EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran

Indian Institute of Technology Bombay

Autumn 2010

Solutions to Assignment 1 Prepared by Sravan Kumar Jatavath

1. BSC with cross-layer probability p . N bits are transmitted.

   (a)

$$\begin{aligned}\Pr(\text{exactly one error}) &= \Pr(\text{error at only one position}) \\ &= \binom{N}{1} p(1-p)^{N-1} \\ &= Np(1-p)^{N-1}\end{aligned}$$

   (b)

$$\begin{aligned}\Pr(\text{atleast one error}) &= 1-\Pr(\text{no error}) \\ &= 1-(1-p)^N\end{aligned}$$

   (c)

$$\begin{aligned}\Pr(\text{atmost one error}) &= \Pr(\text{zero errors})+\Pr(\text{one error}) \\ &= (1-p)^N + N.(1-p)^{N-1} \\ &= (1-p)^{N-1}[1-p+N.p] \\ &= (1-p)^{N-1}[1+p(N-1)].\end{aligned}$$

2. Given that a sequence of N bits is passed through a cascade of two BSCs with crossover probabilities p_1 and p_2 , respectively.

   (a) Pr(exactly k errors)
   For this, we model the cascade as one single BSC. Trivially, for a bit,

$$\begin{aligned}\Pr(\text{error}) &= \Pr(\text{error in BSC1, no error BSC2})+\Pr(\text{no error in BSC1, error in BSC2}) \\ &= p_1\cdot(1-p_2)+p_2\cdot(1-p_1) \\ &= p_1+p_2-2p_1p_2\end{aligned}$$

   Let us denote $p_3 = p_1+p_2-2p_1p_2$. Then Pr(bit error) $= p_3$.

$$\begin{aligned}\Pr(\text{no error}) &= \Pr(\text{error in BSC1, error in BSC2})+\Pr(\text{no error in BSC1,no error in BSC2}) \\ &= p_1\cdot p_2+(1-p_1)\cdot(1-p_2) \\ &= 1+2p_1p_2-p_1-p_2 \\ &= 1-p_3\end{aligned}$$

$$\Pr(\text{exactly } k \text{ errors}) = \binom{N}{k} p_3^k (1-p_3)^{N-k}$$

(b)

$$\Pr(\text{atleast } k \text{ errors}) = \sum_{i=k}^{N} \binom{N}{i} p_3^i (1-p_3)^{N-i}$$

(c)

$$\Pr(\text{atmost } k \text{ errors}) = \sum_{i=0}^{k} \binom{N}{i} p_3^i (1-p_3)^{N-i}$$

3. Since binary source generates bits equally likely to be 0 or 1, maximum likelihood (ML) decoding will be the optimal decoding since it minimizes the average probability of error. The cascade of the two BSCs can be considered to be a single BSC with crossover probability $p_3 = p_1 + p_2 - 2p_1p_2$. If $p_1 < 0.5$ and $p_2 < 0.5$, then $p_3 < 0.5$. Let r be the received codeword and c_i be the transmitted codeword when the source bit is i. Then we have $c_0 = 000$, $c_1 = 111$. The ML rule is given by

$$\hat{c} = \arg\max_{c_i} \Pr(r|c_i) = \arg\max_{c_i} p_3^{d_H(r,c_i)}(1-p_3)^{3-d_H(r,c_i)}$$

where $d_H(x,y)$ is the Hamming distance between x and y.

In this case, the ML rule reduces to minimum distance decoding, i.e. deciding 0 was transmitted if $d_H(r,c_0)$ is smaller than $d_H(r,c_1)$ and deciding 1 was transmitted otherwise.

4. (a) If $p_1 = p_2 = p_3 < \frac{1}{2}$, the situation is essential same as that of 3-repetition code and hence optimal decoding rule will be the minimum distance decoder as above. If $p_1 = p_2 = p_3 > \frac{1}{2}$, the optimal decoder is one which inverts the received bits and then performs minimum distance decoding. If all the probabilities are equal to $\frac{1}{2}$, then any decoding rule will be optimal.

