Codificación de la Información y Seguridad en Redes

Teoría de la Información

Índice de Contenidos

- Introducción.
- Noción de Información.
- Información y sus Fuentes - Modelado
- Códigos - Introducción y Propiedades
- Codificación de las Fuentes de Información.
- Canales para la Transmisión de la Información
- Códigos Detectores y Correctores.

Introducción (1/6)

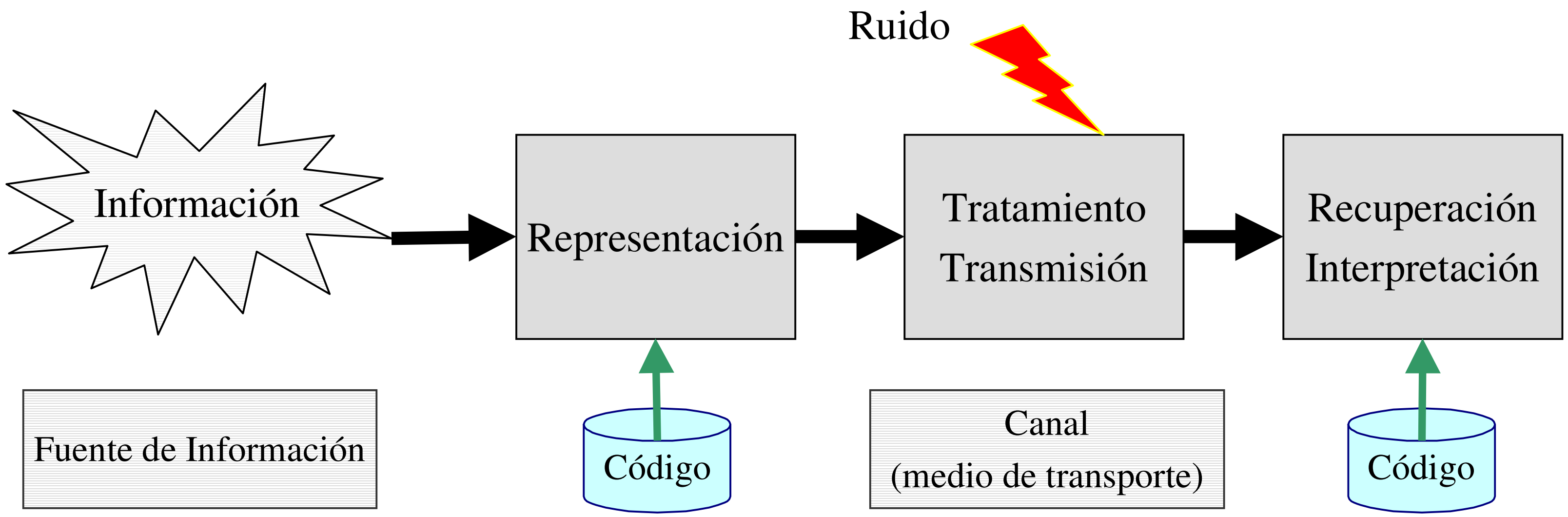
- Objetivos
  - El objetivo de la Teoría de la Información es: ***en una transmisión de información, cómo poder determinar cuándo los datos originales han cambiado, y cuando así sea, cómo se puede recuperar la información original***.
  - Básicamente hay tres aspectos prácticos:
    - Fiabilidad en la transmisión de la información (**detección y recuperación de errores**)
    - Eficiencia en la transmisión de la información (**compresión**)
    - Seguridad en la transmisión de información (**criptografía**)
- Perspectiva
  - Computadoras como dispositivos que adquieren, manipulan y transfieren información.
  - La computadora moderna sólo manipula dos símbolos: "`0`" y "`1`".Cualquier información que se vaya a usar ha de ser representada usando sólo estos dos símbolos.

Introducción (2/6)

- Aplicaciones en el mundo real
  - Representación de la información para ser manipulada por las computadoras (**codificación**).
  - **Compresión** de datos (p.ej..: sonido, imágenes) para su almacenamiento y transmisión.
  - **Encriptación** de la información (p.ej..: transmisiones cifradas, marcas de agua)
  - ...
- Conocimientos previos
  - La mayoría de los principios sobre los que se basan los procedimientos que se verán son parte de la Estadística, Combinatoria y el Álgebra.
    - Nociones elementales de probabilidad
    - Nociones elementales de combinatoria
    - Códigos empleados en informática (para los ejemplos).

Introducción (3/6)

- Esquema a seguir a partir de aquí:
  - Noción de Información.
  - Información y sus Fuentes - Modelado
  - Códigos - Introducción y Propiedades
  - Codificación de las Fuentes de Información.
  - Canales para la Transmisión de la Información
  - Códigos Detectores y Correctores de Errores.



Introducción (4/6)

- Bibliografía:

  - “Teoría de la Información y de la Codificación”, Norman Abramson, Ed. Paraninfo - 1986.
  - “Information Theory for Systems Engineers”, L. P. Hyvärinen, Ed. Springer-Verlag - 1968.
  - “Coding and Information Theory”, S. Roman, Ed. Springer-Verlag - 1992.
  - “Teoría de la Información y Codificación”, G. Cuevas, Ed. Politécnica de Madrid - 1981.
  - “Comunication Systems”, S. Haykin, Ed. John Wiley - 1994.
  - “Introduction to Coding Theory”, J. H. van Lint, Ed. Springer-Verlag - 1992.
  - “An Introduction to Source Coding”, Raymond Veldhuis y Marcel Breeuwer, Ed. Prentice Hall -1993.
  - “Source Coding Theory”, Robert M. Gray, Ed. Kluwer Academic Publishers - 1993.

Introducción (5/6)

- Conocimientos previos en Combinatoria

Número de distintas maneras en las que se puede ordenar un conjunto de n elementos.	$n!$
Número de distintos conjuntos de r elementos en los que se considera el orden con posibilidad de repetición, tomados de entre un total de n elementos.	n^r
Número de distintos conjuntos de r elementos en los que se considera el orden, sin posibilidad de repetir, tomados de entre un total de n elementos.	$\frac{n!}{(n-r)!}$
Número de distintos conjuntos de r elementos sin considerar el orden de dichos elementos y sin repetir ninguno, tomados de entre un total de n elementos.	$\binom{n}{r} = \frac{n!}{r!(n-r)!}$
Número de distintos conjuntos de r elementos sin considerar el orden, con posibilidad de repetición, tomados de entre un total de n elementos.	$\binom{n+r-1}{r}$

Introducción (6/6)

- Conocimientos previos en Probabilidad

Probabilidad del suceso complementario de A	$P(\overline{A}) = 1 - P(A)$
Probabilidad de que se dén simultáneamente dos sucesos A y B, cuando dichos sucesos son independientes	$P(A,B) = P(A) \cdot P(B)$
Probabilidad de que se den simultáneamente dos sucesos A y B, cuando A y B son estadísticamente dependientes uno del otro (**teorema de Bayes**)	$P(A,B) = P(A) \cdot P(B/A)$ $P(A,B) = P(B) \cdot P(A/B)$
Probabilidad de que se de o bien el suceso A, o bien el suceso B, siendo ambos estadísticamente independientes	$P(A \cup B) = P(A) + P(B)$
Probabilidad de que se de o bien el suceso A o bien el suceso B, siendo ambos sucesos estadísticamente dependientes uno del otro	$P(A \cup B) = P(A) + P(B) - P(A,B)$

Noción de Información (1/6)

- Primera Aproximación
  - Habitualmente se dice que la recepción de un mensaje, la visión de una imagen de televisión, oír un sonido, la lectura de una hoja con texto mecanografiado son acciones que proporcionan información.
  - Se dice que un determinado acontecimiento proporciona información cuando ese acontecimiento se refiere a la realización de un hecho que era desconocido de antemano.
    - Hoy el Sol ha salido por el Este - No aporta información.
    - Hoy las bolsas han subido un 5 % - Aporta información (¿útil?)
    - Mañana las acciones de Acerías subirán - Aporta información (¡$$!)
  - Como consecuencia se puede observar una relación muy fuerte con el concepto de probabilidad (una medida de la sorpresa que produce el hecho; hechos poco probables son muy sorprendentes) y hecho estadístico.

Noción de Información (2/6)

- En la información se pueden distinguir tres propiedades:
  - Para afirmar que se recibe información, el mensaje recibido tiene que ser desconocido de antemano.
    - Tiene que haber **incertidumbre** acerca del mensaje a recibir.
  - El receptor debe ser capaz de **entender** el mensaje.
    - Recibir un mensaje en un idioma desconocido no aporta información.
  - El mensaje recibido, si se ha entendido, debe ser **útil** para el receptor
    - En caso contrario, el receptor no pagaría por él mensaje ya que carecería de valor para él.

Noción de Información (3/6)

- **Aspectos relacionados con la Comunicación (*Información*)**
  - **Nivel Sintáctico**.
    - Atiende a aspectos tales como: número de símbolos, número de palabras que se pueden formar con ellos, propiedades estadísticas de estos elementos, las propiedades de los medios por los que se transmiten estos símbolos, ...
    - Aplicación de este nivel: transmisión y procesamiento de la información, fijándose en aspectos tales como **la eficiencia y la fiabilidad**.
    - Es **independiente de la naturaleza de la información**, ya que sólo atiende a los símbolos que la representan.
  - **Nivel Semántico**
    - Un problema relacionado: la traducción automática.
  - **Nivel Pragmático**
    - La utilidad (valor) de la información depende fuertemente del tiempo.

