UNIVERSIDAD DE MÁLAGA

E.T.S. INGENIERÍA INFORMÁTICA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Tema 5. Canales con Ruido

José A. Montenegro

Dpto. Lenguajes y Ciencias de la Computación
ETSI Informática. Universidad de Málaga
monte@lcc.uma.es twitter

26 de septiembre de 2013

1. Definición de canal
   - Transmitir una fuente mediante un canal
   - Entropía Condicional
   - La capacidad de un canal
2. Comunicación utilizando un canal con ruido
   - El BSC extendido
   - Reglas Decisión
   - Corrección Errores
   - El límite de embalaje (The packing bound)
3. La probabilidad de una confusión
   - Codificación según una tasa establecida
   - Transmisión utilizando BSC extendido
   - La tasa de transmisión no puede exceder la capacidad
   - Teorema de Shannon

Definición de canal

- Sea I un alfabeto finito. Consideramos los símbolos de I como entradas en un dispositivo, denominado como canal, él cual lo transmite de forma que no esta libre de errores.
- Como resultado de estos errores, los cuales nosotros denominamos **ruido**, los símbolos que forman la salida del dispositivo pertenecen a otro conjunto J.
- Los conjuntos I y J podrían ser el mismo, pero eso no significa que una entrada especifica $i \in I$ será la salida del mismo símbolo.

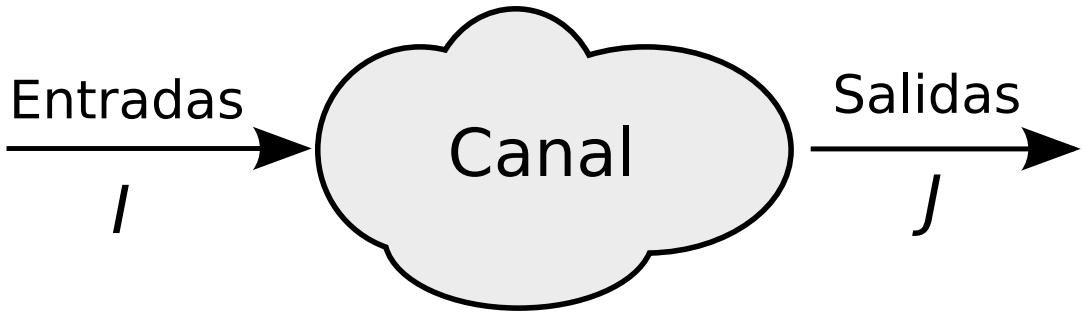

Figura 1 : Representación visual de un canal

- Para cada $i \in I$ y $j \in J$, podemos denotar por $Pr(j|i)$ la probabilidad condicional que la salida es j, dado que la entrada es i:

$$\text{Pr(j | i)} = \text{Pr(salida es j | entrada es i)}.$$

Definición 1 (Canales con Ruido)

Un canal Γ con el conjunto de entrada I y el conjunto de salida J es una matriz cuya entrada son los Pr(j|i):

$$\Gamma_{ij} = Pr(j \mid i)\ (i \in I, j \in J).$$

Las entradas de Γ están etiquetadas por lo que las filas corresponden a las entradas y las columnas corresponde a las salidas.
Si al menos uno de los términos Γ_{ij} con $i \neq j$ es no cero, podemos decir que **el canal tiene ruido**.

Definición 2 (Canal Binario Simétrico)

Un canal binario simétrico (BSC) corresponde a un matriz de la forma

$$\Gamma = \begin{pmatrix} \Gamma_{00} & \Gamma_{01} \\ \Gamma_{10} & \Gamma_{11} \end{pmatrix} = \begin{pmatrix} 1-e & e \\ e & 1-e \end{pmatrix}$$

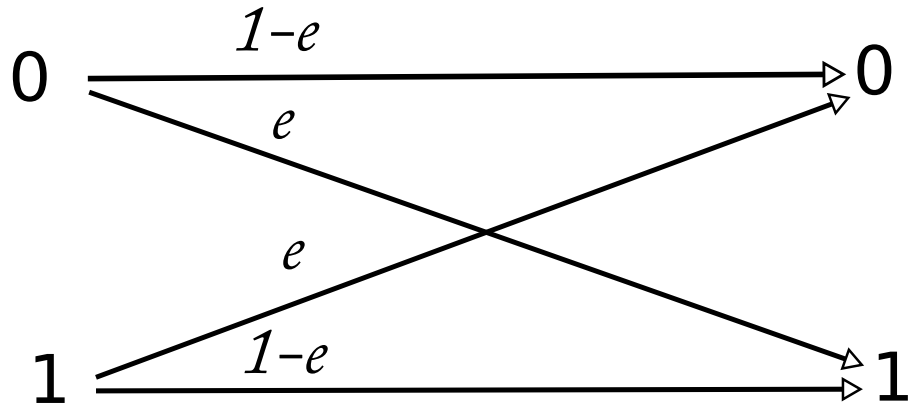

Figura 2 : El canal binario simétrico con probabilidad de error de bit e

- La figura 2 es una representación de un Canal Binario Simétrico.
- Las filas y columnas de la matriz del canal Γ corresponden a 0 y 1, los elementos del alfabeto binario B.
- El hecho que $\Gamma_{01} = \Gamma_{10} = e$ significa que los símbolos de la salida difieren de los símbolos de la entrada con una probabilidad e y nos referimos como la probabilidad de error de bit.
- La probabilidad que un símbolo es transmitido correctamente es $\Gamma_{00} = \Gamma_{11} = 1 - e$.
- Usualmente asumimos que e es un número pequeño positivo: por ejemplo $e = 0{,}01$ significa que un bit de cada 100 es transmitido de forma errónea.
- La gravedad asociada a este porcentaje depende del escenario a estudio, ya que en algunos caso sería una tasa error inaceptable.

Ejemplo 1

La figura 3 muestra un teclado simplificado con 6 letras A,B,C,D,E,F. Dos letras son adyacentes si un borde de una es próxima al borde de la otra. Dado dos teclas adyacentes x e y existe una probabilidad de 0.1 que cuando intento introducir la tecla x pulsaré la tecla Y. Escribe cual es la matriz de canal para esta situación. Si intento introducir $BECA$, ¿Cual es la probabilidad que el teclado registre correctamente?

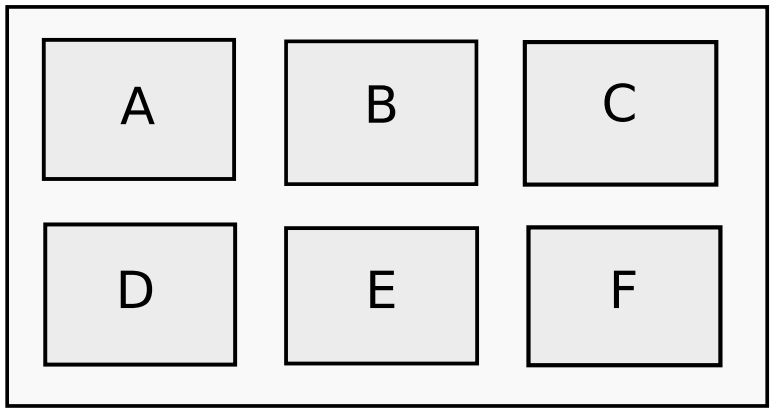

Figura 3 : Representación de un teclado simplificado

Solución:
El conjunto de entrada y salida son {A, B, C, D, E, F }, y la matriz del canal es

$$\Gamma = \begin{pmatrix} 0{,}8 & 0{,}1 & 0 & 0{,}1 & 0 & 0 \\ 0{,}1 & 0{,}7 & 0{,}1 & 0 & 0{,}1 & 0 \\ 0 & 0{,}1 & 0{,}8 & 0 & 0 & 0{,}1 \\ 0{,}1 & 0 & 0 & 0{,}8 & 0{,}1 & 0 \\ 0 & 0{,}1 & 0 & 0{,}1 & 0{,}7 & 0{,}1 \\ 0 & 0 & 0{,}1 & 0 & 0{,}1 & 0{,}8 \end{pmatrix}$$

La probabilidad de introducir correctamente $BECA$ es 0.7 x 0.7 x 0.8 x 0.8 = 0.3136.

Lema 1

La suma en cada fila en una matriz de canal es igual a 1.

$$\sum_{j \in J} \Gamma_{ij} = 1 \text{ para todo } i \in I$$

Ejercicio 1

Un canal asimétrico binario es similar a un BSC, excepto que la probabilidad de error cuando enviamos 0 es a, y la probabilidad de error cuando enviamos 1 es b, donde $a \neq b$. Establezca la matriz para este canal.

Ejercicio 1

Un canal asimétrico binario es similar a un BSC, excepto que la probabilidad de error cuando enviamos 0 es a, y la probabilidad de error cuando enviamos 1 es b, donde $a \neq b$. Establezca la matriz para este canal.

Solución:

$$\Gamma = \begin{pmatrix} 1-a & a \\ b & 1-b \end{pmatrix}$$

Ejercicio 2

Un canal simétrico ternario es un canal para el cual el conjunto de entrada I y el conjunto de salida J son los mismo $\{0, 1, 2\}$, y la probabilidad que un símbolo i sea $j \neq i$ es x. Establezca la matriz para este canal.

Ejercicio 2

Un canal simétrico ternario es un canal para el cual el conjunto de entrada I y el conjunto de salida J son los mismo $\{0, 1, 2\}$, y la probabilidad que un símbolo i sea $j \neq i$ es x. Establezca la matriz para este canal.

Solución:

$$\Gamma = \begin{pmatrix} 1-2x & x & x \\ x & 1-2x & x \\ x & x & 1-2x \end{pmatrix}$$

Transmitir una fuente mediante un canal

- Supóngase que un símbolo i en el conjunto de entrada I ocurre con probabilidad p_i, por lo que tenemos una distribución de probabilidad p en I.
- Podemos pensar que la entrada de un canal Γ es generada por una fuente (I,p).
- Similarmente, estableciendo q_j la probabilidad que el símbolo de salida es j, la salida puede ser considerada como una fuente (J, q).
- El siguiente teorema describe la relación entre p y q.

