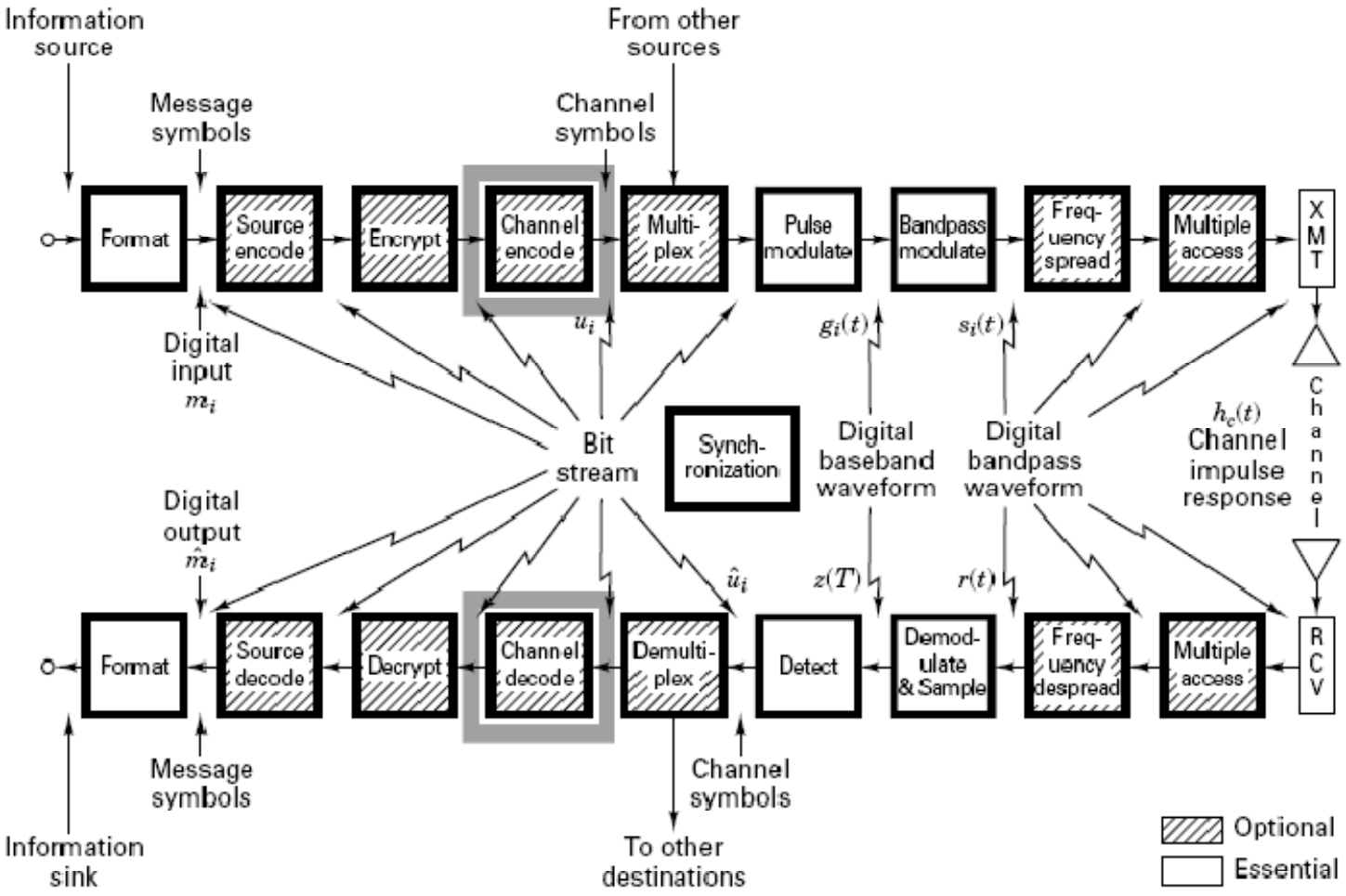
Modul #09

TE3223
SISTEM KOMUNIKASI 2

LINEAR BLOCK CODE

Program Studi S1 Teknik Telekomunikasi
Departemen Teknik Elektro - Sekolah Tinggi Teknologi Telkom
Bandung – 2007

Letak Channel Code



Channel Coding:

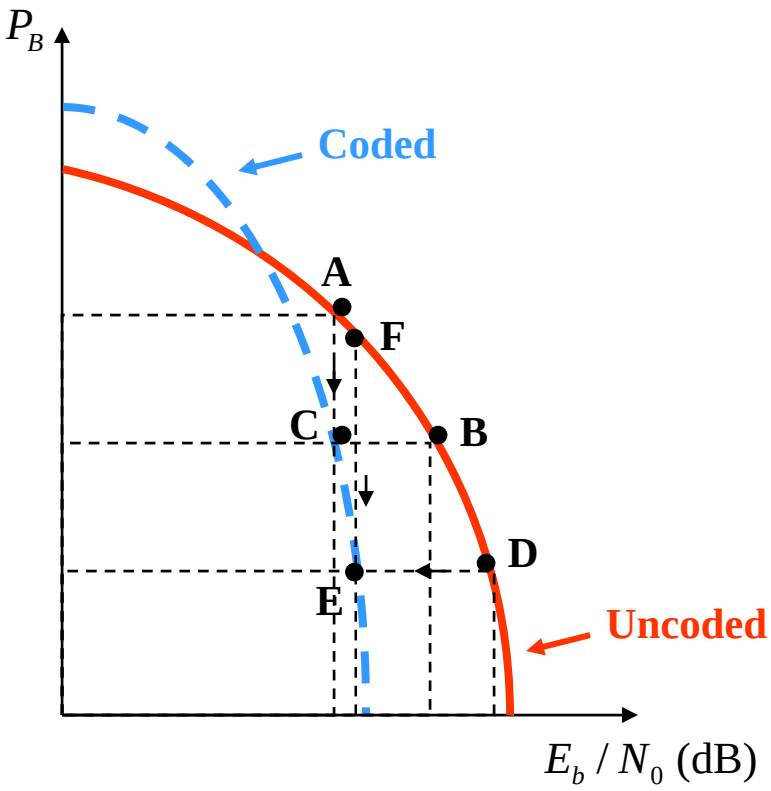
- **Linear Block Code**
- **Cyclic Codes**
- BCH (The Bose Chaudhuri & Hocquenghem) Codes
- **Convolutional Codes**
- Turbo Codes

Referensi:

- "*Digital communications: Fundamentals and Applications*" by Bernard Sklar,Prentice Hall, 2001, ISBN: 0-13-084788-7
- *"Communication Sistems, 4th Edition"; by* Simon Haykin*;* John Wiley & Sons; Ontario; 2000
- "*Error Control Coding: Fundamentals and Applications*"; by Shu Lin & Daniel J Castello; Prentice-Hall; 1983; ISBN: 0-13-283796-X

Dampak menggunakan Channel Coding

- Kinerja vs bandwidth
- Power vs. bandwidth
- Data rate vs. bandwidth
- Capacity vs. bandwidth



Coding gain:

Reduksi Eb/N0 jika menggunakan skema channel coding untuk mencapai kinerja tertentu

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

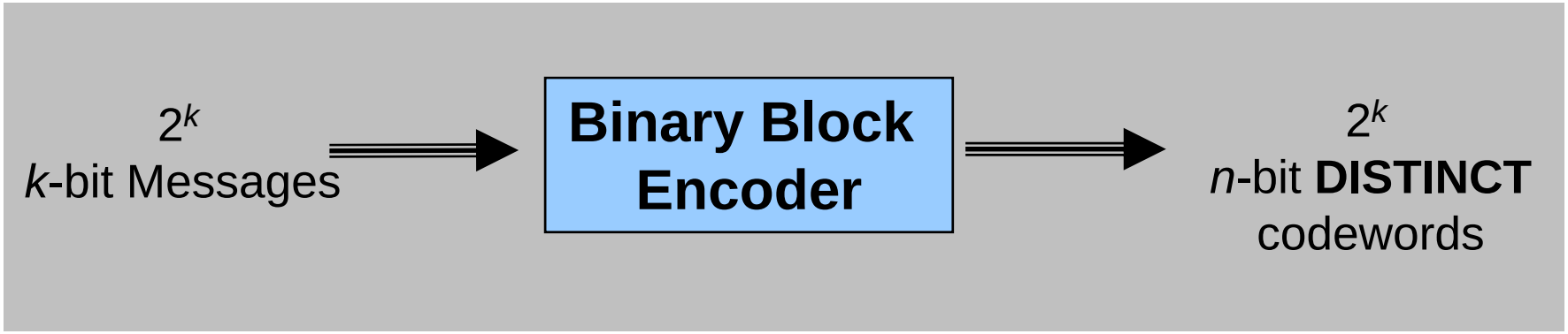
Channel models

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

What are Linear Block Codes?

Linear Block Codes

- Information sequence is segmented into message blocks of ***fixed length***.
- Each *k*-bit information **message** is encoded into an *n*-bit **codeword** (*n*>*k*)



What are Linear Block Codes?

Linear Block Codes

- Modulo-2 sum of any two codewords is …… also a codeword
- Each codeword **v** that belongs to a block code **C** is a linear combination of *k* linearly independent codewords in **C,** i.e.,

$$U=m_0.g_0+m_1.g_1+\ldots+m_{k-1}.g_{k-1}$$
$$g_i=[g_{i0}\ g_{i1}\ \ldots\ g_{i,n-1}]$$

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…

- Fields :
  - Let F be a set of objects on which two operations '+' and '.' are defined.
  - F is said to be a field if and only if
    1. F forms a commutative group under + operation. The additive identity element is labeled "0".

       $\forall a,b \in F \Rightarrow a+b=b+a \in F$

    2. F-{0} forms a commutative group under . Operation. The multiplicative identity element is labeled "1".

       $\forall a,b \in F \Rightarrow a \cdot b=b \cdot a \in F$

    3. The operations "+" and "." distribute:

       $a \cdot (b+c)=(a \cdot b)+(a \cdot c)$

Some definitions…

- Vector space:
  - Let V be a set of **vectors** and F a fields of elements called **scalars**. V forms a vector space over F if:
    1. Commutative: $\forall \mathbf{u}, \mathbf{v} \in V \Rightarrow \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} \in F$
    2. $\forall a \in F, \forall \mathbf{v} \in \mathbf{V} \Rightarrow a \cdot \mathbf{v} = \mathbf{u} \in \mathbf{V}$
    3. Distributive:

       $(a+b)\cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$ and $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$
    1. Associative: $\forall a, b \in F, \forall \mathbf{v} \in V \Rightarrow (a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$
    2. $\forall \mathbf{v} \in \mathbf{V},\ 1 \cdot \mathbf{v} = \mathbf{v}$

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 $\boldsymbol{G} = \{\boldsymbol{g}_1, \boldsymbol{g}_2, ..., \boldsymbol{g}_n\} \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ 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.

