Part I

Groups and Coding

Coding theory

- In today's modern world of communication, data items are constantly being transmitted from point to point.
- The basic problem in transmission of data is that of receiving the data as sent and not receiving a distorted piece of data.

Unit of Information

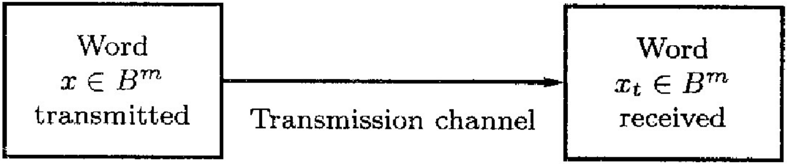
- Message is a finite sequence of characters from a finite alphabet
  $B = \{0, 1\}$
- Word is a sequence of m 0's and 1's.

Groups

- The set B is a group under the binary operation $+$ (mod 2 addition)
- It follows that $B^m = B \times B \times \cdots \times B$ (n factors) is a group under the operator $\oplus$ defined by
  $(x_1, x_2, \ldots, x_m) \oplus (y_1, y_2, \ldots, y_m) =$
  $(x_1 + y_1, x_2 + y_2, \ldots, x_m + y_m)$
- An element in B^m will be written as $(b_1, b_2, \ldots, b_m)$ or more simply as $b_1 b_2 \ldots b_m$

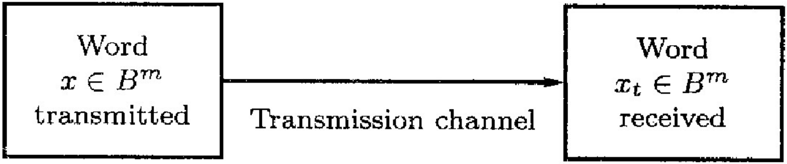
Transmission channel and Noise

- An element $x \in B^m$ is sent through the transmission channel and is received as an element $x_t \in B^m$.



Transmission Channel and Noise

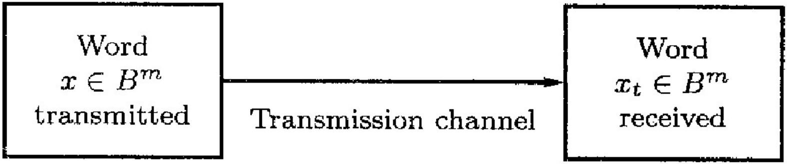
- Noise in the transmission channel may cause a 0 to be received as a 1, or vice versa, lead $x \neq x_t$.



对 $\longrightarrow$ 对

Transmission Channel and Noise

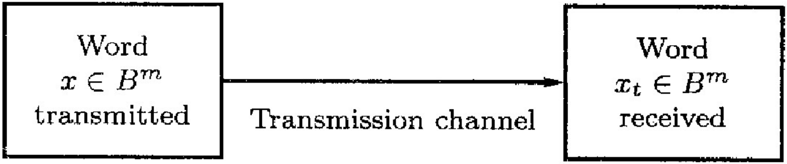
- Noise in the transmission channel may cause a 0 to be received as a 1, or vice versa, lead $x \neq x_t$.



对 ————————> 错

Transmission Channel and Noise

- Noise in the transmission channel may cause a 0 to be received as a 1, or vice versa, lead $x \neq x_t$.



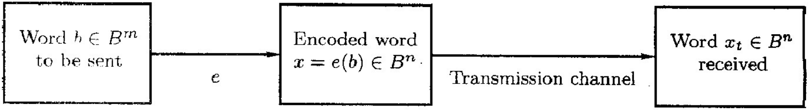
对 ——————> 錯

Coding Theory

- Coding theory has developed techniques for introducing redundant information in transmitted data that help in detecting, and sometimes in correcting, errors.

