La rivelazione degli errori

Mauro Giaconi

La rivelazione degli errori

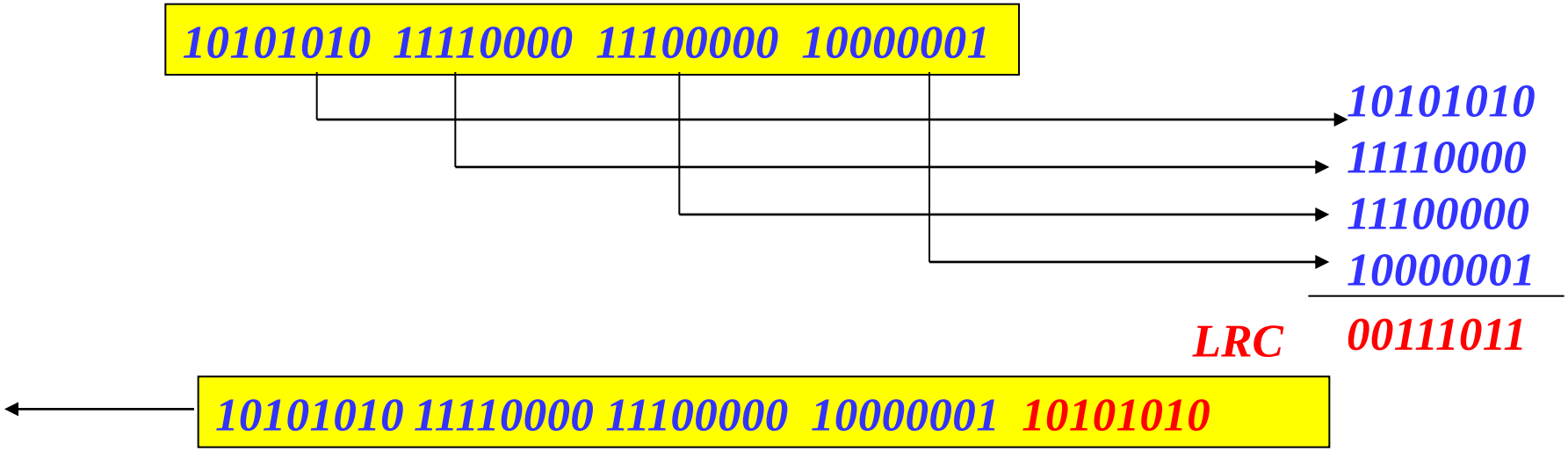
- *La trasmissione dati può contenere errori*
  - *bit isolati*
  - *Burst di errori di lunghezza n (n é la distanza tra gli estremi degli errori in un blocco di dati che contiene errori)*
- *Rivelare gli errori*
  - *Se si trasmettono solo dati gli errori non possono essere rivelati, quindi*
    - *inviare maggiore informazione assieme ai dati così da soddisfare specifiche relazioni tra essi*
      - *pertanto aggiunger ridondanza*

Metodi per la rivelazione degli errori

- *Parity Check*
  - *Aggiungere un singolo bit alla fine del blocco di dati così che il numero totale dei bit 1 sia pari*
    - *parità pari, la parità dispari é chiaramente simile*
      10011100100111 → 10011100100111 0
      11010000100111 → 11010000100111 1
  - *In tal modo si possono rivelare tutte le combinazioni di errori dispari*
  - *il metodo può essere generalizzato, come mostrato nel seguito*

Metodi per la rivelazione degli errori

- *Longitudinal Redundancy Check (LRC)*
  - *Strutturare i dati in una matrice e generare un parity Check per ogni colonna*



- *Rileva tutti i burst di errori sino alla lunghezza n (numero delle colonne)*
- *Non rileva burst di errori di lunghezza n+1 se ci sono n-1 bit non invertiti tra il primo e l'ultimo bit*
- *Se il blocco é malamente corrotto, la probabilità di accettazione é $(1/2)^n$*

Metodi per la rivelazione degli errori - Stima del tasso d'errore

Flusso binario

1 0 0 1 0 1 0 1 1 0 0 1 0 0 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0 0 1

Formazione dei blocchi

1 0 0 1 0 1 0 1 | 1 0 0 1 0 0 1 0 | 1 0 1 1 0 1 0 0 | 1 1 0 1 1 0 0 1

Generazione del bit P_i di parità

1 0 0 1 0 1 0 1 P_1 | 1 0 0 1 0 0 1 0 P_2 | 1 0 1 1 0 1 0 0 P_3 | 1 1 0 1 1 0 0 1 P_4

Allocazione dei bit di parità nell'overhead

1 0 0 1 0 1 0 1 | 1 0 0 1 0 0 1 0 | 1 0 1 1 0 1 0 0 | 1 1 0 1 1 0 0 1 | P_1 P_2 P_3 P_4

La stima del tasso d'errore è corretta in assenza di errori o con un errore per blocco. Essendo gli errori statisticamente a burst, i bit di parità sono calcolati su insiemi di bit intercalati

1	1	1	1	0	0	0	1	0	0	1	0	1	1	1	1	0	0	0	1	1	0	1	0	0	1	0	0	1	0	0	1	P_1	P_2	P_3	P_4

La tecnica, detta BIP-N (Bit Interleaved Parity N), con N numero dei bit di parità, consente di tollerare una sequenza di errori consecutivi di lunghezza massima N

