EE/Ma 127c Error-Correcting Codes - Homework Assignment 1

Ling Li, ling@cs.caltech.edu

April 10, 2001

1.1 Let $f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$ denote the probability distribution function (pdf) of $\mathcal{N}(0, \sigma^2)$. When $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is sent, the probability that $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ is received is

$$p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} f(y_i - x_i)$$

since $y_i = x_i + z_i$ and z_i are i.i.d.$\sim \mathcal{N}(0, \sigma^2)$. Assume all codewords are sent with equal probabilities. Then the maximum-likelihood decoding (MLD) is to find the codeword $\mathbf{x}$ with maximal $p(\mathbf{y}|\mathbf{x})$, i.e., with minimal

$$d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} (y_i - x_i)^2.$$

The $(n, 1)$ repetition code has only two codewords, $(+1, +1, \ldots, +1)$ and $(-1, -1, \ldots, -1)$. Thus finding the minimal $d(\mathbf{x}, \mathbf{y})$ is equivalent to calculating the sign of

$$\sum_{i=1}^{n} (y_i + 1)^2 - \sum_{i=1}^{n} (y_i - 1)^2 = 4 \sum_{i=1}^{n} y_i.$$

Below is an MLD algorithm for this code (and this channel):

(a) Calculate

$$s = \sum_{i=1}^{n} y_i.$$

If $s > 0$, the ML codeword is $(+1, +1, \ldots, +1)$; if $s < 0$, the ML codeword is $(-1, -1, \ldots, -1)$; if $s = 0$, there is a tie and we can use either codeword.

(b) By symmetry, assume the sent codeword is $(+1, +1, \ldots, +1)$. The decoder error probability is

$$P_e = \Pr\{s \le 0 | (+1, +1, \ldots, +1) \text{ sent}\}.$$

From $y_i = x_i + z_i = 1 + z_i$, $s = \sum y_i$ is a random variable$\sim \mathcal{N}(n, n\sigma^2)$. Thus

$$P_e = \Pr\{s - n \le -n | (+1, +1, \ldots, +1) \text{ sent}\} = Q\left(\frac{n}{\sqrt{n\sigma^2}}\right) = Q\left(\sqrt{2\frac{E_b}{N_0}}\right), \qquad (1)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2} dt$.

(c) From (1), the performance of using $(n,1)$ repetition code is just the same as that of uncoded BPSK, if $\frac{E_b}{N_0}$ remains the same.

1.2 Let $d_{\min}$ denote the minimum distance of the code. Let P denote a "best" interleaver (a permutation matrix that maximizes $d_{\min}$). The codeword with information $\mathbf{u}$ is $(\mathbf{u}G, \mathbf{u}PG)$. For a specific input $\mathbf{u} = (1,0,0,0)$, whatever P is, $\mathbf{u}P$ is of weight 1; and since every row of G is of weight 2, the encoder produces a codeword of weight 4. Thus $d_{\min} \leq 4$.

In order to make $d_{\min} = 4$ (we do not know whether $d_{\min} = 4$ is achievable or not; however we can try), there should not be some non-zero codeword $(\mathbf{u}G, \mathbf{u}PG)$ with weight less than 4. Notice that the weight of each row of G is even. Thus the weights of $\mathbf{u}G$ and $\mathbf{u}PG$ are also even. So we need only to ensure for any $\mathbf{u}$, if $\mathbf{u}G = \mathbf{0}$ then $\mathbf{u}PG$ is not of weight 2, and if $\mathbf{u}PG = \mathbf{0}$, then $\mathbf{u}G$ is not of weight 2.

$\mathbf{u}G = \mathbf{0}$ gives $\mathbf{u} = \mathbf{0}$ or $\mathbf{u} = (0,0,1,1)$. $\mathbf{u} = \mathbf{0}$ always gives $\mathbf{u}PG = \mathbf{0}$, which is not of weight 2. For $\mathbf{u} = (0,0,1,1)$, that $\mathbf{u}PG$ is not of weight 2 gives $\mathbf{u}P = (1,1,0,0)$ or $(0,0,1,1)$ (note that the weight of $\mathbf{u}P$ should also be 2). Thus P should be one of

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Similarly, from $\mathbf{u}PG = \mathbf{0}$ and $\mathbf{u}G$ is not of weight 2, we know P should be one of

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & 0 & 0 \end{pmatrix}, \begin{pmatrix} \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Thus there are eight choices for P, which denoted by the positions of 1's in each row, are $(1,2,3,4)$, $(1,2,4,3)$, $(2,1,3,4)$, $(2,1,4,3)$, $(3,4,1,2)$, $(3,4,2,1)$, $(4,3,1,2)$, and $(4,3,2,1)$.

However, the rank of G is 3, and $\mathbf{u}G$ is the same if $u_3 + u_4$ is the same. Thus in order to ensure the code has dimension 4, we have to "shift" u_3 and/or u_4 out of positions 3 and 4. Thus P can only be $(3,4,1,2)$, $(3,4,2,1)$, $(4,3,1,2)$, or $(4,3,2,1)$.