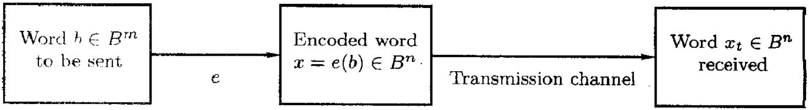
Definition (Encoding Function)

- Choose: an integer $n \geq m$ and a one-to-one function $e : B^m \to B^n$
  - e is called an (m, n) encoding function, representing every word in B^m as a word in B^n.
  - If $b \in B^m$, then $e(b)$ is called the code word representing b.



Encoding Function

- If the transmission channel is noiseless, then $x_t = x$ for all x in B^n.
- In this case $x = e(b)$ is received for each $b \in B^m$, and since e is a known function, b may be identified.
- In general, errors in transmission do occur.
- We will say that the code word $x = e(b)$ has been transmitted with k or fewer errors if x and x_t differ in at least 1 but no more than k positions.



Definition (Error Detection)

- Let $e : B^m \to B^n$ be an (m, n) encoding function.
- e detects k or fewer errors if whenever $x = e(b)$ is transmitted with k or fewer errors, then x_t is not a code word (thus xt could not be x and therefore could not have been correctly transmitted).

Definition (Weight)

- For $b \in B^n$, the number of 1's in x is called the weight of x and is denoted by $|x|$
- Find the weight of each of the following words in B^5.
  - $x = 01000 \quad |x| = 1$
  - $x = 11100 \quad |x| = 3$
  - $x = 00000 \quad |x| = 0$
  - $x = 11111 \quad |x| = 5$

Example (Parity Check Code)

- The following encoding function $e : B^m \to B^{m+1}$ is called the parity $(m, m+1)$ check code:
- If $b = b_1 b_2 \ldots b_m \in B^m$, define

$$e(b) = b_1 b_2 \ldots b_m b_{m+1}$$

- where

$$b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd} \end{cases}$$

Example (Parity Check Code)

- Let $m = 3$. Then
  - $e(000) = 0000$
  - $e(001) = 0011$
  - $e(010) = 0101$
  - $e(011) = 0110$
  - $e(100) = 1001$
  - $e(101) = 1010$
  - $e(110) = 1100$
  - $e(111) = 1111$
- Suppose now that $b = 111$. Then $x = e(b) = 1111$.

Example (3m Encoding Function)

- Consider the $(m, 3m)$ encoding function $e : B^m \to B^{3m}$.
- If $b = b_1 b_2 \ldots b_m \in B^m$, define
  $e(b) = b_1 b_2 \ldots b_m b_1 b_2 \ldots b_m b_1 b_2 \ldots b_m$
  - $e(000) = 000000000$
  - $e(001) = 001001001$
  - $e(010) = 010010010$
  - $e(011) = 011011011$
  - $e(100) = 100100100$
  - $e(101) = 101101101$
  - $e(110) = 110110110$
  - $e(111) = 111111111$

Example (3m Encoding Function)

- Suppose now that $b = 011$, then $e(011) = 011011011$.
- Assume now we receive the word 011111011. This is not a code word, so we have detected the error.

Definition (Hamming Distance)

- Let x and y be words in B^m. The Hamming distance $\delta(x, y)$ between x and y is the weight, $|x \oplus y|$, of $x \oplus y$.
- The distance between $x = x_1x_2 \ldots x_m$ and $y = y_1y_2 \ldots y_m$ is the number of various of i such that $x_i \neq y_i$, that is, the number of positions in which x and y differ.
- Using the weight of $x \oplus y$ is a convenient way to count the number of different positions.

Example

- Find the distance between x and y:
  - $x = 110110,\ y = 000101$
  - $x = 001100,\ y = 010110.$

Solution

- $x \oplus y = 110011$, *so* $|x \oplus y| = 4$
- $x \oplus y = 011010$, *so* $|x \oplus y| = 3$

Theorem (Properties of Distance Function)

- *Let x, y, and z be elements of B^m. Then*
  - *(a)* $\delta(x,y) = \delta(y,x)$
  - *(b)* $\delta(x,y) \geq 0$
  - *(c)* $\delta(x,y) = 0$ *if and only if* $x = y$
  - *(d)* $\delta(x,y) \leq \delta(x,z) + \delta(z,y)$

