*Codici a correzione d’errore*

Sviluppare codici a correzione d’errore è un modo per prevenire la perdita d’informazioni in una comunicazione. Una caratteristica fondamentale di un codice, al fine dello sviluppo di un metodo per correggerne gli errori, è la distanza di Hamming. Si definisce distanza di Hamming in un codice binario il numero di cifre per cui differiscono le parole che hanno più cifre in comune, quindi il numero minimo di cifre il cui cambiamento porta da una parola legale del codice ad un’altra.

Descrivendo in questo modo i codici si può dedurre che:

* Per rilevare *n* errori singoli è necessario un codice che abbia distanza di Hamming pari a *n+1*, poiché n+1 errori singoli sono necessari per passare da una parola legale a un’altra;
* Per correggere *n* errori singoli è necessario un codice che abbia distanza di Hamming pari a *2n+1*, poiché occorre approssimare la parola errata a quella legale più simile.

Un metodo per correggere gli errori singoli è introdurre dei bit di controllo, il cui valore varia in base al valore dei bit di dati. I bit di parità sono bit di controllo il cui valore viene assegnato per mantenere un numero pari di 1 nel codice.

Si definisce codice di Hamming un codice con il quale è possibile correggere tutti gli errori singoli. Tale codice usa un numero variabile di bit di parità in base al numero di bit di dati necessari nella comunicazione. ­Perciò, ogni parola del codice è composta da *n = m + r* bit, dove *m* sono i bit di dati ed *r* sono i bit di controllo. Si può dedurre una relazione tra il numero di bit di dati e quello di bit di controllo necessari: per ogni parola legale ci sono di certo *n* parole a distanza di 1 bit illegali, ottenute variando singolarmente ogni bit della parola. Le parole illegali a distanza 1 da quelle legali sono quindi *2mn*. Tutte le parole del codice sono invece *2n*; poiché *2mn < 2n*, *n < 2r* quindi *m + r < 2r*. Gli *r* bit di controllo sono disposti sulle posizioni che sono potenze di 2 e controllano ciascuno la parità parziale della parola: il bit in posizione 1 controlla la parità dei bit dispari; quello in posizione 2 controlla 2 bit ogni 4 a partire da sé stesso; quello in posizione 4 controlla 4 bit ogni 8 a partire da sé stesso, e così via. Confrontando i bit di parità si può trovare il bit errato perché sarà controllato contemporaneamente dai bit di parità errati.