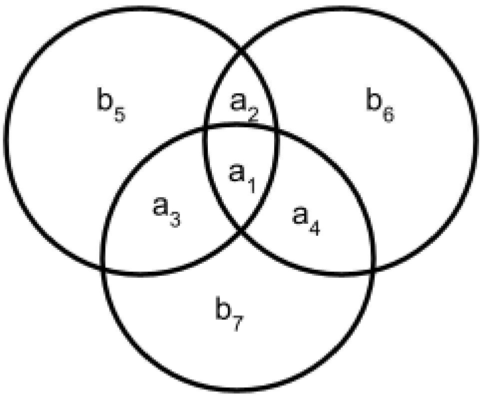
Assignment 2: ECC

[112006234] [Justin Thiadi 程煒財]

Question 2(a):

For $x \in F^4$, show that $y = Ax$ is the same as the encoded result using the set method.

Set Method



We know that:

- a_1, a_2, a_3, a_4 is the original message
- b_5, b_6, b_7 is the area to fill in bits to indicate that each circle has even no. of 1s

The idea is that we have a 4-bits original message (a_1, a_2, a_3, a_4), and we want to encode them into a seven-bit string by appending them with 3 extra parity bits (b_5, b_6, b_7). Thus it'll become $a_1a_2a_3a_4b_5b_6b_7$

Notice that:

When even the following will be 0	**When odd** the following will be 1
$b_5 + a_1 + a_2 + a_3$	$b_5 + a_1 + a_2 + a_3$

Matrix Multiplication

When
$y = Ax$, where $x \in F^4$

$$y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

$$y = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_1 + a_2 + a_3 \\ a_1 + a_2 + a_4 \\ a_1 + a_3 + a_4 \end{bmatrix}$$

Since we are considering binary addition, then the 5th to 7th row of the matrix will each be

- 0 when there are even no. of 1s

$b_6 + a_1 + a_2 + a_4$	$b_6 + a_1 + a_2 + a_4$
$b_7 + a_1 + a_3 + a_4$	$b_7 + a_1 + a_3 + a_4$

Therefore,

value of b5:

when area is even	when area is odd
0 when $a_1 + a_2 + a_3 =$ even no. of 1s	0 when $a_1 + a_2 + a_3 =$ odd no. of 1s
1 when $a_1 + a_2 + a_3 =$ odd no. of 1s	1 when $a_1 + a_2 + a_3 =$ even no. of 1s

Thus,
b_5 can be written as a linear combination of a_1, a_2, and a_3 which satisfy $\mathbf{b_5 = (a_1 + a_2 + a_3) \bmod 2}$

Following the logic from above,
b_6 can be written as a linear combination of a_1, a_2, and a_4 which satisfy
$\mathbf{b_6 = (a_1 + a_2 + a_4) \bmod 2}$

b_7 can be written as a linear combination of a_1, a_3, and a_4 which satisfy
$\mathbf{b_7 = (a_1 + a_3 + a_4) \bmod 2}$

- 1 when there are odd no. of 1s

Let the 5th to 7th row be b_5, b_6, b_7 respectively, it can thus be written as

$\mathbf{b_5 = (a_1 + a_2 + a_3) \bmod 2}$
$\mathbf{b_6 = (a_1 + a_2 + a_4) \bmod 2}$
$\mathbf{b_7 = (a_1 + a_3 + a_4) \bmod 2}$

Therefore, by comparing both result, it can be seen that the result $y = Ax$ is the same as the encoded result using the set method

Question 3(a):

(20%) Suppose the null space of A^T is span$(h_1, h_2, \ldots, h_k)$ and let matrix

$$H = \begin{bmatrix} h_1^T \\ h_2^T \\ \vdots \\ h_k^T \end{bmatrix}.$$

Show that the encoded message y does not have any single bit error if and only if $Hy = 0$. A single bit error of y is $y + e_i$, where e_i is the i-th column vector of an identity matrix I.