Noción de Información (4/6)

- Aproximación Intuitiva a la medida de la información:
  - Si una hoja de papel mecanografiada proporciona X unidades de información, dos hojas de papel mecanografiadas proporcionan 2X unidades de información.
    - Por simplicidad se supone que la Información en la hoja de papel se presenta en forma de caracteres cada uno de ellos inscrito en una celda de tamaño fijo.
    - Si hay r caracteres diferentes en el alfabeto con el que se escribe el mensaje (incluyendo espacio, signos de puntuación, ...), y en la hoja hay espacio para n caracteres, en una hoja se pueden construir un total de r^n mensajes diferentes.
      - Cada uno de esos posibles mensajes (combinación de caracteres) tendrá en principio una probabilidad de aparición de $P=1/ r^n$.
      - Si ahora se utilizan 2 hojas, la probabilidad de uno de esos mensajes es $P'=1/r^{2n}=P^2$.
  - Basándose en esta idea, parece razonable una medida de la información logarítmica con la probabilidad.

Noción de Información (5/6)

- **Definición de Información**: Sea E un suceso que puede presentarse con una probabilidad p(E). Cuando E ocurre se dice que proporciona

$$\boxed{I(E) = \log\left(\frac{1}{P(E)}\right)}$$

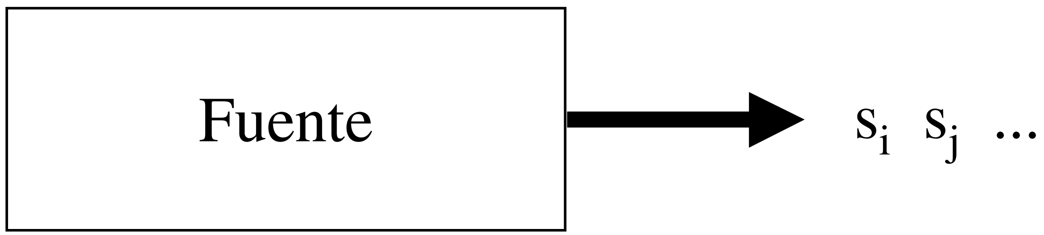
unidades de información.
- Las unidades de medida de la información dependen de la base en la que se calcule el logaritmo que aparece en la fórmula.
  - *Si se usa base 2, la unidad es el bit.*
- **Definición de bit**: la cantidad de información que se recibe cuando se observa un hecho que tiene una probabilidad de ocurrencia de 0.5.
  - **NO CONFUNDIR CON DÍGITO BINARIO.**

Noción de Información (6/6)

- Medio o soporte de la información
  - La información es almacenada o transmitida en/por un **medio físico** que puede alcanzar más de un *estado* a lo largo del tiempo.
  - **Sistema discreto de información**: el medio puede ser dividido en el tiempo o en el espacio en un conjunto discreto de unidades, y cada una de estas unidades tiene un número finito de estados.
  - **Sistema continuo de información**: las unidades del medio no pueden ser definidas de forma independiente unas de otras.
  - Las señales continuas pueden ser transformadas en discretas mediante el procedimiento de **muestreo**.
- Sólo se considerará el caso discreto.

Información y sus Fuentes: Modelos de F.I. (1/10)

- Introducción
  - Los modelos de F.I. proporcionan un mecanismo matemático generador de información, sobre el que medir propiedades.
  - Crear modelos para justificar el comportamiento del sistema modelado, descubrir nuevas propiedades y mejorar su comprensión.
  - Si el modelo no se ajusta a las medidas realizadas sobre el sistema real, se debe cambiar.
- Definición de **fuente de información** (discreta)**:** sistema capaz de generar una secuencia de símbolos pertenecientes a un alfabeto S, finito y fijo: $S = \{ s_1, s_2, ..., s_q \}$



Información y sus Fuentes: Modelos de F.I. (2/10)

- Definición de **F.I. de memoria nula**: F.I. en la que los símbolos que emite la fuente son estadísticamente independientes unos de otros.
  - Queda definida por su **alfabeto** $\{s_i\}$**y las probabilidades** de todos y cada uno de los símbolos de dicho alfabeto $\{p(s_i)\}$
  - La información asociada a la observación del símbolo s_i es

    $$I(s_i)=\log(1/p(s_i))$$
- Definición de **Entropía**: cantidad media de información recibida al observar un símbolo proveniente de la fuente S

$$\boxed{\mathrm{H}(S)=\sum_{i=1}^{q} p(s_i)\log\left(\frac{1}{p(s_i)}\right)}$$

  - **Unidades de medida de la entropía**:

    [unidades de información /símbolo emitido]
  - **Otra definición**: información media necesaria para identificar un símbolo que sale de la fuente.

Información y sus Fuentes: Modelos de F.I. (3/10)

- Propiedades de las funciones Entropía.

  $0 \leq H(S) \leq \log q$

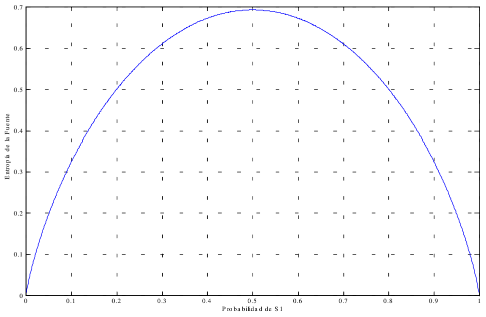
  Mínimo cuando no hay incertidumbre (hecho seguro).

  Máximo cuanto todos los símbolos son equiprobables, es decir, $p(s_i) = 1/q$.

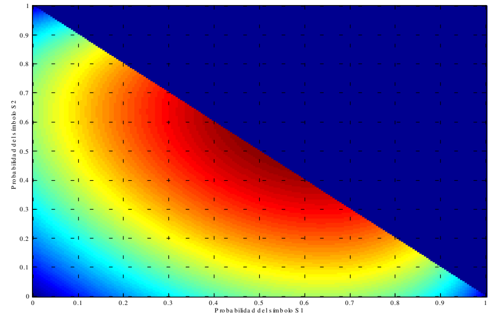
  La entropía es una **función cóncava**.

  Si A y B son dos distribuciones de probabilidad sobre el mismo alfabeto fuente, y m y n son dos números reales positivos tales que m + n = 1, se cumple que $H(mA+nB) \geq mH(A)+nH(B)$.

- Ejemplos
  - Dos símbolos:



Tres símbolos:



Información y sus Fuentes: Modelos de F.I. (4/10)

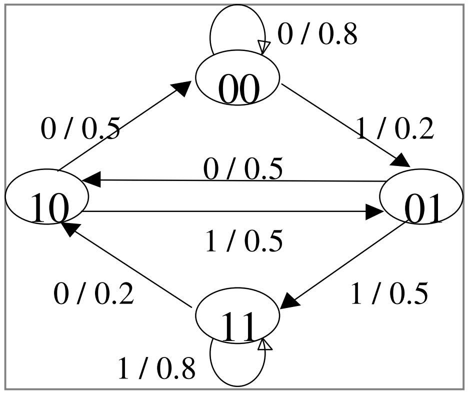
- **Extensiones de una F.I. de Memoria Nula**
  - Aveces resulta útil pensar fuentes que no emiten símbolos aislados, sino paquetes o n-tuplas de símbolos, permitiéndose así modelar la actuación conjunta y simultánea sobre más de un símbolo.
- Sea S una f.i. de memoria nula de alfabeto $\{s_i\}$, con probabilidades $\{p(s_i)\}$. Se llama **extensión de orden n de la fuente S**, (**S^n**) a una fuente de memoria nula de q^n símbolos $\{\sigma_1, \sigma_2, ..., \sigma_{qn}\}$. Donde el símbolo σ_i se corresponde con una secuencia determinada de n símbolos de la fuente S. La probabilidad de σ_i, $P(\sigma_i)$, es la probabilidad de la secuencia correspondiente, es decir, si σ_i representa la secuencia: $(s_{i1}, s_{i2}, ..., s_{in})$ con s_{ij} S, entonces: $P(\sigma_i)=P_{i1}P_{i2}...P_{in}$, ya que la aparición de cada símbolo es estadísticamente independiente de la del resto.
  - La entropía de la extensión de orden n de una f.i. de memoria nula es n veces la de la fuente original: $\mathbf{H(S^n) = n\,H(S)}$

Información y sus Fuentes: Modelos de F.I. (5/10)

- **Fuentes de Información de Markov**
  - La F.I. de memoria nula no es capaz de reflejar las propiedades y estructuras que se pueden encontrar en el lenguaje humano
    - Evidentemente tampoco las correspondientes extensiones que se puedan realizar partiendo de ellas reflejarán ese comportamiento.
  - En el mundo real existen F.I. en las que la probabilidad de aparición de un símbolo es función de la secuencia (finita) formada por los m últimos símbolos emitidos. Ahora se podría decir que la F.I. posee **memoria**. De esta manera surge el concepto de F.I. de Markov.
- Una **F.I. de Markov** vendrá definida por:
  - Su alfabeto: $\mathbf{S=\{s_1,s_2,...,s_q\}}$
  - El conjunto de probabilidades condicionales: $\mathbf{P(s_i / s_{j1},s_{j2},...,s_{jm})}$ con i=1,2,...,q jp=1,2,...,q Donde s_i será el símbolo a generar, y $s_{j1},s_{j2},...,s_{jm}$ es la secuencia de los últimos m símbolos generados, siendo s_{jm} el último de ellos, es decir, que s_i iría detrás de s_{jm}.

Información y sus Fuentes: Modelos de F.I. (6/10)

- **Concepto de estado en una F.I. de Markov**
  - Cada m-tupla formada por los m últimos símbolos generados por la fuente da lugar a un conjunto distinto de probabilidades de aparición de nuevos símbolos - $\mathbf{P(s_i/s_{j1},s_{j2},...,s_{jm})=P(s_i/estado)}$
- Representación gráfica de una fuente de Markov:
  - Los estados son los círculos.
  - Las transiciones debidas a la emisión de un símbolo son los arcos orientados.
  - Las probabilidades de cada transición son las etiquetas de los arcos.
  - Ejemplo de la figura:
    - Dos símbolos: {0,1}
    - Cuatro estados: {00, 01, 10, 11} ("recuerda los dos últimos símbolos emitidos")



Información y sus Fuentes: Modelos de F.I. (7/10)

- Se puede calcular la entropía para una F.I. de Markov:
  - Para cada estado

$$\boxed{\mathrm{H}(S / estado_j) = \sum_{i=1}^{q} p(s_i / estado_j) \log\left(\frac{1}{p(s_i / estado_j)}\right)}$$

Para la fuente completa.

$$\boxed{\mathrm{H}(S) = \sum_{j=1}^{q^m} p(estado_j)\,\mathrm{H}(S / estado_j)}$$

- Se puede realizar la extensión de una F.I. de Markov del mismo modo que se hizo en la de memoria nula.
- Fuente de Información ergódica:
  - (Simplificado) Una F.I. ergódica es aquella que observada durante un tiempo suficientemente largo emite con probabilidad 1 una secuencia "típica" de símbolos
- Fuente afín.

Información y sus Fuentes: Modelos de F.I. (8/10)

- Problema Propuesto:
  - Un teletipo escribe indefinidamente sobre la tira de papel números binarios de tres dígitos binarios separados por un carácter espacio. Ejemplo de salida será: "... 001 111 101 000 ...". La probabilidad de que el dígito binario sea 0 es 0.5, y la de que sea 1 es 0.5. Construir un modelo de fuente de información que reproduzca lo más fielmente posible el comportamiento del teletipo.

Información y sus Fuentes: Modelos de F.I. (9/10)

- Problema Propuesto:
  - Supóngase el conjunto de las posibles ecuaciones algebraicas que se pueden escribir con la variable X y los operadores suma (+), resta (-), multiplicación (*), división (/) e igual (=).
    Un "mecanismo generador de ecuaciones" proporciona ecuaciones algebáicamente correctas, escritas con los símbolos descritos antes (todos operadores son equiprobables entre sí), usando como carácter separador el punto y coma (;). Ejemplo de una posible secuencia de salida es:

    ... ; X*X+X/X=X+X+X/X+X*X;X+X=X/X;...

    Se pide: construir un modelo de F.I. lo más preciso posible para este "mecanismo generador de ecuaciones", en el que los símbolos aparezcan uno en cada instante.

Información y sus Fuentes: Modelos de F.I. (10/10)

- **Estructura del lenguaje**

Códigos - Introducción y Propiedades (1/6)

- **Índice**
  - Necesidad de la codificación
  - Definiciones
  - Síntesis de códigos instantáneos
  - Inecuaciones de Kraft y de McMillan
- **Necesidad de la codificación**
  - Las computadoras modernas sólo trabajan con dos símbolos que se denominan de forma arbitraria "0" y "1". Sin embargo las informaciones que tratan son posiblemente de naturaleza muy diferente. Se impone una etapa previa de **traducción, la codificación**.
  - Aveces la traducción (codificación) es reversible, cuando es posible recomponer sin ninguna pérdida la información original. Otras veces no es reversible, no pudiéndose recomponer la información que fue codificada, obteniéndose ligeras diferencias denominadas **distorsión**.

Códigos - Introducción y Propiedades (2/6)

- Definición de **Código:** Sean $S=\{s_1,...,s_q\}$ y $X=\{x_1,...x_p\}$ dos alfabetos. Se define un código como la *correspondencia* de *todas* las secuencias posibles de símbolos de S a secuencias de símbolos de X.
  - S se le llama *alfabeto fuente* y a X *alfabeto código*.
  - El número de símbolos de S y X puede ser diferente.
  - Es una definición demasiado general para poder ser útil

Ejemplo: $S=\{s_1,...,s_q\}$ y $X=\{x_1,...x_p\}$

s_1	-	x_3
s_1s_4	-	x_3x_1
$s_6s_2s_4s_8$	-	$x_5x_3x_1$
$s_5s_5s_1...s_5$	-	$x_8x_1x_5x_6x_1x_{11}$
. . .		

Códigos - Introducción y Propiedades (3/6)

- Definición de **Código Bloque**: Código que asocia cada uno de los símbolos del alfabeto fuente con una secuencia fija de símbolos del alfabeto código. Estas secuencias fijas se denominan **palabras código**.

Ejemplo: $S=\{s_1,s_2, s_3, s_4\}$ y $X=\{x_1,x_2,x_3\}$

s_i	Palabra código X_i
s_1	$X_1=x_3$
s_2	$X_2=x_3x_1$
s_3	$X_3=x_1x_2x_1$
s_4	$X_4=x_3x_1$

Problema: La secuencia de símbolos del alfabeto código $x_3x_1x_1x_2x_3$ puede haber sido generada al codificar la secuencia de símbolos s_2s_3 ó s_4s_3. Este código en particular no es útil.

- Definición: Un código bloque en el que todas sus palabras código son distintas se denomina **código no singular**.

Códigos - Introducción y Propiedades (3/6)

Ejemplo: $S=\{s_1,s_2, s_3, s_4\}$ y $X=\{x_1,x_2,x_3\}$

s_i	Palabra código X_i
s_1	$X_1=x_3$
s_2	$X_2=x_3x_3$
s_3	$X_3=x_1x_2x_1$
s_4	$X_4=x_3x_1$

Este nuevo código es no singular, y sin embargo, secuencias como la $x_1x_2x_1x_3x_3$ puede haber sido generada por $s_3s_1s_1$ ó s_3s_2.

- Definición **extensión de orden n de un código bloque**: es un código que hace corresponder a cada n-tupla de símbolos del alfabeto fuente la n-tupla de palabras código que codifican cada uno de los símbolos originales $s_{i1}s_{i2}...s_{in} \rightarrow X_{i1}X_{i2}...X_{in}$
  - La extensión de orden n de un código bloque, también es código bloque.

Códigos - Introducción y Propiedades (4/6)

- Definición: Un código se denomina **unívocamente decodificable** si y sólo si su extensión de orden n es no singular para cualquier n finito.
  - Implica la capacidad de determinar cuando una palabra inmersa en una secuencia de símbolos del alfabeto código llega a su final.
  - Un código bloque no singular en el que todas las palabras de código tienen la misma longitud es un código unívocamente decodificable.
  - Los *códigos coma*: un carácter especial, llamado coma, señala el final de cada palabra de código.

Ejemplo: $S=\{s_1,s_2, s_3, s_4\}$ y $X=\{0,1\}$

s_i	Código A	Código B	Código C
s_1	00	0	0
s_2	01	01	10
s_3	10	011	110
s_4	11	0111	1110

