ECSE 308 Notes

Me

October 16, 2022

Contents

1 Chapter A 3

2 Chapter B 4
- 2.1 B1 Signal Sizes . . . 4
- 2.2 B2 LTI Channel . . . 6
  - 2.2.1 Channel Response Equations . . . 7
  - 2.2.2 Constant Gain and Group Delay . . . 8
  - 2.2.3 Equalizer Function . . . 8
  - 2.2.4 Noise and Filtering . . . 8
- 2.3 B3 Analog Modulation . . . 10
  - 2.3.1 DSB-LC AM . . . 10
  - 2.3.2 DSB-SC AM . . . 11
  - 2.3.3 SSB-SC AM . . . 12
  - 2.3.4 FM . . . 12
  - 2.3.5 PM . . . 13
- 2.4 B4 Digital Modulation . . . 14
- 2.5 B5 ISI and AWGN . . . 15

3 Chapter C Notes 16
- 3.1 C1 Parity Check . . . 16
- 3.2 C2 Internet Checksum . . . 17
- 3.3 C3 Linear Codes . . . 19
  - 3.3.1 Introduction to Hamming Weights . . . 19
- 3.4 C4 Linear Codes (Generator) . . . 22

3.5 Arithmetic in GF(2) . . . 25
3.5.1 Multiplication of Polynomials in GF(2) . . . 25
3.5.2 Long Division of Polynomials in GF(2) . . . 25
3.6 Cyclic Redundancy Check . . . 26
3.7 ARQ and FEC . . . 28
3.8 Coding Gain in AWGN Channel . . . 29
3.9 Chapter C Exercises . . . 30
3.9.1 Problem C1 . . . 30
3.9.2 Problem C2 . . . 31
3.9.3 Problem C3 . . . 32
3.9.4 Problem C4 . . . 34
3.9.5 Problem C5 . . . 35
3.9.6 Problem C6 . . . 36
3.9.7 Problem C7 . . . 37
3.9.8 Problem C8 . . . 38

1 Chapter A

2 Chapter B

2.1 B1 Signal Sizes

We begin with mathematical definitions.

Definition. Energy of a signal $x(t) \iff \mathbf{X(f)}$ is a non-negative quantity,

$$E_x = \int |x|^2 dt = \|x\|_2^2$$
$$E_x = \int |\mathbf{X}|^\mathbf{2} \mathbf{df} = \|\mathbf{X}\|_\mathbf{2}^\mathbf{2}$$

It has units of J.

Definition. Power Spectral Density of a signal $x(t) \iff \mathbf{X(f)}$ is a function,

$$P_\mathbf{X} : \Omega \to \mathbb{R}, \quad P_\mathbf{X}(f) = \lim_{d\to\infty} \frac{|\mathbf{X}_d(f)|^2}{d}$$

where $\mathbf{X}_d(f) = \mathcal{F}\left\{x(t)\chi_{\left[-\frac{d}{2},+\frac{d}{2}\right]}\right\}$. $P_\mathbf{X}$ has units W/Hz. Other names are:

- Power Spectrum, and
- Signal Power distribution in the frequency domain.

Definition. Energy Spectral Density of a signal $x(t) \iff \mathbf{X}(f)$ is a function,

$$|\mathbf{X}(f)|^2 : \Omega \to \mathbb{R},$$

It has units J/Hz. Other names are:

- Energy Spectrum, and
- Signal energy distribution in the frequency domain.

Definition. Power of a signal $x(t) \iff \mathbf{X(f)}$ is a quantity

$$P_x = \lim_{d\to\infty} d^{-1} \int |x(t)|^2 \chi_{\left[-\frac{d}{2},+\frac{d}{2}\right]} dt$$

$$P_x = \int P_\mathbf{X} df = \int \lim_{d\to\infty} \frac{|\mathbf{X}_d(f)|^2}{d} df$$

For a sinusoid in $x(t) = A\cos(2\pi f_c t + \theta)$, $P_x = A/2$. It has units of W.

Remark. One should not conflate Power with Power Spectral Density, one is a quantity and the other is a function.

An alternate characterisation of the Power of a signal would be to use the average function for some $|x(t)|^2 \in L^1_{loc}$

$$P_x = \lim_{r\to\infty} A_r(x(0)) = \frac{1}{m(B(r,0))}\int_{B(r,0)} |x(t)|^2 dt$$

Definition. The absolute bandwidth B of a signal is

$$\mu(\text{supp}\,(S(f)) \cap \mathbb{R}^+) = \mu\left(\bigcap\{[a,b],\, 0 \le a \le b,\, \text{supp}\,(S(f) \subseteq [a,b])\}\right)$$

Definition. If the smallest closed interval that contains $\text{supp}\,(S(f)) \cap \mathbb{R}^+$ is given by $[f_1, f_2]$, then the center frequency f_0 of $s(t)$ is

$$f_0 = (f_2 - f_1)/2$$

Definition. A bandlimited signal is one with compact support in the frequency domain. In symbols, $\mathbf{X}(f) \in C_c(\Omega)$.

Definition. A strictly bandlimited, real-valued signal is called a baseband signal if and only if $f_0 = 0$.

What to Remember.

2.2 B2 LTI Channel

Fix an LTI-channel, with transfer function $H(f)$, where f is given in Hertz. We are concerned mostly about its response to sinusoids, so we require the Fourier Transform only. Below are the relationships between an input $\mathbf{X}(f)$ and $\mathbf{Y}(f)$.