Given that:

- Null space of A^T is spanned by $\{h_1, h_2, ..., h_k\}$ where $\{h_1, h_2, ..., h_k\}$ are column vectors
- Matrix $H = \begin{bmatrix} h_1^T \\ h_2^T \\ \vdots \\ h_k^T \end{bmatrix}$ where **each of the rows** of matrix H is in the null space of A^T. Since A^T is spanned by $\{h_1, h_2, ..., h_k\}$, so h_k^T is basically h_k in the form of row vectors

★ Prove if there's no single bit error in y, then $Hy = 0$

(1) Suppose no error in encoded message y, therefore it'll satisfy $y = Ax$ and lies within the subspace that satisfies the null space condition below

(2) We know that each rows of the matrix H spans the null space of A^T, therefore **each rows** of matrix H have to satisfy $A^T h_k^T = 0$, or in other words, $A^T H^T = 0$ as the rows are stacked to form matrix H

(3) Transpose $A^T H^T = 0$ and we get $(A^T H^T)^T = (0)^T$, which results in $HA = 0$

(4) Therefore from (1), it follows that $H(Ax) = 0$, and from (3), we know that $HA = 0$, thus $HAHx = 0$, then $0Hx = 0$, proving that $H(Ax) = 0$.

(5) Notice that also from (1), if y has no single bit error, then it will satisfy $y = Ax$, so if there's no single bit error in y, then $Hy = 0$

★ Prove if $Hy = 0$, then there's no single bit error in y

(1) Prove by contradiction. For the sake of contradiction, assume that $Hy = 0$ is true if there's no single bit error in y

(2) Suppose that y has a single bit error, it's given that $y = y' + e_i$ where y' is the original y with no single bit error and e_i is the i^{th} column vector of an identity matrix I

(3) From (2), it will follow that $Hy = H(y' + e_i)$
$= Hy' + He_i$

(4) Since y' is from the original y, then from our assumption in (1), it will follow that
$Hy = 0 + He_i$
$= He_i$

(5) $He_i \neq 0$, and for y to have no single bit error, $Hy = 0$ based on our assumption in (1). Since it contradicts our initial assumption, then if $Hy = 0$, then there's no single bit error in y

Since we have proven prove both directions of if and only if ($P \Rightarrow Q$ and $Q \Rightarrow P$), therefore it is proven that y doesn't have any single bit error iff $Hy = 0$

Question 3(b):

(20%) Show that with single bit error, if $Hy = v \neq 0$, v must be a column vector of H. Suppose v is the i-th column vector of H, the i-th element of y has an error.

(1) Consider matrix H is written in terms of its columns, where $H = [h_1, h_2, ..., h_j, ..., h_n]$ where h_i is the i^{th} column vector of matrix H and each column vector of H is unique and non-zero that corresponds to a specific position i in the 7-bit encoded message y

(2) Let y be the received message with a single-bit error, which can be represented as $y = y' + e_i$ where y' is the original y with no single bit error and e_i is the i^{th} column vector of an identity matrix I.

(3) If there's a single bit error, $Hy = H(y' + e_i)$.
Since y' is from the original y, then from our proof from 3(a),
it will follow that $Hy = He_i$ and $He_i \neq 0$

(4) Without loss of generality, let's consider the j^{th} element of y has an error

(a) Matrix H is multiplied by e_j and e_j is zero everywhere except for the j^{th} position, then

$$He_j = [h_1, h_2, ..., h_j, ..., h_n] \begin{bmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 1 \\ 0 \\ . \\ . \\ 0 \end{bmatrix} \begin{array}{l} \\ \\ \\ \\ \\ \rightarrow j^{th} position \\ \\ \\ \\ \\ \end{array}$$

This will then result in the j^{th} column vector of matrix H, which will be denoted as v, therefore v must be a column vector of matrix H, due to the nature of the elementary matrix

(b) From (2), we know that with a single-bit error, $y = y' + e_j$. This means that the error position in y is determined by e_j. Then from (3), we know that $Hy = He_j$ and $He_j \neq 0$ where He_j is the j^{th} column vector of matrix H based on (4(a)).

(c) Thus, since $Hy = He_j = v$,
v is the j^{th} column vector of matrix H and the j^{th} position of y has an error

(5) Therefore, we can conclude that If $Hy = v \neq 0$, then v must be one of the columns of H, where there is a single-bit error at the position corresponding to that column.

Question 4(b):

(b) In this case, you will find out that all column vectors of H are different. What are the necessary conditions that make all column vectors of H different.

- Each column vector has to be unique as it represents the error pattern for a single-bit error in a specific position
- Each column vector in matrix H must be non-zero.
- It must be an $m \times n$ matrix where each of the column vectors is in the binary field.
  - where $n \leq 2^{m} - 1$ since we want the column vectors to be unique and the number of possible unique binary vectors of length m is 2^m (as there are m positions in the vector and each position can be either 0 or 1) and it has to be non-zero.