11.1 Coding of Binary Information and Error Detection

The basic unit of information, called a **message**, is a finite sequence of characters from a finite alphabet. We shall choose as our alphabet the set $B = \{0, 1\}$. Every character or symbol that we want to transmit is now represented as a sequence of m elements from B. That is, every character or symbol is represented in binary form. Our basic unit of information, called a **word**, is a sequence of m 0's and 1's.

TABLE 11.1

+	0	1
0	0	1
1	1	0

The set B is a group under the binary operation $+$ whose table is shown in Table 11.1. (See Example 5 of Section 9.4.) If we think of B as the group $\mathbb{Z}_2$, then $+$ is merely mod 2 addition. It follows from Theorem 1 of Section 9.5 that $B^m = B \times B \times \cdots \times B$ (m factors) is a group under the operation $\oplus$ defined by

$$(x_1, x_2, \ldots, x_m) \oplus (y_1, y_2, \ldots, y_m) = (x_1 + y_1, x_2 + y_2, \ldots, x_m + y_m).$$

This group has been introduced in Example 2 of Section 9.5. Its identity is $\bar{0} = (0, 0, \ldots, 0)$ and every element is its own inverse. An element in B^m will be written as $(b_1, b_2, \ldots, b_m)$ or more simply as $b_1 b_2 \cdots b_m$. Observe that B^m has 2^m elements. That is, the order of the group B^m is 2^m.

Figure 11.1 shows the basic process of sending a word from one point to another point over a transmission channel. An element $x \in B^m$ is sent through the transmission channel and is received as an element $x_t \in B^m$. In actual practice, the transmission channel may suffer disturbances, which are generally called **noise**, due to weather interference, electrical problems, and so on, that may cause a 0 to be received as a 1, or vice versa. This erroneous transmission of digits in a word being sent may give rise to the situation where the word received is different from the word that was sent; that is, $x \neq x_t$. If an error does occur, then x_t could be any element of B^m.

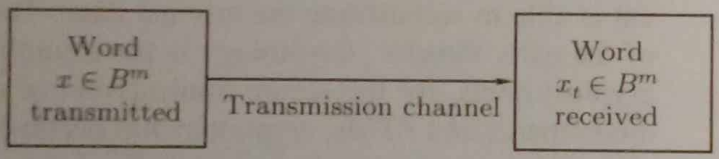

Figure 11.1

The basic task in the transmission of information is to reduce the likelihood of receiving a word that differs from the word that was sent. This is done as follows. We first choose an integer $n > m$ and a one-to-one function $e: B^m \to B^n$. The function e is called an (m, n) **encoding function**, and we view it as a means of representing every word in B^m as a word in B^n. If $b \in B^m$, then $e(b)$ is called the **code word** representing b. The additional 0's and 1's can provide the means to detect or correct errors produced in the transmission channel.

We now transmit the code words by means of a transmission channel. Then each code word $x = e(b)$ is received as the word x_t in B^n. This situation is illustrated in Figure 11.2.

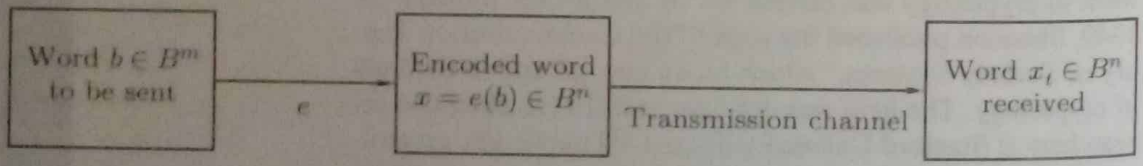

Figure 11.2

Observe that we want an encoding function e to be one to one so that different words in B^m will be assigned different code words.

If the transmission channel is noiseless, then $x_t = x$ for all x in B^n. In this case $x = e(b)$ is received for each $b \in B^m$, and since e is a known function, b may be identified.

In general, errors in transmission do occur. We will say that the code word $x = e(b)$ has been transmitted with **k or fewer errors** if x and x_t differ in at least 1 but no more than k positions.

Let $e: B^m \to B^n$ be an (m, n) encoding function. We say that e **detects k or fewer errors** if whenever $x = e(b)$ is transmitted with k or fewer errors, then x_t is not a code word (thus x_t could not be x and therefore could not have been correctly transmitted). For $x \in B^n$, the number of 1's in x is called the **weight** of x and is denoted by $|x|$.