1. Amplitude relationship (in the time-domain and frequency domain)

$$y(t) = h(t) * x(t)$$

$$\mathbf{Y}(f) = \mathbf{H}(f) \cdot \mathbf{X}(f)$$

2. Energy Spectral Densities (in the frequency domain)

$$|\mathbf{Y}(f)|^2 = |\mathbf{H}(f)|^2 \cdot |\mathbf{X}(f)|^2$$

3. Power Spectral Densities (in the frequency domain)

$$P_{\mathbf{y}}(f) = |\mathbf{H}(f)|^2 \cdot P_{\mathbf{X}}(f)$$

We will hereinafter refer to the transfer function of the LTI channel as 'the LTI channel $\mathbf{H}(f)$' and use those two terms interchangably. We state some characterizations of the transfer function $\mathbf{H}(f)$:

1. Polar decomposition

$$\mathbf{H}(f) = |\mathbf{H}(f)|e^{j\theta(f)}, \quad \theta(f) \coloneqq \angle(\mathbf{H}(f))$$

2. Gain of the channel, or the magnitude response $|\mathbf{H}(f)|$,
3. Phase of the channel, or the phase response $\theta(f)$,
4. Group delay at frequency f,

$$\tau(f) \coloneqq \frac{1}{2\pi}\frac{d\theta(f)}{df}$$

5. Relative channel magnitude attenuation at frequency f,

$$|\mathbf{H}(f)|_{dB}^{-1} = -20\log_{10}|\mathbf{H}(f)|$$

2.2.1 Channel Response Equations

Let us agree to make the following definitions

- $s(t)$: transmitted signal,
- $r(t)$: received signal,
- $\mathbf{H}(f)$: transfer function of LTI channel
- $h(t)$: normalized impulse response to channel
- $i(t)$: additive interference
- $n(t)$: additive noise
- a: attenuation (assumed to be a constant), in addition to channel attenuation
- $r_0(t)$ interference, noise free received component

Equations in the time-domain

$$r(t) = r_0(t) + i(t) + n(t) \tag{1}$$

$$r_0(t) = a^{-1}h(t) * s(t) \tag{2}$$

Likewise in the frequency domain

$$\mathbf{R}(f) = \mathbf{R}_0(f) + \mathbf{I}(f) + \mathbf{N}(f) \tag{3}$$

$$\mathbf{R}_0(f) = a^{-1}\mathbf{H}(f) \cdot \mathbf{S}(f) \tag{4}$$

Combining the two equations, we get

$$r(t) = a^{-1}ht(t) * s(t) + i(t) + n(t) \tag{5}$$

$$\mathbf{R}(f) = a^{-1}\mathbf{H}(f) \cdot \mathbf{S}(f) + \mathbf{I}(f) + \mathbf{N}(f) \tag{6}$$

2.2.2 Constant Gain and Group Delay

Let us consider a real-valued, strictly bandlimited, signal $s(t)$, and a channel $\mathbf{H}(f)$. Suppose that $[f_1, f_2]$ is a closed interval that contains $\mathbf{supp}\,(S(f)) \cap \mathbb{R}^+$, and $|\mathbf{H}(f)| = 1$, and $\tau(f) = \tau_0$ on $[f_1, f_2]$. Then,

$$\tau(f) = \tau_0 = \frac{1}{2\pi}\frac{d}{df}\theta(f) \implies \theta(f) = 2\pi\tau_0 f$$

Writing $\mathbf{H}(f)$ in polar form yields

$$\mathbf{R}_0(f) = a^{-1}|\mathbf{H}(f)|e^{j2\pi\tau_0 f}S(f)$$

Therefore, the interference, noise-free component only suffers from constant attenuation without distortion. If the group delay were not a constant on $[f_1, f_2]$, then a distorted version of $s(t)$ will be received.

$$r_0(t) = a^{-1}s(t + \tau_0)$$

2.2.3 Equalizer Function

If indeed that $\mathbf{H}(f)$ has a non-constant group-delay on $[f_1, f - 2]$, then we can 'undo' the channel response by applying another LTI filter in the form of $\mathbf{Q}(f)$, define

$$\mathbf{Q}(f) = \frac{bae^{j2\pi f\tau'}}{H(f)}$$

Notice the original transfer function $\mathbf{H}(f)$ at the denominator, and the attenuation is undone by a gain factor of a. An ideal equalizer only introduces additional delay in τ' (see the numerator). Applying one $\mathbf{Q}(f)$ after $\mathbf{H}(f)$, we get the new effective transfer function

$$\mathbf{QH}(f) = be^{j2\pi f\tau')} \implies s'(t) = bs(t + \tau')$$

Which just delays the signal by τ' and applies a gain of b.

2.2.4 Noise and Filtering

The ideal bandpass filter has constant group delay of d_F (delay of the filter) over $B = [f_1, f_2]$, and its amplitude response is just the indicator function on B.

$$|\mathbf{B}_F(f)| = \chi_B$$

If we apply $\mathbf{B}_F(f)$ onto $\mathbf{N}(f)$ and $\mathbf{I}(f)$, we can filter out the out of band interference and noise.

Consider the following equations onto the noise-interference free component:

$$\mathbf{R}_{oF}(f) = \mathbf{R}_o(f)\mathbf{B}_F(f) = a^{-1}\mathbf{R}_0(f)e^{j2\pi f d_F} \tag{7}$$

$$r_{oF}(t) = a^{-1}r_o(t + d_F) \tag{8}$$

The effects on the $\mathbf{N}(f)$ and $\mathbf{I}(f)$ hold no surprises,

- $\mathbf{N}_F(f)$ vanishes outside $[f_1, f_2]$
- $\mathbf{I}_F(f)$ vanishes outside $[f_1, f_2]$

What to Remember.

