Codebook for the Hamming code in Ex. 1

d_1	d_2	d_3	d_4	x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	0	1	0	1	0	1
0	0	1	0	0	0	1	0	1	1	0
0	0	1	1	1	0	0	0	0	1	1
0	1	0	0	1	0	0	1	1	0	0
0	1	0	1	0	0	1	1	0	0	1
0	1	1	0	1	0	1	1	0	1	0
0	1	1	1	0	0	0	1	1	1	1
1	0	0	0	1	1	1	0	0	0	0
1	0	0	1	0	1	0	0	1	0	1
1	0	1	0	1	1	0	0	1	1	0
1	0	1	1	0	1	1	0	0	1	1
1	1	0	0	0	1	1	1	1	0	0
1	1	0	1	1	1	0	1	0	0	1
1	1	1	0	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1	1	1	1

Note that

- Each bit of the codeword for linear code is either
  - the same as one of the message bits $x_2 = d_1$
    - Here, the second bit (x_2) of the codeword is the same as the first bit (b_1) of the message
  - the sum of some bits from the message $x_5 = d_2 \oplus d_3 \oplus d_4$
    - Here, the first bit (x_1) of the codeword is the sum of the first, second and fourth bits of the message.
- So, each column in the codebook should also satisfy the above structure (relationship).

Codebook for the Hamming code in Ex. 1

$d_2 \oplus d_3 \oplus d_4$

	d				x_1		x_3	**x**	x_5		
	0	0	0	0	0	0	0	0	0	0	0
d_4	0	0	0	1	1	0	1	0	1	0	1
d_3	0	0	1	0	0	0	1	0	1	1	0
	0	0	1	1	1	0	0	0	0	1	1
d_2	0	1	0	0	1	0	0	1	1	0	0
	0	1	0	1	0	0	1	1	0	0	1
	0	1	1	0	1	0	1	1	0	1	0
	0	1	1	1	0	0	0	1	1	1	1
d_1	1	0	0	0	1	1	1	0	0	0	0
	1	0	0	1	0	1	0	0	1	0	1
	1	0	1	0	1	1	0	0	1	1	0
	1	0	1	1	0	1	1	0	0	1	1
	1	1	0	0	0	1	1	1	1	0	0
	1	1	0	1	1	1	0	1	0	0	1
	1	1	1	0	0	1	0	1	0	1	0
	1	1	1	1	1	1	1	1	1	1	1

- One can "read" the structure (relationship) from the codebook.
- From $x_j = \sum_{i=1}^{k} d_i g_{ij}$, when we look at the message block with a single 1 at position i, then
  - the value of x_j in the corresponding codeword gives g_{ij}
  - $x_1 = d_1 \oplus d_2 \oplus d_4$
  - $x_3 = d_1 \oplus d_3 \oplus d_4$

Codebook for the Hamming code in Ex. 1

	d				x							
	0	0	0	0	0	0	0	0	0	0	0	
d_4	0	0	0	1	1	0	1	0	1	0	1	$\mathbf{g}^{(4)}$
d_3	0	0	1	0	0	0	1	0	1	1	0	$\mathbf{g}^{(3)}$
	0	0	1	1	1	0	0	0	0	1	1	
d_2	0	1	0	0	1	0	0	1	1	0	0	$\mathbf{g}^{(2)}$
	0	1	0	1	0	0	1	1	0	0	1	
	0	1	1	0	1	0	1	1	0	1	0	
	0	1	1	1	0	0	0	1	1	1	1	
d_1	1	0	0	0	1	1	1	0	0	0	0	$\mathbf{g}^{(1)}$
	1	0	0	1	0	1	0	0	1	0	1	
	1	0	1	0	1	1	0	0	1	1	0	
	1	0	1	1	0	1	1	0	0	1	1	
	1	1	0	0	0	1	1	1	1	0	0	
	1	1	0	1	1	1	0	1	0	0	1	
	1	1	1	0	0	1	0	1	0	1	0	
	1	1	1	1	1	1	1	1	1	1	1	

- One can also "read" $\mathbf{G}$ from the codebook.
- From $\underline{\mathbf{x}} = \underline{\mathbf{b}}\mathbf{G} = \sum_{j=1}^{k} b_j \underline{\mathbf{g}}^{(j)}$, when we look at the message block with a single 1 at position i, then the corresponding codeword is the same as $\underline{\mathbf{g}}^{(j)}$.

