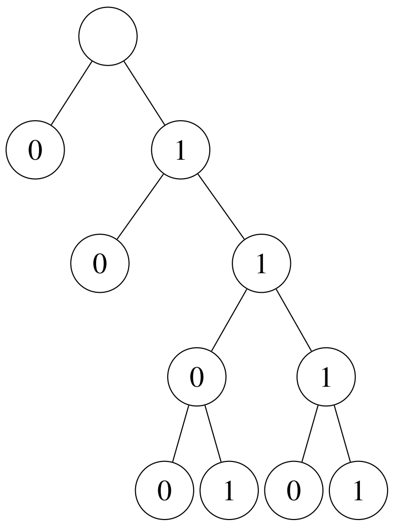


Figure 2.1: Binary tree representing the code $C = \{0, 10, 1100, 1101, 1110, 1111\}$.

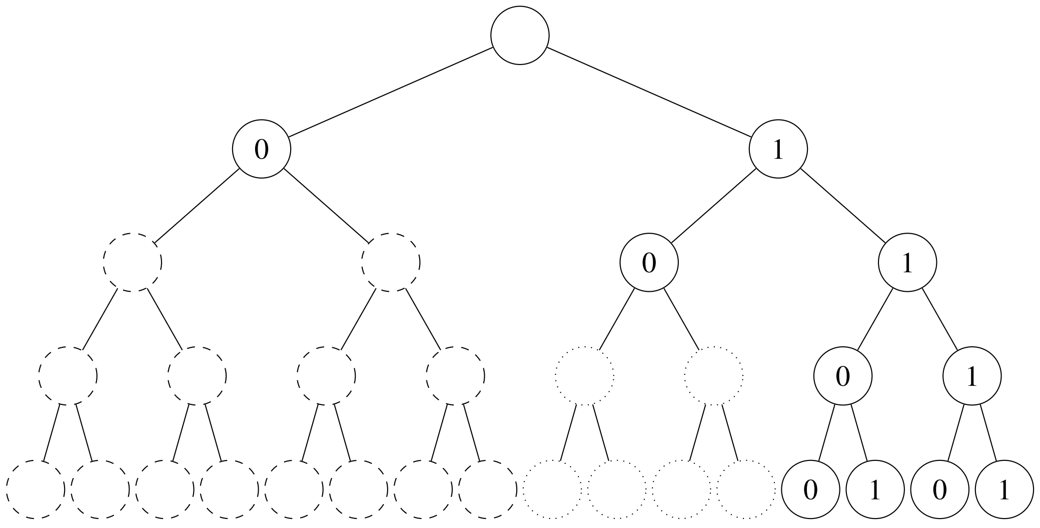


Figure 2.2: Construction of a prefix code from the set of lengths: $1, 2, 4, 4, 4, 4$.

Proof.

$$
\begin{aligned}
H_{|\mathscr{Y}|}(X) - L &= \sum_x p(x)\log_{|\mathscr{Y}|}\frac{1}{p(x)} - \sum_x p(x)l(x) \\
&= \sum_x p(x)\log_{|\mathscr{Y}|}\frac{1}{p(x)} - \sum_x p(x)\log_{|\mathscr{Y}|}|\mathscr{Y}|^{-l(x)} \\
&= \sum_x p(x)\log_{|\mathscr{Y}|}\frac{|\mathscr{Y}|^{-l(x)}}{p(x)} \\
&\le \log_{|\mathscr{Y}|}\sum_x |\mathscr{Y}|^{-l(x)} \\
&\le \log_{|\mathscr{Y}|} 1 = 0 \qquad (2.9)
\end{aligned}
$$

where the first inequality is again an application of Jensen's result Th. 1.4.1 and the second one results from applying McMillan's Th. 2.2.1. ■

One relevant question is: how far is the optimal code from the bound? In exercise 2.4 you will show that at most one bit! Let us first introduce some notation.

Definition 2.2.2 We use the notation $\lceil\rceil$ and $\lfloor\rfloor$ to indicate the rounding "up" and "down" of a real number to the closest integer value. More precisely, let $x \in \mathbb{R}$:

$$\lceil x \rceil = \min\{n \in \mathbb{N} : n \ge x\} \qquad (2.10)$$

$$\lfloor x \rfloor = \max\{n \in \mathbb{N} : n \le x\} \qquad (2.11)$$

■ **Example 2.3** $\lceil 0.3 \rceil = 1, \lfloor 0.3 \rfloor = 0, \lceil -0.3 \rceil = 0$ and $\lfloor -0.3 \rfloor = -1$. ■

Exercise 2.3 Let $p \in (0,1)$, show that $-\lceil \log(1/p) \rceil = \lfloor \log p \rfloor$. ■

Exercise 2.4 Let X be an ensemble and consider a binary code C with lengths $l(C(x)) = \lceil \log 1/p_X(x) \rceil$ for all symbols $x \in \mathscr{X}$. Show that there exist a code C with the indicated lengths that satisfies:

$$H(X) \le L(C) \le H(X) + 1 \qquad (2.12)$$

■

2.3 Huffman codes and their optimality

We will now investigate a scheme that achieves the optimal encoding rate of an ensemble. The algorithm is remarkably simple and was discovered by Huffman [9] while a master student. Let us describe the algorithm.

Given an ensemble X and let C denote the Huffman code of X.

1. Let a, b be two symbols with smallest probability. Create ensemble X' identical to X but replacing a, b with a new symbol c that has probability $p_{X'}(c) = p_X(a) + p_X(b)$.
2. Let $C(a) = C(c)0$ and $C(b) = C(c)1$.
3. If X' has an alphabet with more than one symbol go back to 1.

A first observation on the algorithm is that computationally it is very simple. Since at each iteration there is one symbol less it will terminate in $|\mathscr{A}_X|$ iterations.

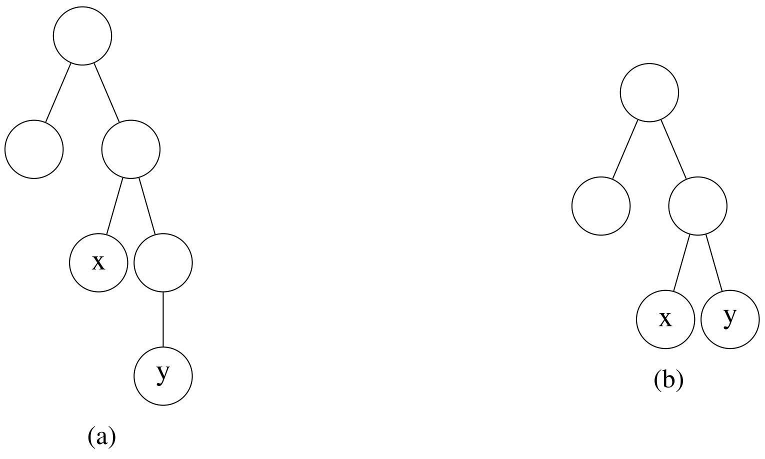


Figure 2.3: On the left we have an abstract representation of a code C where a,b, the two symbols with the longest codewords have different lengths. On the right we have the representation of a new code C' with the longest codeword trimmed.

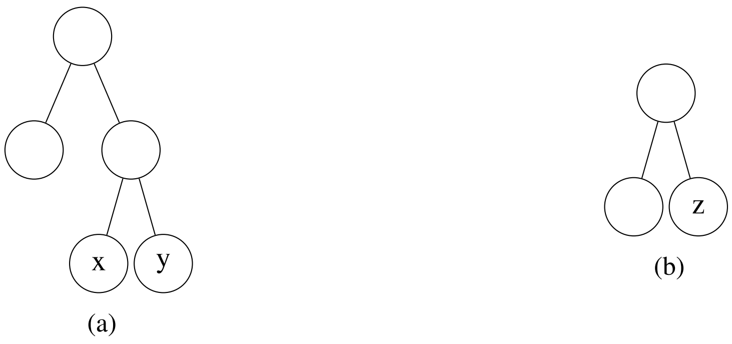


Figure 2.4: On the left we have an abstract representation of a code C where x,y, the two symbols with smallest probability have equal and maximum lengths differing only in the last bit value. On the right we have the representation of a new code C' without symbols x,y and with a new symbol z.

Exercise 2.5 Find the Huffman code of an ensemble X with symbols $\mathscr{A}_X = \{x_1,x_2,x_3,x_4,x_5,x_6\}$ and corresponding probabilities $p_X = \{0.3,0.2,0.18,0.15,0.12,0.05\}$. ■

The prove of optimality of Huffman codes is indirect. What we will prove is that no other code can have lower length based on some properties of the trees associated with Huffman codes. Our discussion is limited to binary trees, for the full discussion, please see the references in Section 2.6.