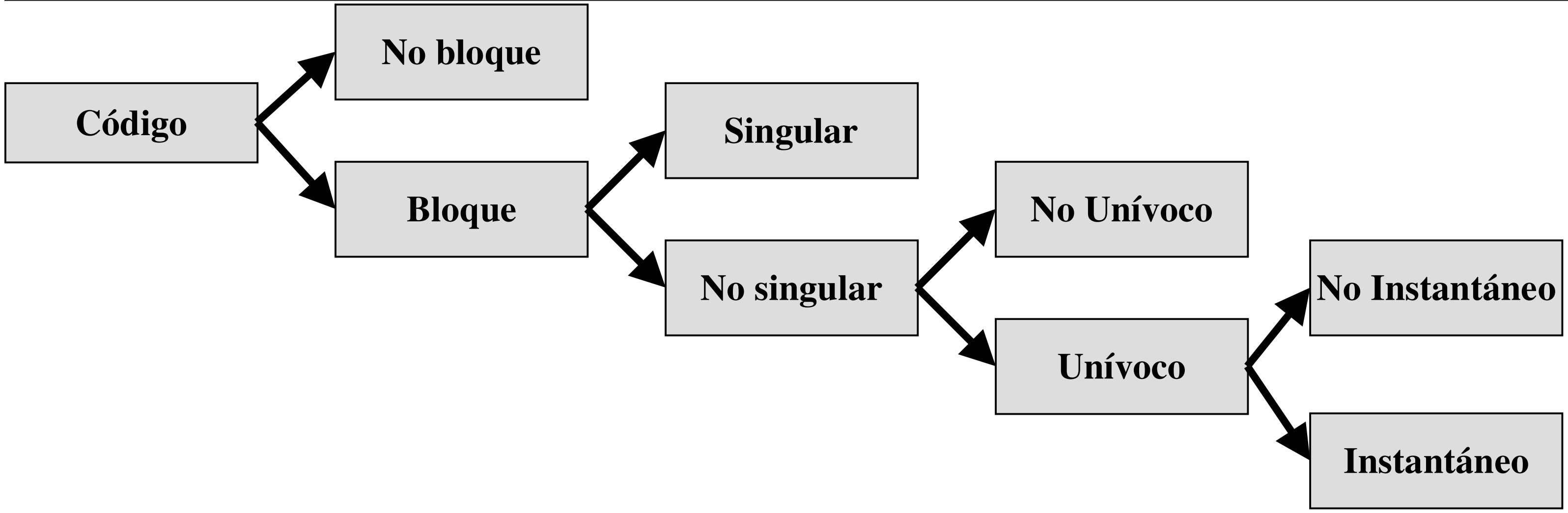
Códigos - Introducción y Propiedades (5/6)

- Definición: Un código unívocamente decodificable se denomina **instantáneo** cuando es posible decodificar las palabras de una secuencia sin precisar el conocimiento de los símbolos que las suceden.
- Definición: Sea $X_i = X_{i1} X_{i2} ... X_{im}$ una palabra de un código. Se denomina **prefijo** de esta palabra a la secuencia de símbolos $X_{i1} X_{i2} ... X_{ij}$ donde $j \leq m$.

- **Síntesis de códigos instantáneos**

  Regla: la condición necesaria y suficiente para que un código sea instantáneo es que ninguna palabra del código coincida con el prefijo de otra.
  - La regla para construir un código instantáneo es simplemente evitar la existencia de palabras que sean prefijos de otras palabras.

Códigos - Introducción y Propiedades (6/6)



- **Inecuación de Kraft**: la condición *necesaria y suficiente* para la existencia de un código instantáneo de longitudes de palabra $l_1, l_2, \ldots l_q$ es que:

$$\boxed{\sum_{i=1}^{q} r^{-l_i} \leq 1}$$

donde q es el cardinal del alfabeto fuente y r el del alfabeto código.

- **Inecuación de McMIllan**. La misma inecuación es condición *suficiente (no necesaria)* para poder construir un código unívoco.

Codificación de las F.I. (1/8)

- Índice
  - Introducción
  - Longitud media de un código
  - Definición de código Compacto
  - Primer teorema de Shannon
  - Codificación de fuentes especiales
  - Códigos de Huffman
  - Rendimiento y Redundancia de un código

Codificación de las F.I. (2/8)

- Introducción
  - Problema: establecer un criterio para poder seleccionar de entre la infinidad de posibilidades aquel código que sea “mejor” u óptimo en algún sentido para una determinada situación.
  - El concepto de óptimo puede ser muy variado e incluso subjetivo:
    - El más “cómodo”.
    - El más fiable (frente a errores).
    - El más seguro (frente a los accesos de usuarios no autorizados).
    - El menos caro en almacenamiento o en transmisión ...
  - Se suele contemplar simultáneamente más de uno de estos aspectos:
    - fiabilidad máxima y coste de transmisión mínimo,
    - seguridad máxima y coste de almacenamiento mínimo, ...
  - En principio se utilizará sólo el criterio de “cuanto más breve mejor”: mayor ahorro en el almacenamiento y en la transmisión.

Codificación de las F.I. (3/8)

- Definición **Longitud media de un código**:

$$\boxed{L = \sum_{i=1}^{q} \mathrm{P}(\mathrm{s}_{\mathrm{i}}) l_i}$$

l_i es la longitud (número de símbolos) de la palabra X_i asociada por el código al símbolo s_i del alfabeto fuente, y $P(s_i)$ es la probabilidad de aparición del símbolo s_i.

  – Con los s_i y los $P(s_i)$ queda definida una fuente de información S.

- Definición: Sea un código unívoco que asocia los símbolos de una fuente S con palabras formadas por símbolos de un alfabeto r-ario. Este código será **compacto** (respecto a S) si su longitud media es igual o menor que la longitud media de todos los códigos unívocos que se pueden aplicar a la misma fuente y al mismo alfabeto.

Codificación de las F.I. (4/8)

$$\boxed{\mathrm{H_r}(S) \leq L}$$

- Esta desigualdad la cumplen todos los códigos r-arios instantáneos que se puedan construir sobre la fuente S
  - La entropía está calculada usando logaritmos en base r.
- **Primer teorema de Shannon** (de la codificación sin ruido). Sea l_n la longitud media de un código instantáneo r-ario que codifica la extensión de orden n de la fuente S. El número medio de símbolos r-arios correspondientes a un símbolo de la fuente S puede hacerse tan pequeño como se quiera, pero no inferior a la entropía de la fuente medida en unidades r-arias.

$$\boxed{\lim_{n\to\infty} \frac{l_n}{n} = \mathrm{H_r}(S)}$$

Codificación de las F.I. (5/8)

- Codificación de **fuentes especiales**
  - Si para una F.I. y un código instantáneo se cumple que

$$p(s_i) = r^{-l_i} \qquad \text{ó} \qquad l_i = -\log_r p(s_i) \qquad / \, l_i \in \{1,2,\ldots\} \qquad \forall i = 1,2,\ldots q$$

  entonces, la longitud media del código instantáneo es la mínima posible, es decir, $H_r(S)=L$.

- Códigos de Huffman (binarios)
  - Son una clase de códigos compactos.
  - Sea S una F.I. Supóngase que se han ordenado (por comodidad) los símbolos de forma que las probabilidades son decrecientes:

$$p(s_1) \geq p(s_2) \geq \cdots \geq p(s_{q-1}) \geq p(s_q)$$

Codificación de las F.I. (6/8)

- Códigos de Huffman (cont.)
  - Se denomina *fuente reducida* a la que se obtiene después de combinar los dos símbolos menos probables en uno nuevo, cuya probabilidad será la suma de probabilidades.
  - A una fuente de q símbolos se la puede aplicar el procedimiento anterior q-2 veces, obteniéndose q-1 fuentes distintas.
    - ¡La última reducción no se puede realizar puesto que el resultado no sería una fuente de información!

Símbolo	$p(s_i)$
s_1	0.6
s_2	0.2
s_3	0.1
s_4	0.1

$p(s_i)$
0.6
0.2
0.2

$p(s_i)$
0.6
0.4

Codificación de las F.I. (7/8)

- Códigos de Huffman (cont.)
  - Comenzando por la última fuente reducida se construyen códigos compactos para cada una de ellas.
  - El paso del código compacto de una fuente reducida a la anterior
    - Copiar las palabras de código al símbolo de procedencia.
    - Si el símbolo procede de la fusión de dos, la palabra se copia a los dos que lo originaron, y para diferenciarlas se las añade a la derecha el símbolo 0 a una, y 1 a la otra (de forma arbitraria)

Símbolo	$p(s_i)$	Palabra
s_1	0.6	0
s_2	0.2	11
s_3	0.1	101
s_4	0.1	100

$p(s_i)$	Palabra
0.6	0
0.2	11
0.2	10

$p(s_i)$	Palabra
0.6	0
0.4	1

Codificación de las F.I. (8/8)

- Rendimiento y redundancia de un código
  - Se define rendimiento de un código instantáneo como

$$\boxed{\eta = \frac{H_r(S)}{L}}$$

  - Se define redundancia de un código instantáneo como

$$\boxed{\text{Redundancia} = 1 - \eta = \frac{L - H_r(S)}{L}}$$

  - Puede acercarse el rendimiento a 1 tanto como se quiera con tal de codificar la extensión de orden n (n lo suficientemente grande) en vez de la fuente sin extender (teorema de Shannon).
    - El precio que se paga es un mecanismo de codificación / decodificación más complejo.

Canales para la Transmisión de la Inf.(1/20)

- Índice
  - Introducción
  - Canales de información
  - Relaciones entre las probabilidades de un canal
  - Entropías a priori y a posteriori
  - Información Mutua
  - Algunos canales especiales
  - Canales en serie

Canales para la Transmisión de la Inf.(2/20)

- Introducción
  - Al igual que se ha modelado el proceso de generación de información, ahora se va a modelar la transmisión/procesamiento de la información.
  - Se ha de poner de manifiesto en el modelo varios aspectos
    - la posibilidad de tener símbolos de distinta naturaleza en el centro emisor y en el centro receptor.
    - la posibilidad de aparición de señales espúreas (incontrolables y aleatorias) que modifiquen el valor del símbolo transmitido, produciéndose **errores**.
  - Si bien anteriormente se codificaba para aumentar la eficiencia (códigos compactos), ahora al existir una probabilidad no nula de aparición de errores, habrá que pensar en codificar intentando minimizar el impacto de esos errores.
  - En este capítulo se verán herramientas matemáticas para valorar la bondad de las transmisiones de un canal discreto y sin memoria.

