Tema 3: CONTROL DE ERRORES

Ingeniería de Protocolos y Servicios

3.1. Introducción

Los errores de transmisión son de algunos órdenes de magnitud superiores a los errores *hardware* de los ordenadores:

- P(error) circuitos internos < 10^{-15}
- P(error) fibra óptica < 10^{-9}
- P(error) cable coaxial < 10^{-6}
- P(error) línea telefónica < 10^{-4}

DTIC
Área Ingeniería Telemática
francesc.burrull@upct.es

Tema 3: CONTROL DE ERRORES

Ingeniería de Protocolos y Servicios

3.1. Introducción

Origen principal de los errores:

- Distorsión Lineal: Ancho de banda del canal
- Distorsión no Lineal: Eco, diafonía, ruido blanco, ruido impulsivo.

Se puede solucionar de manera parcial con aislamiento de cables, filtros, canceladores de eco,…

El resto de errores son tarea del protocolo de comunicaciones

DTIC
Área Ingeniería Telemática
francesc.burrull@upct.es

Tema 3: CONTROL DE ERRORES

Ingeniería de Protocolos y Servicios

3.1. Introducción

Para expresar los errores se usa:

- Media a largo plazo de la probabilidad de error
- Porcentaje de tiempo en que la probabilidad de error media no excede un umbral.
- Porcentaje de segundos libres de error

Los dos últimos indican la calidad global de una línea

DTIC
Área Ingeniería Telemática
francesc.burrull@upct.es

Tema 3: CONTROL DE ERRORES

Ingeniería de Protocolos y Servicios

3.1. Introducción

No existe ningún método que detecte todos los errores posibles: Se pretende reducir los errores al nivel deseado.

Un esquema de control de errores debe adaptarse a las características del canal donde va a ser usado:

- Si los errores son pocos y duración 1 bit, un esquema de paridad es mejor que métodos más complejos
- Si los errores de transmisión son ya menores que los del equipo, un esquema de control de errores solo empeora la situación.

DTIC
Área Ingeniería Telemática
francesc.burrull@upct.es

3.2. Modelos de Error

Definiciones para el canal:

• Discreto: Reconoce un número finito de valores (0 y 1)

• Sin Memoria: La probabilidad de un error es independiente de los errores anteriores

• Simétrico: La probabilidad de error es la misma para las distintas señales.

DTIC
Área Ingeniería Telemática
francesc.burrull@upct.es

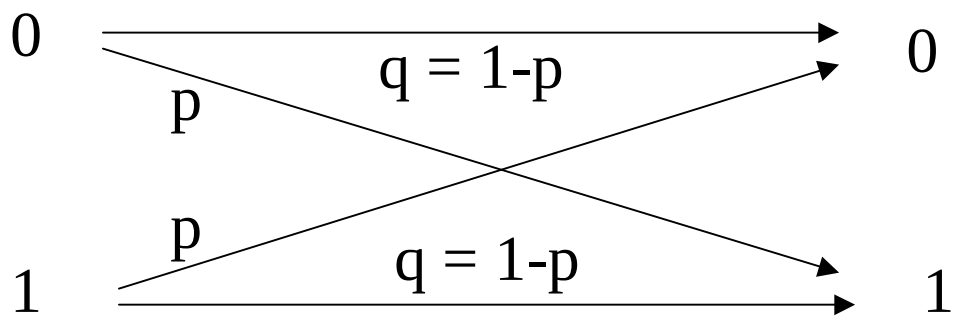
3.2. Modelos de Error

CANAL DISCRETO SIN MEMORIA SIMÉTRICO

No contempla las ráfagas de errores.

Probabilidad de error a largo plazo = p:

- Prob. 1 o más errores en mensaje de n bits = $1-(1-p)^n$



3.2. Modelos de Error

CANAL DISCRETO SIMÉTRICO

Si n bits fueron erróneos es probable que el siguiente sea erróneo (memoria).

Se conoce como Intervalo Libre de Errores (EFI, *Error Free Interval*) a una serie de transmisiones seguidas sin error.

Con la prob. de error media a largo plazo = b, en función de la distribución de errores se tiene:

3.2. Modelos de Error

CANAL DISCRETO SIMÉTRICO

Lineal:

•Prob(EFI>=n) = $(1-b)^n$, con n >= 0

Poisson:

• Prob(EFI>=n) = $e^{-b(n-1)}$, con n >= 1

Benoit Mandelbrot

• Prob(EFI>=n) = $(n^{(1-a)} -(n-1)^{(1-a)})e^{-b(n-1)}$,

con 0 <= a < 1 y n >= 1

DTIC

Área Ingeniería Telemática

francesc.burrull@upct.es

3.3. Tipos de Errores de Transmisión

Los errores de transmisión de datos más importantes son:

- Inserción
- Eliminación
- Duplicación
- Distorsión
- Reordenación

Se dan por falta de sincronización, mal control de flujo,...

