EC 721 Advanced Digital Communications
Spring 2008

Mohamed Essam Khedr

Department of Electronics and Communications

Error correcting codes

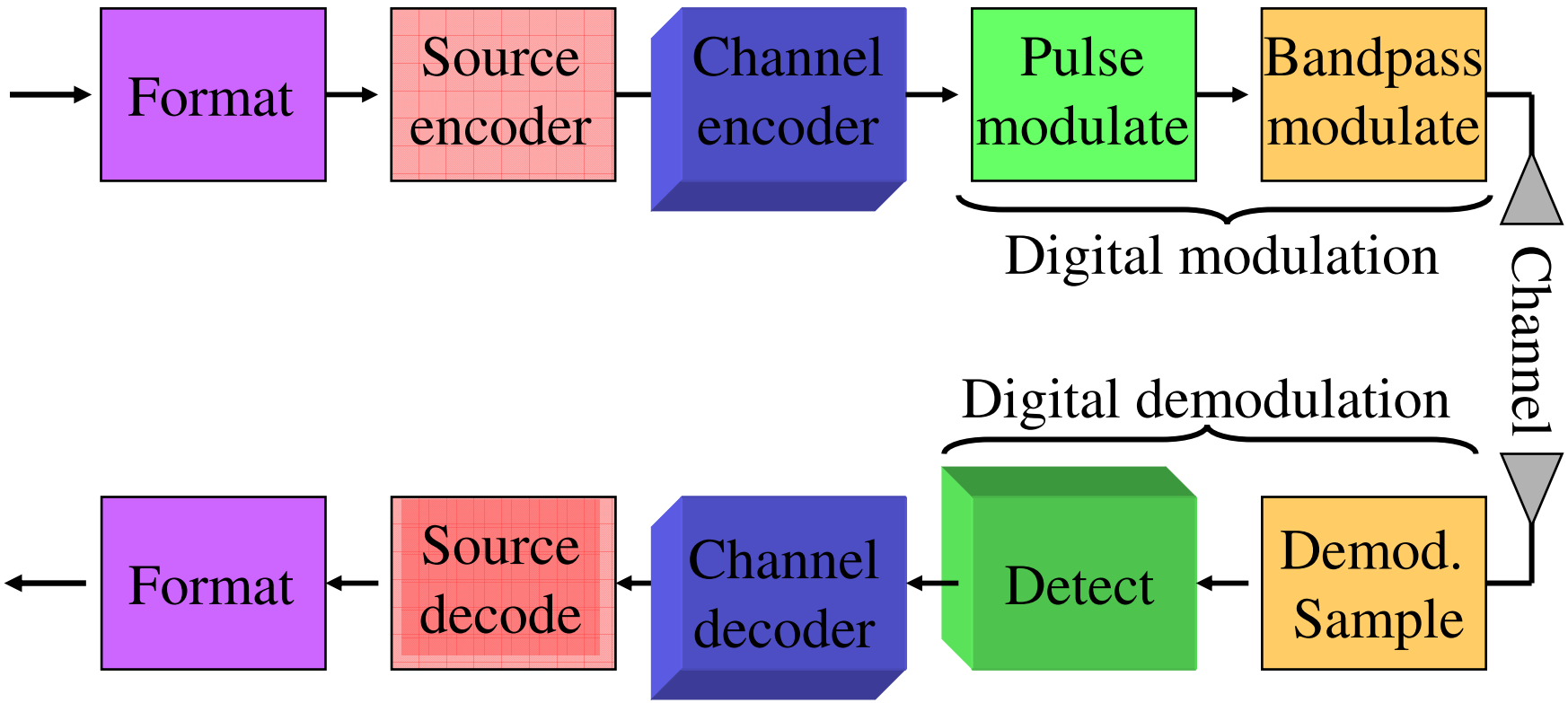
http://webmail.aast.edu/~khedr

Syllabus

- Tentatively

Week 1	Overview, Probabilities, Random variables
Week 2	Random Process, Optimum Detection
Week 3	Digital Signal Representation
Week 4	Signal space and probability of error
Week 5	Probability of error of M-ary techniques
Week 6	Linear block codes
Week 7	
Week 8	
Week 9	
Week 10	
Week 11	
Week 12	
Week 13	
Week 14	
Week 15	

Block diagram of a DCS

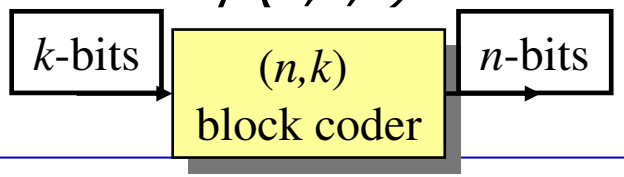


What is channel coding?

- Channel coding:
  - Transforming signals to improve communications performance by increasing the robustness against channel impairments (noise, interference, fading, ..)
  - Waveform coding: Transforming waveforms to better waveforms
  - Structured sequences: Transforming data sequences into better sequences, having structured redundancy.
    - "Better" in the sense of making the decision process less subject to errors.

What is channel coding?

- Coding is mapping of binary source (usually) output sequences of length *k* into binary channel input sequences *n (>k)*
- A block code is denoted by *(n,k)*
- Binary coding produces 2^k codewords of length *n.* Extra bits in codewords are used for error detection/correction
- In this course we concentrate on two coding types: (1) block, and (2) convolutional codes realized by binary numbers:
  - Block codes: mapping of information source into channel inputs done independently: Encoder output depends only on the current *block* of input sequence
  - Convolutional codes: *each source bit* influences *n(L+1)* channel input bits. *n(L+1)* is the constraint length and *L* is the memory depth. These codes are denoted by *(n,k,L).*