Teorema 1

Sea Γ una matriz de canal, y sea las distribuciones asociadas con la fuente de entrada (I,p) y la fuente de salida (J,q) escrita como vectores,

$$p = [p_1, p_2, \ldots, p_m],\ q = [q_1, q_2, \ldots, q_n],\ \textit{entonces:}\ q = p\Gamma.$$

- Ahora entonces tenemos un modelo en el cual el canal Γ puede ser considerado como un enlace entre dos fuentes, (I, p) y (J, q).
- La primera fuente es producida por el Emisor, mientras que la segunda fuente, el resultado de la transmisión mediante Γ, está disponible al Receptor.
- Estas fuentes están relacionadas por la ecuación $q = p\Gamma$.

Ejemplo 2

Establezca las ecuaciones que vinculan $p = [p_0, p_1]$ *y* $q = [q_0, q_1]$ *cuando* Γ *es el BSC con probabilidad de error de bit* e. *Si* $e = 0{,}1$ *y* $p = [0{,}7, 0{,}3]$, *¿Cual es el valor de q?.*

Ejemplo 2

Establezca las ecuaciones que vinculan $p = [p_0, p_1]$ *y* $q = [q_0, q_1]$ *cuando* Γ *es el BSC con probabilidad de error de bit* e. *Si* $e = 0{,}1$ *y* $p = [0{,}7, 0{,}3]$, *¿Cual es el valor de q?.*

Solución:
La ecuación de la matriz es:

$$\begin{pmatrix} q_0 & q_1 \end{pmatrix} = \begin{pmatrix} p_0 & p_1 \end{pmatrix} \begin{pmatrix} 1-e & e \\ e & 1-e \end{pmatrix}$$

la cual es equivalente a las ecuaciones:

$$\begin{aligned} q_0 &= p_0(1-e) + p_1 e \\ q_1 &= p_0 e + p_1(1-e) \end{aligned}$$

Si $e = 0{,}1$ y $p = [0{,}7, 0{,}3]$ entonces $q = [0{,}66, 0{,}34]$

Ejercicio 3

Supongase que las salidas de un canal Γ_1 *son las símbolos de entrada para un canal* Γ_2*, y* Γ *es el resultado del canal combinado. En esta situación diremos que* Γ *es el resultado de combinar* Γ_1 *y* Γ_2 *en series. ¿Cual es la relación entre las matrices* Γ_1 *y* Γ_2 *y* Γ *?*

Ejercicio 3

Supongase que las salidas de un canal Γ_1 son las símbolos de entrada para un canal Γ_2, y Γ es el resultado del canal combinado. En esta situación diremos que Γ es el resultado de combinar Γ_1 y Γ_2 en series. ¿Cual es la relación entre las matrices Γ_1 y Γ_2 y Γ ?

Solución:
Sea p la entrada a Γ_1, q la salida de Γ_1 y la entrada a Γ_2, r la salida de Γ_2.
Entonces r = q Γ_2 = p Γ_1 Γ_2 .
Por tanto Γ es la matriz producto de $\Gamma_1 \times \Gamma_2$.

Ejercicio 4

Considere el canal simétrico binario con probabilidad de error por bit $e = 0{,}01$. *Si la entrada tiene una distribución de probabilidad p = [0.6, 0.4]. ¿Cual es la distribución de probabilidad q?. Compare las entropías de la entrada y salida.*

Ejercicio 4

Considere el canal simétrico binario con probabilidad de error por bit $e = 0{,}01$. Si la entrada tiene una distribución de probabilidad p = [0.6, 0.4]. ¿Cual es la distribución de probabilidad q?. Compare las entropías de la entrada y salida.

Solución:

$$\begin{pmatrix} q_0 & q_1 \end{pmatrix} = \begin{pmatrix} p_0 & p_1 \end{pmatrix} \begin{pmatrix} 1-0{,}01 & 0{,}01 \\ 0{,}01 & 1-0{,}01 \end{pmatrix}$$

$$q_0 = p_0(1-e) + p_1 e = 0{,}6 \times 0{,}99 + 0{,}4 \times 0{,}01 = 0{,}598$$
$$q_1 = p_0 e + p_1(1-e) = 0{,}6 \times 0{,}01 + 0{,}4 \times 0{,}99 = 0{,}402$$

$$H(p) \approx 0{,}9709;\ H(q) \approx 0{,}9721$$

La incertidumbre ha crecido a la hora de transmitir por un canal con ruido.

Entropía Condicional

- La existencia de errores tiende a equiparar las probabilidades, ya que los símbolos que ocurren con más frecuencia son transmitidos erróneamente más a menudo.
- En el ejemplo 2 la incertidumbre de la entrada y la salida son, respectivamente,

$$h(0{,}7) \approx 0{,}881, h(0{,}66) \approx 0{,}925,$$

- Como podemos esperar, la incertidumbre es incrementada por la transmisión a través de un canal con ruido.
- Un problema más sutil es describir la situación desde el punto de vista del Receptor, para aquellos los cuales la salida es la única información disponible sobre la entrada.

Pregunta: ¿Cuanta información sobre la entrada está disponible al Receptor que conoce la salida de Γ?

- Para contestar a esta pregunta, es útil reconsiderar la situación. Estableceremos el modelo en términos de una entrada que es enviada a través de un canal para producir una salida.
- Simplemente una distribución de probabilidad t en el conjunto $I \times J$:

$$t_{ij} = \text{Pr(entrada es } i \text{ y salida es } j).$$
$$t_{ij} = \text{Pr(salida es } j \mid \text{entrada es } i) \times \text{Pr(entrada es } i) = \Gamma_{ij} p_i$$

- Teniendo t, todas las otras cantidades pueden ser derivado a través de t utilizando las ecuaciones

$$p_i = \sum_j t_{ij} \;\; q_j = \sum_i t_{ij} \;\; \Gamma_{ij} = t_{ij}/p_i$$

- Concretamente, p y q son las distribuciones marginales asociadas con t.

Definición 3 (Entropía Condicional)

Con las anotaciones anteriores, la entropía condicional H(p | q) es definida por

$$H(p|q) = H(t)\text{-}H(q).$$

- La motivación es que H(t) mide la incertidumbre sobre el par entrada-salida (i,j) y H(q) mide la incertidumbre sobre la salida j.
- Por tanto, restando la segunda cantidad de la primera representa la incertidumbre de un Receptor que conoce la salida y está intentando determinar la entrada.
- Debido a que las distribuciones de entrada y salida están vinculadas por la ecuación $q = p\Gamma$, por lo que $H(p|q)$ solo depende de Γ y p.
- Usualmente nos referimos a esta cantidad como entropía condicional de p con respecto la transmisión a través de Γ y viene denotado por $H(\Gamma; p)$: $H(\Gamma; p) = H(p|q)$ (donde $q = p\Gamma$)

Ejemplo 3

Sea Γ el BSC con una probabilidad de bit de error e = 0.1, y sea la distribución de la fuente p = [0.7, 0.3]. Calcular $H(\Gamma; p)$.

Ejemplo 3

Sea Γ el BSC con una probabilidad de bit de error e = 0.1, y sea la distribución de la fuente p = [0.7, 0.3]. Calcular $H(\Gamma; p)$.

Solución:
Ya que $t_{ij} = p_i \Gamma_{ij}$

$$\Gamma = \begin{pmatrix} 1-e & e \\ e & 1-e \end{pmatrix} = \begin{pmatrix} 0{,}9 & 0{,}1 \\ 0{,}1 & 0{,}9 \end{pmatrix}; t = \begin{pmatrix} 0{,}63 & 0{,}07 \\ 0{,}03 & 0{,}27 \end{pmatrix}$$

Ahora seguimos con los siguientes cálculos $H(t) \approx 1{,}350$, ya que $q_j = \sum_i t_{ij}$ tenemos que q = [0.66,0.34], y $H(q) \approx 0{,}925$. Por tanto,

$$H(\Gamma; p) = H(t) - H(q) \approx 1{,}350 - 0{,}925 = 0{,}425.$$

El resultado general para un canal simétrico binario es como sigue:

Teorema 2

Sea Γ el BSC con una probabilidad de bit error e, y sea p la distribución de la fuente $[p_0, p_1] = [p, 1-p]$. Entonces

$$H(\Gamma; p) = h(p) + h(e) - h(q),$$

donde q = p(1 - e) + (1 - p) e, y h es la función de entropía estándar definida como $h(x) = xlog_2(1/x) + (1-x)log_2(1/(1-x))$.

Ejercicio 5

Considere el canal simétrico binario con probabilidad de error por bit $e = 0{,}01$. *(Ejercicio 4). Si la entrada tiene una distribución de probabilidad p = [0.6, 0.4]. Calcule la distribución* t *y la entropía condicional* $H(\Gamma; p)$.

Ejercicio 5

Considere el canal simétrico binario con probabilidad de error por bit $e = 0{,}01$. (Ejercicio 4). Si la entrada tiene una distribución de probabilidad p = [0.6, 0.4]. Calcule la distribución t y la entropía condicional $H(\Gamma; p)$.

Solución:
Ya que $t_{ij} = p_i \Gamma_{ij}$

$$\Gamma = \begin{pmatrix} 1-e & e \\ e & 1-e \end{pmatrix} = \begin{pmatrix} 0{,}99 & 0{,}01 \\ 0{,}01 & 0{,}99 \end{pmatrix} t = \begin{pmatrix} 0{,}594 & 0{,}006 \\ 0{,}004 & 0{,}396 \end{pmatrix}$$

Ahora seguimos con los siguientes cálculos $H(t) \approx 1{,}0517$, ya que $q_j = \sum_i t_{ij}$ tenemos que q = [0.598,0.402], y $H(q) \approx 0{,}9721$. Por tanto,

$$H(\Gamma; p) = H(t) - H(q) \approx 1{,}0517 - 0{,}9721 \approx 0{,}0796.$$

Ejercicio 6

Verifica que la respuesta del ejercicio anterior cumple la formula del Teorema 2.

Ejercicio 6

Verifica que la respuesta del ejercicio anterior cumple la formula del Teorema 2.

