Report for 2

Sunday, October 27, 2024 5:23 PM

② For $x \in F^4$, Show that $y = Ax$ is the same as the encoded result using the set method

① The finite field F_4 has exactly 4 elements, which is labelled as

$\{0, 1, \alpha, \alpha+1\}$

- 0 and 1 behave as Standard elements (0 and 1)
- α is a primitive element in F_4 satisfying $\alpha^2 = \alpha + 1$
- Addition in F_4 works similarly to XOR in binary operations
- Multiplication follows field rules, notably $\alpha^2 = \alpha + 1$

Hamming Code (7,4) Basics

↳ The hamming (7,4) is designed to encode a 4-bit message into a 7-bit codeword by adding 3 parity bits. In the matrix form, this encoding can be represented by a 7×4 generator matrix A that multiplies the 4-bit message vector x to produce a 7-bit encoded vector y.

Vector A:

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

*) The first 4 rows are an identity matrix that directly maps the original message bits

*) The last 3 rows represent parity checks, ensuring even parity in the respective overlapping regions (sets) described in the Venn diagram.

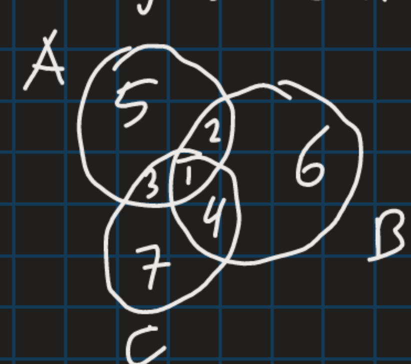
Given a 4-bit message $x = (x_1\ x_2\ x_3\ x_4)^T$, the encoded result y is obtained by:

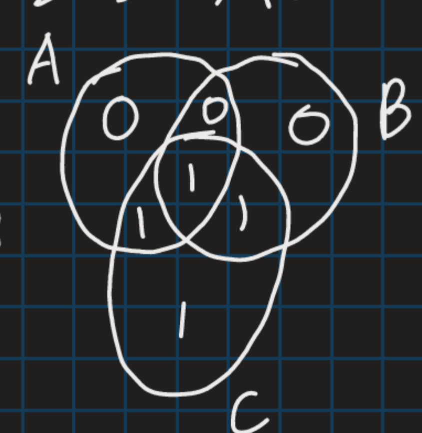
$$y = A \cdot x$$

where y is a 7-bit vector representing the encoded message in terms of both the original bits and the calculated parity bits.

Set method application

⊛ The original 4-bit message $x = (x_1, x_2, x_3, x_4)^T$ placed in corresponding areas





The parity bits b_5, b_6, b_7 are computed to ensure even parity within each circle

- A covers 1,2,3
- B covers 2,1,4
- C covers 3,1,4

To get the parity bits, we can use this method:

$$b_5 = x_1 + x_2 + x_3$$
$$b_6 = x_2 + x_1 + x_4$$
$$b_7 = x_3 + x_1 + x_4$$

where after the adding the values the result is being modulo by 2

From the matrix A, observe that:

- Rows 1 to 4 map directly to the original message bits x_1, x_2, x_3, x_4
- Rows 5,6,7 are represented:
  - *) Row 5: $x_1 + x_2 + x_3$
  - *) Row 6: $x_2 + x_1 + x_4$
  - *) Row 7: $x_3 + x_1 + x_4$

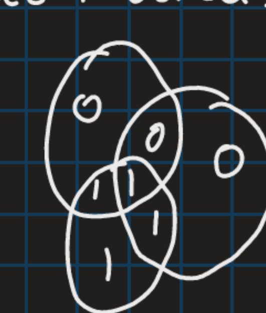
There fore the matrix product $y = Ax$ yields:

$$y = \begin{pmatrix} x_1\\ x_2\\ x_3\\ x_4\\ x_1+x_2+x_3\\ x_2+x_1+x_4\\ x_3+x_1+x_4 \end{pmatrix}$$

This matches the encoding result from the set method

Example: 1011001

Set method:



Result → 1011001

$Y = Ax$

$$A = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&1&0\\ 1&1&0&1\\ 1&0&1&1 \end{pmatrix} \begin{pmatrix} 1\\0\\1\\1 \end{pmatrix} = \begin{pmatrix} 1\\0\\1\\1\\0\\0\\0 \end{pmatrix} = (1011011)^T$$

$7\times4 \quad 4\times1$

Report for 3A

Sunday, October 27, 2024 8:10 PM

(3) a) 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 ith column Vector of an identity Matrix I.