2.3 B3 Analog Modulation

We will discuss three main modulation techniques, namely

1. Amplitude Modulation (AM),
2. Phase Modulation (PM), and
3. Frequency Modulation (FM)

Let us agree to define $m(t) \iff \mathbf{S}(f)$ as some real-valued, strictly bandlimited, baseband signal. And our carrier wave $A_c \cos 2\pi f_c t$ at carrier frequency f_cHz.

Definition. Coherent Demodulation is when the demodulator requires a reference signal which has exactly the same frequency and phase as the carrier signal.

2.3.1 DSB-LC AM

Transmitted Signal

$$s_{LC}(t) = A_c\Big(1 + km(t)\Big)\cos(2\pi f_c t) \tag{9}$$

$$\mathbf{S}_{LC}(f) = \frac{A_c}{2}\Big[\delta(f - f_c) + \delta(f + f_c)\Big] + \frac{kA_c}{2}\Big[\mathbf{M}(f - f_c) + \mathbf{M}(f + f_c)\Big] \tag{10}$$

Modulation Considerations

- k is chosen such that $1 + km(t) \geq 0$ for all $t \geq 0$ to prevent phase reversal,
- AM Modulation index: $\phi = -km_{min} \leq 1$,
- Percentage Modulation: 100ϕ,
- Under/Over-modulation $\phi < 1$ or $\phi > 1$

Power efficiency

- The unmodulated carrier component has power

$$P_c = \frac{A_c^2}{2}$$

- The information signal power,

$$P_s = \frac{(kA_c)^2}{2} \int |m(t)|^2 dt$$

- The required power,

$$P_t = P_c + P_s$$

- It can be shown that assuming that $m(t)$ is a sinusoid, then the information signal power is bounded above by

$$P_s \leq \frac{1}{3} P_t$$

  (Waste power bad!)

What to Remember (DSB-LC AM).

1. Simple and Robust
2. Envelope Detection, does not require coherent demodulation.
3. Bandwidth: $m(t)$ has bandwidth W,then $s_{LC}(t)$ will require $2W$ bandwidth,
4. Low POWER efficiency, because of unmodulated carrier component
5. Bandwidth Overlapping: Require $W \ll f_c$.
6. Within AWGN channel, provides better SNR than DSB-SC, SSB-SC.

2.3.2 DSB-SC AM

Transmitted Signal

$$s_{SC}(t) = A_c k m(t) \cos(2\pi f_c t) \tag{11}$$

$$\mathbf{S}_{SC}(f) = \frac{kA_c}{2} \Big[\mathbf{M}(f - f_c) + \mathbf{M}(f + f_c) \Big] \tag{12}$$

What to Remember (DSB-SC AM).

1. Not as simple as DSB-LC
2. Requires coherent demodulation. Complicated set up.
3. Bandwidth: $2W$, same as DSB-LC
4. Power Efficiency: Higher than DSB-LC

2.3.3 SSB-SC AM

Single-sideband, suppressed carrier. We either choose Upper or Lower side bands (away and towards the origin), because of hermitian symmetry of $\mathbf{S}(f)$.

- Bandwidth: W, improved,
- Hard to realize the phase splitter (unit-step in frequency domain) at baseband, because of the discontinuity at $f = 0$.
- Demodulation is even more complex than DSB-SC

2.3.4 FM

What to Remember.

1. $s_{FM}(t) = A_c \cos(\theta(t))$, with $\theta(t)$ being the 'phase' of the transmitted signal
$$\theta(t) = 2\pi\left(f_c t + k\int_{-\infty}^{t} m(x)dx\right)$$
The instantaneous frequency is therefore
$$\frac{d}{dt}\theta(t) = 2\pi(f_c + km(t))$$
2. Phase proportional to integral of $m(t)$.
3. Peak Frequency Deviation: $\Delta f = k\|m(t)\|_\infty$,
4. FM Index: $\beta = \Delta f/W$, W is the bandwidth of $m(t)$
5. Carson's Rule: required bandwidth for FM $B_{FM} \approx 2(1+\beta)W$

6. FM requires much larger BW than AM,
7. Increasing β increases required BW, and improves $SNR_{out} = SNR_{in}[3\beta^2(1+\beta)/2]$.
8. AM radio systems operate at much lower BW than FM. 500-1700kHz compared to 88-108MHz.

2.3.5 PM

What to Remember.

1. Transmitted Signal

$$s_{PM}(t) = A_c \cos\Big(2\pi f_c t + km(t)\Big)$$

2. Instant Frequency is proportional to $\dfrac{d}{dt}m(t)$.
3. Phase proportional to $m(t)$.

2.4 B4 Digital Modulation

2.5 B5 ISI and AWGN

What to Remember.

1. Nyquist Criterion for Digital Modulation.

$$\varepsilon = \frac{f_s}{B} \leq 1$$

   Where f_s is the symbol rate transmitted over a passband bandwidth B, without ISI.

2. Shannon's Theorem for AWGN bitrate

$$\varepsilon_{max} = \log_2(1 + SNR)$$

3. Effective bitrate R_b (bits per sec),

$$R_b = f_s \log_2 |\mathcal{A}|, \quad |\mathcal{A}| \text{ size of alphabet}$$

3 Chapter C Notes

3.1 C1 Parity Check

Definition. For any k-bit sequence, $d = d_i$, $0 \leq i \leq k-1$. We can append another bit, d_k so that the transmitted sequence is $k+1$ bits, with.

