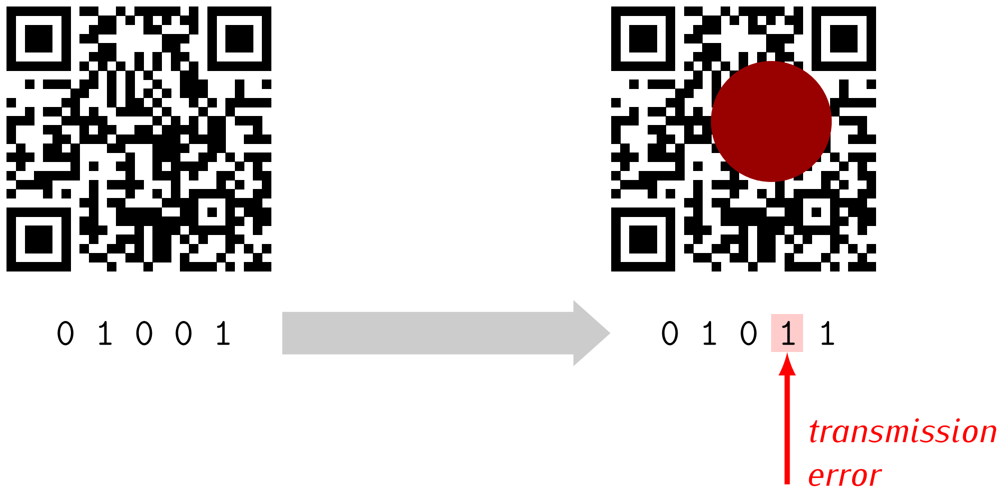
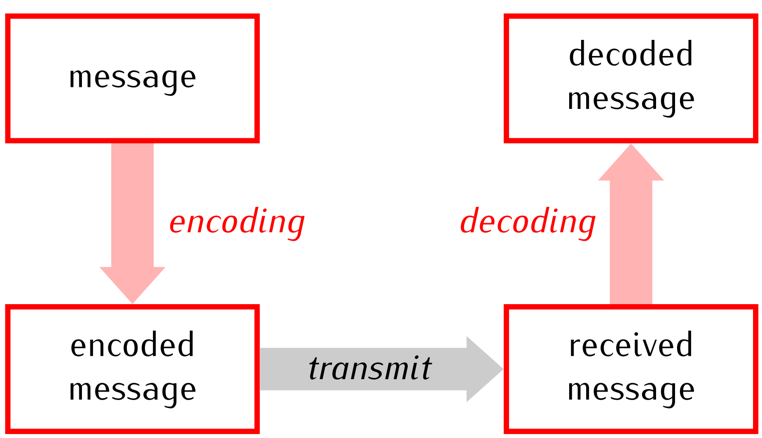


Basic scheme of error correction



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:

1011 $\longrightarrow$ 111 000 111 111 $\longleftarrow$ encoded message

send $\downarrow$

transmission error

decoding: look at triples of bits, the value that repeats at least 2 times is the correct value.

$$\underbrace{111}_{\downarrow\; 1}\ \underbrace{000}_{\downarrow\; 0}\ \underbrace{101}_{\downarrow\; 1}\ \underbrace{111}_{\downarrow\; 1} \longleftarrow \text{received message}$$

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.

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

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

2) Reduce all numbers obtained in step 1 modulo 2. That is, write 0 for each even number and 1 for each odd number.

$$\begin{array}{c} 1\,0\,1\,1\,2\,3\,2 \quad 1\,1\,0\,1\,2\,2\,3 \\ \Big\downarrow {\scriptstyle \text{mod } 2} \\ 1\,0\,1\,1\,0\,1\,0 \quad 1\,1\,0\,1\,0\,0\,1 \end{array} \leftarrow \text{encoded message}$$

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

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.

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

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

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

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 that there is an error in the 3rd bit

Decoded message: 1011 1101

How the Hamming code works:

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

$$\begin{bmatrix}1\\1\\0\\1\\0\\0\\1\end{bmatrix} + \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\\0\\0\\1\end{bmatrix} \leftarrow \text{transmission error}$$

$$\underset{\text{sent}}{s} + \underset{\text{error}}{e_3} = \underset{\text{received}}{r}$$

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

$$\underset{\text{sent}}{s} + \underset{\text{error}}{e_1} = \underset{\text{received}}{r}$$

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

matrix with all entries 0

encoding: $s = E \cdot m$

decoding with no error: $D \cdot s = D(Em) = \underbrace{(DE)}_{=0}m = 0$

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

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

the i^{th} column of D