Proof. of (d).

$$\begin{aligned}
\delta(x,y) &= |x \oplus y| = |x \oplus \mathbf{0} \oplus y| \\
&= |x \oplus z \oplus z \oplus y| \\
&\leq |x \oplus z| + |z \oplus y|
\end{aligned}$$

Definition (Minimum Distance)

- The minimum distance of an encoding function $e : B^m \to B^n$ is the minimum of the distances between all distinct pairs of code words; that is,

$$\min\{\delta(e(x), e(y)) | x, y \in B^m\}$$

Example

- Consider the following $(2, 5)$ encoding function e:
  - $e(00) = 00000$
  - $e(01) = 00111$
  - $e(10) = 01110$
  - $e(11) = 11111$
- Minimum distance?

Theorem (2)

- *An (m, n) encoding function $e : B^m \to B^n$ can detect k or fewer errors*
  - *if and only if*
- *its minimum distance is at least $k + 1$.*

Proof: $\Leftarrow$ the minimum distance is at least $k+1$.

- Let $b \in B^m$, and let $x = e(b) \in B^n$ be the code word representing b.
  - x is transmitted and is received as x_t. If x_t were a code word different from x, then $\delta(x, x_t) \geq k+1$, so x would be transmitted with $k+1$ or more errors.
  - Thus, if x is transmitted with k or fewer errors, then x_t cannot be a code word.
  - This means that e can detect k or fewer errors.

Proof: e can detect k or fewer errors $\Rightarrow$.

- Suppose that the minimum distance between code words is $r \leq k$
- Let x and y be code words with $\delta(x, y) = r$.
  - If $x_t = y$, that is, if x is transmitted and is mistakenly received as y, then $r \leq k$ errors have been committed and have not been detected.
- Thus it contradict with e can detect k or fewer errors.

Example (6)

- How many errors will e detect?
  - $e(000) = 00000000$
  - $e(001) = 10011100$
  - $e(010) = 00101101$
  - $e(011) = 10010101$
  - $e(100) = 10100100$
  - $e(101) = 10001001$
  - $e(110) = 00011100$
  - $e(111) = 00110001$

Definition (Group Codes)

- An (m, n) encoding function $e : B^m \to B^n$ is called a group code if
  - $e(B^m) = \{e(b) | e(b) \in B^n\} = Ran(e)$
- is a subgroup of B^n

Subgroups

- Recall from the definition of subgroup that N is a subgroup of B^n if
  - (a) the identity of B^n is in N,
  - (b) if x and y belong to N, then $x \oplus y \in N$, and
  - (c) if x is in N, then its inverse is in N.

Example (is e a group code?)

- Consider the $(3, 6)$ encoding function $e : B^3 \to B^6$ defined by
  - $e(000) = 000000$
  - $e(001) = 001100$
  - $e(010) = 010011$
  - $e(011) = 011111$
  - $e(100) = 100101$
  - $e(101) = 101001$
  - $e(110) = 110110$
  - $e(111) = 111001$

Example (is e a group code?)

- We must show that the set of all code words
  - $N = \{000000, 001100, 010011, 011111, 100101, 101001, 110110, 111010\}$
- is a subgroup of B^6.

Theorem

- *Let* $e : B^m \to B^n$ *be a group code. The minimum distance of* e *is the minimum weight of a nonzero code word.*

Proof.

- Let δ be the minimum distance of the group code, and suppose that $\delta = \delta(x, y)$, where x and y are distinct code words.
- Also, let η be the minimum weight of a nonzero code word and suppose that $\eta = |z|$ for a code word z.
- Since e is a group code, $x \oplus y$ is a nonzero code word. Thus
  - $\delta = \delta(x, y) = |x \oplus y| \geq \eta$.
- On the other hand, since $\mathbf{0}$ and z are distinct code words,
  - $\eta = |z| = |z \oplus \mathbf{0}| = \delta(z, \mathbf{0}) \geq \delta$
- Hence $\eta = \delta$.