Solución:

$$H(\Gamma; p) = h(p) + h(e) - h(q) = 0{,}9709 + 0{,}0807 - 0{,}9721 \approx 0,0795$$

La capacidad de un canal

- En la vida real podemos encontrar infinidad de ejemplos que nos muestran que rebasar la capacidad de sistema produce que funcione de forma ineficiente.
- En el caso de un canal de comunicación esta situación no está tan clara.
- Haciendo uso de las definiciones que hemos realizado previamente, estableceremos la definición de la capacidad de un canal.
- Hemos definido:
  - $H(p)$: La incertidumbre sobre los símbolos emitidos por una fuente de entrada p;
  - $H(\Gamma; p)$: La incertidumbre sobre los símbolos emitidos por p desde el punto de vista del Receptor quien conoce los símbolos de salida emitidos por la fuente $q = p\Gamma$.

El siguiente teorema confirma que estas cantidades están vinculadas de la forma en la que nosotros esperábamos.

Teorema 3

Sea Γ un canal y p una distribución de entrada para Γ. Entonces

$$H(\Gamma; p) \leq H(p).$$

La igualdad la obtenemos sii p y $q = p\Gamma$ son distribuciones independientes.

- Sea

$$f_\Gamma(p) = H(p) - H(\Gamma; p).$$

- Ya que $f_\Gamma(p)$ es la diferencia entre dos medidas de incertidumbre, podemos pensar que es una medida de información.
- Específicamente, representa la información sobre los símbolos emitidos por la fuente de entrada p que es disponible al Receptor que conoce los símbolos emitidos por la fuente de salida.
- Por ejemplo, supongamos que Γ es el BSC con una probabilidad de error de bit e=0.1 y la distribución de entrada es $p = [0{,}7, 0{,}3]$. Anteriormente hemos calculado que $H(p) = h(0{,}7) \approx 0{,}881$ y $H(\Gamma; p) \approx 0{,}425$, por lo que:

$$f_\Gamma(p) = H(p) - H(\Gamma; p) \approx 0{,}881 - 0{,}425 = 0{,}456$$

- Supongase que dado un canal Γ que acepta un alfabeto de entrada I de tamaño m, o que la matriz del canal tiene m filas, entonces para cada distribución de probabilidad p sobre I tendremos un valor de $f_\Gamma(p)$.

Definición 4 (Capacidad)

La capacidad γ de Γ es máximo valor de $f_\Gamma(p)$, tomado del conjunto P de todas las distribuciones de probabilidad en un conjunto de tamaño m (el número de filas de Γ).

$$\gamma = max f_\Gamma(p) = max(H(p) - H(\Gamma; p))$$

- En general, el cálculo de la capacidad de un canal no es una tarea trivial, pero para el caso de BSC existe una forma fácil.

Teorema 4

La capacidad del BSC con probabilidad de error de bit e $(0 \leq e \leq 1/2)$ *es*

$$\gamma = 1 - h(e),$$

donde $h(e) = e \times log_2(1/e) + (1-e) \times log_2(1/(1-e))$.

- En la mayoría de las situaciones reales, e es pequeño, por lo que el valor de $h(e)$ es cercano a 0 y γ a 1.
- Por ejemplo, en el caso de un BSC con una probabilidad de error de bir de 0.01 es

$$\gamma = 1 - h(0{,}01) = 1 - 0{,}01 log_2(1/0{,}01) - 0{,}99 log_2(1/0{,}99) = 0{,}919.$$

Comunicación utilizando un canal con ruido

- Ahora consideramos la transmisión de los mensajes codificados a través de un canal con ruido.
- Simplificamos el caso general y nos centramos en los mensajes codificados en el alfabeto binario $\mathbb{B} = \{0, 1\}$, transmitidos mediante un canal binario simétrico.
- La fuente emite una cadena de símbolos que son codificados como palabras binarias, todas con la misma longitud n donde n será escogido por alguna condición deseable.

- Por ejemplo, supongase que la fuente es un control remoto que guía un robot a través de una red de calles, desde Norte-Sur a Este-Oeste. Algunas calles presentan obstáculos y algunas de ellas son de una sola dirección.
- Para mover el robot de un punto a otro, el controlador debe enviar una secuencia de símbolos N, S, E, O, según corresponda.
- En este caso el alfabeto es X = {N, S, E, O}. Tomando n = 2, un código apropiado $c : X \to \mathbb{B}^2$ podría ser:

$$N \mapsto 00, S \mapsto 01, E \mapsto 10, O \mapsto 11$$

Comunicación utilizando un canal con ruido

- Utilizando este código la secuencia de instrucciones mostrada en la figura 4 es codificada como sigue:

$$(E, N, N, E, S, E, E, S, O) \mapsto 100000100110100111$$

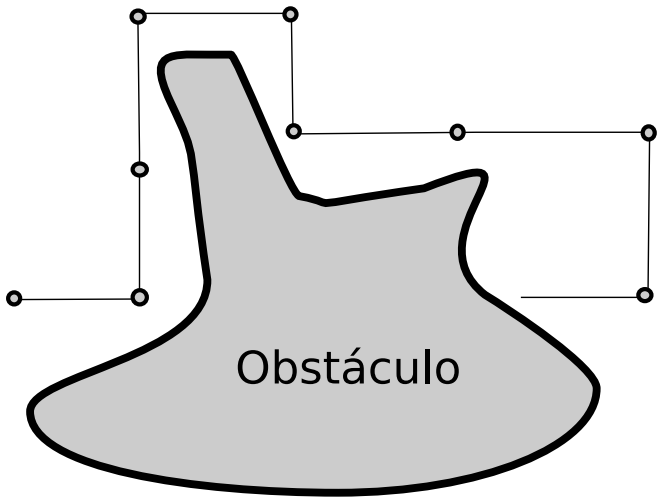

Figura 4 : La ruta E,N,N,E,S,E,E,S,O

- El valor n=2 es claramente el menor valor posible para un código binario para cuatro mensajes.
- Sin embargo, este código tiene una desventaja que si cualquier error ocurre en los bits que son transmitidos, el robot no será capaz de detectarlo.
- Por ejemplo, supongamos que el símbolo que queremos transmitir es S, por lo que 01 es enviado, y si el primer bit es alterado en la transmisión, por lo que 11 es recibido. El robot decodificará como O, y no tiene capacidad de conocer que un error ha sucedido.

- El ejemplo ilustra el siguiente escenario. Los mensajes originados de alguna fuente y son expresados en un alfabeto X. Nos referimos a la salida de esta fuente como la *flujo original*.
- Un Emisor debe transmitir estos mensajes a un Receptor, utilizando un canal binario simétrico. Para realizar esta transmisión el Emisor codifica el mensaje utilizando un código binario $c : X \to \mathbb{B}^n$. Nos referimos al flujo emitido por el Emisor como *flujo codificado*.
- El flujo codificado es una cadena de palabras codificadas, cada una de las cuales es una palabra binaria de longitud n, y por tanto una cadena de bits. En resumen, el Emisor ha realizado una transformación

$$\text{T1: flujo original} \longrightarrow \text{flujo codificado}$$

- Notese que el flujo codificado está basado en un código que es libre de prefijo. Por tanto, en esta fase, el problema de la decodificación es simple.
- Sin embargo, cuando los bits son transmitidos a través de un BSC, no libre de errores. La salida del canal, el cual nos referimos como *flujo recibido*, no es lo mismo que el flujo codificado. En otras palabras el proceso de transmisión tiene un efecto de transformación:

$$\text{T2: flujo codificado} \longrightarrow \text{flujo recibido}$$

- Asumimos que el Receptor tiene una guía de codificación, por lo que el conjunto de palabras codificadas C y la longitud de palabra n son conocidas.
- El flujo recibido puede contener cualquier palabra $z \in B^n$, debido a los errores. Para comprender el mensaje, el Receptor debe primero decidir que palabra codificada $c \in C$ fue enviada cuando z es recibida.

Definición 5 (Regla Decisión)

Sea $C \subseteq \mathbb{B}^n$ un código. Una regla de decisión para C es una función $\sigma : \mathbb{B}^n \to C$ el cual asigna a cada $z \in \mathbb{B}^n$ una palabra codificada $c \in C$.

Utilizar una regla de decisión σ, el Receptor produce un flujo final, y tiene como efecto una transformación

$$\text{T3: flujo recibido} \longrightarrow \text{flujo final}$$

El sistema entero es ilustrado en la figura 5.

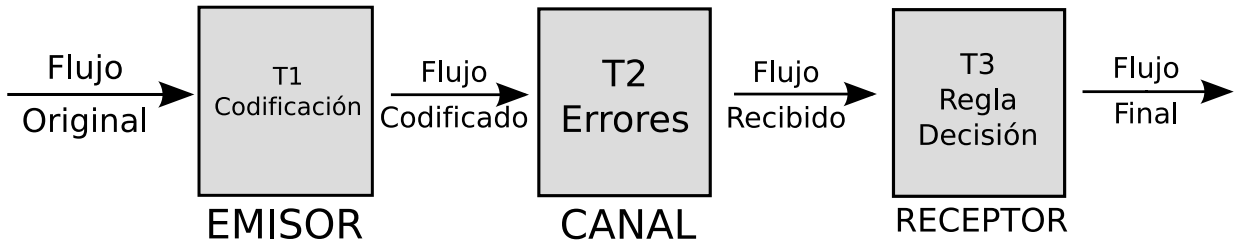

Figura 5 : Un modelo de sistema de comunicación

Definición 6 (Confusión)

Podemos determinar que una confusión ocurre si una palabra codificada en el flujo final no es el mismo que la palabra codificada en la posición correspondiente en el flujo codificado.

- Cuando una confusión sucede, el Receptor malinterpreta el mensaje que fue enviado por el Emisor.
- Las confusiones son causados por los errores introducidos en la fase T2, transmisión a través de un canal con ruido.
- Nuestro propuesta es mostrar que utilizando una elección apropiada del código C en la fase T1, y reglas de decisión adecuadas para C en la fase T3, es posible reducir el número de errores.

- Por ejemplo, consideramos el escenario descrito anteriormente, donde el Emisor es un controlador emitiendo los símbolos N, S, E, O, utilizando el código $N \mapsto 00$, $S \mapsto 01$, $E \mapsto 10$, $O \mapsto 11$.
- El Receptor, divide las palabras de longitud 2, y este caso todas las cuatro posibles palabras de longitud 2 son palabras codificadas ($C = \mathbb{B}^2$).
- Siempre que las palabras codificadas son transmitidas correctamente, las confusiones no tienen cabida cuando el Receptor utiliza la regla de decisión

$$\sigma(z) = z \text{ para todos } z \in \mathbb{B}^2.$$

- Por otro lado, hemos notado que si cualquier bit es transmitido de forma errónea, entonces las confusiones ocurrirán.
- Afortunadamente es posible elegir mejores códigos.

