MAT2040 Project 1

Bokai XU (119010355)

1. Binary Vector Space

Question 1

(1) Matrix Scalar multiplication

$$\alpha = 0, \alpha A = \begin{bmatrix} 0\cdot 1 & 0\cdot 0 & 0\cdot 1 \\ 0\cdot 1 & 0\cdot 1 & 0\cdot 0 \\ 0\cdot 1 & 0\cdot 0 & 0\cdot 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\alpha = 1, \alpha A = \begin{bmatrix} 1\cdot 1 & 1\cdot 0 & 1\cdot 1 \\ 1\cdot 1 & 1\cdot 1 & 1\cdot 0 \\ 1\cdot 1 & 1\cdot 0 & 1\cdot 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

(2) Matrix addition

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

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

$$B + B = \begin{bmatrix} 1+1 & 0+0 & 1+1 \\ 0+0 & 1+1 & 0+0 \\ 1+1 & 1+1 & 1+1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

(3) Matrix-vector multiplication

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

$$= 0 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0\cdot 1 + 1\cdot 0 + 1\cdot 1 \\ 0\cdot 0 + 1\cdot 1 + 1\cdot 0 \\ 0\cdot 1 + 1\cdot 1 + 1\cdot 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0+0+1 \\ 0+1+0 \\ 0+1+1 \end{bmatrix}$$

$$= \begin{bmatrix} 0+1 \\ 1+0 \\ 1+1 \end{bmatrix}$$

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

(4) Matrix-matrix multiplication

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

$$= \begin{bmatrix} 1[1 & 0 & 1] + 0[0 & 1 & 0] + 1[1 & 1 & 1] \\ 1[1 & 0 & 1] + 1[0 & 1 & 0] + 0[1 & 1 & 1] \\ 1[1 & 0 & 1] + 0[0 & 1 & 0] + 1[1 & 1 & 1] \end{bmatrix}$$

$$= \begin{bmatrix} 1\cdot 1 + 0\cdot 0 + 1\cdot 1 & 1\cdot 0 + 0\cdot 1 + 1\cdot 1 & 1\cdot 1 + 0\cdot 0 + 1\cdot 1 \\ 1\cdot 1 + 1\cdot 0 + 0\cdot 1 & 1\cdot 0 + 1\cdot 1 + 0\cdot 1 & 1\cdot 1 + 1\cdot 0 + 0\cdot 1 \\ 1\cdot 1 + 0\cdot 1 + 1\cdot 1 & 1\cdot 0 + 0\cdot 1 + 1\cdot 1 & 1\cdot 1 + 0\cdot 0 + 1\cdot 1 \end{bmatrix}$$

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

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

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

Question 2

(1) Solve binary linear system:

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

To begin with, we need a lemma: Law of Distribution for multiplication in binary field:

$$(a+b)x = ax + bx$$

We only need to prove the situation for two coefficients, then by reduction we can apply it to any multiplication formula.

(i) When $a = 0, b = 0, (a+b)x = 0 \cdot x = 0, ax + bx = 0 \cdot x + 0 \cdot x = 0 + 0 = 0$

$$LHS = RHS$$

So the formula is true in this case.

(ii) When $a = 0, b = 1, (a+b)x = 1 \cdot x = x, ax + bx = 0 \cdot x + 1 \cdot x = 0 + x = x$

$$LHS = RHS$$

So the formula is true in this case.

(iii) When $a = 1, b = 0, (a+b)x = 1 \cdot x = x, ax + bx = 1 \cdot x + 0 \cdot x = x + 0 = x$

$$LHS = RHS$$

So the formula is true in this case.

(iv) When $a = 1, b = 1, (a+b)x = 0 \cdot x = 0, ax + bx = x + x = 0$

$$LHS = RHS$$

So the formula is true in this case.

Now we have proved the Law of Distribution of multiplication in binary field.

we can write the matrix as augmented matrix:

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

Using Law of Distribution, we make some row operations to the augmented matrix

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

Calculate the matrix expression:

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

By Law of Distribution, we can change the matrix into linear equations:

$$x_1 + x_3 = 1$$
$$x_2 + x_3 = 1$$

where x_3 is a free variable, because the third column does not have a pivot. So, the solution of this linear system is:

$$x_1 = 1 - x_3$$
$$x_2 = 1 - x_3$$

So, the solution can be expressed using parametric vector form:

$$S = \begin{bmatrix} 1 - x_3 \\ 1 - x_3 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix}$$

$$x_3 \in \mathbb{B}, x_3 = \{0,1\}$$

When $x_3 = 0$, the solution is:

$$S_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + 0 \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

When $x_3 = 1$, the solution is:

$$S_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + 1 \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \cdot (-1) \\ 1 \cdot (-1) \\ 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+1 \\ 1+1 \\ 0+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

So, the solution set is:

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

(2) LU decomposition:

Using Law of Distribution, we can make row operations to original matrix:

First add row 1 to row 2, and row 3 to eliminate the elements in the first column:

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

Then, add row 2 to row 4:

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

Then, add row 3 to row 4:

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

U is row echelon form.

We should first consider the feasibility to use matrix multiplication to express row operations:

$$1 \cdot 1 = 1$$
$$1 \cdot 0 = 0$$

That is enough for our purpose, if there is a 1 in the entry, we can add 1 unit of the corresponding row to the new matrix.

