

---

**16.36: Ingeniería de sistemas de comunicación**

**Clase 14: Detección de errores y códigos cíclicos**

Eytan Modiano

# Códigos cíclicos

---

- Un código cíclico es un código de bloque lineal donde si  $c$  es una palabra de código, también lo son todos los desplazamientos cíclicos de  $c$ 
  - P.ej.,  $\{000,110,101,011\}$  es un código cíclico
- Los códigos cíclicos se pueden tratar de la misma forma que el resto de los LBC
  - Se pueden hallar las matrices generadoras y de chequeo de paridad
- Un código cíclico puede ser descrito en su totalidad por un polinomio generador  $G$ 
  - Todas las palabras de código son múltiplos del polinomio generador
- En la práctica, los códigos cíclicos se usan para la detección de errores (CRC)
  - Utilizados para redes de paquetes
  - Cuando el recibido detecta un error, solicita la retransmisión

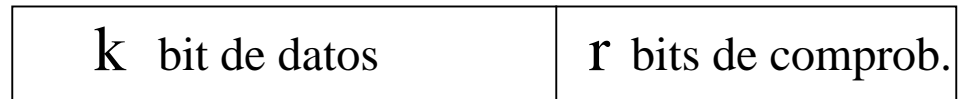
# Técnicas de detección de errores

---

- El receptor la emplea para determinar si un paquete contiene errores
- Si se encuentran errores en un paquete, el receptor solicita al transmisor que vuelva a enviarlo
- Técnicas de detección de errores
  - Comprobación de paridad  
P.ej., bit único
  - Comprobación de redundancia cíclica (CRC)

# Códigos de chequeo de paridad

---



- Cada comprobación de paridad es una suma módulo 2 de los bits de datos

Ejemplo:

$$C_1 = X_1 + X_2 + X_3$$

$$C_2 = X_2 + X_3 + X_4$$

$$C_3 = X_1 + X_2 + X_4$$

# Código de comprobación de paridad simple

---

- El bit es 1 si la trama contiene un número impar de unos; en caso contrario es 0

1011011 -> 1011011 1  
1100110 -> 1100110 0

- Así, la trama codificada contiene un número par de unos
- El receptor cuenta el número de unos que hay en la trama
  - Un número par de unos se interpreta como libre de errores
  - Un número impar de unos indica que se debe haber producido un error
    - Se puede detectar un error simple (o número impar de errores)
    - No es posible detectar un número par de errores
    - No es posible corregir nada

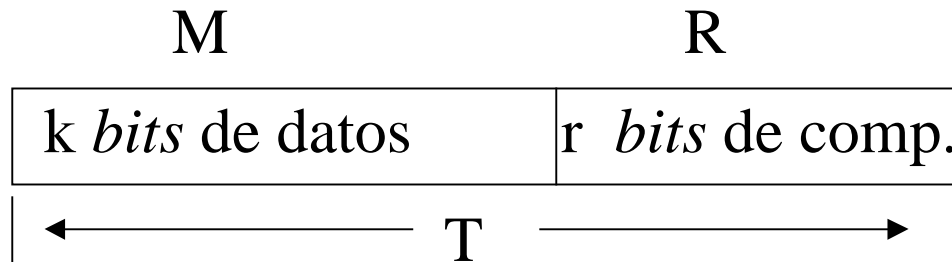
- Probabilidad de error no detectado (errores independientes)

$$P(\text{no detectado}) = \sum_{i \text{ par}} \binom{N}{i} p^i (1-p)^{N-i}$$

$N$  = tamaño de paquete  
 $p$  = prob. de error

# Comprobaciones de redundancia cíclica (CRC)

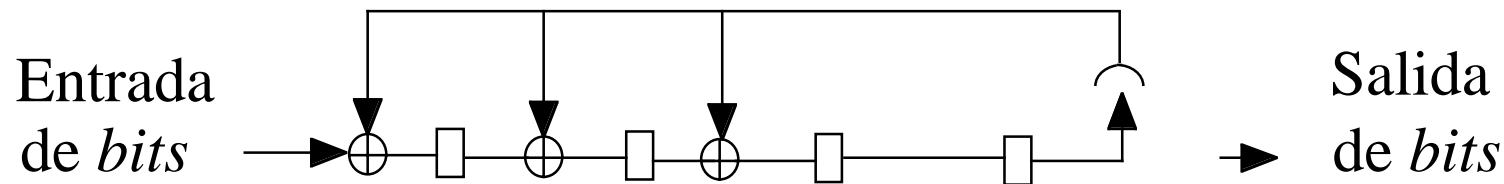
---



M = *bits* de información  
R = *bits* de comprobación  
T = palabra de código

$$T = M 2^r + R$$

- Un CRC se implementa empleando un FRS (*feedback shift register*)