Ejemplo 4

En la situación descrita anteriormente, supongamos que el Emisor utiliza el código

$$N \mapsto 000, S \mapsto 110, E \mapsto 101, O \mapsto 011,$$

y el Receptor utiliza la siguiente regla de decisión:

$$\sigma(000) = 000, \sigma(100) = 011, \sigma(010) = 000, \sigma(001) = 101,$$

$$\sigma(110) = 110, \sigma(101) = 101, \sigma(011) = 011, \sigma(111) = 110.$$

Si una palabra codificada es transmitida sin errores, ¿Es posible encontrar una confusión? Si recibimos la palabra 000 y asumimos que ocurre un error en un bit, ¿Es posible que ocurra la confusión?

Solución:

- Las reglas de decisión propuestas permiten que cuando tenemos una palabra codificada z obtenemos $\sigma(z) = z$. Por tanto si una palabra codificada es transmitida correctamente, no es posible que ocurra ninguna confusión.
- ¿Qué ocurre si un bit en una palabra codificada es transmitida erróneamente?
  - Note que cada palabra codificada contiene un número de 1's pares (0,2). Si tenemos un bit erróneo la palabra tendrá un número impar de 1's y el error puede ser detectado.
  - Sin embargo, si por ejemplo 001 es recibido, entonces el Receptor debe decidir si la palabra codificada era 000, con un error en el último bit, o 101, con un error en el primer bit, o 011, con un error en el segundo bit.
  - Las reglas de decisión propuestas asumen la segunda posibilidad, y por tanto si 001 es recibido entonces tenemos una posibilidad que tengamos una confusión.

Ejemplo 5

En la misma situación que el anterior supóngase que el Emisor utiliza el código

$$N \mapsto 000000, S \mapsto 000111, E \mapsto 111000, W \mapsto 111111.$$

El Receptor utiliza la regla de decisión para cualquier z, $\gamma(z) = c$ es la palabra codificada que se "parece más" a z, o la palabra codificada c para la cual z y c tienen más bit en común. ¿En que circunstancia podría ocurrir una confusión?

Solución:

- Las palabras codificadas han sido escogidas de forma que si un bit es modificado, la palabra resultante "se parece más" todavía a la palabra codificada original que a cualquier otra palabra codificada.
- La regla de decisión propuesta hace uso de esta propiedad.
- Por ejemplo, si 000000 es alterado durante la transmisión a 100000 entonces el Receptor decidirá que recibió 000000, ya que cualquier otra palabra codificada tendría que haber sido afectada por más de un bit para producir 100000.
- Por lo que no solamente detectamos un error en un bit, además es corregido.
- Para que ocurra una confusión es necesario que ocurran al menos dos bit erróneos.

El sistema descrito anteriormente es un sistema complicado que esta formado por varias etapas.

1. Cuantificar los errores que ocurren cuando los bits en una palabra codificada de longitud n son transmitidas a través de BSC con una probabilidad de error de bit e.
2. Discutir las posibles formas de una regla de decisión σ que asigna una palabra codificada a cada (posiblemente errónea) palabra recibida.
3. Tratar de la corrección de los errores de bit, y como dependen de ciertos parámetros numéricos del código utilizado.

Ejercicio 7

En el ejemplo 4 , suponemos que recibimos 111. Si asumimos que solo hay error en un bit, ¿Cuales son las posibilidades para esa instrucción?

Ejercicio 7

En el ejemplo 4 , suponemos que recibimos 111. Si asumimos que solo hay error en un bit, ¿Cuales son las posibilidades para esa instrucción?

Solución:
Una de las siguientes instrucciones S, E, O.

Ejercicio 8

En el ejemplo 5 propusimos una regla de decisión γ basada en la idea que $\gamma(z)$ es la palabra codificada que se "parece más" a z que cualquier otra palabra codificada. Utilizando esta regla, encuentra los valores de $\gamma(z)$ para la siguientes palabras z:

101000, 101111, 100111.

Ejercicio 8

En el ejemplo 5 propusimos una regla de decisión γ basada en la idea que $\gamma(z)$ es la palabra codificada que se "parece más" a z que cualquier otra palabra codificada. Utilizando esta regla, encuentra los valores de $\gamma(z)$ para la siguientes palabras z:

101000, 101111, 100111.

Solución:
$\gamma(101000) = 111000$; E
$\gamma(101111) = 111111$; O
$\gamma(100111) = 000111$; S

Ejercicio 9

En el ejemplo 5 suponemos ahora que recibimos la palabra 100100. ¿Es posible realizar una decisión razonable sobre que palabra codificada fue enviada?

Ejercicio 9

En el ejemplo 5 suponemos ahora que recibimos la palabra 100100. ¿Es posible realizar una decisión razonable sobre que palabra codificada fue enviada?

Solución:
En este caso parece que 100100 está más cercana a 000000 que a cualquier otra.

El BSC extendido

Definición 7 (Producto del canal)

- *Sea* Γ *y* Γ' *canales con alfabetos de entrada,* I,I', *y alfabetos de salida* J,J', *respectivamente.*
- *El producto del canal* $\Gamma'' = \Gamma \times \Gamma'$ *tiene alfabeto de entrada* $I \times I'$ *y alfabeto de salida* $J \times J'$, *y su matriz es dada por la regla:*

$$\Gamma''_{ii'jj'} = \Gamma_{ij}\Gamma'_{i'j'}$$

- *En otras palabras* Γ'' *es un canal con entradas* ii' *y salidas* jj', *y*

$$Pr(\text{salida es } jj' | \text{ entrada es } ii') = Pr(j \mid i)Pr(j' | \ i').$$

- *En el caso* $\Gamma = \Gamma'$, *denotamos* $\Gamma \times \Gamma'$ *como* Γ^2

Ejemplo 6

Supongase que Γ *es el BSC con probabilidad de error de bit* e*. ¿Cual es la matriz del canal para* Γ^2*?*

Ejemplo 6

Supongase que Γ es el BSC con probabilidad de error de bit e. ¿Cual es la matriz del canal para Γ^2?

Solución:

- Las entradas y las salidas para Γ^2 son los cuatro pares 00, 01, 10, 11.
- Si, por ejemplo, la entrada es 00 y la salida es 10, esto significa que un bit ha sido transmitido de forma errónea (probabilidad e), y un bit ha sido transmitido de forma correcta $(1-e)$.
- Por lo que la entrada en la correspondiente posición en Γ^2 es $e(1-e)$. Utilizando argumentos similares, y etiquetando las filas y columnas en el orden 00, 01, 10, 11, la matriz del canal sería:

$$\Gamma^2 = \begin{pmatrix} (1-e)^2 & (1-e)e & (1-e)e & e^2 \\ (1-e)e & (1-e)^2 & e^2 & (1-e)e \\ (1-e)e & e^2 & (1-e)^2 & (1-e)e \\ e^2 & (1-e)e & (1-e)e & (1-e)^2 \end{pmatrix}$$

Definición 8 (Canal Extendido)

- *Supongase que dado un canal Γ con un conjunto de entrada I y conjunto de salida J y un entero positivo n.*
- *Entonces definimos el canal extendido Γ^n como el n producto de las copias de Γ. Las entradas a Γ^n son palabras de longitud n en I, y las salidas son palabras de longitud n en J. Si Γ es un canal simétrico binario, entonces decimos que Γ^n es un BSC extendido.*
- *Las entradas y salidas para un BSC extendido son los miembros de un conjunto $\mathbb{B}^n$ para todas las palabras binarias de longitud n. Podemos obtener una simple fórmula para las entradas de la matriz del canal Γ^n, generalizando el argumento utilizado anteriormente en el caso n=2.*

Definición 9 (Distancia Hamming)

Supongase que dados dos palabras $x, y \in \mathbb{B}^n$,

$$x = x_1 x_2 \dots x_n \; y = y_1 y_2 \dots y_n.$$

La distancia Hamming d(x, y) es el número de elementos donde x *e* y *difieren, o es el número de* i $(1 \leq i \leq n)$ *tal que* $x_i \neq y_i$.

Por ejemplo, considera las siguientes palabras en $\mathbb{B}^7$:

$$\text{x} = 1010100, \text{ y} = 0110100, \text{ z} = 1011110.$$

Las palabras x e y difieren solamente en el primer y segundo bit, por lo que $d(x, y) = 2$. De forma similar $d(x, z) = 3$ y $d(y, z) = 4$.

Teorema 5

Sea x,y $\in \mathbb{B}^n$. *La entrada* $(\Gamma^n)_{xy}$ *en el matriz canal para el BSC extendido con la probabilidad de error por bit* e *es dada por:*

$$(\Gamma^n)_{xy} = e^d(1-e)^{n-d}, \text{ donde } d = d(x, y).$$

Ejercicio 10

Sea (Γ^2) *la matriz del canal para el BSC extendido con e=0.01. Calcula los números en las filas de* (Γ^2) *correspondiente a la entrada 00.*

Ejercicio 10

Sea (Γ^2) la matriz del canal para el BSC extendido con e=0.01. Calcula los números en las filas de (Γ^2) correspondiente a la entrada 00.

Solución:
$(1-e)^2$= 0.9801 $(1-e)\times e = 0{,}0099$ $(1-e)\times e$= 0,0099 e^2=0,0001

Ejercicio 11

Describa la matriz de canal para (Γ^2) *cuando* (Γ) *es el canal binario asimétrico con parámetros a y b.*

Ejercicio 11

Describa la matriz de canal para (Γ^2) cuando (Γ) es el canal binario asimétrico con parámetros a y b.

