EE551: Notable Equations (missing chapter 10)

Compiled by Mohammad Sanad AlTaher

Chapter 8:

Decision Boundary Equation:	$\boldsymbol{r}.\boldsymbol{s_i} + \frac{1}{2}[N_0 \ln P_r(s_i) - \mathcal{E}_i]$	
Binary Antipodal Signals with ML:	$P_r(C) = 1 - Q\left(\sqrt{\frac{2\mathcal{E}_b}{N_0}}\right)$	$P_r(E) = P_2 = 1 - P_r(C) = Q\left(\sqrt{\frac{2\mathcal{E}_b}{N_0}}\right)$
Binary Orthogonal Signals with ML:	$P_r(C) = P_r(s_1)P_r(C \mid s_1) + P_r(s_2)P_r(C \mid s_2)$ $= \frac{1}{2}\left[1 - Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right)\right] + \frac{1}{2}\left[1 - Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right)\right]$ $= 1 - Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right)$	$P_r(E) = P_2 = 1 - P_r(C) = Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right)$
General Binary Signaling with MAP detector	$d_{12}^2 = \boldsymbol{d^2} = \mathcal{E}_1 + \mathcal{E}_2 - 2\sqrt{\mathcal{E}_1\mathcal{E}_2}\rho_{12}$ $\rho_{12} = \frac{1}{\sqrt{\mathcal{E}_1\mathcal{E}_2}}\int_0^{T_b} s_1(t).s_2(t)dt = \frac{\langle \boldsymbol{s_1}, \boldsymbol{s_2} \rangle}{\lVert \boldsymbol{s_1} \rVert \lVert \boldsymbol{s_2} \rVert} = \frac{\boldsymbol{s_1}.\boldsymbol{s_2}}{\sqrt{\mathcal{E}_1\mathcal{E}_2}}$ $r_{th} = \frac{N_0/2}{d} \ln\left(\frac{P_r(s_1)}{P_r(s_2)}\right)$ $\rho_{12} = -1$, when antipodal $\rho_{12} = 0$, when orthogonal	$P_r(C) = P_r(s_1)\left[1 - Q\left(\frac{d + 2r_{th}}{\sqrt{2N_0}}\right)\right] + P_r(s_2)\left[1 - Q\left(\frac{d - 2r_{th}}{\sqrt{2N_0}}\right)\right]$ $P_r(E) = 1 - P_r(C) = P_2 = P_r(s_1)\left[Q\left(\frac{d + 2r_{th}}{\sqrt{2N_0}}\right)\right] + P_r(s_2)\left[Q\left(\frac{d - 2r_{th}}{\sqrt{2N_0}}\right)\right]$
M-ary PAM:	$\mathcal{E}_{\text{bavg}} = \frac{(M^2-1)\mathcal{E}_p}{3\log_2 M} A^2$	$P_r(C) = 1 - \frac{2(M-1)}{M} Q\left(\sqrt{\frac{d_{min}^2}{2N_0}}\right)$ $P_M = \frac{2(M-1)}{M} Q\left(\sqrt{\frac{6\log_2 M}{(M^2-1)} \frac{\mathcal{E}_{\text{bavg}}}{N_0}}\right)$
PSK:	$d_{\min} \approx 2\sqrt{\frac{\pi^2 \log_2 M}{M^2}}\, \mathcal{E}_b$	$P_r(E) = P_4 = 1 - P_r(C) = 2\left[Q\left(\sqrt{\frac{d_{min}^2}{2N_0}}\right)\right] - \left[Q\left(\sqrt{\frac{d_{min}^2}{2N_0}}\right)\right]^2$ $\boldsymbol{P_b = Q\left(\sqrt{\frac{2\mathcal{E}_b}{N_0}}\right)}$
Union Bound:	$P_r(E) = \frac{1}{M}\sum_{i=1}^{M} P_r(E \mid \boldsymbol{s}_i) \le \frac{1}{M}\sum_{i=1}^{M}\left[\sum_{\substack{k=1 \\ k \ne i}}^{M} Q\left(\frac{d_{ik}}{\sqrt{2N_0}}\right)\right]$	

$$\mathrm{P}[X > \alpha] = Q\left(\frac{\alpha - m}{\sigma}\right)$$

$$\mathrm{P}[X < \alpha] = Q\left(\frac{m - \alpha}{\sigma}\right)$$

x	$Q(x)$	x	$Q(x)$	x	$Q(x)$	x	$Q(x)$
0	0.500000	1.8	0.035930	3.6	0.000159	5.4	3.3320×10^{-8}
0.1	0.460170	1.9	0.028717	3.7	0.000108	5.5	1.8990×10^{-8}
0.2	0.420740	2	0.022750	3.8	7.2348×10^{-5}	5.6	1.0718×10^{-8}
0.3	0.382090	2.1	0.017864	3.9	4.8096×10^{-5}	5.7	5.9904×10^{-9}
0.4	0.344580	2.2	0.013903	4	3.1671×10^{-5}	5.8	3.3157×10^{-9}
0.5	0.308540	2.3	0.010724	4.1	2.0658×10^{-5}	5.9	1.8175×10^{-9}
0.6	0.274250	2.4	0.008198	4.2	1.3346×10^{-5}	6	9.8659×10^{-10}
0.7	0.241960	2.5	0.006210	4.3	8.5399×10^{-6}	6.1	5.3034×10^{-10}
0.8	0.211860	2.6	0.004661	4.4	5.4125×10^{-6}	6.2	2.8232×10^{-10}
0.9	0.184060	2.7	0.003467	4.5	3.3977×10^{-6}	6.3	1.4882×10^{-10}
1	0.158660	2.8	0.002555	4.6	2.1125×10^{-6}	6.4	7.7689×10^{-11}
1.1	0.135670	2.9	0.001866	4.7	1.3008×10^{-6}	6.5	4.0160×10^{-11}
1.2	0.115070	3	0.001350	4.8	7.9333×10^{-7}	6.6	2.0558×10^{-11}
1.3	0.096800	3.1	0.000968	4.9	4.7918×10^{-7}	6.7	1.0421×10^{-11}
1.4	0.080757	3.2	0.000687	5	2.8665×10^{-7}	6.8	5.2309×10^{-12}
1.5	0.066807	3.3	0.000483	5.1	1.6983×10^{-7}	6.9	2.6001×10^{-12}
1.6	0.054799	3.4	0.000337	5.2	9.9644×10^{-8}	7	1.2799×10^{-12}
1.7	0.044565	3.5	0.000233	5.3	5.7901×10^{-8}	7.1	6.2378×10^{-13}

Chapter 9:

Orthogonal M-ary Frequency Shift Keying:

Waveforms:

$$u_m(t) = Re\left(s_m(t)e^{j2\pi f_c t}\right) = Re\left(\sqrt{\frac{2\mathcal{E}_s}{T}}e^{j2\pi m\Delta f t}\,e^{j2\pi f_c t}\right) = \sqrt{\frac{2\mathcal{E}_s}{T}}\cos(2\pi f_m t) \quad \text{for } 0 \le t \le T, \quad m = 1,2,\dots,M$$

$$\mathcal{E}_m = \mathcal{E}_s$$

$$f_m = f_c + m\Delta f$$

$$\Delta f = |f_m - f_n|$$

for adjacent tones: $|m-n| = 1$

Orthogonal: (coherent detection) $\langle u_1(t), u_2(t)\rangle = \frac{\mathcal{E}_s}{T}\frac{\sin(2\pi|m-n|\Delta f T)}{2\pi|m-n|\Delta f} = 0 \;\rightarrow\; \Delta f = \frac{k}{2|m-n|T} \;\rightarrow\; \Delta f_{\min} = \frac{1}{2T}$

Orthogonal: (non-coherent detection) $|\langle s_m(t), s_n(t)\rangle| = \frac{2\mathcal{E}}{T}\frac{\sin(\pi|m-n|\Delta f T)}{\pi|m-n|\Delta f} = 0 \;\rightarrow\; \Delta f = \frac{k}{|m-n|T} \;\rightarrow\; \Delta f_{\min} = \frac{1}{T}$

Geometric representation:

N = M	$u_{mn} = 0 \ \forall\, m \neq n$	$u_{mm} = \sqrt{\mathcal{E}_s}$	$d_{mn} = \sqrt{2\mathcal{E}_s}$

Demodulation: (assuming ML and u_1 *is transmitted*)

$$r_1 = \sqrt{\mathcal{E}_s} + n_1, \quad r_2 = n_2, \quad etc. \quad \rightarrow \quad \Pr\{\text{Correct}\} = \Pr\left\{\sqrt{\mathcal{E}} + n_1 > n_2, \cdots, \sqrt{\mathcal{E}} + n_1 > n_M\right\}$$

$$\rightarrow P_c = \int_{-\infty}^{\infty} \Pr\left\{\sqrt{\mathcal{E}} + n_1 > n_2, \cdots, \sqrt{\mathcal{E}} + n_1 > n_M \,\middle|\, n_1\right\} f(n_1)\,dn_1 = \int_{-\infty}^{\infty}\left(\Pr\left\{\sqrt{\mathcal{E}} + n_1 > n_2 \,\middle|\, n_1\right\}\right)^{M-1} f(n_1)\,dn_1$$

