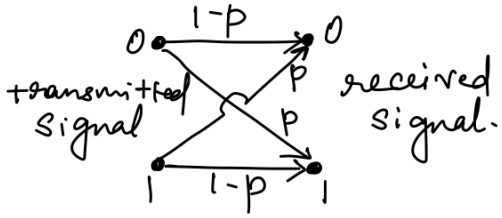
Coding Theory

In this section we introduce an area of applied mathematics called algebraic coding theory. It will be an introductory level as we seek to model the transmission of information represented by strings of the signals 0 and 1.

In digital communications, when information is transmitted in the form of strings of 0^s and 1^s, certain problems arise. As a result of noise in the channel, when a certain signal is transmitted a different signal may be received, thus causing the receiver to make a wrong decision. Hence we want to develop techniques to help us detect and perhaps even correct, transmission errors. However, we can only improve the chances of correct transmissions; there are no guarantees.

The model uses a binary symmetric channel. (binary - since an individual signal is represented by one of the bits 0 or 1). When a transmitter sends the signal 0 or 1 in such a channel, associated with either signal is a (constant) probability p for incorrect transmission. When that probability p is the same for both signals, the channel is called symmetric. Here, for example, we have probability p of sending 0 and having 1 received. The probability of sending signal 0 and having it received correctly is then $1-p$. All possibilities are illustrated in the following figure.



Note:

In coding theory, we assume that the transmission of any signal does not depend in any way on the transmission of prior signals. Consequently, the probability of the occurence of all of these independent events (in their prescribed order) is given by the product of their individual probabilities.

Eg Consider the string $c = 10110$, where c is an element of the group Z_2^5, obtained from the direct product of five copies of $(Z_2, +)$. When sending each bit of c through binary symmetric channel, we assume that probability of incorrect transmission is $p = 0.05$, so that the probability of transmitting c with no errors is $(0.95)^5 = 0.7738$

* What is the probability of sending $c = 10110$ and receiving $r = 00110$? Assume that the probability of incorrect transmission of a bit is $p = 0.05$.

Sol^n $r = 00110$ is the original message with an error in the first position. So the probability of receiving $r = 00110$ is

$$\left(\begin{array}{c}\text{probability of incorrect transmission at 1st position}\end{array}\right) \times \left(\begin{array}{c}\text{probability of correct transmission at remaining positions}\end{array}\right) = 0.05 \times (0.95)^4 = 0.0407$$

* What is the probability of sending $c = 10110$ and receiving (i) $r = 10000$, (ii) $r = 00100$? Assume that the probability of incorrect transmission of a bit is $p = 0.05$.

Sol^n (i) probability of receiving $r = 10000$ is $= (0.95) \times (0.95) \times (0.05) \times (0.05) \times (0.95)$
$= 0.0021$

(ii) probability of receiving $r = 00100$ is $= (0.05) \times (0.95) \times (0.95) \times (0.05) \times (0.95)$
$= 0.0021$

* If $c = 10110$ is transmitted, what is the probability that r differs from c in exactly two places?

Sol^n The desired probability is equal to sum of the probabilities of each error pattern with (error)(error)(no error)(no error)(no error)
Each such pattern has probability $(0.05)^2(0.95)^3$
There are ${}^5C_2$ such patterns, so the probability of two errors in transmission is given by ${}^5C_2 (0.05)^2 (0.95)^3 = 0.0214$

Suppose a signal $c = 10110$ is transmitted and the signal $r = 00110$ is received. Let the probability of incorrect transmission for a bit is 0.05. With the assumption of independent events, the probability of sending c and receiving r, is $(0.05)(0.95)^4 = 0.0407$.

With $e = 10000$, we can write $c + e = r$ and interpret r as the result of the sum of the original message c and the particular error pattern $e = 10000$.

Since $c, r, e \in Z_2^5$ and $-1 = 1$ in Z_2, we can also write $c + r = e$ and $r + e = c$.

Theorem:
Let $c \in Z_n^2$. For the transmission of c through a binary symmetric channel with probability p of incorrect transmission,

(i) the probability of receiving $r = c + e$, where e is a particular error pattern consisting of k 1's and $(n-k)$ 0's is, $p^k(1-p)^{n-k}$.

(ii) the probability that k errors are made in the transmission is ${}^nC_k\, p^k(1-p)^{n-k}$.

Examples
1. Let C be a set of code words, where $C \subseteq Z_2^7$. In each of the following, determine the third term, given any two terms [e (error pattern), r (received word), c (code word)], with $r = c + e$. (i) $c = 1010110$, $r = 1011111$, (ii) $c = 1010110$, $e = 0101101$, (iii) $e = 0101111$, $r = 0000111$.

Soln (i) $e = c + r = 0001001$

(ii) $r = c + e = 1111011$

(iii) $c = r + e = 0101000$.

A binary symmetric channel has probability $p=0.05$ of incorrect transmission. If the code word $c=011011101$ is transmitted, what is the probability that (a) we receive $r=011111101$? (b) we receive $r=111011100$? (c) a single error occurs? (d) a double error occurs?

Soln Given $c=011011101$,

(a) $r=011111101$

out of the 9 positions, there is an error in 4th position

$\therefore P(\text{receiving } r) = (0.05)(0.95)^8 = 0.0332$

(b) $r=111011100$

out of the 9 positions, there is an error in 1st and 9th position, $\therefore P(\text{receiving } r) = (0.05)^2(0.95)^7 = 0.0017$

(c) Probability(error at only one position) $= 0.0332$

Out of the 9 positions, a single error can happen in ${}^9C_1 = 9$ ways

$\therefore$ Probability of single error $= 9 \times 0.0332 = 0.2988$

(d) Probability(error at two positions) $= 0.0017$

Out of the 9 positions, a double error can happen in ${}^9C_2 = 36$ ways

$\therefore$ Probability of double error $= 36 \times 0.0017 = 0.0612$

In actuality, a binary symmetric channel is considered good when $p < 10^{-5}$. However, no matter what else we stipulate, we always want $p < 1/2$.

To improve the accuracy of transmission in a binary symmetric channel, certain types of coding schemes can be used where extra signals are provided.