Cyclic Redundancy Check

- *Si tratta di un potente schema di rivelazione di errori basato sulla divisione binaria di polinomi nell'algebra dei campi finiti (campi di Galois)*
- *Si può realizzare facilmente con poco hardware*
  - *Shift register*
  - *XOR (per addizioni e sottrazioni)*
- *Si considerano blocchi di k bit informative e h bit di ridondanza*

$$\underbrace{xxxxxxxxxx}_{k\ bit}\ \underbrace{yyyy}_{h\ bit}\ \Big\}\ \text{Blocco di lunghezza } k+h = n$$

- *E si associano i bit con coefficient di polinomi, ad esempio*

1 0 1 1 0 1 1

$1x^6+0x^5+1x^4+1x^3+0x^2+1x+1 = x^6+x^4+x^3+x+1$

Cyclic Redundancy Check – il metodo

- *Se M(x) é il polinomio associate al messaggio informativo*
- *E se P(x) é il polinomio associato a CRC (generatore)*
  - *P(x) é noto anche al ricevitore*
- *Si costruisce un polinomio F(x) a partire da M(x) che sia divisibile da P(x)*

$$\frac{F(x)}{P(x)} = Q(x)$$

- *Operativamente, in trasmissione*
  - *Si moltiplica M(x) per x^h*
  - *Si divide $x^h \cdot M(x)$ per P(x), considerando il solo resto R(x)*
  - *Si costruisce e si invia il blocco corrispondente al polinomio $F(x) = x^h \cdot M(x) + R(x)$*
- *Quindi, in ricezione*
  - *Si riceve il blocco corrispondente al polinomio F'(x)*
  - *Si divide F'(x) per P(x)*
  - *Si accetta il blocco se il resto é 0, se no si rifiuta*

Cyclic Redundancy Check

Si deve provare che $x^n \cdot M(x)+C(x)$ è divisibile da $P(x)$, infatti se

$$x^h \cdot M(x) = P(x) \cdot Q(x) + R(x)$$

allora

$$x^h \cdot M(x) + R(x) = P(x) \cdot Q(x)$$

si noti che in binario sottrazione e addizione sono equivalenti

$$A(x) + A(x) = 0$$

Cyclic Redundancy Check – la procedura

- *In trasmissione*
  - *Si deve inviare 1101001 cui corrisponde il polinomio $M(x) = x^6+x^5+x^3+1$*
  - *Si sceglie $P(x) = x^4+x+1$ (grado $r = h+1 = 4$) cui corrisponde il blocco 10011*
    - *$h = 4$ bit di ridondanza*
  - *Si forma il polinomio $x^h \cdot M(x)$ cui corrisponde il blocco 1101001 0000 e il*
  - *polinomio $x^{10}+x^9+x^7+x^4$*
  - *Si divide $x^h \cdot M(x)$ per $P(x)$ per trovare $R(x) = x^2+1$ cui corrisponde il blocco 0101*
  - *Si invia il blocco 1101001 0101*
- *In ricezione*
  - *Se non ci sono errori si riceve 1101001 0101 cui corrisponde il polinomio $x^{10}+x^9+x^7+x^4+ x^2+1$*
  - *Si divide tale polinolio per $P(x) = x^4+x+1$*
  - *Il resto é 0 e si accetta il messaggio*

Cyclic Redundancy Check – esempio di divisione

$$
\begin{array}{l|l}
x^{10}+x^{9}+x^{7}+x^{4} & x^{4}+x+1 \\
\hline
x^{10}+x^{7}+x^{6} & x^{6}+x^{5}+x+1 \\
\hline
x^{9}+x^{6}+x^{4} & \\
x^{9}+x^{6}+x^{5} & \\
\hline
x^{5}+x^{4} & \\
x^{5}+x^{2}+x & \\
\hline
x^{4}+x^{2}+x & \\
x^{4}+x+1 & \\
\hline
x^{2}+1 &
\end{array}
$$

Cyclic Redundancy Check – capacità di rivelazione

- Se vi sono errori, inviato F(x), si riceve F'(x) = F(x)+E(x) ove E(x) é il polinomio errore
- il CRC non rileva errori se la divisione E(x)/P(x) ha resto zero, cioé se P(x) divide E(x)
  - errore su un solo bit $E(x) = x^i$, i dato dalla posizione (i-1) dell'errore
    - se P(x) ha due o più termini, P(x) non divide E(x) quindi l'errore é rilevato
  - due bit errati (doppio errore), $E(x) = x^i+x^j$, $i > j$, $E(x) = x^j(x^{i-j}+1)$
    - posto che P(x) non sia divisibile da x, condizione sufficiente per rivelare tutti i doppi errori é che P(x) non divida (x^t+1) per ogni t sino a i-j (lunghezza del blocco)
      - se P(x), di grado r, é un polinomio irriducibile di $x^{2\wedge r-1}+1$, P(x) non divide (x^t+1) per $t < 2^r-1$ per cui la lunghezza del messaggio globale deve essere $\leq 2^r-1$
  - burst di lunghezza m, $E(x) = x^j(T(x))$, con T(x) polinomio di grado m-1
    - posto che P(x) non sia divisibile da x, se il grado di T(x), m-1, é inferiore al grado di P(x), r, P(x) non divide T(x), quindi un CRC con P(x) di grado r rileva tutti i burst di lunghezza minore di r
  - con lunghezza di burst m> r la percentuale di burst rilevati é $2^{-(r-1)}$ se m =r, $2^{-(r)}$ se m>r
  - errori in numero dispari,
    - se P(x) é prodotto di un un polinomio irriducibile di $x^{2\wedge r-1}+1$ per (x+1) ciò equivale a porre un bit di parità globale, quindi il CRC rivela tutti gli errori dispari