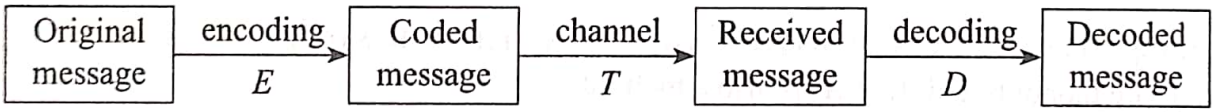
11.7 CODING THEORY

Data communication consists of the transmission of characters from some finite alphabet through some communications channel. Whatever may be the communications channel, be it wires or cables or satellite communication systems, imperfections in the channel will cause a finite probability of error that a transmitted character will be incorrectly received by the receiver. For long messages, even a small error is not tolerable. Generally the characters are encoded in binary as the bits 0 and 1 and the symbols transmitted. Also when bits are transferred from one unit of a system (like memory) to another unit (CPU), errors may creep in and there should be a way of detecting and correcting errors.

Coding theory deals with the ways for improving the reliability of information transformation by systematic codes of various kinds. Most of these efficient codes are group codes, which are based on Lagrange's theorem.

The basic idea used in this is that of encoding and decoding. A sequence of characters to be transmitted is mapped into a longer sequence of the same characters by an encoding scheme. By inspecting the additional information in the extra characters, the receiver is then able to detect/correct errors which have been introduced by noise during transmission. The longer message received is then transferred to a sequence of characters of the original length by a proper method which is called decoding. This process can be pictorially represented as follows:



Definition 1 An $(m, n)-$code for a binary message consists of an encoding scheme $E : B^m \to B^n$ and a decoding scheme $D : B^n \to B^m$ $(m < n)$, which tries to make the transmission of m bit binary words error-free. Here B^n denotes the set of all binary strings of length n.

Example 1 *A simple scheme is to add a extra parity bit and have* $E : B^m \to B^{m+1}$. *If* x *is the m-bit original word and* y *is the* $m + 1$ *bit encoded word, the* $(m + 1)^{th}$ *bit added is* 0 *or* 1 *to make the number of* 1*'s in the encoded word an even number. If* $m = 4$ *and* $x = 0100$, y *is* 01001. *For decoding, the last bit is omitted. If* $y = 01100$, x *is* 0110. *If the received word has odd number of* 1*'s, error has occurred during transmission.*

Example 2 *Consider an encoding scheme* $e : B^m \to B^{5m}$.

$e(a_1 \dots a_m) = a_1 \dots a_m a_1 \dots a_m a_1 \dots a_m a_1 \dots a_m a_1 \dots a_m$.

If $m = 2$,

$e(10) = 1010101010$

The corresponding decoding scheme is defined as follows:

$d(b_1 \dots \dots b_{5m}) = a_1 \dots a_m$

$a_i = 1$ if 3 or more of $b_i, b_{i+m}, b_{i+2m}, b_{i+3m}, b_{i+4m}$ are 1's

$= 0$ otherwise.

Suppose while transmitting 1010101010, the message received is 1011101010, the 4^{th} bit is in error, while decoding it since out of the bits 2, 4, 5, 6, 10 only one is 1, the encoded character 2 is taken as 0.

Hence $d(1011101010) = 10$.

If a double error occurs also, it can be corrected.

If instead of receiving 1010101010, 1011011010 is received, out of bits, 1, 3, 5, 7, 9, four are 1's and hence the encoded character is taken as 1.

Out of bits 2, 4, 6, 8, 10, only one is a 1. Hence the encoded character is taken as 0. So $d(1011011010) = 10$.

The input is a binary sequence. It is divided into blocks of size m and each block of size m is encoded as a binary string of length n and transmitted. Each such binary string used (of length n) is called a codeword. A coding scheme where every m bit string is encoded as a n bit string for the same n is called block code. Block codes are used to detect and correct errors, i.e., find the bits transmitted incorrectly and change them appropriately.

Let B denote the set of all binary sequences of length n. Let $\oplus$ be a binary operation on B such that for x and y in B, $x \oplus y$ is a bit string of length n that has 1's in those positions x and y differ and has 0's in those positions where x and y are the same. For example if $x = 1\ 0\ 0\ 1$, $y = 1\ 1\ 0\ 0$, $x \oplus y$ is $0\ 1\ 0\ 1$. We can show that $(B, \oplus)$ is a group. Closure and associativity can be easily shown, 0^n is the identity and every n bit string is its own inverse.

