Digital Communication

Channel coding, linear block codes, Hamming and cyclic codes

Lecture - 8

Ir. Muhamad Asvial, MSc., PhD

Center for Information and Communication Engineering Research (CICER)

Electrical Engineering Department - University of Indonesia

E-mail: asvial@ee.ui.ac.id

http://www.ee.ui.ac.id/cicer

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 <u>better</u> waveforms
  - Structured sequences: Transforming data sequences into <u>better</u> sequences, having structured redundancy.
    - “Better” in the sense of making the decision process less subject to errors.

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

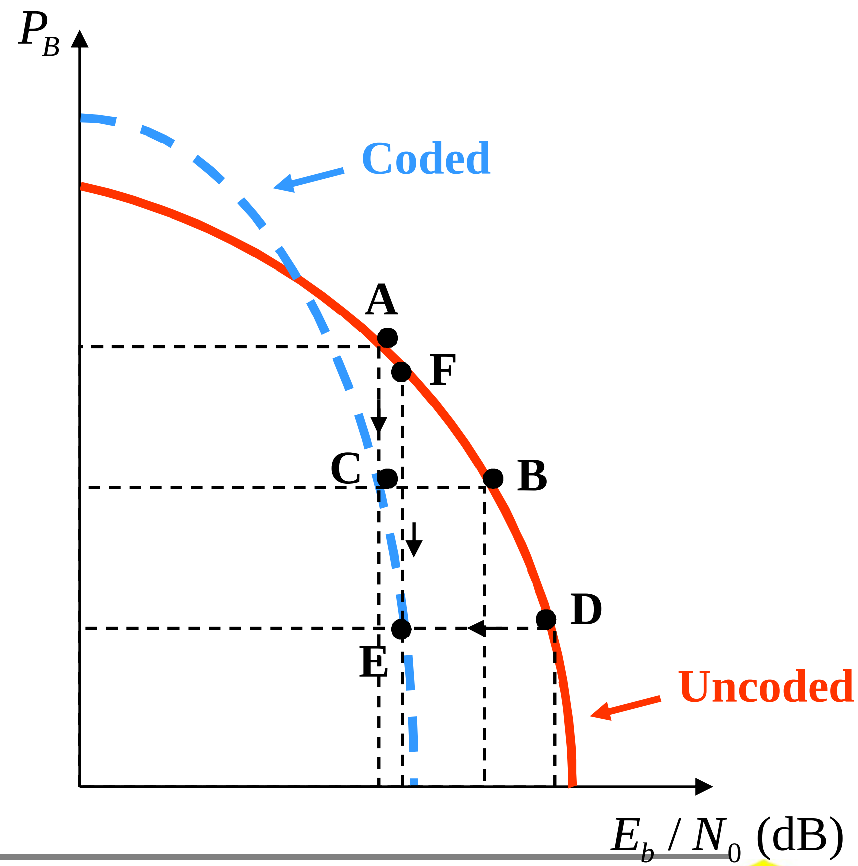
Why using error correction coding?

– 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/No 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

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 <u>field</u> 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".

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

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

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

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:

<u>Commutative:</u>

$$\forall \mathbf{u}, \mathbf{v} \in V \Rightarrow \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} \in F$$

<u>Distributive:</u>

$$\forall a \in F, \forall \mathbf{v} \in \mathbf{V} \Rightarrow a \cdot \mathbf{v} = \mathbf{u} \in \mathbf{V}$$

<u>Associative:</u>

$$(a+b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v} \quad \text{and} \quad a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$$

$$\forall a, b \in F, \forall \mathbf{v} \in V \Rightarrow (a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$$

