Lecture 14:

Channel Capacity:

$$C = B\log_2\left(1+\frac{P}{N_0 B}\right) = B\log_2(1+SNR)$$

$$P = E_b R_b$$

$$C = B\log_2\left(1+\frac{E_b R_b}{N_0 B}\right)$$

$$\eta = \frac{C}{B} = \log_2\left(1+\frac{E_b R_b}{N_0 B}\right)$$

C is the maximum rate (max. of R_b) possible while still maintaining error-free transmission.

when transmitting at C, i.e., $R_b = C$, we have:

$$\frac{E_b}{N_0} \text{ or } \frac{R_b}{B} = \log_2\left(1+\frac{E_b}{N_0}\cdot\frac{R_b}{B}\right)$$

or $$1+\frac{E_b}{N_0}\frac{R_b}{B} = 2^{R_b/B}$$

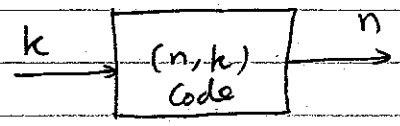
or

$$\frac{E_b}{N_0} = \frac{2^{\frac{R_b}{B}}-1}{\frac{R_b}{B}}$$

Assume, we do not have BW constraint, i.e., we can let $\frac{R_b}{B} \to 0$, then:

$$\frac{E_b}{N_0} = \lim_{R_b/B\to 0} \frac{2^{R_b/B}\ln 2}{1} = \ln 2 \Rightarrow -1.6\,dB$$

Block Coding:



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

Distance:

$$d(C_i, C_j) = \sum_{\ell=1}^{n} C_{i,\ell} \oplus C_{j,\ell} \pmod{q}$$

where q is the number of possible values of components of C_i and C_j

Minimum distance

$$d_{min} = \min\{d(C_i, C_j)\}$$

Weight of a Codeword

$$W(C_i) = \#\text{ of non-zero } C_{i,\ell} \qquad \ell = 1, \ldots, n$$

for Binary codes:

$$W(C_i) = \sum_{\ell=1}^{n} C_{i,\ell}$$

Classes of Block Codes:

Linear Block Codes:

if c_i & $c_j \in \mathbb{C}$

then

$$\alpha_1 c_i + \alpha_2 c_j \in \mathbb{C}$$

where α_1 and α_2 are elements of the code alphabet.

Systematic Codes:

(n, k) code

$\underbrace{k}_{\text{information}}$ $\underbrace{n-k}_{\text{parity}}$

i.e., the first k bits are identical to the [original] information symbols.

Cyclic Codes

if $C = [c_{n-1}, c_{n-2}, \ldots c_0] \in \mathbb{C}$

then $[c_{n-2}, c_{n-3}, \ldots c_0, c_{n-1}] \in \mathbb{C}$

Finite fields

Def.: A field F consists of a set F and two operations $+$ and $\cdot$

1) F is commutative under $+$

$$a+b = b+a$$

2) The identity element w.r.t. $+$

$$a+0 = 0+a = a.$$

3) ~~Non-zero~~ elements of F are commutative under $\cdot$.

$$a \cdot b = b \cdot a.$$

4) The identity element w.r.t. $\cdot$

$$a \cdot 1 = 1 \cdot a = a$$

5) Multiplication is distributive over $+$:

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

6) The additive inverse of a is $-a$ and the multiplicative inverse of a is denoted as a^{-1}.