Example

- The minimum distance of the following group code is 2
  - $e(000) = 000000$
  - $e(001) = 001100$
  - $e(010) = 010011$
  - $e(011) = 011111$
  - $e(100) = 100101$
  - $e(101) = 101001$
  - $e(110) = 110110$
  - $e(111) = 111001$
- To check this directly would require 28 different calculations.

Example (A review on Boolean matrices)

- mod-2 sum $D \oplus E$
- mod-2 Boolean product $D * E$

Theorem

- *Let D and E be $m \times p$ Boolean matrices, and let F be a $p \times n$ Boolean matrix. Then*
  - $(D \oplus E) * F = (D * F) \oplus (E * F)$
- *That is, a distributive property holds for $\oplus$ and $*$.*

Convention

- We shall now consider the element $x = x_1 x_2 \dots x_n \in B^n$ as the $1 \times n$ matrix $[x_1 x_2 \dots x_n]$

Theorem (5)

- *Let* m *and* n *be nonnegative integers with* $m < n$, $r = n - m$, *and let* **H** *be an* $n \times r$ *Boolean matrix.*
- *Then the function* $f_H : B^n \to B^r$ *defined by*
  - $f_H(x) = x * \mathbf{H}, x \in B^n$
- *is a homomorphism from the group* B^n *to the group* B^r.

Proof.

- If x and y are elements in B^n, then

$$\begin{aligned} f_H(x \oplus y) &= (x \oplus y) * \mathbf{H} \\ &= (x * \mathbf{H}) \oplus (y * \mathbf{H}) \\ &= f_H(x) \oplus f_H(y) \end{aligned}$$

- Hence f_H is a homomorphism from B^n to B^r

❀

Corollary (1)

- *Let m, n, r, **H**, and f_H be as in Theorem 5. Then*
  - $N = \{x \in B^n | x * \boldsymbol{H} = \boldsymbol{0}\}$
  - *is a normal subgroup of B^n.*

Proof.

- N is the kernel of the homomorphism f_H, so it is a normal subgroup of B^n.

Example (Parity check matrix)

- Let $m < n$ and $r = n - m$, the following $n \times r$ Boolean matrix is called a parity check matrix.

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{m\times r} \\ \mathbf{I}_r \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1r} \\ h_{21} & h_{22} & \dots & h_{2r} \\ \dots & \dots & & \dots \\ h_{m1} & h_{m2} & \dots & h_{mr} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Example (Encoding function)

- Define an encoding function $e_H : B^m \to B^n$. For $b = b_1 b_2 \ldots b_m$,
- Let $x = e_H(b) = b_1 b_2 \ldots b_m x_1 x_2 \ldots x_r$, where

$$\begin{aligned}
x_1 &= b_1 \cdot h_{11} + b_2 \cdot h_{21} + \cdots + b_m \cdot h_{m1} \\
x_2 &= b_1 \cdot h_{12} + b_2 \cdot h_{22} + \cdots + b_m \cdot h_{m2} \\
\ldots \\
x_r &= b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \cdots + b_m \cdot h_{mr}
\end{aligned}$$

$$\begin{bmatrix} x_1 & x_2 & \ldots & x_r \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & \ldots & b_m \end{bmatrix} * \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1r} \\ h_{21} & h_{22} & \ldots & h_{2r} \\ \ldots & \ldots & & \ldots \\ h_{m1} & h_{m2} & \ldots & h_{mr} \end{bmatrix}$$

Example ($e_H : B^m \to B^n$ in matrix format)