Lemma 2.3.1 If x,y are the two symbols with smallest probability, there exists an optimal code C where $C(x),C(y)$ are the longest codewords, have the same size and differ only in the last bit.

Proof. Consider the tree representation of any code C where the two longest words are of unequal size, i.e. $|C(a)| > |C(b)|$ where a,b are the symbols with longest codewords. Then we could construct a new code where we remove the last bits of codeword $C(b)$ until it has length $|C(a)$. The new code would be shorter. See Fig. 2.3 for a graphical representation. Let us then assume that the longest codewords are of the same length, but that at least one of a,b is different from x,y. Suppose that a is neither x or y and consider a new code C' where we swap $C(a)$ with $C(x)$. That is: $C'(a) = C(x)$ and $C'(x) = C(a)$. Now, we will show that the average length of the new code can

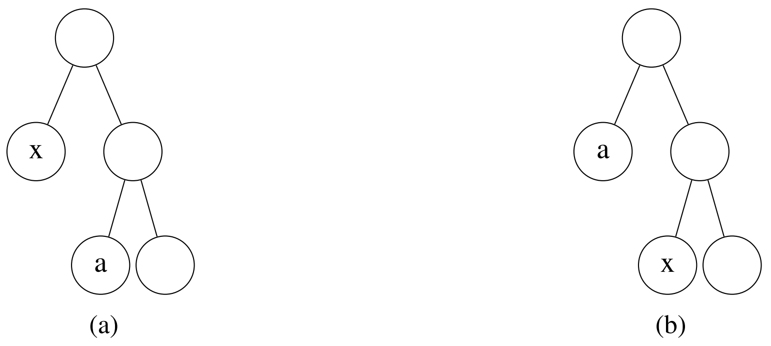


Figure 2.5: On the left we have an abstract representation of a code C where x, one of the two symbols with smallest probability has not maximum length while a which is not one of the two symbols with smallest probability has a maximum length codeword. On the right we have the representation of a new code C' with the codewords of symbols x and a swapped.

not be larger than the average length of C.

$$\begin{aligned} L(C) - L(C') &= \sum_{t \in \mathscr{X}} p_X(t)|C(t)| - \sum_{t \in \mathscr{X}} p_X(t)|C'(t)| && (2.13)\\ &= p_X(x)|C(x)| + p_X(a)|C(a)| - p_X(x)|C'(x)| - p_X(a)|C'(a)| && (2.14)\\ &= p_X(x)(|C(x)| - |C(a)|) - p_X(a)(|C(x)| - |C(a)|) && (2.15)\\ &= (p_X(x) - p_X(a))(|C(x)| - |C(a)|) && (2.16) \end{aligned}$$

The proof is complete since $p_X(x) \le p_X(a)$ and $|C(x)| \le |C(a)|$, which implies that $L(C) - L(C')$ is greater than zero. ■

Lemma 2.3.2 For any code C satisfying that the two symbols with smallest probability have codewords of equal length differing only in the last bit and the code $C\prime$ that results from removing symbols x, y and adding symbol z with $p(z) = p(x) + p(y)$.

$$L(C) = L\left(C'\right) + p(z) \qquad (2.17)$$

Proof. Recall that from the statement we have that $|C(x)| = |C(y)| = |C(z)| - 1$ and consider the following chain of equalities:

$$\begin{aligned} L(C) - L(C') &= \sum_t p(t)|C(t)| - \sum_t p(t)|C'(t)| && (2.18)\\ &= p(x)|C(x)| + p(y)|C(y)| - p(z)|C'(z)| && (2.19)\\ &= p(z) && (2.20) \end{aligned}$$

■

The previous two lemmas strongly point to Huffman codes being optimal. We will not complete the proof here. If you are interested, please look at the references provided in Section 2.6

Theorem 2.3.3 Given an ensemble X, the Huffman code C produces an optimal encoding for the ensemble. That is, for any othe uniquely decodable code C' it holds that $L(C) \le L(C')$.

You might have noticed, that while optimal, Huffman codes are not satisfactory in extreme scenarios. For instance, you could think about the Huffman code for a binary ensemble where one of the symbols have almost unit probability. While the average length is less than one bit from the entropy, if we take the ratio between the average length and the entropy it diverges when one of the elements of the ensemble approaches unit probability.

If we want to transmit not one, but several symbols of some ensemble X, one solution to the situation we described above is to instead of encoding the symbols of the ensemble one by one encode n symbols together. We can model this communication scenario with a joint ensemble that we denote by X^n. The alphabet of the joint ensemble is the cartesian product of the alphabets of the original ensemble and its probability distribution is given by:

$$p_{X^n}(x_1,\dots,x_n) = \prod_{i=1}^{n} p_X(x_i) \tag{2.21}$$

under the assumption that all symbols are drawn independently and identically from the distribution p_X.

■ **Example 2.4** Let X be a binary ensemble with symbols $\{a,b\}$ that occur with probabilities $\{0.7, 0.3\}$. The alphabet of X^2 is $\{a,b\} \times \{a,b\} = \{aa, ab, ba, bb\}$ and the probability of each word is:

$$p_{X^2}(aa) = p_X(a)p_X(a) = 0.49 \tag{2.22}$$
$$p_{X^2}(ab) = p_X(a)p_X(b) = 0.21 \tag{2.23}$$
$$p_{X^2}(ba) = p_X(b)p_X(a) = 0.21 \tag{2.24}$$
$$p_{X^2}(bb) = p_X(b)p_X(b) = 0.09 \tag{2.25}$$

■

Exercise 2.6 Prove that if X, Y are two independent ensembles, then $H(XY) = H(X) + H(Y)$. ■

Exercise 2.7 Prove that $H(X^n) = nH(X)$. ■

Hence, we have on the one hand that $H(X^n) = nH(X)$ and on the other hand that for each extended ensemble there exists a code C_n with length at most one bit from entropy. That is: $L(C_n) \leq H(X^n) + 1 = nH(X) + 1$. If we normalize by n we obtain the following relation:

$$H(X) \leq \frac{L(C_n)}{n} \leq H(X) + \frac{1}{n} \tag{2.26}$$

In consequence, by extending any ensemble enough we can ensure the existence of codes with normalized average length arbitrarily close to the entropy of the original ensemble.

2.4 Exercises

Exercise 2.8 Consider a binary ensemble X with probabilities $\{0.1, 0.9\}$.
1. Find the Huffman code of X and of the ensemble extensions X^2 and X^3.
2. Find the average length of the three codes.
3. Compare the average lengths to the entropy of the corresponding ensemble.

■

Exercise 2.9 A dyadic distribution, is a probability distribution where all symbols have probability 2^{-n} for some integer n. Show that ensembles with dyadic distributions have Huffman codes with average length equal to the entropy of the ensemble. ■

2.5 Solutions to selected exercises

Solution. [Exercise 2.2] We will solve the problem for the first code.
We let $C_0 = \{01, 100, 1101, 0111\}$.
We construct $C_1 = \{11\}$ the set of dangling suffixes from the codewords.
For the next step we take the union of the suffixes in C_1 with respect to the codewords and the suffixes in the set of codewords with respect to the words in C_1. This set is $C_2 = \{01\}$.
The algorithm ends here because C_2 contains a codeword. Hence the code is not uniquely decodable. ■

Solution. [Exercise 2.4] Let us first verify that the lengths given satisfy the Kraft-MacMillan's inequality:

$$\begin{aligned}\sum_{x\in\mathscr{X}} 2^{-\lceil \log 1/p_X(x)\rceil} &= \sum_{x\in\mathscr{X}} 2^{\lfloor \log p_X(x)\rfloor} && (2.27)\\ &\leq \sum_{x\in\mathscr{X}} 2^{\log p_X(x)} && (2.28)\\ &= \sum_{x\in\mathscr{X}} p_X(x) && (2.29)\\ &= 1 && (2.30)\end{aligned}$$

Since the inequality is verified, this implies the existence of a prefix code with the given lengths satisfying $H(X) \leq L(C)$.

Let us now estimate the average length of the code:

$$\begin{aligned}L(C) &= \sum_{x\in\mathscr{X}} p_X(x)|C(x)| && (2.31)\\ &= \sum_{x\in\mathscr{X}} p_X(x)\lceil \log 1/p_X(x)\rceil && (2.32)\\ &\leq \sum_{x\in\mathscr{X}} p_X(x)(\log 1/p_X(x)+1) && (2.33)\\ &\leq H(X)+1 && (2.34)\end{aligned}$$

■

2.6 Further reading

Both Shannon's original paper [16] and Cover and Thomas [3] (chapter 5) provide further detail into the topics discussed here. A popular introduction to data compression is provided by xkcd (the comic stripe) [17].