Canales para la Transmisión de la Inf.(3/20)

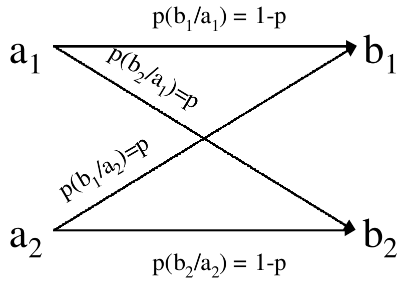
- Características del estudio a realizar
  - Los espacios de entrada (emisor) y de salida (receptor) son *discretos*.
  - La transformación de un símbolo de entrada en uno de salida no depende de las transformaciones anteriores.
  - Las transformaciones no dependen de la elección del origen de tiempos.
- Definición: un **canal de información** viene determinado por
  - un alfabeto de entrada $A=\{a_1,a_2,...a_r\}$,
  - un alfabeto de salida $B=\{b_1,b_2,...b_s\}$, y
  - un conjunto de probabilidades condicionadas $p(b_j/a_i)$=probabilidad de observar a la salida b_j cuando a la entrada se envía a_i.

Canales para la Transmisión de la Inf.(4/20)

- Representación
  - Basta con especificar la matriz de las probabilidades. condicionadas.
    - Cada fila de la matriz está asociada a un símbolo de entrada
    - Cada columna está asociada con un símbolo de salida
- Ejemplo: El Canal Binario Simétrico (BSC)
  - $A=\{a_1,a_2\}$, $B=\{b_1,b_2\}$, $p(b_1/a_1)$, $p(b_2/a_1)$, $p(b_1/a_2)$, $p(b_2/a_2)$.
  - Por ser simétrico:
    $p(b_1/a_1)=p(b_2/a_2) = 1\text{-}p$
    $p(b_1/a_2)=p(b_2/a_1) = p$
    - p es la probabilidad de error y 1-p es la de no error

Salida

$$\begin{array}{cc} \text{Entrada} & \begin{pmatrix} p(b_1/a_1) & p(b_2/a_1) & \cdots & p(b_s/a_1) \\ p(b_1/a_2) & p(b_2/a_2) & \cdots & p(b_s/a_2) \\ \cdots & \cdots & \cdots & \cdots \\ p(b_1/a_r) & p(b_2/a_r) & \cdots & p(b_s/a_r) \end{pmatrix} \end{array}$$



Canales para la Transmisión de la Inf.(5/20)

- Extensión de orden n de un canal
  - En vez de enviar símbolos aislados por el canal, se envían n-tuplas de símbolos de A, y a la salida se obtienen n-tuplas de símbolos de B.
    - El alfabeto de entrada tendrá r^n n-tuplas de la forma $\alpha_i=a_{i1}a_{i2}...a_{in}$
    - El alfabeto de salida tendrá s^n n-tuplas de la forma $\beta j=b_{j1}b_{j2}...b_{jn}$
    - Las probabilidades serán $\Pi_{ij}=p(\beta j/\alpha i)=$ $=p(b_{j1}/a_{i1})p(b_{j2}/a_{i2})...p(b_{jn}/a_{in})$
  - Ejemplo: extensión de orden 2 del BSC (figura)

Salida

Entrada

$$
\begin{array}{c}
 \\ a_1a_1 \\ a_1a_2 \\ a_2a_1 \\ a_2a_2
\end{array}
\begin{array}{c}
\begin{array}{cccc} b_1b_1 & b_1b_2 & b_2b_1 & b_2b_2 \end{array} \\
\begin{pmatrix}
(1-p)^2 & (1-p)p & p(1-p) & p^2 \\
(1-p)p & (1-p)^2 & p^2 & p(1-p) \\
p(1-p) & p^2 & (1-p)^2 & (1-p)p \\
p^2 & p(1-p) & (1-p)p & (1-p)^2
\end{pmatrix}
\end{array}
$$

Canales para la Transmisión de la Inf.(6/20)

- Relaciones de las probabilidades de un canal
  - Los símbolos de entrada al canal provienen de una F.I. con alfabeto $\{a_i\}$ y distribución de probabilidades $\{p(a_i)\}$
  - Los símbolos a la salida del canal aparecerán con las probabilidades $\{p(b_i)\}$
  - Dado que cuando entra un símbolo al canal siempre sale algún símbolo, se debe cumplir:

$$\boxed{\sum_{j=1}^{s} p(b_j / a_i) = 1 \qquad \forall i = 1,2,\cdots\ r}$$

    - La suma de una fila de la matriz debe valer siempre 1.
  - Se puede calcular las probabilidades de los símbolos a la salida del canal:

$$\boxed{p(b_j) = \sum_{i=1}^{r} p(a_i)\, p(b_j / a_i) \qquad \forall j = 1,2,\cdots\ s}$$

    - Se ha aplicado el teorema de Bayes

Canales para la Transmisión de la Inf.(7/20)

- Relaciones de las probabilidades de un canal (cont.)
  - Una vez calculadas las $\{p(b_j)\}$, se pueden calcular las $p(a_i/b_j)$:

$$p(a_i / b_j) = \frac{p(b_j / a_i) p(a_i)}{p(b_j)} = \frac{p(b_j / a_i) p(a_i)}{\sum_{k=1}^{r} p(b_j / a_k) p(a_k)} \qquad \forall i = 1,2,\cdots\ r \qquad \forall j = 1,2,\cdots\ s$$

Si a las $p(b_j/a_i)$ se las denomina **probabilidades de canal hacia adelante**, a las $p(a_i/b_j)$ se las denomina **probabilidades del canal hacia atrás**.

  - Se puede calcular la probabilidad del suceso simultáneo:

$$p(a_i, b_j) = p(a_i / b_j) p(b_j) = p(b_j / a_i) p(a_i)$$

Canales para la Transmisión de la Inf.(8/20)

- Entropías a priori y a posteriori
  - **Recordatorio**: ***Entropía de una fuente es la cantidad media de información necesaria para poder identificar un símbolo emitido por la fuente. Medida de la incertidumbre sobre el símbolo que emitirá la fuente.***
  - El hecho de conocer el símbolo que entra en el canal hace que varíe la probabilidad con la que se pueden observar los distintos símbolos a la salida:
    - $p(b_j)$ es la probabilidad de observar b_j sin conocer qué símbolo entró.
    - $p(b_j/a_i)$ es la probabilidad de observar b_j sabiendo que entró a_i.
  - Lo mismo ocurre con la entrada:
    - $p(a_i)$ es la probabilidad de que entre en el canal el símbolo a_i.
    - $p(a_i/b_j)$ es la probabilidad de que haya entrado a_i, sabiendo que en la salida ha aparecido el b_j.
      - Se llama a **$p(a_i)$ probabilidad a priori**
      - Se llama a **$p(a_i/b_j)$ probabilidad a posteriori**.

Canales para la Transmisión de la Inf.(9/20)

- Entropías a priori y a posteriori (cont.)
  - **Entropía a priori**

$$\boxed{\mathrm{H}(A)=\sum_{A} p(a)\log\left(\frac{1}{p(a)}\right)}$$

  - **Entropía a posteriori**

$$\boxed{\mathrm{H}(A/b_j)=\sum_{A} p(a/b_j)\log\left(\frac{1}{p(a/b_j)}\right)}$$

  - **La entropía media a posteriori**

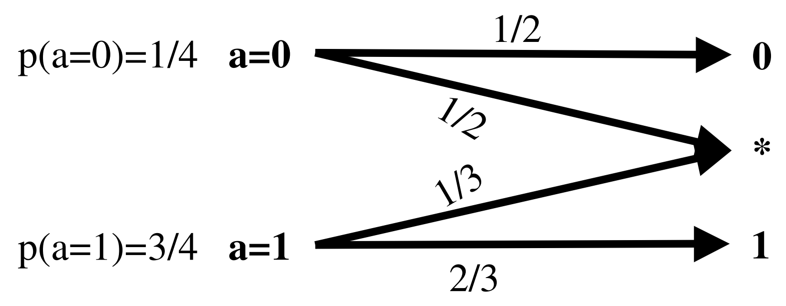
$$\boxed{H(A/B)=\sum_{B} p(b_j)\mathrm{H}(A/b_j)=\sum_{A,B} p(a,b)\log\left(\frac{1}{p(a/b)}\right)}$$

Mide la incertidumbre que queda sobre la entrada del canal después de haber observado un símbolo de salida cualquiera.

Canales para la Transmisión de la Inf.(10/20)

- Entropías a priori y a posteriori (cont.)
  - Otras interpretaciones de H(A/B)
    - H(A/B) también recibe el nombre de **equivocación** de A con respecto a B a través del canal.
    - mide la información que queda en A después de observar B,
    - pérdida de información sobre A causada por el canal.
    - cantidad de información sobre A que no deja pasar el canal.