Definition 2 Let B denote the set of n bit binary strings and $x, y \in B$. The weight of x denoted $w(x)$ is the number of 1's in x. The distance between x and y denoted $d(x, y)$ is the weight of $x \oplus y$, i.e., $w(x \oplus y)$. It is the number of positions in which the two strings differ. It is also called the Hamming distance.

Example 3

Let $x = 0\,1\,1\,0\,0\,1$
and $y = 1\,0\,1\,0\,0\,0$
$w(x) = 3 \quad w(y) = 2$
$x \oplus y = 1\,1\,0\,0\,0\,1$
$w(x \oplus y) = 3$

We can easily verify the following properties of the distance function

(a) $d(x, y) = d(y, x)$
(b) $d(x, y) \geq 0$
(c) $d(x, y) = 0$ if and only if $x = y$
(d) $d(x, y) \leq d(x, z) + d(z, y)$

The last property can be seen as follows

$$w(\alpha \oplus \beta) \leq w(\alpha) + w(\beta)$$

$$w(x \oplus y) = w(x \oplus z + z \oplus y)$$

$$\leq w(x \oplus z) + w(z \oplus y) \qquad \text{taking } \alpha = x \oplus z \text{ and } \beta = z \oplus y$$

i.e., $d(x, y) \leq d(x, z) + d(z, y)$

We can easily verify the following properties of the distance function

(a) $d(x, y) = d(y, x)$
(b) $d(x, y) \geq 0$
(c) $d(x, y) = 0$ if and only if $x = y$
(d) $d(x, y) \leq d(x, z) + d(z, y)$

The last property can be seen as follows

$$w(\alpha \oplus \beta) \leq w(\alpha) + w(\beta)$$
$$w(x \oplus y) = w(x \oplus z + z \oplus y)$$
$$\leq w(x \oplus z) + w(z \oplus y) \qquad \text{taking } \alpha = x \oplus z \text{ and } \beta = z \oplus y$$
$$\text{i.e., } d(x, y) \leq d(x, z) + d(z, y)$$

Minimum Distance, Error Correction and Detection Let G be a block code. The distance of G is the minimum between any pair of distinct codewords in G. The distance of a block code is related to its ability to detect and correct errors. An error occurs if a bit 1 is changed to 0 or 0 is changed to 1.

The relationship between the minimum distance of a code and the amount of error detection or correction possible is given by

$$M - 1 = C + \mathrm{D} \qquad \text{where } C \leq D$$

Here M = minimum distance of a code
C = number of bits in error that can be corrected
D = number of bits in error that can be detected.
No error can be corrected without detecting it. Hence $C \leq D$.

In a $B^m \rightarrow B^n$ code 2^m strings of the total 2^n strings are chosen as codewords. Remaining $2^n - 2^m$ strings are not codewords. In a (2, 5) code, out of 32 strings of length 5, only 4 are valid codewords. While transmitting the length 2 string is coded into length 5 string and transmitted. If the received length 5 string is not a codeword error has occurred. It should be detected and corrected.

An error-detection code is defined according to one less than the minimum error it will not always detect. Thus, if a code detects all single, double and triple errors, and some or no quadruple errors, it is called a triple-error detecting code. This would still be so even if the code detected all quintuple errors. An error correction code is defined in the same manner, i.e., according to one less than the minimum error it will not always correct.

Maximum Likelihood Decoding and Minimum Distance Decoding Let G be a block code where each codeword is of length n and $G = \{x_1, \ldots, x_N\}$ are codewords in G. Suppose a word x was transmitted and the word y was received. If $y \in G$, then we probably think it is the word transmitted. But this need not be so. By some errors, a word x_i might have been received as $x_j = y$. Let $P(x_i \mid y)$ denote the conditional probability that x_i was the transmitted word given that y was the received word. If $P(x_k \mid y)$ is the largest of all conditional probabilities computed, then we conclude that x_k was the transmitted word. Such a criteria for determining the transmitted word is known as maximum-likelihood decoding criterion.

