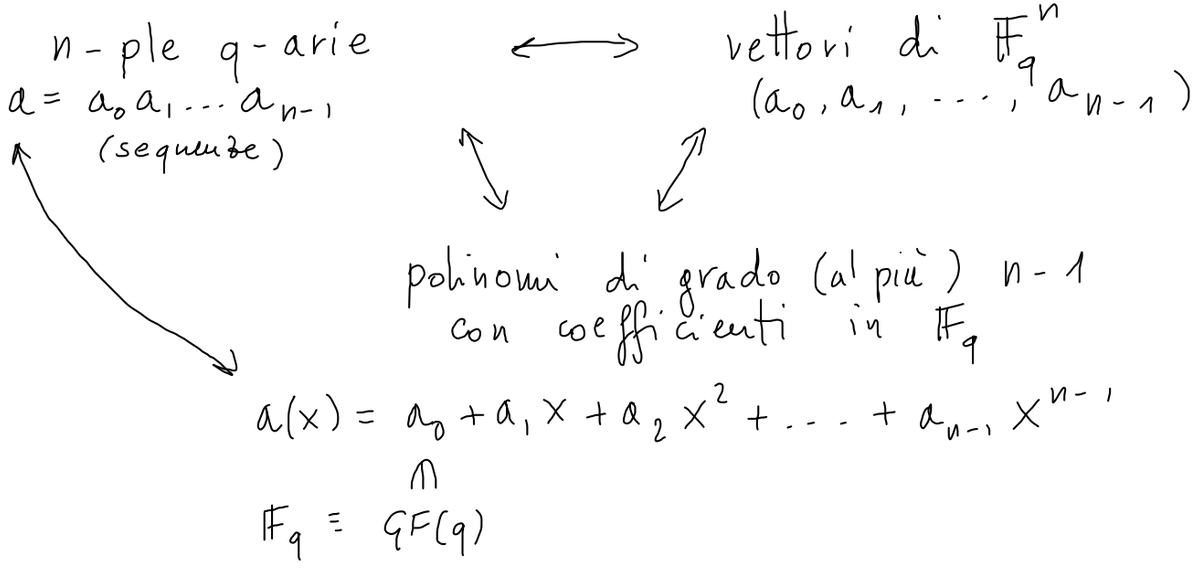
Codici ciclici

Def. Un codice lineare è detto ciclico se qualunque permutazione ciclica di una parola di codice è ancora una parola di codice.

Es. $00101 \in \mathcal{C} \Rightarrow 01010 \in \mathcal{C} \Rightarrow 10100 \in \mathcal{C} \Rightarrow \dots \Rightarrow 10010 \in \mathcal{C} \Rightarrow 00101$



Associo ad ogni n-pla $a = (a_0, a_1, \dots, a_{n-1})$ il polinomio (formale)

$a(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$; se $a \in \mathcal{C}$, scriviamo anche $a(x) \in \mathcal{C}$

Definiamo un anello in cui:

- la somma segue le regole usuali (sommo componente per componente secondo la somma del campo $\mathbb{F}_q$)
- il prodotto viene effettuato come prodotto di polinomi modulo il polinomio $\boxed{d(x) = x^n - 1}$.

Equivale a passare dall'anello $\mathbb{F}_q[x]$ dei polinomi a coefficienti in $\mathbb{F}_q$ all'anello quoziente $\frac{\mathbb{F}_q[x]}{x^n - 1}$ in cui si identificano due polinomi $a(x)$ e $b(x)$ se $a(x) - b(x) = q(x) \cdot \overbrace{(x^n - 1)}^{d(x)}$ (scrivo $a(x) \equiv b(x) \mod d(x)$)

Effettuare una permutazione ciclica di un polinomio $a(x)$ equivale (verso destra di 1 passo) a moltiplicare $a(x)$ per $x \pmod{x^n - 1}$: infatti $x \cdot a(x) = a_0 x + a_1 x^2 + a_2 x^3 + \dots + a_{n-1} x^n$ ($\nearrow x^n = x^n - 1 + 1$)

$$= a_0 x + a_1 x^2 + \dots + \underbrace{a_n (x^n - 1)}_{\equiv 0 \pmod{(x^n - 1)}} + a_{n-1} \equiv a_{n-1} + a_0 x + a_1 x^2 + \dots + a_{n-2} x^{n-1}$$

Σ $(a_{n-1}, a_0, a_1, \dots, a_{n-2})$

$\Rightarrow$ In un codice ciclico, le parole di codice (i polinomi corrispondenti) formano un sottoanello chiuso rispetto alla moltiplicazione per l'indeterminata x.