For even parity, $d_k = \oplus_{i=0}^{k-1} d_i$. The transmitted $k+1$ bit sequence has an even number of bits. The receiver can verify by taking $\oplus$ over all its $k+1$ entries, and

$$r \in \mathbb{B}^{k+1} \text{ is valid } \iff \bigoplus_{i=0}^{k} r_i = 0$$

What to Remember (Even/Odd Parity check).

1. For a k-bit sequence, it becomes a $k+1$-bit sequence.
2. Even parity, the parity check bit is
$$d_k = \bigoplus_{i=0}^{k-1} d_i$$
3. To verify even parity, if $r \in \mathbb{B}^{k+1}$ is valid, if and only if
$$\bigoplus_{i=0}^{k} r_i = 0$$
4. In like fashion, for odd parity, the parity check bit is
$$d_k = 1 \oplus \left(\bigoplus_{i=0}^{k-1} d_i \right) = \bigodot_{i=0}^{k-1} d_i = 0$$
5. To verify odd parity, if $r \in \mathbb{B}^{k+1}$ is valid, (recall that $\oplus$ is the odd counting function), if and only if
$$\bigoplus_{i=0}^{k} r_i = 1$$

3.2 C2 Internet Checksum

Definition. Fix a bit sequence of size $M \times l$, we can view this as a matrix with m rows and l columns. If d is the sequence, then

$$d = \left[d_1, d_2, \cdots, d_m\right]$$

Where each d_m is a vector of size l on its own. So d is a vector containing vectors.

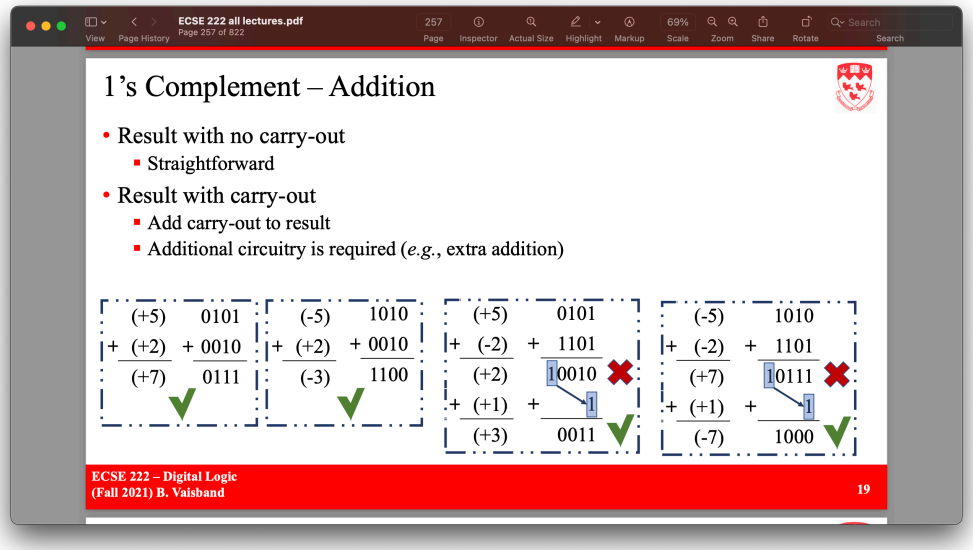
The checksum d_0 is defined inductively. For each $1 \leq m \leq M$,

- We first initialize $d_0 = \vec{0}$, and
- for each $m \in [1, M]$, $d_0 = d_m + d_0$. This is done by one's complement addition.

  One's Complement Addition, fix two vectors of size l, $\vec{x}$, $\vec{y}$, and consider their binary representations, and add them together.

$$\vec{x} + \vec{y} = \left(\sum_{i=0}^{l-1} x_i 2^i\right) + \left(\sum_{i=0}^{l-1} y_i 2^i\right) = \sum_{i=0}^{l} s_i 2^i$$

  The result may be a $l+1$ digit number. If this is so, then the carry-out of the sum is added again to the result. Do this for all $m \leq M$.



- At the end of the process, flip all the bits in d_0

$$d_0 = \Big(1 \oplus d_{l-1}, \cdots 1 \oplus d_0\Big)$$

The result is the following error-checking scheme.

What to Remember (Internet Checksum).

1. If there is no error, then
$$\boxed{\sum_{j\geq 0}^{M} d_j = 0}$$
2. The internet checksum can detect all one-bit error patterns.
3. For a sequence of bits divided in M chunks, the transmitted sequence has $M+1$ chunks.
4. The internet checksum d_0 is obtained by adding all d_j in one's complement, and flipping all the bits (like in one's complement).

3.3 C3 Linear Codes

Definition. Any non-empty, subspace C of F^n with dimension k where $1 \leq k \neq n$ is called a (n, k) linear code. In particular,

If $F + \mathbb{Z}_2$, the n-parity check code is a subspace.

3.3.1 Introduction to Hamming Weights

Fix a code $C \subseteq F^n$, where F^n in this section will always denote the finite cartesian product of $F = GF(p)$. Elements in C are called code words. For any $c \in C$, we define its Hamming Weight

$$\text{wt}(c) = \left|\{i,\, a_i \neq 0\}\right|$$

$\text{wt}(c)$ simply counts the number of non-zero digits. Therefore

- For every $x \in C$, $0 \leq \text{wt}(x) \leq n$,
- If $x \in C$, $\text{wt}(x) = 0 \iff x = 0$ (recall that C is a subspace of F^n, so $0 \in C$),
- $\text{wt}(\cdot)$ induces a metric on C, $d(\cdot, \cdot)$

$$d(x, y) = \text{wt}(x - y), \quad \forall x,\, y \in C$$

To verify that the properties of a metric all hold for this $d(x, y)$ on C

1. $d(x, x) = 0 \iff \text{wt}(x - x) = 0 \iff x - x = 0 \iff x = x$,
2. For every pair of elements $x, y \in C$, $d(x, y) \geq 0$. This comes from the fact that $x - y \in C$ and $\text{wt}(x - y) \geq 0$,
3. If $v, u, w \in C$ then

$$d(v, w) \leq d(v, u) + d(u, w)$$

This is an easy consequence of

$$\text{wt}(a + b) \leq \text{wt}(a) + \text{wt}(b) \tag{13}$$

If we write $v - u = a$, and $u - w = b$, then $a + b = v - w$. Indeed, if $a = (a_i)$, $b = (b_i)$, then if for some $1 \leq j \leq n$ such that $a_j + b_j \neq 0$ then either $a_j \neq 0$ or $b_j \neq 0$. Therefore Equation (13) holds.