An important remark on our exposition is that we have only covered lossless codes. That is codes where no information is lost. While we showed that it is not possible to reliably code at rates below entropy, in many practical applications a certain amount of loss or unreliability is acceptable if in exchange one can increase the compression efficiency. The different theoretical trade-offs and schemes go beyond the scope of this course. For the interested reader we can point to Salomon's encyclopedic treatise on the topic [14].

3. Data transmission

In the previous chapter we investigated the data compression problem. That is, given a source and some noiseless means of communication, the problem is to encode the source in such a way that we minimize the usage of the noiseless communications channel while we allow the receiver to recover the message. Here we will investigate a dual problem, the problem of transmitting a source over a noisy channel. This problem, is the problem that your mobile phone faces each time that it wants to exchange information with the nearest base station. It is also the same problem that your computer faces when it wants to store information on a disk in such a way that it can be recovered at a later time.

3.1 The communications problem

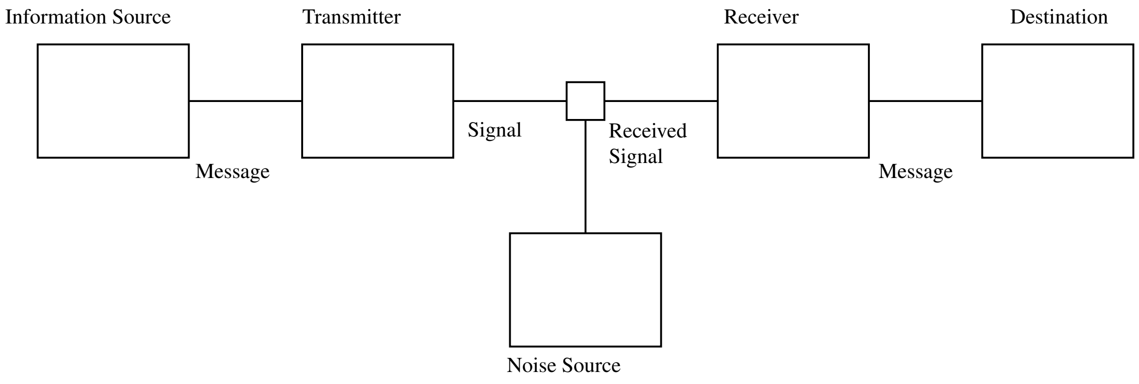


Figure 3.1: This figure reproduces the communications system diagram introduced by Shannon [16].

Let us first of all, depict the building blocks of an idealized communications problem. Our description parallels the one of Shannon [16], see in Fig. 3.1 a graphical representation. The figure shows five entities: an information source, a transmitter, a noise source, a receiver, and a destination. The communications scheme works as follows:

First the information source generates a message m from a set of possible messages M. Then, the transmitter takes m and encodes it into n channel symbols. We define the coding rate R as:

$$R = \frac{\log M}{n} \tag{3.1}$$

The channel is a physical medium of transmission. Mathematically, we can model it as a system taking symbols from input alphabet $\mathscr{X}$ to symbols of output alphabet $\mathscr{Y}$ and characterized by a transition probability matrix that maps the probability of every symbol y if symbol x is sent. The receiver tries to undo the encoding given the noisy received signal and at the end of the scheme the destination receives the $\hat{m}$ possibly identical to m.

3.2 Detection, correction and minimum distance

Let us recall our original example of transmitting the weather forecast. Let us recall that the set of messages is binary : rain and sun. If we are interested in transmitting one of these messages through a noiseless channel, it should be clear that unless one of the two messages has zero probability the encoding with minimum average length will assign to rain the codeword 0 and to sun 1 or viceversa.

Let us now imagine that we want to transmit the weather forecast through a noisy channel. For instance a channel that takes a binary symbol as input and outputs the same symbol with probability $1-p$ or flips it with probability p. In this new scenario, unless we change the encoding, the messages transmitted will be erroneous with probability p. The most obvious way of protecting against error is repeating the message.

The repetition code of length 2 is $C = \{00, 11\}$. Now, if one of the bits is flipped, we will receive a word that is not a codeword. With this scheme, we can detect any one bit error. Unfortunately, if we receive the word 01 it could be that the first bit flipped or that the second bit flipped. In the first case the codeword sent would be 11, while in the second case 00. That is, this scheme allows us to detect any one bit error pattern, but not to correct it.

The repetition code of length 3 is $C = \{000, 111\}$. Now, by the same argument as before, we can detect any two bit error pattern. Moreover, if we were guaranteed that at most one error occurred, we could also correct it. For instance, if we receive the word 100 and we know that at most one error occurred, we can coclude that the codeword 000 was transmitted.

Now let us imagine that bits are not flipped, but erased with a certain probability, and that when bits are erased they are replaced by an erasure symbol e. For instance, if we send the codeword 00 over a channel that erases each symbol with probability e, we could receive the word $0e$ (question: with what probability would we receive it?). The only codeword compatible with $0e$ is 00 and we can see by inspection that the length two repetition code can correct any error pattern consisting of a single erasure.

In the following we will introduce the necessary definitions to understand quantitatively these previous examples.

First, we introduce a distance function between vectors.

Definition 3.2.1 The Hamming distance between two vectors $x, y \in D^n$ is given by:

$$d(x,y) = |i : x_i \neq y_i, 1 \leq i \leq n| \tag{3.2}$$

An useful way of interpreting the Hamming distance is as the minimum number of positions that it is necessary to change in x to transform it to y.

■ **Example 3.1** The Hamming distance between vectors $x = (1,2,0,1,2)$ and $y = (2,1,0,1,2)$ is two because they differ in the first two entries. Alternatively, from the definition

$$d(x,y) = |i : x_i \neq y_i, 1 \leq i \leq n| = |1,2| = 2 \tag{3.3}$$

■

A function $d : \mathscr{X} \times \mathscr{X} \mapsto \mathbb{R}$ is a distance function if it verifies the following properties:

1. Identity: $d(x,y) = 0$ if and only if $x = y$
2. Symmetry: $d(y,x) = d(x,y)$
3. Triangle inequality: $d(x,y) \leq d(x,z) + d(z,y)$

Exercise 3.1 Show that the Hamming distance is a valid distance function ■

In the following whenever we refer to a distance, we will refer to the Hamming distance unless explicitly stated otherwise.

The decoding strategy that we described above is called nearest neighbor decoding or minimum distance decoding. A minimum distance decoder is a decoder that outputs the codeword closest in distance to the received vector y, or in the case that there are more than one it will choose from the set of closest codewords uniformly at random.

$$\text{dec}(x) = \operatorname*{argmin}_{x \in C} d(x,y) \tag{3.4}$$

■ **Example 3.2** A minimum distance decoder for the repetition code of length 3 will output 000 when it receives as input the word 001 since 000 has a smaller hamming distance to 001 than the other codeword in the code: 111. ■

Now we introduce block codes. In the previous chapter we mostly worked with variable length codes. For error correction, we will restrict our analysis to codes with all codewords of the same length.

Definition 3.2.2 A binary block code is a function $C : \{0,1\}^k \mapsto \{0,1\}^n$, where $k \geq n$ are natural numbers.

To understand the behavior of a decoder quantitatively we need to introduce measures of failure and success. The error probability of a codeword x is the probability that a decoder outputs a codeword different than x.

$$p_e(x) = \sum_{y \in \{0,1\}^n} p(y|x) p(\text{dec}(y) \neq x) \tag{3.5}$$

and the error rate of a code:

$$p_e(C) = \sum_{w \in C} p(w) p_e(w) \tag{3.6}$$

Let us now study the effect of the repetition code in error rate on two important communications channels.

Exercise 3.2 Consider $C = \{000, 111\}$, suppose that we send each symbol of the word 000 through a BSC(p).

- What is the probability of having no errors?
- What is the probability of having one error?
- What is the probability of having two errors?
- What is the probability of having three errors?
- What is the error probability with a minimum distance decoder?

■

Exercise 3.3 Consider $C = \{000, 111\}$, suppose that we send each symbol of the word 000 through a BEC(p).

- What is the probability of having no erasures?
- What is the probability of having one erasure?
- What is the probability of having two erasures?
- What is the probability of having three erasures?
- What is the error probability with a minimum distance decoder?

■

From solving the previous two exercises you can realize that the performance of the minimum distance decoder is linked to the minimum distance between all codewords. This is an important metric for a code and we will use the following notation:

$$d_{\min}(C) = \min_{x,y \in C, x \neq y} d(x,y) \tag{3.7}$$

Now, let us make explicit this intuition with the following set set of exercises. Recall that the number of strings of length n with k ones is $\binom{n}{k}$.