   (b) If $p_1 > p_2 > p_3$, no single decoding rule is optimal for all values of p_1, p_2 and p_3. Suppose $p_1 < \frac{1}{2}$.

$$\begin{aligned}
p(000|0) &= (1-p_1)(1-p_2)(1-p_3) > p_1p_2p_3 = p(000|1)\\
p(001|0) &= (1-p_1)(1-p_2)p_3 > p_1p_2(1-p_3) = p(001|1)\\
p(010|0) &= (1-p_1)p_2(1-p_3) > p_1(1-p_2)p_3 = p(010|1)\\
p(100|0) &= p_1(1-p_2)(1-p_3) > (1-p_1)p_2p_3 = p(100|1)
\end{aligned}$$

   Hence, the received codewords 000,010,100 resulting in the decision that a 0 was transmitted. The received codewords 111,101,011 result in the decision that a 1 was transmitted. Decisions for for 001 and 110 depends on the relative magnitudes of p_1, p_2 and p_3

5. (a) $a \star b = a - b$
   $(a \star b) \star c = (a - b) - c = a - b - c$
   $a \star (b \star c) = a - (b - c) = a - b + c \Rightarrow$ NOT Associative

   (b) $a \star b = a + b + ab$
   $(a \star b) \star c = (a + b + ab) + c + c(a + b + ab) = (a + b + c) + (ab + bc + ac) + abc$
   $a \star (b \star c) = a + (b + c + bc) + a(b + c + bc) = a + b + c + (ab + bc + ac) + abc$
   $\Rightarrow$ Associative.

   (c) $a \star b = \frac{a+b}{5}$ and $b \star c = \frac{b+c}{5}$
   $(a \star b) \star c = \frac{\frac{a+b}{5}+c}{5} = \frac{a+b+5c}{25}$
   $a \star (b \star c) = \frac{a+\frac{b+c}{5}}{5} = \frac{5a+b+c}{25} \Rightarrow$ NOT Associative

   (d) $(a, b) \star (c, d) = (ad + bc, bd)$
   $((a, b) \star (c, d)) \star (e, f) = ((ad + bc)f + bde, bdf)$
   $(a, b) \star (c, d) \star (e, f) = (adf + b(cf + de), bdf) = ((ad + bc)f + bde, bdf) \Rightarrow$ Associative

   (e) $a \star b = \frac{a}{b}$
   $(a \star b) \star c = \frac{(\frac{a}{b})}{c} = \frac{a}{bc}$ $\qquad a \star (b \star c) = \frac{a}{\frac{b}{c}} = \frac{ac}{b}$
   $\Rightarrow$ Not Associative.

6. (a) $a \star b = a - b \neq b - a = b \star a \Rightarrow$ NOT Commutative

   (b) Commutative (by symmetry of the operation with respect to a and b)

   (c) Commutative (by symmetry of the operation with respect to a and b)

   (d) $(a, b) \star (c, d)$ =(ad+bc,bd),(c,d)$\star$(a,b) =(bc+ad,bd)
   $\Rightarrow$ Commutative

   (e) $\frac{a}{b} \neq \frac{b}{a} \Rightarrow$ NOT Commutative

7. (a) Let $\mathbb{Q}^*$ be the set of rational numbers with odd denominators, i.e. $\mathbb{Q}^* = \{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{N}, q = 1 \bmod 2, \gcd(p, q) = 1\}$. We need to verify closure, associativity, existence of identity and inverse.

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}$$

   qs is odd as both q and s are odd. If the numerator and denominator have factors in common, they will be odd factors and eliminating them will still result in an odd denominator. Hence, closure is satisfied. Addition is trivially associative.
   Zero is the identity, since $\frac{p}{q}+\frac{0}{1}=\frac{p}{q}$ and $\frac{0}{1} \in \mathbb{Q}^*$.
   Additive inverse of $\frac{p}{q} = -\frac{p}{q}$, as $\frac{p}{q} + (-\frac{p}{q}) = 0$ and $(-\frac{p}{q}) + (\frac{p}{q}) = 0$ and -$\frac{p}{q} \in \mathbb{Q}^*$ with odd denominators.

