

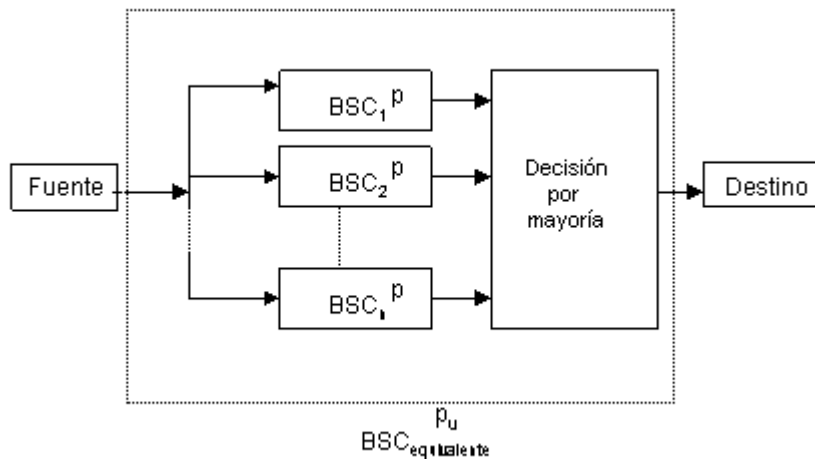
Control de Transmisión de Datos

22/05/09

Ejercicio 1. En un sistema de transmisión de datos se utilizan n canales independientes e iguales en paralelo, binarios y simétricos (BSC), con probabilidad de error p . En todos ellos se transmite simultáneamente la salida de una fuente de datos binaria $\{0, 1\}$ hasta un único receptor de datos. El receptor recibe las n salidas de los canales BSC y detecta cuál es el símbolo que más se repite. Este símbolo detectado es el que se entrega finalmente al destino.

Se define p_u como la probabilidad de error del símbolo enviado por la fuente en el destino final. Considerando que n sólo toma valores impares y utilizando que $e = \lfloor \frac{n-1}{2} \rfloor$, determine:

- p_u en función de p , n y e . Aproxime el resultado para $p \ll 1$.
- el valor de la capacidad del canal BSC equivalente para los casos en que n toma los valores 3, 5 o 7, cuando $p=0.01$. Discuta los resultados obtenidos.



Ejercicio 2. Sea $\mathfrak{F}_1 = \{1, 2, 3, 4\}$ y $\mathfrak{F}_2 = \{2, 4, 6\}$ dos fuentes equiprobables independientes. Sea una fuente \mathfrak{F} cuya salida en el mínimo común múltiplo de la salida de las fuentes anteriores,

$$\mathfrak{F} = \text{mcm}(\mathfrak{F}_1, \mathfrak{F}_2)$$

- calcule la entropía $H(\mathfrak{F})$
- calcule las informaciones mutuas: $I(\mathfrak{F}_1; \mathfrak{F})$ e $I(\mathfrak{F}_2; \mathfrak{F})$
- suponga que le proponen adivinar \mathfrak{F} y como ayuda le dejan escoger entre conocer \mathfrak{F}_1 o conocer \mathfrak{F}_2 . Utilizando el resultado del apartado anterior, justifique la opción que elegiría.
- determine la eficiencia de la codificación binaria utilizando el algoritmo de Huffman de la fuente \mathfrak{F} .

Ejercicio 3. Un sistema de clave pública, análogo al RSA, tiene por módulo $n = 385$.

- Determine el número de elementos que tienen inverso respecto al producto, $\phi(n)$, en el anillo conmutativo Z_n
- ¿ Qué exponente público, e , elegiría de entre el conjunto de valores $\{2, 3, 5, 7\}$?
- ¿Cuál es el exponente privado, d , asociado al exponente público elegido e ?
- Halle el valor del criptograma c asociado al mensaje $m = 192$.