Exercise 3.4 Show that a code C can detect all error patterns with s errors if and only if $d_{\min}(C) \geq s+1$ ■

Exercise 3.5 Show that a code C can correct all error patterns with t errors if and only if $d_{\min}(C) \geq 2t+1$ ■

Exercise 3.6 Show that a code C can detect all erasure patterns with e errors if and only if $d_{\min}(C) \geq e+1$ ■

Exercise 3.7 Given a code with minimum distance 12, find the maximum number of errors it can detect, the maximum number of errors it can correct and the maximum number of erasures it can correct. ■

Definition 3.2.3 An $[n,k,d]_q$ code is a code that encodes k symbols from a q-ary alphabet into n symbols of a q-ary alphabet and has minimum distance d.

■ **Example 3.3** The binary repetition code of length 3 is a $[3,1,3]_2$ code. ■

A typical coding theory problem is given two or three of the parameters in $[n,k,d]_q$ find the best code that matches those values. For instance:

- Given n,k,q find within the set of codes encoding k q-ary symbols into n, the code with the maximum minimum distance:

$$B_q(n,k) = \max \tag{3.8}$$

- Given n,k,q find within the set of codes encoding k q-ary symbols into n, the code with the maximum minimum distance:

$$A_q(n,k) = \max \tag{3.9}$$

- Given n,k,q find within the set of codes encoding k q-ary symbols into n, the code with the maximum minimum distance:

Exercise 3.8 Find $B_2(n,1)$ ■

Exercise 3.9 Find $B_2(n,n)$ ■

Definition 3.2.4 Two codes C and C' are equivalent if the set of codewords coincide up to a permutation in the position of the symbols, relabeling of the symbols or both.

■ **Example 3.4** The codes $C = \{001,110\}$ and $C' = \{100,011\}$ are equivalent because the codewords coincide up to a permutation of the position of the symbols. ■

■ **Example 3.5** The codes $C = \{001,110\}$ and $C' = \{000,111\}$ are equivalent because the codewords coincide up to a relabelling of the symbols. ■

3.3 Refresher on linear algebra

A vector space that is going to be very useful in the following is the n-dimensional binary vector space that we will denote by V_n. This is the vector space of length n binary strings over $\mathbb{F}_2$.

Let us define first the finite field F_2. It is the set $\{0,1\}$ together with the operations $+,\cdot$ defined as follows:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \tag{3.10}$$

and

$$\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \tag{3.11}$$

Addition over V_n follows from addition in $\mathbb{F}_2$. That is, given $x,y \in \{0,1\}^n$.

$$x + y = (x_1 + y_1, \ldots, x_n + y_n) \tag{3.12}$$

where $x_i + y_i$ follows the rules from (3.10). Similarly scalar multiplication in V_n follows from the multiplication rules in $\mathbb{F}_2$, given $s \in \{0,1\}$ and $x \in \{0,1\}^n$:

$$s\dot{x} = (s \cdot x_1, \ldots, s \cdot x_n) \tag{3.13}$$

where $s \cdot x_i$ follows the rules from (3.11).

Definition 3.3.1 The Hamming weight $w : \{0,1\}^n \mapsto \mathbb{N}$ of a binary string is given by its number of ones. Given $x \in \{0,1\}^n$:

$$w(x) = \sum_{i=1}^{n} x_i \tag{3.14}$$

Exercise 3.10 Show that given $x,y \in \{0,1\}^n$, $d(x,y) = w(x+y)$. ■

In the following we state several important properties and definitions of vector spaces that will be of use in coding theory. Some of these, we state only for V_n for simplicity. If these notions are unfamiliar or not completely understood, please review your text on the matter.

Definition 3.3.2 U is a subspace of V if $U \subseteq V$ and U is a vector space.

Example 3.6 $\{000, 111\}$ is subspace of V_3. ■

Definition 3.3.3 A linear combination of the vectors $v^1, v^2, \dots, v^n \in \{0,1\}^n$ is a vector $s_1 \cdot v^1 + s_2 \cdot v^2 + \ldots + s_n \cdot v^n$ where $s_1, s_2, \dots, s_n \in \mathbb{F}_2$.

Example 3.7 $0 \cdot (0,0,1) + 1 \cdot (1,1,0) = (1,1,0)$ is a linear combination of the vectors $(0,0,1)$ and $(1,1,0)$. ■

Definition 3.3.4 The set of linear combinations of a set of vectors is called its span.

Exercise 3.11 Show that the span of a set of vectors is a vector space. ■

Definition 3.3.5 A set of vectors $v^1, v^2, \dots, v^k \in \{0,1\}^n$ is linearly dependent if there exist $s_1, s_2, \dots, s_k \in \{0,1\}^k$ different from $0, \dots 0$ such that $s_1 \cdot v^1 + s_2 \cdot v^2 + \ldots + s_n \cdot v^n = 0$.

Definition 3.3.6 A set of vectors $v^1, v^2, \dots, v^k \in \{0,1\}^n$ is linearly independent if the $s_1, s_2, \dots, s_k \in \{0,1\}^k$ different from $0, \dots 0$ such that $s_1 \cdot v^1 + s_2 \cdot v^2 + \ldots + s_n \cdot v^n = 0$.

3.4 Bounds on codes

We will now introduce some notation about spheres on V_n that will allow us to bound the possible binary codes.

Definition 3.4.1 Given $x \in \{0,1\}^n$, and $r \in \mathbb{N}$ we define the sphere of radius r centered around x as the set of points with distance at most r: $S_r(x) = \{y : d(x,y) \leq r$.

Exercise 3.12 Find the set of points $S_1(x)$ with $x = (0,1,0)$. ■

Exercise 3.13 Let $x \in \{0,1\}^n$ and $r \in \mathbb{N}$, show that the number of elements in $S_r(x)$ is:

$$|S_r(x)| = \sum_{i=0}^{r} \binom{n}{i} \tag{3.15}$$

■

We now have the tools to prove to important bounds for the existence of codes. The first of these bounds is called the Hamming bound, from the mathematician that proved it, but also the sphere packing bound since it argues that a code can only correct all patterns of some weight t if it can fit as many spheres of radius t in V_n as the number of codewords.

Theorem 3.4.1 — Hamming bound. An $[n,k,d]$ code satisfies

$$2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n \tag{3.16}$$

where $t = \lfloor \frac{d-1}{2} \rfloor$.

Proof. As shown in exercise 3.13, a $S_t(x)$ sphere contains $\sum_{i=0}^{t} \binom{n}{i}$ words. For t to be the maximum weight of the error patterns the code can correct it needs to be possible to place a sphere of radius t around each of the 2^k codewords and these spheres need to be disjoint. This gives a total number of words of $2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n$ which is only possible if this number is smaller than the total number of words in the space 2^n. ■

A code is called perfect if it attains the sphere packing bound with equality.

Now we will discuss a second bound, the Singleton bound, also based on dimensionality, but this time the argument stems from the distinguishability of codewords under erasure.

Theorem 3.4.2 — Singleton bound. An $[n,k,d]$-code satisfies $d \leq n-k+1$.

Proof. In a code with minimum distance d, if we erase $d-1$ positions of the code, all codewords need to be still different. However, the number of words of length $n-d+1$ is 2^{n-d+1} which can not be larger than the total number of words in the code 2^k, i.e. $2^{n-d+1} \leq 2^k$. The proof follows by taking the logarithm of both sides and solving for d. ■

A code that meets the Singleton bound with equality is called maximum distance separable code.

3.5 Binary linear codes

A binary linear code of length n is a subspace of V_n.

Exercise 3.14 Show that the repetition code of length 3 is a subspace of V_3. ■

Exercise 3.15 If C is a binary linear code then:

$$\min_{x,y\in C} d(x,y) = \min_{x\in C\setminus\{0\}} w(x) \tag{3.17}$$

■

Definition 3.5.1 Given a $[n,k,d]$ linear code, a matrix with k rows and n columns where each row is an element of a basis of the code is called a generator matrix.

■ **Example 3.8** A generator matrix for the length three repetition code is given by:

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \tag{3.18}$$

■

Exercise 3.16 Two generator matrices G_1, G_2 with coefficients in $\{0,1\}$ generate two equivalent binary codes if it is possible to transform G_1 into G_2 by a series of row permutations, column permutations and additions of one row into another. ■

Lemma 3.5.1 Any generator matrix G of an $[n,k,d]$ binary linear code can transformed to a generator matrix of the form $G' = (I_k|A)$ where I_k is the d-dimensional identity matrix and A is an arbitrary $n-k \times k$ matrix. This matrix form is called *standard form*.

