Codici ciclici

Un codice lineare a blocchi (n, k) è ciclico se è chiuso rispetto alla traslazione ciclica (ruotando una parola si ottiene un'altra parola).

Rappresentazione con polinomi

Si possono rappresentare le parole di codice con polinomi di grado $\leq n-1$ in $\mathbb{F}_2[x]$:

$$c_{n-1} \cdots c_0 \to c_{n-1}x^{n-1} + \cdots + c_1 x^1 + c_0,$$

con operazioni modulo $x^n - 1$ (per mantenere il grado $< n$) suoi polinomi e modulo 2 sui coefficienti.

Indichiamo con $c^{(i)}(x)$ la rotazione ciclica a sinistra di i posizioni del polinomio $c(x)$.

Teorema

Se $c(x) \in C$ e $a(x) \in \mathbb{F}_2[x]$ con $\deg a < n$, allora $a(x)f(x) \bmod x^n - 1 \in C$.

Infatti,

$$\begin{aligned} a(x)f(x) &= (a_{n-1}x^{x-1} + \cdots + a_0)f(x) \\ &= a_{n-1}x^{n-1}f(x) + \cdots + a_0 f(x) \end{aligned}$$

e visto che $a_i \in \{0, 1\}$, ciascun termine di questa somma è 0 o $x^i f(x)$, ovvero $f(x)$ shiftato a sinistra di i posizioni. Quindi sono tutte parole di codice, e visto che il codice è lineare sommandole si ottiene una parola di codice.

In particolare quindi $c^{(i)}(x) = x^i c(x) \bmod x^n - 1$.

Polinomio generatore e di controllo di parità

$$\begin{aligned} C &= \{a(x)g(x) \mid a(x) \in \mathbb{F}_2\} \\ &= \{a(x) \mid a(x)h(x) = 0\} \end{aligned}$$