Hamming Distance Between Two Strings in A Binary Code of Equal Length

---- the number of positions in which the strings differ.

Example: u = 1010110
v = 1000110

The Hamming distance between code words u and v is 1.

Example: u = 1000110
v = 0111001

The Hamming distance between code words u and v is 7.

Nearest-Neighbor Decoding

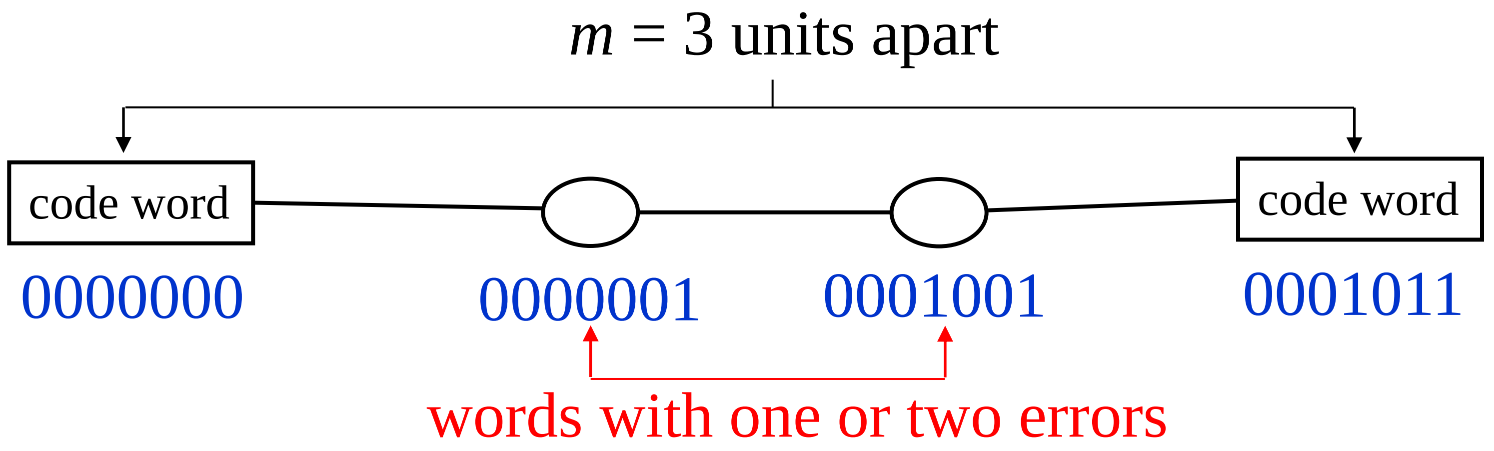
Method decodes a received message as the code word that agrees with the message in the most positions.

1. Compare the string with an error (call it u) to all other strings of the same length.
2. The string the least distance from u is taken as the true message.
3. If there is more than one possible answer, then the error cannot be corrected.

Error Detection

For a given set of block codes, let m be the minimum distance between two different codewords.

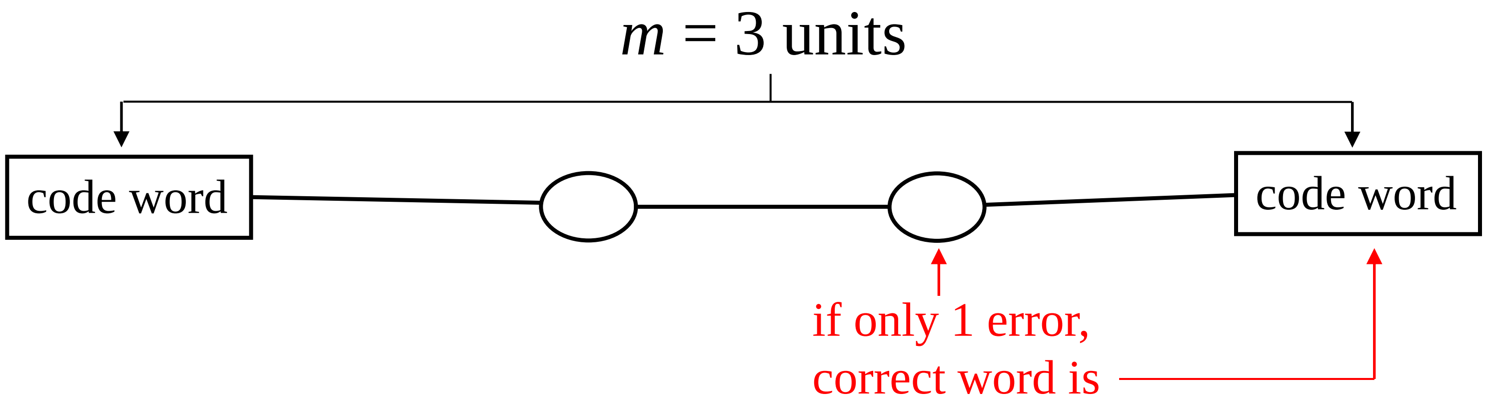
Error detection: the code can detect any $m - 1$ or fewer errors. For example:

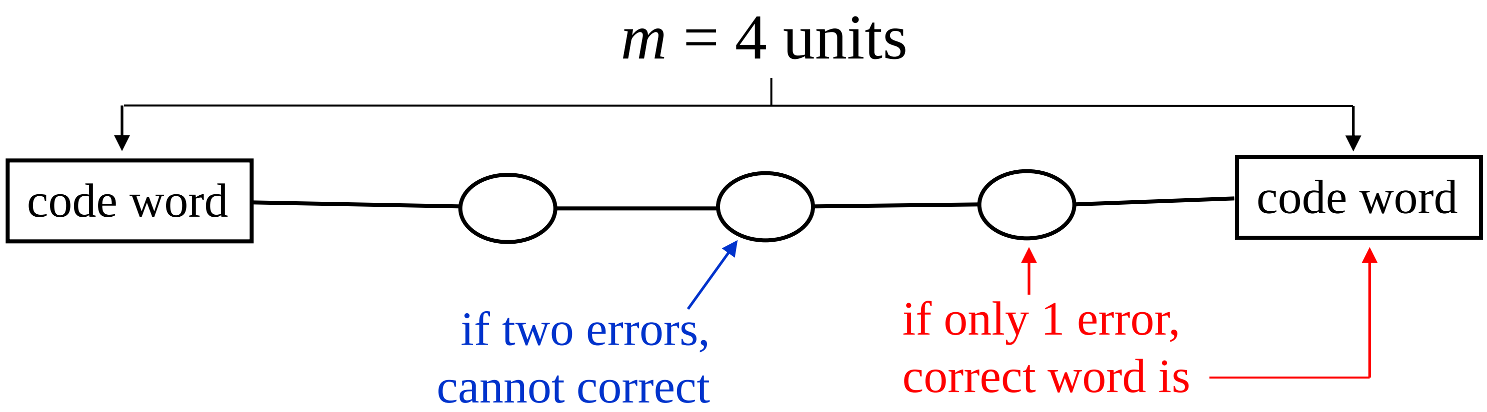


Error Correction

Again, let m be the minimum distance between two different codewords. Then

- If m is odd, the code will correct any $(m - 1)/2$ or fewer errors;
- If m is even, the code will correct any $(m - 2)/2$ or fewer errors;





Parity check bits are sums mod 2

The check bits are the sum mod 2 of the message bits:

010000100   010000010   010101001

$0+1+0+0+0+0+1+0 = 0 \pmod 2$

$0+1+0+0+0+0+0+1 = 0 \pmod 2$

$0+1+0+1+0+1+0+0 = 1 \pmod 2$

Example for a (3,4) Block Code

W_k is the set of binary strings of length k.

Consider the three-digit messages, $m_1m_2m_3$:

$$W_3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

Adding a single parity check digit produces a (3,4) block code $m_1m_2m_3c_1$ where $c_1 = m_1 + m_2 + m_3 \pmod 2$.

For example, the message 010 is encoded as 0101.

The resulting set of codewords is

$$C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}.$$

Note that minimum Hamming distance between any two codewords is 2. Any single error results in a string not included in the set of codewords, C.

Adding More Check Bits

In the preceding (3,4) block code, we can detect that there is an error in the string 0100 since it is not a codeword from

C = {0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111}.

Even if there is only one error, we cannot determine which codeword was intended. (0000, 0101, 0110, or 1100?)