Exercise 3.17 Take the following generator matrix to standard form:

$$G = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{3.19}$$

■

Let us now take a step back and think about the general communications problem. There is a certain number of messages that we want to transmit. In order to protect the messages we are going to encode them into a codeword of a code. In principle, for this it is enough to have a large lookup table that tells us what is the codeword associated with each message. However, if the set of messages is the set of strings of length k, there are 2^k possible strings. Even for modest values of k the lookup table strategy soon becomes impractical.

Given a $[n,k,d]$ linear code with generator matrix G, we can encode a string $m \in \{0,1\}^k$ simply by multiplying m with the generator matrix:

$$m \mapsto m \cdot G \tag{3.20}$$

where we adopt the convention that vectors are represented by a one-row matrix.

If G is in standard form, the encoding takes a particular simple form. Since $G = (I_k|A)$, a string m gets mapped to $m|m \cdot A$. In this case, we call the first k bits of a codeword the information bits and the remaining $n-k$ bits the redundancy bits.

Exercise 3.18 Consider the $[k,k+1,d]$ code that takes a string $m = (m_1, \dots, m_k)$ and encodes it into the codeword $c = (m_1, \dots, m_k, \sum_{i=1}^{k})$.

- What is the generator matrix of the code?
- What is the minimum distance of the code?

■

Let us now think about the decoding problem with linear codes. Again, technically, a large lookup table with each word in the space of n-bit strings and the corresponding decoding decision would work. However, very soon this becomes impractical. Within the scope of this course we will not cover any truly practical decoder, but we will now describe a first step into feasible decoding strategies. For this, we need to introduce some additional algebra concepts.

Definition 3.5.2 Let C be an $[n,k,d]$ code, and $v \in \{0,1\}^n$. We call the set

$$v + C = \{v + c, c \in C\} \tag{3.21}$$

a coset of C.

Exercise 3.19 Show that if $y \in x + C$ then $x \in y + C$. ■

The following theorem is an adaptation of Lagrange's theorem for our particular needs.

Theorem 3.5.2 Let C be an $[n,k,d]$ code. Then

- All vectors belong to some coset.
- Each coset has 2^k elements.
- Two cosets either have no common element either they completely coincide.
- There are 2^{n-k} cosets.

Proof.

- The code C is a subspace of V_n, hence the zero word always belongs to C. This implies that for any vector $v \in \{0,1\}^n$, $v = v + 0$ and trivially $v \in v + C$.
- Since all codewords are different we have that for any two codewords c_1, c_2, $c_1 \neq c_2$ which directly implies that $c_1 + v \neq c_2 + v$.
- This follows from exercise 3.19. Suppose that there exists some v such that $v \in x + C$ and $v \in y + C$. Then, we have that $v + C = x + C$ and also that $v + C = y + C$.

- There are 2^k words per coset, and all cosets are disjoint, hence there are a total of $2^n/2^k$ cosets.

■

Exercise 3.20 Find the cosets of the code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \tag{3.22}$$

■

We call the vector with minimum hamming weight its leader, if there is more than one vector with minimum weight, any of them can be the coset leader.

■ **Example 3.9** The set $0+C = \{000, 111\}$ is a coset of the repetition code of length 3. The coset leader is 000. ■

We will now present a scheme for decoding known as the standard array. The standard array is a table with 2^{n-k} rows and 2^k columns. The top row consists of the elements of the coset $0+C$ (the codewords) beginning with the zero word. Each other row consists of the element of one of the cosets beginning with the coset leader.

■ **Example 3.10** Consider the repetition code of length 3. A standard array for this code would be:

$$\begin{matrix} 000 & 111 \\ 001 & 110 \\ 010 & 101 \\ 100 & 011 \end{matrix} \tag{3.23}$$

■

The standard array of a code can be used to construct a simple decoding algorithm. Suppose that we receive some vector y, then we can find y in the standard array look for the coset leader t and output $y+t$. This algorithm is in fact a minimum distance decoder.

Exercise 3.21 Show that the output of a standard array based decoder is always a codeword ■

Exercise 3.22 Show that the standard array based decoder is a minimum distance decoder ■

■ **Example 3.11** Consider the standard array of the repetition code as given in example 3.10. If the vector $y = 101$ is received, the output would of the decoder would be y added to the coset leader 010 which is the codeword 111. ■

Definition 3.5.3 A parity check matrix for a $[n,k,d]$ code C is an $n-k \times n$ matrix H for which the set $\{x | Hx^T = 0\}$ is the set of codewords of C.

■ **Example 3.12** A parity check matrix for the repetition code of length three is:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \tag{3.24}$$

■

3.6 Hamming codes

A Hamming code is a family of codes defined for lengths $n = 2^r - 1$ with $r \in \mathbb{N}$ and $r \geq 2$.. The parity check matrix of the Hamming code of length n, H_n has as columns all the non-zero elements of V_r.

■ **Example 3.13** The first Hamming code is defined for length $n = 2^2 - 1 = 3$. The parity check matrix of H_3 has as columns all the non-zero elements of V_2: $\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}$. Thus:

$$\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix} \tag{3.25}$$

■

Exercise 3.23 How many bits does a Hamming code encode? (That is, what is the value of k?) ■

Let us now see some properties of Hamming codes.

Lemma 3.6.1 Hamming codes have minimum distance three.

Proof. In order to prove that Hamming codes have minimum distance three, we will first prove that they can not have minimum distance one or two.

If the minimum distance was one, there would exist a codeword with hamming weight one c. That is, a vector with only one one at position i. Moreover, since c is a codeword $Hc^T = 0$, which can only hold if the the i-th column of H is a zero vector. However, this is not possible because the parity check matrix of a Hamming code consists of all non-zero vectors of V_r.

Now let us assume that the minimum distance is two. This implies that there exists a codeword with two ones, one at position i and one at position j. Moreover,

$$Hc^T = \begin{pmatrix} \dots & h_1^i & \dots & h_1^j & \dots \\ \dots & h_2^i & \dots & h_2^j & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \dots & h_{n-k}^i & \dots & h_{n-k}^j & \dots \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_i \\ \vdots \\ c_j \\ \vdots \end{pmatrix} = \begin{pmatrix} h_1^i + h_1^j \\ \vdots \\ h_{n-k}^i + h_{n-k}^j \end{pmatrix} \tag{3.26}$$

and since c is a codeword the equation above shold equal the zero vector which is only possible if $h_t^i + h_t^j = 0$ for $t \in \{1, \dots, n\}$. That is if the i-th column is equal to the j-th column, which contradicts the definition of the parity check matrix of a Hamming code.

Finally, we can show that the minimum distance of Hamming codes is three by constructing a codeword of weight three. Consider the word $c = (1,1,1,0,\dots,0)$ and the following valid parity check matrix for a Hamming code:

$$H = \begin{pmatrix} 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & \dots \\ 1 & 0 & 1 & \dots \end{pmatrix} \tag{3.27}$$

If we multiply H with c we obtain the zero vector which indicates that c is a codeword. ■

Exercise 3.24 Show that Hamming codes meet the Hamming bound. ■

3.7 Channel capacity

In this section we are going to informally explore the usefulness of different transmission channels. Let us first explore some examples of channels.

The first channel that we introduce is the binary symmetric channel (BSC). This is a binary channel that takes the input to the output with probability $1-p$ and with probability p it flips the value of the input. See figure 3.2 for a graphical depiction.

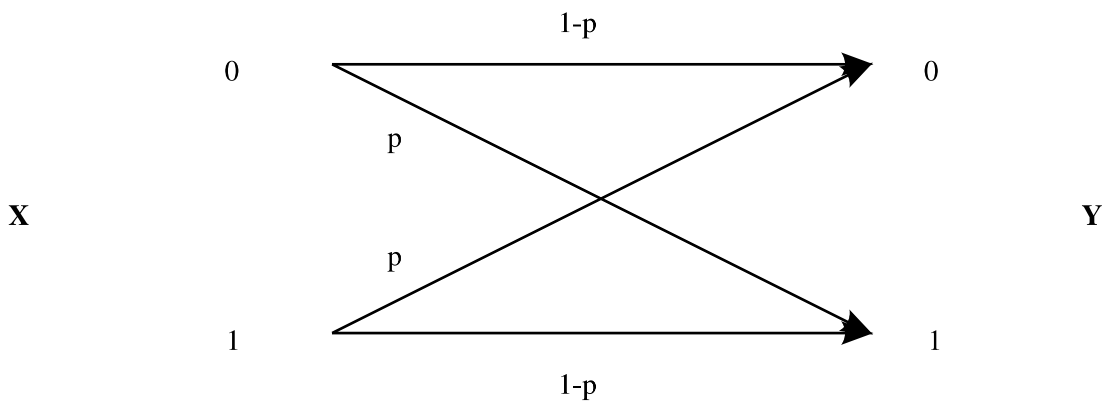


Figure 3.2: Binary Symmetric Channel.