$e_H(B^m)$

$$
\begin{aligned}
&= B^m * [I_m \ H_{m\times r}] \\
&= \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1r} \\ b_{21} & b_{22} & \dots & b_{2r} \\ \dots & \dots & & \dots \\ b_{2^m 1} & b_{2^m 2} & \dots & b_{2^m r} \end{bmatrix} \begin{bmatrix} 1 & \dots & 0 & h_{11} & h_{12} & \dots & h_{1r} \\ 0 & \dots & 0 & h_{21} & h_{22} & \dots & h_{2r} \\ \dots & & \dots & \dots & \dots & & \dots \\ 0 & \dots & 1 & h_{m1} & h_{m2} & \dots & h_{mr} \end{bmatrix} \\
&= \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1r} & x_{11} & x_{12} & \dots & x_{1r} \\ b_{21} & b_{22} & \dots & b_{2r} & x_{21} & x_{22} & \dots & x_{2r} \\ \dots & \dots & & \dots & \dots & \dots & & \dots \\ b_{2^m 1} & b_{2^m 2} & \dots & b_{2^m r} & x_{2^m 1} & x_{2^m 2} & \dots & x_{2^m r} \end{bmatrix}
\end{aligned}
$$

Theorem (6)

- *Let*
  - $x = y_1 y_2 \ldots y_m x_1 \ldots x_r \in B^n$
- *Then*
  - $x * \boldsymbol{H} = \boldsymbol{0} \iff x = e_H(b)$ *for some* $b \in B^m$

Proof: $x * \mathbf{H} = \mathbf{0} \Rightarrow x = e_H(b)$ for some $b \in B^m$.

- Suppose that $x * \mathbf{H} = \mathbf{0}$

$$
\begin{aligned}
& x * \mathbf{H} \\
= \; & \begin{bmatrix} y_1 & y_2 & \dots & y_m & x_1 & x_2 & \dots & x_r \end{bmatrix} * \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1r} \\ h_{21} & h_{22} & \dots & h_{2r} \\ \dots & \dots & & \dots \\ h_{m1} & h_{m2} & \dots & h_{mr} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix} \\
= \; & \begin{bmatrix} y_1 \cdot h_{11} + y_2 \cdot h_{21} + \cdots + y_m \cdot h_{m1} + x_1 & y_1 \cdot h_{12} + y_2 \cdot h_{22} + \cdots + y_m \cdot h_{m2} + x_2 \end{bmatrix} \\
= \; & \begin{bmatrix} 0 & 0 & \dots & 0 \end{bmatrix}
\end{aligned}
$$

Proof: $x * \mathbf{H} = \mathbf{0} \Rightarrow x = e_H(b)$ for some $b \in B^m$.

- Last equation

$$\begin{aligned} y_1 \cdot h_{11} + y_2 \cdot h_{21} + \cdots + y_m \cdot h_{m1} + x_1 &= 0 \\ y_1 \cdot h_{12} + y_2 \cdot h_{22} + \cdots + y_m \cdot h_{m2} + x_2 &= 0 \\ \cdots \\ y_1 \cdot h_{1r} + y_2 \cdot h_{2r} + \cdots + y_m \cdot h_{mr} + x_r &= 0 \end{aligned}$$

Proof: $x * \mathbf{H} = \mathbf{0} \Rightarrow x = e_H(b)$ for some $b \in B^m$.

- Note that $x_i + x_i = 0$. So add x_i to i^{th} row and get

$$\begin{aligned}
y_1 \cdot h_{11} + y_2 \cdot h_{21} + \cdots + y_m \cdot h_{m1} &= x_1 \\
y_1 \cdot h_{12} + y_2 \cdot h_{22} + \cdots + y_m \cdot h_{m2} &= x_2 \\
&\cdots \\
y_1 \cdot h_{1r} + y_2 \cdot h_{2r} + \cdots + y_m \cdot h_{mr} &= x_r
\end{aligned}$$

Proof: $x * \mathbf{H} = \mathbf{0} \Rightarrow x = e_H(b)$ for some $b \in B^m$.

- Letting $b_1 = y_1, b_2 = y_2, \ldots, b_m = y_m$, we see that $x_1, x_2, \ldots, x_r$ satisfy the equations in (1).

$$\begin{bmatrix} x_1 & x_2 & \ldots & x_r \end{bmatrix} = \begin{bmatrix} y_1 & y_2 & \ldots & y_m \end{bmatrix} * \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1r} \\ h_{21} & h_{22} & \ldots & h_{2r} \\ \ldots & \ldots & & \ldots \\ h_{m1} & h_{m2} & \ldots & h_{mr} \end{bmatrix}$$

- Thus $b = b_1 b_2 \ldots b_m$ and $x = e_H(b)$

Proof: $x * \mathbf{H} = \mathbf{0} \Leftarrow x = e_H(b)$ for some $b \in B^m$.