Solución:

$$\Gamma^2 = \begin{pmatrix} (1-a)^2 & (1-a)a & (1-a)a & a^2 \\ (1-a)b & (1-a)(1-b) & ab & a(1-b) \\ (1-a)b & ab & (1-a)(1-b) & (1-b)a \\ b^2 & b(1-a) & (1-b)a & (1-a)(1-b) \end{pmatrix}$$

Reglas Decisión

- Previamente hemos presentado la idea de regla de decisión σ para un código $C \subseteq \mathbb{B}^n$.
- La idea es que cuando una palabra $z \in \mathbb{B}^n$ es recibida, el Receptor debe intentar hacer una elección razonable a cual palabra codificada corresponde $\sigma(z) \in C$.
- Como ejemplo podemos considerar el código

$$C = \{000, 110, 101, 011\},$$

- y las reglas de decisión arbitrarias σ son:

$$\sigma(000) = 000,\ \sigma(100) = 011,\ \sigma(010) = 000,\ \sigma(001) = 101,$$

$$\sigma(110) = 110,\ \sigma(101) = 101,\ \sigma(011) = 011,\ \sigma(111) = 110.$$

- Ya que la palabra 011 es una palabra codificada, es razonable definir $\sigma(011) = 011$.
- Por otro lado, 100 no es una palabra codificada, y estableciendo $\sigma(100) = 011$ asumimos que un error ha ocurrido en los tres bits, lo cual es claramente poco probable.
- Una buena regla de decisión depende del sistema de comunicación, en particular, el código C y la matriz del canal Γ.
- El Receptor debe utilizar esta información para formular una regla de decisión que proporcione la mejor opción de establecer la elección adecuada.

Definición 10 (Regla del Observador Ideal)

La regla del observador ideal dice que, dado z, el Receptor debería escoger $\sigma(z)$ igual a una palabra codificada c con la máxima probabilidad que c fue enviada teniendo z.

- Desafortunadamente, las probabilidades condicionales que implica esta definición son de la forma $Pr(c|z)$ y no tienen por que estar disponibles al Receptor.
- Para calcular $Pr(c|z)$ es necesario igualar las dos expresiones para la probabilidad t_{cz} de un par entrada-salida (c,z):

$$t_{cz} = q_z Pr(c|z)$$
$$t_{cz} = p_c Pr(z|c).$$

- Por definición $Pr(z|c)$ es el término Γ_{cz} en la matriz del canal.
- Sin embargo $Pr(c|z) = p_c \Gamma_{cz}/q_z$ involucra la distribución de entrada p así como Γ.
- En general las características de la entrada no son conocidas en el Receptor, pero si las las características del canal, en particular las probabilidades $\Gamma_{cz} = Pr(z|c)$.
- Por tanto podemos definir una regla más práctica de la siguiente forma:

Definición 11 (Regla de la máxima posibilidad)

La regla de la máxima posibilidad dice que, dado z, el Receptor debería escoger $\sigma(z)$ igual a una palabra codificada c que cumpla

$$Pr(z|c) \geq Pr(z|c') \text{ para todo } c' \in C.$$

- La regla de la máxima posibilidad dice que $\sigma(z)$ debe ser una palabra codificada c para la cual la probabilidad que z sea recibida, dada que c es enviada debe ser máxima.
- Escribiendo la condición como $\Gamma_{cz} \geq \Gamma_{c'z}$ la regla puede ser expresada:
  - Dado z, escoger el mayor término Γ_{cz} en la columna z de la matriz del canal y establece $\sigma(z) = c$.
- En el caso que exista más de una c que satisfaga esta condición, el receptor deberá escoger una de forma arbitraria.

Definición 12 (Regla de la Mínima distancia)

La regla de la mínima distancia (o regla MD) dice que dado $z \in \mathbb{B}^n$, el Receptor debe escoger $\sigma(z)$ sea una palabra codificada c tal que $d(z, c)$ es mínimo.

Teorema 6

Para un BSC extendido con $e < 1/2$, la regla de la máxima posibilidad es equivalente a la regla MD.

Ejemplo 7

Supongamos que el código $C \subseteq \mathbb{B}^8$ *tiene siete palabras codificadas*

$$c_1 = 0000\ 0000\ c_2 = 0011\ 1000\ c_3 = 1100\ 0001\ c_4 = 0000\ 1110$$

$$c_5 = 1011\ 1011\ c_6 = 0011\ 0110\ c_7 = 1100\ 1011.$$

Si σ *es la reglaMD, ¿Qué valor debe asignar el Receptor a:*

$$(i)\ \sigma(1010\ 1011)\ (ii)\ \sigma(1100\ 1001)\ ?$$

Solución:
(i) Las distancias $d(z, c_i)$ para z = 1010 1011 son:

i :	1	2	3	4	5	6	7
$d(z, c_i)$:	5	4	4	4	1	5	2

Por tanto la palabra codificada a z es c_5= 1011 1011. Acorde con el teorema, esta es también la palabra codificada c para la cual la probabilidad de recibir z, dado que c fue enviada, es la mayor.
(ii) Las distancias $d(z', c_i)$ para z'= 1100 1001 son:

i :	1	2	3	4	5	6	7
$d(z, c_i)$:	4	5	1	5	4	8	1

En este caso tenemos dos palabras codificadas c_3 y c_7 que pueden ser escogidas como $\sigma(z')$. El Receptor puede fijar una de las dos opciones, o cuando z' ocurre, elegirá una de las dos opciones de forma aleatoria.

Ejercicio 12

Sea $C \subseteq \mathbb{B}^8$ con palabras codificadas como:

$$c_1 = 00000000 \; c_2 = 00111000 \; c_3 = 11000001 \; c_4 = 00001110$$

$$c_5 = 10111011 \; c_6 = 00110110 \; c_7 = 11001011.$$

Utilizando la regla MD σ, encontrar $\sigma(z)$ cuando z es i) 1000 1011, ii) 1011 1010, iii) 1100 0101.

Solución:

i) $10001011 \mapsto c_7$

$i:$	1	2	3	4	5	6	7
$d(z, c_i):$	4	5	3	3	2	6	1

ii) $10111010 \mapsto c_5$

$i:$	1	2	3	4	5	6	7
$d(z, c_i):$	5	2	6	4	1	3	4

iii) $11000101 \mapsto c_3$

$i:$	1	2	3	4	5	6	7
$d(z, c_i):$	4	7	1	5	6	6	2

Ejercicio 13

Considere el código C que consiste de 10 palabras en $\mathbb{B}^5$ que tienen exactamente dos bits igual a 1. Si un error es realizado en la transmisión del código, ¿Cuales son las posibles palabras recibidas?. Para cada z, realizar una lista de palabras codificadas que están cercas a z.

Solución:
Las palabras del código son:

$$c_1 = 11000,\ c_2 = 10100,\ c_3 = 10010,\ c_4 = 10001,\ c_5 = 01100,\ c_6 = 01010,$$
$$c_7 = 01001,\ c_8 = 00110,\ c_9 = 00101,\ c_{10} = 00011.$$

Si transmito 11000 y hay un error los posibles palabras codificadas erróneas son:

$$z_1 = 10000,\ z_2 = 01000,\ z_3 = 11100,\ z_4 = 11010,\ z_5 = 11001$$

En el caso de $z_1 = 10000$

$i:$	1	2	3	4	5	6	7	8	9	10
$d(z, c_i):$	1	1	1	1	3	3	3	3	3	3

Corrección Errores

- El propósito de una regla de decisión es asegurar que, tanto como sea posible, los errores sean corregidos.
- Nos centraremos en la regla MD para BSC extendido, donde la efectividad de la regla depende de ciertos parámetros del código.

Definición 13 (Mínima Distancia)

Sea d(c,c') la distancia Hamming entre dos palabras codificadas c y c' en un código $C \subseteq \mathbb{B}^n$. La mínima distancia de C es

$$\delta = min\ d(c, c') \text{ para todo } c \neq c'$$

- Por ejemplo, supóngase $C \subseteq \mathbb{B}^6$ tiene cuatro palabras codificadas

$$000\ 000,\ 111\ 000,\ 001\ 110,\ 110\ 011$$

- La distancia entre las palabras codificadas son como sigue:

$$d(000000, 111000) = 3,\ d(000000, 001110) = 3,\ d(000000, 110011) = 4,$$
$$d(111000, 001110) = 4,\ d(111000, 110011) = 3,\ d(001110, 110011) = 5.$$

- por lo que la mínima distancia es $\delta = 3$.

Definición 14 (Vecindario)

Para cualquier $x \in \mathbb{B}^n$ y cualquier $r \geq 0$, el vecindario de x con radio r es el conjunto

$$N_r(x) = \{y \in \mathbb{B}^n \mid d(x, y) \leq r\}.$$

- Equivalentemente, el vecindario $N_r(x)$ contiene todas las palabras que pueden ser obtenidos desde x no cometiendo más de r bit errores.
- Por ejemplo, si establecemos $x = 11010 \in \mathbb{B}^5$.
  - El vecindario $N_1(x)$ contiene x y las cinco palabras obtenidas al realizar un error en x,
  - $N_1(x) = \{11010, 01010, 10010, 11110, 11000, 11011\}$.

Lema 2

Si C es un código con $\delta \geq 2r+1$, entonces para cada palabra codificada $c, c' \in C$, el vecindario $N_r(c)$ y $N_r(c')$ son disjuntos (Vea figura 6).

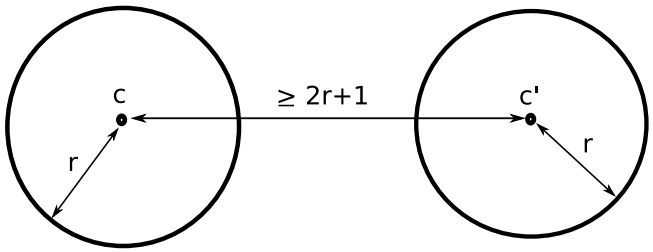

Figura 6 : Si $\delta \geq 2r+1$ entonces $N_r(c)$ y $N_r(c')$ son disjuntos

Teorema 7

Supongase el Emisor utiliza un código C que tiene la mínima distancia $\delta \geq 2r + 1$, y el Receptor utiliza la regla MD.
Entonces, siempre que no se produzcan error en más de r bits en la transmisión de cualquier palabra codificada, no cabe que una confusión suceda.
Cada palabra recibida será restaurada a una palabra codificada correcta.

Definición 15 (Código Corrector Error)

Un código $C \subseteq \mathbb{B}^n$ es un código corrector de error r si $\delta \geq 2r + 1$.

- La definición esta basada en la suposición que utilizamos la regla MD.
- Un código con $\delta \geq 2r + 1$ corrige r errores. Por ejemplo, si δ es al menos 3, entonces C corrige 1 error.

Ejercicio 14

Construya un código corrector-1 $C \subseteq \mathbb{B}^6$ *con* $|C| = 5$.