$$\forall \mathbf{v} \in \mathbf{V},\ 1 \cdot \mathbf{v} = \mathbf{v}$$

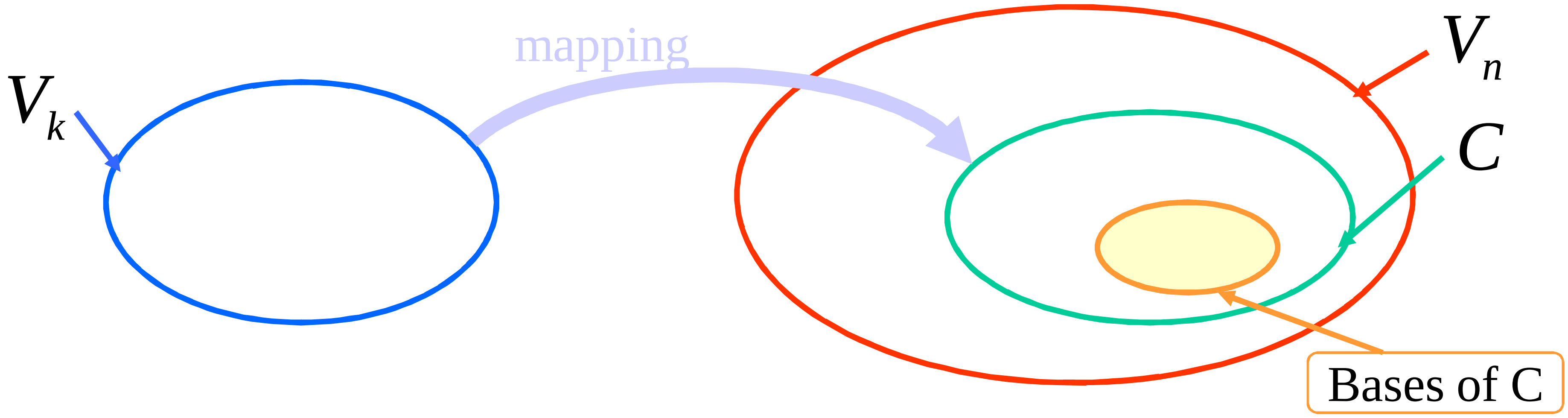
Linear block codes

- 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.

$$V_k \rightarrow C \subset V_n$$

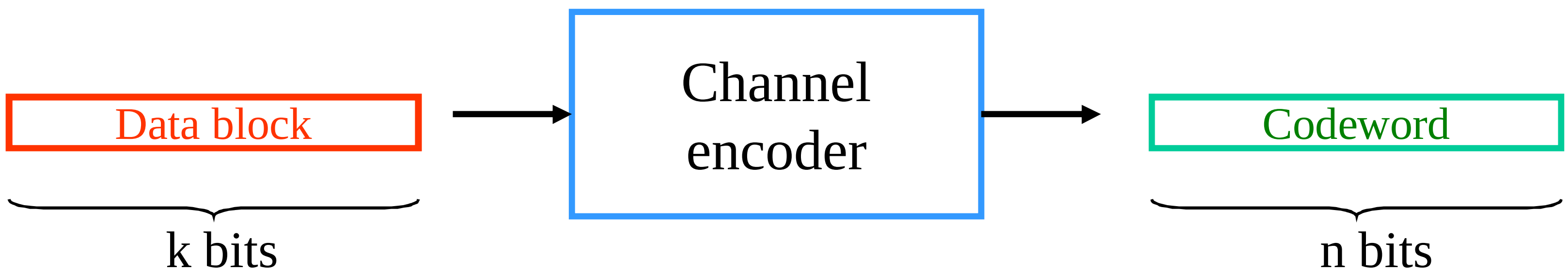
    - Members of C are called code-words.
    - The all-zero codeword is a codeword.
    - Any linear combination of code-words is a codeword.

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.



$n\text{-}k$ Redundant bits

$R_c = \dfrac{k}{n}$ 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.
- The minimum distance of a block code is

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

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

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

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

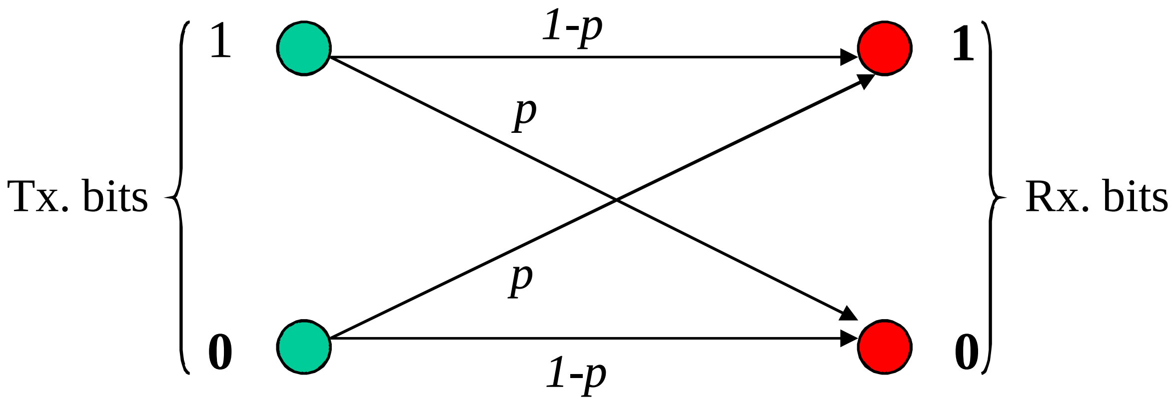
  - p is the transition probability or bit error probability over channel.

- 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

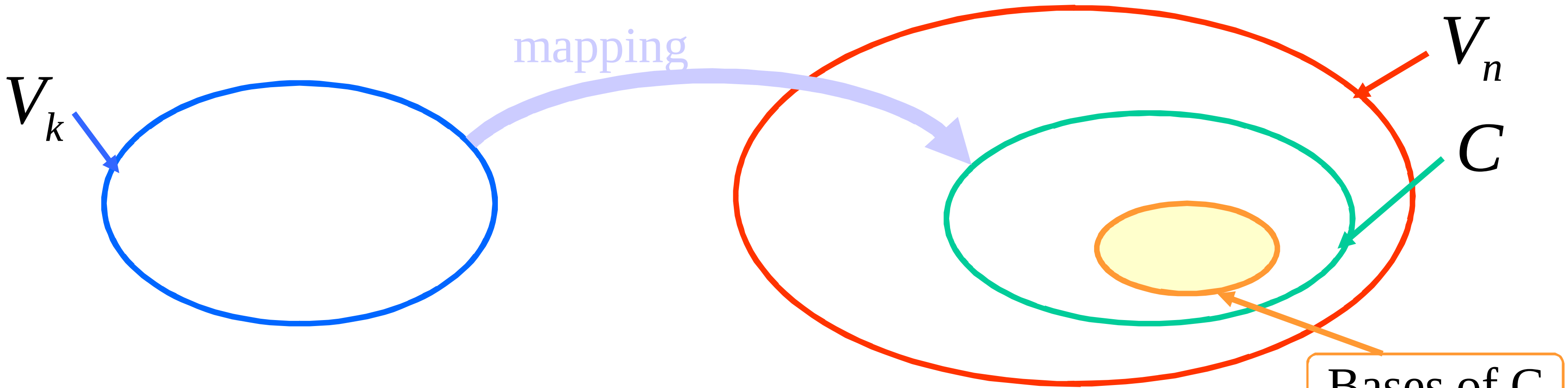


  – Note that for coded systems, the coded bits are modulated and transmitted over channel. For example, for M-PSK modulation on AWGN channels (M>2):

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

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

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

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

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

– 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

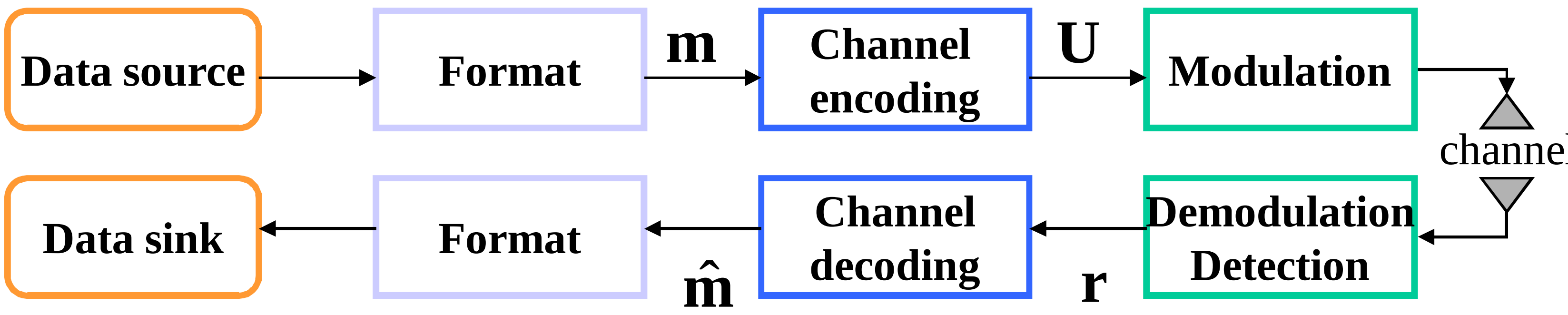
- For any linear code we can find an matrix $\mathbf{H}_{(n-k)\times n}$, which its rows are orthogonal to rows of $\mathbf{G}$:

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

- **H** is called the parity check matrix and its rows are linearly independent.
- For systematic linear block codes:

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

Linear block codes – cont'd



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

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

$\mathbf{e} = (e_1, e_2, \ldots., e_n)$ 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

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)

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

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

Cyclic block codes

- Cyclic codes are a subclass of linear block codes.
- Encoding and syndrome calculation are easily performed using feedback shift-registers.
  - Hence, relatively long block codes can be implemented with a reasonable complexity.
- BCH and Reed-Solomon codes are cyclic codes.

Cyclic block codes

- A linear (n,k) code is called a Cyclic code if all cyclic shifts of a codeword are also a codeword.

$$\boxed{\mathbf{U} = (u_0, u_1, u_2, \ldots, u_{n-1})}$$

"*i*" cyclic shifts of **U**

$$\boxed{\mathbf{U}^{(i)} = (u_{n-i}, u_{n-i+1}, \ldots, u_{n-1}, u_0, u_1, u_2, \ldots, u_{n-i-1})}$$

  – Example:

$$\mathbf{U} = (1101)$$

$$\mathbf{U}^{(1)} = (1110) \quad \mathbf{U}^{(2)} = (0111) \quad \mathbf{U}^{(3)} = (1011) \quad \mathbf{U}^{(4)} = (1101) = \mathbf{U}$$

Cyclic block codes

- Syndrome decoding for Cyclic codes:
  - Received codeword in polynomial form is given by

Received codeword

$$\mathbf{r}(X) = \mathbf{U}(X) + \mathbf{e}(X)$$

Error pattern

  - The syndrome is the reminder obtained by dividing the received polynomial by the generator polynomial.

$$\mathbf{r}(X) = \mathbf{q}(X)\mathbf{g}(X) + \mathbf{S}(X)$$

Syndrome

  - With syndrome and Standard array, error is estimated.
    - In Cyclic codes, the size of standard array is considerably reduced.

CICER

Example of the block codes