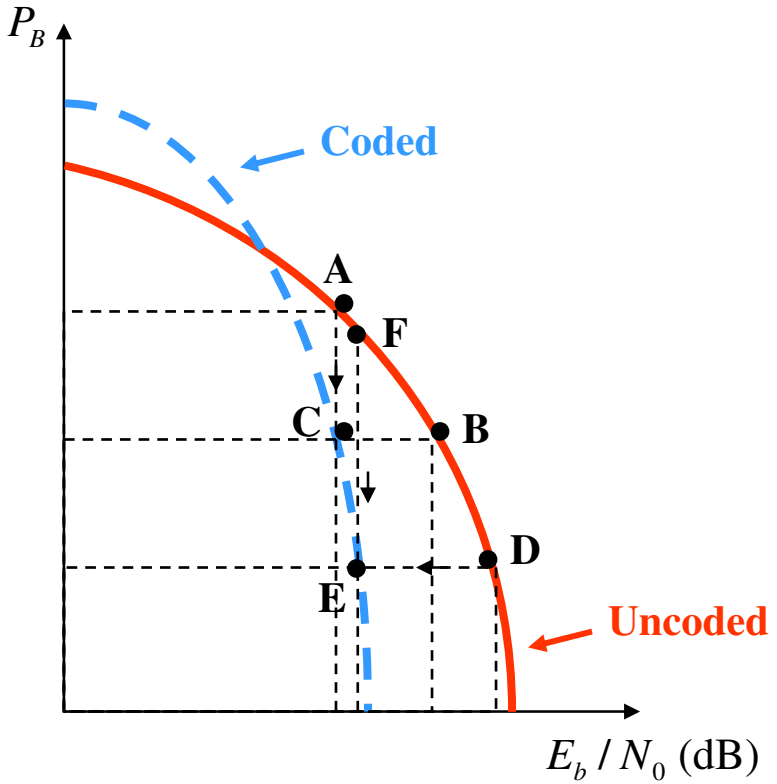


Error control techniques

- Automatic Repeat reQuest (ARQ)
  - Full-duplex connection, error detection codes
  - The receiver sends a feedback to the transmitter, saying that if any error is detected in the received packet or not (Not-Acknowledgement (NACK) and Acknowledgement (ACK), respectively).
  - The transmitter retransmits the previously sent packet if it receives NACK.
- Forward Error Correction (FEC)
  - Simplex connection, error correction codes
  - The receiver tries to correct some errors
- Hybrid ARQ (ARQ+FEC)
  - Full-duplex, error detection and correction codes

Why using error correction coding?

- Error performance vs. bandwidth
- Power vs. bandwidth
- Data rate vs. bandwidth
- Capacity vs. bandwidth



Coding gain:

For a given bit-error probability, the reduction in the Eb/N0 that can be realized through the use of code:

$$G\,[\mathrm{dB}] = \left(\frac{E_b}{N_0}\right)_{\mathrm{u}}\,[\mathrm{dB}] - \left(\frac{E_b}{N_0}\right)_{\mathrm{c}}\,[\mathrm{dB}]$$

Channel models

- Discrete memory-less channels
  - Discrete input, discrete output
- Binary Symmetric channels
  - Binary input, binary output
- Gaussian channels
  - Discrete input, continuous output

Linear block codes

- Let us review some basic definitions first which are useful in understanding Linear block codes.

Some definitions

- Binary field :
  - The set {0,1}, under modulo 2 binary addition and multiplication forms a field.

Addition	Multiplication
$0 \oplus 0 = 0$	$0 \cdot 0 = 0$
$0 \oplus 1 = 1$	$0 \cdot 1 = 0$
$1 \oplus 0 = 1$	$1 \cdot 0 = 0$
$1 \oplus 1 = 0$	$1 \cdot 1 = 1$

  - Binary field is also called Galois field, GF(2).

Some definitions…

- Examples of vector spaces
  - The set of binary n-tuples, denoted by V_n

$$V_4 = \{(0000), (0001), (0010), (0011), (0100), (0101), (0111),$$
$$(1000), (1001), (1010), (1011), (1100), (1101), (1111)\}$$

- Vector subspace:
  - A subset S of the vector space V_n is called a subspace if:
    - The all-zero vector is in S.
    - The sum of any two vectors in S is also in S.
    - Example:
      $\{(0000), (0101), (1010), (1111)\}$ is a subspace of V_4.

Some definitions…

- Spanning set:
  - A collection of vectors $G = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$, the linear combinations of which include all vectors in a vector space V, is said to be a spanning set for V or to span V.
    - Example:
      $\{(1000), (0110), (1100), (0011), (1001)\}$ spans V_4.
- Bases:
  - A spanning set for V that has minimal cardinality is called a basis for V.
    - Cardinality of a set is the number of objects in the set.
    - Example:
      $\{(1000), (0100), (0010), (0001)\}$ is a basis for V_4.

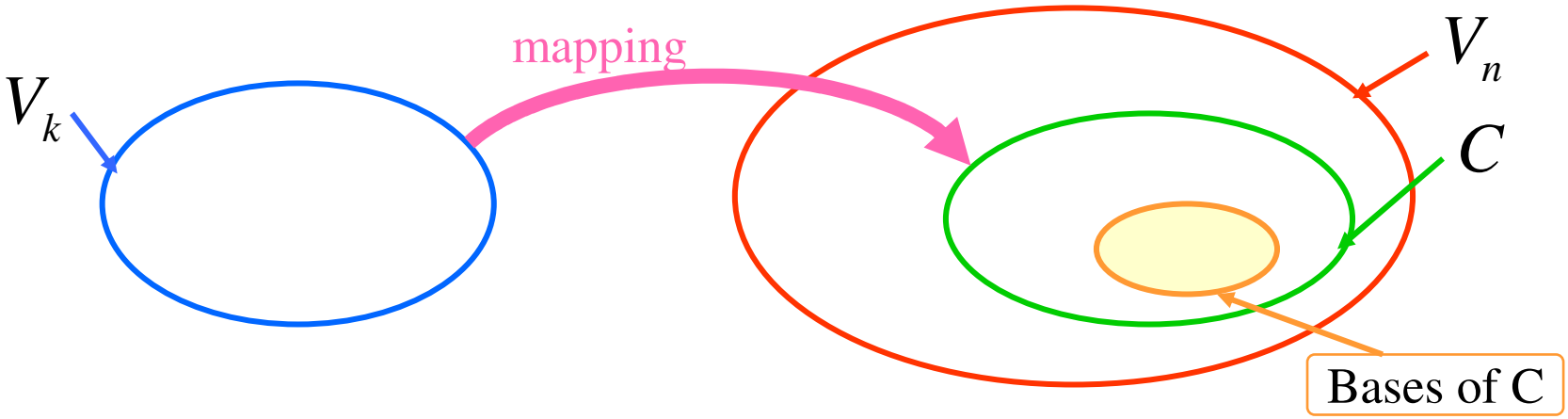
Linear block codes

- Linear block code (n,k)
  - A set $C \subset V_n$ with cardinality 2^k is called a linear block code if, and only if, it is a subspace of the vector space V_n .