For any prime p there exists a finite field with p elements; GF(p) called Galois Field.

e.g., $p = 2 \Rightarrow GF(2)$

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

+ is mod. 2 +

For any prime p and any integer m, the field GF(p) can be extended to GF(p^m) field: Called <u>extension field</u>

The elements of the GF(p^m) can be represented as powers of an element α → GF(2^m) e.g.,

$$F = \{0, 1, \alpha, \alpha^2, \ldots \alpha^j, \ldots\}$$

In order to make this a finite field, we need to constraint the number of elements, say by imposing the relation:

$$\alpha^{2^m - 1} = 1$$

give example of GF(2^3) with $P(x) = x^3 + x + 1$

Then

$$\alpha^{2^m+n} = \alpha^{2^m-1} \cdot \alpha^{n+1} = \alpha^{n+1}$$

and the finite field will have 2^m elements

$$GF(2^m) = \{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}\}$$

Multiplication in $GF(2^m)$ is defined as

$$\alpha^j \cdot \alpha^i = \alpha^{i+j}$$

Addition is defined as

$$\alpha^i + \alpha^j = (\alpha_{i,0} + \alpha_{j,0}) + (\alpha_{i,1} + \alpha_{j,1})\lambda + \cdots (\alpha_{j,m-1}, \alpha_{i,n}$$

where $\alpha_i(x) = \alpha_{i,0} + \alpha_{i,1}x + \cdots \alpha_{i,m-1}x^{m-1} = \alpha^i$

represents α^m.

Example:

$$GF(2^6) = GF(64)$$

Primitive Polynomials: Irreducible polynomials $p(x)$ that divides x^n+1 the smallest n for which it divides x^n+1 is $n = 2^m - 1$. For $m = 6$,

$$p(x) = 1 + x + x^6$$

has this property.

We use

$$p(\alpha) = 0$$

i.e.,

$$\alpha^6 + \alpha + 1 = 0$$

to close the field (make it finite).

0		0 0 0 0 0 0	0
1	α^0	0 0 0 0 0 1	1
α	α^1	0 0 0 0 1 0	α
α^2		0 0 0 1 0 0	α^2
α^3		0 0 1 0 0 0	α^3
α^4		0 1 0 0 0 0	α^4
α^5		1 0 0 0 0 0	α^5
α^6	$\alpha+1$	0 0 0 0 1 1	$\alpha+1$
α^7		0 0 0 1 1 0	$\alpha^2+\alpha$
α^8		0 0 1 1 0 0	
α^9			

Table 6.2 Three Representations of the Elements of GF(64)