Furthermore, define a ball $B_r(w)$ about some $w \in F^n$ as follows

$$B_r(w) = \{x \in F^n,\, d(w,x) \leq r\} \tag{14}$$

Notice how this differs from a regular ball in a metric space. We now turn our attention to a quantity which will be of great interest. Fix a (n,k) linear code C, the minimum distance d of C is defined to be the smallest distance between two distinct code words in C, precisely

$$d = \min\{d(v,w),\, v,\, w \in C,\, v \neq w\} \tag{15}$$

This immediately implies that $d \geq 1$. If our code contains only one element (namely if C is the trivial subspace), then $d = +\infty$.

Definition. A code C uses the Nearest Neighbour Decoding if w is a received word, and if $w \notin C$, then w is decoded as the code word in C that is the closest to it with respect to $d(\cdot,\cdot)$. If $w \in C$ then it is decoded as w. If there is a tie, then the nearest neighbour is chosen arbitrarily.

WTS. If C is an n-code with minimum distance d, (meaning that it does not have to be a subspace). If C uses Nearest Neighbour Decoding, and if $t = d(w,c)$, there w and c are the received and transmitted words, then

- If $t < d$, then C can detect t errors,
- If $2t < d$, then C can correct t errors.

Proof. Let $c \in C$ and the received code w satisfies $d(w,c) = t < d$, so the received code is t distance away from the original code. Since $w \notin C$ by definition of d (if $w \in C$ then that would mean $d \leq t$). C can detect such an error, and we say that C can correct $t < d$ errors.

If $2t < d$, then w lies only within the t-ball of c. This is because the t-balls about the code words in C are pairwise disjoint. Indeed, if $w \in B_t(c) \cap B_t(c')$ for another code word $c' \in C$, then

$$d \leq d(c',c) \leq d(w,c) + d(w,c') \leq 2t$$

Leading to a contradiction. $\square$

We are ready to prove the main theorems in this Chapter concerning Linear Codes.

WTS. Let C be an (n, k)-code that uses Nearest Neighbour Decoding, and d be the same as above. Then

1. $d = \min\{\text{wt}(w),\, w \in C,\, w \neq 0\}$,
2. C can detect $t \geq 1$ errors if and only if $t < d$,
3. C can correct $t \geq 1$ errors if and only if $2t < d$,
4. If C can correct $t \geq 1$ errors, and denote $|F| = q$ (if $F = \mathbb{Z}_2$, then $|F| = 2$), then

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t \leq q^{n-k}$$

Proof. We skip the proof for now. □

Definition. The coding rate for a (n, k)-linear code is k/n.

Definition. A binary linear code is called MDS (maximum distance-separable) code if and only if d is equal to its upper bound. (Also called Perfect Codes).

$$d = \{d(x, y),\, x, y \in C,\, x \neq y\} = (n - k) + 1$$

3.4 C4 Linear Codes (Generator)

Definition. A systematic linear code refers to the structure in which the k information bits are preserved as the k most significant bits.

This means that they are shifted to the left-most entries in the array.

- Advantages: Ease of extraction without complex mapping

This means that the generator matrix G for code $C \subseteq F^n$, is in the form

$$G = \begin{bmatrix} I_k & A \end{bmatrix}$$

Where A is a $k \times (n-k)$ matrix.

Codeword Generation

Let D be a $1 \times n$ matrix representing a k-bit data stream, with

$$D = \Big(d_{k-1},\, d_{k-2},\, \cdots,\, d_0 \Big)$$

D comes in the form of a row vector, and we right-multiply it with a $k \times n$ matrix G to obtain the transmitted vector $c \in C$, where $C \subseteq F^n$ is a k-dimensional subspace.

$$c = DG,\, C \in \mathbb{B}^{1 \times n}$$

We call this matrix G, the generator matrix. This matrix always exists given any linear code $C \subseteq F^n$ with dimension k. A few observations must be made,

- Let T be the linear transformation that 'encodes' our k-bit codes into row vectors in F^n, in symbols

  $$T : \mathbb{B}^{1 \times k} \to \mathbb{B}^{1 \times n},$$

  G will be the matrix that represents this linear transformation.

- The generator matrix G has k-independent rows, where each row represents a valid code-word $g_i \in C \subseteq F^n$. Such that any $c \in C$ is in the span of the rows of G.

- The parity check matrix, H is a $(n-k) \times n$, and satisfies

$$GH^T = 0$$

If we left-multiply by some $d \in \mathbb{B}^{1\times k}$ then $dG = c$ for some $c \in C$, and $cH^T = 0$ for every $c \in C$.

If H is a $(n-k) \times n$ matrix, with rank (dimension of column-span) of $(n-k)$, this forces the row-space of H^T to have dimension $(n-k)$, since

$$C = \operatorname{im} T = \{T(x),\, x \in \mathbb{B}^k\}$$

We usually say that H is a $(n-k)\times n$ matrix, with rank (column-span) $n-k$. And this forces the row-space of H^T to have dimension $(n-k)$.