We can devise a code capable of correcting errors by adding more check bits, which are determined by adding certain combinations of the message bits using parity check equations, just as before. For example:

$$c_1 = m_1 + m_2$$
$$c_2 = m_2 + m_3$$
$$c_3 = m_1 + m_3$$

Remember, this is mod 2 addition!

Example of a (3,6) Block Code

Suppose we want to find the check bits for the message 010 in the previous example. Then we set $m_1 = 0$, $m_2 = 1$, $m_3 = 0$ and use the parity check equations:

$$c_1 = m_1 + m_2 = 0 + 1 = 1$$
$$c_2 = m_2 + m_3 = 1 + 0 = 1$$
$$c_3 = m_1 + m_3 = 0 + 0 = 0$$

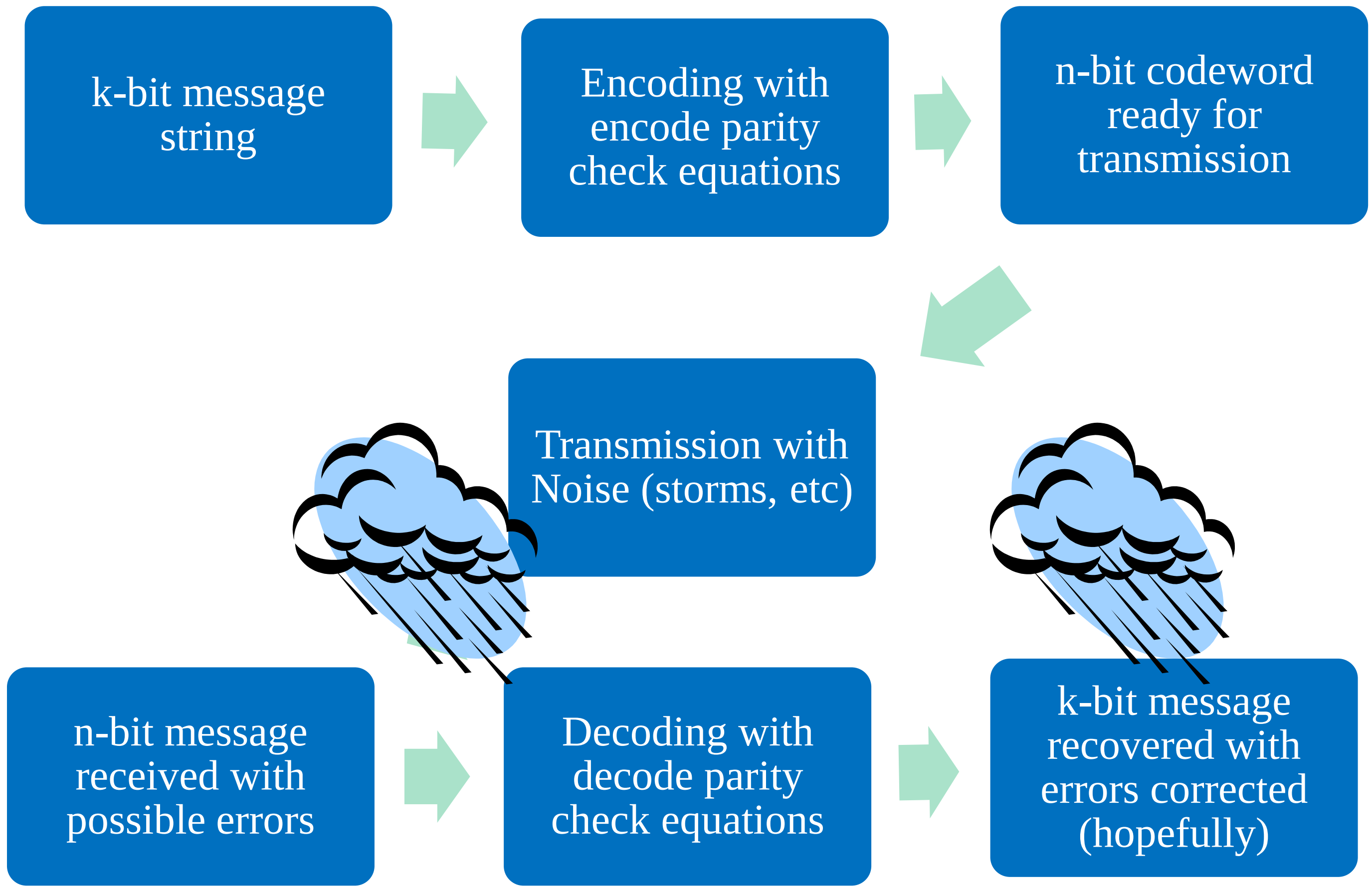
So the message 010 becomes encoded as 010110.

