We can do better, but the next part will not work with an arbitrary invertible matrix A. It will work though e.g. if all entries of A and A^{-1} are integers.

5) Reduce all numbers obtained in step 4 modulo 27. That is, add or subtract from each number a multiple of 27 to get a number between 0 and 26.

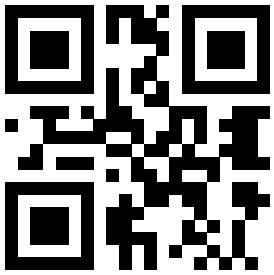
6) Replace numbers by letters.

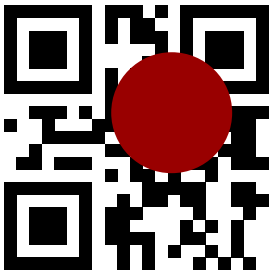
Decryption.

1) Replace letters by numbers, split into vectors, and multiply each vector by A^{-1}

2) Write the new vectors as a sequence of numbers, reduce each number modulo 27.

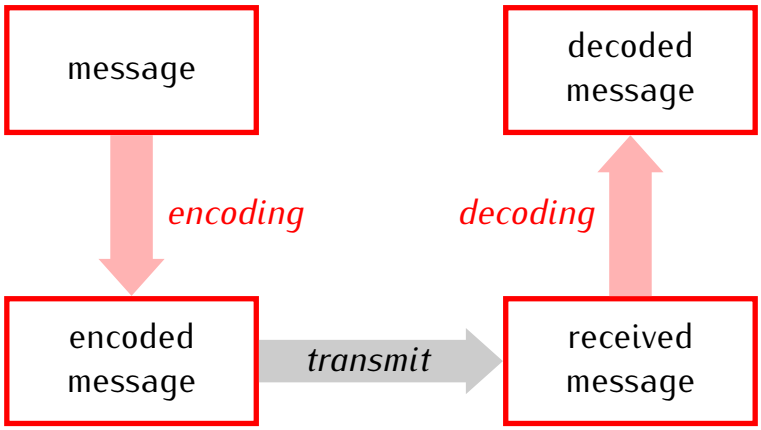
3) Replace numbers by letters





Problem: How to detect and correct transmission errors?

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

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

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

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

encoding matrix

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

decoding matrix

message: 10111101

Encoding.

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

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.

Encoded message:

Received message:

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

Decoded message: