0 1 0 1 1   *send* →   0 1 0 0 1

↑ *transmission error*

Problem: How to detect and correct transmission errors?

Basic scheme of error correction

message		decoded message

encoding ↓   ↑ *decoding*

encoded message	*send* →	received message
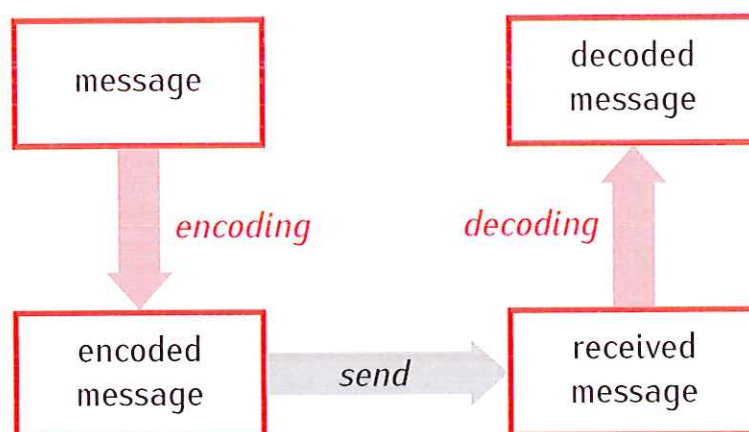
Working assumption for this lecture: We expect at most one transmission error in any message up to 20 bits long.

A simple error correcting code: triple repeat.

message: 1011

encoding: repeat each bit 3 times;

111 000 111 111   ← encoded message

↓ send

transmission error

decoding: 111 000 101 111   ← received message

look at
triples of
bits, the value   1   0   1   1   ← decoded message
that appears at
least 2 times is
the correct value

Problem: The encoded message is 3 times longer than the original message.

Better error correction: Hamming (7,4) code.

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \qquad D = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

encoding matrix   decoding matrix

message: 10111101

Encoding.

1) Split the message into vectors with 4 entries, and multiply each vector by the encoding matrix E.

$$\underbrace{1011}_{\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}} \quad \underbrace{1101}_{\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}}$$

$$E \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 2 \\ 3 \\ 2 \end{bmatrix}, \quad E \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 2 \\ 2 \\ 3 \end{bmatrix}$$

2) Reduce all numbers obtained in step 1 modulo 2. That is, add or subtract from each number a multiple of 2 to get either 0 or 1.

1 0 1 1 2 3 2   1 1 0 1 2 2 3

mod 2 ↓

1 0 1 1 0 1 0   1 1 0 1 0 0 1   ← encoded message

111

Encoded message: 1 0 11 0 1 0 1 1 0 1 0 0 1

↓ send   ↑ ← transmission error

Received message: 1 0 1 1 0 1 0 1 1 1 1 0 0 1

Decoding. Split the received message into vectors with 7 entries, multiply each vector by the decoding matrix D, and reduce modulo 2.

1 0 11 0 1 0 1 1 1 1 0 0 1

$$D \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 2 \end{bmatrix} \xrightarrow{\text{mod } 2} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

the zero vector means no error in this piece of the message

↳ decoded message: 1 0 1 1 0 1 0

$$D \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ 4 \end{bmatrix} \xrightarrow{\text{mod } 2} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

this is the 3rd column of D, which means there is an error in the 3rd bit

↳ decoded message: 1 1 0 1 0 0 1

Decoded message: 1 0 11 1 1 0 1

112

How the Hamming code works:

1) Adding a transmission error means adding a standard basis vector (mod 2):

$$
\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \textcolor{red}{①} \\ 0 \\ 0 \\ 1 \end{bmatrix} \longleftarrow \text{transmission error}
$$

$$
\begin{matrix} S \\ \text{sent} \end{matrix} \quad + \quad \begin{matrix} e_3 \\ \text{error} \end{matrix} \quad = \quad \begin{matrix} r \\ \text{received} \end{matrix}
$$

$$
\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \xrightarrow{\text{mod } 2} \begin{bmatrix} \textcolor{red}{⓪} \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \longleftarrow \text{transmission error}
$$

$$
\begin{matrix} S \\ \text{sent} \end{matrix} \quad + \quad \begin{matrix} e_1 \\ \text{error} \end{matrix} \quad = \quad \begin{matrix} r \\ \text{received} \end{matrix}
$$

2) <u>Check</u>: $D \cdot E = 0$ (mod 2)

↳ matrix with all entries 0

<u>encoding</u>: $s = E \cdot m$

<u>decoding with no error</u>: $D \cdot s = D \cdot (E \cdot m) = \overset{0}{\overline{(DE)}} m = 0$

<u>decoding with error</u>: $r = s + e_i = Em + e_i$

$Dr = D(Em + e_i) = DEm + De_i = 0 + De_i = \boxed{De_i}$

↑ the ith column of D.

113