For $m, n \in \mathbb{Z}^+$, let $n > m$.

Consider $\emptyset \neq W \subseteq Z_2^m$. Set W consists of messages to be transmitted.

we append to each $w \in W$, $n-m$ extra signals to form the code word c, where $c \in Z_2^n$.

This process is called encoding and is represented by the function $E : W \to Z_2^n$. Then $E(w) = c$ and $E(W) = C \subseteq Z_2^n$.

Since the function E simply appends extra bits to the (distinct) messages the encoding process is one-to-one.

Upon transmission, c is received as $T(c)$, where $T(c) \in Z_2^n$. T is not a function because $T(c)$ may be different at different transmission times (for the noise in the channel changes with time).

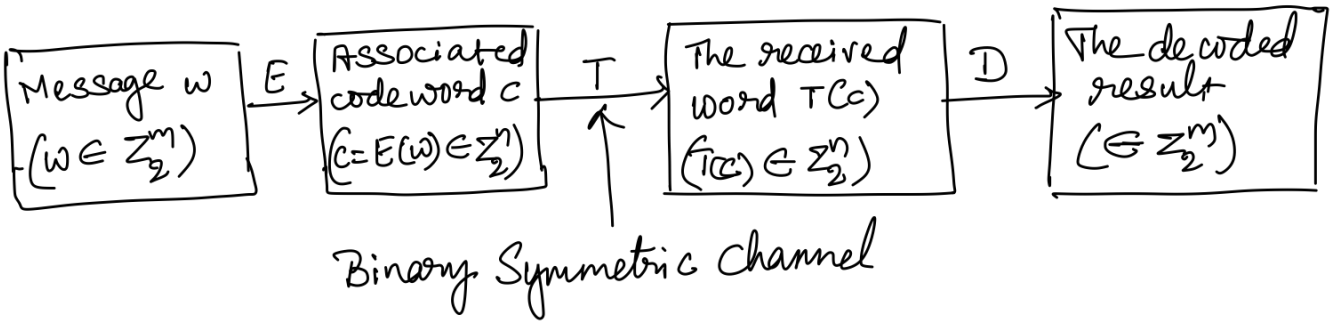
Upon receiving $T(c)$, we want to apply a decoding function $D : Z_2^n \to Z_2^m$ to remove the extra signal and, we hope, obtain the original message w.

Ideally $D \circ T \circ E$ should be the identity function on W, with $D : C \to W$. Since this cannot be expected, we seek functions E and D such that there is a high probability of correctly decoding the received word $T(c)$ and recapturing the original message w.

In addition, we want the ratio $\frac{m}{n}$ to be as large as possible so that an excessive number of signals are not appended to w in getting the code word $c = E(w)$. This ratio $\frac{m}{n}$ measures the efficiency of our scheme and is called the rate of the code.

Finally, the functions E and D should be more theoretical results; they must be practical in the sense that they can be implemented electronically.

In such a scheme, the functions E and D are called the encoding and decoding functions, respectively, of an (n, m) block code.



Parity-check code

Consider the $(m+1, m)$ block code for $m = 8$.
Let $W = Z_2^8$. For any $w = w_1 w_2 \cdots w_8 \in W$, define
$E: Z_2^8 \to Z_2^9$ by $E(w) = w_2 w_2 \cdots w_8 w_9$,
where $w_9 = \sum_{i=1}^{8} w_i$, with the addition performed modulo 2.
ex $E(11001101) = 110011011$, $E(00110011) = 001100110$
For all $w \in Z_2^8$, $E(w)$ contains an even number of 1's.
So for $w = 11010110$ and $E(w) = 110101101$, if we receive
$T(c) = T(E(w))$ as 100101101, from the odd number
of 1's in $T(c)$ we know that a mistake has occured
in transmission. Hence we are able to detect single
errors in transmission.
The probability of sending the code word 110101101
and making at most one error in transmission is

$$\underbrace{(1-p)^9}_{\text{all bits transmitted correctly}} + \underbrace{{}^9C_1\, p(1-p)^8}_{\text{an error is detected at one position.}}$$

For $p = 0.001$, the probability is $(0.999)^9 + {}^9C_1 (0.001)(0.999)^8$
$= 0.999964$
If we detect an error and we are able to relay
a signal back to the transmitter to repeat the
transmission of the code word, and continue this
process until the received word has an even number
of 1's then the probability of sending the code word
110101101 and receiving the correct transmission is
approximately 0.999964.

If an even ~~positive~~ number of ones errors occur in transmission, $T(c)$ is accepted as the correct word and we interpret its first eight components as the original message.

This scheme is called the $(m+1, m)$ parity-check code (even parity-check code as we are looking for even number of ones to occur) and is appropriate only when multiple errors are not likely to occur

If we send the message 1101011 through the channel, we have probability $(0.999)^8 = 0.992028$ of correct transmission.

By using this parity-check code, we increase our chances of getting the correct message to approximately 0.999964.

However (i) an extra signal is sent (perhaps additional transmission are required)

(ii) the rate of code has decreased from 1 to $\frac{8}{9}$.

Note:

1. If we are looking for an even number of ones to occur in $T(c)$, then its called even parity check code.
2. If we are looking for an odd number of ones to occur in $T(c)$, then its called odd parity check code.

example

Suppose 160 bits are sent in successive strings of length 8. Find the probability of receiving the correct message (i) without any coding scheme, (ii) with the parity-check method. Assume $p = 0.001$

Sol^n (i) P(receiving correct message without any coding scheme) $= (0.999)^{160} = 0.852076$.

(ii) P(receiving correct message with parity-check method)

$= \left[(0.999) + {}^{9}C_{8}(0.001)(0.999)^{8}\right]^{20}$

$= (0.999964)^{20} = 0.999280$

* Suppose the message $w = 110101$ is sent. Find the probability of receiving the correct message (i) without any coding scheme. (ii) with the parity-check method. Assume $p = 0.05$.

Sol^n

(i) Probability(receiving correct code without any coding method) $= (0.95)^6 = 0.7351$

(ii) In the parity-check method, we append a bit to the code word, such that the new code has even number of 1s.