- Ejemplo



H(A)=0.811, H(B)=1.406

H(A/b=0)=0 H(A/b=*)=0.918

H(A/b=1)=0

H(A/B)=0.344

- H(A/b=*)>H(A)
  - Hay más incertidumbre después de observar la salida.
- H(A/B) ≥ H(A)
  - **En promedio nunca** se pierde información al conocer la salida.

Canales para la Transmisión de la Inf.(11/20)

- Definición: **Información Mutua** de un canal con alfabeto de entrada A y alfabeto de salida B es

$$I(A;B) = H(A) - H(A/B)$$

  Es la cantidad de información sobre A, menos la cantidad de información que todavía hay en A después de observar la salida
  - Es la cantidad de información que se obtiene de A gracias al conocimiento de B.
  - Es la incertidumbre sobre la entrada del canal que se resuelve observando la salida del canal.
  - Es la cantidad de información sobre A que atraviesa el canal.
- De forma análoga

$$I(B;A) = H(B) - H(B/A)$$

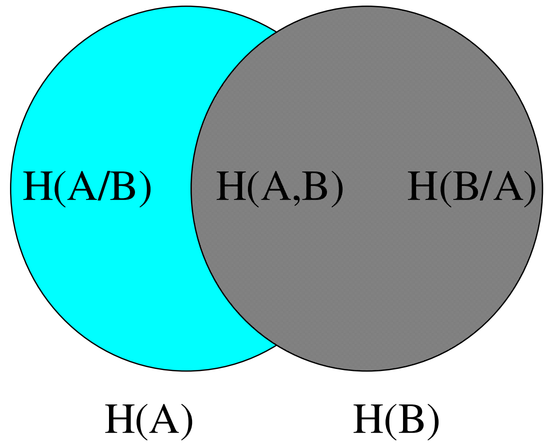
  - medida de la incertidumbre sobre la salida del canal que se resuelve enviando la entrada

Canales para la Transimisión de la Inf.(12/20)

- Propiedades de la Información mutua
  - La información mutua depende de
    - la fuente que genere los símbolos de entrada al canal (sus probabilidades)
    - el propio canal, a través de las probabilidades $p(b_j/a_i)$ del canal.
      - Es decir, la información mutua depende del canal y de cómo se use el canal.
  - La información mutua siempre es positiva
    - Nunca se pierde información (en media) al observar la salida del canal.
  - La condición para que la información mutua sea nula es que los símbolos de entrada y de salida del canal sean estadísticamente independientes: $p(b_j,a_i)= p(b_j)\ p(a_i)$
  - La información mutua es simétrica respecto de A y B:

$$I(A;B)=I(B;A)$$

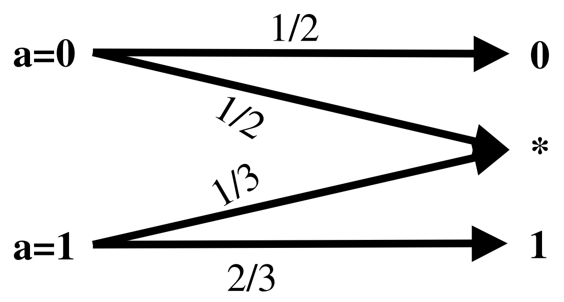
Canales para la Transmisión de la Inf.(13/20)



- Información Mutua (cont.)
  - La información mutua permite obtener un índice que indica lo bien o mal que se está usando un canal (obviamente, lo que cambia es la fuente que genera los símbolos de entrada al canal).
  - Recíprocamente, permite elegir el canal adecuado para la transmisión de los símbolos generados por una fuente fija.

Canales para la Transmisión de la Inf.(14/20)

- Ejemplo 1:



p(a=0)=1/4, p(a=1)=3/4

H(A)=0.811

H(A/b=0)=0

H(A/b=*)=0.918

H(A/b=1)=0

H(A/B)=0.344

I(A;B)=0.467

- Ejemplo 2:

Igual canal que en el ejemplo 1.

p(a=0)=3/4, p(a=1)=1/4

H(A)=0.811

H(A/b=0)=0

H(A/b=*)=0.684

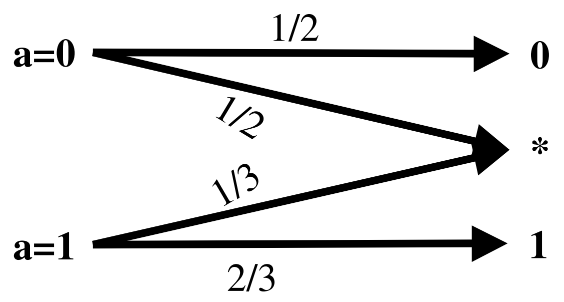
H(A/b=1)=0

H(A/B)=0.313

I(A;B)=0.497

Canales para la Transmisión de la Inf.(15/20)

- Ejemplo 3:



p(a=0)=1/4, p(a=1)=3/4

H(A)=0.811

H(A/b=0)=0

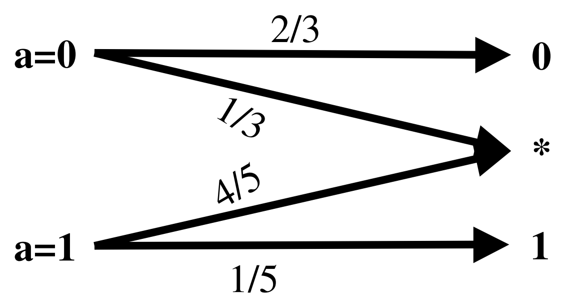
H(A/b=*)=0.918

H(A/b=1)=0

H(A/B)=0.344

I(A;B)=0.467

- Ejemplo 4:



p(a=0)=1/4, p(a=1)=3/4

H(A)=0.811

H(A/b=0)=0

H(A/b=*)=0.534

H(A/b=1)=0

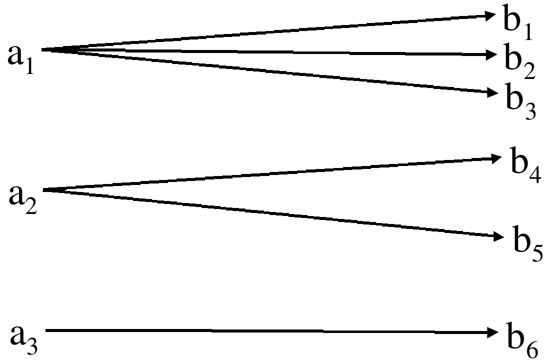
H(A/B)=0.365

I(A;B)=0.445

Canales para la Transmisión de la Inf.(16/20)

- Definición: un canal definido por una matriz con un elemento y sólo uno distinto de cero en cada columna se denomina **canal sin pérdida**.
  - Observada la salida del canal se conoce la entrada con total certeza.
  - La equivocación H(A/B)=0
    - no hay incertidumbre sobre la entrada después de observar la salida.
  - I(A;B)=H(A)
    - Toda la información generada por la fuente se recoge a la salida del canal.

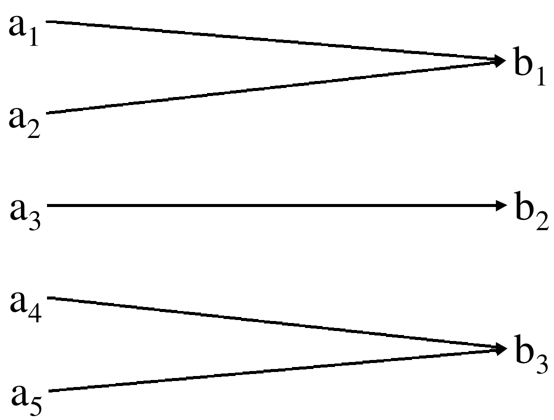
$$\begin{pmatrix} 1/3 & 1/3 & 1/3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$



Canales para la Transmisión de la Inf.(17/20)

- Definición: un canal definido por una matriz con un elemento y sólo uno distinto de cero en cada fila se denomina **canal determinista** (o canal determinante).
  - Una entrada determina perfectamente el símbolo a salir.
  - La equivocación H(B/A)=0
    - no hay incertidumbre sobre la salida después de enviar la entrada.
  - I(A;B)=H(B)

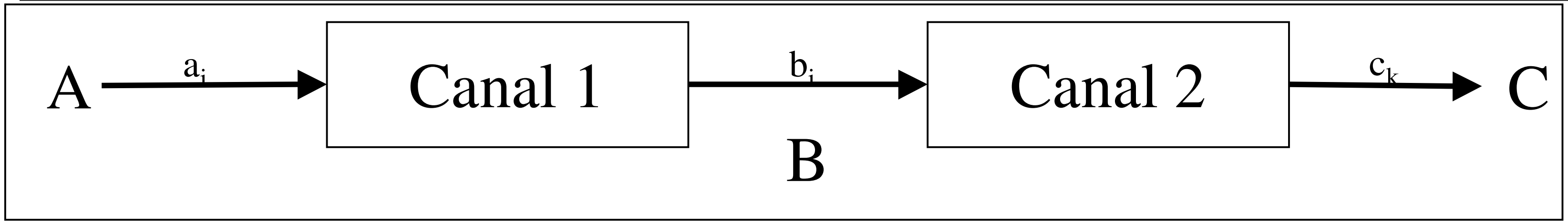
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$



Canales para la Transmisión de la Inf.(18/20)

- Definición: un canal sin pérdida y determinista recibe el nombre de **canal sin ruido**.
- Definición: un canal definido por una matriz en la que las filas son idénticas recibe el nombre de **canal inútil**.
  - Los símbolos de entrada y salida son estadísticamente independientes.
  - Para cualquier distribución de entrada se cumple que $H(A/B)=H(A)$, y por lo tanto $I(A;B)=0$.

