1. A signal \( X \in \{0, 1\} \) is transmitted through a binary symmetric channel with crossover probability \( p \). Assume \( X = 0 \) or \( 1 \) with equal probability. Suppose \( X \) is sent \( n \) times, each time the channel output \( Y_i \) follows

\[
Y_i = X \oplus Z_i,
\]

where “\( \oplus \)” is the modulo 2 addition, and \( Z_i \)’s are independent \( \text{Bern}(p) \) random variables. Further assume \( X \) and all \( Z_i \)’s are independent.

a. Compute

\[
P(Y_1 = y_1, \ldots, Y_n = y_n | X = x)
\]

where \( y_i \in \{0, 1\} \) for \( i = 1, 2, \ldots, n \).

b. Suppose \( T = \sum_{i=1}^{n} Y_i \). Compute

\[
P(T = t)
\]

for \( t = 0, \ldots, n \).

c. Compute the conditional distribution \( \{Y_1, \ldots, Y_n\} \) given \( T \), i.e.

\[
P(Y_1 = y_1, \ldots, Y_n = y_n | T = t).
\]

Further show that \( \{Y_1, \ldots, Y_n\} \) is conditionally independent of \( X \) given \( T \).

d. Find the decoder \( \hat{X} \) that minimizes \( P(X \neq \hat{X}) \). (Hint: the answer can be given in terms of \( T \))

**Solution**

a.

\[
P(Y_1 = y_1, \ldots, Y_n = y_n | X = x) = P(X \oplus Z_1 = y_1, \ldots, X \oplus Z_n = y_n | X = x)
\]

\[
= P(X \oplus Z_1 \oplus X = y_1 \oplus X, \ldots, X \oplus Z_n \oplus X = y_n \oplus X | X = x)
\]

\[
= P(Z_1 = y_1 \oplus x, \ldots, Z_n = y_n \oplus x | X = x)
\]

\[
= \prod_{i=1}^{n} p^{y_i \oplus x}(1-p)^{1-y_i \oplus x}
\]

b.

\[
P(T = t) = P(X = 0)P(T = t|X = 0) + P(X = 1)P(T = t|X = 1)
\]

\[
= \frac{1}{2} \binom{n}{t} p^t (1-p)^{n-t} + \frac{1}{2} \binom{n}{t} p^{n-t}(1-p)^t
\]
c. 
\[ P(Y_1 = y_1, \ldots, Y_n = y_n | T = t) = P(Y_1 = y_1, \ldots, Y_n = y_n, T = t) \]
\[ = P(X = 0)P(Y_1 = y_1, \ldots, Y_n = y_n, T = t | X = 0) + P(X = 1)P(Y_1 = y_1, \ldots, Y_n = y_n, T = t | X = 1) \]
\[ = \frac{P(X = 0)P(Y_1 = y_1, \ldots, Y_n = y_n, T = t | X = 0) + P(X = 1)P(Y_1 = y_1, \ldots, Y_n = y_n, T = t | X = 1)}{P(T = t)} \]
\[ \geq \frac{\text{part(a), (b)}}{\left( \begin{array}{c} n \end{array} \right) p^t(1 - p)^{n-t} + \left( \begin{array}{c} n \end{array} \right) p^t(1 - p)^{n-t} (1 - p)^t \right)}{1_{(t=\Sigma y_i)}} \]
\[ = \frac{1}{\left( \begin{array}{c} n \end{array} \right)} 1_{(t=\Sigma y_i)} \]
\[ = \frac{p^t(1 - p)^{n-t}}{\left( \begin{array}{c} n \end{array} \right)} 1_{(t=\Sigma y_i)} = \frac{1 - p^t p^{n-t}}{\left( \begin{array}{c} n \end{array} \right)} 1_{(t=\Sigma y_i)} \]
\[ = P(Y_1 = y_1, \ldots, Y_n = y_n | T = t, X = 0) = P(Y_1 = y_1, \ldots, Y_n = y_n | T = t, X = 1) \]