Power Representation	Polynomial Representation	6-Bit Symbol Representation
$0 = \alpha^{63}$	0	0 0 0 0 0 0
$1 = \alpha^{0}$	1	0 0 0 0 0 1
α	x^1	0 0 0 0 1 0
α^2	x^2	0 0 0 1 0 0
α^3	x^3	0 0 1 0 0 0
α^4	x^4	0 1 0 0 0 0
α^5	x^5	1 0 0 0 0 0
α^6	$x^1 + 1$	0 0 0 0 1 1
α^7	$x^2 + x^1$	0 0 0 1 1 0
α^8	$x^3 + x^2$	0 0 1 1 0 0
α^9	$x^4 + x^3$	0 1 1 0 0 0
α^{10}	$x^5 + x^4$	1 1 0 0 0 0
α^{11}	$x^5 + x^1 + 1$	1 0 0 0 1 1
α^{12}	$x^2 + 1$	0 0 0 1 0 1
α^{13}	$x^3 + x^1$	0 0 1 0 1 0
α^{14}	$x^4 + x^2$	0 1 0 1 0 0
α^{15}	$x^5 + x^3$	1 0 1 0 0 0
α^{16}	$x^4 + x^1 + 1$	0 1 0 0 1 1
α^{17}	$x^5 + x^2 + x^1$	1 0 0 1 1 0
α^{18}	$x^3 + x^2 + x^1 + 1$	0 0 1 1 1 1
α^{19}	$x^4 + x^3 + x^2 + x^1$	0 1 1 1 1 0
α^{20}	$x^5 + x^4 + x^3 + x^2$	1 1 1 1 0 0
α^{21}	$x^5 + x^4 + x^3 + x^1 + 1$	1 1 1 0 1 1
α^{22}	$x^5 + x^4 + x^2 + 1$	1 1 0 1 0 1
α^{23}	$x^5 + x^3 + 1$	1 0 1 0 0 1
α^{24}	$x^4 + 1$	0 1 0 0 0 1
α^{25}	$x^5 + x^1$	1 0 0 0 1 0
α^{26}	$x^2 + x^1 + 1$	0 0 0 1 1 1
α^{27}	$x^3 + x^2 + x^1$	0 0 1 1 1 0
α^{28}	$x^4 + x^3 + x^2$	0 1 1 1 0 0
α^{29}	$x^5 + x^4 + x^3$	1 1 1 0 0 0
α^{30}	$x^5 + x^4 + x^1 + 1$	1 1 0 0 1 1
α^{31}	$x^5 + x^2 + 1$	1 0 0 1 0 1
α^{32}	$x^3 + 1$	0 0 1 0 0 1
α^{33}	$x^4 + x^1$	0 1 0 0 1 0
α^{34}	$x^5 + x^2$	1 0 0 1 0 0
α^{35}	$x^3 + x^1 + 1$	0 0 1 0 1 1
α^{36}	$x^4 + x^2 + x^1$	0 1 0 1 1 0
α^{37}	$x^5 + x^3 + x^2$	1 0 1 1 0 0
α^{38}	$x^4 + x^3 + x^1 + 1$	0 1 1 0 1 1
α^{39}	$x^5 + x^4 + x^2 + x^1$	1 1 0 1 1 0
α^{40}	$x^5 + x^3 + x^2 + x^1 + 1$	1 0 1 1 1 1
α^{41}	$x^4 + x^3 + x^2 + 1$	0 1 1 1 0 1
α^{42}	$x^5 + x^4 + x^3 + x^1$	1 1 1 0 1 0
α^{43}	$x^5 + x^4 + x^2 + x^1 + 1$	1 1 0 1 1 1
α^{44}	$x^5 + x^3 + x^2 + 1$	1 0 1 1 0 1
α^{45}	$x^4 + x^3 + 1$	0 1 1 0 0 1
α^{46}	$x^5 + x^4 + x^1$	1 1 0 0 1 0
α^{47}	$x^5 + x^2 + x^1 + 1$	1 0 0 1 1 1
α^{48}	$x^3 + x^2 + 1$	0 0 1 1 0 1
α^{49}	$x^4 + x^3 + x^1$	0 1 1 0 1 0
α^{50}	$x^5 + x^4 + x^2$	1 1 0 1 0 0
α^{51}	$x^5 + x^3 + x^1 + 1$	1 0 1 0 1 1
α^{52}	$x^4 + x^2 + 1$	0 1 0 1 0 1
α^{53}	$x^5 + x^3 + x^1$	1 0 1 0 1 0
α^{54}	$x^4 + x^2 + x^1 + 1$	0 1 0 1 1 1
α^{55}	$x^5 + x^3 + x^2 + x^1$	1 0 1 1 1 0
α^{56}	$x^4 + x^3 + x^2 + x^1 + 1$	0 1 1 1 1 1
α^{57}	$x^5 + x^4 + x^3 + x^2 + x^1$	1 1 1 1 1 0
α^{58}	$x^5 + x^4 + x^3 + x^2 + x^1 + 1$	1 1 1 1 1 1
α^{59}	$x^5 + x^4 + x^3 + x^2 + 1$	1 1 1 1 0 1
α^{60}	$x^5 + x^4 + x^3 + 1$	1 1 1 0 0 1
α^{61}	$x^5 + x^4 + 1$	1 1 0 0 0 1
α^{62}	$x^5 + 1$	1 0 0 0 0 1

Reed-Solomon Codes:

$d(x)$: information polynomial

$p(x)$: parity polynomial

$c(x)$: codeword polynomial

$g(x)$: generating polynomial

$q(x)$: quotient polynomial

$r(x)$: remainder polynomial.

$$d(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_{2t+1}x^{2t+1} + c_{2t}x^{2t}$$

where $2t = n - k$

$$p(x) = c_0 + c_1 x + \cdots + c_{2t-1}x^{2t-1}$$

$$c(x) = d(x) + p(x) = \sum_{i=0}^{n-1} c_i x^i$$

$$g(x) = (x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t}) = \sum_{i=0}^{2t} g_i x^i$$

to generate $c(x)$, first we write

$$d(x) = g(x)q(x) + r(x)$$

by dividing $d(x)$ by $g(x)$. This results in irrelevant $q(x)$ and important $r(x)$.

Now, the codeword polynomial can be represented as:

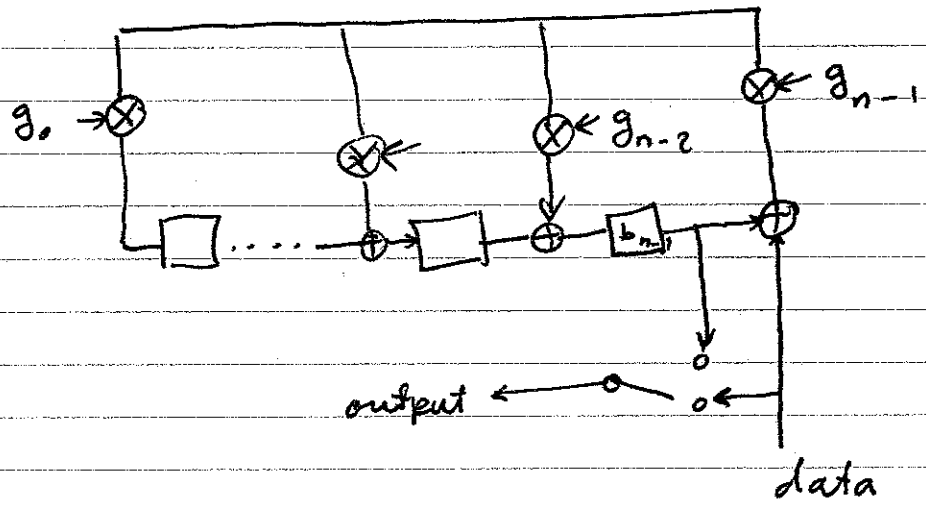
$$c(x) = p(x) + g(x)q(x) + r(x)$$

Since $c(x)$ has to ~~divide~~ be divisible by $g(x)$

[as $c(x) = g(x)d(x)$] then $r(x) = p(x) \Rightarrow p(x) = r(x)$

$\Rightarrow c(x) = g(x)q(x)$

Encoder for RS code



Encoder

$$c(x) = x^{n-k}$$

Example of RS Code:

Take $m = 4 \Rightarrow n = 2^m - 1 = 2^4 - 1 = 15$

So, the blocklength is 15 nibbles (4-bits) or 60 bits.

Take as the primitive polynomial $p(x) = x^4 + x + 1$

Then the elements of the $GF(2^4)$ are:

0	0 0 0 0	0
1	0 0 0 1	α^0
α	0 0 1 0	α^1
α^2	0 1 0 0	α^2
α^3	1 0 0 0	
α^4	0 0 1 1	$\alpha + 1$
α^5	0 1 1 0	$\alpha^2 + \alpha$
α^6	1 1 0 0	$\alpha^3 + \alpha^2$
α^7	1 0 1 1	$\alpha^3 + \alpha + 1$
α^8	0 1 0 1	$\alpha^2 + 1$
α^9	1 0 1 0	$\alpha^3 + \alpha$
α^{10}	0 1 1 1	$\alpha^2 + \alpha + 1$
α^{11}	1 1 1 0	$\alpha^3 + \alpha^2 + \alpha$
α^{12}	1 1 1 1	$\alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	1 1 0 1	$\alpha^3 + \alpha^2 + 1$
α^{14}	1 0 0 1	$\alpha^3 + 1$
$\alpha^{15} = 1$	0 0 0 1	$1 = \alpha^0$