Canales para la Transmisión de la Inf.(19/20)



- Canales de Información en Serie
    - Canal 1: $\{A,B,P_{ij}\}$ definido por un alfabeto de entrada A, un alfabeto de salida B y las probabilidades condicionadas P_{ij}
    - Canal 2:$\{B,C,Q_{ij}\}$ definido por un alfabeto de entrada B (el mismo alfabeto que en el canal 1 es de salida), un alfabeto de salida C y las probabilidades condicionadas Q_{ij}
  - Se utilizan los símbolos que aparecen a la salida del canal 1 como símbolos en la entrada del canal 2.
  - Al transmitirse la información por los dos canales en serie, la equivocación aumenta: $H(A/C) \geq H(A/B)$. Y por lo tanto, la información mutua disminuye: $I(A;B) \geq I(A;C)$
    - ***Los canales tienden a perder información***.

Canales para la Transmisión de la Inf. (20/20)

- **Capacidad de un Canal**.
  - Dado que la "bondad" de un canal se mide con la Información mutua, y esta depende del canal en sí y del uso que se dé al canal (la fuente de información conectada a su entrada), ¿cuán bueno puede llegar a ser un canal?
  - Definición: Se denomina **capacidad (C) de un canal** al valor máximo posible de la información mutua (variando las probabilidades que definen la fuente conectada a su entrada)

$$C = \max_{P(a_i)} I(A;B)$$

Cód. Detectores y Correctores de Errores (1/16)

- Índice de contenidos
  - Introducción
  - Primera aproximación
  - Definiciones
  - Códigos detectores de errores
  - Códigos correctores de errores

Cód. Detectores y Correctores de Errores (2/16)

- Introducción
  - Al introducir el concepto y los modelos de canales para la transmisión de la información, se presentó el hecho real de la existencia de errores aleatorios durante la transmisión de la información.
  - Si bien en la actualidad, los modernos canales presentan una probabilidad de error (cambio de 1 por 0 y viceversa) del orden de 10^{-6} (una en un millón) e inferiores, ese cambio accidental se puede llegar a producir.
  - Hay que agregar un mecanismo ajeno al medio de transmisión (canal) que mejore la calidad (fiabilidad) de la transmisión. Este mecanismo se concretará en la creación de **códigos detectores y correctores de errores**.

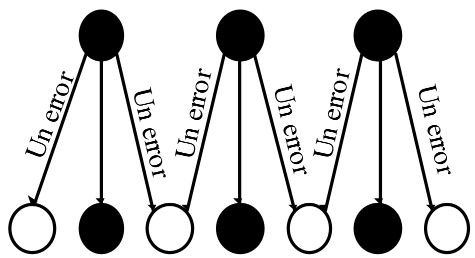
NOTA:Por comodidad se utilizarán a partir de ahora códigos de longitud de palabra constante, y si no se indica lo contrario, se supondrá además códigos binarios.

Cód. Detectores y Correctores de Errores (3/16)

- Primera aproximación: Cada símbolo es enviado un total de N veces seguidas por parte del emisor.
  - El receptor evalúa la secuencia de símbolos recibidos:
    - Si los N símbolos recibidos son iguales **NO HAY ERROR**.
    - Si los N símbolos recibidos no son todos iguales **HAY ERROR**
      - Parece "lógico" que el símbolo más veces repetido debería ser el símbolo enviado.
  - El receptor sabe que los únicos posibles mensajes (correctos o sin errores) están formados por N-tuplas de símbolos todos iguales. Si recibe una N-tupla que no cumple esta condición (que no pertenece al código que esperaba), sabrá que se ha producido algún error.
  - Un código de longitud constante en el que se usen todas las posibles combinaciones de dígitos como palabras de dicho código, no puede servir para detectar la aparición de errores ya que toda palabra válida se transforma en otra palabra válida.
  - ***Una condición necesaria para que un código permita la detección de errores es que no se utilicen todas las posibles combinaciones de símbolos como palabras código.***

Cód. Detectores y Correctores de Errores (4/16)

- ***La condición necesaria y suficiente que se debe cumplir para poder detectar la aparición de un error en un dígito binario es que toda combinación perteneciente al código se transforme (al variar uno cualquiera de sus dígitos) en una combinación que no pertenezca al código.***



Cód Detectores y Correctores de Errores (5/16)

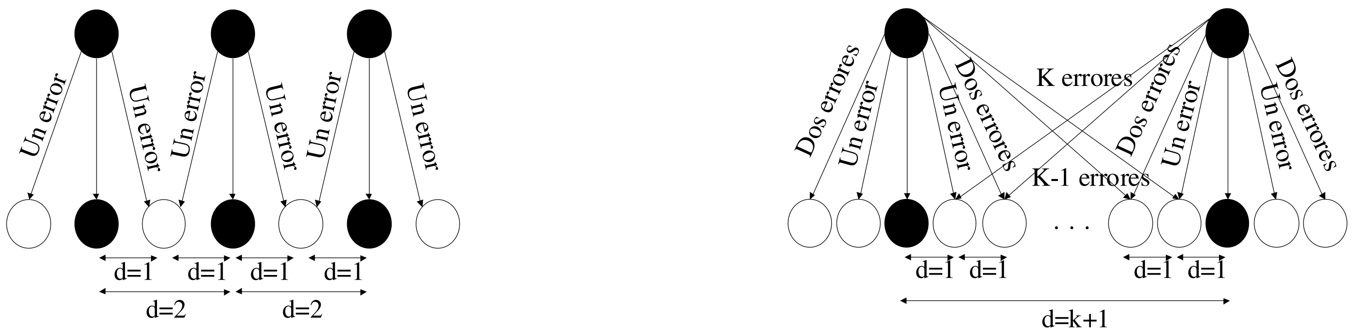
- Definición: **Distancia de Hamming** entre dos combinaciones de n dígitos binarios es el número de dígitos que hay que cambiar para pasar de la una a la otra.
  - El nombre de distancia proviene de que esta operación puede contemplarse como una aplicación d: $B^n \times B^n$, donde B es un alfabeto binario, que verifica las propiedades del concepto matemático de **métrica**:
    - $\forall\ x, y \in B^n\ /\ d(x, y) = 0 \quad x = y$
    - $\forall\ x, y \in B^n\ /\ d(x, y) = d(y, x)$
    - $\forall\ x, y, z \in B^n\ /\ d(x, z) \quad d(x, y) + d(y, z)$ (Desigualdad triangular)
  - Ejemplo:
    - d (100001,111000) = 3
- Definición: **Distancia mínima de un código** (binario) es la distancia de Hamming más pequeña entre dos combinaciones cualesquiera del código.

Cód. Detectores y Correctores de Errores (6/16)

- Sea C un código binario en el que sobre el alfabeto fuente se ha definido una relación de orden estricto.

- Definición: Si una vez ordenadas las palabras de código siguiendo el criterio establecido para los símbolos del alfabeto fuente, siempre se tiene que dos palabras consecutivas tienen distancia 1, se dice que C es un **código continuo**.
- Definición: Si en un código además de ser continuo, la distancia de Hamming entre la primera y la última palabra es uno, el código se llama **cíclico**.

Cód. Detectores y Correctores de Errores (7/16)



- La condición necesaria y suficiente para que un código sea capaz de detectar errores es que su distancia mínima de Hamming sea mayor que 1.
- En forma general: *la condición necesaria y suficiente para que un código permita detectar el error producido por la variación de un número de dígitos igual o menor que k durante la transmisión de la palabra de código, es que su distancia mínima sea al menos k+1.*

Cód. Detectores y Correctores de Errores (8/16)

- Ejemplos de códigos detectores de error:
  - **Códigos de paridad**: se añade a cada palabra del código de partida en una posición predeterminada un nuevo dígito cuyo valor (0 ó 1) es tal que
    - en los códigos de paridad par la nueva palabra resultante tenga un número de 1's par (0 unos es par)
    - en los códigos de paridad impar la nueva palabra resultante tenga un número de 1's impar.
  - **Códigos de peso constante**: el código se define tal que en todas sus palabras haya un número de dígitos a 1 constante
    - **Peso** de una combinación binaria es el número de dígitos que son "1".