To get Matrix H, we can transpose matrix A and then multiply it with $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$

$x_i = h_i$ (I just changed the Variable)

$$H = A^T x_i$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \xrightarrow{A^T} A^T = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}}_{4\times 7} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}}_{7\times 1} = \begin{bmatrix} x_1+x_5+x_6+x_7 \\ x_2+x_5+x_6 \\ x_3+x_5+x_7 \\ x_4+x_6+x_7 \end{bmatrix} \Rightarrow$$ Expressed as a linear combination

Can be rewriten as

$$x_1 = -x_5-x_6-x_7$$
$$x_2 = -x_5-x_6$$
$$x_3 = -x_5-x_7$$
$$x_4 = -x_6-x_7$$

The 7×1 can be rewritten as:

$$\begin{pmatrix} -x_5-x_6-x_7 \\ -x_5-x_6 \\ -x_5-x_7 \\ -x_6-x_7 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = x_5\begin{pmatrix} -1 \\ -1 \\ -1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_6\begin{pmatrix} -1 \\ -1 \\ 0 \\ -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + x_7\begin{pmatrix} -1 \\ 0 \\ -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$\Downarrow$ it is the transpose of Vector (x_i)

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

Given info:

- Matrix A: The generator matrix for a code. It maps a message Vector x to a codeword $y = Ax$
- Null Space of A^T: The null space of the Transpose of A, A^T is spanned by vectors $h_1, h_2, \ldots h_k$ where each $h_i \in \mathbb{R}^n$. This means that for each h_i we have:

$$A^T h_i = 0$$

- Parity check matrix H: Define a matrix H as follows:

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

Where each row of H is the transpose of a vector h_i in the null space of A^T. Consequently, the matrix H satisfies:

$$HA = 0$$

The matrix H is known as a Parity-check matrix for the code defined by A

- The encoded message: For a message Vector x, the encoded message (codeword) is $y = Ax$, which is in the column space of A
- The single-bit error in y is represented by $y + e_i$, where e_i is the i-th column of the identity matrix I. This means e_i is a vector with a 1 in the ith position and 0s elsewhere

(1) Show that if $y = Ax$ (no error), then $Hy = 0$

Assume y is an error-free encoded message, which means it was generated as $y = Ax$ for some message vector x

Substitute $y = Ax$ into Hy

$$Hy = H(Ax) = (HA)x$$

By definition of H, we know that $HA = 0$ (since each row of H is in the null space of A^T, meaning $HA = 0$)

$$Hy = 0 \cdot x = \underline{\underline{0}}$$

This implies that if $y = Ax$, then $Hy = 0$. This shows that any valid (error-free) codeword y satisfies $Hy = 0$

Ex:

To mantain values within binary constraints (0 or 1)

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 4 \end{bmatrix} \% 2 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

(2) Show that if there is a single-bit error, then $Hy' \neq 0$

(*) Suppose there is single-bit error in the encoded message y. This message is represented as:

$$y' = y + e_i$$

where e_i is the ith standard basis vector (or column of the identity matrix I). The vector e_i has a 1 in the i-th position and 0's elsewhere.

(*) Compute Hy' by substituting $y' = y + e_i$

$$Hy' = H(y+e_i) = \underbrace{Hy}_{\text{By (1) we know the value is 0}} + He_i \Rightarrow Hy + He_i = Hy'$$
$$Hy' = 0 + He_i = He_i$$

(*) Analyze He_i:

- e_i is not in the column space of A because it represents a single bit error that disrupts the structure of the codeword
- Since e_i is not a linear combination of the columns of A, it follows that $He_i \neq 0$. This is because H is specifically constructed to detect any deviation from the column space of A.