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$$

for a (15, 11) Code since $n-k = 4 = 2t$

$\Rightarrow t = 2$

$$g(x) = [x^2 + (\alpha+\alpha^2)x + \alpha^3][x^2 + (\alpha^4+\alpha^3)x + \alpha^7]$$

$$g(x) = [x^2 + \alpha^5 x + \alpha^3][x^2 + \alpha^{10} x + \alpha^7]$$

$$g(x) = x^4 + \alpha^{15}x^3 + \alpha^7 x^2 + \alpha^5 x^3 + \alpha^{12}x^2 + \alpha^{12}x + \alpha^3 x^2 + \alpha^{10}x + \alpha^{10}$$

$$g(x) = x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}$$

$g_0 = \alpha^{10}$, $g_1 = \alpha^3$, $g_2 = \alpha^6$

$g_3 = \alpha^{13}$, $g_4 = \alpha^0$

$\alpha^5 + \alpha^7 = \alpha^2 + \alpha + \alpha^3 + 1$

$= \alpha^3 + \alpha^2 + 1$

$= \alpha^{13}$

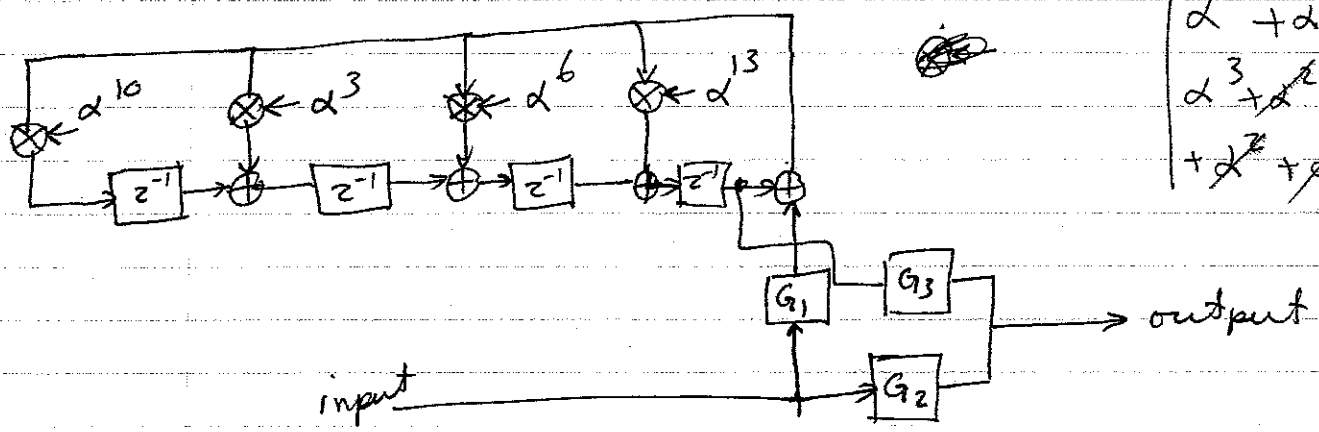
$\alpha^7 + \alpha^{12} + \alpha^3$

$= \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha$

$= \alpha^3 + \alpha^2$

$\alpha^{12} + \alpha^{10} =$

$\alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + 1$



Reed-Solomon Decoding:

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

$$r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$$

$$e(x) = r(x) - c(x) = e_0 + e_1 x + \cdots + e_{n-1} x^{n-1}$$

since:

$$c(x) = \underbrace{(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t})}_{g(x)}\, q(x)$$

$$c(\alpha^i) = 0 \qquad i = 1, \ldots, 2t$$

so:

$$S_i = r(\alpha^i) = e(\alpha^i) \qquad i = 1, \ldots, 2t$$

i.e., the syndrome only depends on the error pattern.