Example 1 Find the weight of each of the following words in B^5:

(a) $x = 01000$ **(b)** $x = 11100$ **(c)** $x = 00000$ **(d)** $x = 11111$

Solution

(a) $|x| = 1$ **(b)** $|x| = 3$ **(c)** $|x| = 0$ **(d)** $|x| = 5$ ◆

Example 2 *Parity Check Code*

The following encoding function $e: B^m \to B^{m+1}$ is called the **parity $(m, m+1)$ check code**: If $b = b_1 b_2 \cdots b_m \in B^m$, define

$$e(b) = b_1 b_2 \cdots b_m b_{m+1},$$

where

$$b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd.} \end{cases}$$

Observe that b_{m+1} is zero if and only if the number of 1's in b is an even number. It then follows that every code word $e(b)$ has even weight. A single error in the transmission of a code word will change the received word to a word of odd weight and therefore can be detected. In the same way we see that any odd number of errors can be detected.

For a concrete illustration of this encoding function, let $m = 3$. Then

$$\left.\begin{array}{l} e(000) = 0000 \\ e(001) = 0011 \\ e(010) = 0101 \\ e(011) = 0110 \\ e(100) = 1001 \\ e(101) = 1010 \\ e(110) = 1100 \\ e(111) = 1111 \end{array}\right\} \text{ code words.}$$

Suppose now that $b = 111$. Then $x = e(b) = 1111$. If the transmission channel transmits x as $x_t = 1101$, then $|x_t| = 3$, and we know that an odd number of errors (at least one) has occurred. ◆

It should be noted that if the received word has even weight, then we cannot conclude that the code word was transmitted correctly, since this encoding function does not detect an even number of errors. Despite this limitation, the parity check code is widely used.

Example 3 Consider the following $(m, 3m)$ encoding function $e: B^m \to B^{3m}$. If

$$b = b_1 b_2 \cdots b_m \in B^m,$$

define

$$e(b) = e(b_1b_2\cdots b_m) = b_1b_2\cdots b_mb_1b_2\cdots b_mb_1b_2\cdots b_m.$$

That is, the encoding function e repeats each word of B^m three times. For a concrete example, let $m = 3$. Then

$$\left.\begin{aligned} e(000) &= 000000000\\ e(001) &= 001001001\\ e(010) &= 010010010\\ e(011) &= 011011011\\ e(100) &= 100100100\\ e(101) &= 101101101\\ e(110) &= 110110110\\ e(111) &= 111111111 \end{aligned}\right\} \text{ code words.}$$

Suppose now that $b = 011$. Then $e(011) = 011\underline{0}11011$. Assume now that the transmission channel makes an error in the underlined digit and that we receive the word 011111011. This is not a code word, so we have detected the error. It is not hard to see that any single error and any two errors can be detected. ◆

Let x and y be words in B^m. The **Hamming distance** $\delta(x, y)$ between x and y is the weight, $|x \oplus y|$, of $x \oplus y$. Thus the distance between $x = x_1x_2\cdots x_m$ and $y = y_1y_2\cdots y_m$ is the number of values of i such that $x_i \neq y_i$, that is, the number of positions in which x and y differ. Using the weight of $x \oplus y$ is a convenient way to count the number of different positions.

Example 4 Find the distance between x and y:

(a) $x = 110110$, $y = 000101$

(b) $x = 001100$, $y = 010110$

Solution

(a) $x \oplus y = 110011$, so $|x \oplus y| = 4$

(b) $x \oplus y = 011010$, so $|x \oplus y| = 3$ ◆

THEOREM 1 *Properties of the Distance Function*

Let x, y, and z be elements of B^m. Then

(a) $\delta(x, y) = \delta(y, x)$

(b) $\delta(x, y) \geq 0$

(c) $\delta(x, y) = 0$ if and only if $x = y$

(d) $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Proof

Properties (a), (b), and (c) are simple to prove and are left as exercises.

(d) For a and b in B^m,

$$|a \oplus b| \leq |a| + |b|,$$

since at any position where a and b differ one of them must contain a 1. Also, if $a \in B^m$, then $a \oplus a = \bar{0}$, the identity element in B^m. Then

$$\begin{aligned} \delta(x, y) = |x \oplus y| &= |x \oplus \bar{0} \oplus y| = |x \oplus z \oplus z \oplus y|\\ &\leq |x \oplus z| + |z \oplus y|\\ &= \delta(x, z) + \delta(z, y). \end{aligned}$$

■

The **minimum distance** of an encoding function $e: B^m \to B^n$ is the minimum of the distances between all distinct pairs of code words; that is,

$$\min\{\delta(e(x), e(y)) \mid x, y \in B^m\}.$$

Example 5 Consider the following (2, 5) encoding function e:

$$\left.\begin{aligned} e(00) &= 00000 \\ e(10) &= 00111 \\ e(01) &= 01110 \\ e(11) &= 11111 \end{aligned}\right\} \text{ code words.}$$

The minimum distance is 2, as can be checked by computing the minimum of the distances between all six distinct pairs of code words. ◆

THEOREM 2 An (m, n) encoding function $e: B^m \to B^n$ can detect k or fewer errors if and only if its minimum distance is at least $k + 1$.