$$V_k \rightarrow C \subset V_n$$

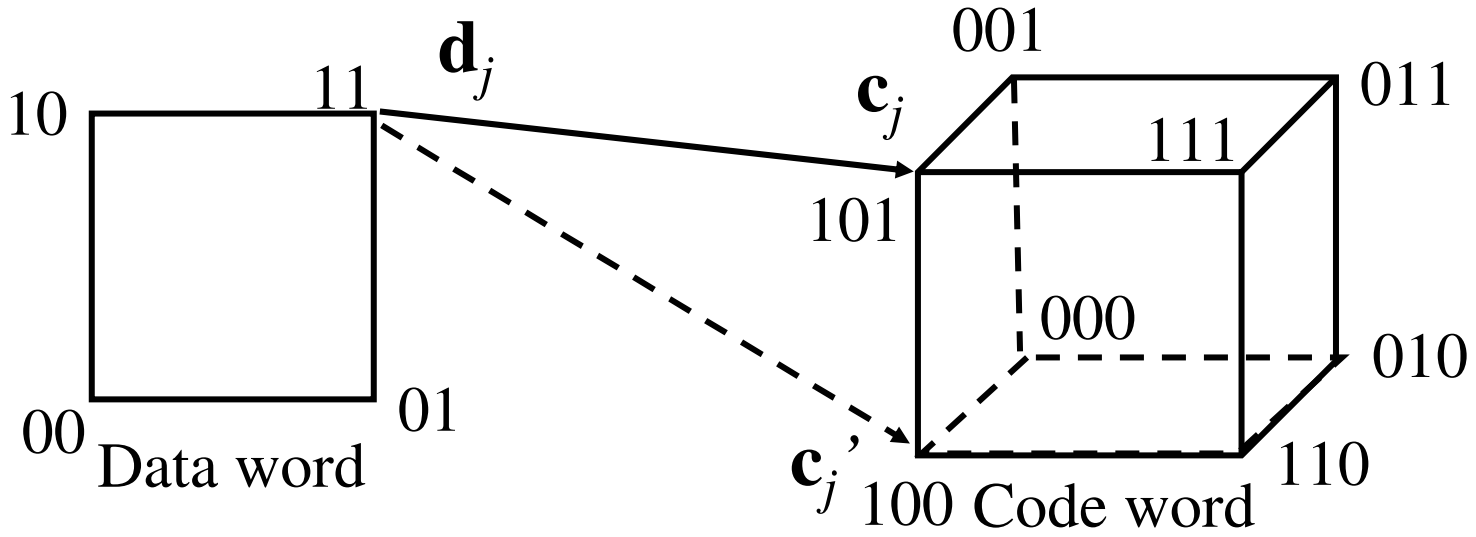
    - Members of C are called code-words.
    - The all-zero codeword is a codeword.
    - Any linear combination of code-words is a codeword.

Linear block codes – cont'd



of bits for FEC

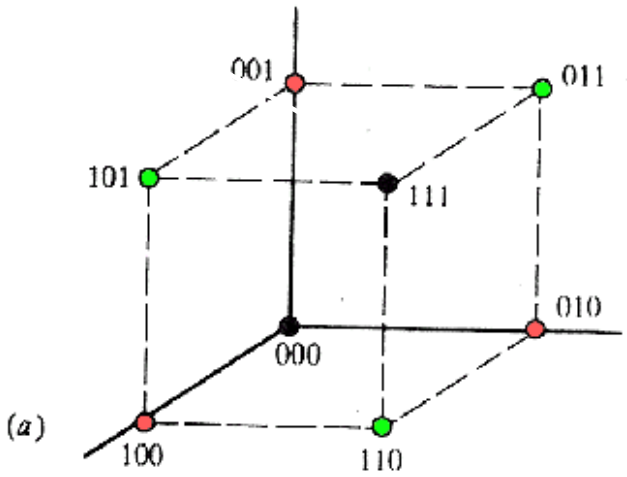
- Want to correct t errors in an (n,k) code
  - Data word $\mathbf{d} = [d_1, d_2, \ldots, d_k] \Rightarrow 2^k$ data words
  - Code word $\mathbf{c} = [c_1, c_2, \ldots, c_n] \Rightarrow 2^n$ code words



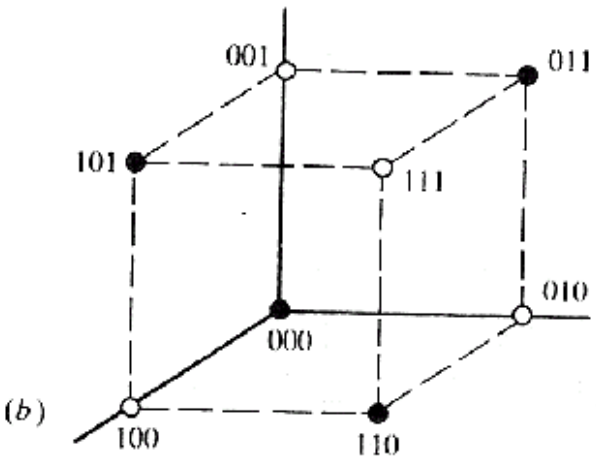
Representing codes by vectors

- Code strength is measured by Hamming distance that tells how different code words are:
  - Codes are more powerful when their minimum Hamming distance d_{min} (over all codes in the code family) is large
- Hamming distance d(X,Y) is the number of bits that are different between code words
- (*n*,*k*) codes can be mapped into *n*-dimensional grid:

3-bit repetition code

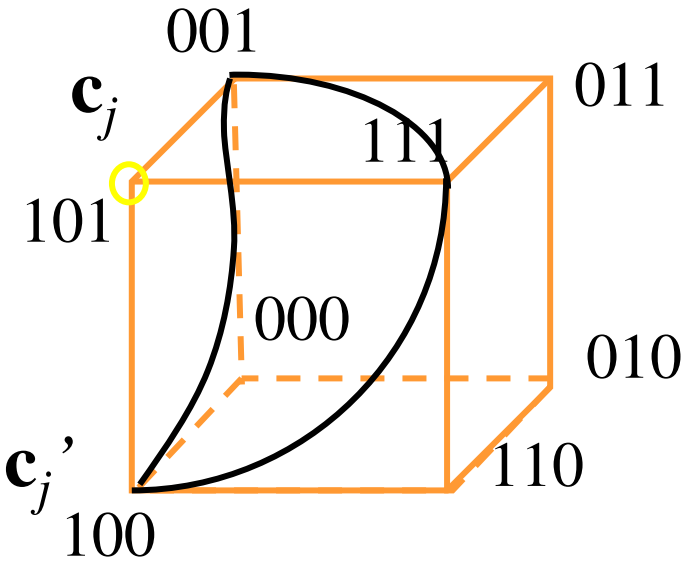


3-bit parity code



Error Detection

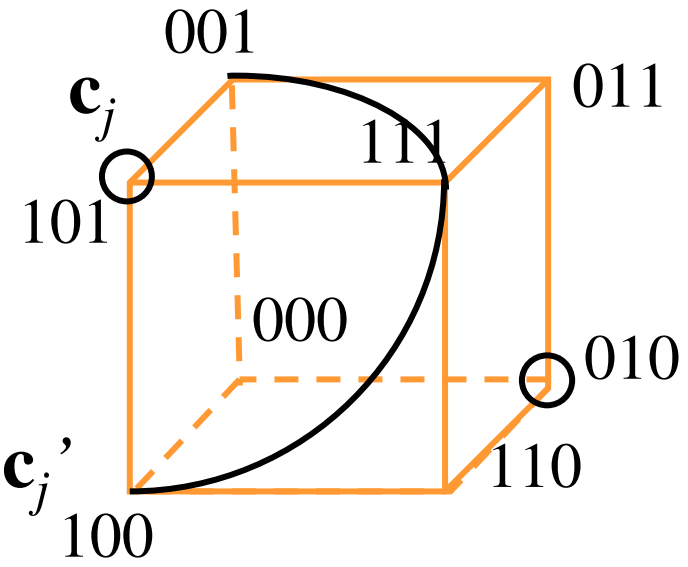
- If a code can detect a t bit error, then c_j' must be within a Hamming sphere of t
- For example, if $c_j=101$, and $t=1$, then '100','111', and '001' lie in the Hamming sphere.



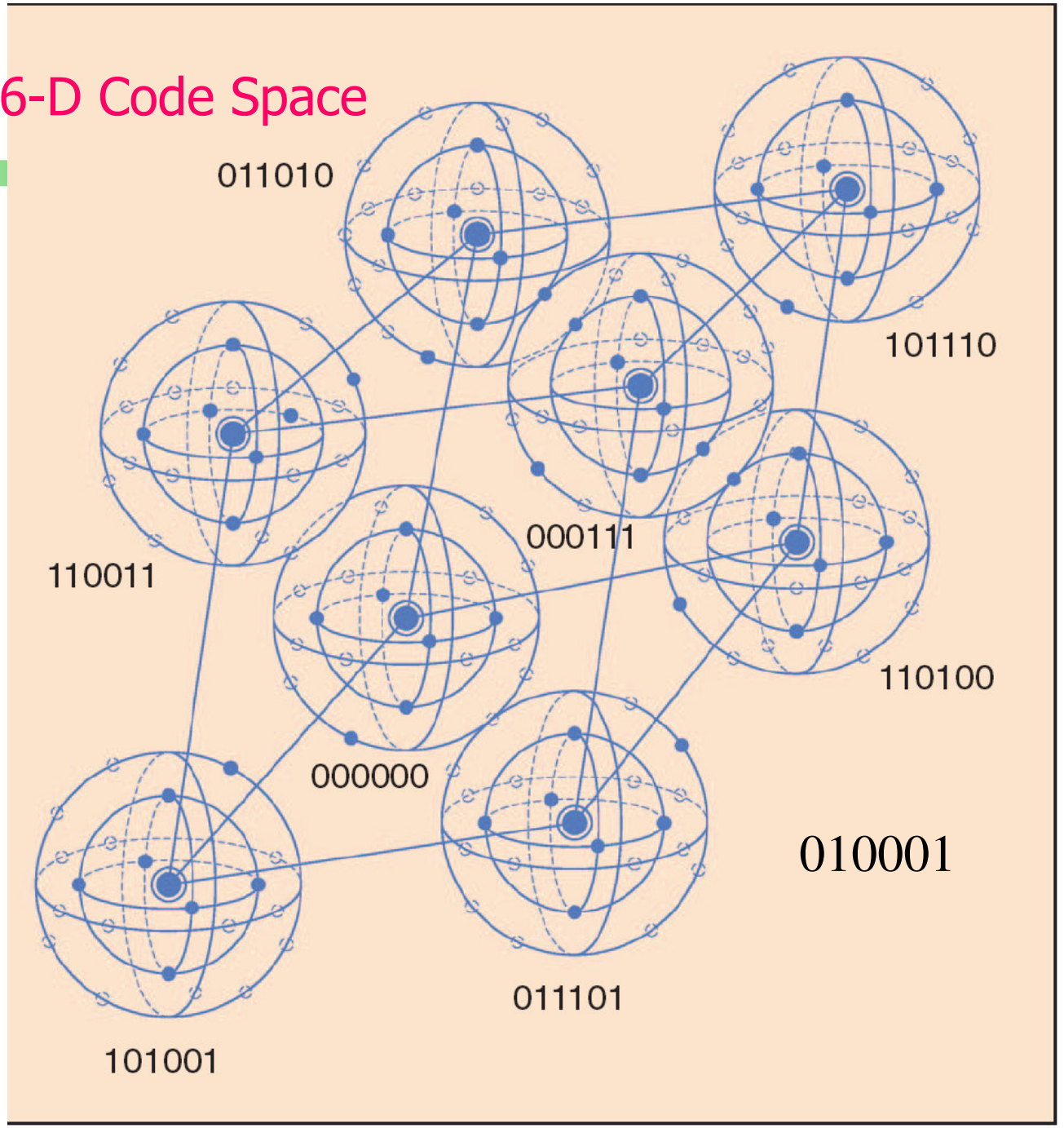
Code word

Error Correction

- To correct an error, the Hamming spheres around a code word must be nonoverlapping, $d_{min} = 2t + 1$