The following equation is of utmost importance, if the rank of H is $n-k$, then

$$\boxed{C = \{w \in \mathbb{B}^n,\, wH^T = 0\}} \tag{16}$$

Every valid codeword $c \in C \subseteq \mathbb{B}^n$ must satisfy this property.

The proof is quite straight-forward, we have already shown that $C \subseteq \{w \in \mathbb{B}^n, wH^T = 0\}$, the second part of the proof just consists of showing that $\dim \ker H^T = (n-k)$. The reader should consult Chapter 8.8 of Nicholson's Linear Algebra for more details.

- Assume that $c \in C$ is transmitted, and the receiver receives some $v \in F^n$, where possibly $v \notin C$, then we define
  - $z = v - c$ as the error,
  - If $v \notin C$, then by Equation (16), $s = vH^T \neq 0$. Such a word $s \in \mathbb{B}^{(n-k)\times 1}$ is called the syndrome.

Note a couple of things, the receiver has the vector v, and wishes to recover $c \in C$. For this task, it suffices to recover z, the error, since we can always subtract $c = v - z$. Furthermore, $cH^T = 0 \iff Hc^T = 0$, and by linearity,

$$c = v - z \implies Hc^T = Hv^T - Hz^T \implies s = Hv^T = Hv^T$$

If we can solve for the error vector v, then we can solve for the original codeword by subtraction, what remains is to solve the homogeneous system of equations $s = Hv^T$.

- The set of all possible errors that can be applied to c is $\mathbb{B}^{1\times n}$, but the syndrome is only a $\mathbb{B}^{(n-k)\times 1}$ vector. So there can be no one-to-one correspondence. The take-away is this, given a syndrome vector $s = Hv^T$, where v is the received vector, the search for the error vector z, has to be reduced from $\mathbb{B}^n$ to $\mathbb{B}^{n-k}$ for a one-to-one correspondence.
- Intuitively speaking, the larger $n - k$, the larger the syndrome vector; and the more likely we can recover the correct error vector, and thus recover c.

3.5 Arithmetic in GF(2)

3.5.1 Multiplication of Polynomials in GF(2)

If we want to multiply $(x^5 + x^2 + 1)(x^3 + 1)$, we write the coefficients of the two polynomials in the form

$$(x^5 + x^2 + 1)(x^3 + 1) \iff (5,\ 2,\ 0)(3,\ 0)$$

Find the set of sums across the two tuples, given by

$$(8,\ 5,\ 5,\ 2,\ 3,\ 0)$$

Then retain only the ones that have an odd number of terms (here the two 5 cancel out), and we get

$$(8,\ 3,\ 2,\ 0) \iff x^8 + x^3 + x^2 + x^0$$

Let us try with another example with $(1 + x)(x + x^2)$

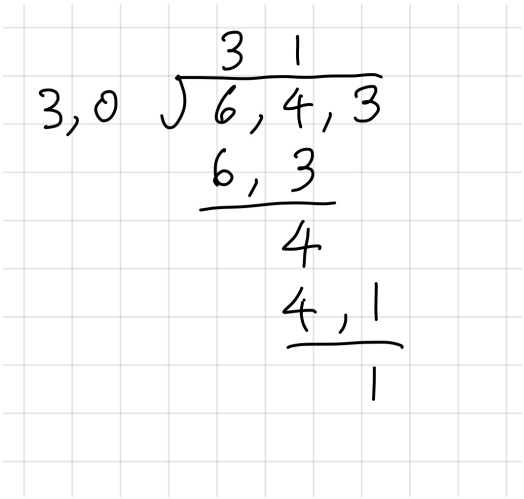
$$(1 + x)(x + x^2) \iff (1,\ 0)(1,\ 2)$$

The set of sums is $(2,\ 3,\ 1,\ 2)$, and flipping the required coefficients we get

$$(3, 1) \implies (1 + x)(x + x^2) = x^3 + x$$

3.5.2 Long Division of Polynomials in GF(2)

Assume that $G(X) = (3, 0) = x^3 + x^0$, and $D(X) = (3, 1, 0) = x^3 + x^1 + x^0$, if we wish to find $R(X)$ then we wish to find the remainder of $\frac{X^3 D(X)}{G(X)}$



3.6 Cyclic Redundancy Check

We begin with some size considerations. Suppose that

- We are given a data vector, D of k-bits. We can represent D using a binary polynomial of $k-1$ degree, denoted by $D(X)$
- In CRC, the transmitter then generates a $n-k$ bit sequence called a Frame-Check Sequence (FCS) or $R(X)$. ($n-k-1$ polynomial),
- The transmitted frame, $T(X)$ is n bits in size. ($n-1$ polynomial).
- For any CRC scheme, where n, and k are fixed numbers. There has to be a generator polynomial, $G(X)$ of degree $n-k$.
- $R(X)$ is the remainder when $X^{n-k}D(X)$ is divided by $G(X)$.
- $X^{n-k}D(X)$ simply shifts the bits in $D(X)$ leftwards by $n-k$. $R(X)$ has to have degree $n-k$.
- The transmitted frame $T(X) = X^{n-k}D(X) + R(X)$.