$\therefore$

$$P_c = \int_{-\infty}^{\infty}\left[1 - Q\left(\frac{n_1 + \sqrt{\mathcal{E}}}{\sqrt{\frac{N_0}{2}}}\right)\right]^{M-1} f(n_1)\,dn_1$$

where $f(n_1)$ is the pdf of noise n_1

Λ

$$P_e = 1 - P_c = \int_{-\infty}^{\infty}\left(1 - \left[1 - Q\left(\frac{n_1 + \sqrt{\mathcal{E}}}{\sqrt{\frac{N_0}{2}}}\right)\right]^{M-1}\right)\frac{1}{\sqrt{\pi N_0}}e^{-\frac{n_1^2}{N_0}}\,dn_1$$

$$\therefore \quad P_e = \int_{-\infty}^{\infty}\left(1 - [1 - Q(x)]^{M-1}\right)\frac{1}{\sqrt{2\pi}}e^{-\frac{(x-\sqrt{2k\gamma_b})^2}{2}}\,dx$$

where $x = \frac{n_1 + \sqrt{\mathcal{E}}}{\sqrt{N_0/2}}$, and $\gamma_b = \mathcal{E}_b/N_0$, and $k = \log_2(M)$

Non-coherent BFSK:

$s_m(t) = \sqrt{\frac{2\mathcal{E}_s}{T}}\cos(2\pi f_m t)$	$r(t) = \sqrt{\frac{2\mathcal{E}_s}{T}}\cos(2\pi f_m t + \theta_m) + n(t)$	$\theta_m = -2\pi f_m \tau$

In absence of noise:

$$r_1(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_1 t + \theta_1) \qquad r_2(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_2 t + \theta_2)$$

$\because$ $\theta_1 \ \Lambda\ \theta_2$ are random with uniform distribution, four basis must be constructed:

$$s_1(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_1 t + \theta_1) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_1 t)\cos(\theta_1) - \sqrt{\frac{2E_b}{T_b}}\sin(2\pi f_1 t)\sin(\theta_1)$$

$$s_2(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_2 t + \theta_2) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_2 t)\cos(\theta_2) - \sqrt{\frac{2E_b}{T_b}}\sin(2\pi f_2 t)\sin(\theta_2)$$

$$\psi_{1c}(t) = \sqrt{2/T_b}\cos(2\pi f_1 t) \qquad \psi_{1s}(t) = -\sqrt{2/T_b}\sin(2\pi f_1 t)$$

$$\psi_{2c}(t) = \sqrt{2/T_b}\cos(2\pi f_2 t) \qquad \psi_{2s}(t) = -\sqrt{2/T_b}\sin(2\pi f_2 t)$$

$\therefore$

$$\mathbf{s_1} = [\ \sqrt{E_b}\cos\theta_1 \quad \sqrt{E_b}\sin\theta_1 \quad 0 \quad 0\ ]$$

$$\mathbf{s_2} = [\ 0 \quad 0 \quad \sqrt{E_b}\cos\theta_2 \quad \sqrt{E_b}\sin\theta_2\ ]$$

Decision rule: (if s_1 is transmitted)

$$I_0\left(\frac{2\sqrt{E({r_{1c}}^2 + {r_{1s}}^2)}}{N_0}\right) \ge I_0\left(\frac{2\sqrt{E({r_{2c}}^2 + {r_{2s}}^2)}}{N_0}\right) \quad \rightarrow \quad \text{(envelope detection)} \quad \sqrt{r_{1c}^2 + r_{1s}^2} \ge \sqrt{r_{2c}^2 + r_{2s}^2}$$

where $I_0(x)$ is the modified Bessel function:

$$\frac{1}{2\pi}\int_0^{2\pi}\exp\left[\frac{2\sqrt{E}r_{1c}\cos(\phi_1) + 2\sqrt{E}r_{1s}\sin(\phi_1)}{N_0}\right]d\phi_1 = I_0\left(\frac{2\sqrt{E({r_{1c}}^2 + {r_{1s}}^2)}}{N_0}\right)$$

$$P_e = \frac{1}{2}\exp\left(-\frac{E_b}{2N_0}\right)$$

η-band-limit:

$$\frac{\int_{-W}^{W}|X(f)|^2\,df}{\int_{-\infty}^{\infty}|X(f)|^2\,df} \ge 1 - \eta$$

where η is some out-of-band ratio

Dimensionality Theorem:

Max dimensions

$$N \approx KWT$$

where T is the signal duration and K is some constant usually chosen equal to 2

<table>
<tr><td rowspan="3">Bandwidth efficiency:</td><td colspan="3">$\frac{R}{W}$ where R is the bit rate and W is the bandwidth, bandwidth is calculated from PSD of transmitted waveform</td></tr>
<tr><td colspan="3">$$\frac{R}{W} = 2\frac{log_2(M)}{N}$$ bits/sec/Hz</td></tr>
<tr><td colspan="3">Assuming modulations satisfy $W = \frac{N}{2T}$
M-ary FSK: (N=M) $\frac{R}{W} \leq 1$
Suitable for channels with power constraints:
• Improves energy performance (reduces SNR for given P_e)
• Increases required bandwidth

SSB PAM: (N = 1) $\frac{R}{W} > 1$
PSK and QAM: (N = 1) $\frac{R}{W} \geq 1$
Suitable for channels with bandwidth constraints:
• Reduce required bandwidth
• Worsen energy performance (increases required SNR for given P_e)</td></tr>
<tr><td rowspan="3">Shannon's channel coding theorem:</td><td colspan="3">Capacity: max number of bits per channel that can be sent reliably
$$C = \frac{1}{2}\log_2\left(1 + \frac{P}{WN_0}\right) \quad \textit{bits/channel use}$$</td></tr>
<tr><td colspan="3">With 2WT channel uses/transmission and $1/T$ transmissions/second:
$$C = W \cdot log_2\left(1 + \frac{P}{WN_0}\right) \rightarrow \frac{R}{W} < log_2\left(1 + \frac{P}{WN_0}\right)$$ bits/second</td></tr>
<tr><td colspan="3">$$\because \varepsilon_b = \frac{PT}{log_2(M)} = \frac{P}{R}$$ $$\therefore \frac{R}{W} < log_2\left(1 + \frac{R}{W}\frac{\varepsilon_b}{N_0}\right)$$</td></tr>
<tr><td rowspan="2">Shannon limit:</td><td>If R < C, then P_e can be made arbitrarily small by extending code size</td><td colspan="2">If R > C, then P_e is bounded away from zero.</td></tr>
<tr><td colspan="3">$$C = \max_{p(x)} I(X;Y)$$</td></tr>
</table>

Chapter 12:

Self-information:	$I(x_k) = \log_a \frac{1}{P(x_k)}$ $I_k = \log_a \frac{1}{p_k} = -\log_a p_k$ • If a = 2, info is bits/symbol • If a = 10, info is Hartley/symbol • If a = e, info is Nat/symbol
Entropy:	$\mathrm{H}(X) = \mathbb{E}(I_k) = \sum_{1}^{N} p_k \log \frac{1}{p_k} = -\sum_{1}^{N} p_k \log p_k$ $\mathrm{H}(X) \leq \log N$ $\mathrm{H}(X) \geq \mathrm{H}(X\|Y)$
Joint and conditional entropy:	$\mathrm{H}(Y\|X) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(y\|x) = \mathbb{E}(-\log p(Y\|X))$ $\mathrm{H}(X\|Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x\|y) = \mathbb{E}(-\log p(X\|Y))$ $\because \quad p(x_i,y_j) = p(y_j\|x_i)p(x_i) = p(x_i\|y_j)p(y_j)$ $\rightarrow \quad \mathrm{H}(X,Y) = \mathrm{H}(X) + \mathrm{H}(Y\|X) \;\wedge\; \mathrm{H}(X,Y) = \mathrm{H}(Y) + \mathrm{H}(X\|Y)$
Mutual information:	$I(X;Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i,y_j)\log\frac{p(x_i,y_j)}{p(x_i)p(y_j)} = \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i,y_j)\log\frac{p(y_j\|x_i)p(x_i)}{p(x_i)p(y_j)}$ $I(X;Y) = I(Y;X) = \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X,Y) = \mathrm{H}(Y) - \mathrm{H}(Y\|X) = \mathrm{H}(X) - \mathrm{H}(X\|Y)$ $I(X;Y) \geq 0$ with equality if X and Y are independent $I(X;X) = H(X)$
Source coding theorem:	Given N symbols each with a unique set of R bits: If N is integer power of 2: $R = \log_2 N$ bit/symbol If N is not a power of 2: $R = \lfloor \log_2 N \rfloor + 1$ bit/symbol $\rightarrow \quad R \geq \log_2 N \;\wedge\; \mathrm{H}(X) \leq \log_2 N \;\therefore\; R \geq \mathrm{H}(X) \;\wedge\; \eta = \frac{H(X)}{R}$ coding efficiency Average code length: $\bar{R} = \sum_{k=1}^{N} l(x_i)\, P(x_i)$ Condition: $H(X) \leq \bar{R} < H(X) + 1$
Huffman coding algorithm:	• Order source symbols by decreasing probability • Group the d least probable symbols, where: $\frac{N}{D-1} = INT + \frac{R}{D-1}$ If $R = 0 \rightarrow d = D - 1$ | If $R = 1 \rightarrow d = D$ | If $R > 1 \rightarrow d = R$ • Add the probabilities of each group • After the first group of d symbols was coded, other groups contain D symbols, and so on. (D is equal to the base) If blocks of J symbols are encoded at a time, then: $H(X) \leq \frac{\bar{R}_J}{J} < H(X) + \frac{1}{J}$ $\frac{\bar{R}_J}{J} = \bar{R}$
Mutual information and channel capacity for discrete-valued I/O:	1) Find entropy of Y for fixed input X = x: $H(Y\|X=x) = E\left[-\log_2 p_{Y\|X}(Y\|x)\right] = -\sum_{y\in\Omega_Y} p_{Y\|X}(y\|x)\log_2 p_{Y\|X}(y\|x)$ Conditional probability $p_{Y\|X}$ behave like normal probabilities 2) Find the average conditional entropy by averaging the values from the previous step over X: $H(Y\|X) = \sum_{x\in\Omega_X} H(Y\|X=x)\, p_X(x) = -\sum_{x\in\Omega_X} p_X(x)\sum_{y\in\Omega_Y} p_{Y\|X}(y\|x)\log_2 p_{Y\|X}(y\|x)$

	3) Evaluate H(Y) from the given probabilities of the values of Y or from: $$p_Y(y) = \sum_{x \in \Omega_X} p_{Y\|X}(y\|x) p_X(x)$$
	4) Find mutual information: $$I(X,Y) = H(Y) - H(Y\|X) = -\sum_{y \in \Omega_y} p_Y(y)\log_2(p_Y(y)) + \sum_{x \in \Omega_X} p_X(x) \sum_{y \in \Omega_y} p_{Y\|X}(y\|x)\log_2 p_{Y\|X}(y\|x)$$
	5) Channel capacity is then: $$C_S = \max_{p_X(x)} I(X,Y)$$ [bits per channel use]
	H(Y) and H(Y|X) depend on the input distribution. In some cases where the transition probabilities are symmetric, H(Y|X) cancel out, then maximizing I(X,Y) is done by maximizing H(Y).
Binary Symmetric Channel:	$$I(X,Y) = H(Y) - H(Y \mid X) = \ldots = H(Y) + p\log_2 p + (1-p)\log_2(1-p)$$ where p is the bit flip probability
	since max entropy of binary random variable is 1 and outputs are equiprobable: $$C_s = 1 + p\log_2 p + (1-p)\log_2(1-p)$$ If p = 0.5, $C_s = 0$; If p = 0 or 1, $C_s = 1$
Channel capacity:	$$0 \le C \le \min(H(\mathcal{X}), H(\mathcal{Y})) \le \min(\log\|\mathcal{X}\|, \log\|\mathcal{Y}\|)$$ for n uses of channel: $$C^{(n)} = \frac{1}{n} \max_{\mathbf{p}_{x_{1:n}}} I(\mathcal{X}_{1:n}; \mathcal{Y}_{1:n})$$

Chapter 13:

Hamming weight and distance:

Weight: w(v)
Number of 1s in the sequence v

Distance: d(v,w)
Number of bit positions that are different between the two sequences v and w

Property #1:
$$d(\mathbf{v},\mathbf{w}) + d(\mathbf{w},\mathbf{x}) \geq d(\mathbf{v},\mathbf{x})$$

Property #2:
$$d(\mathbf{v},\mathbf{w}) = w(\mathbf{v}+\mathbf{w}) \rightarrow d_{min} = w_{min}$$