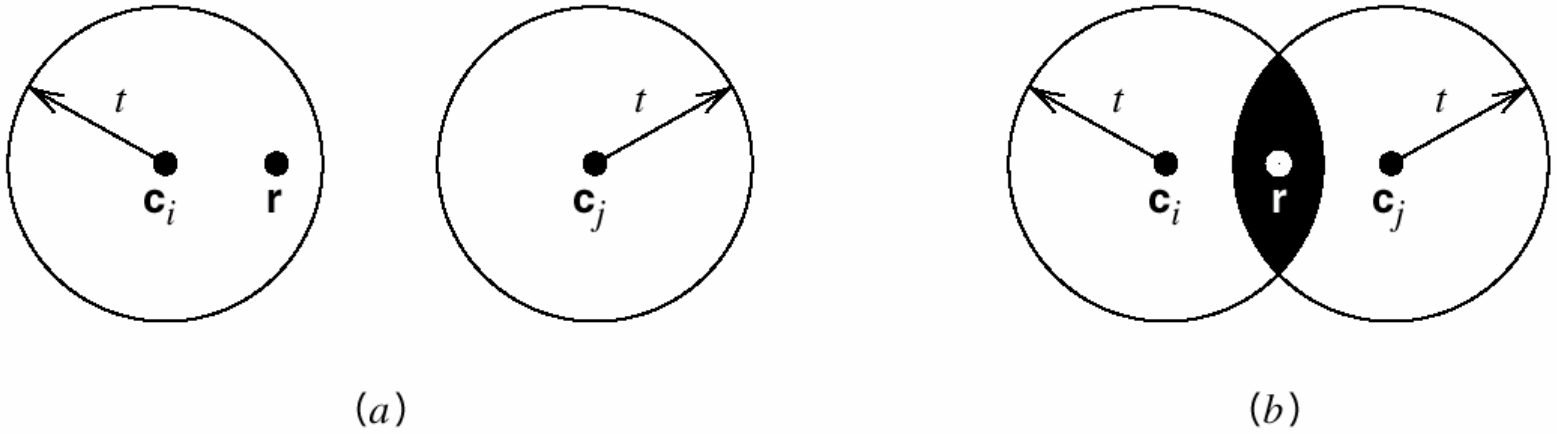


6-D Code Space



▲ *4. Visualization of eight code words in a 6-tuple space.*

(a) Hamming distance $d(\mathbf{c}_i, \mathbf{c}_j) \geq 2t + 1$.
(b) Hamming distance $d(\mathbf{c}_i, \mathbf{c}_j) < 2t$.
The received vector is denoted by **r**.



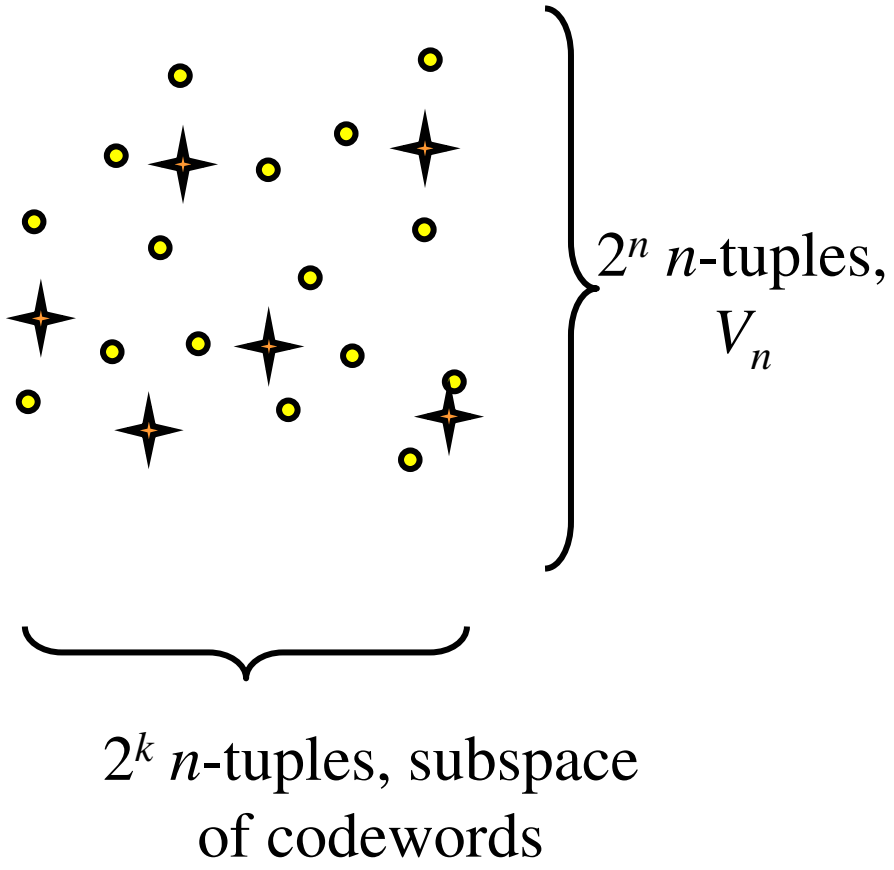
Block Code Error Detection and Correction

- (6,3) code $2^3 => 2^6$, $d_{min}=3$
- Can detect 2 bit errors, correct 1 bit
  - 110100 sent; 110101 received
- Erasure: Suppose code word 110011 sent but two digits were erased (xx0011), correct code word has smallest Hamming distance

Message	Code-word	1	2
000	000000	4	2
100	110100	**1**	3
010	011010	3	2
110	101110	3	3
001	101001	3	2
101	011101	2	3
011	110011	2	**0**
111	000111	3	1

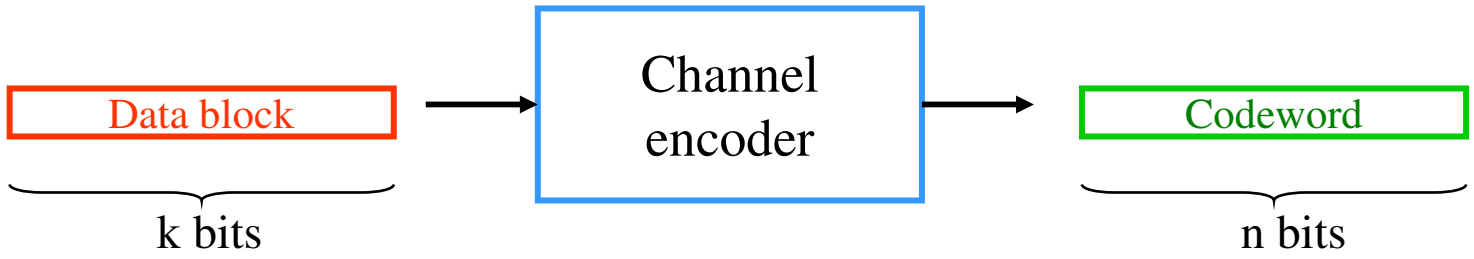
Geometric View

- Want code efficiency, so the space should be packed with as many code words as possible
- Code words should be as far apart as possible to minimize errors