Ejercicio 14

Construya un código corrector-1 $C \subseteq \mathbb{B}^6$ con $|C| = 5$.

Solución:
En el ejemplo anterior teníamos

$$000\ 000,\ 111\ 000,\ 001\ 110,\ 110\ 011$$

La distancia eran:

$$d(000000, 111000) = 3,\ d(000000, 001110) = 3,\ d(000000, 110011) = 4,$$
$$d(111000, 001110) = 4,\ d(111000, 110011) = 3,\ d(001110, 110011) = 5.$$

Debemos añadir una palabra, longitud 5. Es posible añadir 010 101.

$$d(000000, 010101) = 3,\ d(111000, 010101) = 4,$$
$$d(001110, 010101) = 4,\ d(110011, 010101) = 3.$$

por lo que la mínima distancia sigue siendo $\delta = 3$.

Ejercicio 15

Para el código C construido en el ejercicio anterior, ¿Cuantas palabras no pueden ser corregidas bajo el supuesto que hemos realizado la corrección de al menos un bit?

Ejercicio 15

Para el código C construido en el ejercicio anterior, ¿Cuantas palabras no pueden ser corregidas bajo el supuesto que hemos realizado la corrección de al menos un bit?

Solución:
Para cada $c \in C$, hay 6 palabras que pueden ser derivadas con un sólo error, por lo que $|N_1(c)| = 7$.
Por tanto, con las 5 palabras tenemos 5 x 7 =35 palabras que pueden ser corregidas, por lo que el número de palabras que no pueden ser corregidas son $2^6 - 35 = 29$.

El límite de embalaje (The packing bound)

- Cuando intentamos construir códigos correctores con un δ dado, nos encontramos ante un problema.
- Escoger un conjunto de palabras codificadas C $\in \mathbb{B}^n$, tal que las palabras codificadas estén muy separadas (en el sentido de la distancia Hamming), implica una restricción en el número de palabras codificadas $|C|$.

Teorema 8 (Límite de embalaje)

Si $C \subseteq \mathbb{B}^n$ es un código con $\delta \geq 2r+1$, entonces

$$|C| \left(1 + n + \binom{n}{2} + \ldots + \binom{n}{r}\right) \leq 2^n$$

Ejemplo 8

Debemos emitir número de ID, de la forma de cadenas de n bits, a 100 empleados. Los empleados pueden cometer errores utilizando sus ID's, por lo que hemos decidido que debemos utilizar un código corrector de 2 bits. ¿Cual es el menor valor de n para que esto sea posible?

Ejemplo 8

Debemos emitir número de ID, de la forma de cadenas de n bits, a 100 empleados. Los empleados pueden cometer errores utilizando sus ID's, por lo que hemos decidido que debemos utilizar un código corrector de 2 bits. ¿Cual es el menor valor de n para que esto sea posible?

Solución:
Para r $= 2$ errores y $|C| = 100$ el límite de embalaje

$$100\,(1 + n + n(n-1)/2) \leq 2^n = 50(n^2 + n + 2) \leq 2^n$$

Por prueba y error, el menor valor de n que mantiene esta inegualdad es n=14.
Por supuesto, el problema de construir un conjunto con 100 palabras codificadas, cada una de longitud 14, se mantiene.

- Vamos a denotar como $A(n, \delta)$ el mayor valor de $|C|$ para el cual existe un código $C \subseteq \mathbb{B}^n$ con mínima distancia δ.
- El límite de embalaje nos proporciona un límite superior para $A(n, \delta)$, pero no tenemos garantía que un código de ese tamaño exista.
- En realidad el problema de evaluar $A(n, \delta)$ es un problema en general muy complicado.

Ejemplo 9

¿Cual es el valor de $A(10, 7)$, el tamaño más grande posible de un código $C \subseteq \mathbb{B}^{10}$ con una distancia mínima $\delta = 7$?

Ejemplo 9

¿Cual es el valor de $A(10,7)$, el tamaño más grande posible de un código $C \subseteq \mathbb{B}^{10}$ con una distancia mínima $\delta = 7$?

Solución:
En este caso necesitamos $\delta = 2r + 1$ con r=3, por lo que el límite de embalaje es

$$|C| \left(1 + 10 + \begin{pmatrix} 10 \\ 2 \end{pmatrix} + \begin{pmatrix} 10 \\ 3 \end{pmatrix} \right) \leq 2^{10}$$

que es, $|C| \leq 1024/176$. Ya que $|C|$ es un entero, tendremos que $A(10,7) \leq 5$

- Hay otra forma muy útil de interpretar las restricciones impuestas por el límite de embalaje.
- Cuando $C \subseteq \mathbb{B}^n$ y $|C| = m$, una palabra codificada $c \in C$ transmite (al menos) $log_2 m$ bits de información, pero requiere n bits de datos.

Definición 16 (Tasa de Información)

La tasa de información de un código $C \subseteq \mathbb{B}^n$ es

$$\rho = \frac{log_2|C|}{n}$$

- Por ejemplo, supongamos $C \subseteq \mathbb{B}^6$ tiene cuatro palabras codificadas

$$000000,\ 111000,\ 001110,\ 110011.$$

- En este caso n=6 y $|C| = 4 = 2^2$, por lo que la tasa de información es $\rho = 2/6 = 1/3$.
- Esto corresponde al hecho que C requiere 6 bits de datos para codificar 2 bits de información.
- Si suponemos que un megabyte puede ser transmitido por segundo, cuando C es utilizado para codificar los datos, solamente un tercio de un megabyte de información es realmente transmitida por segundo.
- Construir un código $C \subseteq \mathbb{B}^n$ con un tamaño dado $|C|$ y dado un valor dado de δ es equivalente a construir un código con valores dados de n, ρ y δ.
- El límite de embalaje nos muestra que existe una compensación entre ρ y δ.

Ejercicio 16

Si necesitamos un código $C \subseteq \mathbb{B}^6$ con tasa de información de al menos 0.35, ¿Cual es el menor valor posible de $|C|$?

Ejercicio 16

Si necesitamos un código $C \subseteq \mathbb{B}^6$ con tasa de información de al menos 0.35, ¿Cual es el menor valor posible de $|C|$?

Solución:
$\rho = \frac{log_2|C|}{n}$; $0{,}35 = \frac{log_2|C|}{6}$ $2,1 = log_2|C|$ Por tanto $|C| = 5$

Ejercicio 17

Muestra que $(log_2 9)/6 = 0{,}528$ *es un límite superior para la tasa de información de un código* $C \subseteq \mathbb{B}^6$ *corrector 1*

Solución:
Según el límite del embalaje tenemos $|C|(1+n) \leq 2^6; 7|C| \leq 64$; Por tanto $|C| \leq 9$ y la tasa es $\rho = log_2 9/6$

Ejercicio 18

Queremos emitir números ID, en la forma de cadena de n bits, a 1000 personas, utilizando un código corrector-1.¿Cual es el menor valor para n que hace esta situación posible?

Ejercicio 18

Queremos emitir números ID, en la forma de cadena de n bits, a 1000 personas, utilizando un código corrector-1.¿Cual es el menor valor para n que hace esta situación posible?

Solución:
Tenemos $|C| = 1000$ personas y r=1. Por lo que el límite de embalaje nos proporciona $1000(1+n) \leq 2^n; 1000 + 1000n \leq 2^n$; Con n=14 tenemos $15000 \leq 16384$

La probabilidad de una confusión

Volvemos (Figura 7) al modelo de comunicaciones anteriormente descrito.

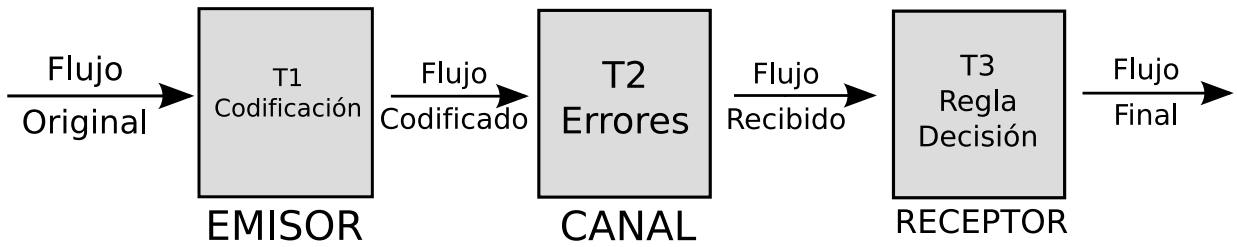

Figura 7 : Un modelo de sistema de comunicación

- Supongase que el flujo original es emitido por una fuente que produce símbolos de un alfabeto X, acorde a la distribución de probabilidad p sobre X.
- Cuando el Emisor utiliza el código C, la probabilidad de enviar una palabra codificada $c \in C$ es la misma que la probabilidad que la fuente emita el símbolo $x \in X$ para el cual c es la palabra codificada. Por tanto consideramos el flujo codificado como emitido por una fuente (C,p).
- Ya que p puede ser desconocido, la regla de decisión apropiada es la regla de máxima posibilidad. Dado que el canal es el BSC extendido, el Receptor puede utilizar la forma equivalente, la regla MD.
- Para cada $c \in C$, denotamos por F(c) el conjunto de palabras las cuales la regla MD σ no asigna c:

$$F(c) = \{z \in \mathbb{B}^n | \sigma(z) \neq c\}.$$

- Acorde con la Definición 6 una confusión ocurre cuando una palabra codificada $c \in C$ es alterada en transmisión y la palabra recibida está en F(c). En esta situación, el Receptor decidirá una palabra codificada c'diferente de la c que fue enviada.
- Para una palabra codificada c sea M_c la probabilidad cuando c es enviada y la palabra recibida z está en F(c), en otras palabras M_c es la suma de las probabilidades condicionales $Pr(z|c)$ para $z \in F(c)$:

$$M_c = \sum_{z \in F(c)} Pr(z|c)$$

Definición 17 (Probabilidad de una confusión)

La probabilidad de una confusión cuando el flujo codificado corresponde a una fuente (C, p)

$$M(C, p) = \sum_{c \in C} p_c M_c$$

- El objetivo es escoger el código C para que M(C,p) sea tan pequeño como sea posible.