We can write transformations above as matrix multiplication:

$$E_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$
$$E_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$
$$E_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Then the original matrix can be expressed as:

$$E_3 E_2 E_1 A = U$$

That is, A is equal to:

$$A = E_1^{-1} E_2^{-1} E_3^{-1} U$$

the inverse of an elementary matrix in binary field is the same as the original matrix, because $1 + 1 = 0$ is true in this field.

where,

$$E_1^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$
$$E_2^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$
$$E_3^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$
$$L = E_1^{-1} E_2^{-1} E_3^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

So, the LU decomposition for A is:

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, U = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Question 3

Let $\boldsymbol{a} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ and $\boldsymbol{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ be two arbitrary vectors in $\mathbb{B}^n$, then there are only four cases for addition between elements in $\boldsymbol{a}$ and $\boldsymbol{b}$, that is:

$$a_i = 0, b_i = 0$$
$$a_i = 0, b_i = 1$$
$$a_i = 1, b_i = 0$$
$$a_i = 1, b_i = 1$$

So, for any elements in $\boldsymbol{a} + \boldsymbol{b}$, say ith element of $\boldsymbol{a} + \boldsymbol{b}$, we have:

$$(a + b)_i = a_i + b_i = \{0,1\}$$

To prove the space is a vector space, we need to prove eight axioms,

A1. $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}$ for any $\boldsymbol{x}$ and $\boldsymbol{y}$ in V.

A2. $(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z})$ for any $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{z}$ in V.

A3. There exists an element $\boldsymbol{0}$ in such that $\boldsymbol{x} + \boldsymbol{0} = \boldsymbol{x}$ for each $\boldsymbol{x} \in V$.

A4. For each $\boldsymbol{x} \in V$, there exists an element $-\boldsymbol{x} \in V$ such that $\boldsymbol{x} + (-\boldsymbol{x}) = \boldsymbol{0}$.

A5. $\alpha(\boldsymbol{x} + \boldsymbol{y}) = \alpha\boldsymbol{x} + \alpha\boldsymbol{y}$ for each scalar α and any $\boldsymbol{x}$ and $\boldsymbol{y}$ in V.

A6. $(\alpha + \beta)\boldsymbol{x} = \alpha\boldsymbol{x} + \beta\boldsymbol{x}$ for any scalars α and β and any $\boldsymbol{x} \in V$.

A7. $(\alpha\beta)\boldsymbol{x} = \alpha(\beta\boldsymbol{x})$ for any scalars α and β and any $\boldsymbol{x} \in V$.

A8. $1\boldsymbol{x} = \boldsymbol{x}$ for all $\boldsymbol{x} \in V$.

Proof:

A1. $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}$ for any $\boldsymbol{x}$ and $\boldsymbol{y}$ in V.

Proof:

Let $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and $\boldsymbol{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ be two arbitrary vectors in V. Then by the addition law of binary matrix, $\boldsymbol{x} + \boldsymbol{y} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}$, denote each entry of $\boldsymbol{x} + \boldsymbol{y}$ as $x_i + y_i$, from the addition law of binary numbers,
because there are only four cases:

$$x_i = 0, y_i = 0, x_i + y_i = 0$$
$$x_i = 0, y_i = 1, x_i + y_i = 1$$
$$x_i = 1, y_i = 0, x_i + y_i = 1$$
$$x_i = 1, y_i = 1, x_i + y_i = 0$$

If we do the opposite, $\boldsymbol{y} + \boldsymbol{x} = \begin{bmatrix} y_1 + x_1 \\ \vdots \\ y_n + x_n \end{bmatrix}$, because there are only four cases:

$$x_i = 0, y_i = 0, x_i + y_i = 0$$
$$x_i = 1, y_i = 0, x_i + y_i = 1$$
$$x_i = 0, y_i = 1, x_i + y_i = 1$$
$$x_i = 1, y_i = 1, x_i + y_i = 0$$

The result is the same in each corresponding row.

So, $\begin{bmatrix} y_1 + x_1 \\ \vdots \\ y_n + x_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}$, then we have $\boldsymbol{y} + \boldsymbol{x} = \boldsymbol{x} + \boldsymbol{y}$.

A2. $(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z})$ for any $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{z}$ in V.

Proof:

Let $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and $\boldsymbol{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ and $\boldsymbol{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$ be three arbitrary vectors in V. Then by the addition law of binary matrix, $(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \begin{bmatrix} (x_1 + y_1) + z_1 \\ \vdots \\ (x_n + y_n) + z_n \end{bmatrix}$, denote each entry of $(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z}$ as $(x_i + y_i) + z_i$, from the addition law of binary numbers, because there are only 8 (2 * 2 * 2) cases:

$$x_i = 0, y_i = 0, z_i = 0, (x_i + y_i) + z_i = 0 + 0 = 0$$
$$x_i = 0, y_i = 0, z_i = 1, (x_i + y_i) + z_i = 0 + 1 = 1$$
$$x_i = 0, y_i = 1, z_i = 0, (x_i + y_i) + z_i = 1 + 0 = 1$$
$$x_i = 0, y_i = 1, z_i = 1, (x_i + y_i) + z_i = 1 + 1 = 0$$
$$x_i = 1, y_i = 0, z_i = 0, (x_i + y_i) + z_i = 1 + 0 = 1$$
$$x_i = 1, y_i = 0, z_i = 1, (x_i + y_i) + z_i = 1 + 1 = 0$$
$$x_i = 1, y_i = 1, z_i = 0, (x_i + y_i) + z_i = 0 + 0 = 0$$
$$x_i = 1, y_i = 1, z_i = 1, (x_i + y_i) + z_i = 0 + 1 = 1$$

and in the opposite,

$$\boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z}) = \begin{bmatrix} (x_1 + y_1) + z_1 \\ \vdots \\ (x_n + y_n) + z_n \end{bmatrix}$$