Código Original	
S_i	Palabra
A	00000
B	00001
C	10001
D	11100

Código de Pariad (par)		
S_i	Palabra Original	Dígito de Paridad (par)
A	00000	0
B	00001	1
C	10001	0
D	11100	1

Código de Pariad (impar)		
S_i	Palabra Original	Dígito de Paridad (impar)
A	00000	1
B	00001	0
C	10001	1
D	11100	0

Código 2 entre 5	
Dígito Decimal	Palabra de Código
0	01100
1	11000
2	10100
3	10010
4	01010
5	00110
6	10001
7	01001
8	00101
9	00011

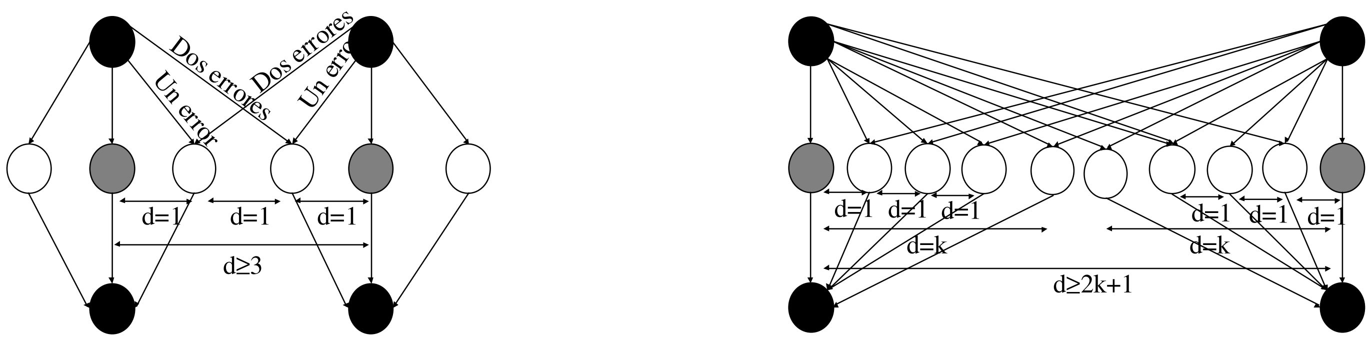
Cód. Detectores y Correctores de Errores (9/16)

- ¿Qué hacer cuando se ha detectado la presencia de errores en una transmisión?
  - Parece razonable que se pida al emisor que repita el mensaje, confiando en que la segunda vez ya no haya errores. Pero, ¿y si no es posible o rentable mantener la comunicación desde el receptor al emisor?
  - El propio código puede incluir mecanismos que además de permitir la detección de la aparición de los errores en la transmisión, determine en qué posición o posiciones se encuentran los errores, y dado que se está tratando con códigos binarios, lo que se recibió como un 1, en realidad era un 0, ó viceversa.
  - Una vez detectada la presencia de un error, el problema es determinar su situación.

Cód. Detectores y Correctores de Errores (10/16)

- Códigos Correctores de Errores
  - Si la probabilidad de que en la transmisión de un dígito binario se produzca un error es P, la probabilidad de que en la transmisión de dos dígitos binarios se produzcan simultáneamente 2 errores es P^2 (supuesto un canal sin memoria), P^3 para tres errores...
  - Si se observa una palabra con errores (no perteneciente al código), se corregirá
    - hacia la palabra de código más parecida (distancia de Hamming más pequeña), o lo que es lo mismo
    - hacia la palabra de código que con más probabilidad se haya enviado (y ya que el hecho de producirse un número bajo de errores es más probable que el hecho de que se hayan producido muchos errores, se corregirá a la más "próxima").

Cód. Detectores y Correctores de Errores (11/16)



- La condición necesaria y suficiente para que un código sea corrector de orden 1 (de un error) es que su distancia mínima sea 3.
  - Si se producen 2 errores en la transmisión, este hecho se detectará, pero se corregirá incorrectamente.
- La condición necesaria y suficiente para que un código sea corrector de k errores es que su distancia mínima sea de 2k +1

Cód. Detectores y Correctores de Errores (12/16)

- Ejemplo de Códigos Correctores. Códigos de Hamming (1)
  - Generación del código
    - Se parte de un código de distancia mínima 1, cuya longitud es n.
    - A este código se le han de añadir p dígitos, llamados **dígitos de control**. El número p es el menor entero positivo que verifica: $2^p \geq n+p+1$.
    - Las posiciones de estos dígitos de control en la nueva palabra de código (de longitud $n+p$) son las potencias de dos: $2^0, 2^1$, ... 2^{p-1}.
    - Los valores de estos nuevos dígitos se determinan al realizar los controles de paridad mostrados en la figura.

Posición	n+p	n+p-1	...	2^{p-1}	...	9	2^3	7	6	5	2^2	3	2^1	2^0
Dígito	D_n	D_{n-1}	...	P_{p-1}	...	D_5	P_3	D_4	D_3	D_2	P_2	D_1	P_1	P_0

D_i=Dígitos del código original

P_j=Dígitos de control

Núm.	C_{p-1}	C_{p-2}	...	C_2	C_1	C_0
0	0	0		0	0	0
1	0	0		0	0	1
2	0	0		0	1	0
3	0	0		0	1	1
4	0	0		1	0	0
5	0	0		1	0	1
6	0	0		1	1	0
7	0	0		1	1	1
...			...			
$2^{p-1}-3$	1	1		1	0	1
$2^{p-1}-2$	1	1		1	1	0
$2^{p-1}-1$	1	1		1	1	1

Control1	1	3	5	7	...
Control2	2	3	6	7	...
Control3	4	5	6	7	...
Control4	8	9	10	11	...
...					

Cód. Detectores y Correctores de Errores (13/16)

- Ejemplo de Códigos Correctores. Códigos de Hamming (2)
  - Verificación de la palabra recibida.
    - Se verifican los controles de paridad.
      - Aquellos que sean correctos indican que en las correspondientes posiciones *no hay error*.
      - Aquellos que son incorrectos indican que entre las posiciones controladas hay una (y sólo una, por hipótesis) errónea.
    - Por eliminación, se localiza la posición errónea y se corrige.
      - *El método rápido*: se asocia a cada control correcto un "0", y a los incorrectos un "1". El número binario resultante de ordenar los controles de paridad indica la posición del dígito erróneo.
  - Se puede demostrar que los códigos de Hamming así construidos son de distancia mínima 3, con lo que permite la detección de la ocurrencia de dos errores, y la corrección de uno solo
    - Si se producen dos errores, se detectará esta situación, pero la corrección no será la adecuada, produciéndose probablemente un resultado incorrecto.

Cód. Detectores y Correctores de Errores (14/16)

- ***Ejemplo: Construir a partir de la palabra de código `0011` una palabra del código de Hamming (paridad par) capaz de detectar y corregir un dígito erróneo en la transmisión.***
- Longitud $n=4$, $2^p \geq 4+p+1$. El p mínimo es 3. Será necesario añadir tres dígitos de control en las posiciones 2^0, 2^1 y 2^2. Estos dígitos de control tomarán valores según criterio de paridad par de las posiciones indicadas en la tabla.

Número	C_2	C_1	C_0
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

Palabra Original

Posición	7	6	5	4	3	2	1
Dígito	0	0	1	P_2	1	P_1	P_0

Control 1 en las posiciones: 1, 3, 5 y 7 = $\{P_0, 1, 1, 0\}$ Luego $P_0 = 0$

Control 2 en las posiciones: 2, 3, 6 y 7 = $\{P_1, 1, 0, 0\}$ Luego $P_1 = 1$

Control 3 en las posiciones: 4, 5, 6 y 7 = $\{P_2, 1, 0, 0\}$ Luego $P_2 = 1$

Se envía

Posición	7	6	5	4	3	2	1
Dígito	0	0	1	1	1	1	0

Cód. Detectores y Correctores de Errores (15/16)

- ***Ejemplo:* *Se ha recibido la palabra* `0010100`*, sabiendo que fue originada por un código de Hamming corrector de un error con criterio de paridad par, determinar cuál fue la palabra transmitida*.**
- Longitud $n+p=7$, $2^p \geq 7+1$. El p mínimo es 3. A la palabra original de 4 dígitos se la han añadido tres dígitos de control en las posiciones 2^0, 2^1 y 2^2. Los controles de paridad que hay que realizar son los indicados en la tabla.

Número	C_2	C_1	C_0
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

Palabra Recibida

Posición	7	6	5	4	3	2	1
Dígito	0	0	1	0	1	0	0

Control 1 en las posiciones: 1 3 5 7 = {0, 1, 1, 0} Par - Correcto 0

Control 2 en las posiciones: 2 3 6 7 = {0, 1, 0, 0} Impar - ERROR 1

Control 3 en las posiciones: 4 5 6 7 = {0, 1, 0, 0} Impar - ERROR 1

1 1 0 Error en 6

Se envió

Posición	7	6	5	4	3	2	1
Dígito	0	1	1	0	1	0	0

Cód. Detectores y Correctores de Errores (16/16)

- Conclusiones:
  - El hecho de considerar la posibilidad de aparición de errores en la transmisión de la información obliga a construir códigos más fiables.
  - Estos códigos que permiten la detección y corrección de errores se basan en **añadir redundancias** (de alguna manera repiten la información, o parte de ella), lo que hace que la longitud media de los códigos así resultantes sea mayor que la mínima necesaria para codificar los símbolos del alfabeto fuente.
  - Una cuestión a tener en cuenta es que los errores en los canales de transmisión reales no suelen aparecer aislados, sino todo lo contrario, aparecen agrupados, lo que obliga a un tratamiento especial.