It may not be easy to calculate the conditional probability $P(x_i \mid y)$. So generally another criterion is used which is the minimum distance decoding criterion. This is the one related to the error-detection explained in the previous section. For $i = 1, 2, \ldots, N$, we compute $d(x_i, y)$ and conclude that x_k was the transmitted word if $d(x_k, y)$ is the smallest among all distances computed. If it is assumed that the occurrence of errors in the positions are independent, and that the probability of the occurrence of an error is p, then $P(x_i \mid y) = (1-p)^{n-t} p^t$, where $t = d(x_i, y)$. For $p < \frac{1}{2}$, the smaller $d(x_i, y)$ is, the larger $p(x_i \mid y)$ will be. Thus we see both criteria are equivalent.

Theorem 1 A code of distance $2t + 1$ can correct t or fewer transmission errors when the minimum-distance decoding criteria is considered.

Group codes In this subsection, we consider a class of block codes known as group codes. Let B be the set of all binary sequences of length n. A subset G of B is called a group code if $(G, \oplus)$ is a subgroup of $(B, \oplus)$.

Example 4 *Consider the following* (3, 6) *block code.*
It can be easily checked that it is a group code. f is the encoding function from $B^3 \rightarrow B^6$.

$a^0 = f(000) = 0\ 0\ 0\ 0\ 0\ 0$
$a^1 = f(001) = 0\ 0\ 1\ 1\ 1\ 1$
$a^2 = f(010) = 0\ 1\ 0\ 0\ 1\ 1$
$a^3 = f(011) = 0\ 1\ 1\ 1\ 0\ 0$
$a^4 = f(100) = 1\ 0\ 0\ 1\ 1\ 0$
$a^5 = f(101) = 1\ 0\ 1\ 0\ 0\ 1$
$a^6 = f(110) = 1\ 1\ 0\ 1\ 0\ 1$
$a^7 = f(111) = 1\ 1\ 1\ 0\ 1\ 0$

$(\{a^0, a^1, \ldots, a^7\}, \oplus)$ is a subgroup of $(B^6, \oplus)$. The minimum distance of the above code is 3.

Theorem 2 Let $f: B^m \rightarrow B^n$ be a group code. The minimum distance of the group code f is the minimum weight of a nonzero codeword.

In the example considered above, $d = 3$ and w is also 3.

Now let us see how we can generate group codes. If $X = [x_{ij}]$ and $Y = [y_{ij}]$ are Boolean matrices of size $m \times n$, then $Z = X \oplus Y$ is a Boolean matrix of size $m \times n$ where $z_{ij} = x_{ij} \oplus y_{ij}$. If X is a $m \times n$ Boolean matrix and Y is a $n \times p$ Boolean matrix Z is a $m \times p$ Boolean matrix where $z_{ij} = x_{i1} \cdot y_{1j} \oplus x_{i2} \cdot y_{2j} \oplus \cdots \oplus x_{in} \cdot y_{nj}$ where $\cdot$ denotes $\wedge$ and $\oplus$ mod 2 addition, $(X \oplus Y) * W = (X * W) \oplus (Y * W)$ where $*$ is Boolean matrix multiplication. Here X and Y are $m \times n$ matrices and W is a $n \times p$ matrix.

Let us consider a coding scheme $e : B^m \to B^n$ $(m < n)$. We want the resulting codewords to form a subgroup of B^n. For this, consider a Boolean matrix E of size $m \times n$. The first $m \times m$ submatrix form an identity matrix of size $m \times m$. For example, if E can be chosen as $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$.

(In fact the identity matrix need not be in the first m columns. It can be anywhere).

Then the coding of a word $x = x^1 x^2 x^3$ is given by $x * E$. 000 will be coded as 000000.

Theorem 3 The set of codewords defined by a coding scheme using a Boolean matrix form a group.

Proof: The order of the group is finite. Hence it is enough to prove closure property above. We have also seen that 0^m will be coded as 0^n which will serve as the identity. Suppose E is a $m \times n$ Boolean matrix and the coding scheme $e : B^m \to B^n$ is defined as $e(x) = x * E$, where $*$ denotes Boolean matrix multiplication. Let x' and $x'' \in B^m$ and $x = x' \oplus x''$. $e(x) = e(x' \oplus x'')$.