There are only 8 (2 * 2 * 2) cases:

$$x_i = 0, y_i = 0, z_i = 0, x_i + (y_i + z_i) = 0 + 0 = 0$$
$$x_i = 0, y_i = 0, z_i = 1, x_i + (y_i + z_i) = 0 + 1 = 1$$
$$x_i = 0, y_i = 1, z_i = 0, x_i + (y_i + z_i) = 1 + 0 = 1$$
$$x_i = 0, y_i = 1, z_i = 1, x_i + (y_i + z_i) = 1 + 1 = 0$$
$$x_i = 1, y_i = 0, z_i = 0, x_i + (y_i + z_i) = 1 + 0 = 1$$
$$x_i = 1, y_i = 0, z_i = 1, x_i + (y_i + z_i) = 1 + 1 = 0$$
$$x_i = 1, y_i = 1, z_i = 0, x_i + (y_i + z_i) = 0 + 0 = 0$$
$$x_i = 1, y_i = 1, z_i = 1, x_i + (y_i + z_i) = 0 + 1 = 1$$

All pairs of equations are equal, so,

$$\begin{bmatrix} (x_1 + y_1) + z_1 \\ \vdots \\ (x_n + y_n) + z_n \end{bmatrix} = \begin{bmatrix} (x_1 + y_1) + z_1 \\ \vdots \\ (x_n + y_n) + z_n \end{bmatrix}$$

That means,

$$(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}=\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$$

Proved.

A3. There exists an element $\mathbf{0}$ in such that $\boldsymbol{x}+\mathbf{0}=\boldsymbol{x}$ for each $\boldsymbol{x}\in V$.

Proof:

Suppose $\mathbf{0}=\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}$, then for any $\boldsymbol{x}\in V$, say $\boldsymbol{x}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$, we assume $\boldsymbol{x}+\mathbf{0}=\boldsymbol{x}$ is true.

So, our mission is to find all the coefficients of $\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}$.

By the Law of Addition of binary matrix,

$$\mathbf{0}+\boldsymbol{x}=\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}+\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}=\begin{bmatrix}a_1+x_1\\ \vdots\\ a_n+x_n\end{bmatrix}$$

Note that,

$$\boldsymbol{x}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$$

And there is a constraint,

$$\mathbf{0}+\boldsymbol{x}=\boldsymbol{x}$$

So,

$$\begin{bmatrix}a_1+x_1\\ \vdots\\ a_n+x_n\end{bmatrix}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$$

Then each entry is equal. Denote a_i+x_i to be an arbitrary entry of LHS, and x_i to be the corresponding entry of RHS, then $a_i+x_i=x_i$.
By the Law of Addition of binary field,

$$a_i+x_i+x_i=x_i+x_i$$

We have proved that $x_i+x_i=0$ for all $x_i\in\mathbb{B}$ before, then

$$a_i+x_i+x_i=x_i+x_i\Leftrightarrow a_i=0$$

So, each entry of $\mathbf{0}$ is 0. So, there exist $\mathbf{0}=\begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix}$ such that $\mathbf{0}+\boldsymbol{x}=\boldsymbol{x}$. Proved.

A4. For each $\boldsymbol{x}\in V$, there exists an element $-\boldsymbol{x}\in V$ such that $\boldsymbol{x}+(-\boldsymbol{x})=\mathbf{0}$.

Proof:

Define $-\boldsymbol{x}$ to be $-\boldsymbol{x}=\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}$. Then $\boldsymbol{x}+(-\boldsymbol{x})=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}+\begin{bmatrix}a_1\\ \vdots\\ a_n\end{bmatrix}=\begin{bmatrix}x_1+a_1\\ \vdots\\ x_n+a_n\end{bmatrix}$. Let $\boldsymbol{x}+(-\boldsymbol{x})=$

$\mathbf{0} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$, as proved before. Then we have $x_i + a_i = 0$ for all i. Then by the law of addition in binary field, $x_i + x_i + a_i = x_i$. That is, $0 + a_i = x_i \Leftrightarrow a_i = x_i$. Then we can express $-\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, this vector exists for every $\boldsymbol{x} \in V$. Proved.

A5. $\alpha(\boldsymbol{x} + \boldsymbol{y}) = \alpha\boldsymbol{x} + \alpha\boldsymbol{y}$ for each scalar α and any $\boldsymbol{x}$ and $\boldsymbol{y}$ in V.

Proof:

Let $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and $\boldsymbol{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ be two arbitrary vectors in V. Then by the addition law of binary matrix, $\alpha(\boldsymbol{x} + \boldsymbol{y}) = \begin{bmatrix} \alpha(x_1 + y_1) \\ \vdots \\ \alpha(x_n + y_n) \end{bmatrix}$, denote each entry of $\alpha(\boldsymbol{x} + \boldsymbol{y})$ as $\alpha(x_i + y_i)$, $\alpha\boldsymbol{x} + \alpha\boldsymbol{y} = \begin{bmatrix} \alpha x_1 + \alpha y_1 \\ \vdots \\ \alpha x_n + \alpha y_n \end{bmatrix}$, denote each entry of $\alpha\boldsymbol{x} + \alpha\boldsymbol{y}$ as $\alpha x_i + \alpha y_i$. from the addition law of binary numbers, and given $\alpha \in \mathbb{B}$, we know that α can only take value from {0,1}. because there are only 8 (2 * 2 *2) cases:

$$x_i = 0, y_i = 0, \alpha = 0, \alpha(x_i + y_i) = 0$$
$$x_i = 0, y_i = 0, \alpha = 1, \alpha(x_i + y_i) = 0$$
$$x_i = 0, y_i = 1, \alpha = 0, \alpha(x_i + y_i) = 0$$
$$x_i = 0, y_i = 1, \alpha = 1, \alpha(x_i + y_i) = 1$$
$$x_i = 1, y_i = 0, \alpha = 0, \alpha(x_i + y_i) = 0$$
$$x_i = 1, y_i = 0, \alpha = 1, \alpha(x_i + y_i) = 1$$
$$x_i = 1, y_i = 1, \alpha = 0, \alpha(x_i + y_i) = 0$$
$$x_i = 1, y_i = 1, \alpha = 1, \alpha(x_i + y_i) = 0$$

