**Il codice di Hamming**

Occasionalmente le memorie dei calcolatori possono commettere degli errori per via di picchi di tensioni sulle linee di alimentazione o per altre cause. Per proteggersi da questi errori alcune memorie utilizzano codici di rilevamenti e/o di correzione degli errori.

Quando si applicano questi codici si aggiungono dei bit extra a ogni parola di memoria secondo una modalità particolare. Quando una parola viene letta in memoria si controllano questi bit consecutivi per vedere se si è verificato un errore. Supponiamo che una parola di memoria sia costituita da m bit di dati ai quali vengono aggiunti r bit ridondanti o di controllo. Quindi la lunghezza totale della parola sarà n=m+r. per determinare tra due parole il numero di bit diversi bisogna semplicemente calcolare l’or esclusivo tra i bit delle due parole e contare quanti valgono 1, questo valore viene chiamato distanza di Hamming. Il suo significato principale è che se fra due parole esiste una distanza di Hamming pari a d, allora saranno necessari d errori singoli per trasformare una parola in un’altra.

Con una parola di m bit tutte le 2m combinazioni di bit sono legali, ma per via del modo in cui sono calcolati i bit di controllo, solo 2m delle 2n parole di codice sono valide. Se una lettura da memoria restituisce una parola non valida, il calcolatore sa che è avvenuto un errore. Conoscendo l’algoritmo che calcola i bit di controllo è possibile costruire una lista di parole di codice lecite e, da questa lista, trovare le due parole la cui distanza di Hamming è minima. Questa distanza è la distanza dell’intero codice.

Le proprietà di rilevazione e di correzione degli errori di una parola di codice dipendono dalla distanza di Hamming. Per rilevare d errori singoli è necessaria una parola con distanza d+1, poiché con tale distanza non esiste alcun codice in cui d errori singoli possano cambiare una parola valida in un’altra parola valida. In modo analogo per correggere d errori singoli è necessario un codice con distanza 2d+1, poiché in questo modo le parole di codice legali sono sufficientemente lontane l’una dall’altra, anche con d cambiamenti la parola di codice originata continua ad essere più vicina rispetto a tutte le altre parole di codice, potendola quindi determinare in modo univoco.

In un codice di Hamming gli r bit di parità sono aggiunti a una parola a m bit. I bit sono numerati a partire da uno e non da zero a partire dalla prima posizione a sinistra. Tutti i bit la cui posizione è una potenza di due sono bit di parità, quelli restanti sono invece i dati. Ciascun bit di parità controlla alcune posizioni specifiche dei bit dei dati ed è impostato in modo che sia pari il numero totale di bit che hanno valore 1 nelle posizioni controllate. Ogni posizione è controllata da due bit precedenti la cui somma dà la posizione che bisogna controllare. Un metodo semplice per trovare i bit errati bisogna calcolare inizialmente tutti i bit di parità. Se sono tutti corretti, significa che non si è verificato alcun problema (o più di uno). Successivamente si sommano i bit di parità errati, contando 1 per il bit di parità 1, 2 per il bit di parità 2, 9 per il bit di parità 9, e la somma corrisponde al bit errato e successivamente viene corretto.