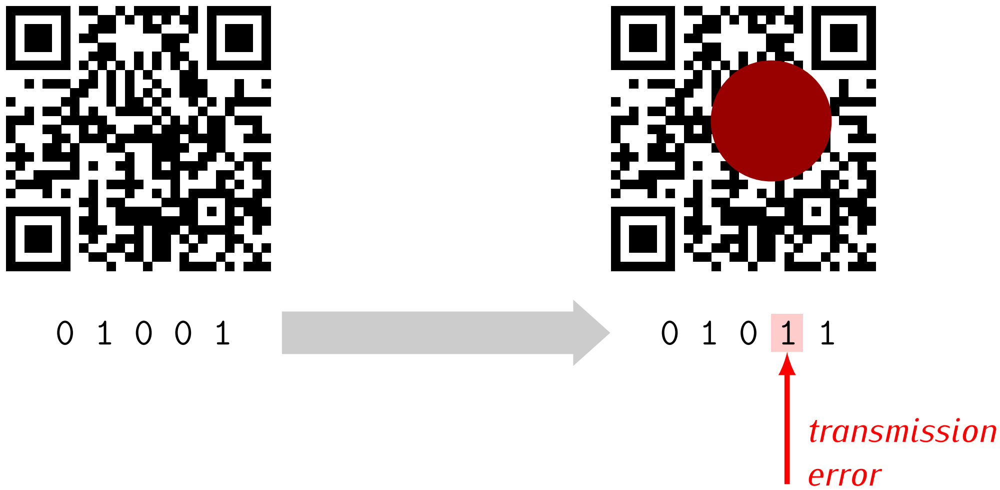
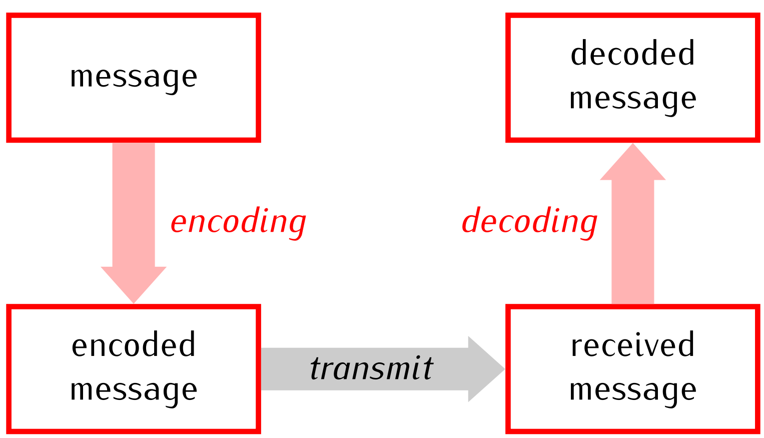


Basic scheme of error correction



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 that appears at least 2 times is the correct value

1 0 1 1 ← decoded message

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.

$$\underbrace{1011}\ \underbrace{1101}$$

$$\downarrow \qquad \downarrow$$

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

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

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.

$$1\ 0\ 1\ 1\ 2\ 3\ 2\ 1\ 1\ 0\ 1\ 2\ 2\ 3$$

$$\Big\downarrow \text{mod } 2$$

$$1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1 \leftarrow \text{encoded message}$$

Encoded message: 1 0 1 1 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.

$$\underbrace{1\,0\,1\,1\,0\,1\,0}\ \underbrace{1\,1\,1\,1\,0\,0\,1}$$

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

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

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

decoded message: $\boxed{1\,0\,1\,1}$ 0 1 0

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

decoded message: $\boxed{1\,1\,0\,1}$ 0 0 1

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

Decoded message: 1 0 1 1 1 1 0 1

How the Hamming code works:

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

$$\underset{\substack{s\\ \text{sent}}}{\begin{bmatrix}1\\1\\0\\1\\0\\0\\1\end{bmatrix}} + \underset{\substack{e_3\\ \text{error}}}{\begin{bmatrix}0\\0\\1\\0\\0\\0\\0\end{bmatrix}} = \underset{\substack{r\\ \text{received}}}{\begin{bmatrix}1\\1\\1\\1\\0\\0\\1\end{bmatrix}} \leftarrow \text{transmission error}$$

$$\underset{\substack{s\\ \text{sent}}}{\begin{bmatrix}1\\1\\0\\1\\0\\0\\1\end{bmatrix}} + \underset{\substack{e_1\\ \text{error}}}{\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\end{bmatrix}} = \underset{\substack{r\\ \text{received}}}{\begin{bmatrix}2\\1\\0\\1\\0\\0\\1\end{bmatrix}} \xrightarrow{\text{mod } 2} \begin{bmatrix}0\\1\\0\\1\\0\\0\\1\end{bmatrix} \leftarrow \text{transmission error}$$

2) Check: $D \cdot E = 0 \pmod 2$

0 ← matrix with all entries 0

encoding: $s = E \cdot m$

decoding with no error: $D \cdot s = D \cdot (E \cdot m) = \overbrace{(DE)}^{0} m = 0$

decoding with error: $r = s + e_i = Em + e_i$

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

↑ the ith column of D.