Ejemplo 10

Estamos realizando un mando para manejar una aplicación remota y debemos mandar solamente dos mensajes $ARRIBA$, $ABAJO$. Tenemos dos posibles códigos:

$$\textit{(i)}\ ARRIBA \mapsto 0,\ ABAJO \mapsto 1;$$
$$\textit{(ii)}\ ARRIBA \mapsto 000,\ ABAJO \mapsto 111;$$

Los mensajes codificados son transmitidos vía un BSC extendido con una probabilidad de error de bit e, y utilizamos la regla MD. ¿Qué código tiene la menor probabilidad de una posible confusión?

Solución:

1. Aquí n = 1 y el código es $C_1 = \{0, 1\}$. La regla MD es $\sigma(0) = 0$, $\sigma(1) = 1$, y los conjuntos F(c) son: $F(0) = \{1\}$,$F(1) = \{0\}$.
   Las probabilidades M_0 y M_1 son: $M_0 = Pr(1|0) = e$, $M_1 = Pr(0|1) = e$.
   Por tanto, para cualquier distribución p = [p, 1 - p] en C_1,

$$M(C_1, p) = p \times e + (1 - p) \times e = e.$$

2. Aquí n = 3 y el código es $C_3 = \{000, 111\}$. La regla MD es

$$\sigma(000) = \sigma(100) = \sigma(010) = \sigma(001) = 000,$$

$$\sigma(011) = \sigma(101) = \sigma(110) = \sigma(111) = 111.$$

   Con esta regla

$$F(000) = \{011, 101, 110, 111\}, F(111) = \{000, 001, 010, 100\}.$$

Continua ...

- Si la palabra codificada 000 es enviada, la probabilidad M_{000} de una confusión es por tanto:

$$Pr(011|000)+ Pr(101|000) + Pr(110|000) + Pr(111|000) = e^2(1-e) + e^2(1-e) + e^2(1-e) + e^3.$$

- Una aproximación rápida que podemos establece que los cuatro términos son menores que e^2 $(3e^2 - 2e^3)$, por lo que $M_{000} < 4e^2$.
- Un cálculo similar muestra también que $M_{111} < 4e^2$.
- Por tanto, para cualquier distribución $p = [p, 1-p]$ en C_3,

$$M(C_3, p) < p(4e^2) + (1-p)(4e^2) = 4e^2.$$

- Por tanto, cuando e es pequeña, $M(C_3, p)$ es inferior que $M(C_1, p)$. Por ejemplo, cuando $e = 0{,}001$, tenemos

$$M(C_1, p) = 0{,}001,\ M(C_3, p) < 0{,}000004.$$

Lema 3

Si $C \subseteq \mathbb{B}^n$ es un código corrector de r-error, y z está en F(c), entonces $d(z, c) \geq r + 1$.

Ejercicio 19

Sea $C = \{00000, 11100, 00111\}$. *Si* σ *es una regla de decisión MD para C, muestra que F(c) es un conjunto de al menos un tamaño 12, para cada palabra codificada c.*

Ejercicio 19

Sea $C = \{00000, 11100, 00111\}$. Si σ es una regla de decisión MD para C, muestra que F(c) es un conjunto de al menos un tamaño 12, para cada palabra codificada c.

Solución:
Para cada $c \in C$ hay otras dos palabras codificadas La regla MD no asigna estas palabras codificadas a c, ni las palabras con distancia 1. Por tanto F(c) contiene al menos 2 x (1+5) =12 palabras.

Ejercicio 20

Considere el código $C = \{0, 1\}$ como la entrada a un BSC con probabilidad de error e=0.2. Verifica que la regla de decisión de la máxima posibilidad es dada por la regla $\sigma(0) = 0$, $\sigma(1) = 1$, y la probabilidad de un error es 0.2 para cualquier distribución p sobre C.

Solución:

- La regla de máxima posibilidad dice que $\sigma(z) = c$ cuando $Pr(z|c) \geq Pr(z|c')$ para toda $c' \in C$.
- Utilizando la matriz del canal la condición es que $\sigma(z) = c$, donde Γ_{cz} es el máximo elemento en la columna z.
- Aquí la matriz es

$$\begin{pmatrix} 0{,}8 & 0{,}2 \\ 0{,}2 & 0{,}8 \end{pmatrix}$$

- tenemos $\sigma(0) = 0{,}\sigma(1) = 1$ que da lugar a $M_0 = 0{,}2$ y $M_1 = 0{,}2$.
- Por tanto para cada distribución de entrada **p**= (p,1-p) la probabilidad de confusión es $p \times M_0 + (1 - p) \times M_1 = 0{,}2$.

Codificación según una tasa establecida

- Continuamos discutiendo el modelo mostrado en la figura 7. Específicamente, en la fase T1 representa codificación con un código binario C, fase T2 representa una transmisión a través de un BSC extendido y la fase T3 representa la aplicación de la regla MD.

  Duda a plantear: ¿Es posible escoger el código C para que la probabilidad de una confusión sea arbitrariamente pequeña, mientras es transmitida a una tasa dada ρ?

- Podemos contestar que es posible, siempre que ρ no sea muy grande.
- En realidad, la clave para mantener una tasa de información dada ρ es codificar bloques de símbolos, más que símbolos individuales. Es conveniente suponer que el flujo original está en forma de una cadena de bits.

- Este puede ser establecido mediante una regla simple 'pre-coding'. Por ejemplo, si el flujo original es una secuencia de comandos N, S, E, O, podemos utilizar la regla 'pre-coding' $N \mapsto 00$, $S \mapsto 01$, $E \mapsto 10$, $O \mapsto 11$.
- Consideramos la siguiente estrategia para la fase T1. El Emisor divide el flujo original de bits en bloques de un cierto tamaño, k, y asigna a cada bloque una palabra codificada perteneciente a un código C. Hay 2^k posibles bloques, por lo que es necesario un código del tamaño $|C| = 2^k$.
- Para asegurar que la tasa de información no es menor que algún valor dado ρ, el Emisor debe determinar la longitud apropiada n para las palabras codificadas.

- La tasa de información de el código C es $(log_2|C|)/n = k/n$. Por tanto el Emisor debe escoger los parámetros k,n, y el código $C \subseteq \mathbb{B}^n$, tal que :

$$|C| = 2^k \text{ y } k \geq \rho \times n.$$

- El Emisor también desea escoger el código C para que la probabilidad de una confusión es pequeña, conociendo que el flujo codificado puede ser transmitido a través de un BSC extendido con una probabilidad de error de bit e, y el Receptor deberá utilizar la regla de decisión MD.
- Estas condiciones implica que un compromiso entre los parámetros ρ y δ.

Ejemplo 11

Supongase que la tasa de información deseada es $\rho = 0{,}8$ *y que el Emisor quiere utilizar un código corrector 1* $(\delta \geq 3)$ *. ¿Cuales son los valores más pequeños posibles de n y k?*

Solución:

- Si $C \subseteq \mathbb{B}^n$ es un código corrector de error 1 con $|C| = 2^k$, mediante el límite de embalaje tenemos $2^k(1+n) \leq 2^n$.
- También, para alcanzar la tasa de $\rho = 0{,}8$, el Emisor debe asegurar que k no es menor que $0{,}8 \times n$.
- Por tanto necesitamos la asignación del menor valor de n para el cual hay un entero k que satisface

$$n + 1 \leq 2^{n-k} \text{ y } 5k \geq 4n.$$

- Mediante prueba y error el menor posible es $n = 25, k = 20$.
- El ejemplo muestra que al menos 2^{20} (sobre un millón) palabras codificadas de longitud 25 son necesarias para alcanzar la tasa requerida $\rho = 0{,}8$.

Ejemplo 12

Sea C el código que asigna a cada bloque de 3 bits, $y_1y_2y_3$, la palabra codificada $x_1x_2x_3x_4x_5x_6 \in \mathbb{B}^6$ definida como sigue:

$$x_1 = y_1$$
$$x_2 = y_2$$
$$x_3 = y_3$$
$$x_4 = 0 \text{ si } y_1 = y_2, \text{ si no } x_4 = 1$$
$$x_5 = 0 \text{ si } y_2 = y_3, \text{ si no } x_5 = 1$$
$$x_6 = 0 \text{ si } y_1 = y_3, \text{ si no } x_6 = 1$$

Muestra que C es un código corrector de error 1 y su transferencia es $\rho = 0{,}5$.

Solución:
Explicitamente el código es:

$$000 \mapsto 000000, 001 \mapsto 001011, 010 \mapsto 010110, 100 \mapsto 100101,$$
$$011 \mapsto 011101, 101 \mapsto 101110, 110 \mapsto 110011, 111 \mapsto 111000.$$

Verificando las distancias entre pares de palabras codificadas, la mínima distancia es 3.
Por lo que C es un código corrector de error 1 y ya que n $= 6$ y k=3 la tasa de información es $1/2$.

Ejercicio 21

Supongase que el Emisor quiere codificar bloques de tamaño k con palabras de longitud n, utilizando un código de corrección-1. Si tenemos como requisito transmitir con tasa de información no menor que 0.6. ¿Cual es el menor valor posible de n y k?

Ejercicio 21

Supongase que el Emisor quiere codificar bloques de tamaño k con palabras de longitud n, utilizando un código de corrección-1. Si tenemos como requisito transmitir con tasa de información no menor que 0.6. ¿Cual es el menor valor posible de n y k?

Solución:

- $\rho = k/n$; $0{,}6 = k/n$. $k \geq 0{,}6n$; $5k \geq 3n$
- $2^k(1+n) \leq 2^n$, $(1+n) \leq 2^{n-k}$
- n= 10, k=6.

Transmisión utilizando BSC extendido

- Consideramos la etapa T2 de nuestro modelo, la transmisión de un flujo codificado utilizando un BSC extendido con la posibilidad que ocurran errores de bit.
- Comenzamos mostrando que si la capacidad del BSC es γ, entonces la capacidad de Γ^n es $n\gamma$. Intuitivamente esto es porque Γ^n puede ser consideradas como n copias de Γ "en paralelo", y las copias son independientes.
- El flujo codificado puede tener interdependencias entres sus bits pero cuando cada bit individual es transmitido a través de Γ^n existe la misma probabilidad que un error ocurra, independientemente de lo que ocurra con los otros bits.
- Este hecho es implícito en la definición general de Γ^n como el producto de n copias de Γ (Definiciones 6.6 y 6.7).