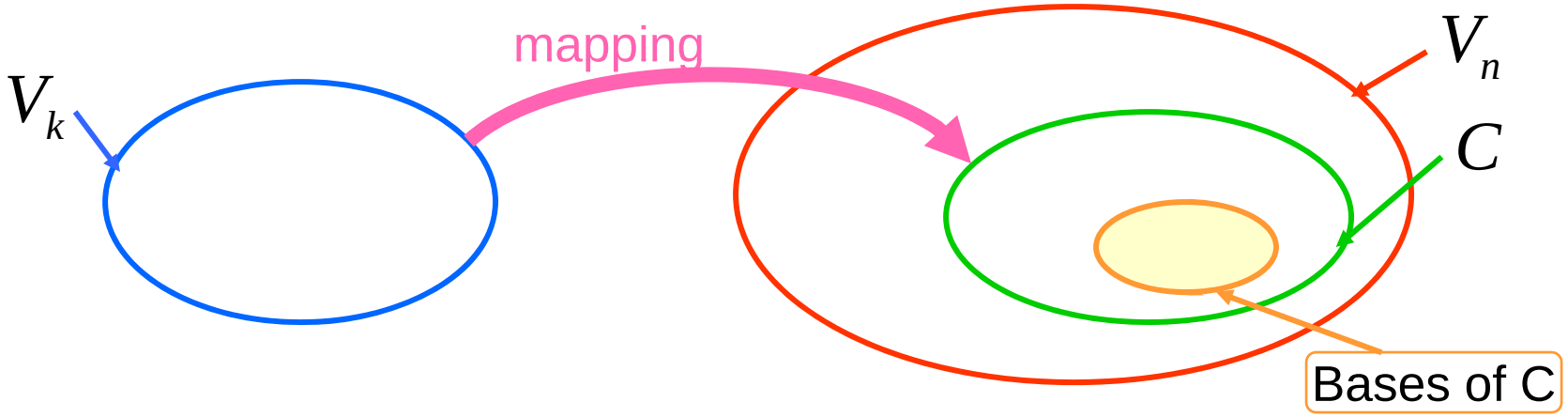
Linear block codes

- 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 .

$$V_k \rightarrow C \subset V_n$$

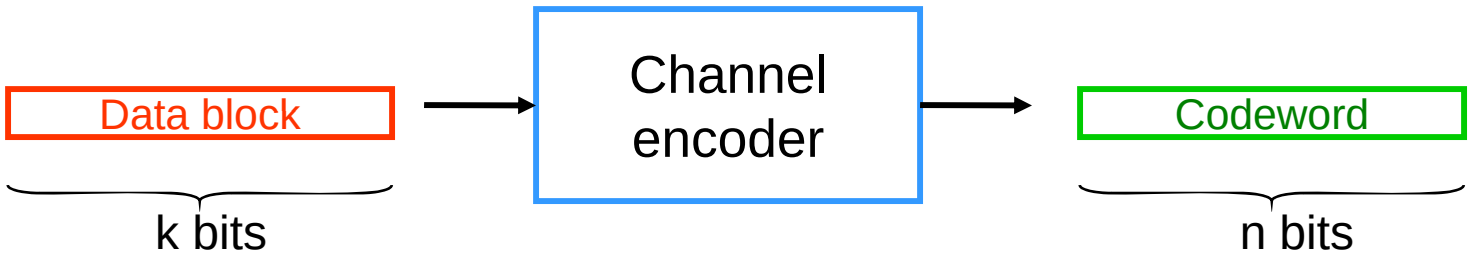
  - Members of C are called code-words.
  - The all-zero codeword is a codeword.
  - Any linear combination of code-words is a codeword.

Linear block codes – cont'd



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

$$P_M \leq \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j}$$

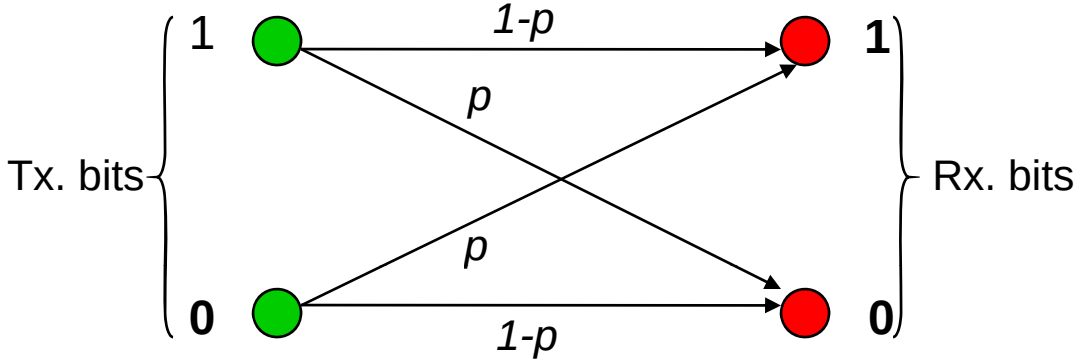
  - p is the transition probability or bit error probability over channel.