We present now a second noisy channel, the binary erasure channel (BEC). The BEC was introduced by Elias in his famous paper "Coding for Two Noisy Channels" [5]. The BEC has two input elements while the output alphabet is composed of three elements: 0, 1, and e, which stands for an erasure in the channel. In this channel the bits are either correctly transmitted with probability $1-p$, or are erased with probability p. See figure 3.3 for a graphical depiction.

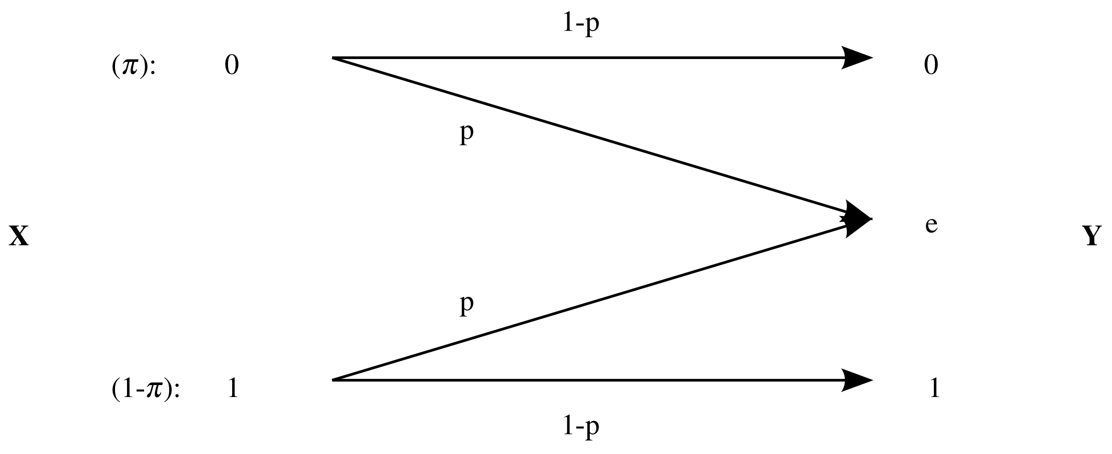


Figure 3.3: Binary Erasure Channel.

■ **Example 3.14** The transition matrices of the binary symmetric and the binary erasure channel are given by:

$$\begin{pmatrix} p_{YX}(0|0) & p_{YX}(1|0) \\ p_{YX}(0|1) & p_{YX}(1|1) \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \tag{3.28}$$

and

$$\begin{pmatrix} p_{YX}(0|0) & p_{YX}(e|0) & p_{YX}(1|0) \\ p_{YX}(0|1) & p_{YX}(e|1) & p_{YX}(1|1) \end{pmatrix} = \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix} \tag{3.29}$$

■

We can say that it is possible to communicate reliably at a certain rate over a noisy channel, if it is possible to make the decoding error as small as desired by encoding large enough blocks. The capacity of a channel is the largest rate at which it is possible to communicate reliably through the channel. The capacity of a channel is given by the following formula.

$$C = \max_{p(x)} I(X;Y) \tag{3.30}$$

This result was proved by Shannon [16]. The proof consists of two parts. The converse part shows that any code with a rate larger than capacity can not achieve an error rate lower than a certain bound that is independent of the block length. The achievability part shows that for any desired error rate there exist codes for any codign rate below the capacity of the channel.

Exercise 3.25 Find the capacity of the binary symmetric channel. ■

Exercise 3.26 Find the capacity of the binary erasure channel. ■

It might seem that the capacity of a BSC that flips bits with probability p is greater than the capacity of a BEC that erases bits with probability p. Fig. 3.4 shows that it is the opposite situation. On the range $p \in (0, 0.5)$, the capacity of the BEC is greater than the capacity of the BSC. Bits on the BEC are either perfectly known or perfectly unknown, however, it is not possible to distinguished flipped bits from correct bits in the BSC.

In the following we analyze the capacity of a large class of channels. A channel is called weakly symmetric if all rows are permutations of each other and all columns add up to the same value.

■ **Example 3.15** The following transition matrix corresponds to a weakly symmetric channel.

$$\begin{pmatrix} 1/5 & 1/5 & 1/5 & 2/5 & 0 \\ 1/5 & 1/5 & 1/5 & 0 & 2/5 \end{pmatrix} \tag{3.31}$$

■

Lemma 3.7.1 The capacity of a weakly symmetric channel N is given by:

$$C(N) = \log|Y| - H(\text{row}) \tag{3.32}$$

where $|Y|$ is the number of elements of the output alphabet and $H(\text{row})$ is the entropy of one of the rows of the transition matrix.

Proof.

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) && (3.33) \\ &= H(Y) - H(\text{row}) && (3.34) \\ &\le \log|Y| - H(\text{row}) && (3.35) \end{aligned}$$

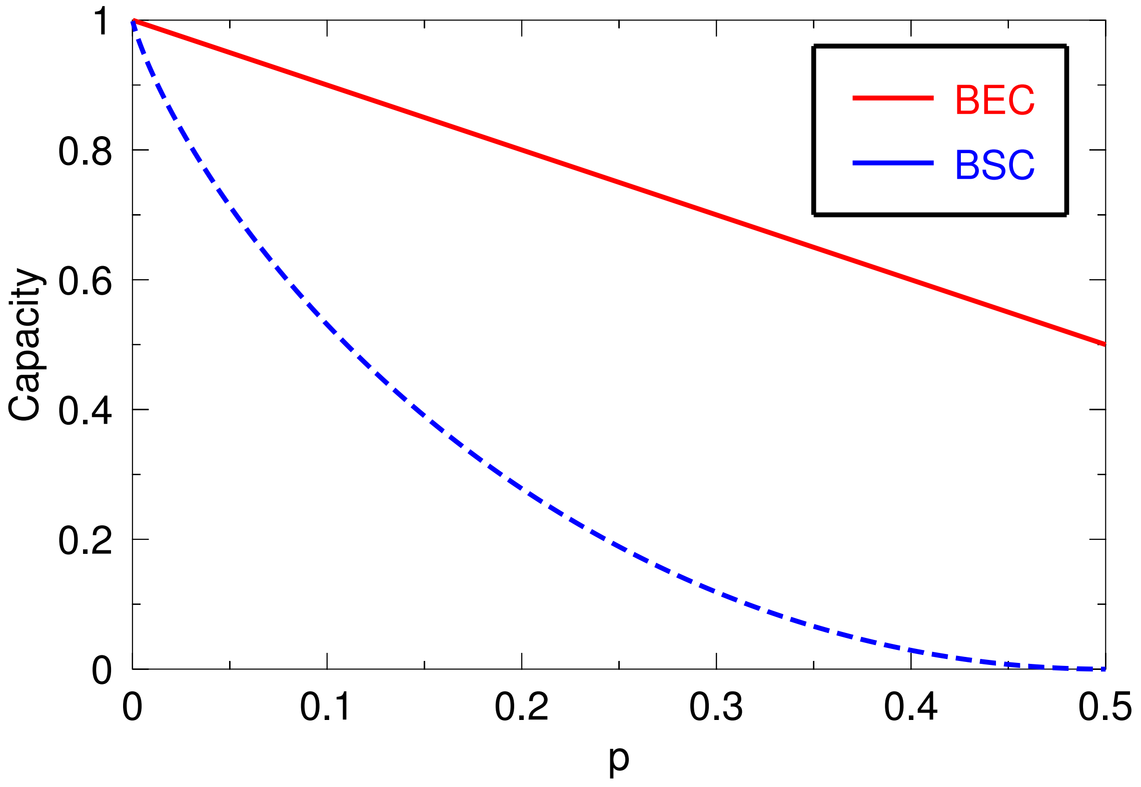


Figure 3.4: The capacity of the BEC and BSC.

where the second equality follows because the entropy of $H(Y|x)$ coincides with the entropy of one of the rows of the transition matrix.