The complete set of codewords is

C(3,6) = {000000, 001011, 010110, 011101,
100101, 101110, 110011, 111000}

and the minimum Hamming distance between codewords is 3.

Encoding and Decoding (*k*,*n*) Block Codes



From Parity Check Sums to Encoding Matrices

Remembering the various parity check equations can be difficult. A compact representation of these parity check equations is to put them in the form of a **matrix.** A matrix is simply a rectangular array of numbers with **rows** and **columns** of numbers. Below are some examples of matrices.

$$\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Size of Matrices

The size of a matrix is determined by its number of rows and columns. A matrix with *k* rows and *n* columns is called "*k* by *n*" which is written "$k \times n$".

3×2 matrix

$$\begin{array}{r} 1^{\text{st}}\text{ row} \\ \\ 3^{\text{rd}}\text{ row} \end{array} \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 3 & 0 \end{bmatrix}$$

3×6 matrix

$$\begin{array}{c} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \\ \begin{array}{cccccc} & 2^{\text{nd}}\text{ column} & & & 5^{\text{th}}\text{ column} & \end{array} \end{array}$$

Generator Matrix for (3,6) Block Code

This 3×6 matrix that will help us generate the codewords that are transmitted using the parity check equations in our example. The 3 rows of the matrix will correspond to the 3 message bits. The 6 columns will correspond to the 6 bits in the transmitted codeword.

$$\begin{array}{c c}
\begin{array}{c} m_1 \\ m_2 \\ m_3 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \\
 & \begin{array}{cccccc} m_1 & m_2 & m_3 & c_1 & c_2 & c_3 \end{array}
\end{array}$$

Using the Generator Matrix to find the Codeword

$$m_1 + m_3 = c_3$$

$$\begin{array}{cc} \begin{array}{c} m_1 \\ m_2 \\ m_3 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \\ & \begin{array}{cccccc} m_1 & m_2 & m_3 & c_1 & c_2 & c_3 \end{array} \end{array}$$

The 1's in each column in the matrix tell you which message bits to add together to get the codeword bit for that column.

Example using the Generator Matrix

Find the transmitted codeword for the message 101.

$$\begin{array}{c} 1 \\ 0 \\ 1 \end{array}\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\begin{array}{ccccccc} & 1 & 0 & 0 & 1 & 0 & 1 \\ + & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline & 1 & 0 & 1 & 1 & 1 & 0 \end{array}$$

Thus, the transmitted codeword is 101110.

Find the Generator Matrix Given Parity Check Equations

Construct the generator matrix of a (3, 5) block code with the following parity check equations:

$$c_1 = m_2 + m_3 \qquad c_2 = m_1 + m_3$$

$$\begin{array}{c} \\ m_1 \\ m_2 \\ m_3 \\ \\ \end{array} \begin{array}{c} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \\ \begin{array}{ccccc} m_1 & m_2 & m_3 & c_1 & c_2 \end{array} \end{array}$$

Producing a Linear Code with a Generator Matrix

We can use a generator matrix to create a collection of codewords that we call a "linear code". To produce a linear code, we start with all binary strings of a certain length. We will denote all strings of length k as W_k.

$$W_1 = \{0, 1\}$$

$$W_2 = \{00, 01, 10, 11\}$$

$$W_3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

The set W_k **will have** $\mathbf{2^k}$ **elements**.

(3,5) Linear Code generated by previous matrix

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

$$c_1 = m_2 + m_3$$
$$c_2 = m_1 + m_3$$

$$W_3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

$$C(3,5) = \{00000, 00111, 01010, 01101,$$
$$10001, 10110, 11011, 11100\}$$