Let $e(x) = y_1 y_2 \ldots y_n$ and $E = [e_{ij}]$

$$y_j = \sum_{i=1}^{m} x_i e_{ij} = \sum_{i=1}^{m} (x_i' \oplus x_i'') e_{ij}$$

The term $(x_i' \oplus x_i'')e_{ij} = 0$ if $e_{ij} = 0$

It is $x_i' \oplus x_i''$ if $e_{ij} = 1$

$x_i' e_{ij} = x_i'$ and $x_i'' e_{ij} = x_i''$ if $e_{ij} = 1$

Hence $\sum_{i=1}^{m} (x_i' \oplus x_i'')e_{ij} = \sum_{i=1}^{m} x_i' e_{ij} \oplus \sum_{i=1}^{m} x_i'' e_{ij}$

Hence $E(x) = E(x') + E(x'')$

If $y' = x' * E$ and $y'' = x'' * E$

$e(x') = y'$ and $e(x'') = y''$

Hence it follows that

$y = e(x) = e(x' \oplus x'') = e(x') \oplus e(x'') = y' \oplus y''$

Thus closure is proved. So the set of codewords form a group.

Extra Examples

Decoding in Group Codes For group codes, there is an efficient way to determine the transmitted word corresponding to a received word. Let $(G, \oplus)$ be a group code. Let y be the received word. We know that $d(x_i, y) = w(x_i \oplus y)$. Hence the weights of the words in the coset $G \oplus y$ are the distances between codewords in G and y. If $\{x_0, x_1, \ldots, x_n\}$ are the words in G, we want to select x_j such that $x_j \oplus y$ is the smallest. Select

the word with smallest weight in $G \oplus y$. Let this be x'. If more than one has the smallest weight select any one of them. $x' = x_j \oplus y$ for the transmitted word x_j and hence $x_j = x' \oplus y$, so for a group code $(G, \oplus)$, the decoding procedure is as follows:

1. Determine all cosets of G
2. For each coset, pick the word of smallest weight, (one of the smallest weight if there are more than one) This is called the leader of the coset.
3. For a received word y, $x' \oplus y$ is the sent word, where x' is the leader of the coset containing y.

Example 5 *Consider the group code* $(G, \oplus)$ *which is a subgroup of* $(B^6, \oplus)$.

$G = \{a^0, a^1, \ldots, a^7\}$ as given in Example 4.

Consider the cosets of G. The following table gives the cosets of G.

000000	100110	010011	011100	001111	101001	110101	111010
100000	000110	110011	111100	101111	001001	010101	011010
010000	110110	000011	001100	011111	111001	100101	101010
001000	101110	011011	010100	000111	100001	111101	110010
000100	100010	010111	011000	001011	101101	110001	111110
000010	100100	010001	011110	001101	111011	110110	111000
000001	100111	010000	011101	001110	101000	110100	111011
000101	100011	010110	011001	001010	101100	110000	111111

The first row is G itself. The coset leaders are given in the first column. Except for the last row, coset leaders are uniquely chosen. In the last row 000101 is chosen as coset leader. 001010 or 110000 could also be a leader. If the received word is 011110, locate it in the fourth column, sixth row of the table. The coset leader is 000010 and so the transmitted word is $011110 \oplus 000010 = 011100$. It is decoded as 011. A single error is found and corrected (minimum distance 3 code can correct single errors). If 111111 is the codeword received, a double error has occurred as the sent word could be 001111 or 110101 or 111010. It is located in the last row last column. If 000101 is chosen as the coset leader, the sent word is $111111 \oplus 000101 = 111010$. If 001010 is chosen as the coset leader, the sent word is $111111 \oplus 001010 = 110101$. If 110000 is chosen as the coset leader, the sent word is $110000 \oplus 111111 = 001111$. A double error cannot be corrected. Decoding may take any one of 001111 or 110101 or 111010 and give 001 or 110 or 111. ◀

Hamming Codes An ingenious family of perfect codes which will correct all single errors was given by RW Hamming.