Now let us compute the distribution of Y under a uniform distribution on the input.

$$p_Y(y) = \sum_{x\in X} p_{YX}(y|x)p_X(x) \tag{3.36}$$

$$= \frac{1}{|X|}\sum_{x\in X} p_{YX}(y|x) \tag{3.37}$$

The sum in the right hand side of equation (3.45) corresponds to a column in the transition matrix. In other words, the probability is the same for all y which implies that Y is also uniformly distributed which, in turn, implies that the upper bound on the mutual information can be achieved with a uniform distribution on the input. ■

3.8 Exercises

Exercise 3.27 Let C be a linear binary code. Prove that either all codewords have even Hamming weight or half of the codewords have even weight and half odd weight. ■

Exercise 3.28 Find the capacity of a channel given by transition matrix

$$\begin{pmatrix} 1-e & e & 0 & 0 \\ 0 & 0 & e & 1-e \end{pmatrix} \tag{3.38}$$

■

3.9 Solutions to selected exercises

Solution. [Exercise 3.2]

- This is the probability of having no bit flip: $(1-p)^3$.
- This is the probability of having one of the three bit flipped, there are $\binom{3}{1}$ ways in which this can happen and each one has probability $(1-p)^2 p$. Hence: $3(1-p)^2 p$.
- This is the probability of having two of the three bits flipped, there are $\binom{3}{2}$ ways in which this can happen and each one has probability $(1-p)p^2$. Hence: $3(1-p)p^2$.
- This is the probability of having the three of the three bits flipped, there are $\binom{3}{3}$ ways in which this can happen and it has probability p^3. Hence: p^3.
- The decoder will output the wrong guess when there are either two or three errors. Hence the error probability is: $3(1-p)p^2 + p^3$.

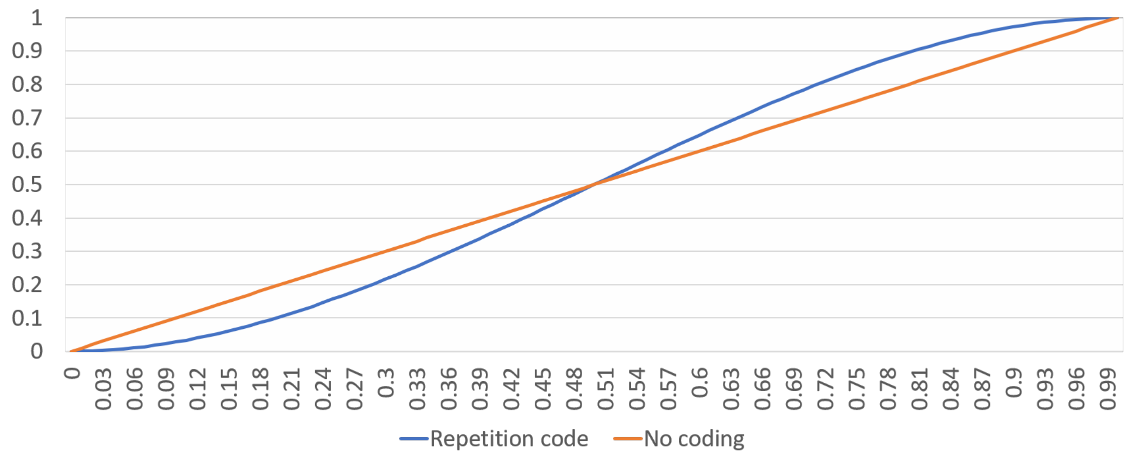


Figure 3.5: Decoding error vs crossover probability for the repetition code and for uncoded transmission.

■

Solution. [Exercise 3.3]

- This is the probability of having no bit erased: $(1-e)^3$.
- This is the probability of having one of the three bits erased, there are $\binom{3}{1}$ ways in which this can happen and each one has probability $(1-e)^2 e$. Hence: $3(1-e)^2 e$.
- This is the probability of having two of the three bits erased, there are $\binom{3}{2}$ ways in which this can happen and each one has probability $(1-e)e^2$. Hence: $3(1-e)e^2$.
- This is the probability of having the three of the three bits erased, there are $\binom{3}{3}$ ways in which this can happen and it has probability e^3. Hence: e^3.
- Since there are no bit flips, even when there are two erasures, there is a single codeword compatible. When there are three erasures, the decoder has no information but can choose uniformly at random either $(0,0,0)$ or $(1,1,1)$. Hence, the error probability is: $\frac{1}{2}e^3$.

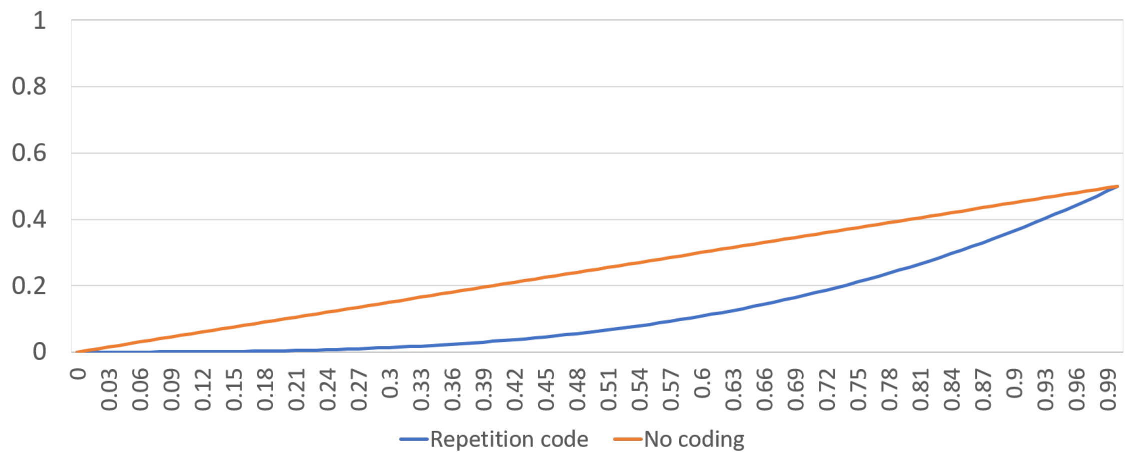


Figure 3.6: Decoding error vs erasure probability for the repetition code and for uncoded transmission.

■

Solution. [Exercise 3.18]

- In order to construct the generator matrix, it is enough to understand the action of the code on a basis of the original space. Let $u_1 = (1,0,\dots,0), u_2 = (0,1,0,\dots,0),\dots,u_n = (0,\dots,0,1)$ be the elements of the canonical basis. Since the code maps them to $(1,0,\dots,0,1), u_2 = (0,1,0,\dots,0,1),\dots,u_n = (0,\dots,0,1,1)$, we conclude that the generator matrix is of the form:

$$G = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix} = \left(\begin{array}{c|c} & 1 \\ I_k & 1 \\ & \vdots \\ & 1 \end{array} \right) \tag{3.39}$$

- The minimum distance of this code is two. We can see it by looking at the first k bits of a codeword. If two codewords only differ in one position, that also means that their sum is off by one, hence the last position will also be different.

■

Solution. [Exercise 3.19] If $y \in x + C$ then, there exists some codeword c such that $y = x + c$. Moreover, $y + c = x + c + c = x$, hence $x \in y + C$. ■

Solution. [Exercise 3.20] Let us first find the coset $0 + C$, that is, the set of codewords:

$$\begin{aligned} 0 + C &= \{(0 \quad 0) \cdot G, (0 \quad 1) \cdot G, (1 \quad 0) \cdot G, (1 \quad 1) \cdot G\} && (3.40) \\ &= \{(0 \quad 0 \quad 0 \quad 0), (0 \quad 1 \quad 1 \quad 1), (1 \quad 0 \quad 0 \quad 1), (1 \quad 1 \quad 1 \quad 0)\} && (3.41) \end{aligned}$$

We can construct the following cosets by adding the set of codewords to low weight vectors:

$$(0 \quad 0 \quad 0 \quad 1) + C = \{(0 \quad 0 \quad 0 \quad 1), (0 \quad 1 \quad 1 \quad 0), (1 \quad 0 \quad 0 \quad 0), (1 \quad 1 \quad 1 \quad 1)\} \tag{3.42}$$

$$(0 \quad 0 \quad 1 \quad 0) + C = \{(0 \quad 0 \quad 1 \quad 0), (0 \quad 1 \quad 0 \quad 1), (1 \quad 0 \quad 1 \quad 1), (1 \quad 1 \quad 0 \quad 0)\} \tag{3.43}$$

$$(0 \quad 1 \quad 0 \quad 0) + C = \{(0 \quad 1 \quad 0 \quad 0), (0 \quad 0 \quad 1 \quad 1), (1 \quad 1 \quad 0 \quad 1), (1 \quad 0 \quad 1 \quad 0)\} \tag{3.44}$$

■

Solution. [Exercise 3.21] If y and t belong to the same coset this means that they there exists some $x \in \{0,1\}^n$ and $c_1, c_2 \in C$ such that $y = x + c_1$ and $t = x + c_2$. Then $t + y = x + c_1 + x + c_2 = c_1 + c_2$, moreover since C is a vector space $c_1 + c_2 \in C$. That is, $t + y$ is a codeword. ■

Solution. [Exercise 3.22] Recall that upon receiving y, the standard array decoder output $y + t$ where t is a coset leader of $y + C$.