From the RHS, we find that there are only 8 (2 * 2 *2) cases:

$$x_i = 0, y_i = 0, \alpha = 0, \alpha x_i + \alpha y_i = 0$$
$$x_i = 0, y_i = 0, \alpha = 1, \alpha x_i + \alpha y_i = 0$$
$$x_i = 0, y_i = 1, \alpha = 0, \alpha x_i + \alpha y_i = 0$$
$$x_i = 0, y_i = 1, \alpha = 1, \alpha x_i + \alpha y_i = 1$$
$$x_i = 1, y_i = 0, \alpha = 0, \alpha x_i + \alpha y_i = 0$$
$$x_i = 1, y_i = 0, \alpha = 1, \alpha x_i + \alpha y_i = 1$$
$$x_i = 1, y_i = 1, \alpha = 0, \alpha x_i + \alpha y_i = 0$$
$$x_i = 1, y_i = 1, \alpha = 1, \alpha x_i + \alpha y_i) = 0$$

The result is the same in each corresponding row.

So, $\begin{bmatrix} \alpha(x_1 + y_1) \\ \vdots \\ \alpha(x_n + y_n) \end{bmatrix} = \begin{bmatrix} \alpha x_1 + \alpha y_1 \\ \vdots \\ \alpha x_n + \alpha y_n \end{bmatrix}$, , then we have $\alpha(\boldsymbol{x} + \boldsymbol{y}) = \alpha\boldsymbol{x} + \alpha\boldsymbol{y}$.

Proved.

A6. $(\alpha+\beta)\boldsymbol{x}=\alpha\boldsymbol{x}+\beta\boldsymbol{x}$ for any scalars α and β and any $\boldsymbol{x}\in V$.

Proof:

Let $\boldsymbol{x}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$ be arbitrary vector in V. And α and β are two numbers in $\mathbb{B}$. Then by the addition law of binary matrix, $(\alpha+\beta)\boldsymbol{x}=\begin{bmatrix}(\alpha+\beta)x_1\\ \vdots\\ (\alpha+\beta)x_n\end{bmatrix}$, denote each entry of $(\alpha+\beta)\boldsymbol{x}$ as $(\alpha+\beta)x_i$, $\alpha\boldsymbol{x}+\beta\boldsymbol{x}=\begin{bmatrix}\alpha x_1+\beta x_1\\ \vdots\\ \alpha x_n+\beta x_n\end{bmatrix}$, denote each entry of $\alpha\boldsymbol{x}+\beta\boldsymbol{x}$ as $\alpha x_n+\beta x_n$. From the addition law of binary numbers, and given $\alpha\in\mathbb{B}$, we know that α and β can only take values from {0,1}.
because there are only 8 (2 * 2 * 2) cases:

$$x_i=0,\alpha=0,\beta=0,(\alpha+\beta)x_i=0$$
$$x_i=0,\alpha=0,\beta=1,(\alpha+\beta)x_i=0$$
$$x_i=0,\alpha=1,\beta=0,(\alpha+\beta)x_i=0$$
$$x_i=0,\alpha=1,\beta=1,(\alpha+\beta)x_i=0$$
$$x_i=1,\alpha=0,\beta=0,(\alpha+\beta)x_i=0$$
$$x_i=1,\alpha=0,\beta=1,(\alpha+\beta)x_i=1$$
$$x_i=1,\alpha=1,\beta=0,(\alpha+\beta)x_i=1$$
$$x_i=1,\alpha=1,\beta=1,(\alpha+\beta)x_i=0$$

From the RHS, we find that there are only 8 (2 * 2 * 2) cases:

$$x_i=0,\alpha=0,\beta=0,\alpha x_i+\beta x_i=0$$
$$x_i=0,\alpha=0,\beta=1,\alpha x_i+\beta x_i=0$$
$$x_i=0,\alpha=1,\beta=0,\alpha x_i+\beta x_i=0$$
$$x_i=0,\alpha=1,\beta=1,\alpha x_i+\beta x_i=0$$
$$x_i=1,\alpha=0,\beta=0,\alpha x_i+\beta x_i=0$$
$$x_i=1,\alpha=0,\beta=1,\alpha x_i+\beta x_i=1$$
$$x_i=1,\alpha=1,\beta=0,\alpha x_i+\beta x_i=1$$
$$x_i=1,\alpha=1,\beta=1,\alpha x_i+\beta x_i=0$$

The result is the same in each corresponding row.

So, $\begin{bmatrix}(\alpha+\beta)x_1\\ \vdots\\ (\alpha+\beta)x_n\end{bmatrix}=\begin{bmatrix}\alpha x_1+\beta x_1\\ \vdots\\ \alpha x_n+\beta x_n\end{bmatrix}$, then we have $(\alpha+\beta)\boldsymbol{x}=\alpha\boldsymbol{x}+\beta\boldsymbol{x}$.

Proved.

A7. $(\alpha\beta)\boldsymbol{x}=\alpha(\beta\boldsymbol{x})$ for any scalars α and β and any $\boldsymbol{x}\in V$.