   (b) Let $\mathbb{Q}^*$ be the set of rationals with even denominators, i.e. $\mathbb{Q}^* = \{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{N}, q = 0 \bmod 2, \gcd(p, q) = 1\}$.
   $\frac{p}{q} \in \mathbb{Q}^* \Rightarrow \gcd(p, q) = 1$, q=even.
   Consider $\frac{r}{s} \in \mathbb{Q}^*$ where , $s = 2k$ with k=odd
   $\frac{r}{s} + \frac{r}{s} = \frac{2r}{s} = \frac{2r}{2k} = \frac{r}{k}$
   But, k is odd, hence $\frac{r}{k} = \frac{r}{s} + \frac{r}{s} \notin \mathbb{Q}^*$.

Hence, this set is NOT closed under addition and is NOT a group.

(c) $\mathbb{Q}^*$ = set of rational numbers with absolute value less than 1, i.e. $\mathbb{Q}^*$=$\{a : a \in \mathbb{Q}, |a| < 1\}$.
Consider $b, c \in \mathbb{Q}^*$, such that $b = c = 0.5$. Then $b + c = 1 \notin \mathbb{Q}^*$. Hence, this is NOT the group under addition.

(d) $\mathbb{Q}^*$= set of rational numbers with absolute values $\geq$ 1 and zero, i.e. $\mathbb{Q}^* = \{0\} \cup \{a : a \in \mathbb{Q}, |a| \geq 1\}$
Consider,$a, b \in \mathbb{Q}^*, a = 1.5, b = -1.0, a + b = 0.5 < 1$. Thus $a + b \notin \mathbb{Q}^*$. Hence, this is NOT a group under addition.

8. G = {z $\in$ C | z^n = 1 for some n $\in$ Z^+ }.

(a) Operation : Multiplication
$a \in G$, b $\in G \Rightarrow a^k = 1$, $b^l = 1$ for some k,l $\in Z^+$.
c = a.b = $1^{\frac{1}{k}}$. $1^{\frac{1}{l}}$ = $1^{\frac{l+k}{lk}} \Rightarrow (a.b)^{\frac{lk}{l+k}} = (c)^{\frac{lk}{l+k}} = 1$.
Consider, (ab)$^{k+l}$ = a^{k+l}.b^{k+l} = (a^k)^l.(b^l)^k = 1
k$\in$ Z$^+$, l $\in$ Z$^+$ $\Rightarrow$ k+l $\in$ Z$^+$
Hence, closure.(i.e., multiplication is valid binary operation here)

Note that 1$\in G$, and 1.a = a.1 = a. Hence, identity.
Now, for a$\in G$, a^n=1 for some n $\in$ Z$^+$.
If n=1, a=1 and a=a^{-1}(trivially).
If n$\neq$1, choose a^{-1} = a^{n-1}
$\Rightarrow$ a.a^{n-1} = a^{n-1} = a^n = 1
Hence, inverse exists. Hence,this G is a group under multiplication.

(b) Operation : Addition
Consider a=1, b=1, a,b $\in G$ (trivially)
a+b = 2 > 1 $\Rightarrow$ There exists no n$\in$Z$^+$ such that 2^n=1, since 2$^n \geq$ 2 for n$\in$ Z$^+$.
Hence, addition NOT a valid close binary operation here. Hence, G is NOT a group under addition.

9. Let G = {a+b$\sqrt{2}$ $\in$R || a,b$\in$Q}

(a) Operation : Addition
consider z$_1$, z$_2$ $\in G$, z$_1$=a+b$\sqrt{2}$, z$_2$ = c+d$\sqrt{2}$
z$_3$ = z$_1$ + z$_2$ = (a+c) + (b+d)$\sqrt{2}$
a+c$\in$Q, b+d$\in$Q $\Rightarrow$ z$_3$ $\in G$
Hence, addition a valid binary operation over this group.
Addition is trivially associative.
0 is an identity, since 0+0$\sqrt{2}$, 0$\in$Q and 0+a+b$\sqrt{2}$ = a+b$\sqrt{2}$+0 = a+b$\sqrt{2}$.
Inverse for z$_1$ = a+b$\sqrt{2}$ will trivially be $-$a$-$b$\sqrt{2}$. Since $-$a,$-$b$\in$Q