The Hamming codes are single-error-correcting codes (with minimum distance 3) which are perfect in the sense that for any r there exists a $(m = 2^r - 1 - r, n = 2^r - 1)$ code which corrects each single error which might occur, no other errors. We already noted that if minimum distance 3 code is suggested, it will correct all single errors but cannot detect double errors and a double error may be taken as a wrong single error and corrected wrongly. If the decoding table in this case is constructed as in the earlier section, the coset leaders will consist of 00…0, and patterns where one of these 0's is replaced by 1. Hamming codes also provide a simple decoding scheme for locating the error and hence correct it. Though their length can be other than $2^r - 1$, in this section we assume the codewords to be of length $2^r - 1$.

The technique for constructing a Hamming code is as follows:

1. Choose an integer r. The message word is of length $2^r - 1 - r$ and the codeword is of length $2^r - 1$.
2. If the codeword is $b_1\, b_2 \ldots b_{2^r-1}$, the bits $b_1, b_2, b_4, b_8, \ldots, b_{2^r-1}$ are checkbits.
If the message word is $a_1\, a_2 \ldots a_{2^r-1-r}$ then $b_3 = a_1, b_5 = a_2, b_6 = a_3, b_7 = a_4 \ldots$ and so on

$b_{2^r-1} = a_{2^r-1-r}$

Suppose $r = 3$ codeword is of length 7 and message word is of length 4.
$a = a_1 a_2\, a_3\, a_4$ is the message word
and $b = b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, b_7$ is the codeword
$b_3 = a_1, b_5 = a_2, b_6 = a_3, b_7 = a_4$ and b_1, b_2, b_4 are checkbits.
3. Form a matrix of $2^r - 1$ rows and r columns, where the row i is the binary number with value i. The matrix for $r = 3$ is

$$\begin{bmatrix} 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{bmatrix}$$

4. Take $bM = 0$ where Boolean matrix multiplication is used. Suppose the codeword is $b = b_1 \ldots b_7$, we get

$$b_4 + b_5 + b_6 + b_7 = 0$$
$$b_2 + b_3 + b_6 + b_7 = 0$$
$$b_1 + b_3 + b_5 + b_7 = 0$$

If the message word is $a_1\, a_2\, a_3\, a_4$, we get

$$b_4 + a_2 + a_3 + a_4 = 0 \pmod 2$$
$$b_2 + a_1 + a_3 + a_4 = 0$$
$$b_1 + a_1 + a_2 + a_4 = 0$$

i.e., b_1 is chosen so that it gets even parity with a_1, a_2, a_4. b_2 is chosen so that it gets even parity with a_1, a_3, a_4. b_4 is chosen so that it gets even parity with a_2, a_3, a_4.

The above procedure yields codewords which will have minimum weight 3, except for θ^{2^r-1}.

There is a simple way to decode these codes. Let a be the sent word and b' be the received word. If a single error has occurred then b' differs from b in one bit position (say the ith bit). Then consider the error vector which has 1 in the ith position and 0 in other positions. Then $b' = b \oplus e$ so that $(b \oplus e)M = bM \oplus eM$. But $bM = 0$. Therefore $b'M = eM$. If the error vector is 0, the result is 0 as no error has occurred. If the error vector is of the form $\underbrace{000\ldots0}_{i-1}\ 1\ \underbrace{000\ldots0}_{2^r-1-i}$ then when this is multiplied by M, the 1 picks out the ith row of the matrix M, which is really the number i represented in binary. This shows that the ith bit is in error and flipping it gives the corrected codeword.

Example 6 *Consider a* (4, 7) *Hamming code. Consider a codeword* $b = 0\,0\,0\,1\,1\,1\,1$. $bM = 0\,0\,0$ *and no error has occurred. Suppose in b, the fifth bit is changed to* 0. *Now the received word* b' *is* $0\,0\,0\,1\,0\,1\,1$. *This is obtained by adding* $e = 0\,0\,0\,0\,1\,0\,0$ to b.

$$b'M = 0\,0\,0\,1\,0\,1\,1 \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = 1\,0\,1$$

This shows the 5th bit is in error and it is changed from 0 to 1.

This cannot detect double errors as the minimum distance is 3. Hamming code may be extended to perfect codes with minimum weight 4 by adding a parity bit to each codeword. This will give a single error-correcting, double error-detecting code.