3.4. Redundancia

Cualquier método de detección de errores se basa en el análisis de la redundancia en mensajes.

Además de detectar, el receptor puede corregir errores, habiendo dos formas de hacerlo:

- *Forward error control* (Corrección)

  Utilizan códigos correctores. Se corrige en el receptor
- *Feedback error control* (Detección)

  Utilizan códigos detectores. Al detectar un error se pide retransmisión

3.4. Redundancia

•Tasa de error residual: Si f es la fracción de errores que van a ser detectados, y p la probabilidad de error, la probabilidad de error después de la detección es p(1-f)

•Un esquema de control de errores pretende bajar (imposible eliminar) la prob. de error a cierta cota.

•*Code rate*: d/(d+e) -d bits mensaje, e bits redundancia-

•Hay que elegir el método de control de errores adecuado, en función de p (y los costes de retransmisión).

3.5. Tipos de Códigos

Existen 2 tipos básicos:

- Códigos de bloque: Las palabras código tienen igual longitud. Cada mensaje genera de manera estática una palabra código. Refinando se tienen:
  - Códigos lineales
  - Códigos cíclicos
  - Códigos sistemáticos
- Códigos de convolución: La palabra código depende del mensaje y de códigos anteriores.

3.6. Bit de Paridad

Añadir un bit a cada mensaje obteniendo un numero par/impar de unos.

Si q=1-p es la prob.de transmitir correctamente un bit:

- prob. de transmitir correctamente un mensaje de n bits es $q^{(n+1)}$
- prob. Un solo error en n+1 bits es $(n+1)pq^n$ (binomial)
- prob. error residual: $1- q^{(n+1)} - (n+1)pq^n$
  - ej. n=7 y p= 10^{-4} $\Longrightarrow$ p.e.r. de $2{,}8 \cdot 10^{-7}$

3.7. Corrección de Errores

Un esquema de corrección de errores usará un subconjunto reducido de combinaciones de bits para codificar mensajes, escogiéndolas de manera que para convertir un mensaje válido en otro haya que equivocarse en muchos bits.

La corrección se realiza escogiendo el código válido más "parecido" al código recibido (menos bits de diferencia)

3.7. Corrección de Errores

Ejemplo: Código de repetición. Cada bit se transmite 5 veces.

Mensaje “0” -> Código 00000

Mensaje “1” -> Código 11111

De las 2^5=32 combinaciones de 5 bits se han escogido 2.

Code Rate = d/d+e = 1/1+4 = 0.2

3.7. Corrección de Errores

Suponiendo que se quiere transmitir el mensaje 01000001 (A):

00000 11111 00000 00000 00000 00000 00000 11111

Si en recepción se obtiene:

00000 11110 00011 00111 01111 00000 00000 11111

Corrección (corrige 1 o 2 bits): 01011001 (Y) -FECHíbrido (corrige 1 bit, detecta 2 o 3 bits): 01xx1001

Detección (detecta 1,2,3 o 4 bits): 0xxxx001.

francesc.burrull@upct.es

3.7. Corrección de Errores

El *code rate* de un código corrector suele ser más bajo que el de un código detector. Así, se usarán cuando la comunicación receptor-emisor sea complicada, como:

- Retardo de transmisión muy elevado (ej. sonda espacial)
- Ausencia de canal de retorno (ej. emisora *broadcast*)
- Tasa de error elevada (incluso repeticiones con errores)

3.7. Corrección de Errores

Ejemplo:

Extensión del bit de paridad para corregir errores

LRC (*longitudinal redundancy check*): Redundancia horizontal de 1 bit por mensaje

VRC (*vertical redundancy check*): Redundancia vertical de 8 bits por n mensajes.

Usando código ASCII de 7 bits y n=4

3.7. Corrección de Errores

Ejemplo:

		LRC
H = 72d =	1001000	0
O = 79d =	1001111	1
L = 76d =	1001100	1
A = 65d =	1000001	0
VCR	0001010	0

de 40 bits se puede corregir 1.

Code rate = 28/(12+28) = 0.7

3.7. Corrección de Errores

EJEMPLO (J. H. Van Lint, 1971):

•Tirar una moneda a A veces por segundo: Secuencia aleat.

