

Decodifica di codici ciclici

Ricevuto il messaggio $r(x) = c(x) + e(x)$, con $e(x)$ vettore di errore, se la sindrome $s(x)$ di $r(x)$ ha peso minore o uguale alla capacità di correzione di errori del codice, allora $e(x) = s(x)$.

Questo permette di correggere solo errori nei bit di parità, visto che $\deg s(x) < q$ ($s(x) = r(x) \bmod g(x)$, $\deg g(x) = q$). Tuttavia si possono effettuare rotazioni cicliche a sinistra di $s(x)$ finché non si ottiene un polinomio $x^i s(x)$ che ha sindrome $s'(x)$ di peso sufficientemente basso; allora $e(x) = x^{n-i} s'(x)$.