The conditional independence holds since \( P(Y_1 = y_1, \ldots, Y_n = y_n | T, X) \) does not depend on \( X \).

d. The posterior ratio
\[ \frac{P(X = 1 | Y_1, \ldots, Y_n)}{P(X = 0 | Y_1, \ldots, Y_n)} = \frac{P(Y_1, \ldots, Y_n | X = 1)}{P(Y_1, \ldots, Y_n | X = 0)} \] (Bayes rule)
\[ = \frac{P(Y_1, \ldots, Y_n, T | X = 1)}{P(Y_1, \ldots, Y_n, T | X = 0)} \] (T is fully determined by the Y's)
\[ = \frac{P(Y_1, \ldots, Y_n, T, X = 1)P(T | X = 1)}{P(Y_1, \ldots, Y_n, T, X = 0)P(T | X = 0)} \]
\[ = \frac{P(T | X = 1)P(T | X = 0)}{P(T | X = 1)P(T | X = 0)} \] (conditional independence as derived in (c))
\[ = \frac{\left( \begin{array}{c} n \end{array} \right) p^{n-T} (1 - p)^T}{\left( \begin{array}{c} n \end{array} \right) p^T (1 - p)^{n-T}} \]
\[ = \frac{p}{1 - p}^{n-2T} \]

As a result,
\[ \frac{P(X = 1 | Y_1, \ldots, Y_n)}{P(X = 0 | Y_1, \ldots, Y_n)} \geq 1 \iff (n - 2T) \log \left( \frac{p}{1 - p} \right) \geq 0 \]

So a MAP decoder \( \hat{X} = 1_{\{n - 2T \geq 0\}} 1_{\{p \geq 0.5\}} + 1_{\{n - 2T \leq 0\}} 1_{\{p \leq 0.5\}} \).

2. Let \( [X, Y, Z]^T \) be a Gaussian random vector with zero mean and covariance matrix \( \Sigma \) given by
\[ \Sigma = \begin{bmatrix} a & b_1 & c \\ b_1 & a & b_2 \\ c & b_2 & a \end{bmatrix}, \quad (1) \]

where \( a, b_1, b_2, c \) are real valued constants.

a. Let \( \hat{X}(Z) \) be the MMSE estimator of \( X \) given \( Z \). Specify the joint pdf of \( \hat{X}(Z) \) and \( Y \) (in terms of \( a, b_1, b_2, c \)).
b. Let $\tilde{X}$ be the MMSE estimator of $X$ given both $Y$ and $Z$, and $\tilde{X}'$ be the MMSE estimator of $\hat{X}(Z)$ given $Y$. Which of the following statements is true? Justify your answer.

i. $\tilde{X}$ can be better than $\tilde{X}'$ (i.e. it is possible that $E(X - \tilde{X})^2 < E(X - \tilde{X}')^2$).

ii. $\tilde{X}'$ can be better than $\tilde{X}$.

iii. $\tilde{X}' = \tilde{X}$ for all possible values of the above constants.

Solution

a. First note that

$$\hat{X}(Z) = \frac{c}{a}Z. \quad (2)$$

Thus

$$\begin{bmatrix} \hat{X}(Z) \\ Y \end{bmatrix} = \begin{bmatrix} c/a & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} Z \\ Y \end{bmatrix}. \quad (3)$$

Thus

$$\begin{bmatrix} \hat{X}(Z) \\ Y \end{bmatrix} \sim \mathcal{N} \left( \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} c^2/a & b_2c/a \\ b_2c/a & a \end{bmatrix} \right). \quad (4)$$

b. We show that $\tilde{X}$ can be better than $\tilde{X}'$. Let $X$ be independent of $Z$ and $Y$ be independent of $Z$, but $X, Y$ are dependent. In other words, $c = b_2 = 0, b_1 > 0$. Then

$$\tilde{X}' = 0, \quad (5)$$

whose corresponding MSE is $a$. However, the MSE of $\tilde{X}$ is less than $a$. 

---

Review Session #4 Solutions Page 3 of 3