The following example should enlighten things a bit. Let $G(X) = x^3+1$, and the corresponding information bits be $D = [1101] = x^3 + x^2 + x^0$. Degree on $G(X)$ is $3 = n-k$, and Degree on $D(X)$ is $3 = k-1$, therefore $k = 4$ and $n-7$. Shifting $D(X)$ by 3 bits to the left yields

$$X^{n-k}D(X) = X^3D(X) = x^6 + x^5 + x^3$$

Dividing $X^{n-k}/G(X)$ give us the remainder $R(X) = x^1$. Since $R(X)$ must have degree $n-k-1 = 2$, we can write $R(X) = [010]$. And the transmitted frame is $T(X) = [1101010]$.

What to Remember. Cyclic Redundancy Check Computations

Vector sizes

1. D: Data Vector, k bits. Degree: $k-1$,
2. G: Generator Polynomial, Degree: $n-k$,
3. R: Remainder/Frame Check Sequence, Degree: $n-k-1$.

Computations

1. Given D and G. Determine n, and k by

$$\deg G = n - k \tag{17}$$
$$\deg D = k - 1 \tag{18}$$

2. Shift D by $n - k$ bits.
3. Compute $R(X)$ by remainder of $X^{n-k}D(X)/G(X)$,
4. Concatenate $T(X) = X^{n-k}D(X) + R(X)$.
5. Extra: Verify that $T(X)$ has n-bits in total. (A polynomial of $n - 1$ degree).

Factoids

1. Given a transmitted codeword $T(X)$ from a generator polynomial $G(X)$. It is always possible to fool the scheme by using an error $E(X) = G(X)$. This is because $T(X) + E(X) = T(X) + G(X)$ divides $G(X)$.
2. Simple to implement,
3. Well suited to detect burst errors (useful because common transmission errors are burst errors),
4. Irreducible polynomial of degree m, not divisible by any polynomial with degree $0 < k < m$.
5. Primitive polynomial of degree m, not divisible by any polynomial in the form $x^k + 1$, $0 < k < 2^m$
6. If G is an irreducible polynomial of degree L, then CRC can detect all BURST errors of $0 < k < L$.
7. If G is a primitive polynomial of degree L, then CRC can detect all two-bit errors separated by $N < 2^L$ bits.
8. A factor of $(x + 1)$ detects any odd number of bit errors.
9. Single error patterns are detected by G having two or more terms.

3.7 ARQ and FEC

Definition. Automatic Repeat Request (ARQ)

Definition. Forward Error Correction (FEC).

3.8 Coding Gain in AWGN Channel

Consider the following graphic.

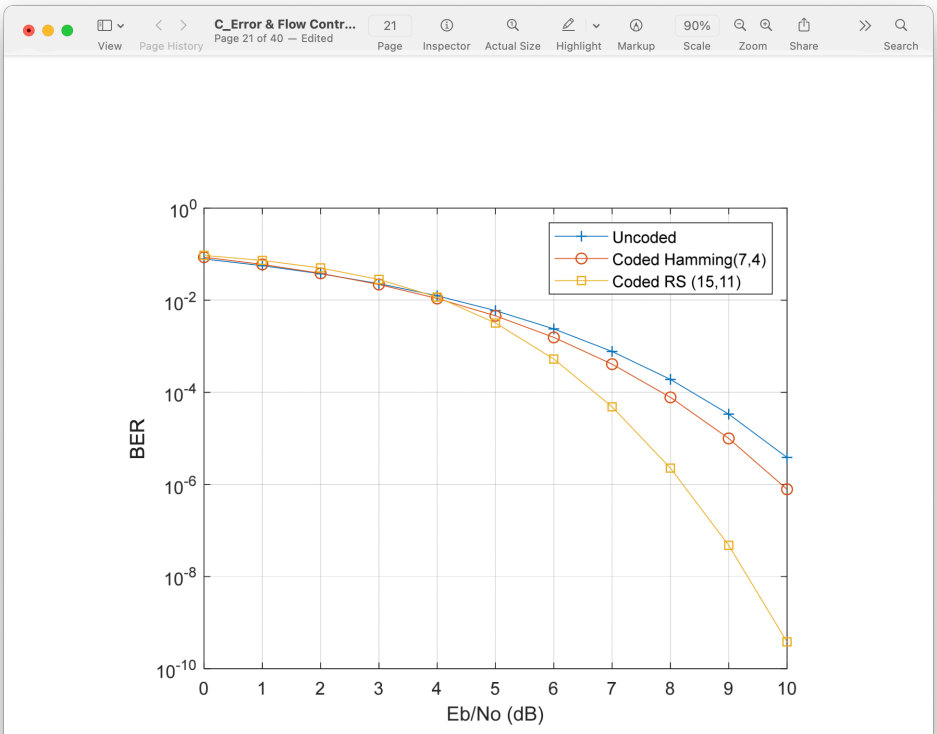


Figure 10: Performance comparison between coded and un-coded 4QAM signals.

Figure 10 illustrates the performance comparison on a AWGN channel between 4-QAM modulated signals without coding and with two error correction codes, namely the (7,4) Hamming and (15,11) Reed-Solomon codes. It can be illustrated that at low E_b/N_0, the un-coded scheme has a slightly higher performance than the two coded schemes. This can be explained by the fact that at very low E_b/N_0, errors happen very frequently and the coded schemes are unable to make successful correction and can introduce more the errors. However, as E_b/N_0 increases, the error correction ability of coded schemes quickly reveals

At low E_b/N_0 uncoded signals have a lower BER (bit-error rate) than coded signals. But as E_b/N_0 increases, coded signals are better.

Definition. Coding Gain: the improvement in power saving, E_b/N_0 at the same BER.

3.9 Chapter C Exercises

3.9.1 Problem C1

WTS. A transmission link with a bit error rate of p = 0.001 is used for transferring 10-byte frames. Calculate

(a) The probability that there is exactly one error bit in the received frame?

