Digital Communications I: Modulation and Coding Course

Spring - 2015

Jeffrey N. Denenberg

Lecture 6: Linear Block Codes

Last time we talked about:

- Evaluating the average probability of symbol error for different bandpass modulation schemes

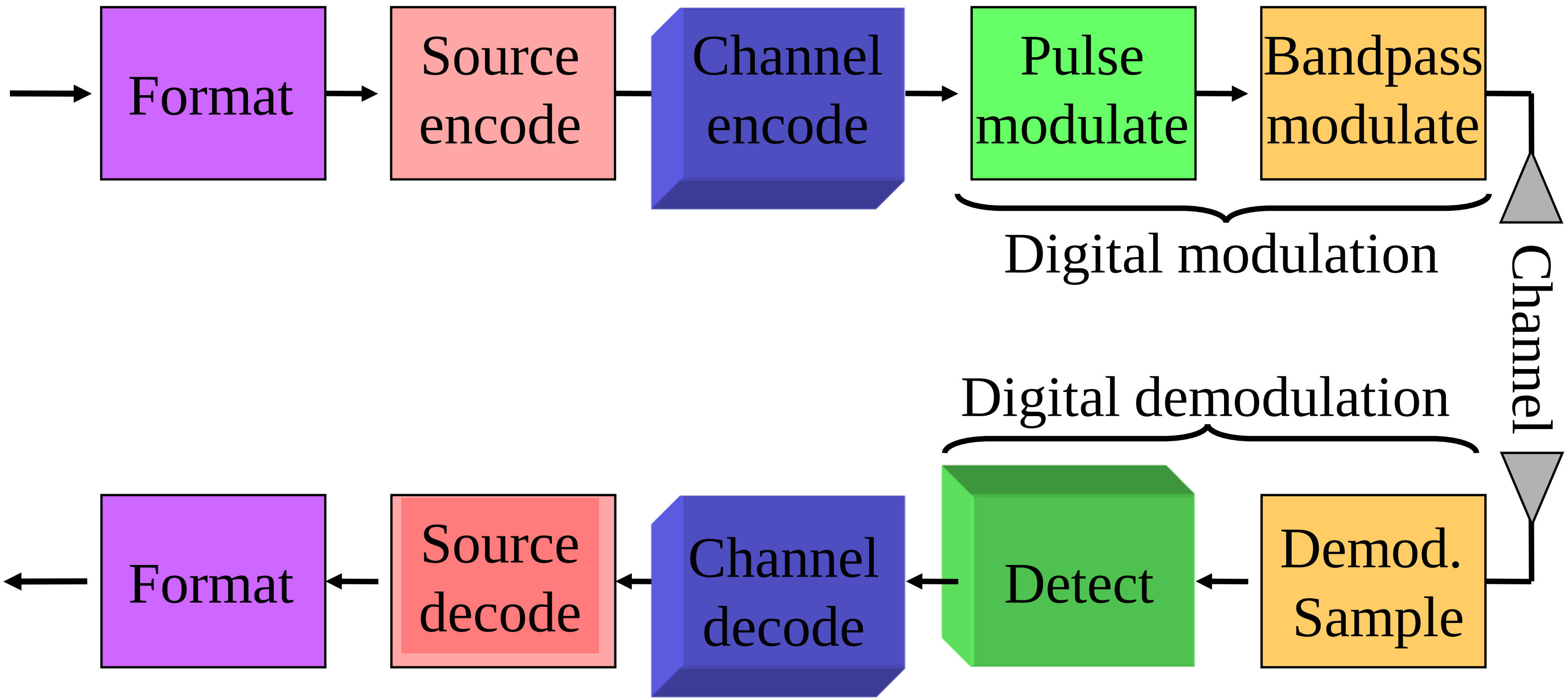
- Comparing different modulation schemes based on their error performances.

Today, we are going to talk about:

- Channel coding

- Linear block codes
  - The error detection and correction capability
  - Encoding and decoding
  - Hamming codes
  - Cyclic codes

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.

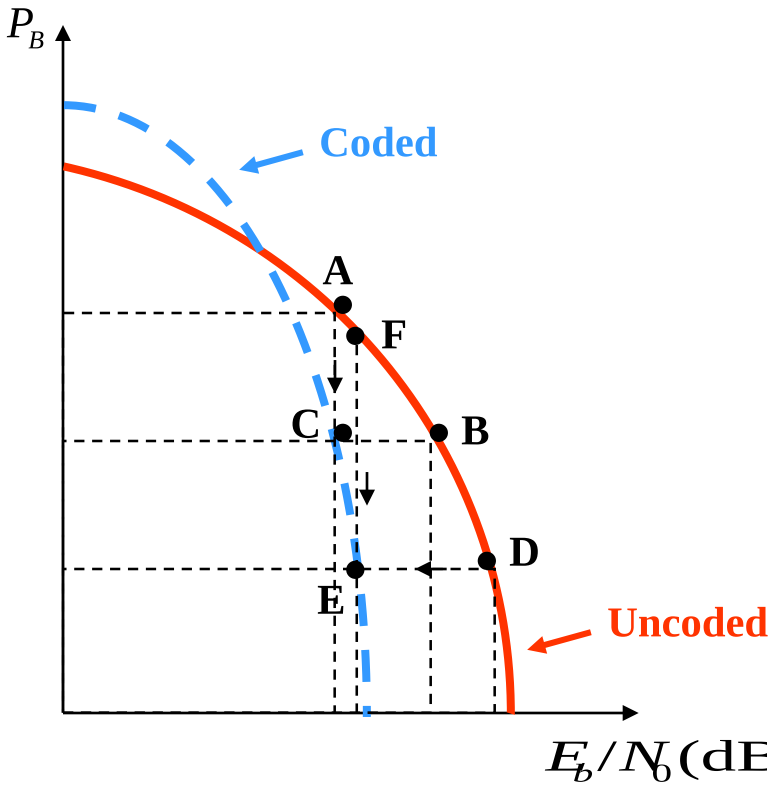
    -"Better" in the sense of making the decision process less subject to errors.

Error control techniques

- Automatic Repeat reQuest (ARQ)
  - Full-duplex connection, error detection codes
  - The receiver sends 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:

$$G\,[\text{dB}] = \left(\frac{E_b}{N_0}\right)_u [\text{dB}] - \left(\frac{E_b}{N_0}\right)_c [\text{dB}]$$

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 that 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…

- **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".

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

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

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

    1. The operations "+" and "." are distributive:

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

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

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:

$$\{(0000), (0101), (1010), (1111)\} \text{ is a subspace of } V_4.$$

Some definitions…

- Spanning set:
  - A collection of vectors $G = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$, is said to be a <u>spanning set</u> for *V* or to <u>span</u> *V* if

    linear combinations of the vectors in *G* include all vectors in the vector space *V*,
    - Example:

    $$\{(1000),(0110),(1100),(0011),(1001)\} \text{ spans } V_4.$$
- Bases:
  - The spanning set of V that has minimal cardinality is called the basis for V.
    - Cardinality of a set is the number of objects in the set.
    - Example:

    $$\{(1000),(0100),(0010),(0001)\} \text{ is a basis for } V_4.$$

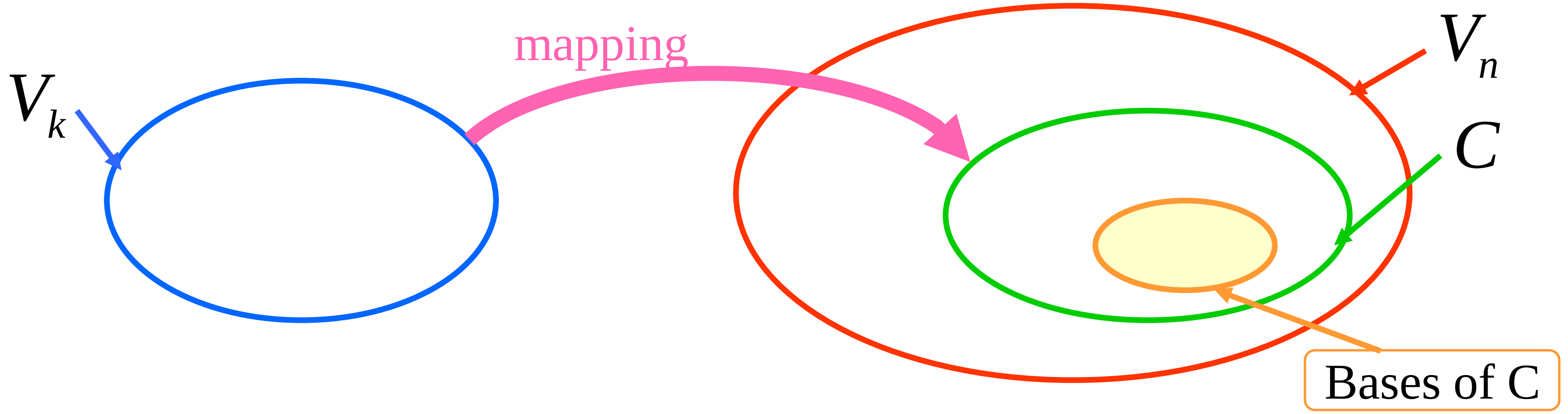
Linear block codes

- 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.