Linear Block Codes:

$$\mathbf{c} = \boldsymbol{x}\,\mathbf{G}$$

c: code matrix with 1 column and **n** rows
x: the message matrix with **k** columns and 1 row
G: generator matrix with **n** columns and **k** rows (n, k)

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

$\mathbf{I}_k = k \times k$ identity matrix
$\mathbf{P}_k = k \times (n-k)$ matrix
P: parity matrix

$$\mathbf{c} = (c_1, c_2, \ldots, c_n) = (\underbrace{x_1, x_2, x_3, \ldots, x_k}_{\text{message bits}}, \underbrace{p_1, p_2, \ldots, p_{n-k}}_{\text{parity check bits}})$$

or flipped with parity check bits before message bits if $G = [P|I_k]$

$$\mathbf{H} = [-\mathbf{P}^T \mid \mathbf{I}_{n-k}] \underset{\text{binary codes}}{=} [\mathbf{P}^T \mid \mathbf{I}_{n-k}]$$ found from **G**

s.t. $\mathbf{cH}^T = 0 \quad \wedge \quad \mathbf{GH}^T = 0$

Number of Independent columns of H is equal to d_{min} of H, number of dependent columns = $d_{min} - 1$

For an (n,k) code: $d_{min} \leq n - k + 1$

Codes with d_{min} detect $d_{min} - 1$ errors and correct up to $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ in each codeword.

Hamming codes: $(m \geq 2)$

Code length:	number of info bits:	Number of parity bits:	Error correction capability:	Min distance:
$n = 2^m - 1$	$k = 2^m - m - 1$	$n - k = m$	$t = 1$	$d_{min} = 3$

Hard decision decoding: (error detection)

$\because \boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \rightarrow \boldsymbol{S} = \boldsymbol{rH^T} = \boldsymbol{eH^T}$

r: received codeword
e: error pattern
S: syndrome of **r**

2^n possible received vectors
2^k valid codewords
2^{n-k} possible syndromes

2^{n-k} error patterns can be corrected

Error patterns:
$$\binom{n}{e_t} = \frac{n!}{e_t!\,(n-e_t)!}$$

where n is the number of bits in the codeword, and e_t is the type of error (single error implies $e_t = 1$, double error implies $e_t = 2$, etc.)

Polynomial (Cyclic) codes:

Matrices represented previously are now represented as polynomials: (X is the indeterminate)

$$\mathbf{c} = [c_0, c_1, \ldots, c_{n-1}] \rightarrow c(X) = c_0 + c_1X + c_2X^2 + \cdots + c_{n-1}X^{n-1}$$

$$\mathbf{C}(X) = \mathbf{m}(X)\mathbf{g}(X)$$

$g(X) = 1 + g_1X + g_2X^2 + \cdots + g_{n-k-1}X^{n-k-1} + X^{n-k}$ factor of $\boldsymbol{X^n} + \mathbf{1}$

$\mathbf{m}(X) = m_0 + m_1X + m_2X^2 + \ldots + m_{k-1}X^{k-1}$ degree $(k-1)$

rows of the generator matrix have a cyclic shift, e.g., if element x occurs in column 3 of the first row, it will be in column 4 of the second row.

$\because \boldsymbol{GH^T} = \mathbf{0} \rightarrow$
$$\mathbf{g}(X)\mathbf{h}(X) = X^n + 1$$

Steps to finding cyclic codes:
1) Multiply the message polynomial m(X) by X^{n-k}
2) Divide the result from the previous step by the generator polynomial g(X) to obtain the remainder
3) Add the remainder p(X) to X^{n-k}m(X) to form the codeword c(X)

$\mathbf{p}(X) = X^{n-k}\mathbf{m}(X) \bmod \mathbf{g}(X)$
$X^{n-k}\mathbf{m}(X) = \mathbf{q}(X)\mathbf{g}(X) + \mathbf{p}(X)$

$$\boldsymbol{c}(\boldsymbol{x}) = \boldsymbol{X^{n-k}m}(\boldsymbol{X}) + \boldsymbol{p}(\boldsymbol{X}) = \boldsymbol{q}(\boldsymbol{X})\boldsymbol{g}(\boldsymbol{X})$$

Syndrome decoding:
$$\because r(X) = C(X) + e(X) = m(X)g(X) + e(X) = q(X)g(X) + S(X)$$

Syndrome S(X) is the remainder found by dividing r(X) by g(X)

$$\therefore \hat{C}(X) = r(X) + \hat{e}(X) \qquad \text{(corrected codeword)}$$