Proof:

Let $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ be arbitrary vector in V. And α and β are two numbers in $\mathbb{B}$. Then by the addition law of binary matrix, $(\alpha\beta)\boldsymbol{x} = \begin{bmatrix} (\alpha\beta)x_1 \\ \vdots \\ (\alpha\beta)x_n \end{bmatrix}$, denote each entry of $(\alpha\beta)\boldsymbol{x}$ as $(\alpha\beta)x_i$, $\alpha(\beta\boldsymbol{x}) = \begin{bmatrix} \alpha(\beta x_1) \\ \vdots \\ \alpha(\beta x_n) \end{bmatrix}$, denote each entry of $\alpha(\beta\boldsymbol{x})$ as $\alpha(\beta x_i)$. From the addition law of binary numbers, and given $\alpha \in \mathbb{B}$, we know that α and β can only take values from $\{0,1\}$.

because there are only 8 (2 * 2 * 2) cases:

$$x_i = 0, \alpha = 0, \beta = 0, (\alpha\beta)x_i = 0$$
$$x_i = 0, \alpha = 0, \beta = 1, (\alpha\beta)x_i = 0$$
$$x_i = 0, \alpha = 1, \beta = 0, (\alpha\beta)x_i = 0$$
$$x_i = 0, \alpha = 1, \beta = 1, (\alpha\beta)x_i = 0$$
$$x_i = 1, \alpha = 0, \beta = 0, (\alpha\beta)x_i = 0$$
$$x_i = 1, \alpha = 0, \beta = 1, (\alpha\beta)x_i = 0$$
$$x_i = 1, \alpha = 1, \beta = 0, (\alpha\beta)x_i = 0$$
$$x_i = 1, \alpha = 1, \beta = 1, (\alpha\beta)x_i = 1$$

From the RHS, we find that there are only 8 (2 * 2 * 2) cases:

$$x_i = 0, \alpha = 0, \beta = 0, \alpha(\beta x_i) = 0$$
$$x_i = 0, \alpha = 0, \beta = 1, \alpha(\beta x_i) = 0$$
$$x_i = 0, \alpha = 1, \beta = 0, \alpha(\beta x_i) = 0$$
$$x_i = 0, \alpha = 1, \beta = 1, \alpha(\beta x_i) = 0$$
$$x_i = 1, \alpha = 0, \beta = 0, \alpha(\beta x_i) = 0$$
$$x_i = 1, \alpha = 0, \beta = 1, \alpha(\beta x_i) = 0$$
$$x_i = 1, \alpha = 1, \beta = 0, \alpha(\beta x_i) = 0$$
$$x_i = 1, \alpha = 1, \beta = 1, \alpha(\beta x_i) = 1$$

The result is the same in each corresponding row.

So, $\begin{bmatrix} (\alpha\beta)x_1 \\ \vdots \\ (\alpha\beta)x_n \end{bmatrix} = \begin{bmatrix} \alpha(\beta x_1) \\ \vdots \\ \alpha(\beta x_n) \end{bmatrix}$, then we have $(\alpha\beta)\boldsymbol{x} = \alpha(\beta\boldsymbol{x})$.

Proved.

A8. $1\boldsymbol{x} = \boldsymbol{x}$ for all $\boldsymbol{x} \in V$.

Proof:

Let $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ be arbitrary vector in V. Then by the scalar multiplication law of binary matrix, $1\boldsymbol{x} = \begin{bmatrix} 1x_1 \\ \vdots \\ 1x_n \end{bmatrix}$, denote each entry of $1\boldsymbol{x}$ as $1x_i$, from the multiplication law of binary numbers,
because there are only two cases:

$$x_i = 0, 1x_i = 0$$
$$x_i = 1, 1x_i = 1$$

If we do the opposite, $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, because there are only two cases:

$$x_i = 0, x_i = 0$$
$$x_i = 1, x_i = 1$$

The result is the same in each corresponding row.

So, $\begin{bmatrix} 1x_1 \\ \vdots \\ 1x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, then we have $1\boldsymbol{x} = \boldsymbol{x}$.

Proved.

Question 4

The vector $\boldsymbol{a}$ in space $\mathbb{B}^n$ consists of n independent elements. Each of the elements has a value inside $\mathbb{B} = \{0,1\}$, so, we can assign any of these two values to that element. There are k elements in total, so the total number of combinations is:

$$2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 = 2^k$$

So, the total number of vectors is equal to the total number of combinations, that is, 2^k.

Appendix:

Let the generator matrix be $G = \begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} \end{bmatrix}$ and the vector $x \in \mathbb{B}^n$, then the desired space can be expressed as $\{G\boldsymbol{x} : x \in \mathbb{B}^k\}$.

Question 5:
Consider an arbitrary binary linear equation:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix}$$

where all the numbers above are inside the binary space $\mathbb{B}$.

To solve the equation, we use augmented matrix:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} & c_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & c_m \end{bmatrix}$$

Suppose we have turned it into row echelon form, yields:

$$\begin{bmatrix} a'_{11} & \cdots & a'_{1n} & c'_1 \\ 0 & \ddots & \vdots & \vdots \\ 0 & 0 & a'_{mn} & c'_m \end{bmatrix}$$

Suppose there are k pivots in this row echelon form, then the number of free variables is $n-k$, so the solution can be written in vector parametric form. Then we can find 2^{n-k} combinations of free variable, because $x_i \in \mathbb{B}$. Each x_i only has two possible values, so the total number of combinations are 2^{n-k},because there are only $n-k$ free variables.

We find that the solutions of binary linear equations are always countable and limited. And for linear equations defined on $\mathbb{R}$, we usually have unlimited solutions from one linear equation. The only exception is that when the matrix is in full rank, there are 0 free variable, so we have only 1 solution, which is finite.

The difference lies in whether the number of solutions is finite: In binary case, the number of solutions is finite, while in real number case, the number of solutions is infinite.
In binary case, the number of solutions is determined by the number of free variables, while in real number case, they have no correlation.

