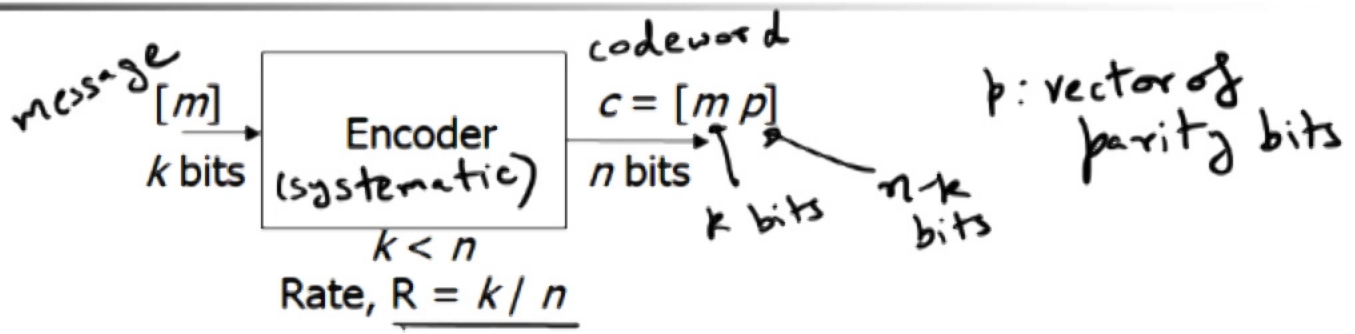
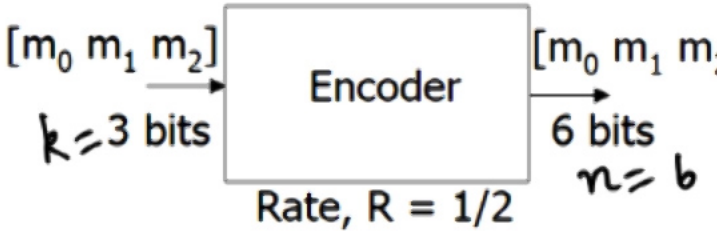
Summary

- Error-correcting codes provide significant coding gains
  - Coding gain has to be calculated using the BER vs. E_b/N_0 plot
  - Longer codes provide better coding gains
  - Need to find good codes
  - Good decoders are important
- Efficient implementation of encoding, error detection and error correction are most important in practice

Basics of linear codes: Encoder



Encoder: forms codeword c by adding $n - k$ parity bits p to the message m



(6,3) code

$p_0 = m_0 + m_1 \pmod 2$
$p_1 = m_1 + m_2 \pmod 2$
$p_2 = m_0 + m_2 \pmod 2$

XORs of a subset of message bits

(binary XOR) mod 2 addition

inputs		output
0	0	0
0	1	1
1	0	1
1	1	0

Matrix description

- All operations are mod 2. Note -1=+1.

$$[p_0 \quad p_1 \quad p_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$m_0+m_1 \quad m_1+m_2 \quad m_0+m_2$

identity

identity I_3

parity part P

Generator matrix

$$[m_0 \quad m_1 \quad m_2 \quad p_0 \quad p_1 \quad p_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

codeword c = message m × Generator matrix

$G = [I \; P]$

Parity-check matrix

$H = [P^T \; I]$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ p_0 \\ p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

P^T I_3 c^T

$m_0+m_1+p_0=0$

$p_0=m_0+m_1$

$$Hc^T = 0 \pmod 2$$

In general...