(b) What is the frame error probability, i.e., the probability that the received frame contains at least one error bit?

(c) If the frame length is halved, what is the frame error probability?

Proof. Let $n = 80$ bits. Using the Binomial distribution, it is trivial to verify that

Part A

The probability there is one error bit in the frame is given by

$$P(k = 1) = \binom{n}{1} p(1-p)^{n-1} = 0.0739$$

Part B

The probability that there is at least one error is given by

$$P(k \geq 1) = 1 - (1-p)^n = 0.0769$$

Part C

The probability of a frame error given $m = n/2 = 40$ is

$$P^m(k \geq 1) = 1 - (1-p)^m = 0.0392$$

□

3.9.2 Problem C2

WTS. Assume that transmitting data is divided into chunks of 3-bit long, and then odd-parity is applied to form a parity codeword. In the new 4-bit parity codeword space, list all the valid and invalid codewords.

Proof. We are using odd parity, so for any $c \in \mathbb{B}^4$,

$$c \in C \iff \bigoplus_{i=0}^{3} c_i = 1$$

Equivalently, $c \notin C \iff \bigoplus_{i=0}^{c} c_i = 0$. Let us list C^c, the complement of C.

$$C^c = \{[0000], [1111], [0011], [0101], [1001], [0110], [1010], [1001]\}$$

And therefore

$$C = \{[0001], [0010], [0100], [1000], [1110], [1101], [1011], [0111]\}$$

□

3.9.3 Problem C3

WTS. Using the 16-bit Internet Checksum:

(a) Calculate the Internet checksum for the four 16-bit words of data as follows: E308 E309 00FF 0F0F.

(b) Suppose that the received data and checksum are contaminated with error as follows: E308 E309 00FF 0F0E 29DF. Verify that the internet checksum can detect the error.

(c) Find an example of a 2-bit error that can fool Internet checksum for the above data and checksum.

Proof. Part a. Procedure for calculating the internet checksum:

1. Using HEX mode on Calculator, add all the data bits together.

$$E308 + E309 + 00FF + 0F0F = 0001D61F$$

2. Since there is a carry-out of '1', we subtract 10000 and add 1, equivalently:

$$0001D61F - 10000 + 1 = D620$$

3. Taking the one's complement, (bitwise XOR) of the sum. This is equivalent to subtracting with FFFF, therefore

$$FFFF - D620 = 29DF$$

Part b. Verify that the internet checksum detects the error. The procedure is as follows

1. Using HEX mode on Calculator, add all the shit together again,

$$E308 + E309 + 00FF + 0F0E + 29DF = 0001FFFD$$

2. Carry-out of '1', we need to subtract 10000 and add 1, hence

$$0001FFFD - 10000 + 1 = FFFE$$

3. Take one's complement. Which equates to

$$FFFF - FFFE = 0001 \neq 0000$$

4. Therefore the internet checksum detects the error.

Part c. We note that $\boldsymbol{E309}$ and $\boldsymbol{E308}$ are one bit different from each other, therefore we can apply the error which swaps $\boldsymbol{9}$ with $\boldsymbol{8}$. Resulting in E309 E308 00FF 0F0F 29DF.

□

3.9.4 Problem C4

WTS. Let $G(x) = x^3 + 1$, and the information bits $D(x) = x^3 + x^2 + 1$.

(a) Find the corresponding CRC codeword,

(b) If the CRC codeword is contaminated with $E(x) = x^3 + x^2$, show that the above CRC coding scheme detects this error, and

(c) Find a 2-bit error pattern that can fool this CRC scheme.

Proof. Part A

Obviously, $k = 4$ and $n - k = 3$, so $x^3 D(x) = x^6 + x^5 + x^3$. Dividing $x^3 D(x)$ by $x^3 + 1 = G(x)$, we have

$$x^3 D(x) = (x^3 + x^2)G(x) + x^2$$

Therefore $R(x) = x^2$. And the transmitted frame becomes $x^6 + x^5 + x^3 + x^2 = 1101100$.

Part B

$Z(x) = x^6 + x^5 + x^3 + x^2 + E(x) = x^6 + x^5$. Dividing by $G(x)$ we have

$$Z(x) = (x^3 + x^2 + 1)G(x) + (x^2 + 1)$$

Since $x^2 + 1 \neq 0$, the CRC scheme detects the error.

Part C

Take $E(x) = x^3 + 1$, then the set of valid codewords is a subspace, $Z(x) = x^6 + x^5 + x^3 + x^2 + E(x)$ is divided by G(x) cleanly. □

3.9.5 Problem C5

WTS.

Proof. □

3.9.6 Problem C6

WTS. Find the Hamming distance between the following codewords: A = [000000], B = [101010], C = [000111]

Proof. This is trivial, $d(A, B) = \mathrm{wt}(B) = 3$, $d(A, C) = \mathrm{wt}(C) = 3$, and $d(B, C) = 4$. The minimum distance is 3. □

3.9.7 Problem C7

WTS. Consider the coding scheme in problem 6, what is the maximum number of detectable bit errors and the maximum number of bit errors that can be corrected? If the receiver receives a codeword of R = [111010], which valid codeword should it correct to? Explain why.

Proof. The maximum number of detectable bit errors is 2. The maximum number of bit errors that can be corrected is 1.

If the receiver receives $\boldsymbol{R} = [111010]$, then it assumes there is 1 error (since it can only correct 1 error). Flipping the second bit corrects $\boldsymbol{R}$ to $\boldsymbol{B} = [101010]$. □

3.9.8 Problem C8

WTS.

Proof. □