Exercises

1. Find the weights of
   a) 10110, b) 110110.
2. Find the minimum distance between
   a) 11110 and 10001 b) 1010101 and 0001100
3. Find the minimum distance of the following (2, 4) encoding scheme
   a) $e(00) = 0000$ b) $e(01) = 1011$
   c) $e(10) = 0110$ d) $e(11) = 1100$.
4. Let e be the encoding function $B^m \to B^{m+1}$ where the $(m+1)^{th}$ bit is added to get even parity. Let $d : B^{m+1} \to B^m$ be the corresponding decoding function:
   a) $m = 4$ What is $e(1010)$, $e(1110)$?
   What is $d(11011)$, $d(10100)$?
   b) $m = 6$ What is $e(110101)$, $e(101100)$?
   What is $d(1101100)$, $d(1101001)$, $d(1010100)$?
5. Let e be the encoding function $B^m \to B^{m+1}$ where the $(m+1)^{th}$ bit is added to get odd parity. Let $d : B^{m+1} \to B^m$ be the corresponding decoding function.
   a) $m = 4$ What is $e(1010)$, $e(111)$?
   What is $d(11010)$, $d(10101)$, $d(11000)$?
   b) $m = 6$ What is $e(110101)$, $e(101100)$?
   What is $d(1101101)$, $d(1101001)$?
6. Let e be an encoding scheme $B^m \to B^{3m}$ such that $e(a_1 \ldots a_m) = a_1 \ldots a_m a_1 \ldots a_m a_1 \ldots a_m$. How would you define a decoding scheme so that single errors can be corrected?
7. Consider the encoding scheme $e : B^3 \to B^{15}$ as discussed in Example 2.
   a) What is $e(101)$?
   b) What is $d(101001001101101)$, $d(111011110111111)$?
8. If minimum distance of a code is 5, how many errors can it correct/detect?
9. Consider the following code $e : B^2 \to B^5$
   $e(00) = 00000$
   $e(01) = 01110$
   $e(10) = 10101$
   $e(11) = 11011$
   a) Show that it is a group code.
   b) What is the minimum distance of the code?
   c) Discuss the error detection/correction capability of this code.
10. Consider the (2, 4) group encoding function $e : B^2 \to B^4$ defined by
    $e(00) = 0000$ $e(01) = 0111$
    $e(10) = 1001$ $e(11) = 1111$.
    Decode the following words using minimum distance decoding criterion.
    (a) 0011 (b) 1011 (c) 1111
11. Consider the (3, 6) group encoding function $e : B^3 \to B^6$ defined by
    $e(000) = 000000$ $e(100) = 100101$
    $e(001) = 000110$ $e(101) = 100011$
    $e(010) = 010010$ $e(110) = 110111$
    $e(011) = 010100$ $e(111) = 110001$.
    Decode the following words using minimum distance decoding criterion.
    (a) 011110 (b) 101011 (c) 110010.
12. Consider a (m, n) code and let $r = n - m$.
    a) Given an encoding matrix G, show that there exits a parity-check matrix H such that
    (i) If G is $m \times n$, H is $n \times n(n-m)$.
    (ii) $GH = 0$.
    (iii) Each column h_i, $1 \le i \le n - m$ of H is such that for no scalars θ_i, not all zero, does $\sum_{i=1}^{n-m} a_i h_i = 0$,

that is, the columns of H are linearly independent.

H is called a parity-check matrix because, for any codeword c in the code generated by G, $cH = 0$.

b) Show that given a parity-check matrix for a code, the minimum weight of a codeword (not the 0 codeword) is equal to the minimum number of rows of H which can be added together to give 0.

13. One Hamming code is described by the following matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

(a) Generator matrix (b) Parity–check matrix

Assuming that no more than one error occurs during transmission, what was the transmitted codeword vector when

a) 0111110 is received?

b) 0001111 is received?

14. Consider a (3, 6) code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

What is the probability that a message of six digits will be received and accepted as correctly transmitted through a binary symmetric channel, when in fact at least one error has occurred?

15. Show that if *you* try to use a 2×5 Boolean matrix which does not contain an identity matrix as a matrix for an encoding scheme $e : B^2 \rightarrow B^5$ *you* may not get proper encoding scheme.

11.8 POLYNOMIAL RINGS AND POLYNOMIAL CODES