$\therefore$ the new code $c = 1101010$

$\therefore$ Probability(receiving correct code with parity-check method) $= (0.95)^7 + {}^{7}C_{1}(0.05)(0.95)^6 = 0.9556$

* For the given codes, apply (i) the even parity check and (ii) the odd parity check and hence write the transmitted code.

(a) $w = 1011$, (b) $w = 1010$, (c) 101101, (d) 110111

Sol^n

code word	even parity	odd parity
(a) 1011	10111	10110
(b) 1010	10100	10101
(c) 101101	1011010	1011011
(d) 110111	1101111	1101110

* For the code 101101, apply the odd parity check. If the following codes are received, determine whether the received codes are correct or not and whether the error is detected or not.

(i) $r = 1011011$, (ii) $r = 1111011$, (iii) $r = 1001111$

Sol"

	original code (w)	transmitted code after odd parity (c)	received code (r)	error in received code Yes / NO	If there is error is error detected Yes / NO
(i)	101101	1011011	1011011	NO	—
(ii)	101101	1011011	1111011	Yes	Yes
(iii)	101101	1011011	1001111	Yes	NO (as there are odd number of ones in both c and r)

* For the code 110111 apply the even parity check. If the following codes are received, determine whether the received codes are correct or not and whether the error is detected or not.

(i) $r = 1101111$, (ii) $r = 1100111$, (iii) $r = 1001011$

Sol"

	original code (w)	transmitted code after odd parity (c)	received code (r)	error in received code Yes / NO	If there is error is error detected Yes / NO
(i)	110111	1101111	1101111	NO	—
(ii)	110111	1101111	1100111	Yes	Yes
(iii)	110111	1101111	1001011	Yes	NO (as there are even number of ones in both c and r)

Triple repetition code:

The $(3m, m)$ triple repetition code is one where we can both detect and correct single errors in transmission.

With $m = 8$ and $W = Z_2^8$, we define $E : Z_2^8 \to Z_2^{24}$ by

$E(w_1, w_2, \ldots, w_8) = w_1 w_2 \ldots w_8 w_1 w_2 \ldots w_8 w_1 w_2 \ldots w_8$.

eg If $w = 10110111$, then $c = E(w) = 101101111011011110110111$

The decoding function $D : Z_2^{24} \to Z_2^8$ is carried out by the majority rule.

eg If $T(c) = 101001110011011110110111$, then we have errors occuring in positions 4, 9 and 24.

We decode $T(c)$ by examining the first, ninth and seventeenth positions to see what signal appears more times.

Here it is 1 (which occurs twice), so we decode the first entry in the decoded message as 1.

Continuing with the entries in the second, tenth and eighteenth positions, the result for the second entry of the decoded message is 0 (which occurs all three times).

3^{rd}, 11^{th} and 19^{th} positions are 1, 1, 1, so decoded message is 1

4^{th}, 12^{th} and 20^{th} positions are 0, 1, 1, so decoded message is 1

5^{th}, 13^{th} and 21^{st} positions are 0, 0, 0, so decoded message is 0

6^{th}, 14^{th} and 22^{nd} positions are 1, 1, 1, so decoded message is 1

7^{th}, 15^{th} and 23^{rd} positions are 1, 1, 1, so decoded message is 1

8^{th}, 16^{th} and 24^{th} positions are 1, 1, 0, so decoded message is 1

So the decoded message is 10110111

Although we have more than one transmission error here, it is acceptable, as the two errors occur after eight or sixteen spaces after the first, i.e, the two incorrect transmissions occur for the same bit of the original message.

With $p = 0.001$, the probability of correctly decoding a single bit is (by majority rule can make at most 1 error out of 3 positions) $(0.999)^3 + {}^3C_1 (0.001)(0.999)^2 = 0.999997$.

So the probability of receiving and correctly decoding the eight-bit message is $(0.999997)^8 = 0.999976$.

Here we transmit 24 signals for this message, so the rate is now $\frac{8}{24} = \frac{1}{3}$

(i) The triple repetition code increases the accuracy and ability to detect and correct single errors (from 0.999964 to 0.999976)

(ii) The rate of code has decreased from $\frac{8}{9}$ to $\frac{1}{3}$.

(iii) But we do not waste time with retransmission.

Examples

1. Let $E: Z_2^3 \to Z_2^9$ be the encoding function for the (9,3) triple repetition code.

(a) If $D: Z_2^9 \to Z_2^3$ is the corresponding decoding function, apply D to decode the received words (i) 111101100, (ii) 010011111.

(b) Find three different received words r for which $D(r) = 000$.

(c) For each $w \in Z_2^3$, what is $|D^{-1}(w)|$?

(a) $r = 111101100$

1st, 4th and 7th positions have 1, 1, 1 ∴ decoded message is 1

2nd, 5th and 8th positions have 1, 0, 0 ∴ decoded message is 0

3rd, 6th and 9th positions have 1, 1, 0 ∴ decoded message is 1

∴ the final decoded word is 101

$r = 010011111$

1st, 4th and 7th positions have 0, 0, 1 ∴ decoded message is 0

2nd, 5th and 8th positions have 1, 1, 1. decoded message is 1

3rd, 6th and 9th positions have 0, 1, 1 ∴ decoded message is 1

∴ the final decoded word is 011

(b) $D(r) = 000$

∴ in the 1st, 4th and 7th positions, 0 should be majority.

2nd, 5th and 8th positions, 0 should be majority.

3rd, 6th and 9th positions, 0 should be majority.

∴ the possible received messages are

000000000, 100000000, 010000000

(c) $D: Z_2^9 \to Z_2^3$ $\quad |Z_2^9| = 512, \quad |Z_2^3| = 8$

$\therefore \forall\, w \in Z_2^3 \quad |D^{-1}(w)| = \frac{|Z_2^9|}{|Z_2^3|} = 64.$

* The $(5m, m)$ five-times repetition code has encoding function $E: Z_2^m \to Z_2^{5m}$, where $E(w) = wwwww$. Decoding with $Z_2^{5m} \to Z_2^m$ is accomplished by the majority rule (here we are able to correct single and double errors made in transmission).

(a) With $p = 0.05$, what is the probability for the transmission and correct decoding of the signal 0?