The final answer is:
For linear equation where numbers are Real Values, the solution type is: (1) Unique solution, (2) infinitely many solutions, (3) no solution.
For linear equation where numbers are Binary Values, the solution type is: (1) Unique solution, (2) finitely many solutions, (3) no solution.

2. Error Correcting Codes
Suppose the generator matrix is G,

$$G\boldsymbol{x} = G\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

Suppose $G\boldsymbol{x}$ and $G\boldsymbol{y}$ are both from subspace of $\mathbb{B}^7$, i.e.,

$$G\boldsymbol{x} = G\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

and,

$$G\boldsymbol{y} = G\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$$

where x_1, x_2, x_3, x_4 and y_1, y_2, y_3, y_4 are all from $\mathbb{B}$, so they can only take values in {0,1}, and then,

$$G\boldsymbol{x} + G\boldsymbol{y} = G\begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \\ x_4 + y_4 \end{bmatrix}$$

where $x_i + y_i$ will always be {0,1}, so $G\boldsymbol{x} + G\boldsymbol{y}$ will be inside $G\boldsymbol{x}$. (Property 1 proved).
Let α take values in {0,1}, then,

$$\alpha G\boldsymbol{x} = G\alpha\boldsymbol{x} = G\begin{bmatrix} \alpha x_1 \\ \alpha x_2 \\ \alpha x_3 \\ \alpha x_4 \end{bmatrix}$$

According to the Law of Multiplication in binary filed,

$$\alpha x_i \in \mathbb{B}$$

So, $\alpha G\boldsymbol{x}$ is also inside $G\boldsymbol{x}$. (Property 2 proved).

Then we conclude that $G\boldsymbol{x}$ is a subspace of $\mathbb{B}^7$.
Then we construct generator matrix:
Because the given vector is:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_2 + x_3 + x_4 \\ x_1 + x_3 + x_4 \\ x_1 + x_2 + x_4 \end{bmatrix}$$

It can be written as:

$$= \begin{bmatrix} 1 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 + 0 \cdot x_4 \\ 0 \cdot x_1 + 1 \cdot x_2 + 0 \cdot x_3 + 0 \cdot x_4 \\ 0 \cdot x_1 + 0 \cdot x_2 + 1 \cdot x_3 + 0 \cdot x_4 \\ 0 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 + 1 \cdot x_4 \\ 0 \cdot x_1 + 1 \cdot x_2 + 1 \cdot x_3 + 1 \cdot x_4 \\ 1 \cdot x_1 + 0 \cdot x_2 + 1 \cdot x_3 + 1 \cdot x_4 \\ 1 \cdot x_1 + 1 \cdot x_2 + 0 \cdot x_3 + 1 \cdot x_4 \end{bmatrix}$$

Then we have:

$$= \begin{bmatrix} 1 \cdot x_1 \\ 0 \cdot x_1 \\ 0 \cdot x_1 \\ 0 \cdot x_1 \\ 0 \cdot x_1 \\ 1 \cdot x_1 \\ 1 \cdot x_1 \end{bmatrix} + \begin{bmatrix} 0 \cdot x_2 \\ 1 \cdot x_2 \\ 0 \cdot x_2 \\ 0 \cdot x_2 \\ 1 \cdot x_2 \\ 0 \cdot x_2 \\ 1 \cdot x_2 \end{bmatrix} + \begin{bmatrix} 0 \cdot x_3 \\ 0 \cdot x_3 \\ 1 \cdot x_3 \\ 0 \cdot x_3 \\ 1 \cdot x_3 \\ 1 \cdot x_3 \\ 0 \cdot x_3 \end{bmatrix} + \begin{bmatrix} 0 \cdot x_4 \\ 0 \cdot x_4 \\ 0 \cdot x_4 \\ 1 \cdot x_4 \\ 1 \cdot x_4 \\ 1 \cdot x_4 \\ 1 \cdot x_4 \end{bmatrix}$$

Furthermore,

$$= x_1\begin{bmatrix}1\\0\\0\\0\\0\\1\\1\end{bmatrix} + x_2\begin{bmatrix}0\\1\\0\\0\\1\\0\\1\end{bmatrix} + x_3\begin{bmatrix}0\\0\\1\\0\\1\\1\\0\end{bmatrix} + x_4\begin{bmatrix}0\\0\\0\\1\\1\\1\\1\end{bmatrix}$$

By the Law of Matrix Multiplication,

$$= \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\0&1&1&1\\1&0&1&1\\1&1&0&1\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}$$

So, the generator matrix is:

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

because $\boldsymbol{Gx}$ can represent all codeword vectors.

Question 7

To solve the binary linear equation

$$H\boldsymbol{x} = \mathbf{0}$$

where

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

This equation can be written as:

$$\begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{bmatrix} = \mathbf{0}$$

which is equivalent to:

$$x_2 + x_3 + x_4 + x_5 = 0$$
$$x_1 + x_3 + x_4 + x_6 = 0$$
$$x_1 + x_2 + x_4 + x_7 = 0$$

Then,

$$x_2 + x_3 + x_4 + x_5 + x_5 = 0 + x_5$$
$$x_1 + x_3 + x_4 + x_6 + x_6 = 0 + x_6$$
$$x_1 + x_2 + x_4 + x_7 + x_7 = 0 + x_7$$

Because $x_i + x_i = 0$,

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

There are three pivots in matrix H, so pivot variables are x_5, x_6, x_7. and thus four free variables are x_1, x_2, x_3, x_4. So, the solution can be expressed in vector parametric form:

$$S = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_2 + x_3 + x_4 \\ x_1 + x_3 + x_4 \\ x_1 + x_2 + x_4 \end{bmatrix}$$

That is our desired result. Proved.

