

Control de Transmisión de Datos

Grupo 20. 1 de diciembre de 2004

Notas:

1. Los resultados no justificados no serán tenidos en cuenta.
 2. Los problemas se entregarán por separado, numerando las hojas y poniendo nombre y apellidos en cada hoja.
 3. Un error conceptual grave anula todo el problema.
-

PROBLEMA 1 (3,5 PUNTOS)

Se dispone de un código (6,3) binario lineal y sistemático y sean Y_1 , Y_2 e Y_3 palabras código, siendo $Y_1=110110$, $Y_2=101011$, $Y_3=011101$

Calcúlese

- a) Capacidad correctora del código. ¿Es un código perfecto? (0,5 puntos)
- b) ¿Cómo se codifica el mensaje 111? (1 punto)
- c) Indíquese si la siguiente matriz puede ser de comprobación (1 punto)

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

- d) Supóngase que se ha recibido la palabra $Z=001001$. ¿Cuál sería la decisión del decodificador si se utiliza el código como corrector? (1 punto)

PROBLEMA 2 (3,5 PUNTOS)

Sea una fuente de información con memoria cuyo alfabeto es de 3 símbolos {A, B, C} con $p(A|A)=0,4$; $p(B|A)=0,25$; $p(A|B)=p(B|B)=0,4$; $p(A|C)=1$

- a) Calcule la relación señal a ruido mínima a la entrada del receptor (en escala lineal) para que sea posible transmitir 20.000 símbolos de fuente por un canal de $W=1\text{KHz}$ en un tiempo de 2 segundos. (2 puntos)
- b) Realice una codificación de Huffman (binaria) de la fuente extendida de orden 2. Calcule la eficiencia de codificación. (1,5 puntos)

PROBLEMA 3 (3 PUNTOS)

Pedro y Antonio quieren diseñar un sistema de juegos seguros por la red. Para empezar, prueban el juego de adivinar el resultado del lanzamiento de una moneda al aire. Un jugador debe lanzar una moneda al aire (o elegir un bit aleatorio), y el otro debe acertar el resultado. Asimismo, el segundo jugador debe poder verificar que el primero no le ha engañado. La solución elegida no puede hacer uso de terceras entidades a las que el primer jugador le indique el resultado.

Utilizando algoritmos y protocolos criptográficos, indíquese un posible esquema para el que el juego sea justo y verificable.