Assume, we have p errors at locations $j_1, j_2, \cdots j_p$ then

$$e(x) = e_{j_1} x^{j_1} + e_{j_2} x^{j_2} + \cdots + e_{j_p} x^{j_p}$$

$$S_1 = e(\alpha) = e_{j_1} \alpha^{j_1} + e_{j_2} \alpha^{j_2} + \cdots + e_{j_p} \alpha^{j_p}$$

$$S_2 = e(\alpha^2) = e_{j_1} (\alpha^{j_1})^2 + e_{j_2} (\alpha^{j_2})^2 + \cdots + e_{j_p} (\alpha^{j_p})^2$$

$$\vdots$$

$$S_{2t} \quad e(\alpha^{2t}) = e_{j_1} (\alpha^{j_1})^{2t} + e_{j_2} (\alpha^{j_2})^{2t} + \cdots + e_{j_p} (\alpha^{j_p})^{2t}$$

let $\alpha^{j_1} = \beta_1$, $\alpha^{j_2} = \beta_2$, ... $\alpha^{j_p} = \beta_p$

then:

$$S_1 = e_{j_1}\beta_1 + e_{j_2}\beta_2 + \cdots + e_{j_p}\beta_p$$

$$S_2 = e_{j_1}\beta_1^2 + e_{j_2}\beta_2^2 + \cdots + e_{j_p}\beta_p^2$$

$$\vdots$$

$$S_{2t} = e_{j_1}\beta_1^{2t} + e_{j_2}\beta_2^{2t} + \cdots + e_{j_p}\beta_p^{2t}$$

2t equations in 2p un-knowns: p, β_{j_i}'s and p, e_{j_i}'s. So, the maximum of p is t, i.e., at most t errors locations/values can be found.

Decoding Procedure:

$r(\alpha^i) = [\cdots((r_{n-1}\alpha^i + r_{n-2})\alpha^i + r_{n-3})\cdots]\alpha^i + r_0$

1) Find syndromes:

$$S_i = r(\alpha^i) \qquad i = 1, 2, \cdots, 2t$$

2) Find error locator polynomial

$$\sigma(x) = (1+\beta_1 x)(1+\beta_2 x)\cdots(1+\beta_p x) = \sigma_0 + \sigma_1 x + \cdots \sigma_p x^p$$

where $\sigma_0 = 1$

$$\sigma_1 = \beta_1 + \beta_2 + \cdots + \beta_p$$

$$\sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \cdots + \beta_{p-1}\beta_p$$

$$\vdots$$

$$\sigma_p = \beta_1\beta_2\cdots\beta_p$$

Syndromes and σ_j's can be related as

$$S_1 + \sigma_1 = 0$$

$$S_2 + \sigma_1 S_1 + 2\sigma_2 = 0$$

$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3 = 0$$

$$\vdots$$

$$S_p + \sigma_1 S_{p-1} + \cdots \sigma_{p-1} S_1 + p\sigma_p = 0$$

3) Solve $\sigma(x)$ using Chien search to find β_j's (error locations)

4) Find error values.

5) Correct errors.

Coded Performance

Prob. of Symbol (m-bit) error

$$P_e = \sum_{i=t+1}^{n} \frac{i+t}{n} \binom{n}{i} P_c^i (1-P_c)^{n-i}$$

where P_c is the un-coded symbol error probability,

i.e. $P_c = 1-(1-P_u)^m \approx m P_u$

where P_u is the un-coded bit error probability

for example for BPSK or QPSK

$$P_u = Q\left(\sqrt{\frac{2E_c}{N_o}}\right) = \frac{1}{2}\,erfc\left(\sqrt{\frac{E_c}{N_o}}\right)$$

where E_c is the energy per uncoded bit

$$E_c = \frac{k}{n}E_b = r E_b$$

So:

$$P_u = Q\left(\sqrt{\frac{2E_b}{N_o}\times\frac{r}{1}}\right) = \frac{1}{2}\,erfc\left(\sqrt{\frac{E_b}{N_o}r}\right)$$

where r is the code rate $\left(r = \frac{k}{n}\right)$

Coded bit error rate will be:

$$P_B \approx \frac{1}{2}P_E = \frac{1}{2n}\sum_{i=t+1}^{n}\frac{(i+t)}{m}\binom{n}{i}P_c^{\,i}(1-P_c)^{n-i}$$

for non-bi case

assuming that out of m bits in error (in a symb on the average, half of the bits are in error.