(b) Answer part (a) for the message 110 in place of the signal 0.

(c) For $m = 2$, decode the received word $r = 01110010001$.

(d) If $m = 2$, find three received words r where $D(r) = 00$.

(e) For $m = 2$ and $D: Z_2^{10} \to Z_2^2$, what is $|D^{-1}(w)|$ for each $w \in Z_2^2$?

Sol^n (a) Here $w = 0$, $\therefore E: Z_2^1 \to Z_2^5$, $\therefore T(w) = 00000$

then $D: Z_2^5 \to Z_2^1$

With $p = 0.05$, the probability of correctly decoding a single bit is (by majority rule can make at most 2 error out of 5 positions)

$(0.95)^5 + {}^5C_1 (0.05)(0.95)^4 + {}^5C_2 (0.05)^2 (0.95)^3 = 0.998842$

So the probability of receiving and correctly decoding the one-bit message is $(0.998842)^1 = 0.998842$.

(b) Here $w = 110$, $E: Z_2^3 \to Z_2^{15}$, $\therefore T(w) = 110110110$

then $D: Z_2^{15} \to Z_2^3$

With $p = 0.05$, the probability of correctly decoding a single bit is (by majority rule can make at most 2 error out of 5 positions)

$(0.95)^5 + {}^5C_1 (0.05)(0.95)^4 + {}^5C_2 (0.05)^2 (0.95)^3 = 0.998842$

So the probability of receiving and correctly decoding the three-bit message is $(0.998842)^3 = 0.996530$

(c) with $m=2$, received word $r = 0111001001$.

The $1^{st}, 3^{rd}, 5^{th}, 7^{th}$ and 9^{th} positions have $0, 1, 0, 1, 0$

by majority rule the correct message is 0

The $2^{nd}, 4^{th}, 6^{th}, 8^{th}$ and 10^{th} positions have $1, 1, 0, 0, 1$

by majority rule the correct message is 1

The decoded message is 01.

(d) $m=2$, and $D(r)=00$, the received word r is

0000000000, 0000000011, 1100000000

(e) $m=2$, $D: Z_2^{10} \to Z_2^2$

for each $w \in Z_2^2$, $|D^{-1}(w)| = \frac{|Z_2^{10}|}{|Z_2^2|} = 256.$

Error-detecting and error-correcting capabilities of a coding scheme.

Consider a code $C \subseteq Z_2^4$, where $c_1 = 0111$, $c_2 = 1111 \in C$. Both the transmitter and the receiver know the elements of C. So if the transmitter sends c_1 but the person receiving the code word receives $T(c_1)$ as 1111, then he or she feels that c_2 was transmitted and makes whatever decision (a wrong one) c_2 implies. Consequently, although only one transmission error was made, the result could be unpleasant. Unfortunately we have two code words that are almost the same. They are rather close to each other, for they differ in only one component

weight of an element, distance between two elements.

For any element $x = x_1 x_2 \cdots x_n \in Z_2^n$, where $n \in Z^+$, the weight of x, denoted by $wt(x)$, is the number of components x_i of x, for $1 \le i \le n$, where $x_i = 1$.

If $y \in Z_2^n$, the distance between x and y, denoted as $d(x, y)$, is the number of components where $x_i \neq y_i$, for $1 \le i \le n$

$\therefore$ For $x, y \in Z_2^n$, $d(x, y) = \sum_{i=1}^{n} d(x_i, y_i)$,

where for each $1 \le i \le n$, $d(x_i, y_i) = \begin{cases} 0, & \text{if } x_i = y_i \\ 1, & \text{if } x_i \neq y_i \end{cases}$

example

* For $n = 5$, let $x = 01001$ and $y = 11101$. Find $wt(x)$, $wt(y)$, $d(x, y)$, $wt(x+y)$.

Sol^n $wt(x) = 2$, $wt(y) = 4$, $d(x, y) = 2$.

$x + y = 10100$, $\therefore wt(x+y) = 2$.

Lemma: For all $x, y \in Z_2^n$, $wt(x+y) \le wt(x) + wt(y)$.

Proof: We prove this lemma by examining, for each $1 \le i \le n$, the components $x_i, y_i, x_i + y_i$ of $x, y, x+y$ respectively. Only one situation would cause this inequality to be false: if $x_i + y_i = 1$ while $x_i = 0$ and $y_i = 0$, for some $1 \le i \le n$. But this will never occur because $x_i + y_i = 1$ implies that exactly one of x_i and y_i is 1.

Example

Verify $wt(x+y) \le wt(x) + wt(y)$, for $x = 01001$, $y = 11101$

Soln Given $x = 01001$, $y = 11101$, $\therefore x + y = 10100$

$wt(x) = 2$, $wt(y) = 4$, $wt(x+y) = 2$

and $2 < 2 + 4$ is true.

i.e. $wt(x+y) < wt(x) + wt(y)$

Theorem: The distance function d defined on $Z_2^n \times Z_2^n$ satisfies the following for all $x, y, z \in Z_2^n$.

(a) $d(x,y) \ge 0$, (b) $d(x,y) = 0$ iff $x = y$, (c) $d(x,y) = d(y,x)$,

(d) $d(x,z) \le d(x,y) + d(y,z)$.

Proof:

(a) $d(x,y) = \sum_{i=1}^{n} d(x_i, y_i) = 0$ if $x_i = y_i \ \forall \ 1 \le i \le n$.

≥ 1 if $\exists$ atleast one $x_i \ne y_i$

$\therefore d(x,y) \ge 0$

(b) Let $d(x,y) = 0 \Rightarrow \sum_{i=1}^{n} d(x_i, y_i) = 0 \Rightarrow x_i = y_i \ \forall \ 1 \le i \le n$. i.e. $x = y$

Let $x = y$, then $x_i = y_i \ \forall \ 1 \le i \le n \Rightarrow \sum_{i=1}^{n} d(x_i, y_i) = 0 \Rightarrow d(x,y) = 0$

(c) Let $d(x,y) = \sum_{i=1}^{n} d(x_i, y_i) = \sum_{i=1}^{n} d(y_i, x_i) = d(y,x)$

(d) In Z_2^n $y + y = 0$ $\therefore d(x,z) = wt(x+z) = wt(x+y+y+z)$

$\le wt(x+y) + wt(y+z)$ (by lemma)

$= d(x,y) + d(y,z)$

Hamming metric

When a function satisfies the four properties:

(a) $d(x,y) \geq 0$,

(b) $d(x,y) = 0$ iff $x = y$,

(c) $d(x,y) = d(y,x)$,

(d) $d(x,z) \leq d(x,y) + d(y,z)$, then it is called a distance function or metric, and we call (Z_2^n, d) a metric space. Hence d (as given above) is often referred to as the Hamming metric.