Therefore, $Hy' = He_i \neq 0$

Report for 3B

Monday, October 28, 2024 12:54 AM

③ b) 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 ith element of y has an error.

- Encoding Matrix A: A generator matrix A for encoding messages
- Parity check matrix H: The matrix H is constructed such that it spans the null space of A^T meaning that $HA = 0$.

- Single-bit error representation: A single-bit error in Y is represented by $y' = y + e_i$ where e_i is the ith column of the identity matrix. This means only the ith bit of y is flipped.

Let y be an error-free codeword, so $Hy = 0$. Now consider a single bit error in the i-th position, so the codeword y' is

$$y' = y + e_i$$

Where e_i is the standard basis vector with a 1 in the i-th position and 0's elsewhere.

$$Hy' = H(y + e_i) = \underbrace{Hy}_{0} + He_i$$

So $Hy' = He_i$

The vector e_i is the ith column of the identity matrix, so when multiplied by H, He_i gives the ith column of H. So:

$$Hy' = He_i = h_i$$

Where h_i is the i-th column of H. Therefore, the result $v = Hy'$ is not only non-zero (Indicating an error), but it also corresponds specifically to a column of H. This column identifies the exact position of bit error in Y.

According to the set theory, each bit in y corresponds to a specific region in the Venn diagram with 3 overlapping circles. The parity bits are chosen to ensure that each of these circles have an even number of 1's.

① Single-bit error detection: When a single bit error occurs, it will disrupt the even parity in specific circles. For example: If the error is in a region covered by circles A and B but not C then both A and B will have an odd number of 1s, but C will remain even.

② Correspondence to columns of H: Each column of H corresponds to a unique pattern of circles where a single bit error would disturb the parity. For instance: the i-th column of H represents the unique signature (pattern of parity violations) associated with an error in the i-th position of y.

- If $v = h_i$, where h_i is the i-th column of H, the positions of 1s in h_i indicate which sets (or circles in the Venn diagram) have had their parity disrupted due to an error in position i of y.

∴) The error occured in the i-th position, because only the i-th column of H produced the observed pattern of parity violations.

Report for 4B

Monday, October 28, 2024 2:29 AM

4 b) The necessary condition is that the Parity-check Matrix must have sufficient rows to distinguish every possible error location. This requirement is essential for detecting and locating single-bit errors in any position of the encoded message vector y.

key conditions:

*) Unique error syndromes: Each column of H corresponds to a distinct syndrome, which is the result of multiplying H by a single bit error vector. If every column of H is distinct, then each possible error location will produce a unique syndrome. This allows us to uniquely identify where a single bit error has occured.

*) Number of columns in H: Suppose y is an n-bit encoded message, meaning $y \in F_2^n$. Then H must have n columns, with each column representing the error syndrome for a single-bit error in one of the n-positions

*) Number of rows in H: To ensure that each column of H is unique, H must have at least enough rows to provide a unique binary pattern for each of the n columns. This is equivalent to requiring H to have at least $\log_2(n)$ so that each column has a unique combination of 0s and 1s.

- In other words, if H has m rows, it can distinguish up to 2^m unique columns.
- To cover all n bit positions in y with unique syndromes, we require $2^m \geq n$ which implies $\underset{\text{number of rows}}{m} \geq \lceil \log_2(\underset{\text{number of columns}}{n}) \rceil$

Ex: Hamming Code (7,4)

$n=7$ (encoded message length $=7$ bits)
$m=3$ (parity check matrix H has 3 rows)

With 3 rows, H can have up to $2^3=8$ distinct columns. Since $n=7$, this is sufficient for each bit position to have a unique syndrome, which allows for detection and correction for any single bit error in the 7-bit encoded message.