Linear block codes – cont'd

- The information bit stream is chopped into blocks of k bits.
- Each block is encoded to a larger block of n bits.
- The coded bits are modulated and sent over channel.
- The reverse procedure is done at the receiver.



n-k Redundant bits

$$R_c = \frac{k}{n} \quad \text{Code rate}$$

Linear block codes – cont'd

- The Hamming weight of vector **U**, denoted by w(**U**), is the number of non-zero elements in **U**.
- The Hamming distance between two vectors **U** and **V**, is the number of elements in which they differ.

$$d(\mathbf{U},\mathbf{V}) = w(\mathbf{U} \oplus \mathbf{V})$$

- The minimum distance of a block code is

$$d_{\min} = \min_{i \neq j} d(\mathbf{U}_i, \mathbf{U}_j) = \min_i w(\mathbf{U}_i)$$

Linear block codes – cont'd

- Error detection capability is given by

$$e = d_{\min} - 1$$

- Error correcting-capability **t** of a code, which is defined as the maximum number of guaranteed correctable errors per codeword, is

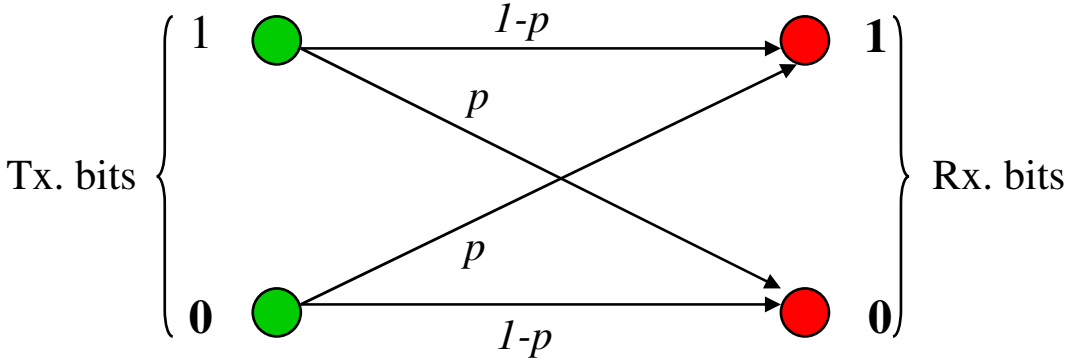
$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

Linear block codes – cont'd

- For memory less channels, the probability that the decoder commits an erroneous decoding is $$P_M \leq \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j}$$
  - p is the transition probability or bit error probability over channel.
- The decoded bit error probability is $$P_B \approx \frac{1}{n} \sum_{j=t+1}^{n} j \binom{n}{j} p^j (1-p)^{n-j}$$

Linear block codes – cont'd

- Discrete, memoryless, symmetric channel model

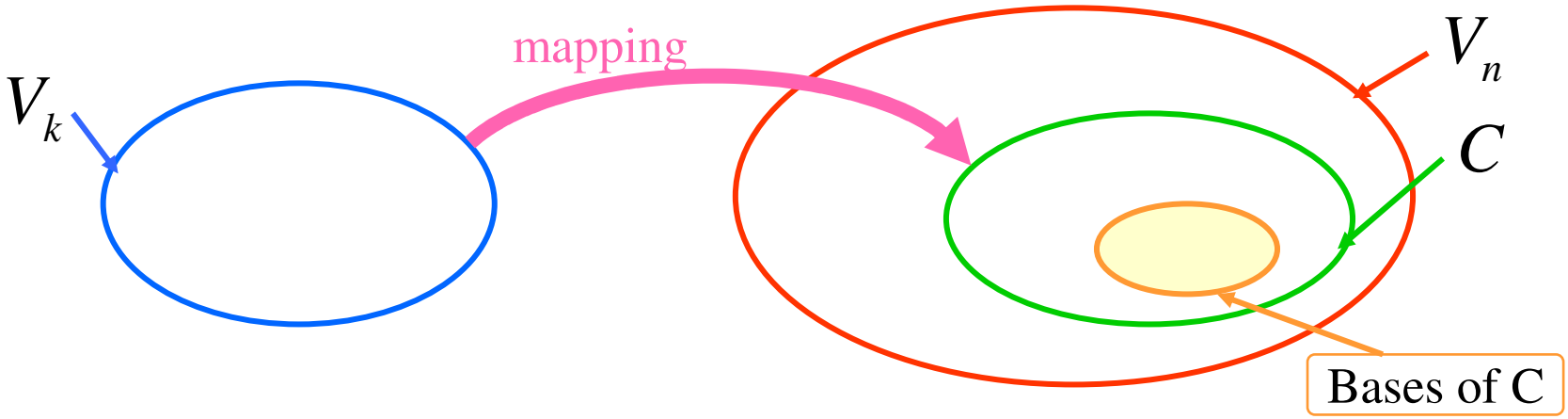


  - Note that for coded systems, the coded bits are modulated and transmitted over channel. For example, for M-PSK modulation on AWGN channels (M>2):

$$p \approx \frac{2}{\log_2 M} Q\left(\sqrt{\frac{2(\log_2 M)E_c}{N_0}} \sin\left(\frac{\pi}{M}\right)\right) = \frac{2}{\log_2 M} Q\left(\sqrt{\frac{2(\log_2 M)E_b R_c}{N_0}} \sin\left(\frac{\pi}{M}\right)\right)$$

where E_c is energy per coded bit, given by $E_c = R_c E_b$

Linear block codes –cont'd



- A matrix G is constructed by taking as its rows the vectors on the basis, $\{\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_k\}$.

$$\mathbf{G} = \begin{bmatrix} \mathbf{V}_1 \\ \vdots \\ \mathbf{V}_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}$$

Linear block codes – cont'd

- Encoding in (n,k) block code

$$\mathbf{U} = \mathbf{mG}$$

$$(u_1, u_2, \ldots, u_n) = (m_1, m_2, \ldots, m_k) \cdot \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \\ \vdots \\ \mathbf{V}_k \end{bmatrix}$$

$$(u_1, u_2, \ldots, u_n) = m_1 \cdot \mathbf{V}_1 + m_2 \cdot \mathbf{V}_2 + \ldots + m_2 \cdot \mathbf{V}_k$$

  - The rows of G, are linearly independent.