Sphere of radius k

For $n, k \in Z^+$ and $x \in Z_2^n$, the sphere of radius k centered at x is defined as $S(x,k) = \{y \in Z_2^n \mid d(x,y) \leq k\}$.

example

* For $n=3$ and $x = 110 \in Z_2^3$, find $S(x,1)$ and $S(x,2)$.

sol^n $S(x,1) = \{y \in Z_2^3 \mid d(x,y) \leq 1\} = \{110, 010, 100, 111\}$

$S(x,2) = \{y \in Z_2^3 \mid d(x,y) \leq 2\} = \{110, 010, 100, 111, 000, 101, 011\}$.

Theorem 1

Let $E: W \to C$ be an encoding function with the set of messages $W \subseteq Z_2^m$ and the set of code words $E(W) = C \subseteq Z_2^n$ where $m < n$. For $k \in Z^+$, we can detect transmission errors of weight $\leq k$ if and only if the minimum distance between code words is at least $k+1$.

Theorem 2

Let $E: W \to C$ be an encoding function with the set of messages $W \subseteq Z_2^m$ and the set of code words $E(W) = C \subseteq Z_2^n$ where $m < n$, and $k \in Z^+$, then we can construct a decoding function $D: Z_2^n \to W$ that corrects all transmission errors of weight $\leq k$ if and only if the minimum distance between code words is at least $2k+1$.

3, 3, 6, 6, 3, 3

example

* With $W = Z_2^2$, let $E: W \to Z_2^6$ be given by

$E(00) = 000000$, $E(10) = 101010$, $E(01) = 010101$, $E(11) = 111111$

r_1 r_2 r_3 r_4

$d(r_1, r_2) = 3$, $d(r_1, r_3) = 3$, $d(r_1, r_4) = 6$, $d(r_2, r_3) = 6$, $d(r_2, r_4) = 3$, $d(r_3, r_4) = 3$

The minimum distance between the code words is 3.

by Theorem 1, $k+1 = 3 \Rightarrow k = 2$, by Theorem 2, $2k+1 = 3 \Rightarrow k = 1$.

So, we can detect double errors and correct single errors.

With $S(000000, 1) = \{x \in Z_2^6 \mid d(000000, x) \leq 1\}$

$= \{000000, 100000, 010000, 001000, 000100, 000010, 000001\}$,

the decoding function $D: Z_2^6 \to W$ gives $D(x) = 00$, $\forall x \in S(000000, 1)$

[By majority rule at (1st, 3rd, 5th) positions and (2nd, 4th, 6th) positions]

With $S(010101, 1) = \{x \in Z_2^6 \mid d(010101, x) \leq 1\}$

$= \{010101, 110101, 000101, 011101, 010001, 010111, 010100\}$,

and here $D(x) = 01$ $\forall x \in S(010101, 1)$. [by majority rule]

We observe that the definition of D accounts for

$7 + 7 = 14$ [7 from $S(000000, 1)$ & 7 from $S(010101, 1)$]

of the elements of Z_2^6. Similarly $S(101010)$ & $S(111111)$ contribute 14 more elements of Z_2^6 to the definition of D.

Since $|Z_2^6| = 64$, there remains 36 (64 − 28) other elements to account for.

We define $D(x) = 00$ for any other message for these 36 other elements and have a decoding function that will correct single errors.

With regard to detection, if $c = 010101$ and $T(c) = r = 111101$, we can detect this double error because r is not a code word.

But if $T(c) = r_1 = 111111$, a triple error has occured, so we think that $c = 111111$ and incorrectly decode r_1 as 11, instead of as the correct message 01.

* With $W = Z_2^2$, let $E: W \to Z_2^6$ be given by
$E(00) = 000000$, $E(10) = 101010$, $E(01) = 010101$, $E(11) = 111111$
List the elements in $S(101010, 1)$ and $S(111111, 1)$.

Sol^n $S(101010, 1) = \{x \in Z_2^6 \mid d(101010, x) < 1\}$
$= \{101010, 001010, 111010, 100010, 101110, 101000, 101011\}$

$S(111111, 1) = \{x \in Z_2^6 \mid d(111111, x) \leq 1\}$
$= \{111111, 011111, 101111, 110111, 111011, 111101, 111110\}$

* With $W = Z_2^2$, let $E: W \to Z_2^6$ be given by
$E(00) = 000000$, $E(10) = 101010$, $E(01) = 010101$, $E(11) = 111111$
Decode each of the following received word
(a) 110101, (b) 101011, (c) 001111 (d) 110000.

Sol^n (a) 110101 majority at 1st, 3rd & 5th position is 0
majority at 2nd, 4th & 6th position is 1
∴ the decoded word is 01.

(b) 101011 majority at 1st, 3rd & 5th position is 1
majority at 2nd, 4th & 6th position is 0
∴ the decoded word is 10

(c) 001111 majority at 1st, 3rd & 5th position is 1
majority at 2nd, 4th & 6th position is 1
∴ the decoded word is 11.

(d) 110000 majority at 1st, 3rd & 5th position is 0
majority at 2nd, 4th & 6th position is 0
∴ the decoded word is 00

* (a) If $x \in Z_2^{10}$, determine $|S(x,1)|$, $|S(x,2)|$, $|S(x,3)|$.

(b) For $n,k \in Z^+$, with $1 \le k \le n$, if $x \in Z_2^n$, what is $|S(x,k)|$?

