

## Hamming Codes

A Hamming code word is generated by multiplying the data bits by a generator matrix  $G$  using [modulo-2 arithmetic](#). This multiplication's result is called the code word vector  $(c_1, c_2, c_3, \dots, c_n)$ , consisting of the original data bits and the calculated parity bits.

An example of Hamming (7,4) code generator matrix:

$$G = [I \mid A]$$

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

$$2^4 = 16 \text{ codewords}$$

$$\begin{matrix} \downarrow \\ [0 & 1 & 0 & 1] \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} = [0 & 1 & 0 & 1 & 1 & 0 & 1]$$

Codewords have Hamming distance 3

# Hamming Codes

16 codewords with 7 bits

Any codeword has a different codeword at Hamming distance 3 ( $d_{min}=3$ )

It is possible to show that  $d_{min}$  is equal to the minimum Hamming weight (i.e., the number of non zero bits) of the codewords

0	0	0	0	0	0	0	Minimum weight=3
0	0	0	1	1	1	0	←
0	0	1	0	1	0	1	weight=4
0	0	1	1	0	1	1	←
0	1	0	0	0	1	1	
0	1	0	1	1	0	1	
0	1	1	0	1	1	0	
0	1	1	1	0	0	0	
1	0	0	0	1	1	1	
1	0	0	1	0	0	1	$d_{min} = 3$
1	0	1	0	0	1	0	←
1	0	1	1	1	0	0	←
1	1	0	0	1	0	0	
1	1	0	1	0	1	0	
1	1	1	0	0	0	1	
1	1	1	1	1	1	1	

## Hamming Codes

Codes have minimum distance  $d_{\min} = 3$

They can correct up to  $t=1$  error by decoding the received bits with the closest codeword (in Hamming distance)

$$N = 7, \quad t = 1$$

$$P_e(\text{block}) = \sum_{k=t+1}^N \binom{N}{k} p^k (1-p)^{N-k}$$

## BCH (Bose, Chaudhuri, Hocquenghem) Codes

Binary BCH codes  $(n,k)$  have parameters

$$-n=2^m-1$$

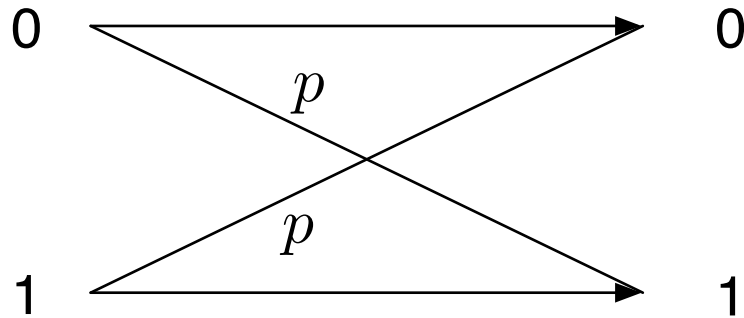
$$-n-k \leq mt \text{ with } m \geq 3, t \geq 1$$

$$-d_{\min}=2t+1$$

*Example:  $n=255, k=187, t=9$  ( $m=8$ ) define a BCH code mapping 187 bits into 255 bits, with an error correcting capability of 9 bits*

- Reed Solomon codes are non binary codes. CD (Sony & Philips, 1980) use a RS(28,24) on GF( $2^8$ ),  $t=2$  symbol (byte) correcting code (24·8=192 bits are mapped into 28·8=224 bits). Symbols are then interleaved so that consecutive symbol errors correspond to different codewords  
(Cross-Interleaved Reed-Solomon Coding, or CIRC)

## Binary Symmetric Channel - Capacità di canale



$$p = P[1|0] = P[0|1]$$

$$P[1|0] \triangleq \frac{P[1,0]}{P[0]}$$

$$P_e = p = P[1,0] + P[0,1] = P[1|0]P[0] + P[0|1]P[1]$$

$$C = 1 - H(p)$$

$$H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$$

$\frac{k}{n} < C \rightarrow$  Trasmissione arbitrariamente affidabile

$k, n$  grandi