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

Checking linearity of a code

	d				x						
	0	0	0	0	0	0	0	0	0	0	0
d_4	0	0	0	1	1	0	1	0	1	0	1
d_3	0	0	1	0	0	0	1	0	1	1	0
	0	0	1	1	1	0	0	0	0	1	1
d_2	0	1	0	0	1	0	0	1	1	0	0
	0	1	0	1	0	0	1	1	0	0	1
	0	1	1	0	1	0	1	1	0	1	0
	0	1	1	1	0	0	0	1	1	1	1
d_1	1	0	0	0	1	1	1	0	0	0	0
	1	0	0	1	0	1	0	0	1	0	1
	1	0	1	0	1	1	0	0	1	1	0
	1	0	1	1	0	1	1	0	0	1	1
	1	1	0	0	0	1	1	1	1	0	0
	1	1	0	1	1	1	0	1	0	0	1
	1	1	1	0	0	1	0	1	0	1	0
	1	1	1	1	1	1	1	1	1	1	1

- Another technique for checking linearity of a code when the codebook is provided is to look at each column of the codeword part.
- Write down the equation by reading the structure from appropriate rows discussed earlier.
  - For example, here, we read $x_1 = d_1 \oplus d_2 \oplus d_4$.
- Then, we add the corresponding columns of the message part and check whether the sum is the same as the corresponding codeword column.
- So, we need to check n summations.
  - Direct checking discussed previously consider $\binom{n-1}{2}$ summations.

$\binom{16}{2} = \frac{\cancel{16}^{8} \times 15}{\cancel{2}} = 120$ pairs

$\binom{15}{2} = \frac{15 \times \cancel{14}^{7}}{\cancel{2}} = 105$ pairs

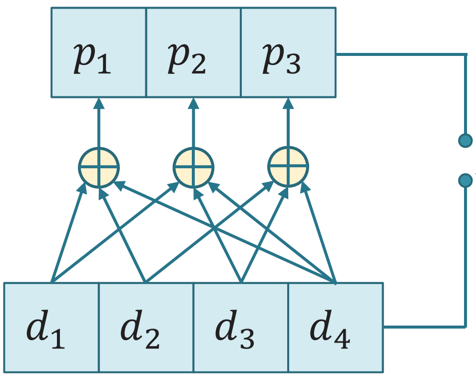
Checking linearity of a code

	d_1	d_2	$\underline{\mathbf{d}}$	d_4	$\underline{\mathbf{x}}$							
	0	0	0	0	0	0	0	0	0	0	0	
d_4	0	0	0	1	$\boxed{1}$	0	1	0	1	0	1	$\underline{\mathbf{g}}^{(4)}$
d_3	0	0	1	0	$\boxed{0}$	0	1	0	1	1	0	$\underline{\mathbf{g}}^{(3)}$
	0	0	1	1	1	0	0	0	0	1	1	
d_2	0	1	0	0	$\boxed{1}$	0	0	1	1	0	0	$\underline{\mathbf{g}}^{(2)}$
	0	1	0	1	0	0	1	1	0	0	1	
	0	1	1	0	1	0	1	1	0	1	0	
	0	1	1	1	0	0	0	1	1	1	1	
d_1	1	0	0	0	$\boxed{1}$	1	1	0	0	0	0	$\underline{\mathbf{g}}^{(1)}$
	1	0	0	1	0	1	0	0	1	0	1	
	1	0	1	0	1	1	0	0	1	1	0	
	1	0	1	1	0	1	1	0	0	1	1	
	1	1	0	0	1	1	1	1	1	0	0	
	1	1	0	1	1	1	0	1	0	0	1	
	1	1	1	0	0	1	0	1	0	1	0	
	1	1	1	1	1	1	1	1	1	1	1	

- Here is an example of non-linear code.
- Again, we read $x_1 = d_1 \oplus d_2 \oplus d_4$.
- We add the message columns corresponding to d_1, d_2, d_4,
  - We see that the first bit of the 13th codeword does not conform with the structure above.
  - The corresponding message is 1100.
  - We see that $\mathbf{g}^{(1)}$ and $\mathbf{g}^{(2)}$ are codewords but $\mathbf{g}^{(1)} \oplus \mathbf{g}^{(2)} =$ 0111100 is not one of the codewords.

Implementation

- Linear block codes are typically implemented with modulo-2 adders tied to the appropriate stages of a shift register.



$\underline{\mathbf{x}} = [p_1 \quad d_1 \quad p_2 \quad d_2 \quad p_3 \quad d_3 \quad d_4]$

where

$$p_1 = d_1 \oplus d_2 \oplus d_4$$
$$p_2 = d_1 \oplus d_3 \oplus d_4$$
$$p_3 = d_2 \oplus d_3 \oplus d_4$$