$n = 5$ $\longleftrightarrow$ 00101 $\xrightarrow{\text{ruoto a dx}}$ 10010

c $\qquad$ c

$0 \cdot x^0 + 0 \cdot x^1 + 1 \cdot x^2 + 0 \cdot x^3 + 1 \cdot x^4$ $\qquad$ $0 \cdot x^1 + 0 \cdot x^2 + 1 \cdot x^3 + 0 \cdot x^4 + \boxed{1 \cdot x^5}$ $\quad 1 \cdot x^0$

moltiplico per x e ridotto modulo $x^n - 1$

$x^n - 1 \equiv 0$

$x^n \equiv 1 \equiv x^0$

S sottoanello formato dalle parole di codice (di un codice ciclico)

(sottoanello di $\mathbb{F}[x]/(x^n - 1)$)

$\forall a(x) \in S$, $\boxed{x \cdot a(x) \in S}$ $\qquad$ $\forall a(x) \in S, b(x) \in S, \; a(x) + b(x) \in S$

$\forall a(x) \in S$, $\forall \alpha \in \mathbb{F}_q$, $\alpha \cdot a(x) \in S$ $\qquad$ (si dice che S è un ideale)

$$\forall\, p(x) \in \frac{\mathbb{F}[x]}{x^n - 1} \qquad \forall a(x) \in S \qquad\qquad x^n \equiv 1$$

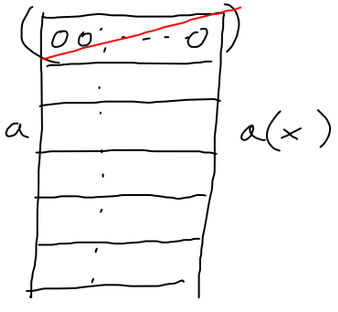
$$p(x)a(x) = (p_0 + p_1 x + \dots + p_{n-1} x^{n-1})\, a(x)$$

$$= p_0\, a(x) + p_1 x\, a(x) + \dots + p_{n-1} x^{n-1}\, a(x) \quad \in S$$

$p_0 \in \mathbb{F}_q$, $a(x) \in S$; $x\,a(x) \in S$; $x^{n-1}\,a(x) \in S$; $p(x)a(x) \in S$

Consideriamo un qualunque $a(x) \in \mathcal{C}$ non-nullo di grado minimo

e sia f il suo grado ($f \le n-1$)



Se il coefficiente di grado f (a_f) è pari ad 1,

possiamo dividere il polinomio per a_f e ottenere ancora una parola di codice.

→ Posso assumere che $a_f = 1$. (polinomio monico).

$$a(x) = a_0 + a_1 x + \dots + a_f x^f + 0$$

$$\tilde{a}(x) = a_f^{-1} a_0 + a_f^{-1} a_1 + \dots + 1 \cdot x^f$$

$\tilde{a}(x) \in \mathcal{C}$

Non esistono altri polinomi monici di grado f in $\mathcal{C}$;
altrimenti la differenza tra un tale polinomio $b(x)$ e $a(x)$
sarebbe un polinomio di grado $< f$

$$a_0 + \dots + a_{f-1}x^{f-1} + 1 \cdot x^f$$
$$b_0 + \dots + b_{f-1}x^{f-1} + 1 \cdot x^f$$

$$\longrightarrow b(x) - a(x) = (b_0 - a_0) + \dots + (b_{f-1} - a_{f-1})x^{f-1} + 0$$

0 (cancellato)

$\in \mathcal{C}$

(contraddizione perché $a(x)$ è di grado minimo tra tutti i polinomi non-nulli in $\mathcal{C}$).

$\longrightarrow$ Il polinomio di grado minimo monico in $\mathcal{C}$ è unico; è chiamato il <u>polinomio generatore</u> del codice.
È indicato con $m(x)$ (a volte con $g(x)$).

Teorema. Ogni polinomio $a(x) \in \mathcal{C}$ è un multiplo di $m(x)$.

Dim. Sia $a(x) \in \mathcal{C}$; dividendo $a(x)$ per $m(x)$ si ottiene:

$$a(x) = \underbrace{q(x)}_{\text{quoziente}}\,\underbrace{m(x)}_{\text{divisore}} + \underbrace{r(x)}_{\text{resto}} \quad ; \quad \text{quindi} \quad r(x) = \underbrace{a(x)}_{\in \mathcal{C}} - \underbrace{\underbrace{q(x)}_{\in \frac{\mathbb{F}_q[x]}{x^n-1}}\,\underbrace{m(x)}_{\in \mathcal{C}}}_{\in \mathcal{C}} \in \mathcal{C}$$

$gr(a) \leq n-1$

$gr(m) = f$

$\boxed{gr(r) < f}$

Se fosse $r(x) \neq 0$, avrei trovato un nuovo polinomio non-nullo in $\mathcal{C}$ di grado minore di f; contraddizione!

$\Rightarrow r(x) \equiv 0 \Rightarrow \boxed{a(x) \equiv q(x)\,m(x)}$; $a(x)$ è un multiplo di $m(x)$. QED.