Soln $S(x,1) = \{ y \in Z_2^{10} \mid d(x,y) \le 1 \}$

$= \{ y \in Z_2^{10} \mid d(x,y) = 0 \text{ or } d(x,y) = 1 \}$

for $d(x,y)=0$, y should be same as x, there is only one such possibility

for $d(x,y)=1$, y should differ from x, at only one position, and there are ${}^{10}C_1 = 10$ such possibilities.

$\therefore |S(x,1)| = 1 + 10 = 11$

$S(x,2) = \{ y \in Z_2^{10} \mid d(x,y) \le 2 \} = \{ y \in Z_2^{10} \mid d(x,y)=0 \text{ or } d(x,y)=1 \text{ or } d(x,y)=2 \}$

for $d(x,y)=0$, there is only one possibility.

for $d(x,y)=1$, there are 10 possibilities.

for $d(x,y)=2$, y should differ from x, at only two positions, and there are ${}^{10}C_2 = 45$ possibilities

$\therefore |S(x,2)| = 1 + 10 + 45 = 56$

Similarly $|S(x,3)| = 1 + {}^{10}C_1 + {}^{10}C_2 + {}^{10}C_3 = 176$

(b) with $1 \le k \le n$, for $x \in Z_2^n$,

$$|S(x,k)| = 1 + {}^nC_1 + {}^nC_2 + \dots + {}^nC_k = \sum_{i=0}^{k} {}^nC_k$$

* Let $E : Z_2^5 \to Z_2^{25}$ be an encoding function where the minimum distance between code words is 9. What is the largest value of k such that we can detect errors of weight $\le k$? If we wish to correct errors of weight $\le n$, what is the maximum value of n?

Soln We can use Theorem 1 to find k. $\therefore k+1 = 9 \Rightarrow k = 8$

We can use Theorem 2 to find n. $\therefore 2n+1 = 9 \Rightarrow n = 4$

* For each of the following encoding functions, find the minimum distance between the code words. Discuss the error-detecting and error-correcting capabilities of each code.

(a) : $E: Z_2^2 \to Z_2^5$

$00 \to 00001, 01 \to 01010, 10 \to 10100, 11 \to 11111$

(b) $E: Z_2^2 \to Z_2^{10}$

$00 \to 0000000000$ $01 \to 0000011111$

$10 \to 1111100000$ $11 \to 1111111111$

(c) $E: Z_2^3 \to Z_2^6$

$000 \to 000111$ $001 \to 001001$ $010 \to 010010$ $011 \to 011100$

$100 \to 100100$ $101 \to 101010$ $110 \to 110001$ $111 \to 111000$

(d) $E: Z_2^3 \to Z_2^8$

$000 \to 00011111$ $001 \to 00111010$

$010 \to 01010101$ $011 \to 01110000$

$100 \to 10001101$ $101 \to 10101000$

$110 \to 11000100$ $111 \to 11100011$

Sol^n

(a) $d(00001, 01010) = 3$, $d(00001, 10100) = 3$, $d(00001, 11111) = 4$

$d(01010, 10100) = 4$, $d(01010, 11111) = 3$, $d(10100, 11111) = 3$

$\therefore$ minimum distance between code words is 3.

Applying Theorem 1 $k+1 = 3 \Rightarrow k = 2$

$\therefore$ the code can detect all error of weigth ≤ 2.

Apply Theorem 2 $2k+1 = 3 \Rightarrow k = 1$

$\therefore$ the code can correct all errors of weight ≤ 1

(b) let the code words be denoted as follows:
$0000000000 = r_1$, $0000011111 = r_2$, $1111100000 = r_3$, $1111111111 = r_4$

$d(r_1, r_2) = 5$, $d(r_1, r_3) = 5$, $d(r_1, r_4) = 10$, $d(r_2, r_3) = 10$, $d(r_2, r_4) = 5$, $d(r_3, r_4) = 5$

∴ minimum distance between code words is 5.

Applying Theorem 1 $k+1 = 5 \Rightarrow k = 4$

∴ the code can detect all error of weight ≤ 4.

Apply Theorem 2 $2k+1 = 5 \Rightarrow k = 2$

∴ the code can correct all errors of weight ≤ 2

(c) Let the code words be denoted as follows:

$000111 = r_1$, $001001 = r_2$, $010010 = r_3$, $011100 = r_4$

$100100 = r_5$, $101010 = r_6$, $110001 = r_7$, $111000 = r_8$

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8
r_1	×	3	3	4	3	4	4	6
r_2	3	×	4	3	4	3	3	3
r_3	3	4	×	3	4	3	3	3
r_4	4	3	3	×	3	4	4	2
r_5	3	4	4	3	×	3	3	3
r_6	4	3	3	4	3	×	4	2
r_7	4	3	3	4	3	4	×	2
r_8	6	3	3	2	3	2	2	×

∴ minimum distance between code words is 2.

Applying Theorem 1 $k+1 = 2 \Rightarrow k = 1$

the code can detect all error of weight ≤ 1

Apply Theorem 2 $2k+1 = 2 \Rightarrow k = \frac{1}{2}$

the code can correct all errors of weight $\leq \frac{1}{2}$

i.e. the code cannot correct any error.

In this section the encoding and decoding functions are given by matrices over Z_2. One of these matrices will help us to locate the nearest code word for a given received word. This will be especially helpful as the set C of code words grows larger.

Let $G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ be a 3×6 matrix over Z_2.

The first 3 columns of G_1 form the 3×3 identity matrix I_3. Letting A denote the matrix formed from the last three columns of G_1, we write $G_1 = [I_3 | A]$ to denote its structure. The (partitioned) matrix G_1 is called a <u>generator matrix</u>

G_1 is used to define an encoding function $E: Z_2^3 \to Z_2^6$ as follows:

For $w \in Z_2^3$, $E(w) = wG_1$ is the element in Z_2^6 obtained by multiplying w, considered as a three-dimensional row vector, by the matrix G_1 on its right.

[in the calculations here we have $1+1=0$]

[Even if the set W of messages is not all of Z_2^3, we will assume that all of Z_2^3 is encoded and that the transmitter and receiver will both know the real messages of importance and their corresponding code words]

ex $E[110] = (1\,1\,0)G_1 = [1\,1\,0]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [1\,1\,0\,1\,0\,1]$,

& $E[010] = (0\,1\,0)G_1 = [0\,1\,0]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [0\,1\,0\,0\,1\,1]$

Note that $E[110]$ is obtained by adding first two rows of G_1, whereas $E[010]$ is simply the second row of G_1.