1.3 By Bayes' rule,

$$\begin{aligned} \Pr\{u_i = a | \mathbf{Y} = \mathbf{y}\} &= \frac{1}{\Pr\{\mathbf{Y} = \mathbf{y}\}} \sum_{\mathbf{u}:u_i = a} \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{U} = \mathbf{u}\} \Pr\{\mathbf{U} = \mathbf{u}\} \\ &= \frac{1}{\Pr\{\mathbf{Y} = \mathbf{y}\}} p^0(a) \sum_{\mathbf{u}:u_i = a} \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{X} = \mathbf{u}G\} \prod_{j \neq i} p^0(u_j) \end{aligned}$$

Let

$$Q_i(a) = \sum_{\mathbf{u}:u_i = a} \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{X} = \mathbf{u}G\} \prod_{j \neq i} p^0(u_j).$$

That is,

$$\begin{aligned} Q_1(a) &= \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{X} = (a,0)G\} p^0(0) + \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{X} = (a,1)G\} p^0(1), \\ Q_2(a) &= \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{X} = (0,a)G\} p^0(0) + \Pr\{\mathbf{Y} = \mathbf{y} | \mathbf{X} = (1,a)G\} p^0(1). \end{aligned}$$

Then the *a posteriori* probability for u_i is (where $j \neq i$)

$$\log \frac{\Pr\{u_i = 0|\mathbf{Y} = \mathbf{y}\}}{\Pr\{u_i = 1|\mathbf{Y} = \mathbf{y}\}} = \log \frac{p^0(0)}{p^0(1)} + \log \frac{Q_i(0)}{Q_i(1)}$$

(a) $p^0(0) = p^0(1) = \frac{1}{2}$, $\mathbf{y} = ABCD$. We have* $Q_1(0) = \frac{5}{2^{10}}$, $Q_1(1) = \frac{17}{2^{13}}$, $Q_2(0) = \frac{3}{2^{10}}$, $Q_2(1) = \frac{33}{2^{13}}$. Thus the "extrinsic information" for u_1 is $\log \frac{Q_1(0)}{Q_1(1)} = \log \frac{40}{17} \approx 1.2345$, for u_2 is $\log \frac{Q_2(0)}{Q_2(1)} = \log \frac{8}{11} \approx -0.4594$. Since $\log \frac{p^0(0)}{p^0(1)} = 0$, the *a posteriori* probabilities are equal to the extrinsic informations.

(b) $p^0(0) = \frac{1}{3}$, $p^0(1) = \frac{2}{3}$, $\mathbf{y} = ABCD$. We have $Q_1(0) = \frac{3}{2^9}$, $Q_1(1) = \frac{3}{2^{11}}$, $Q_2(0) = \frac{5}{3\times 2^9}$, $Q_2(1) = \frac{17}{3\times 2^{11}}$. Thus the "extrinsic information" for u_1 is $\log \frac{Q_1(0)}{Q_1(1)} = 2$, for u_2 is $\log \frac{Q_2(0)}{Q_2(1)} = \log \frac{20}{17} \approx 0.2345$. Since $\log \frac{p^0(0)}{p^0(1)} = -1$, the *a posteriori* probability of u_1 is 1 and that of u_2 is $\log \frac{10}{17} \approx -0.7655$.

1.4 Every path from u to v that passes edge e consists of 3 parts: a path from u to x, the edge e (which is from x to y), and a path from y to v. Thus

(a)

$$\begin{aligned}
\mu_e(u,v) &= \sum_{P:u \overset{e}{\mapsto} v} w(P) \\
&= \sum_{P_1:u\mapsto x} \sum_{P_2:y\mapsto v} w(P_1 e P_2) \\
&= \sum_{P_1:u\mapsto x} \sum_{P_2:y\mapsto v} w(P_1)w(e)w(P_2) && (2) \\
&= \left(\sum_{P_1:u\mapsto x} w(P_1)\right) \cdot w(e) \cdot \left(\sum_{P_2:y\mapsto v} w(P_2)\right) && (3) \\
&= \mu(u,x) \cdot w(e) \cdot \mu(y,v).
\end{aligned}$$

(b) Suppose totally there are M paths from u to x and N paths from y to v. Then there are MN paths from u to v that passes e. And suppose we already have those $w(P_1)$ and $w(P_2)$. Equation (2) needs $2MN$ multiplications and $MN-1$ additions. If we "lift" $w(e)$ out of the loop (that is, using the distribution law), (2) still needs $MN+1$ multiplications and $MN-1$ additions. However, equation (3) needs 2 multiplications and $M+N-2$ additions. The computational savings are $2(MN-1)$ multiplications and $(M-1)(N-1)$ additions, for the first case, and $MN-1$ multiplications and $(M-1)(N-1)$ additions for "lifting" $w(e)$ out of the loop.

---

*Example calculation for u_1:

$$\begin{aligned}
Q_1(0) &= \Pr\{\mathbf{Y} = ABCD|\mathbf{X} = 0000\}\, p^0(0) + \Pr\{\mathbf{Y} = ABCD|\mathbf{X} = 0111\}\, p^0(1) \\
&= \frac{1}{2}\cdot\frac{1}{4}\cdot\frac{1}{8}\cdot\frac{1}{8}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{8}\cdot\frac{1}{4}\cdot\frac{1}{2}\cdot\frac{1}{2} = \frac{5}{2^{10}}, \\
Q_1(1) &= \Pr\{\mathbf{Y} = ABCD|\mathbf{X} = 1011\}\, p^0(0) + \Pr\{\mathbf{Y} = ABCD|\mathbf{X} = 1100\}\, p^0(1) \\
&= \frac{1}{8}\cdot\frac{1}{4}\cdot\frac{1}{4}\cdot\frac{1}{2}\cdot\frac{1}{2} + \frac{1}{8}\cdot\frac{1}{8}\cdot\frac{1}{8}\cdot\frac{1}{8}\cdot\frac{1}{2} = \frac{17}{2^{13}}.
\end{aligned}$$