- 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

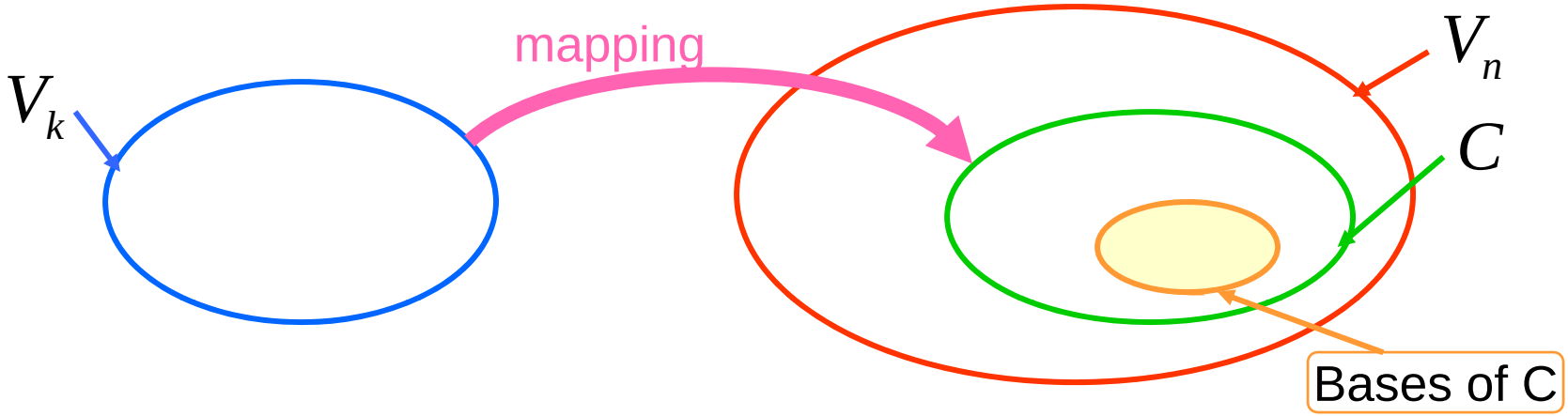


  - Note that for coded systems, the coded bits are modulated and transmitted over channel. For example, for M-PSK modulation on AWGN channels (M>2):

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

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)

$$\mathbf{G} = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \\ \mathbf{V}_3 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,0\,1 \end{bmatrix}$$

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

Example: Block code (7,3)

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

m= [0 1 1 0]

⇓

Linear Block Encoder (**U**=**m**.**G**)

⇓

U= $\mathbf{g}_1+\mathbf{g}_2$

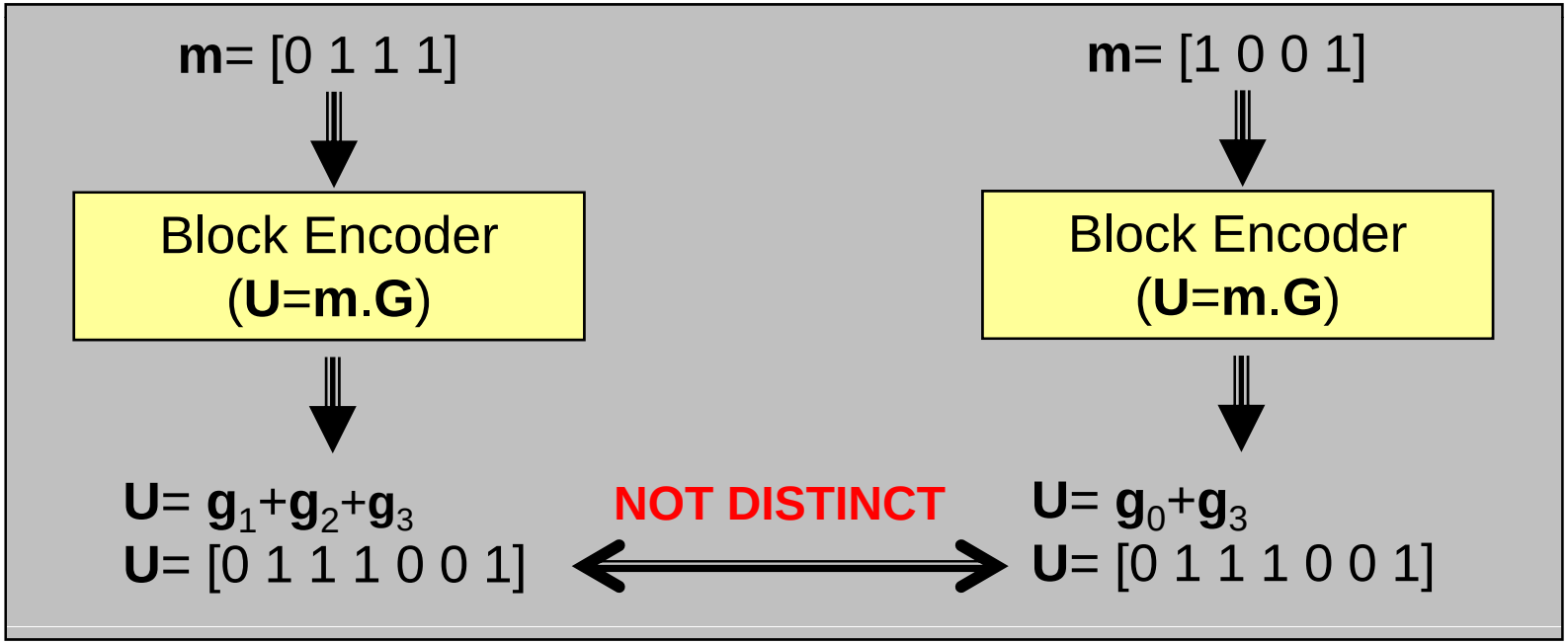
U= [1 0 0 0 1 1 0]