•Canal broadcast binario simétrico sin memoria de capacidad 2A bits/s y P(error)=$2\cdot 10^{-2}$

•1 bit para codificar cara o cruz

Transmisión tal cual: 2% de los resultados son incorrectos

3.7. Corrección de Errores

EJEMPLO (J. H. Van Lint, 1971):

•Solución 1:

Codificar cada resultado con 2 bits. Así los receptores detectarán la mayor parte de los errores

P(error no detectado) = $(2.10^{-2})^2$ = 0,04 %

Problema: No hay retransmisión para corregir los errores. Es necesario un esquema corrector de errores

P(error) = 1 - P(no error en 2 bits) = 3,96 % (peor)

3.7. Corrección de Errores

EJEMPLO (J. H. Van Lint, 1971):

•Solución 2:

Codificar 2 resultados con 4 bits.

Resultado	Código transmisión	Códigos válidos en recepción
cc	0000	0000 1000 0100 0010
cx	1001	1001 0001 1101 1011
xc	0111	0111 1111 0011 0101
xx	1110	1110 0110 1010 1100

3.7. Corrección de Errores

EJEMPLO (J. H. Van Lint, 1971):

Este código resiste errores de 1 bit en las posiciones 1, 2 o 3.

P(error) = 1 - P(no error) = 1 - $[q^4 + 3pq^3]$ = 2,12 %

• Transmitiendo a 2A y *code rate* = 0.5 (como antes) se ha bajado de 3,96 % a 2,12 %

• Se puede iterar (mejorar) el proceso con 8 bits para codificar 4 resultados, escogiendo adecuadamente 2^4 códigos de los 2^8 posibles.

3.7. Corrección de Errores

DISTANCIA DE HAMMING

Es la mínima diferencia en bits entre 2 palabras de un código.

Un código de distancia n permite:

- Detectar n-1 bits erróneos
- Corregir (n-1)/2 bits erróneos

Se conoce como Decodificación por Máxima Verosimilitud

3.8. Códigos de Bloque Lineales

Para transmitir n mensajes es necesario $\log_2 n$ (=m) bits, redondeando m al entero mayor más cercano.

Para proteger los m bits se pueden usar c bits adicionales, resultando en $2^{(m+c)}$ posibles códigos, de los cuales se usarán n.

Se escojen n códigos tal que difieran el máximo número de bits entre ellos.

3.8. Códigos de Bloque Lineales

Se pretende corregir 1 bit: Distancia Hamming mínima de 3 bits

¿Cuantos bits de redundancia c habrá que añadir a m?

- Para cada palabra código de m+c bits se pueden generar justamente m+c códigos de un solo bit erróneo
- Para proteger de un solo error, cada palabra código (de las 2^m) necesita de por lo menos m+c+1 códigos

Igualando: $(m+c+1)\cdot 2^m = 2^{(m+c)}$

Se obtiene: $m+c+1 = 2^c$

3.8. Códigos de Bloque Lineales

CÓDIGOS DE HAMMING

Palabra código de m+c bits (de 1 a (m+c)).

Posición del bit i-ésimo de redundancia:

$2^{(i-1)}$, con $1 <= i <= \log_2(m+c)$

Su valor se calcula haciendo la suma módulo 2 de las posiciones (expresadas como suma de potencias de 2) donde el bit i-ésimo tiene presencia.

3.8. Códigos de Bloque Lineales

CÓDIGOS DE HAMMING: Ejemplo:

4 bits de redundancia protegen 11 de info. (*Code Rate* 0.73)

0	1	0	1	0	1	0	0	0	1	1	0	0	1	1	Tx.
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	1	0	1	0	1	0	0	0	1	0	0	0	1	1	Rx.
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	0		1				1								

$2^0 + 2^1 + 2^3$ ⇒ **11**

3.8. Códigos de Bloque Lineales

REPRESENTACIÓN MATRICIAL

Si reordenamos la palabra código del ejemplo anterior escribiendo los datos seguidos de la redundancia:

D1 D2 D3 D4 D5 D6 D7 D8 D9 D10 D11 C1 C2 C3 C4

Obtenemos:

- C1 = D1 + D2 + D4 + D5 + D7 + D9 + D11
- C2 = D1 + D3 + D4 + D6 + D7 + D10 + D11
- C3 = D2 + D3 + D4 + D8 + D9 + D10 + D11
- C4 = D5 + D6 + D7 + D8 + D9 + D10 + D11

3.8. Códigos de Bloque Lineales

REPRESENTACIÓN MATRICIAL

Reescribiendo:

$$D1 + D2 + \quad + D4 + D5 + \quad + D7 + \quad + D9 + \quad + D11 + C1 = 0$$

$$D1 + \quad + D3 + D4 + \quad + D6 + D7 + \quad + D10 + D11 + C2 = 0$$

$$+ D2 + D3 + D4 + \quad + D8 + D9 + D10 + D11 + C3 = 0$$

$$+ D5 + D6 + D7 + D8 + D9 + D10 + D11 + C4 = 0$$

3.8. Códigos de Bloque Lineales

REPRESENTACIÓN MATRICIAL

C^t: Matriz traspuesta de la palabra de datos (1 columna, 15 filas)

$$\left(\begin{array}{ccccccccccc|cccc} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \cdot C^t = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \end{array}\right) \Rightarrow H \cdot C^t = \mathbf{0}$$

H: Matriz de control de paridad

3.8. Códigos de Bloque Lineales

REPRESENTACIÓN MATRICIAL

Los errores de transmisión se pueden formalizar como un vector de error **E** que se añade a la palabra código.