$\mod (x^n-1)$

$$= q_0 m(x) + q_1 x\, m(x) + q_2 x^2 m(x) + \dots + q_\ell x^\ell m(x)$$

Questo ci permette di strutturare la matrice generatrice G di un codice ciclico come matrice delle permutazioni cicliche del polinomio generatore:

$$m(x) = g_0 + g_1 x + \dots + g_f \cdot x^f \quad (g_f = 1)$$

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_f & & & \leftarrow m(x) \\ & g_0 & g_1 & & g_{f-1} & g_f & & \leftarrow x \cdot m(x) \\ & & \ddots & & & \ddots & & \leftarrow x^2 \cdot m(x) \\ & & & & g_0 & g_1 & \cdots & g_f \leftarrow x^{k-1} m(x) \end{bmatrix}$$

(k righe, n colonne)

$$f + k = n \quad \Rightarrow f = n - k$$

$$z = u \cdot G$$

Per specificare G, prima utilizzavamo $(k \times n)$ elementi di $\mathbb{F}_q$

Ora ci bastano f elementi di $\mathbb{F}_q$ ($f+1$ coefficienti di $m(x)$)

Come determinare la matrice di controllo H a partire da $m(x)$?

Supponiamo di avere un polinomio $h(x)$ tale che $h(x) \cdot m(x) \equiv 0 \pmod{(x^n - 1)}$

Se $a(x) \in C$, per il teorema visto prima ho $a(x) = b(x) \cdot m(x)$

(per qualche $b(x)$ nell'anello quoziente);

quindi $h(x)\, a(x) \equiv h(x)\, b(x)\, m(x) \equiv \underbrace{h(x)\, m(x)}_{\equiv 0}\, b(x) \equiv 0 \pmod{(x^n - 1)}$

$h(x)$ è chiamato polinomio di controllo.

$h(x)$ non è unico:

$$(x\, h(x))\, a(x) = h(x)\, \underbrace{x\, a(x)}_{\in C} \equiv 0$$

$$(x^2 h(x))\, a(x) = h(x)\, x^2 a(x) \equiv 0$$

$$\vdots$$

Ogni permutazione ciclica di h è ancora un polinomio di controllo.

$C^\perp$

$p(x)$ $\quad p \cdot a^T = 0$

Prop. Se $a(x) = (a_0, a_1, \dots, a_{n-1})$, $b(x) = (b_0, b_1, \dots, b_{n-1})$

allora $a(x)\,b(x) \equiv 0 \pmod{x^n - 1}$ se e solo se

la n-pla $(a_0, a_1, \dots, a_{n-1})$ è ortogonale alla n-pla $(b_{n-1}, b_{n-2}, \dots, b_0) \equiv b$ ←

e a tutte le sue permutazioni cicliche.

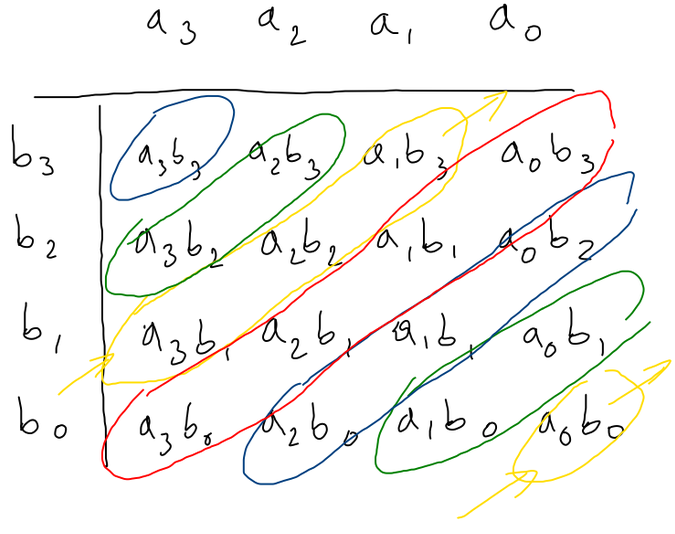
Dim. (attraverso un esempio).

$(n=4)$

$$a(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

$$b(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3$$

$$a(x)b(x) \bmod (x^4 - 1) = (a_0 b_0 + a_1 b_3 + a_2 b_2 + a_3 b_1)\, x^0 +$$
$$(a_1 b_0 + a_0 b_1 + a_3 b_2 + a_2 b_3)\, x^1 +$$
$$(a_2 b_0 + a_1 b_1 + a_0 b_2 + a_3 b_3)\, x^2 +$$
$$(a_3 b_0 + a_2 b_1 + a_1 b_2 + a_3 b_0)\, x^3$$



→ Il polinomio generatore dello spazio $C^{\perp}$

è $h^*(x) = x^k h(x^{-1})$ (cioè il polinomio che corrisponde a $\overleftarrow{h}$)

Esempio. $(3, 4, 7)$ $\quad 3 + 4x + 7x^2 = h(x)$

$(7, 4, 3)$ $\quad 7 + 4x + 3x^2 = x^2 h(x^{-1})$

$= x^2 \underbrace{(3 + 4x^{-1} + 7x^2)}_{h(x^{-1})}$

La matrice di controllo H ha la forma:

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 \\ & h_k & h_{k-1} & \cdots & h_0 \\ & & \ddots & & \ddots \\ h_k & & & h_0 & \end{bmatrix} \leftarrow \overleftarrow{h}$$

$(h^*(x))$

$x^{-1} h^*(x)$

$\vdots$

$x^{-1} \equiv x^{n-1}$

$x^n \equiv 1$