So for $W = \{000, 100, 010, 001, 110, 101, 011, 111\}$ the code words are $C = \{000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000\} \subseteq Z_2^6$

and one can recapture the corresponding message by simply dropping the last three components of the code word. In addition the minimum distance between code words is 3, so we can detect errors of weight ≤ 2 and correct single errors

For any $w = w_1 w_2 w_3 \in Z_2^3$, $E(w) = w_1 w_2 w_3 w_4 w_5 w_6 \in Z_2^6$.

Since $E(w) = [w_1 w_2 w_3] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [w_1 w_2 w_3 (w_1+w_3)(w_1+w_2)(w_2+w_3)]$

$\Rightarrow w_4 = w_1 + w_3$, $w_5 = w_1 + w_2$, $w_6 = w_2 + w_3$ and these equations are called the parity-check equations.

Since $w_i \in Z_2$, for each $1 \leq i \leq 6$, $w_i = -w_i$.

So the above equations can be written as

$$\left.\begin{aligned} w_1 + w_3 - w_4 &= 0 \\ w_1 + w_2 - w_5 &= 0 \\ w_2 + w_3 - w_6 &= 0 \end{aligned}\right\} \text{ OR } \begin{aligned} w_1 + 0 + w_3 + w_4 + 0 + 0 &= 0 \\ w_1 + w_2 + 0 + 0 + w_5 + 0 &= 0 \\ 0 + w_2 + w_3 + 0 + 0 + w_6 &= 0 \end{aligned}$$

Hence $$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

or $H.(E(w))^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, where $(E(w))^{tr}$ denotes the transpose of $E(w)$.

Consequently, if $r = r_1 r_2 \dots r_6 \in Z_2^6$, we can identify r as a code word if and only if $H.r^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Writing $H = [B | I_3]$, we notice that if the rows and columns of B are interchanged, then we get A. Hence $B = A^{tr}$

Since the minimum distance between the code words of this example is 3, we should be able to develop a decoding function that corrects single errors.

Suppose we receive $r = 110110$

we want to find the code word c that is the nearest neighbour of r.

If there is a long list of code words against which to check r, we would be better off to first examine Hr^{tr}, which is called the syndrome of r.

Here $$Hr^{tr} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

(is the second column of H)

$\therefore r$ is not a code word.

We want to atleast detect an error

we know the code words are:

$C = \{000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000\}$

$c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5 \quad c_6 \quad c_7 \quad c_8$

The received word is $r = 110110$

$d(c_1, r) = 4, d(c_2, r) = 1, d(c_3, r) = 3, d(c_4, r) = 5, d(c_5, r) = 2, d(c_6, r) = 4,$
$d(c_7, r) = 2, d(c_8, r) = 3$

$\therefore d(100110, r) = 1$ is the minimum.

writing $r = c + e = 100110 + 010000$, we find that the transmission error occurs in the second component of r.

Changing the second component of r, we get c;

the message w comprises of first three components of c.

Let $r = c + e$, where c is a code word and e is an error pattern of weight 1.
Suppose that 1 is in the i^{th} component of e, where $1 \le i \le 6$
Then $H \cdot r^{tr} = H \cdot (c+e)^{tr} = H \cdot (c^{tr} + e^{tr}) = H \cdot c^{tr} + H \cdot e^{tr}$
With c a code word, it follows that $H \cdot c^{tr} = 0$,
so $H \cdot r^{tr} = H \cdot e^{tr} = i^{th}$ column of matrix H.
Thus c and r differ only in the i^{th} component, and we can determine c by simply changing the i^{th} component of r.

Correct multiple errors

Suppose we receive $r = 000111$.
Then $H \cdot r^{tr} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, which is not a column of H.

Yet $H \cdot r^{tr}$ can be obtained as the sum of two columns of H
If $H \cdot r^{tr}$ came from the first and sixth columns of H, correcting these components in r results in the code word 100110
If we sum the third and fifth columns of H to get this syndrome, upon changing the third and fifth component of r we get a second code word, 001101.
So we cannot expect H to correct multiple errors.
[This is no surprise, since the minimum distance between code words is 3 $\Rightarrow 2k+1 = 3 \Rightarrow k = 1$ i.e. the code can correct errors of at most 1]

Parity-check matrix and Generator matrix

For $m, n \in \mathbb{Z}^+$ with $m < n$, the encoding function $E: Z_2^m \to Z_2^n$ is given by an $m \times n$ matrix G over Z_2. The matrix G is called the <u>generator matrix</u> for the code and has the form $[I_m | A]$, where A is an $m \times (n-m)$ matrix.

Here, $E(w) = wG$ for each message $w \in Z_2^m$, and the code $C = E(Z_2^m) \subset Z_2^n$.

The associated parity-check matrix H is an $(n-m) \times n$ matrix of the form $[A^{tr} | I_{n-m}]$.

This matrix can also be used to define the encoding function E, because if $w = w_1 w_2 \cdots w_m \in Z_2^m$, then $E(w) = w_1 w_2 \cdots w_m w_{m+1} \cdots w_n$, where $w_{m+1} \cdots w_n$ can be determined from the set of $n-m$ (parity-check) equations that arise from $H \cdot (E(w))^{tr} = 0$, the column vector of $n-m$ 0s.

This unique parity-check matrix H also provides a decoding scheme that corrects single errors in transmission if:

(a) H does not contain a column of 0s.

[If the i^{th} column of H had all 0s and $H \cdot r^{tr} = 0$ for a received word r, we couldn't decide whether r was a code word or a received word whose i^{th} component was incorrectly transmitted. We do not want to compare r with all code words when C is large.]

(b) No two columns of H are the same.

[If the i^{th} and j^{th} columns of H are the same and $H \cdot r^{tr}$ equals this repeated column, then how would we decide which component of r to change?]

When H satisfies the above two conditions, we get the following decoding algorithm.