- Conversely if $x = e_H(b)$

$$x = e_H(b_1 b_2 \ldots b_m) = \begin{bmatrix} b_1 & b_2 & \ldots & b_m & x_1 & x_2 & \ldots & x_r \end{bmatrix}$$

$$\begin{bmatrix} x_1 & x_2 & \ldots & x_r \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & \ldots & b_m \end{bmatrix} * \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1r} \\ h_{21} & h_{22} & \ldots & h_{2r} \\ \ldots & \ldots & & \ldots \\ h_{m1} & h_{m2} & \ldots & h_{mr} \end{bmatrix}$$

❀

Proof: $x * \mathbf{H} = \mathbf{0} \Leftarrow x = e_H(b)$ for some $b \in B^m$.

$$\begin{bmatrix} x_1 & x_2 & \dots & x_r \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & \dots & b_m \end{bmatrix} * \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1r} \\ h_{21} & h_{22} & \dots & h_{2r} \\ \dots & \dots & & \dots \\ h_{m1} & h_{m2} & \dots & h_{mr} \end{bmatrix}$$

$$\begin{aligned} x_1 &= b_1 \cdot h_{11} + b_2 \cdot h_{21} + \cdots + b_m \cdot h_{m1} \\ x_2 &= b_1 \cdot h_{12} + b_2 \cdot h_{22} + \cdots + b_m \cdot h_{m2} \\ (&\Leftrightarrow b_1 \cdot h_{12} + b_2 \cdot h_{22} + \cdots + b_m \cdot h_{m2} + x_2 = 0) \\ \dots & \\ x_r &= b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \cdots + b_m \cdot h_{mr} \end{aligned}$$

Proof: $x * \mathbf{H} = \mathbf{0} \Leftarrow x = e_H(b)$ for some $b \in B^m$.

$$x * \mathbf{H}$$

$$= \begin{bmatrix} b_1 & b_2 & \dots & b_m & x_1 & x_2 & \dots & x_r \end{bmatrix} * \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1r} \\ h_{21} & h_{22} & \dots & h_{2r} \\ \dots & \dots & & \dots \\ h_{m1} & h_{m2} & \dots & h_{mr} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= [b_1 \cdot h_{11} + b_2 \cdot h_{21} + \cdots + b_m \cdot h_{m1} + x_1 \quad b_1 \cdot h_{12} + b_2 \cdot h_{22} + \cdots + b_m \cdot h_{m2} + x_2$$

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

- which shows $x * \mathbf{H} = \mathbf{0}$

❀

Corollary (2)

- $e_H(B^m) = \{e_H(b) | b \in B^m\}$ *is a subgroup of* B^n

Proof.

- The result follows from the observation that
  - $e_H(B^m) = ker(f_H)$
  - and from Corollary 1.
- Thus e_H is a group code.

Example

- Let $m = 2, n = 5$, and

$$H = \begin{bmatrix} H_{2\times 3} \\ I_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

- Determine the group code $e_H : B^2 \to B^5$.

Solution

$$
\begin{aligned}
e_H(B^m) &= B^m * [I_2 \; H_{2\times 3}] \\
&= \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

A Question

- What does **H** mean?

Homework

- $16, 18, 20, 26@page412$
- 编程作业：给定H(读取文件方式，第一行两个整数m, n，第二行$m \times (n-m)$个0或1，也就是矩阵H的上半部分，下半部单位矩阵自行生成)，计算群码编码函数e_H。
  1. 计算该编码函数能检测到多少位错误
  2. 交互输出字的码字
- 编程作业：针对$(8, 12)$编码e，找出最小距离最大的群码编码函数，输出H及最小距离。