Message (m)	Codeword	
0000	0000000	
0001	**1010001**	$\mathbf{g}_3$
0010	**1110010**	$\mathbf{g}_2$
0011	0100011	
0100	**0110100**	$\mathbf{g}_1$
0101	1100101	
0110	**1000110**	
0111	0010111	
1000	**1101000**	$\mathbf{g}_0$
1001	0111001	
1010	0011010	
1011	1001011	
1100	1011100	
1101	0001101	
1110	0101110	
1111	1111111	

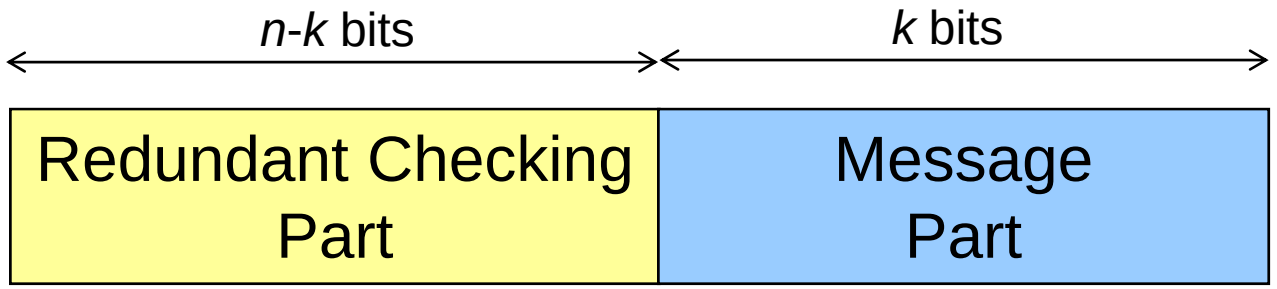
Example

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Linearly Dependent



Linear Systematic Block Codes



p-matrix *kxk- identity matrix*

$$\mathbf{G}=[\mathbf{P}\ \mathbf{I}_k]=\begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{10} & p_{11} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

The Parity Check Matrix

- For any *k x n* matrix **G** with *k* linearly independent rows, there exists an (*n-k*) *x n* matrix **H** (Parity Check Matrix), such that
  - $\mathbf{G.H^T=0}$

$$\mathbf{H}=\left[\mathbf{I}_k\ \mathbf{P}^{\mathbf{T}}\right]=\begin{bmatrix} 1 & 0 & \dots & 0 & p_{00} & p_{01} & \dots & p_{k-1,0} \\ 0 & 1 & \dots & 0 & p_{01} & p_{11} & \dots & p_{k-1,1} \\ . & . & & . & . & . & & . \\ . & . & & . & . & . & & . \\ . & . & & . & . & . & & . \\ 0 & 0 & \dots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \dots & p_{k-1,n-k-1} \end{bmatrix}$$

Example

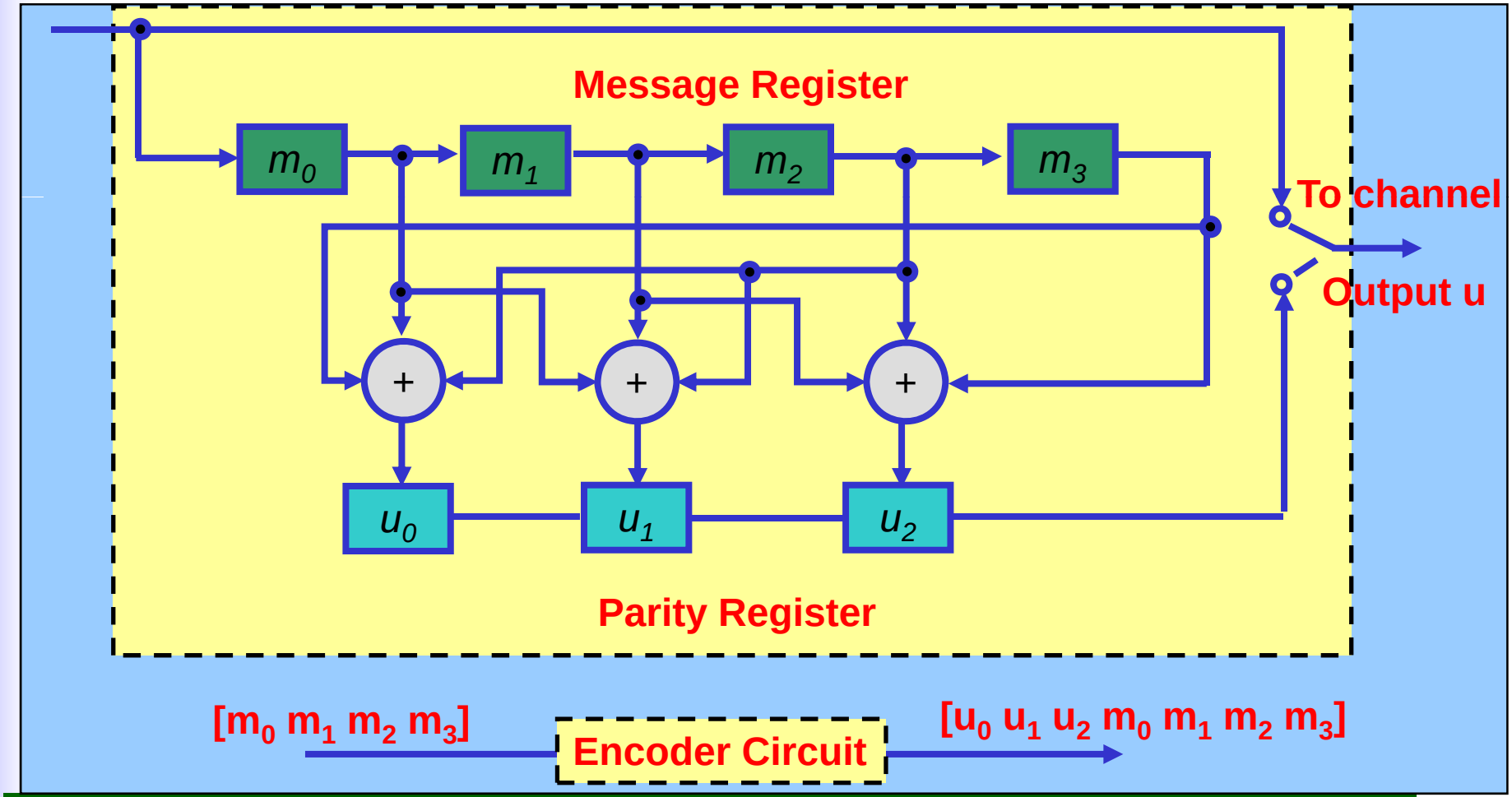
$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

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

Encoding Circuit

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

Input m

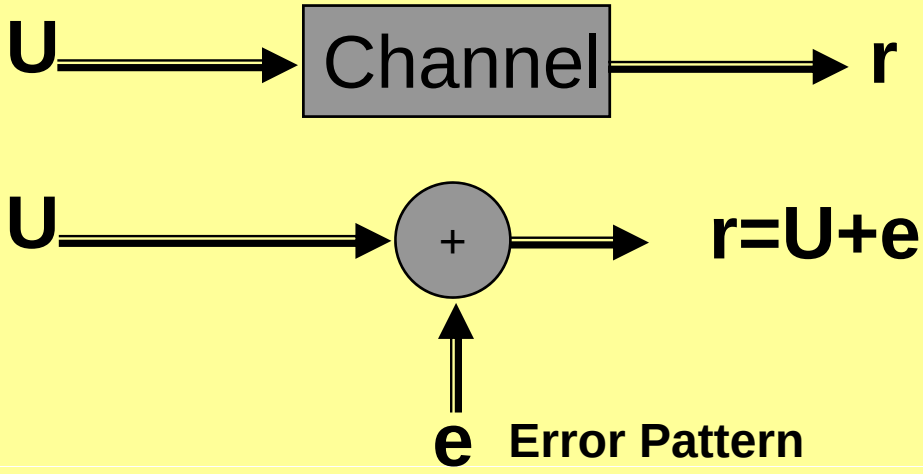


Syndrome

- Characteristic of parity check matrix (**H**)

$$r.H^T = 0 \Rightarrow r \in C$$

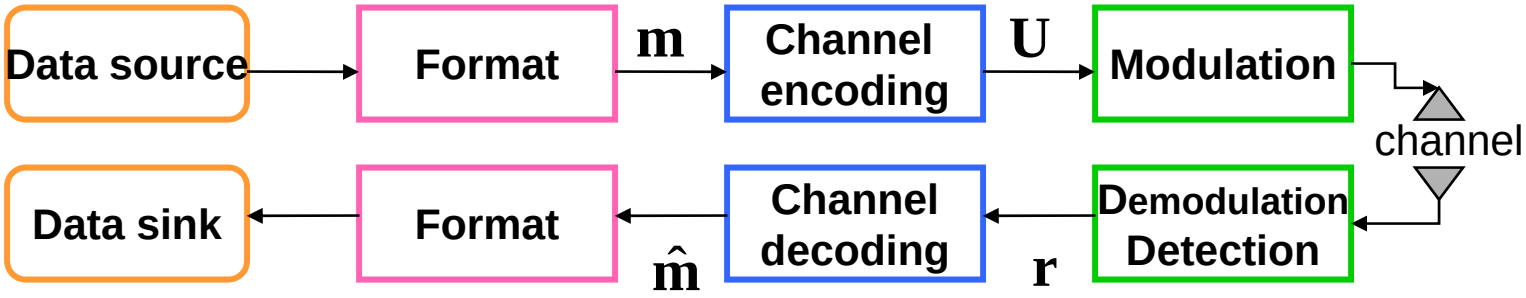
$$r.H^T \neq 0 \Rightarrow r \notin C$$



Syndrome

$$s = r.H^T$$

Linear block codes – cont'd



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

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

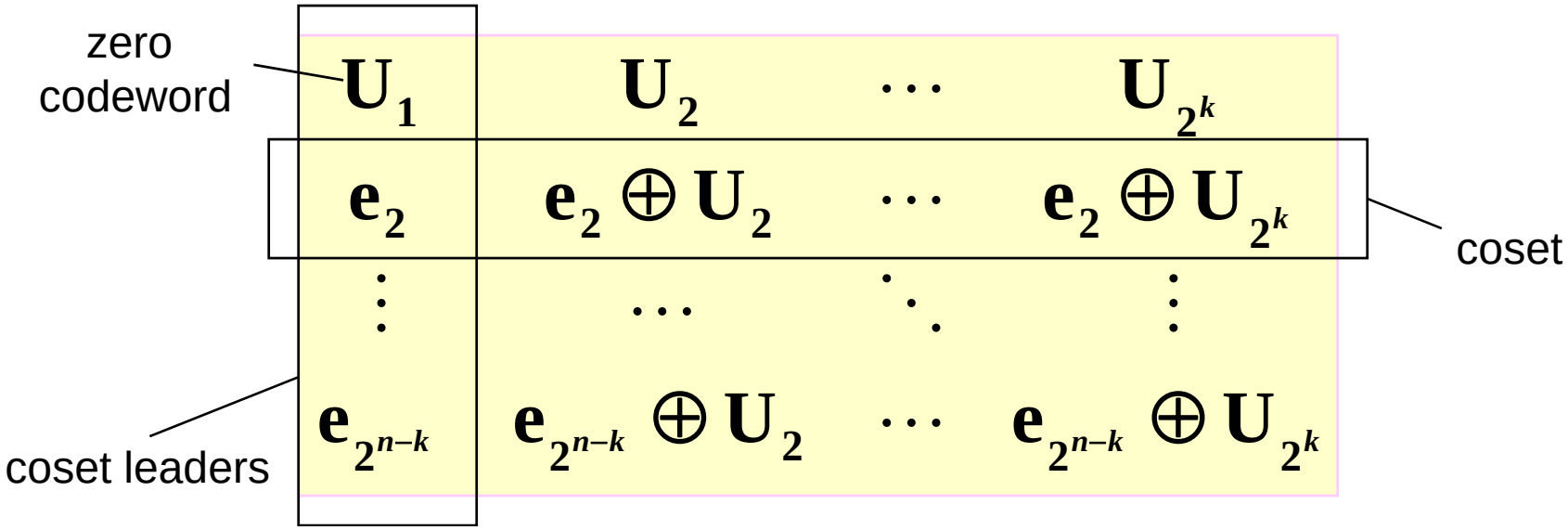
$\mathbf{e} = (e_1, e_2, ..., e_n)$ error pattern or vector

- 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
  - For row $i = 2,3,...,2^{n-k}$, find a vector in V_n of minimum weight which is not already listed in the array.
  - 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

codewords

000000	110100	011010	101110	101001	011101	110011	000111
000001	110101	011011	101111	101000	011100	110010	000110
000010	110111	011000	101100	101011	011111	110001	000101
000100	110011	011100	101010	101101	011010	110111	000110
001000	111100	⋮			⋮		⋮
010000	100100						
100000	010100				⋮		
010001	100101		…			…	010110

coset

Coset leaders

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:

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

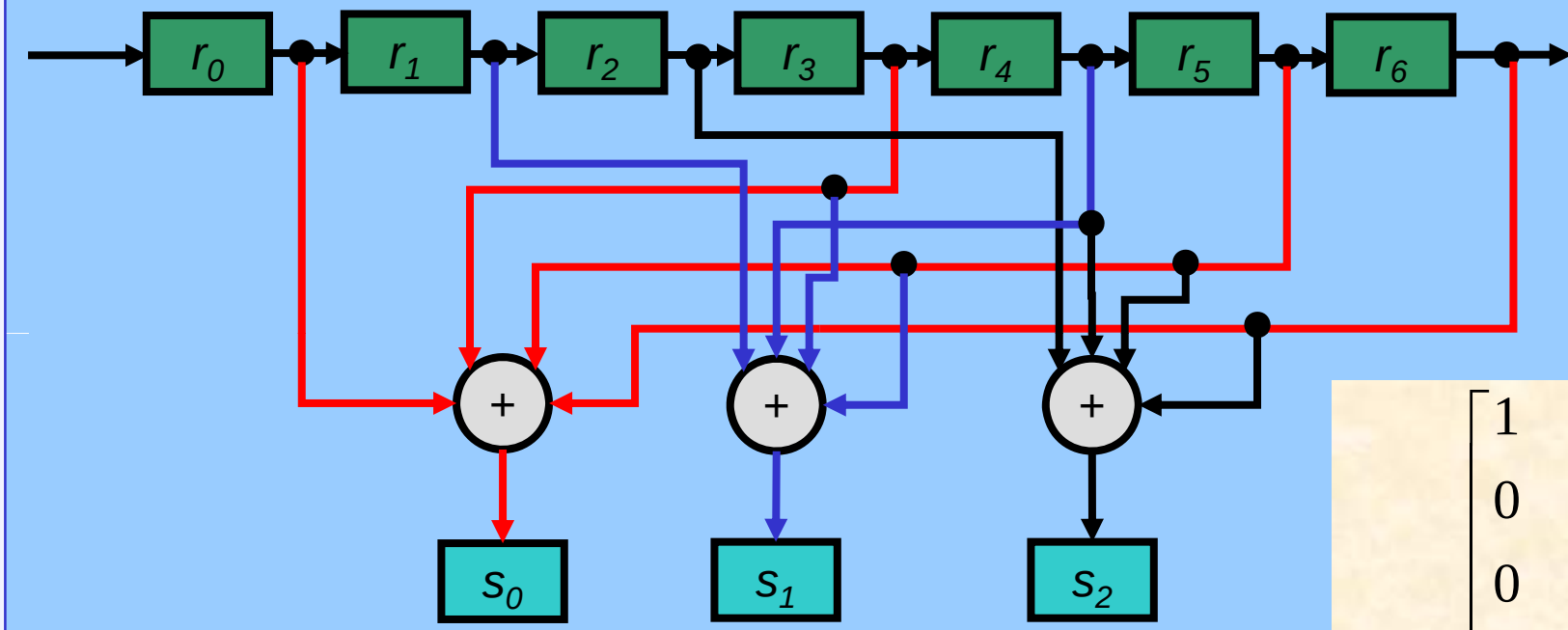
➡ Error pattern corresponding to this syndrome is

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

➡ The corrected vector is estimated

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

Syndrome Circuit



$$s_0 = r_0 + r_3 + r_5 + r_6$$

$$s_1 = r_1 + r_3 + r_4 + r_5$$

$$s_2 = r_2 + r_4 + r_5 + r_6$$

$$\mathbf{H}^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

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 :	$t = 1$

Richard Hamming

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

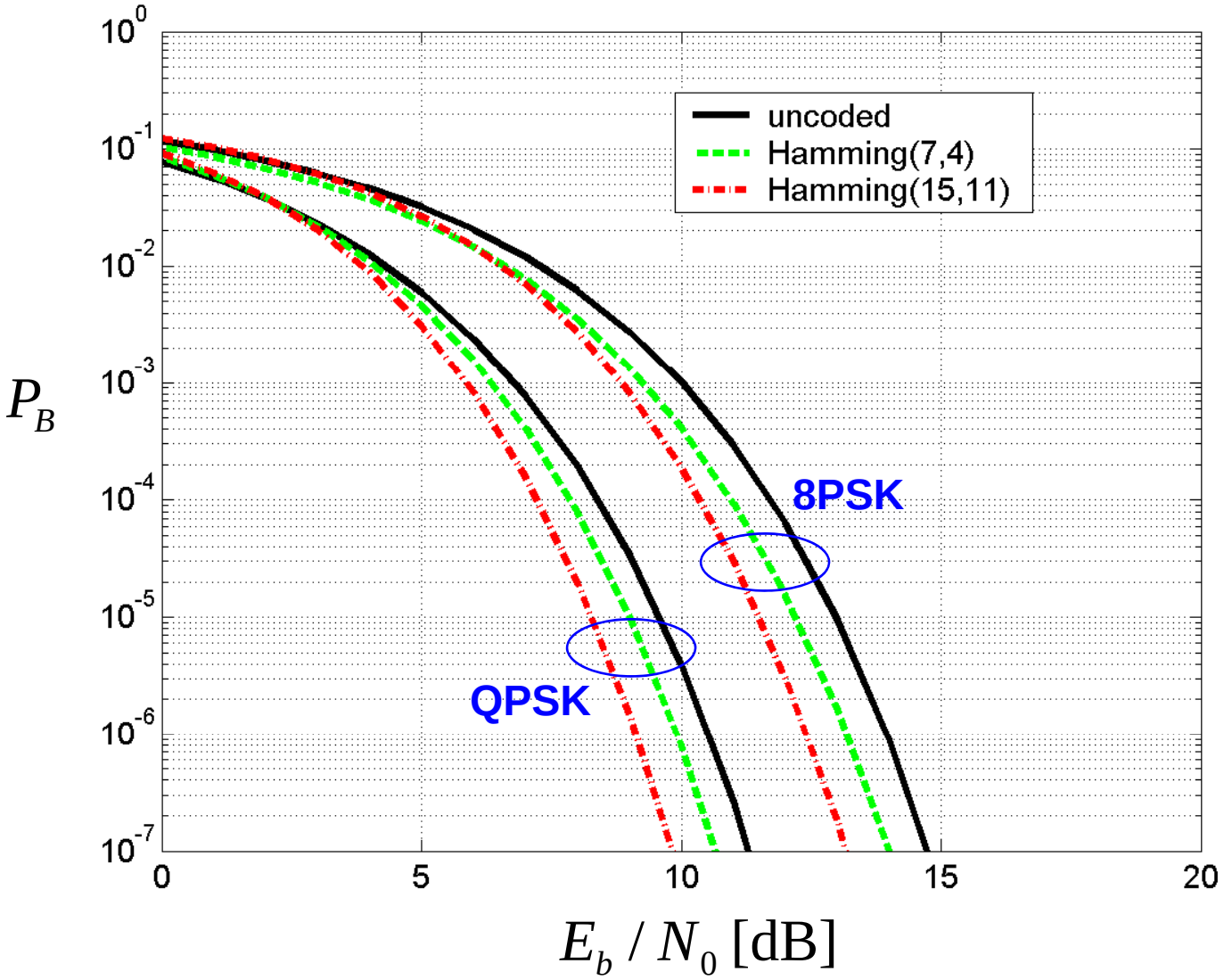
Hamming codes

- 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



Tugas, Dikumpulkan !

Consider a (7,4) code whose generator matrix is

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

1. Find all the codewords of the code.
2. What is the error-correcting capability of the code?
3. What is the error-detecting capability of the code?
4. Find **H**, the parity-check matrix of the code.
5. Construct the syndrome table for the code.
6. Compute the syndrome for the received vector 1 1 0 1 1 0 1. Is this a valid vector? If not, what was the most probable sent message?