(b) Operation : Multiplication
G= {a+b$\sqrt{2}$ $\in$R || a,b$\in$Q and a,b both not 0 simultaneously}

z$_1$ $\in G$, z$_2$ $\in G$, z$_1$ = a+b$\sqrt{2}$, z$_2$ = c+d$\sqrt{2}$
z$_1$.z$_2$ = (a+b$\sqrt{2}$)(c+d$\sqrt{2}$) = (ac+2bd) + (ad+bc)$\sqrt{2}$
ac+2bd$\in G$, ad+bc$\in G$
if ac+2bd$\neq$0 when ad+bc=0 and vice versa which can be verified as follows,
ad+bc=0 $\Rightarrow$ ad=$-$bc $\Rightarrow$ a=$\frac{-bc}{d}$
Need to show, $\frac{-bc^2}{d}$+2bd $\neq 0$
$-$c^2 + 2d^2 $\neq 0$
2d^2 $\neq$ c^2
$\sqrt{2}$d $\neq \pm$c which is trivial since c,d$\in$Q.
Similarly, the other case follows.
Now, z$_1$ Associativity is trivial for multiplication.
1.z$_1$ = z$_1$.1 = z$_1$ $\Rightarrow$ 1 is the identity.
Now, for inverse,
we need z$_1$.z$_2$ = z$_2$.z$_1$ = 1
$\Rightarrow$ (a+b$\sqrt{2}$)z$_2$ = 1
z$_2$ = $\frac{a}{(a+b\sqrt{2})}$
z$_2$ = $\frac{a}{(a^2-2b^2)}$ + $\frac{-b}{(a^2-2b^2)}$ $\sqrt{2}$
$\frac{a}{a^2-2b^2}$ $\in$Q , $\frac{-b}{a^2-2b^2}$ $\in$Q, z$_2$ $\in G$
Hence, G is a group under multiplication.

10. To prove that a group G is abelian if $x^2 = 1$ for all $x \in G$. Here the operation is some kind of a product and 1 is the identity of the operation. So every element x is equal to its inverse x^{-1}. For any $x, y \in G$, $xy \in G$, so $(xy)^2 = 1$.

$$1 = (xy)^2 = xyxy \Rightarrow xyx = y^{-1} = y$$

Now

$$xy = x(xyx) = x^2yx = 1 \cdot yx = yx$$

Since x and y is arbitrarily chosen, G is abelian.

11. To prove that A×B is *abelian* iff A,B are *abelian.*

(a) Given A,B are abelian. We want to prove that A×B abelian.
Let a$\in$A, b$\in$B, then (a,b) $\in$ A×B.
Now, consider,
(a$_1$,b$_1$)$\star$(a$_2$,b$_2$) = (a$_3$,b$_3$) = (a$_1\star$a$_2$, b$_1\star$b$_2$) = (a$_2\star$a$_1$, b$_2\star$b$_1$)
(a$_2$,b$_2$)$\star$(a$_1$,b$_1$) = (a$_2\star$a$_1$, b$_2\star$b$_1$)
Hence, A × B is abelian.

(b) Given A×B is abelian.
To Prove That: A,B abelian.
(a$_1$,b$_1$)$\star$(a$_2$,b$_2$) = (a$_2$,b$_2$)$\star$(a$_1$,b$_1$)
(a$_1\star$a$_2$, b$_1\star$b$_2$) = (a$_2\star$a$_1$, b$_2\star$b$_1$)
a$_1\star$a$_2$ = a$_2\star$a$_1$ $\Rightarrow$ A is abelian
b$_1\star$b$_2$ = b$_2\star$b$_1$ $\Rightarrow$ B is abelian

12. m is a positive integer which is not a prime
    Set G = {1,2,3,......,(m-1)}
    Operation = (multiplication) mod m
    since m$\neq$prime,
    m will have factors other than 1,m.
    $\Rightarrow \exists$ a,b s.t m=ab and a,b$\in$ {1,2,3,......,(m-1)}
    Hence, (a.b)mod m = m mod m = 0
    Hence, this set is NOT closed under multiplication. Hence it is not a valid binary operation.
    Hence, G is NOT a group.