Question 8

Given that we have at most 1 error, that means if $\boldsymbol{s} = \mathbf{0}$, there will be no errors.

Given that we have at most 1 error, there will will be exactly 1 error if $\boldsymbol{s} \neq \mathbf{0}$.

Given $H\boldsymbol{x} = \mathbf{0}$,

$$\boldsymbol{s} = H\boldsymbol{y} = H(\boldsymbol{x} + \boldsymbol{e}) = H\boldsymbol{x} + H\boldsymbol{e} = H\boldsymbol{e}$$

Then, we can find that:

if

$$H\boldsymbol{y} = \mathbf{0},$$

we will have:

$$\boldsymbol{s} = \mathbf{0}$$

which means:

$$H\boldsymbol{e} = \mathbf{0}$$

is True as well,

because we have at most 1 error, $\boldsymbol{e}$ can only have 1 nonzero entry, so $H\boldsymbol{e} \neq \mathbf{0}$ always exists.

then if we know:

$$H\boldsymbol{e} = \mathbf{0}$$

That means the only solution is:

$$\boldsymbol{e} = \mathbf{0}$$

So, we plug

$$\boldsymbol{y} = (1,1,0,1,0,0,1)^T$$

into the check matrix:

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

$$= \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0+1+1+0 \\ 1+0+1+0 \\ 1+1+1+1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

So, by the theorem we proved above,

$$\boldsymbol{e} = \mathbf{0}$$

is True as well,

So, $\boldsymbol{x}$ can be obtained by:

$$\begin{aligned} & \boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e} \\ \Leftrightarrow\ & \boldsymbol{y} + \boldsymbol{e} = \boldsymbol{x} + \boldsymbol{e} + \boldsymbol{e} \\ \Leftrightarrow\ & \boldsymbol{y} + \boldsymbol{e} = \boldsymbol{x} + \mathbf{0} \\ \Leftrightarrow\ & \boldsymbol{x} = \boldsymbol{y} + \boldsymbol{e} \end{aligned}$$

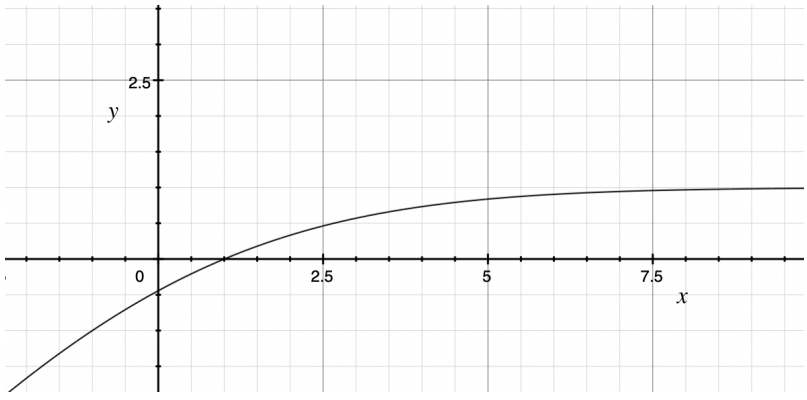
Then, we have:

$$\boldsymbol{x} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

The answer is:

$$\boldsymbol{x} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Question 9 (1)



The efficiency function of $2^m - 1, 2^m - m - 1$ Hamming Code

Suppose there exist a generator matrix G of that Hamming Code codewords.

There will be $2^m - m - 1$ free variables, because the $(2^m - 1, 2^m - m - 1)$ Hamming Code codewords are expressed in terms of those free variables.

Then any vector in this space can be denoted as:

$$G\boldsymbol{x} = G\begin{bmatrix} x_1 \\ \vdots \\ x_{2^m-m-1} \end{bmatrix}$$

Suppose $G\boldsymbol{x}$ and $G\boldsymbol{y}$ are both from **our desired** subspace of $\mathbb{B}^{2^m-1}$, i.e.,

$$G\boldsymbol{x} = G\begin{bmatrix} x_1 \\ \vdots \\ x_{2^m-m-1} \end{bmatrix}$$

and

$$G\boldsymbol{y} = G\begin{bmatrix} y_1 \\ \vdots \\ y_{2^m-m-1} \end{bmatrix}$$

where $x_1, \dots, x_{2^m-m-1}$, and $y_1, \dots, y_{2^m-m-1}$ are all from $\mathbb{B}$, so they can only take values in {0,1}, and then,

$$G\boldsymbol{x} + G\boldsymbol{y} = G\begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_{2^m-m-1} + y_{2^m-m-1} \end{bmatrix}$$

where $x_i + y_i$ will always be {0,1}, so $G\boldsymbol{x} + G\boldsymbol{y}$ will be inside $G\boldsymbol{x}$. (Property 1 proved).
Let α take values in {0,1}, then,

$$\alpha G\boldsymbol{x} = Ga\boldsymbol{x} = G\begin{bmatrix} \alpha x_1 \\ \vdots \\ \alpha x_{2^m-m-1} \end{bmatrix}$$

According to the Law of Multiplication in binary filed,

$$\alpha x_i \in \mathbb{B}$$

So, $\alpha G\boldsymbol{x}$ is also inside $G\boldsymbol{x}$. (Property 2 proved).
Then we conclude that $G\boldsymbol{x}$ is a subspace of $\mathbb{B}^{2^m-1}$.

