DISCRETE MATHEMATICS

W W L CHEN

Chapter 10

INTRODUCTION TO CODING THEORY

10.1. Introduction

The purpose of this chapter and the next two is to give an introduction to algebraic coding theory, which was inspired by the work of Golay and Hamming. The study will involve elements of algebra, probability and combinatorics. Consider the transmission of a message in the form of a string of 0's and 1's. There may be interference ("noise"), and a different message may be received, so we need to address the problem of accuracy. On the other hand, certain information may be extremely sensitive, so we need to address the problem of security.

We shall be concerned with the problem of accuracy in this chapter and the next. In Chapter 12, we shall discuss a simple version of a security code. Here we begin by looking at an example.

Example 10.1.1. Suppose that we send the string $w = 0101100$. Then we can identify this string with the element $\mathbf{w} = (0,1,0,1,1,0,0)$ of the cartesian product

$$\mathbb{Z}_2^7 = \underbrace{\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{7}.$$

Suppose now that the message received is the string $v = 0111101$. We can now identify this string with the element $\mathbf{v} = (0,1,1,1,1,0,1) \in \mathbb{Z}_2^7$. Also, we can think of the "error" as $\mathbf{e} = (0,0,1,0,0,0,1) \in \mathbb{Z}_2^7$, where an entry 1 will indicate an error in transmission (so we know that the 3rd and 7th entries have been incorrectly received while all other entries have been correctly received). Note that if we interpret $\mathbf{w}$, $\mathbf{v}$ and $\mathbf{e}$ as elements of the group $\mathbb{Z}_2^7$ with coordinate-wise addition modulo 2, then we have

$$\begin{aligned} \mathbf{w} + \mathbf{v} &= \mathbf{e}, \\ \mathbf{w} + \mathbf{e} &= \mathbf{v}, \\ \mathbf{v} + \mathbf{e} &= \mathbf{w}. \end{aligned}$$

Suppose now that for each digit of w, there is a probability p of incorrect transmission. Suppose we also assume that the transmission of any signal does not in any way depend on the transmission of prior signals. Then the probability of having the error $\mathbf{e} = (0, 0, 1, 0, 0, 0, 1)$ is

$$(1-p)^2 p(1-p)^3 p = p^2(1-p)^5.$$

We now formalize the above.

Suppose that we send the string $w = w_1 \ldots w_n \in \{0,1\}^n$. We identify this string with the element $\mathbf{w} = (w_1, \ldots, w_n)$ of the cartesian product

$$\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n}.$$

Suppose now that the message received is the string $v = v_1 \ldots v_n \in \{0,1\}^n$. We identify this string with the element $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}_2^n$. Then the "error" $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{Z}_2^n$ is defined by

$$\mathbf{e} = \mathbf{w} + \mathbf{v}$$

if we interpret $\mathbf{w}$, $\mathbf{v}$ and $\mathbf{e}$ as elements of the group $\mathbb{Z}_2^n$ with coordinate-wise addition modulo 2. Note also that $\mathbf{w} + \mathbf{e} = \mathbf{v}$ and $\mathbf{v} + \mathbf{e} = \mathbf{w}$.

We shall make no distinction between the strings $w, v, e \in \{0,1\}^n$ and their corresponding elements $\mathbf{w}, \mathbf{v}, \mathbf{e} \in \mathbb{Z}_2^n$, and shall henceforth abuse notation and write $w, v, e \in \mathbb{Z}_2^n$ and $e = w + v$ to mean $\mathbf{w}, \mathbf{v}, \mathbf{e} \in \mathbb{Z}_2^n$ and $\mathbf{e} = \mathbf{w} + \mathbf{v}$ respectively.

PROPOSITION 10A. *Suppose that $w \in \mathbb{Z}_2^n$. Suppose further that for each digit of w, there is a probability p of incorrect transmission, and that the transmission of any signal does not in any way depend on the transmission of prior signals.*

(a) The probability of the string $e \in \mathbb{Z}_2^n$ having a particular pattern which consists of k 1's and $(n-k)$ 0's is $p^k(1-p)^{n-k}$.

(b) The probability of the string $e \in \mathbb{Z}_2^n$ having exactly k 1's is

$$\binom{n}{k} p^k (1-p)^{n-k}.$$

PROOF. (a) The probability of the k fixed positions all having entries 1 is p^k, and the probability of the remaining positions all having entries 0 is $(1-p)^{n-k}$. The result follows.

(b) Note that there are exactly $\binom{n}{k}$ patterns of the string $e \in \mathbb{Z}_2^n$ with exactly k 1's. ◯

Note now that if p is "small", then the probability of having 2 errors in the received signal is "negligible" compared to the probability of having 1 error in the received signal.