$$\boxed{V_k \to C \subset V_n}$$

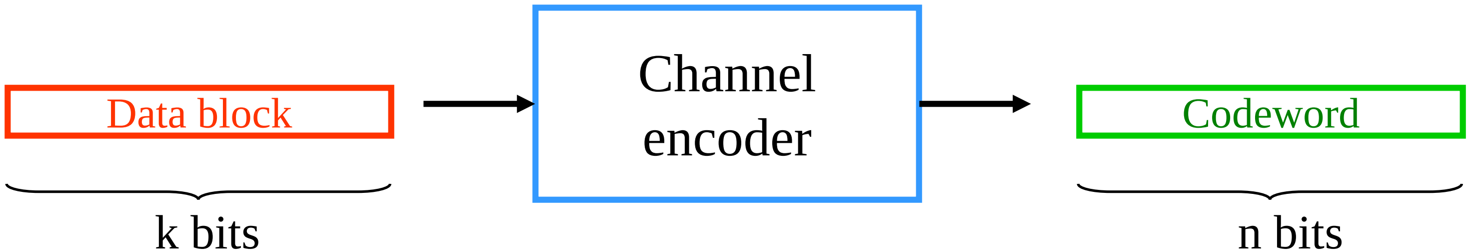
    - Members of C are called code-words.
    - The all-zero codeword is a codeword.
    - Any linear combination of code-words is a codeword.

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 the channel.
- The reverse procedure is done at the receiver.



$n-k$ Redundant bits

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

Linear block codes – cont'd

- The Hamming weight of the 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 is defined as the maximum number of guaranteed correctable errors per codeword, that 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

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

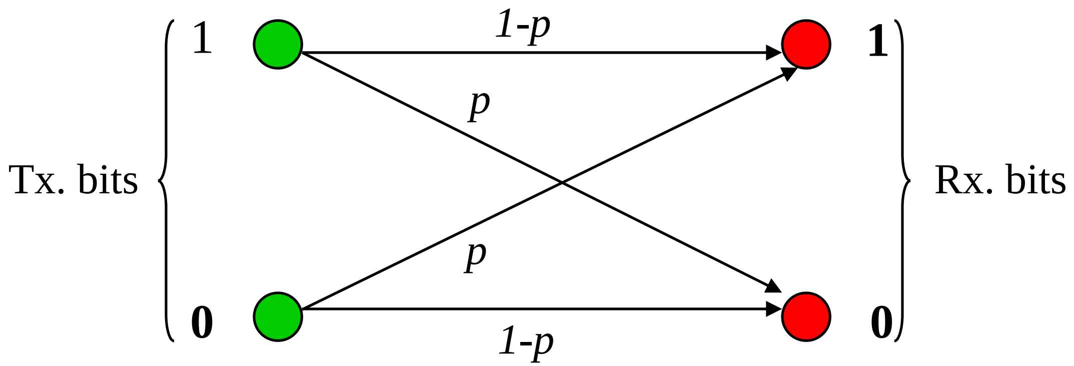
  - p is the transition probability or bit error probability over channel.