Question 9 (2)

We begin with parity-check matrix:
These matrices have $2^m - 1$ columns, and each column is binary number with length of m, i.e,

$$\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix}$$

where $a_i \in \mathbb{B}$ for all i.
Then, we know that each entry has 2 possible outcomes, so we have 2^m combinations in total. Then we ignore the combination which all entries are 0, then we have $2^m - 1$ combinations available.
The order of the vector in the matrix H does not matter, cause we don't know the generator matrix yet. It is arbitrary.
Then we construct such a matrix arbitrarily, say,

$$H = \begin{bmatrix} a_{1,1} & \cdots & a_{2^m-1,1} \\ \vdots & \ddots & \vdots \\ a_{1,m} & \cdots & a_{2^m-1,m} \end{bmatrix}$$

For example, when $m = 4$, we generate a parity-check matrix H:

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

It has 4 rows and 15 columns.

Re-arrange the matrix H to find out pivot columns:

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

Them, the first 4 columns form an identity matrix, the remaining columns are divided from the identity matrix.

Consider the binary linear equation:

$$H\boldsymbol{x} = \mathbf{0}$$

From the example, we can find that there exist $15 - 4 = 11$ free variables. In general case, we have $2^m - m - 1$ free variables.

The solution of

$$H\boldsymbol{x} = \mathbf{0}$$

is the space spanned by the generator matrix G:

$$H\boldsymbol{x} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Then solve this equation, we get:

$$x_1 = x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15}$$
$$x_2 = x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15}$$
$$x_3 = x_6 + x_7 + x_8 + x_{10} + x_{11} + x_{14} + x_{15}$$
$$x_4 = x_5 + x_7 + x_8 + x_9 + x_{11} + x_{13} + x_{15}$$

So, the codewords can be represented by:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix} = \begin{bmatrix} x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} \\ x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15} \\ x_6 + x_7 + x_8 + x_{10} + x_{11} + x_{14} + x_{15} \\ x_5 + x_7 + x_8 + x_9 + x_{11} + x_{13} + x_{15} \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix}$$

$$= \begin{bmatrix} & & & & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & & & & & 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 & & 1 & 1 & & & 1 & 1 \\ 1 & & 1 & 1 & 1 & & 1 & & 1 & & 1 \\ 1 & & & & & & & & & & \\ & 1 & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & 1 & & & & & & & \\ & & & & 1 & & & & & & \\ & & & & & 1 & & & & & \\ & & & & & & 1 & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & 1 & \\ & & & & & & & & & & 1 \end{bmatrix} \begin{bmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix}$$

So, the generator matrix is clear:

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

In general case:

$$H\boldsymbol{x} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \quad 0 & 0 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & \quad 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \ddots & 0 & 0 & \quad 1 & 1 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & \quad 0 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & \quad 1 & 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_{2^m-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

Then solve this equation, we get:

$$
\begin{aligned}
x_1 &= \sum_{i \in S_1} x_i \\
x_2 &= \sum_{i \in S_2} x_i \\
x_3 &= \sum_{i \in S_3} x_i \\
&\cdots \\
x_m &= \sum_{i \in S_m} x_i
\end{aligned}
$$

where S_j refers to a subset of $\{x_{m+1}, x_{m+2}, \ldots, x_{2^m-1}\}$ with length of $2^m - 2m - 1$. So, the codewords can be represented by:

$$
\begin{bmatrix} x_1 \\ \vdots \\ x_m \\ x_{m+1} \\ \vdots \\ x_{2^m-1} \end{bmatrix} = \begin{bmatrix} \sum_{i \in S_1} x_i \\ \vdots \\ \sum_{i \in S_m} x_i \\ x_{m+1} \\ \vdots \\ x_{2^m-1} \end{bmatrix}
$$

This vector can be further expressed in matrix-vector multiplication form,

$$
= \begin{bmatrix}
* & & & & * & * & * & * & * & * & * \\
* & * & * & & & & & * & * & * & * \\
 & * & * & * & & * & * & & & * & * \\
 & & * & * & * & & * & & * & & * \\
 & & & & & & & & & & \\
1 & & & & & & & & & & \\
 & 1 & & & & & & & & & \\
 & & 1 & & & & & & & & \\
 & & & 1 & & & & & & & \\
 & & & & 1 & & & & & & \\
 & & & & & \ddots & & & & & \\
 & & & & & & 1 & & & & \\
 & & & & & & & 1 & & & \\
 & & & & & & & & 1 & & \\
 & & & & & & & & & 1 & \\
 & & & & & & & & & & 1
\end{bmatrix} \begin{bmatrix} x_{m+1} \\ \vdots \\ x_{2^m-1} \end{bmatrix}
$$

So, the generator matrix is clear:

$$G = \begin{bmatrix} * & & & & * & * & * & * & * & * & * \\ * & * & * & & & & & * & * & * & * \\ & * & * & * & & * & * & & & * & * \\ & & * & * & * & & * & & * & & * \\ 1 & & & & & & & & & & \\ & 1 & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & 1 & & & & & & & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 1 & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & 1 & \\ & & & & & & & & & & 1 \end{bmatrix}$$

Then we have solved for the generator matrix.

So, the algorithm is:

(1) Arbitrarily construct a parity-check matrix, we can do it using binary number sequentially.
(2) Solve the equation $H\boldsymbol{x} = \mathbf{0}$, and get pivot variables in terms of free variables.
(3) Solve for generator matrix G, by applying matrix-vector multiplication.
(4) Encoding: Provide a signal $\boldsymbol{s}$ to be encoded, calculate $G\boldsymbol{s}$ to obtain the encoded signal $\boldsymbol{s}'$.
(5) Add some error (if possible) to the encoded signal $\boldsymbol{s}' = \boldsymbol{s} + \boldsymbol{e}$. We will observe $\boldsymbol{s}'$ now.
(6) **Decoding:** Calculate $H\boldsymbol{s}'$ to check if there is any error. Obtain the error vector $\boldsymbol{e}$ by do the above operations. Add the error back to get original signal $\boldsymbol{s} = \boldsymbol{s}' + \boldsymbol{e}$.