Linear block codes – cont'd

- Example: Block code (6,3)

$$\mathbf{G} = \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \\ \mathbf{V}_3 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,0\,1 \end{bmatrix}$$

Message vector	Codeword
000	000000
100	110100
010	011010
110	101110
001	101001
101	011101
011	110011
111	000111

Linear block codes – cont'd

- Systematic block code (n,k)
  - For a systematic code, the first (or last) k elements in the codeword are information bits.

$$\mathbf{G} = [\mathbf{P} \vdots \mathbf{I}_k]$$

$$\mathbf{I}_k = k \times k \text{ identity matrix}$$

$$\mathbf{P}_k = k \times (n-k) \text{ matrix}$$

$$\mathbf{U} = (u_1, u_2, \ldots, u_n) = (\underbrace{p_1, p_2, \ldots, p_{n-k}}_{\text{parity bits}}, \underbrace{m_1, m_2, \ldots, m_k}_{\text{message bits}})$$

Linear block codes – cont'd

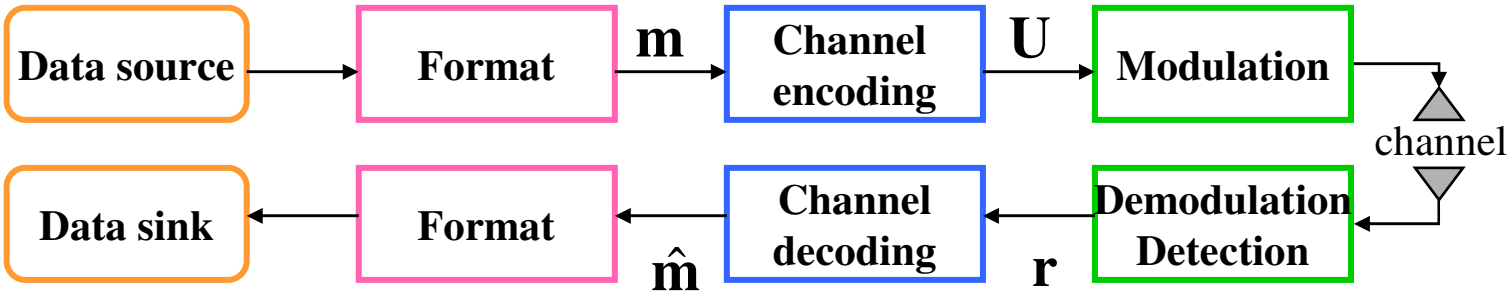
- For any linear code we can find an matrix $\mathbf{H}_{(n-k)\times n}$, which its rows are orthogonal to rows of $\mathbf{G}$:

$$\mathbf{G}\mathbf{H}^T = \mathbf{0}$$

- $\mathbf{H}$ is called the parity check matrix and its rows are linearly independent.
- For systematic linear block codes:

$$\mathbf{H} = [\mathbf{I}_{n-k} \vdots \mathbf{P}^T]$$

Linear block codes – cont'd



$$\mathbf{r} = \mathbf{U} + \mathbf{e}$$

$\mathbf{r} = (r_1, r_2, ..., r_n)$ received codeword or vector

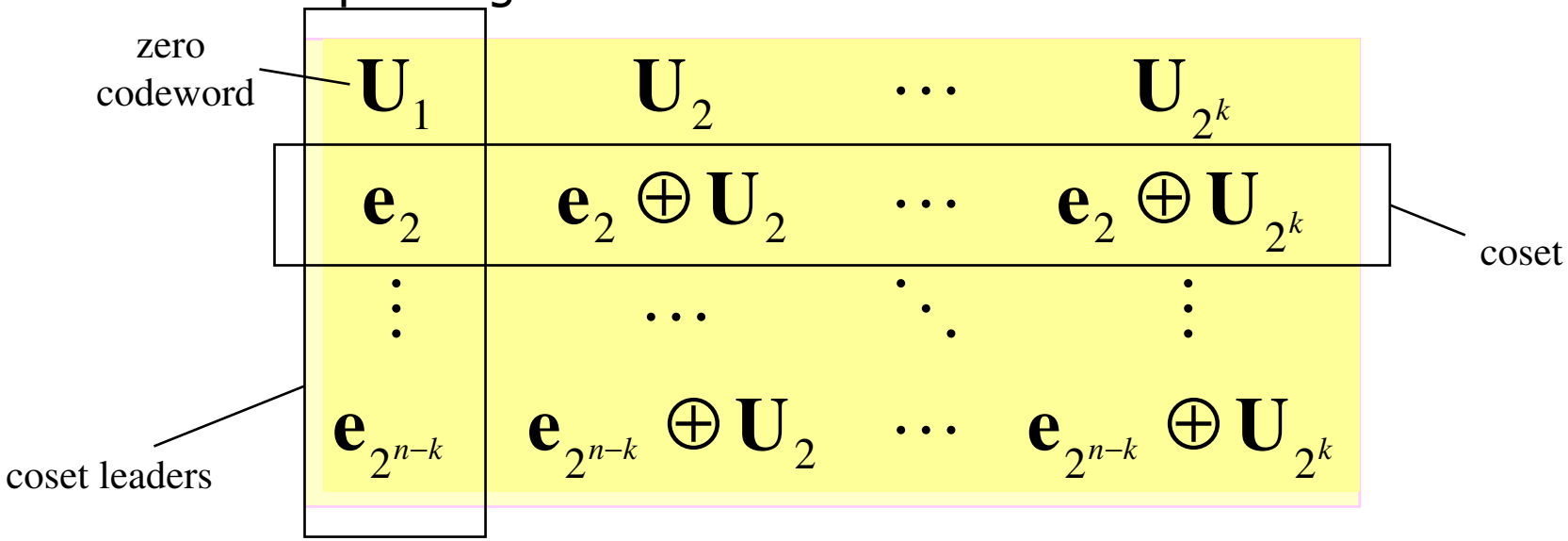
$\mathbf{e} = (e_1, e_2, ..., e_n)$ error pattern or vector

- Syndrome testing:
  - **S** is syndrome of **r**, corresponding to the error pattern **e**.

$$\mathbf{S} = \mathbf{r}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$$

Linear block codes – cont'd

- Standard array
  1. For row $i = 2,3,\ldots,2^{n-k}$ find a vector in V_n of minimum weight which is not already listed in the array.
  2. Call this pattern $\mathbf{e}_i$ and form the $i:\text{th}$ row as the corresponding coset



