Polinomio di controllo di parità per codici ciclici

Dato il polinomio generatore $g(x)$ del codice ciclico (n, k) C, il polinomio di controllo di parità $h(x)$ è il polinomio (di grado k) tale che

$$g(x)h(x) = x^n - 1 = 0$$

Ricevuto il messaggio $r(x)$, si può calcolare la sindrome $s(x)$:

$$s(x) = r(x)h(x) = r(x) \bmod g(x).$$

Vale:

$$r(x) \in C \iff s(x) = 0$$

Dove le operazioni sono sempre svolte modulo $p^n - 1$ sui polinomi e 2 sui coefficienti.

Matrice

$$H = \begin{pmatrix} h_k & \cdots & h_0 & 0 & \cdots & & 0 \\ 0 & h_k & \cdots & h_0 & 0 & \cdots & 0 \\ & & \ddots & & & & \\ 0 & \cdots & 0 & h_k & \cdots & & h_0 \end{pmatrix}.$$