10.2. Improvement to Accuracy

One way to decrease the possibility of error is to use extra digits. Suppose that $m \in \mathbb{N}$, and that we wish to transmit strings in $\mathbb{Z}_2^m$, of length m.

(1) We shall first of all add, or concatenate, extra digits to each string in $\mathbb{Z}_2^m$ in order to make it a string in $\mathbb{Z}_2^n$, of length n. This process is known as encoding and is represented by a function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$. The set $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$ is called the code, and its elements are called the code words.

(2) To ensure that different strings do not end up the same during encoding, we must ensure that the function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is one-to-one.
(3) Suppose now that $w \in \mathbb{Z}_2^m$, and that $c = \alpha(w) \in \mathbb{Z}_2^n$. Suppose further that during transmission, the string $c \in \mathbb{Z}_2^n$ is received as $\tau(c)$. As errors may occur during transmission, τ is not a function.
(4) On receipt of the transmission, we now want to decode the message $\tau(c)$ (in the hope that it is actually c) to recover w. This is known as the decoding process, and is represented by a function $\sigma : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$.
(5) Ideally the composition $\sigma \circ \tau \circ \alpha$ should be the identity function. As this cannot be achieved, we hope to find two functions $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ and $\sigma : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ so that $(\sigma \circ \tau \circ \alpha)(w) = w$ or the error $\tau(c) \neq c$ can be detected with a high probability.
(6) This scheme is known as the (n, m) block code. The ratio m/n is known as the rate of the code, and measures the efficiency of our scheme. Naturally, we hope that it will not be necessary to add too many digits during encoding.

Example 10.2.1. Consider an $(8, 7)$ block code. Define the encoding function $\alpha : \mathbb{Z}_2^7 \to \mathbb{Z}_2^8$ in the following way: For each string $w = w_1 \ldots w_7 \in \mathbb{Z}_2^7$, let $\alpha(w) = w_1 \ldots w_7 w_8$, where the extra digit $w_8 = w_1 + \ldots + w_7 \pmod 2$. It is easy to see that for every $w \in \mathbb{Z}_2^7$, the string $\alpha(w)$ always contains an even number of 1's. It follows that a single error in transmission will always be detected. Note, however, that while an error may be detected, we have no way to correct it.

Example 10.2.2. Consider next a $(21, 7)$ block code. Define the encoding function $\alpha : \mathbb{Z}_2^7 \to \mathbb{Z}_2^{21}$ in the following way. For each string $w = w_1 \ldots w_7 \in \mathbb{Z}_2^7$, let $c = \alpha(w) = w_1 \ldots w_7 w_1 \ldots w_7 w_1 \ldots w_7$; in other words, we repeat the string two more times. After transmission, suppose that the string $\tau(c) = v_1 \ldots v_7 v_1' \ldots v_7' v_1'' \ldots v_7''$. We now use the decoding function $\sigma : \mathbb{Z}_2^{21} \to \mathbb{Z}_2^7$, where

$$\sigma(v_1 \ldots v_7 v_1' \ldots v_7' v_1'' \ldots v_7'') = u_1 \ldots u_7,$$

and where, for every $j = 1, \ldots, 7$, the digit u_j is equal to the majority of the three entries v_j, v_j' and v_j''. It follows that if at most one entry among v_j, v_j' and v_j'' is different from w_j, then we still have $u_j = w_j$.

10.3. The Hamming Metric

In this section, we discuss some ideas due to Hamming. Throughout this section, we have $n \in \mathbb{N}$.

Definition. Suppose that $x = x_1 \ldots x_n \in \mathbb{Z}_2^n$. Then the weight of x is given by

$$\omega(x) = |\{j = 1, \ldots, n : x_j = 1\}|;$$

in other words, $\omega(x)$ denotes the number of non-zero entries among the digits of x.

Definition. Suppose that $x = x_1 \ldots x_n \in \mathbb{Z}_2^n$ and $y = y_1 \ldots y_n \in \mathbb{Z}_2^n$. Then the distance between x and y is given by

$$\delta(x, y) = |\{j = 1, \ldots, n : x_j \neq y_j\}|;$$

in other words, $\delta(x, y)$ denotes the number of pairs of corresponding entries of x and y which are different.

PROPOSITION 10B. *Suppose that $x, y \in \mathbb{Z}_2^n$. Then $\delta(x, y) = \omega(x + y)$.*

Proof. Note simply that $x_j \neq y_j$ if and only if $x_j + y_j = 1$. ◯

PROPOSITION 10C. *Suppose that $x, y \in \mathbb{Z}_2^n$. Then $\omega(x+y) \le \omega(x) + \omega(y)$.*

PROOF. Suppose that $x = x_1 \ldots x_n$ and $y = y_1 \ldots y_n$. Let $x + y = z_1 \ldots z_n$. It is easy to check that for every $j = 1, \ldots, n$, we have

$$z_j \le x_j + y_j, \tag{1}$$

where the addition + on the right-hand side of (1) is ordinary addition. The required result follows easily. ◯

PROPOSITION 10D. *The distance function $\delta : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{N} \cup \{0\}$ satisfies the following conditions. For every $x, y, z \in \mathbb{Z}_2^n$,*
(a) $\delta(x, y) \ge 0$;
(b) $\delta(x, y) = 0$ if and only if $x = y$;
(c) $\delta(x, y) = \delta(y, x)$; and
(d) $\delta(x, z) \le \delta(x, y) + \delta(y, z)$.

PROOF. The proof of (a)–(c) is straightforward. To prove (d), note that in $\mathbb{Z}_2^n$, we have $y + y = 0$. It follows that

$$\omega(x + z) = \omega(x + y + y + z) \le \omega(x + y) + \omega(y + z).$$

(d) follows on noting Proposition 10C. ◯

REMARK. The pair $(\mathbb{Z}_2^n, \delta)$ is an example of a metric space, and the function δ is usually called the Hamming metric.

DEFINITION. Suppose that $k \in \mathbb{N}$, and that $x \in \mathbb{Z}_2^n$. Then the set

$$B(x, k) = \{y \in \mathbb{Z}_2^n : \delta(x, y) \le k\}$$

is called the closed ball with centre x and radius k.

EXAMPLE 10.3.1. Suppose that $n = 5$ and $k = 1$. Then

$$B(10101, 1) = \{10101, 00101, 11101, 10001, 10111, 10100\}.$$

The key ideas in this section are summarized by the following result.

PROPOSITION 10E. *Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is an encoding function, and that $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$.*
(a) If $\delta(x, y) > k$ for all strings $x, y \in \mathcal{C}$ with $x \ne y$, then a transmission with $\delta(c, \tau(c)) \le k$ can always be detected; in other words, a transmission with at most k errors can always be detected.
(b) If $\delta(x, y) > 2k$ for all strings $x, y \in \mathcal{C}$ with $x \ne y$, then a transmission with $\delta(c, \tau(c)) \le k$ can always be detected and corrected; in other words, a transmission with at most k errors can always be detected and corrected.

PROOF. (a) Since $\delta(x, y) > k$ for all strings $x, y \in \mathcal{C}$ with $x \ne y$, it follows that for every $c \in \mathcal{C}$, we must have $B(c, k) \cap \mathcal{C} = \{c\}$. It follows that with a transmission with at least 1 and at most k errors, we must have $\tau(c) \ne c$ and $\tau(c) \in B(c, k)$. It follows that $\tau(c) \notin \mathcal{C}$.

(b) In view of (a), clearly any transmission with at least 1 and at most k errors can be detected. On the other hand, for any $x \in \mathcal{C}$ with $x \ne c$, we have $2k < \delta(c, x) \le \delta(c, \tau(c)) + \delta(\tau(c), x)$. Since $\delta(c, \tau(c)) \le k$, we must have, for any $x \in \mathcal{C}$ with $x \ne c$, that $\delta(x, \tau(c)) > k$, so that $\tau(c) \notin B(x, k)$. Hence we know precisely which element of $\mathcal{C}$ has given rise to $\tau(c)$. ◯

Problems for Chapter 10

1. Consider the $(8,7)$ block code discussed in Section 10.2. Check the following messages for possible errors:
   a) 10110101 b) 01010101 c) 11111101

2. Consider the $(21,7)$ block code discussed in Section 10.2. Decode the strings below:
   a) 101011010101101010110 b) 110010111001111110101 c) 011110101111110111101

3. For each of the following encoding functions, find the minimum distance between code words. Discuss also the error-detecting and error-correcting capabilities of each code:
   a) $\alpha : \mathbb{Z}_2^2 \to \mathbb{Z}_2^{24}$
   $00 \to 000000000000000000000000$
   $01 \to 111111111111000000000000$
   $10 \to 000000000000111111111111$
   $11 \to 111111111111111111111111$

   b) $\alpha : \mathbb{Z}_2^3 \to \mathbb{Z}_2^7$
   $000 \to 0001110$ $001 \to 0010011$
   $010 \to 0100101$ $011 \to 0111000$
   $100 \to 1001001$ $101 \to 1010101$
   $110 \to 1100010$ $111 \to 1110000$