# Comprobaciones de redundancia cíclica

---

$$T = M 2^r + R$$

- ¿Cómo se calcula R (los *bits* de comprobación)?
  - Se selecciona una cadena generadora G de r+1 *bits* de longitud
  - Se selecciona R de modo que T sea un múltiplo de G ( $T = A * G$ , para algún A)
  - Entonces, cuando se divida T por G, el resto será 0 => sin errores
  - Todo se hace utilizando aritmética modular (módulo 2)

$$T = M 2^r + R = A * G \Rightarrow M 2^r = A * G + R \text{ (aritmética de módulo 2)}$$

Sea R = resto de  $M 2^r / G$  y T múltiplo de G

- La selección de G resulta crucial para el rendimiento de un CRC

## Ejemplo

---

$$r = 3, G = 1001$$

$$M = 110101 \Rightarrow M2^r = 110101000$$

$$\begin{array}{r} 110011 \\ \hline 1001 \overline{) 110101000} \\ \underline{1001} \phantom{000} \downarrow \downarrow \downarrow \downarrow \\ 01000 \phantom{00} \downarrow \downarrow \downarrow \\ \underline{1001} \phantom{00} \downarrow \downarrow \\ 0001100 \phantom{0} \downarrow \\ \underline{1001} \phantom{00} \\ 01010 \\ \underline{1001} \\ 011 \end{array}$$

División de  
módulo 2

$$011 = R \text{ (3 bits)}$$

# Búsqueda de errores

---

- Sea T' la secuencia recibida
- Dividir T' entre G
  - Si el resto = 0, dar por hecho que no hay errores
  - Si el resto es distinto de cero, se deben haber producido errores

Ejemplo:

Se envía T = 110101011

Se recibe T' = 110101011

(no hay errores)

No hay forma de saber cuántos errores se han producido o qué *bits* contienen errores

$$\begin{array}{r} 1001 \overline{) 110101011} \\ \underline{1001} \phantom{000} \phantom{000} \phantom{000} \phantom{000} \\ 01000 \phantom{000} \phantom{000} \phantom{000} \\ \underline{1001} \phantom{000} \phantom{000} \phantom{000} \\ 0001101 \phantom{000} \\ \underline{1001} \phantom{000} \\ 01001 \phantom{000} \\ \underline{1001} \\ 000 \end{array}$$

000 => Sin errores

# División de módulo 2 como división polinómica

---

# Implementación de un CRC

---

# Eficacia de la técnica de detección de errores

---

- La eficacia de un código para la detección de errores se suele medir con respecto a tres parámetros:

1) Distancia mínima del código ( $d$ ) (núm. mín. de errores de bit no detectados)

La distancia mínima de un código es el menor número de errores que una palabra de código puede asignar a otra. Si se producen menos de  $d$  errores, se detectarán siempre. Incluso si hay más de  $d$  errores, se suelen detectar (aunque no siempre)

2) Capacidad de detección de ráfagas ( $B$ ) (la long. máx. de ráfaga siempre se detecta)

3) Probabilidad de patrón aleatorio de bits mal asumido como libre de errores (buen cálculo si el núm. de errores en una trama  $\gg d$  o  $B$ ):

– Útil cuando se pierde el entramado

–  $K$  bits de información  $\Rightarrow 2^k$  palabras de código válidas

– Con  $r$  bits de comprobación, la probabilidad de que una cadena aleatoria de longitud  $k+r$  se asigne a una de las  $2^k$  palabras de código válidas es  $2^k/2^{k+r} = 2^{-r}$

# Rendimiento del CRC

---

- Para  $r$  bits de comprobación por trama y una longitud de trama menor que  $2^r - 1$ , se detecta lo siguiente:
  - 1) Todos los patrones de 1, 2 ó 3 errores ( $d > 3$ )
  - 2) Todas las ráfagas de errores de  $r$  o menos bits
  - 3) Número elevado de errores aleatorios con probabilidad  $1 - 2^{-r}$
- Los DLC estándar utilizan un CRC con  $r = 16$  y la opción de  $r = 32$ 
  - CRC-16,  $G = X^{16} + X^{15} + X^2 + 1 = 11000000000000101$

# Características de error de la capa física

---

- La mayoría de las capas físicas (canales de comunicaciones) no se describen correctamente con un solo parámetro BER
- La mayor parte de los procesos de errores físicos suelen crear una mezcla de errores aleatorios y de ráfagas
- Un canal con un BER de  $10^{-7}$  y un tamaño medio de ráfaga de 1.000 bits es muy distinto de uno con errores aleatorios independientes
- Ejemplo: para una longitud media de trama de  $10^4$  bits:
  - Canal aleatorio:  $E[\text{tasa de error de la trama}] \sim 10^{-3}$
  - Canal de ráfagas:  $E[\text{tasa de error de la trama}] \sim 10^{-6}$
- Es mejor caracterizar un canal por su tasa de error de trama
- Esto representa un problema difícil en los sistemas reales