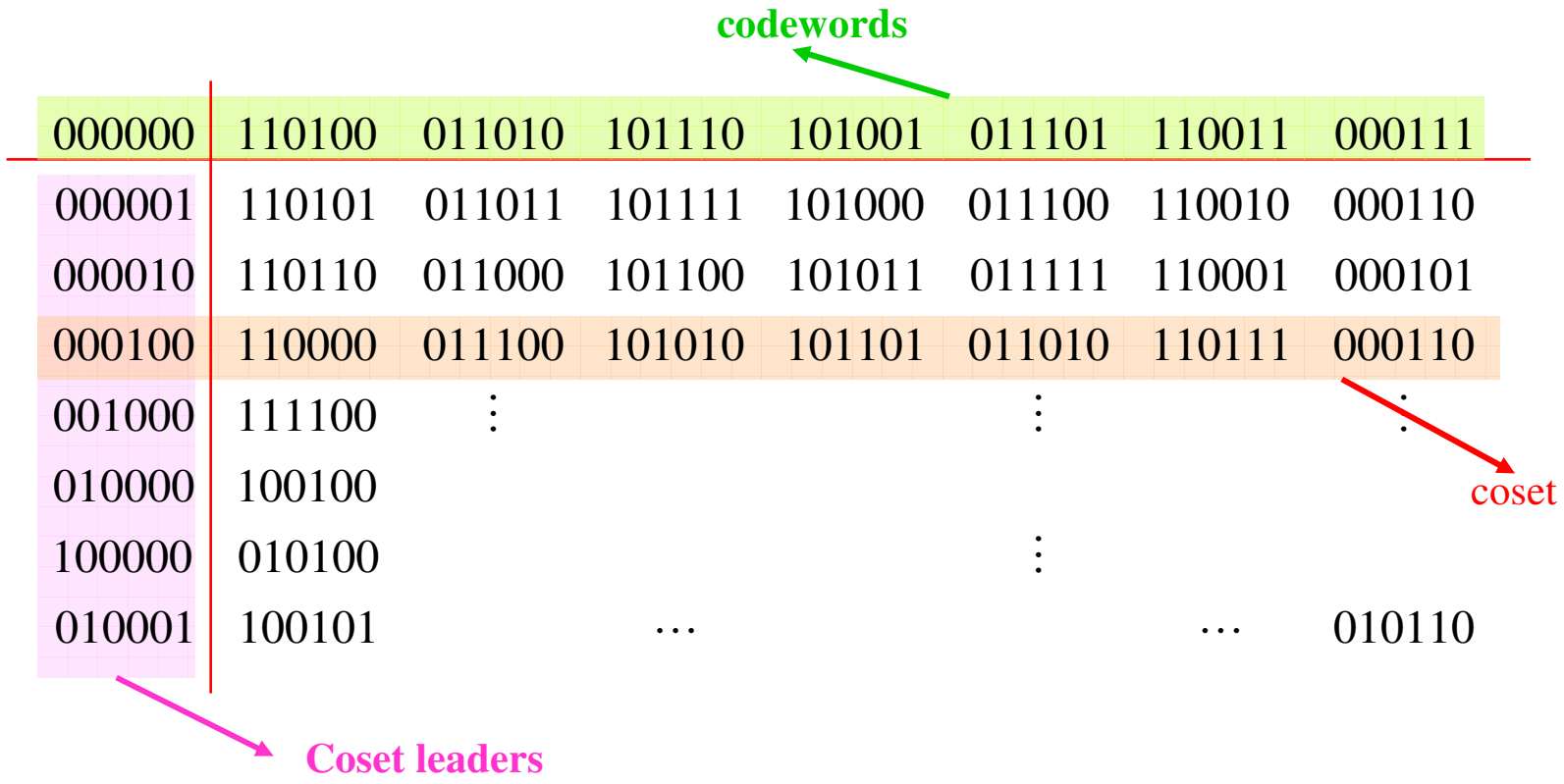
Linear block codes – cont'd

- Standard array and syndrome table decoding
  1. Calculate $\mathbf{S} = \mathbf{r}\mathbf{H}^T$
  2. Find the coset leader, $\hat{\mathbf{e}} = \mathbf{e}_i$, corresponding to $\mathbf{S}$.
  3. Calculate $\hat{\mathbf{U}} = \mathbf{r} + \hat{\mathbf{e}}$ and corresponding $\hat{\mathbf{m}}$.

  - Note that $\hat{\mathbf{U}} = \mathbf{r} + \hat{\mathbf{e}} = (\mathbf{U} + \mathbf{e}) + \hat{\mathbf{e}} = \mathbf{U} + (\mathbf{e} + \hat{\mathbf{e}})$
    - If $\hat{\mathbf{e}} = \mathbf{e}$, error is corrected.
    - If $\hat{\mathbf{e}} \neq \mathbf{e}$, undetectable decoding error occurs.

Linear block codes – cont'd

- Example: Standard array for the (6,3) code



Linear block codes – cont'd

Error pattern	Syndrome
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100
010001	111

$\mathbf{U} = (101110)$ transmitted.

$\mathbf{r} = (001110)$ is received.

➡ The syndrome of $\mathbf{r}$ is computed:

$$\mathbf{S} = \mathbf{r}\mathbf{H}^T = (001110)\mathbf{H}^T = (100)$$

➡ Error pattern corresponding to this syndrome is

$$\hat{\mathbf{e}} = (100000)$$

➡ The corrected vector is estimated

$$\hat{\mathbf{U}} = \mathbf{r} + \hat{\mathbf{e}} = (001110) + (100000) = (101110)$$

Hamming codes

- Hamming codes
  - Hamming codes are a subclass of linear block codes and belong to the category of *perfect codes*.
  - Hamming codes are expressed as a function of a single integer $m \geq 2$.

Code length :	$n = 2^m - 1$
Number of information bits :	$k = 2^m - m - 1$
Number of parity bits :	$n\text{-}k = m$
Error correction capability :	$t = 1$

  - The columns of the parity-check matrix, **H**, consist of all non-zero binary m-tuples.

Hamming codes

- Example: Systematic Hamming code (7,4)

$$\mathbf{H} = \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right] = [\mathbf{I}_{3\times 3} \vdots \mathbf{P}^T]$$

$$\mathbf{G} = \left[\begin{array}{ccc:cccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] = [\mathbf{P} \vdots \mathbf{I}_{4\times 4}]$$

Example of the block codes