Suppose that there exists a codeword c' such that $d(y, c') < d(y, y + t)$. We can rewrite it as $w(t') < w(t)$ where $t' = y + c'$. However, note that $t' \in y + C$, which is a contradiction since t' can not have smaller weight than a coset leader.

Note that there is a small subtlety in the sense that when more than one codeword is at minimum distance, the standard array based decoder will not choose the codeword uniformly at random. ■

Solution. [Exercise 3.26]

In the binary symmetric channel the two symbols of the input alphabet are either perfectly transmitted with probability $1 - p$ or flipped with probability p.

Consider an arbitrary distribution on the input symbols and the associated random variable X. Let us first find the mutual information between the input X and the induced random variable at the output of the channel Y [3]:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) && (3.45)\\ &= H(Y) - \sum_x p(x) H(Y|x) && (3.46)\\ &= H(Y) - \sum_x p(x) H(p, 1-p) && (3.47)\\ &= H(Y) - H(p, 1-p) \sum_x p(x) && (3.48)\\ &\le 1 - H(p, 1-p) && (3.49) \end{aligned}$$

where the upper bound follows from Y being a binary random variable.

If we can find a distribution on the input symbols that achieve the upper bound we show that the upper bound is the capacity of the channel. Consider a uniform distribution on the input and let us find the induced distribution at the output of the channel:

$$\begin{aligned} p_Y(0) &= p_{YX}(0,0) + p_{YX}(0,1) && (3.50)\\ &= p_X(0) p_{YX}(0|0) + p_X(1) p_{YX}(0|1) && (3.51)\\ &= \frac{1}{2}(1-p) + \frac{1}{2}p && (3.52)\\ &= \frac{1}{2} && (3.53) \end{aligned}$$

and $p_Y(1) = 1 - p_Y(0) = \frac{1}{2}$. In consequence, if the input symbols are uniformly distributed $H(Y) = 1$ and the upper bound is achieved. ■

Solution. [Exercise 3.27]

Consider an arbitrary distribution on the input $p_X(0) = x, p_X(1) = 1 - x$. Let us find what is the induced probability at the output.

$$\begin{aligned} p_Y(0) &= p_{YX}(0,0) + p_{YX}(0,1) && (3.54)\\ &= p_X(0) p_{YX}(0|0) + p_X(1) p_{YX}(0|1) && (3.55)\\ &= x(1-p)\ , && (3.56) \end{aligned}$$

$$\begin{aligned} p_Y(1) &= p_{YX}(1,0) + p_{YX}(1,1) && (3.57)\\ &= p_X(0)p_{YX}(1|0) + p_X(1)p_{YX}(1|1) && (3.58)\\ &= (1-x)(1-p) && (3.59)\end{aligned}$$

and

$$\begin{aligned} p_Y(e) &= p_{YX}(e,0) + p_{YX}(e,1) && (3.60)\\ &= p_X(0)p_{YX}(e|0) + p_X(1)p_{YX}(e|1) && (3.61)\\ &= xp + (1-x)p && (3.62)\\ &= p\ . && (3.63)\end{aligned}$$

Now we will find $H(X|Y)$. For this we need the conditional distributions on the input alphabet for each value of the output alphabet.

$$\begin{aligned} p_{XY}(0|0) &= \frac{p_{XY}(00)}{p_Y(0)} && (3.64)\\ &= \frac{p_{YX}(0|0)p_X(0)}{p_Y(0)} && (3.65)\\ &= \frac{(1-p)x}{(1-p)x} && (3.66)\\ &= 1, && (3.67)\end{aligned}$$

which implies $P_{XY}(1|0) = 0$. Similarly, $P_{XY}(1|1) = 1$ and $P_{XY}(0|1) = 0$. Finally, for e:

$$\begin{aligned} p_{XY}(0|e) &= \frac{p_{XY}(0e)}{p_Y(e)} && (3.68)\\ &= \frac{p_{YX}(e|0)p_X(0)}{p_Y(e)} && (3.69)\\ &= \frac{px}{p} && (3.70)\\ &= x && (3.71)\end{aligned}$$

and $p_{XY}(1|e) = 1-x$.

We can now develop $H(X|Y)$:

$$\begin{aligned} H(X|Y) &= x(1-p)H(X|Y=0)\\ &\quad + pH(X|Y=e)\\ &\quad + (1-x)(1-p)H(X|Y=1) && (3.72)\\ &= pH(x,1-x) && (3.73)\end{aligned}$$

The second equality holds from $H(X|Y=1) = H(X|Y=0) = 0$. We can now plug Eq. 3.80 in Eq. 1.30 and bound from above the mutual information:

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) && (3.74)\\ &= H(x,1-x) - pH(x,1-x) && (3.75)\\ &\leq 1-p && (3.76)\end{aligned}$$

equality in Eq. 3.84 is achieved again by the uniform distribution. That is, for $x = \frac{1}{2}$. ■

3.10 Further reading

We have covered in this chapter several topics on data transmission. For a quick introduction to coding theory, we refer to the first chapter in MacKay [12] and to section 7.11 in Cover and Thomas [3]. For a more in depth introduction to coding theory, we refer to the book by Hill [8].

For the noisy channel theorem and computing capacity we refer to chapters 9 and 10 in MacKay [12] and to chapter 7 in Cover and Thomas [3].

Finally, the treatment of the noisy channel theorem in this class, does not follow the common structure via typical sequences but instead it is based on the extremely concise proof in [11].

Bibliography

[1] J. Aczel and Z. Daroczy. *On measures of information and their characterizations*. Academic Press, 1975 (cited on page 19).

[2] J. Aczel, B. Forte, and C. T. Ng. “Why the Shannon and Hartley Entropies Are Natural”. In: *Advances in Applied Probability* 6.1 (1974), pages 131–146. ISSN: 00018678 (cited on page 19).

[3] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, Aug. 1991 (cited on pages 19, 23, 30, 47, 48).

[4] I. Csiszár. “Axiomatic Characterizations of Information Measures”. In: *Entropy* 10 (2008), pages 261–273 (cited on page 19).

[5] Peter Elias. “Coding for two noisy channels”. In: *Information Theory, 3rd London Symposium, London, England, Sept. 1955*. 1955 (cited on page 41).

[6] Robert M Fano. *Transmission of Information: A Statistical Theory of Communication MIT Press*. Cambridge, Mass. and Wiley, New York, 1961 (cited on page 42).

[7] A. Feinstein. *Foundations of Information Theory*. McGraw-Hill, 1958 (cited on page 19).

[8] Raymond Hill. *A first course in coding theory*. Oxford University Press, 1986 (cited on page 48).

[9] David A Huffman. “A method for the construction of minimum-redundancy codes”. In: *Proceedings of the IRE* 40.9 (1952), pages 1098–1101 (cited on page 26).

[10] J. Karush. “A simple proof of an inequality of McMillan (Corresp.)” In: *IRE Transactions on Information Theory* 7.2 (Apr. 1961), page 118 (cited on page 23).

[11] Yuval Lomnitz and Meir Feder. “A simpler derivation of the coding theorem”. In: *arXiv preprint arXiv:1205.1389* (2012) (cited on page 48).

[12] David JC MacKay. *Information theory, inference and learning algorithms*. Cambridge university press, 2003 (cited on pages 19, 48).

[13] B. McMillan. “Two inequalities implied by unique decipherability”. In: *IRE Transactions on Information Theory* 2 (Dec. 1956), pages 115–116 (cited on page 23).

[14] David Salomon and Giovanni Motta. *Handbook of data compression*. Springer Science & Business Media, 2010 (cited on pages 23, 30).

[15] August Albert Sardinas and George W Patterson. “A necessary and sufficient condition for unique decomposition of coded messages”. In: *Proceedings of the Institute of Radio Engineers*. Volume 41. 3. 1953, pages 425–425 (cited on page 22).

[16] C. E. Shannon. “A mathematical theory of Communication”. In: *The Bell system technical journal* 27 (July 1948), pages 379–423 (cited on pages 19, 30, 31, 42).

[17] *Twitter and Shannon*. `https://what-if.xkcd.com/34/`. Accessed: 2019-08-03 (cited on page 30).

Index

Axiomatic derivation of entropy, 11

Binary linear codes, 38
Bounds on codes, 37

Channel capacity, 41
Code length and fundamental limits, 23
Codes, 21

Detection, correction and minimum distance, 32

Entropy, 13
Exercises, 16, 29, 46

Further reading, 19, 30, 47

Hamming codes, 41
Huffman codes and their optimality, 26

Joint entropy, conditional entropy and mutual information, 14

Refresher on linear algebra, 36
Refresher on probability theory, 10

Solutions to selected exercises, 17, 30, 46
Surprising information, 9

The communications problem, 31