- Code: Set of codewords
- Generator matrix of a linear code
  - k x n generator matrix G (rank k)
    - Systematic form $G = [I_k \; P]$
  - Message m encoded as $c = m\,G$
    - If G is systematic, $c = [m \; p]$
- Parity-check matrix for same linear code
  - $n - k$ x n parity-check matrix H (rank n-k)
    - Systematic form $H = [P^T \; I_{n-k}]$
    - Codeword c satisfies $H\,c^T = 0$

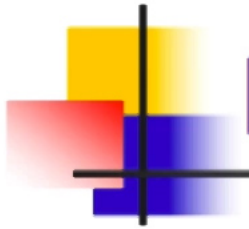
(n,k) code

k message bits → n codeword bits

# of codewords $= 2^k$

P: $k \times n-k$ matrix

$G\,H^T$ = all-zeros



Linear Codes: Vector space view

- Notation: (n, k) linear code
  - Message length = k ; Codeword length = n
- Forms a k-dimensional vector subspace of the n-dimensional binary vector space
  - mod-2 sum of two codewords is another codeword
- Rows of G : Basis for the codespace
  - $c = m\,G$
- Rows of H : Basis for dual of codespace
  - $H\,c^{\mathsf{T}} = 0$
  - Vector x is a codeword iff $H\,x^{T} = 0$

Examples

- (3,1) Repetition Code = {000, 111}

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

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

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

Examples

- (3,1) Repetition Code = {000, 111}

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

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

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

Minimum Distance

- Hamming distance between two binary vectors is the number of places where they are different.
  - dist(000, 111) = 3
  - dist(1101,0110) = 3

- Minimum distance of a code: The minimum Hamming distance between any two codewords
  - d_{min} of (3,1) repetition code = 3
  - d_{min} of (5,1) repetition code = 5
  - d_{min} of (6,3) example code = 3 (How?)

- (n,k,d) – code:
  - Block-length = n, Dimension = k, d_{min} = d

Examples

- (3,1) Repetition Code = {000, 111}

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

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

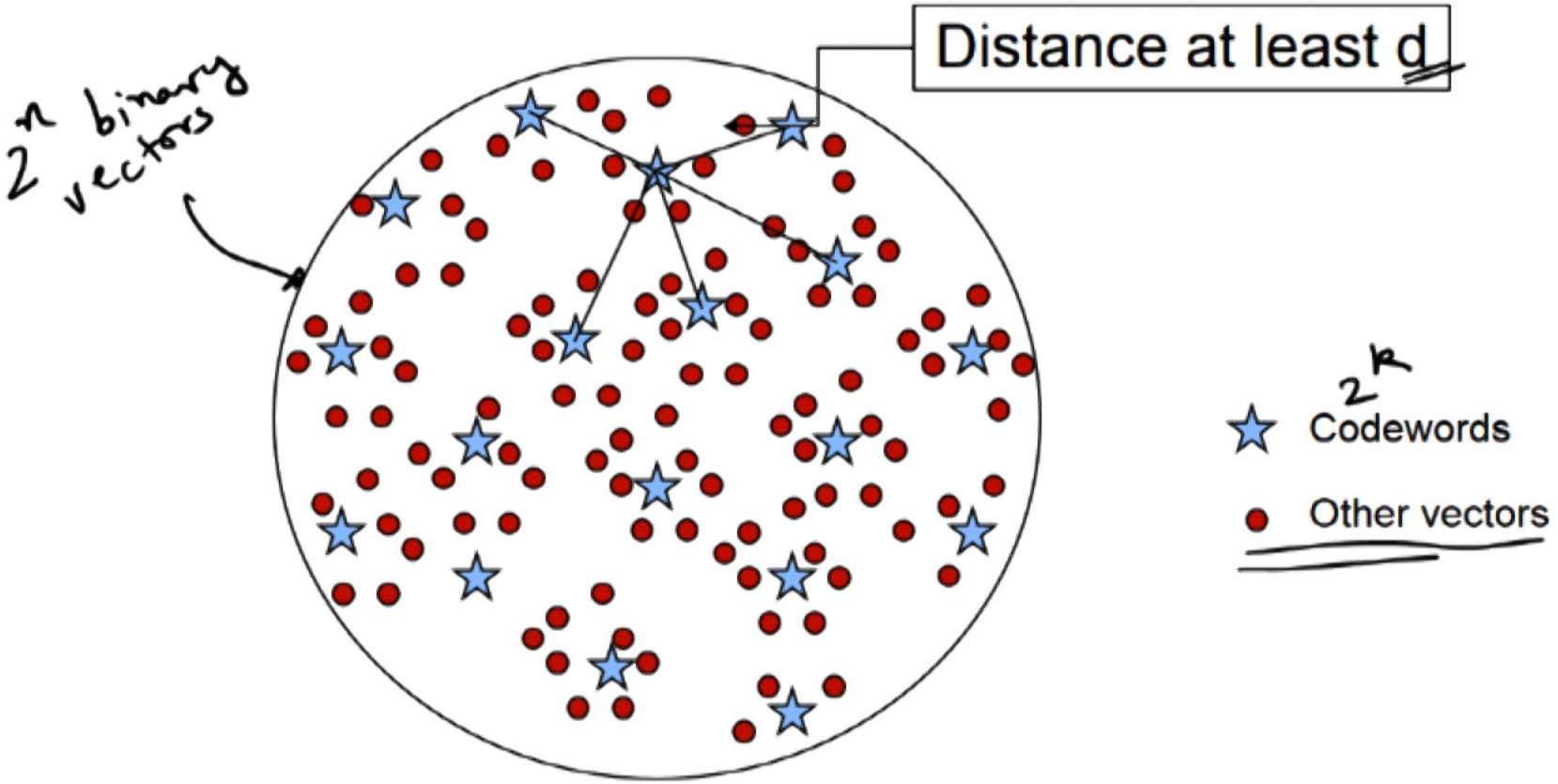
$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \qquad H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Minimum Distance: Linear Codes

