Codici ciclici

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

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

n-ple q-arie $\longleftrightarrow$ vettori di $\vec{q}^{\,n}$

$a_0 a_1 a_2 \dots a_{n-1}$ $\qquad$ $(a_0, a_1, \dots, a_{n-1})$

$\updownarrow$ $\qquad$ $\updownarrow$

polinomi di grado $n-1$
con coefficienti in $GF(q)$ (campo di ordine q)

$$a(x) = \underset{\substack{\cap \\ GF(q)}}{a_0} + \underset{\substack{\cap \\ GF(q)}}{a_1} x + a_2 x^2 + a_3 x^3 + \dots + a_{n-1} x^{n-1}$$

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 $\underline{a \in \mathcal{C}}$, scriviamo anche $\underline{a(x) \in \mathcal{C}}$

Definiamo un anello in cui:

- la somma segue le regole usuali (sommo le componenti nel campo $GF(q)$)
- il prodotto viene effettuato modulo $d(x)$ dove

$$d(x) = x^n - 1 \qquad x^n \equiv 1$$

$$\Updownarrow$$

Passiamo dell'anello $\mathbb{F}[x]$ all'anello quoziente $\mathbb{F}[x]/(x^n-1)$ formato delle classi resto modulo $d(x)$; notare che $x^n - 1 \equiv 0 \pmod{d(x)}$

Effettuare una permutazione ciclica di a nell'anello quoziente $\mathbb{F}[x]/(x^n-1)$ equivale a moltiplicare $a(x)$ per x:

$$\underbrace{x \cdot a(x)} = x\,(a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1})$$

$$= a_0 x + a_1 x^2 + a_2 x^3 + \dots + a_{n-2} x^{n-1} + a_{n-1} \underset{\overset{\equiv}{1}}{x^n} \equiv$$

$$\equiv a_{n-1} + a_0 x + a_1 x^2 + a_2 x^3 + \dots + a_{n-2} x^{n-1} \triangleq b(x)$$

$$(a_{n-1}, a_0, a_1, a_2, \dots, a_{n-2}) = b$$

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

S sottoanello formato dalle parole di codice (di $\mathbb{F}[x]/(x^n-1)$)

$\forall a(x) \in S$, $x \cdot a(x) \in S$ } Poiché il codice è ciclico

$\alpha \cdot a(x) \in S$

$\forall a(x), b(x) \in S$, $a(x)+b(x) \in S$ } Poiché il codice è lineare

$\forall a(x) \in S$
$\forall p(x) \in \mathbb{F}[x]/(x^n-1)$, $a(x) \cdot \underbrace{(p_0 + p_1 x + \dots + p_{n-1} x^{n-1})}_{p(x)\ \in S,\ \notin S} \in S$ $\quad$ S è un (ideale)

Consideriamo un qualunque $a(x) \in C$ non-nulla di grado minimo,
e sia f il suo grado (il grado è al più $n-1$).
Se il coefficiente di grado massimo di $a(x)$ non è 1 (polinomio monico),
possiamo dividere per un elemento di $GF(q)$, ottenendo ancora un elemento di C.
Non esistono altri polinomi monici di grado f in C:
altrimenti la loro differenza sarebbe in C
e avrebbe grado $< f$, contraddicendo
la scelta di $a(x)$.

f 2

$a(x) = 1 \cdot x^{7} + 3 \cdot x^5 + 8 \cdot x^4 + \dots$

$b(x) = 1 \cdot x^{7} + 2 \cdot x^5 + 6 \cdot x^4 + \dots$

$C \ni a(x) - b(x) = \underbrace{0} + 1 \cdot x^5 + 2 \cdot x^4 + \dots$

avrebbe grado $< f$

$\rightarrow$ Il polinomio monico di grado minimo in C
è unico. È il polinomio generatore del codice $(m(x))$.

Teorema (6.6): Ogni polinomio $a(x) \in \mathcal{C}$ è un multiplo di $m(x)$.

Dim. Sia $a(x) \in \mathcal{C}$ qualunque. Dividendo $a(x)$ per $m(x)$, otteniamo:

$$a(x) = \underbrace{q(x)}_{\text{quoziente}} \cdot m(x) + \underbrace{r(x)}_{\text{resto}} \quad , \quad \text{con } \operatorname{grado}(r(x)) < \operatorname{grado}(m(x)) = f.$$

Ma allora $r(x) = \underbrace{a(x)}_{\in \mathcal{C}} - \underbrace{q(x) \cdot \underbrace{m(x)}_{\in \mathcal{C}}}_{\substack{\in \mathcal{C} \\ \text{(rimango nel} \\ \text{sottoanello } \mathcal{C})}} \in \mathcal{C}$

Ma allora $r(x) \equiv 0$, perché altrimenti esisterebbe un polinomio non-nullo $\in \mathcal{C}$ di grado $< f$. Quindi $a(x) \equiv q(x) \cdot m(x)$. QED

Questo ci permette di strutturare la matrice generatrice G di un codice ciclico attraverso la parola di codice $m(x)$ e le sue permutazioni cicliche:

$$m(x) = g_0 + g_1 x + g_2 x^2 + \dots + \overset{1}{\overset{\parallel}{g_f}} \cdot x^f$$

$\Downarrow$

$$k \left\{ \; G = \underbrace{\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_f & 0 & 0 & 0 \\ & g_0 & g_1 & g_2 & \cdots & g_f & 0 & 0 \\ & & \ddots & \ddots & & & \ddots & \\ & & & g_0 & g_1 & & & g_f \end{bmatrix}}_{n} \right. \begin{array}{l} \leftarrow m(x) \in \mathcal{C} \\ \leftarrow x \cdot m(x) \in \mathcal{C} \\ \\ \\ \end{array}$$

K

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

Anziché specificare G ($k \times n$ elementi), mi basta specificare $m(x)$ ($f+1$ elementi)

Come determinare la matrice di controllo H, se conosciamo $m(x)$?

