Polinomio generatore per codici ciclici

Chiamiamo generatore $g(x)$ l'unico (se si considerano solo polinomi monici) polinomio non nullo di grado minimo nel codice ciclico (n, k) C.

Proprietà:

- $\deg g(x) = n - k$;
- i multipli di $g(x)$ modulo $x^n - 1$ sono le parole di codice, ovvero C contiene tutti e soli i polinomi di grado $\leq n - 1$ divisibili per $g(x)$;
- $g(x)$ divide $x^n - 1$, e ogni divisore di $x^n - 1$ di grado $n - k$ genera un codice ciclico (n, k). Quindi se $x^n - 1$ ha m fattori, ci sono 2^m codici ciclici di lunghezza n (contando anche $n = k$ e $n = q$);
- $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ è una base di C, quindi si può costruire la matrice generatrice

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix},$$

dove ogni riga di coefficienti si ottiene traslando di una posizione la riga precedente, e ha al più q posizioni non nulle ($\deg g(x) = q$):

$$G = \begin{pmatrix} g_q & \cdots & g_0 & 0 & \cdots & & 0 \\ 0 & g_q & \cdots & g_0 & 0 & \cdots & 0 \\ & & \ddots & & & & \\ 0 & \cdots & 0 & g_q & \cdots & & g_0 \end{pmatrix}.$$

Esempio: da $x^5 - 1 = (1 + x)(1 + x + x^2 + x^3 + x^4)$ si deduce che ci sono 3 codici ciclici con $n = 5$: 1) $g(x) = 1$, $q = 0$ quindi tutte le parole da 5 bit 2) $g(x) = 1 + x$, con $k = 4$ 3) $g(x) = 1 + x + x^2 + x^3 + x^4$.