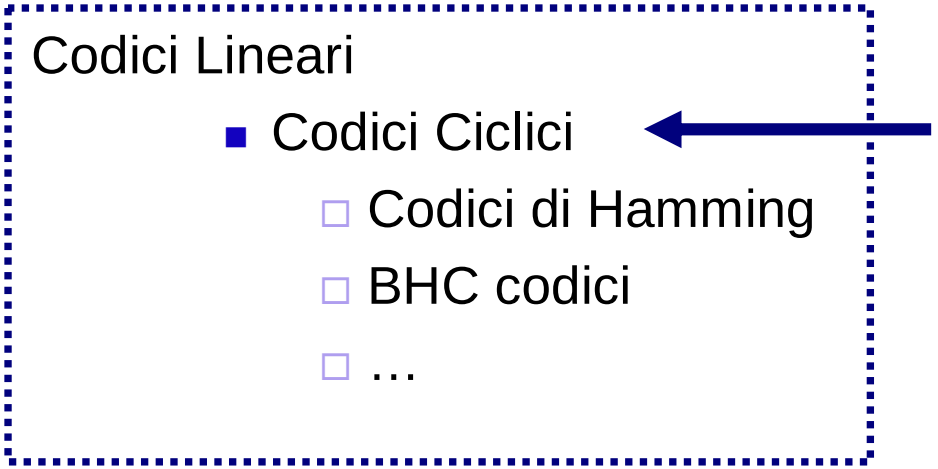
Codici Ciclici

Chiara Gasparri

Codici ciclici



- Nei codici ciclici le matrice generatrice e di controllo sono sostituite da polinomi
- **Definizione**. Un codice lineare C di lunghezza n si dice ciclico se, applicando ad una qualsiasi parola c una permutazione circolare di un posto a destra π(c), si ottiene un'altra parola di C

Rappresentazione algebrica

Possiamo dare una rappresentazione algebrica dei codici ciclici attraverso l'uso di polinomi.

Consideriamo l'insieme P(x) dei polinomi in x a coefficienti {1,0}

Ad ogni n-pla binaria $c = (c_0, c_1, \ldots, c_{n-1})$

associamo il polinomio $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1})$

Ogni codice ciclico di lunghezza n può essere rappresentato come un sottoinsieme di P(x), i cui elementi hanno grado al più n-1

Rappresentazione algebrica

Definita la relazione di congruenza $f(x) \equiv p(x)(\mathrm{mod}\, h(x))$

E scegliendo come modulo il polinomio $x^n + 1$ otteniamo l'insieme $P_n(x)$ di tutti i polinomi di P(x) aventi al più grado (n-1)

Su $P_n(x)$ definiamo l'addizione e la moltiplicazione $(\mathrm{mod}(x^n + 1))$ ottenendo così uno spazio vettoriale

- L'applicazione che ad ogni $c = (c_0, c_1, \ldots, c_{n-1})$ associa $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$

È un isomorfismo tra gli spazi vettoriali $V = \{0,1\}^n$ e $\mathrm{P_n}(x)$

Codici Ciclici – alcuni teoremi

Teorema. Sia C un codice lineare ciclico e sia f(x) una parola di C.

Allora il polinomio $a(x) f(x) \bmod(x^n + 1)$ è ancora una parola del codice C, qualsiasi sia il polinomio a(x) di $P_n(x)$

Dimostrazione. Sia $a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$

Allora in $P_n(x)$ si ha $a(x) f(x) = (a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) f(x) =$

$= a_0 f(x) + a_1 x f(x) + \ldots + a_{n-1} x^{n-1} f(x)$

Essendo gli $a_i \in \{0,1\}$ ogni $a_i x^i f(x)$ è zero oppure è uno shift di f(x), quindi ogni addendo è una parola di C. Inoltre, essendo C lineare, la somma degli elementi di C è un elemento di C.

Il teorema è dimostrato.

Lemma. Sia C un codice lineare ciclico. Allora in C c'è un unico polinomio g(x) non nullo, di grado minimo

Polinomio generatore

Definizione. Definiamo polinomio generatore di un codice ciclico C un polinomio g(x) di C non nullo e di grado minimo

---

Teorema. Un polinomio c(x) di $P_n(x)$ è in C se e solo se è multiplo di g(x) secondo un polinomio a(x) di $P_n(x)$ cioè se e solo se c(x) = a(x) g(x)

Teorema. Sia C un codice ciclico di lunghezza n e sia g(x) il suo polinomio generatore. Se grado(g(x))= n-k allora

1. c(x) è un polinomio di C sse c(x) = a(x) g(x) , essendo grado (a(x))< k
2. I polinomi g(x), x g(x), …. x^{k-1} g(x) costituiscono una base per C
3. C ha dimensione k, quindi è un (n, k)-codice

Matrice generatrice e polinomio di controllo

- Dai teoremi dimostrati e dalla definizione di matrice generatrice si evince che dato un polinomio generatore di un (n,k)-codice ciclico C, la matrice generatrice di C è

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

- Definiamo anche il polinomio di controllo di C come quel polinomio h(x) tale che

$$g(x)h(x) = x^n + 1$$

Codifica nei codici ciclici

È più semplice dal punto di vista computazionale, dato che usiamo operazioni su polinomi invece che su matrici

- Ad un messaggio $m = a_0, a_1, \ldots, a_{n-1}$
- Associamo il **polinomio messaggio** $m(x) = (a_0 + a_1 x + \ldots + a_{n-1} x^{n-1})$
- Che a sua volta può essere codificato nella parola c(x)=m(x)g(x)

E' possibile utilizzare il polinomio di controllo e verificare che c(x) è una parola di C dalla proprietà c(x) h(x) = 0

Alcuni codici ciclici

- I **codici di Hamming** sono $(2^r - 1, 2^r - 1 - r)$-codici ciclici e sono generati dal polinomio minimo $m_\alpha(x)$ di un elemento primitivo α di $GF(2^r)$

  I codici di Hamming sono di notevole importanza in quanto 1-correttori perfetti e presentano uno schema di decodifica molto semplice

---

- I **BCH codici** sono codici pluricorrettori con uno schema di decodifica semplice

  Rappresentano una classe molto vasta in quanto per ogni intero positivo r e per ogni intero positivo t con $k \geq n - rt$ esiste un BCH codice di lunghezza pari a $n = 2^r - 1$ che è t-correttore ed ha dimensioni $k \geq n - rt$