For binary case $P_B = P_E = \frac{1}{n}\sum (i+n)\binom{n}{i}P_c^{\,i}(1-P_c$

14-17

example: (204, 188) RS Code for DVB

$$t = \frac{204 - 188}{2} = 8 \text{ bytes}$$

So, it can correct any error burst of length $(t-1)m = 56$ bits

$$P_B = \frac{1}{2} \sum_{i=9}^{204} \left(\frac{i+8}{204}\right) \binom{204}{i} P_c^i (1 - P_c)^{204-i}$$

$$P_c = 1 - (1 - P_u)^8 \simeq 8 P_u$$

Assume that, we use this code with a QPSK (or BPSK) modulator with $\frac{E_b}{N_0} = 4$ dB

without coding $P_B = \frac{1}{2} \text{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right) = 0.0125 = 1.25 \times 10^{-2}$

for coded case

$$\frac{E_c}{N_0} = \frac{E_b}{N_0} \times \frac{188}{204} = 10^{0.4} \left(\frac{188}{204}\right) = 2.3149$$

$$P_u = 0.0157 = 1.57 \times 10^{-2} \Rightarrow P_c = 8 P_u = 0.125$$

$$P_B = \frac{1}{2} \sum_{i=9}^{204} \left(\frac{i+8}{204}\right) \binom{204}{i} (0.125)^i (1 - 0.125)^{204-i}$$

$$P_B \simeq \frac{1}{2} \left(\frac{17}{204}\right) \binom{204}{9} (0.125)^9 (1 - 0.125)^{195}$$

$$P_B \simeq 2.15 \times 10^{-6}$$

Hilroy

Example:

Consider a system using QPSK at $\frac{E_b}{N_0} = 6$ dB. Study the effect of using a (255, 239) RS Code:

a) Uncoded

$$\frac{E_b}{N_0} = 6 \text{ dB} \Rightarrow \frac{E_b}{N_0} = 10^{0.6} = 3.981 \Rightarrow P_B = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

$$Q(x) \approx \frac{1}{\sqrt{\pi}x} e^{-\frac{x^2}{2}} \Rightarrow P_B = Q\left(\sqrt{3.981 \times 2}\right) = Q\left(\sqrt{7.962}\right) \approx \frac{1}{\sqrt{\pi}\times\sqrt{7.962}} e^{-\frac{7.962}{2}} = 0.00373 \approx \frac{4}{1000}$$

b) Coded

$$\frac{E_c}{N_0} = \frac{239}{255} \times \frac{E_b}{N_0} = 3.731$$

$$P_u = Q\left(\sqrt{7.462}\right) \approx \frac{1}{\sqrt{\pi}\sqrt{7.462}} e^{-\frac{7.462}{2}} = 0.00495$$

$$P_c = 8 \times 0.00495 \approx 0.0396$$

$$P_B = \frac{1}{2\times 255} \sum_{i=9}^{255} (i+8)\binom{255}{i}(0.0396)^i (1-0.0396)^{255-i}$$

$$P_B \simeq \frac{1}{2\times 255}(9+8)\binom{255}{9}(0.0396)^9 (1-0.0396)^{246} \simeq 0.0041$$

uncoded) $\frac{E_b}{N_0} = 7 \Rightarrow \frac{E_b}{N_0} = 10^{0.7} \simeq 5.015 \Rightarrow P_B = Q\left(\sqrt{10.023}\right) \simeq 0.001187 \approx 1.2\times 10^{-3}$

coded $\frac{E_b}{N_0} = 4.7 \Rightarrow P_u = Q\left(\sqrt{9.4}\right) = 0.00167 \Rightarrow P_c = 0.01336$

$P_B = 0.0001799 \approx 1.8\times 10^{-4}$