The Hamming [7,4,3] Code

Encode: $x_0x_1x_2x_3 \to p_0p_1x_0p_2x_1x_2x_3$, where

$$p_0 = x_0 \oplus x_1 \oplus x_3,$$
$$p_1 = x_0 \oplus x_2 \oplus x_3,$$
$$p_2 = x_1 \oplus x_2 \oplus x_3.$$

The encoded block satisfies

$$p_0 \oplus x_0 \oplus x_1 \oplus x_3 = 0,$$
$$p_1 \oplus x_0 \oplus x_2 \oplus x_3 = 0,$$
$$p_2 \oplus x_1 \oplus x_2 \oplus x_3 = 0.$$

Decode: Say we receive $p_0'p_1'x_0'p_2'x_1'x_2'x_3'$. ($p_i' = p_i$, $x_j' = x_j$ if no errors)

Let

$$c_0 = p_0' \oplus x_0' \oplus x_1' \oplus x_3',$$
$$c_1 = p_1' \oplus x_0' \oplus x_2' \oplus x_3',$$
$$c_2 = p_2' \oplus x_1' \oplus x_2' \oplus x_3'.$$

Suppose at most one error has occurred in transmission.

Position of error	**Error**	c_0	c_1	c_2	$(c_2c_1c_0)_{10}$
--	none	0	0	0	0
1	$p_0' \neq p_0$	1	0	0	1
2	$p_1' \neq p_1$	0	1	0	2
3	$x_0' \neq x_0$	1	1	0	3
4	$p_2' \neq p_2$	0	0	1	4
5	$x_1' \neq x_1$	1	0	1	5
6	$x_2' \neq x_2$	0	1	1	6
7	$x_3' \neq x_3$	1	1	1	7

So $(c_2c_1c_0)_{10}$ tells us the position of the error (0 = no error).

We decode as follows:

$(c_2c_1c_0)_{10}$	Decode to
3	$\overline{x_0'}x_1'x_2'x_3'$
5	$x_0'\overline{x_1'}x_2'x_3'$
6	$x_0'x_1'\overline{x_2'}x_3'$
7	$x_0'x_1'x_2'\overline{x_3'}$
other values	$x_0'x_1'x_2'x_3'$

We can also encode like this: $(x_0x_1x_2x_3) \to (x_0x_1x_2x_3)\,\mathbf{G}$, where

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

G is called the <u>generator matrix</u> for the code.

Another useful matrix is the parity-check matrix (often denoted **H**).

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The rows of H are orthogonal to the rows of **G**.

$$(p_0'p_1'x_0'p_2'x_1'x_2'x_3')\,\mathbf{H}^{\mathrm{T}} = (p_2' \oplus x_1' \oplus x_2' \oplus x_3',\ p_1' \oplus x_0' \oplus x_2' \oplus x_3',\ p_0' \oplus x_0' \oplus x_1' \oplus x_3') = (c_2, c_1, c_0)$$