For any $r \in Z_2^n$, if $T(c) = r$, then:

1. With $H \cdot r^{tr} = 0$, we feel that the transmission was correct and that r is the code word that was transmitted. The decoded message then consists of the first m components of r.
2. With $H \cdot r^{tr}$ equal to the i^{th} column of H, we feel that there has been a single error in transmission and change the i^{th} component of r in order to get the code word c. Here the first m components of c yield the original message.
3. If neither case 1 nor case 2 occurs, we feel that there has been more than one transmission error and we cannot provide a reliable way to decode in this situation.

Note: If we start with a parity-check matrix $H = [B | I_{n-m}]$ and use it, as described above, to define the function $\hat{E}$, then we obtain the same set of code words that is generated by the unique associated generator matrix $G = [I_m | B^{tr}]$.

examples

For $E: Z_2^3 \to Z_2^6$

(a) Use the parity-check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

to decode the following received words.

(i) 111101 (R_1), (ii) 110101 (R_2), (iii) 001111 (R_3), (iv) 100100 (R_4)

(v) 110001 (R_5), (vi) 111111 (R_6), (vii) 111100 (R_7) (viii) 010100. (R_8)

(b) Are all the results in part (a) uniquely determined?

Sol^n Consider $H \cdot R_1^{tr}$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \therefore H \cdot R_1^{tr} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

Similarly we can obtain all other decoded words.

(a) The decoded words are

(i) 101, (ii) 000, (iii) 010, (iv) 010, (v) 100, (vi) 111 (vii) 100 (viii) 111

(i) 3rd column single error; (ii) no error; (iii) 5th column single error; (iv) 5th column single error; (v) 4th column single error; (vi) sum of 1st & 6th 2 errors; (vii) 4th column single error; (viii) sum of 1st & 6th 2 errors

	received word	correction at position	decoded word		considering 1st 3 bits decoded word
(i)	111101	3rd	110101		110
(ii)	110101	nil	110101		110
(iii)	001111	5th	001101		001
(iv)	100100	5th	100110		100
(v)	110001	4th	110101		110
(vi)	111111	1st & 6th	011110	(there are other possibilities)	011
(vii)	111100	4th	111000		111
(viii)	010100	1st & 6th	110101	(there are other possibilities)	110

(b) No, not all results are uniquely determined

(vi) & (viii) received words have other possibilities.

* The encoding function $E: Z_2^2 \to Z_2^5$ is given by the generator matrix $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.

(a) Determine all code words. What can we say about the error-detection capability of this code? What about its error-correction capability?

(b) Find the associated parity-check matrix H.

(c) Use H to decode each of the following received words. (i) 11011, (ii) 10101, (iii) 11010 (iv) 00111 (v) 11101 (vi) 00110.

Soln. $W = \{00, 10, 01, 11\}$

$\left[\because C = wG = [0\ 0] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 00000\right]$

$\therefore C = \{\underset{c_1}{00000}, \underset{c_2}{10110}, \underset{c_3}{01011}, \underset{c_4}{11101}\}$

$d(c_1, c_2) = 3,\ d(c_1, c_3) = 3,\ d(c_1, c_4) = 4,\ d(c_2, c_3) = 4,\ d(c_2, c_4) = 3,\ d(c_3, c_4) = 3$

The minimum distance between code words is 3.

The code can detect all errors of weight ≤ 2 $[\because k+1 = 3 \Rightarrow k = 2]$ and correct all single $(\because 2k+1 = 3 \Rightarrow k = 1)$ errors.

(b) Here $E: Z_2^2 \to Z_2^5$ $\therefore m = 2,\ n = 5$ $G = [I_2 \mid A]$

where $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$\therefore H = [A^{tr} \mid I_3] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

(c) Given (i) 11011, (ii) 10101, (iii) 11010, (iv) 00111, (v) 11101, (vi) 00110

using $H.R^{tr}$ - decoded words are 110, 011, 111, 111, 000, 110

errors happening at 1st, 2nd, (1st & 5th), (1st & 5th), nil, 1st positions

decoded words after correction are

01011, 11101, 01011, 10110, 11101, 10110

Considering the first 2 bits, the decoded words are

01, 11, 01, 10, 11, 10

* Define the encoding function $E: Z_2^3 \to Z_2^6$ by means of the parity-check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

(a) Determine all code words.

(b) Does this code correct all single errors in transmission?

Soln Given $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

if $x = x_1x_2x_3x_4x_5x_6 \in Z_2^6$, x is identified as a code word iff

$$H \cdot x^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \text{ i.e., } \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow x_1 + 0 + x_3 + x_4 + 0 + 0 = 0 \Rightarrow x_4 = x_1 + x_3$

$x_1 + x_2 + 0 + 0 + x_5 + 0 = 0 \Rightarrow x_5 = x_1 + x_2$

$x_1 + 0 + x_3 + 0 + 0 + x_6 = 0 \Rightarrow x_6 = x_1 + x_3$

with $x_1\ x_2\ x_3$ as	$x_4\ x_5\ x_6$ is	the code word is	
0 0 0	0 0 0	0 0 0 0 0 0	C_1
1 0 0	1 1 1	1 0 0 1 1 1	C_2
0 1 0	0 1 0	0 1 0 0 1 0	C_3
0 0 1	1 0 1	0 0 1 1 0 1	C_4
1 1 0	1 0 1	1 1 0 1 0 1	C_5
1 0 1	0 1 0	1 0 1 0 1 0	C_6
0 1 1	1 1 1	0 1 1 1 1 1	C_7
1 1 1	0 0 0	1 1 1 0 0 0	C_8

d	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
C_1	–	4	2	3	4	3	5	3
C_2	4	–	4	3	2	3	3	5
C_3	2	4	–	5	4	3	3	3
C_4	3	3	5	–	3	4	2	4
C_5	4	2	4	3	–	5	3	3
C_6	3	3	3	4	5	–	4	2
C_7	5	3	3	2	3	4	–	4
C_8	3	5	3	4	3	2	4	–

Since the minimum distance between code words is 2

$\Rightarrow 2k+1 = 2 \Rightarrow k = \frac{1}{2}$, i.e., this code cannot correct single errors in transmission.