En recepción:

$$H \cdot (C^t + \mathbf{E}) = \mathbf{s}$$

El vector **s** se llama síndome. Al tratarse de códigos de bloque lineales, si coincidiera con una palabra código, el error **E** no sería detectado (**s** = **0**)

3.8. Códigos de Bloque Lineales

RÁFAGAS DE ERRORES (*Bursts*)

• Hasta ahora se ha visto la corrección de un bit erróneo, pero si los errores vienen a ráfagas lo anterior no sirve.

• La extensión de los códigos de Hamming a errores múltiples resulta compleja

• Métodos para la corrección de errores múltiples los hay: Códigos BCH, Reed-Solomon. No son objetivo del curso

3.8. Códigos de Bloque Lineales

ENTRELAZADO DE CÓDIGOS

Es un método general contra ráfagas de errores, consistente en cambiar el orden de transmisión de los datos.

Si los mensajes son de n bits y se esperan ráfagas de errores de longitud k bits, se puede almacenar k mensajes a transmitir en búferes de tamaño $k \cdot n$, escribiendo en el búfer por filas, y leyendo del mismo para transmisión por columnas. Una ráfaga provoca un error por mensaje

3.8. Códigos de Bloque Lineales

ENTRELAZADO DE CÓDIGOS

Ejemplo: Códigos de 7 bits y ráfagas de 3 bits

Cód.: A=a1 a2 a3 a4 a5 a6 a7, B=b1 b2 b3 b4 b5 b6 b7, C=c1 c2 c3 c4 c5 c6 c7

Tx: a1 b1 c1 a2 b2 c2 a3 b3 c3 a4 b4 c4 a5 b5 c5 a6 b6 c6 a7 b7 c7

Rx: a1 b1 c1 a2 b2 c2 a3 xx xx xx b4 c4 a5 b5 c5 a6 b6 c6 a7 b7 c7

Cód. Rx: A=a1a2 a3 xx a5 a6 a7, B=b1 b2 xx b4 b5 b6 b7, C=c1 c2 xx c4 c5 c6 c7

Corregible si, p.ej., se trataba de un código de Hamming 3,4

3.9. Control de Redundancia Cíclico (CRC)

• Es un código lineal para la detección de errores.

• Si P es la palabra código, G el polinomio generador de grado r, y R el resto, de grado r-1, de $P \cdot x^r/G$

• Transmisión: $T = P \cdot x^r - R$

Errores de transmisión aparecen como un polinomio E añadido al código transmitido. Así, al buscar el resto:

• Recepción: $(T+E)/G = T/G + E/G = E/G$

3.9. Control de Redundancia Cíclico (CRC)

- Se detectan todas las ráfagas de longitud r.
- Para que una ráfaga de mayor longitud no sea detectada el error E ha de ser múltiplo de G
- Transmitiendo n+r bits y suponiendo patrones de error aleatorios, se puede obtener que 2^{-r} errores no se detectan

3.9. Control de Redundancia Cíclico (CRC)

POLINOMIOS GENERADORES STANDARD

CRC-12: $x^{12} + x^{11} + x^3 + x^2 + 1$

CRC-CCITT: $x^{16} + x^{12} + x^5 + 1 =$

$= (x+1) \cdot (x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1)$

CRC-32 (IEEE-802):

$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

3.10. *Checksum* Aritmético

CRC detecta mejor que *checksum*, pero el cálculo del CRC tiene un coste en algún factor:

- Tiempo de CPU
- Uso de tablas
- Hardware específico

Cuando no es justificable la implementación de CRC, puede implementarse algún algoritmo de *checksum*.

3.11. Resumen

El control de errores es un módulo funcional dentro de la jerarquía de protocolos que, en caso de ser implementado, debe ser transparente al resto del protocolo.

Transforma un canal con tasa de error p en uno $p \cdot (1-f)$, con f fracción de errores detectados.

Cualquier esquema utilizado debe adecuarse a las características de los errores en el canal de transmisión, velocidad de transmisión requerida y error residual deseado.