- 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

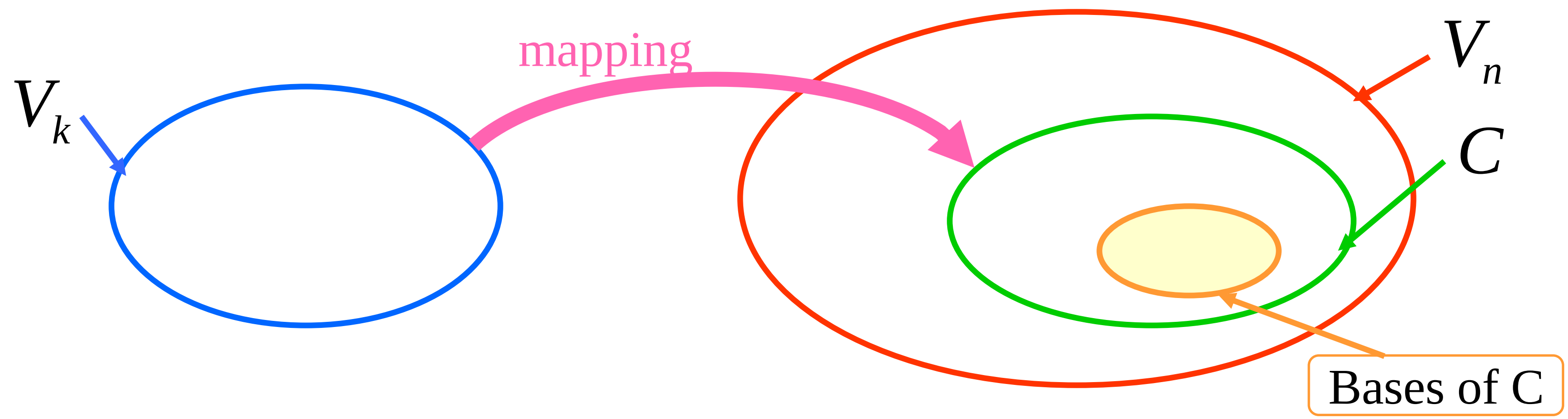


- Note that for coded systems, the coded bits are modulated and transmitted over the channel. For example, for M-PSK modulation on AWGN channels (M>2):

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

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 of 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

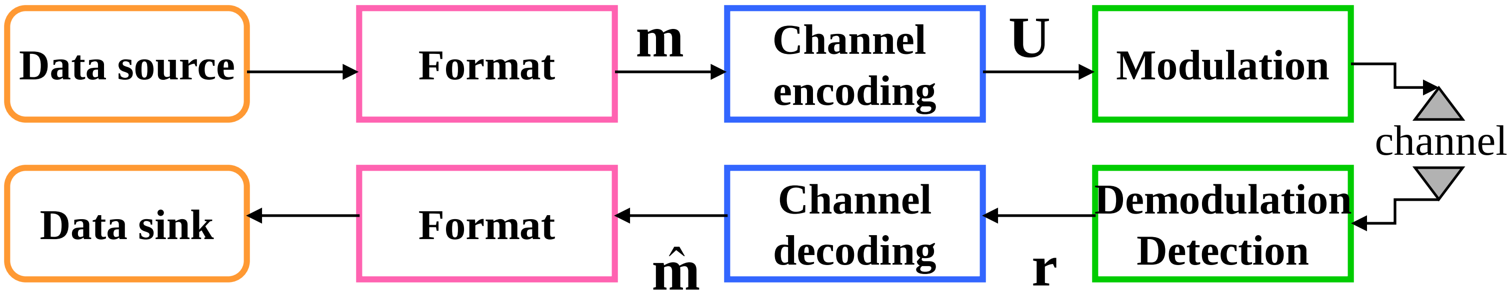
- For any linear code we can find a matrix $\mathbf{H}_{(n-k)\times n}$, such that its rows are orthogonal to the rows of $\mathbf{G}$:

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

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

zero codeword

$$\begin{array}{cccc}
\mathbf{U}_1 & \mathbf{U}_2 & \cdots & \mathbf{U}_{2^k} \\
\mathbf{e}_2 & \mathbf{e}_2 \oplus \mathbf{U}_2 & \cdots & \mathbf{e}_2 \oplus \mathbf{U}_{2^k} \\
\vdots & \cdots & \ddots & \vdots \\
\mathbf{e}_{2^{n-k}} & \mathbf{e}_{2^{n-k}} \oplus \mathbf{U}_2 & \cdots & \mathbf{e}_{2^{n-k}} \oplus \mathbf{U}_{2^k}
\end{array}$$

coset

coset leaders

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 the 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 $\hat{\mathbf{e}} = \mathbf{e}$, the 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	$\vdots$			$\vdots$		$\vdots$
010000	100100						
100000	010100				$\vdots$		
010001	100101		$\cdots$			$\cdots$	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

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

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 codewords.

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

"$\boldsymbol{i}$" 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

- Algebraic structure of Cyclic codes, implies expressing codewords in polynomial form

$$\boxed{\mathbf{U}(X) = u_0 + u_1 X + u_2 X^2 + \ldots + u_{n-1} X^{n-1} \qquad \text{degree}(n\text{-}1)}$$

- Relationship between a codeword and its cyclic shifts:

$$X\mathbf{U}(X) = u_0 X + u_1 X^2 + \ldots, u_{n-2} X^{n-1} + u_{n-1} X^n$$

$$= \underbrace{u_{n-1} + u_0 X + u_1 X^2 + \ldots + u_{n-2} X^{n-1}}_{\mathbf{U}^{(1)}(X)} + \underbrace{u_{n-1} X^n + u_{n-1}}_{u_{n-1}(X^n + 1)}$$

$$= \mathbf{U}^{(1)}(X) + u_{n-1}(X^n + 1)$$

  - Hence:

$$\mathbf{U}^{(1)}(X) = X\mathbf{U}(X) \text{ modulo}(X^n + 1)$$

By extension

$$\boxed{\mathbf{U}^{(i)}(X) = X^i \mathbf{U}(X) \text{ modulo}(X^n + 1)}$$

Cyclic block codes

- Basic properties of Cyclic codes:
  - Let C be a binary (n,k) linear cyclic code
    1. Within the set of code polynomials in C, there is a unique monic polynomial $\mathbf{g}(X)$ with minimal degree $r<n$. $\mathbf{g}(X)$ is called the generator polynomial.
       $$\mathbf{g}(X) = g_0 + g_1 X + \ldots + g_r X^r$$
    1. Every code polynomial $\mathbf{U}(X)$ in C can be expressed uniquely as $\mathbf{U}(X) = \mathbf{m}(X)\mathbf{g}(X)$
    2. The generator polynomial $\mathbf{g}(X)$ is a factor of
       $X^n + 1$

Cyclic block codes

- The orthogonality of **G** and **H** in polynomial form is expressed as $\mathbf{g}(X)\mathbf{h}(X) = X^n + 1$. This means $\mathbf{h}(X)$ is also a factor of $X^n + 1$

1. The row $i, i = 1,\ldots,k$, of the generator matrix is formed by the coefficients of the "$i-1$" cyclic shift of the generator polynomial.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}(X) \\ X\mathbf{g}(X) \\ \vdots \\ X^{k-1}\mathbf{g}(X) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & & & & \mathbf{0} \\ & g_0 & g_1 & \cdots & g_r & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & g_0 & g_1 & \cdots & g_r & \\ \mathbf{0} & & & & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

Cyclic block codes

- Systematic encoding algorithm for an (n,k) Cyclic code:

1. Multiply the message polynomial $\mathbf{m}(X)$ by X^{n-k}

1. Divide the result of Step 1 by the generator polynomial $\mathbf{g}(X)$. Let $\mathbf{p}(X)$ be the reminder.

1. Add $\mathbf{p}(X)$ to $X^{n-k}\mathbf{m}(X)$ to form the codeword $\mathbf{U}(X)$

Cyclic block codes

- **Example:** For the systematic (7,4) Cyclic code with generator polynomial $\mathbf{g}(X) = 1 + X + X^3$
  1. Find the codeword for the message $\mathbf{m} = (1011)$

$$n = 7, \quad k = 4, \quad n - k = 3$$

$$\mathbf{m} = (1011) \Rightarrow \mathbf{m}(X) = 1 + X^2 + X^3$$

$$X^{n-k}\mathbf{m}(X) = X^3\mathbf{m}(X) = X^3(1 + X^2 + X^3) = X^3 + X^5 + X^6$$

Divide $X^{n-k}\mathbf{m}(X)$ by $\mathbf{g}(X)$:

$$X^3 + X^5 + X^6 = \underbrace{(1 + X + X^2 + X^3)}_{\text{quotient } \mathbf{q}(X)}\underbrace{(1 + X + X^3)}_{\text{generator } \mathbf{g}(X)} + \underbrace{1}_{\text{remainder } \mathbf{p}(X)}$$

Form the codeword polynomial :

$$\boxed{\begin{aligned} &\mathbf{U}(X) = \mathbf{p}(X) + X^3\mathbf{m}(X) \\ &\mathbf{U} = (\underbrace{1\ 0\ 0}_{\text{parity bits}}\quad \underbrace{1\ 0\ 1\ 1}_{\text{message bits}}) \end{aligned}}\mathbf{U}(X) = 1 + X^3 + X^5 + X^6$$

Cyclic block codes

- Find the generator and parity check matrices, **G** and **H**, respectively.

$$\mathbf{g}(X) = 1 + 1 \cdot X + 0 \cdot X^2 + 1 \cdot X^3 \Rightarrow (g_0, g_1, g_2, g_3) = (1101)$$

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

Not in systematic form.
We do the following:

- $\text{row}(1) + \text{row}(3) \rightarrow \text{row}(3)$
- $\text{row}(1) + \text{row}(2) + \text{row}(4) \rightarrow \text{row}(4)$

$$\mathbf{G} = \begin{bmatrix} \underbrace{\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{matrix}}_{\mathbf{P}} & \vdots & \underbrace{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}}_{\mathbf{I}_{4\times 4}} \end{bmatrix}$$

$$\mathbf{H} = \begin{bmatrix} \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{\mathbf{I}_{3\times 3}} & \vdots & \underbrace{\begin{matrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{matrix}}_{\mathbf{P}^T} \end{bmatrix}$$

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 remainder 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, the error is estimated.
    - In Cyclic codes, the size of standard array is considerably reduced.

Example of the block codes