Scriviamo $\quad h(x) \cdot m(x) \equiv 0$ (poiché devono essere valide le equazioni di controllo)

$\uparrow$ polinomio nullo

Se $a(x) \in \mathcal{C}$, per il Teorema 6.6 $a(x) = m(x) \cdot b(x)$. (per qualche $b(x)$)

Quindi $\quad h(x)\, a(x) = \underbrace{h(x) \cdot m(x)}_{\equiv 0} b(x) \equiv 0$

$\mathcal{C}^\perp$

funge da equazione di controllo del codice.

Un tale polinomio $h(x)$ è detto polinomio di controllo.

Non è unico:

$\underbrace{a(x) \cdot x}_{\in \mathcal{C}} \cdot h(x) \equiv 0 \quad \longrightarrow$ anche $x \cdot h(x)$ è un polinomio di controllo

$\underbrace{a(x) \cdot x^2}_{\in \mathcal{C}} \cdot h(x) \equiv 0 \quad \longrightarrow$ anche $x^2 \cdot h(x)$ " " " " "

$a(x)\, x^{n-k-1} \cdot h(x) \equiv 0 \quad \longrightarrow$ anche $x^{n-k-1}\, h(x)$ " " " " "

Prop. (6.3) Se $a(x) = (a_0 a_1 \dots a_{n-1})$, $b(x) = (b_0 b_1 \dots b_{n-1})$

allora $a(x) \cdot b(x) \equiv 0$ se e solo se

la n-pla a è ortogonale alla n-pla $(b_{n-1} b_{n-2} \dots b_1 b_0) = \overleftarrow{b}$

e a tutte le sue permutazioni cicliche.

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

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

$n = 4$

$$a(x) \cdot b(x) \mod (x^n - 1) =$$

$$= (\underbrace{a_0 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3}_{0}) \cdot x^0 +$$

$(x^n \equiv 1)$

$$(\underbrace{a_1 b_0 + a_0 b_1 + a_3 b_2 + a_2 b_3}_{0}) \cdot x^1 +$$

$x^4 \equiv 1$

$$(\underbrace{a_2 b_0 + a_1 b_1 + a_0 b_2 + a_3 b_3}_{0}) \cdot x^2 +$$

$x^5 \equiv x$

$$(\underbrace{a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3}_{0}) \cdot x^3$$

$$\equiv 0$$

$x^6 \equiv x^2$ $\quad$ $x^5 \equiv x$

$$\begin{array}{c|cccc|c}
 & a_3 & a_2 & a_1 & a_0 & \\
\hline
b_3 & a_3b_3 & a_2b_3 & a_1b_3 & a_0b_3 & x^3 \\
b_2 & a_3b_2 & a_2b_2 & a_1b_2 & a_0b_2 & x^2 \\
b_1 & a_3b_1 & a_2b_1 & a_1b_1 & a_0b_1 & x \\
b_0 & a_3b_0 & a_2b_0 & a_1b_0 & a_0b_0 & x^0
\end{array}$$

$\vec{a}$ ortogonale a $\overleftarrow{b} = (b_3 b_2 b_1 b_0)$

$\Rightarrow$ Il polinomio generatore di $\mathcal{C}^{\perp}$ è $h^*(x) = x^k \cdot h(x^{-1})$

corrisponde a h

$(3,4,7)$ $\quad 3 + 4x + 7x^2$

$(7,4,3)$ $\quad 7 + 4x + 3x^2$

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

La matrice di controllo H è data

$$H = \begin{bmatrix} & & & \underbrace{h_k \; \cdots \; h_1 \; h_0}_{\text{coefficienti di } h^*(x)} \\ & & h_k \; \cdots \; h_1 \; h_0 & \\ & h_k \; \cdots \; h_1 \; h_0 & & \\ \iddots & \iddots & & \\ h_k \; \cdots \; h_1 \; h_0 & & & \end{bmatrix}$$

Esempio. (6.4.2)

$$\begin{cases} n = 2^3 - 1 = 7 \\ \underbrace{n-k = 3}, \quad k = 4 \end{cases}$$

$$\frac{m(x) = x^{\overset{n-k}{3}} + x + 1 \quad (\text{in } GF(2))}{C(7,4)}$$

$$\begin{array}{ccccccc} x^0 & x^1 & x^2 & x^3 & x^4 & x^5 & x^6 \\ (1 & 1 & 0 & 1 & 0 & 0 & 0) \end{array}$$

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$k \times n$

4×7

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \quad (n-k) \times n$$

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

$x^7 + 1 \equiv$

(mod $x^7 - 1$)

$\rightarrow h(x) = x^4 + x^2 + x + 1$

$\#$

$h^*(x) = 1 + x^2 + x^3 + x^4$

$= (10111)$