Proof

Suppose that the minimum distance between any two code words is at least $k + 1$. Let $b \in B^m$, and let $x = e(b) \in B^n$ be the code word representing b. Then x is transmitted and is received as x_t. If x_t were a code word different from x, then $\delta(x, x_t) \geq k + 1$, so x would be transmitted with $k + 1$ or more errors. Thus, if x is transmitted with k or fewer errors, then x_t cannot be a code word. This means that e can detect k or fewer errors.

Conversely, suppose that the minimum distance between code words is $r \leq k$, and let x and y be code words with $\delta(x, y) = r$. If $x_t = y$, that is, if x is transmitted and is mistakenly received as y, then $r \leq k$ errors have been committed and have not been detected. Thus it is not true that e can detect k or fewer errors. ■

Example 6 Consider the (3, 8) encoding function $e: B^3 \to B^8$ defined by

$$\left.\begin{aligned} e(000) &= 00000000 \\ e(001) &= 10111000 \\ e(010) &= 00101101 \\ e(011) &= 10010101 \\ e(100) &= 10100100 \\ e(101) &= 10001001 \\ e(110) &= 00011100 \\ e(111) &= 00110001 \end{aligned}\right\} \text{ code words.}$$

How many errors will e detect?

Solution

The minimum distance of e is 3, as can be checked by computing the minimum of the distances between all 28 distinct pairs of code words. By Theorem 2, the code will detect k or fewer errors if and only if its minimum distance is at least $k + 1$. Since the minimum distance is 3, we have $3 \geq k + 1$ or $k \leq 2$. Thus the code will detect two or fewer errors. ◆

Group Codes

So far, we have not made use of the fact that $(B^n, \oplus)$ is a group. We shall now consider an encoding function that makes use of this property of B^n.

An (m, n) encoding function $e: B^m \to B^n$ is called a **group code** if

$$e(B^m) = \{e(b) \mid b \in B^m\} = \text{Ran}(e)$$

is a subgroup of B^n.

Recall from the definition of subgroup given in Section 9.4 that N is a subgroup of B^n if (a) the identity of B^n is in N, (b) if x and y belong to N, then $x \oplus y \in N$, and (c) if x is in N, then its inverse is in N. Property (c) need not be checked here, since every element in B^n is its own inverse. Moreover, since B^n is Abelian, every subgroup of B^n is a normal subgroup.

Example 7 Consider the (3, 6) encoding function $e: B^3 \to B^6$ defined by

$$\left.\begin{array}{l} e(000) = 000000 \\ e(001) = 001100 \\ e(010) = 010011 \\ e(011) = 011111 \\ e(100) = 100101 \\ e(101) = 101001 \\ e(110) = 110110 \\ e(111) = 111010 \end{array}\right\} \text{code words.}$$

Show that this encoding function is a group code.

Solution

We must show that the set of all code words

$$N = \{000000, 001100, 010011, 011111, 100101, 101001, 110110, 111010\}$$

is a subgroup of B^6. This is done by first noting that the identity of B^6 belongs to N. Next we verify, by trying all possibilities, that if x and y are elements in N, then $x \oplus y$ is in N. Hence N is a subgroup of B^6, and the given encoding function is a group code. ◆

The strategy of the next proof is similar to the way we often show two sets A and B are the same by showing that $A \subseteq B$ and $B \subseteq A$. Here we show that $\delta = \eta$ by proving $\delta \leq \eta$ and $\eta \leq \delta$.

THEOREM 3 Let $e: B^m \to B^n$ be a group code. The minimum distance of e is the minimum weight of a nonzero code word.

Proof

Let δ be the minimum distance of the group code, and suppose that $\delta = \delta(x, y)$, where x and y are distinct code words. Also, let η be the minimum weight of a nonzero code word and suppose that $\eta = |z|$ for a code word z. Since e is a group code, $x \oplus y$ is a nonzero code word. Thus

$$\delta = \delta(x, y) = |x \oplus y| \geq \eta.$$

On the other hand, since 0 and z are distinct code words,

$$\eta = |z| = |z \oplus 0| = \delta(z, 0) \geq \delta.$$

Hence $\eta = \delta$. ■

One advantage of a group code is given in the following example.