- En nuestro modelo las entradas a Γ^n son palabras codificadas $c_1 \dots c_n \in C$ y las salidas son las palabras $z_1 \dots z_n \in \mathbb{B}^n$. Tenemos

$$(\Gamma^n)c_1 \dots c_n z_1 \dots z_n = Pr(z_1 \dots z_n | c_1 \dots c_n) = Pr(z_1|c_1) \dots Pr(z_n|c_n)$$
$$= \Gamma c_1 z_1 \dots \Gamma c_n z_n.$$

- Para el caso de BSC tenemos una fórmula explícita para las entradas de Γ^n, pero no la necesitamos aquí.
- Suponemos que el flujo codificado es emitido por una fuente (C,p).
- Entonces el flujo recibido es una fuente ($\mathbb{B}^n$,q), donde q = p Γ^n.

Lema 4

Sea Γ el BSC con probabilidad de error e. Entonces, con la notación anterior,

$$H(q|p) = n \times h(e)$$

Teorema 9

Si la capacidad de el BSC Γ es $\gamma = 1 - h(e)$, entonces la capacidad de Γ^n es $n \times \gamma$

- Ahora Consideramos que la incertidumbre de la situación desde el punto de vista del Receptor. Anteriormente hemos denotada esta cantidad por $H(\Gamma^n; p) = H(p|q)$.
- En este caso representa la incertidumbre (por palabra codificada) del flujo codificado (C,p) dado el flujo recibido.
- Si cada palabra codificada tiene n bits, la incertidumbre por bit es $H(\Gamma^n; p)/n$.
- El siguiente teorema muestra que, cuando la tasa de información requerida excede la capacidad del canal, esta cantidad no puede ser restablecida arbitrariamente para todas las distribuciones p, sin embargo podemos elegir C y n.

Teorema 10

Sea $C \subseteq \mathbb{B}^n$ un código con ratio de información ρ, y sea p^* la distribución en el cual cada palabra codificada en C es igualmente probable.
Supóngase que el flujo emitido por una fuente (C, p^*) es transmitida a través del BSC extendido Γ^n, donde Γ tiene la capacidad γ. Entonces

$$H(\Gamma^n; p^*) \geq n(\rho - \gamma).$$

El resultado es trivial cuando $\rho < \gamma$, ya que la parte derecha es negativa y es siempre verdad por definición y por tanto la parte izquierda no es negativa.
Sin embargo, como veremos el resultado es muy significante cuando $\rho > \gamma$.

Ejercicio 22

Supongamos que un código binario con tasa de información 0.9 es transmitida mediante un BSC extendido con probabilidad de error 0.03. ¿Excede la tasa la capacidad? Si cada palabra codificada es equiprobable, ¿Que podemos decir sobre la incertidumbre desde el punto de vista del Receptor?

Ejercicio 22

Supongamos que un código binario con tasa de información 0.9 es transmitida mediante un BSC extendido con probabilidad de error 0.03. ¿Excede la tasa la capacidad? Si cada palabra codificada es equiprobable, ¿Que podemos decir sobre la incertidumbre desde el punto de vista del Receptor?

Solución:
Ya que e $= 0.03$, tenemos que $\gamma = 1 - h(e) \approx 0{,}80$. Por tanto la incertidumbre es de al menos $0{,}1 \times n$ donde n es la longitud de las palabras codificadas.

La tasa de transmisión no puede exceder la capacidad

- Nos centraremos ahora en el caso de que si la probabilidad de una confusión debe de ser arbitrariamente pequeña, entonces la capacidad del canal es el límite superior de la tasa al cual la información puede ser transmitida.
- Considere la fase T3 de nuestro modelo, donde el Receptor convierte el flujo recibido en un flujo final utilizando la regla MD.
- El flujo final es una secuencia de palabras codificadas, producidas por la fuente (C,p) y existen dos elementos de incertidumbre asociado con ello:

1. Receptor no conoce si se ha producido una confusión.
   - La probabilidad de una confusión es M = M(c,p) y la probabilidad de no confusión es 1-M.
   - La incertidumbre asociada a esta situación es h(M):

$$h(M) = M \log(1/M) + (1 - M) \log(1/(1 - M)).$$

2. Si una confusión ha ocurrido, entonces la palabra codificada correcta ha sido reemplazada por una incorrecta.
   - En este caso el Receptor no conoce cual de las otras palabras codificadas $|C| - 1$ es la correcta.
   - La probabilidad de un error es M, y la incertidumbre asociada con $|C| - 1$ elecciones es al menos $log(|C| - 1)$,
   - Por lo que este hace una contribución de al menos $Mlog(|C| - 1)$ a la incertidumbre total.

- La aplicación de la regla de decisión puede solamente incrementar la incertidumbre.
- Por tanto la incertidumbre del flujo final, el cual es la suma de dos cantidades descritas anteriormente, es un límite superior para la incertidumbre del flujo recibido:

$$H(\Gamma; p) \leqslant h(M) + Mlog(|C| - 1).$$

- Este resultado es conocido como la igualdad de Fano y juega una parte importante en el siguiente teorema 12.

Teorema 11 (Inegualdad de Fano)

Sea $C \subseteq \mathbb{B}^n$, y sea M = M (C,p) la probabilidad de un error cuando la fuente (C,p) es transmitida a través del BSC extendido Γ^n, y la regla de decisión MD es utilizada. Entonces

$$H(\Gamma^n; p) \leq h(M) + Mlog(|C| - 1).$$

Recordamos que la razón de codificar un flujo de bits de la forma que:

1. La información es transmitida a un ratio establecido ρ
2. La probabilidad de una confusión, M, es arbitrariamente pequeña.

- Para satisfacer estos criterios debemos construir códigos $C_n \subseteq \mathbb{B}^n$ para una secuencia infinita de valores de n.
- Si $|C_n| = 2^{k_n}$, el criterio 1 debe ser satisfecho estableciendo que k_n es al menos $\rho \times n$.
- Si esa situación ocurre, podemos dividir el flujo en bloques de tamaños k_n y asignar una palabra codificada en C_n a cada bloque.
- Sin embargo en el siguiente resultado muestra no podemos cumplir 2 si ρ es mayor que γ.

Teorema 12

Supongase que, para una secuencia infinita de valores de n, hemos construido códigos $C_n \subseteq \mathbb{B}^n$ *tal que* $|C_n| \geqslant 2 \times \rho \times n$.
Sea p^* *la distribución equiprobable en* C_n.
Si $\rho > \gamma$, *entonces la probabilidad de una confusión* $M(C_n, p^*)$ *no tiende a cero cuando* $n \to \infty$.

Ejercicio 23

Supongamos que utilizamos el BSC extendido para transmitir palabras codificadas de longitud 18, y la regla MD es utilizada por el receptor. Experimentalmente hemos encontrado que un código con 64000 palabras codificadas pueden ser transmitida con una probabilidad de confusión despreciable. ¿Qué conclusión podemos establecer sobre a probabilidad de error de bit e?

Ejercicio 23

Supongamos que utilizamos el BSC extendido para transmitir palabras codificadas de longitud 18, y la regla MD es utilizada por el receptor. Experimentalmente hemos encontrado que un código con 64000 palabras codificadas pueden ser transmitida con una probabilidad de confusión despreciable. ¿Qué conclusión podemos establecer sobre a probabilidad de error de bit e?

Solución:
La tasa del código es $(log_2 64000/18 \approx 16/18 \approx 0{,}889$.
Ya que la probabilidad de una confusión es despreciable, podemos inferir que la capacidad del canal es al menos 0.889.
Por tanto $1 - h(e) \geq 0{,}889$, o lo que es lo mismo $h(e) \leq 0{,}111$.
Esto implica que $e < 0{,}015$

Teorema de Shannon

- El resultado teórico mas representante en la Teoría de la Información es el Teorema de Shannon.
- Establece que si $\rho < \gamma$ entonces es posible encontrar una secuencia infinita de códigos C_n tal que

$$C_n \subseteq \mathbb{B}^n \text{ , } |C_n| \geqslant 2 \times \rho \times n, \text{ y } M(C_n, p) \to 0 \text{ cuando } n \to \infty.$$

- Por ejemplo, supongamos que queremos transmitir un flujo de bits, utilizando un dispositivo para el cual la probabilidad de error de bit es estimado a ser 0.03.
- Además sabemos que la probabilidad de confusión debe ser menor que 10^{-6}.
- Conociendo el Teorema de Shannon, podemos intentar diseñar nuestro sistema de la siguiente forma.

  Paso 1 Establece un valor específico de ρ menor que γ. Aquí la capacidad de BSC con e $= 0.03$ es $\gamma = 1 - h(e) = 0{,}8$ aproximadamente, por lo que un valor adecuado para $\rho = 0{,}75$.

  Paso 2 Basándonos en el Teorema de Shannon, escoger un código $C_n \subseteq \mathbb{B}^n$ tal que

  $$|C_n| = 2^k \text{ (donde } k \geq 0{,}75n\text{), y } M(C_n, p) < 10^{-6}.$$

  Paso 3 Divide el flujo original en bloques de longitud k y codificar los bloques utilizando las palabras codificadas de C_n.

  Paso 4 Transmitir el flujo codificado y aplicar la regla MD al flujo recibido.

- En la práctica, encontraremos dificultades si intentamos implementar este plan.
- El paso 2 del Teorema de Shannon nos dice que un código apropiado C_n existe, pero no dice como encontrarlo.
- El mismo problema ocurre en el paso 3, donde tenemos que establecer una regla que asigna una palabra codificada de longitud n a cada bloque de k bits, o en otras palabras tenemos que especificar una función de codificación $\mathbb{B}^k \to \mathbb{B}^n$.
- Por tanto, aunque el Teorema de Shannon es un resultado teórico, no permite establecer un conjunto de instrucciones.
- En el siguiente tema describiremos algunas técnicas matemáticas que pueden ser utilizada para construir buenas funciones de codificación $\mathbb{B}^k \to \mathbb{B}^n$ para muchos valores de $\rho = k/n$

José A. Montenegro Montes
Dpto. Lenguajes y Ciencias de la Computación
ETSI Informática. Universidad de Málaga
monte@lcc.uma.es
twitter

UNIVERSIDAD DE MÁLAGA

E.T.S. INGENIERÍA INFORMÁTICA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA