Coding Theory

Introduction

Coding theory deals with the fast and accurate transmission of messages over an electronic "channel" (telephone, telegraph, radio, TV, satellite, computer relay, etc.) that is subject to "noise" (atmospheric conditions, interference from nearby electronic devices, equipment failures, etc.). The noise may cause errors so that the message received is not the same as the one that was sent. The aim of coding theory is to enable the receiver to detect such errors and, if possible, to correct them.*

EXAMPLE Suppose that the message to be sent is a single digit, either 1 or 0. The message might be, for example, a signal to tell a satellite whether or not to orbit a distant planet. With a single-digit message, the receiver has no way to tell if an error has occurred. But suppose instead that a four-digit message is sent: 1111 for 1 or 0000 for 0. Then this code can correct single errors. For instance, if 1101 is received, then it seems likely that a single error has been made and that 1111 is the correct message. It's possible, of course, that three errors were made and the correct message is 0000. But this is much less likely than a single error.† The code can *detect* double errors, but not correct them. For instance, if 1100 is received, then two errors probably have been made, but the intended message isn't clear.

This example illustrates in simplified form the basic components of coding theory. The numerical *message words* (0 and 1) are translated into *codewords* (0000 and 1111). Only codewords are transmitted, but in the example any four-digit string of 0's and 1's is a possible *received word*. By comparing received words with codewords and deciding the most likely error, a *decoder* detects errors and, when possible, corrects them.* Finally, the corrected codewords are translated back to message words, or an error is signaled for received words that can't be corrected.

Linear Codes

For each positive integer n, $B(n)$ denotes the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ of n copies of $\mathbb{Z}_2$. With coordinatewise addition, $B(n)$ is an additive group of order 2^n (Exercise 10). The elements of $B(n)$ will be written as strings of 0's and 1's of length n. If $0 < k < n$, then an **(n,k) binary linear code** consists of a subgroup C of $B(n)$ of order 2^k. For convenience, C is often called an (n,k) code, a linear code, or just a code.** The elements of C are called **codewords**. Only codewords are transmitted, but any element of $B(n)$ can be a **received word**.

In the preceding example, $C = \{0000, 1111\}$ is a $(4,1)$ code since C is a subgroup of order 2^1 of the group $B(4) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ of order 2^4. In this case the set of message words is just $\mathbb{Z}_2$. Similarly, when dealing with any (n,k) code we shall consider the group $B(k) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (k copies of $\mathbb{Z}_2$), which has order 2^k, to be the set of **message words**.

If a codeword u is transmitted and the word w is received, then the number of errors in the transmission is the number of coordinates in which u and w differ, that is, the Hamming distance from u to w. Since a large number of transmission errors is less likely than a small number (Exercise 27), the nearest codeword to a received word is most likely to be the codeword that was transmitted. Therefore, *a received word is decoded as the codeword that is nearest to it in Hamming distance.* If there is more than one codeword nearest to it, the decoder signals an error.* This process is called **nearest-neighbor decoding.****

A linear code is said to correct t **errors** if every codeword that is transmitted with t or fewer errors is correctly decoded by nearest-neighbor decoding.

Basic Definitions

DEFINITION *The **Hamming weight** of an element u of B(n) is the number of nonzero coordinates in u; it is denoted Wt(u).*

EXAMPLE If $u = 11011$ in $B(5)$, then $\mathrm{Wt}(u) = 4$. Similarly, $v = 1010010 \in B(7)$ has weight 3, and 0000000 has weight 0.

DEFINITION *Let $u, v \in B(n)$. The **Hamming distance** between u and v, denoted $d(u,v)$, is the number of coordinates in which u and v differ.**

EXAMPLE If $u = 00101$ and $v = 10111$ in $B(5)$, then $d(u,v) = 2$ because u and v differ in the first and fourth coordinates. In $B(4)$ the distance between 0000 and 1111 is 4.

Useful Theorems

Theorem 1: A linear code corrects t errors if and only if the hamming distance between any two code words is at least $2t+1$

Theorem 2: A linear code detects t errors if and only if the hamming distance between any two code words is at least $t+1$

Theorem 3: A linear code detects $2t$ errors and corrects t errors if and only if the hamming weight of every nonzero code word is at least $2t+1$

Standard Generator Matrix Technique

One efficient technique for constructing linear codes is based on matrix multiplication. Codes constructed in this way are automatically equipped with an encoding algorithm that assigns each message word to a unique codeword.

EXAMPLE We shall construct a $(7,4)$ code. The message words will be the elements of $B(4)$, and the codewords elements of $B(7)$. Message words are considered as row vectors and converted to codewords by right multiplying by the following matrix, whose entries are in $\mathbb{Z}_2$:

Standard Generator Matrix Technique

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

For instance, the message word 1101 is converted to the codeword 1101001 because

$$(1 \quad 1 \quad 0 \quad 1) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1).$$

Standard Generator Matrix Technique

The complete set C of codewords may be found similarly:

Message Word	*Codeword*	*Message Word*	*Codeword*
0000	0000000	1000	1000011
0001	0001111	1001	1001100
0010	0010110	1010	1010101
0011	0011001	1011	1011010
0100	0100101	1100	1100110
0101	0101010	1101	1101001
0110	0110011	1110	1110000
0111	0111100	1111	1111111

Standard Generator Matrix Technique

The table shows that every nonzero code word has hamming weight at least 3= 2(1)+1, t=1

Hence this code detects 2 errors and corrects 1 error

<u>Exercise:</u>

List all code words generated by the following matrix then determine the number of errors that will be detected and corrected

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

Standard Array Decoding (Coset Decoding)

EXAMPLE Let C be the (5,2) code {00000, 10110, 01101, 11011}. From the elements of $B(5)$ *not* in C, choose one of smallest weight (which in this case is weight 1), say $e_1 = 10000$. Form its coset $e_1 + C$ by adding e_1 successively to the elements of C and list the coset elements, with $e_1 + c$ directly below c for each $c \in C$:

C:	00000	10110	01101	11011
$e_1 + C$:	10000	00110	11101	01011

Thus, for example, 11101 is directly below $01101 \in C$ because $e_1 + 01101 = 10000 + 01101 = 11101$. Among the elements not listed above, choose one of smallest weight, say $e_2 = 01000$, and list its coset in the same way (with $e_2 + c$ below $c \in C$):

Standard Array Decoding (Coset Decoding)

C:	00000	10110	01101	11011
$e_1 + C$:	10000	00110	11101	01011
$e_2 + C$:	01000	11110	00101	10011

Among the elements not yet listed, choose one of smallest weight and list its coset, and continue in this way until every element of $B(5)$ is on the table. Verify that this is a complete table:

00000	10110	01101	11011	Codewords
10000	00110	11101	01011	
01000	11110	00101	10011	
00100	10010	01001	11111	Received Words
00010	10100	01111	11001	
00001	10111	01100	11010	
11000	01110	10101	00011	
10001	00111	11100	01010	

Standard Array Decoding (Coset Decoding)

The decoding rule (which will be justified below) is: *Decode a received word w as the codeword at the top of the column in which w appears*. For instance, 01001 (fourth row) is decoded as 01101; and 01010 (last row) is decoded as 11011. Similarly, 11000 (seventh row) is decoded as 00000.

Exercise:

Construct the standard array table for the following set of code words (0000, 0111, 1000,1111) then correct the following : 1101, 1010