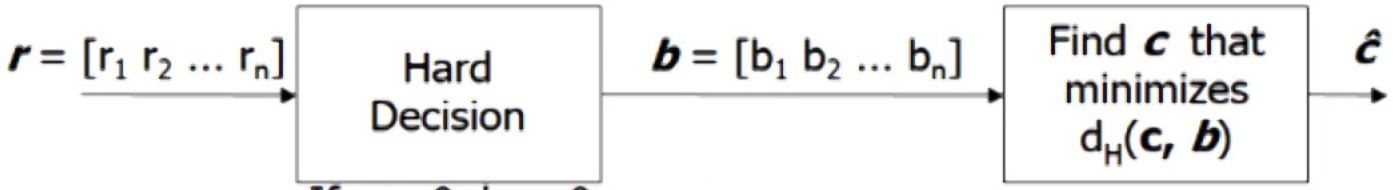
- Minimum Distance
  - Hamming weight of a binary vector is defined to be the number of 1s in it
  - dist(u,v)=weight(u+v) (+ modulo 2)
  - d_{min} of a linear block code is the minimum weight of a nonzero codeword
    - u,v : distinct codewords; w = u+v: nonzero codeword
    - min dist(u,v) = min weight(u+v) = min weight(w)

Avoid low-weight codewords

Geometry of an (n,k,d) code



Example: (7,4) Hamming Code



If $r_i > 0$, $b_i = 0$

If $r_i < 0$, $b_i = 1$.

Message	Codeword	
0000	0000000	4
0001	0001011	5
0010	0010110	
0101	0101100	
1011	1011000	
0110	0110001	
1100	1100010	
1000	1000101	1

Message	Codeword	
0100	0100111	
1001	1001110	
0011	0011101	
0111	0111010	
1110	1110100	
1101	1101001	
1010	1010011	2
1111	1111111	

- $\boldsymbol{b} = [1010101]$, $\hat{\boldsymbol{c}} = ?$ 1000101
- $\boldsymbol{b} = [0110110]$, $\hat{\boldsymbol{c}} = ?$

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

(4 × 7)