Prof. Lidia Angeleri
Università di Verona, 2008/2009
Corso di Laurea in Matematica Applicata

Algebra Computazionale

Modulo 1 : Programma svolto

§1. Codici lineari e matrici generatrici

1.1 Esempi di campi finiti: $\mathbb{F}_2, \mathbb{F}_3$

1.2 Codici

1.3 Matrici generatrici, forma standard

1.4 Codici equivalenti

1.5 Teorema: A meno di equivalenza si può assumere la matrice generatrice in forma standard

1.6 Esempio: codice binario a ripetizione

1.7 Esempio: Codice di Hamming $\mathcal{H}_3$

1.8 Esempio

§2. Codici duali e matrici di parità

2.1 Proposizione

2.2 Codice duale, matrice di parità

2.3 Teorema: determinare la matrice di parità a partire dalla matrice generatrice in forma standard

2.4 Esempio: la matrice di parità del codice binario a ripetizione

2.5 Esempio: la matrice di parità del tetracodice

2.6 Proposizione: Codici duali di codici equivalenti

§3. Pesi e distanze

3.1 Distanza, peso, distanza minima, peso minimo

3.2 Proposizione: La distanza è una metrica.

3.3 Esempio: Pesi su $\mathbb{F}_2$

3.4 Spettro dei pesi

3.5 Esempi

3.6 Teorema sullo spettro dei pesi

3.7 Osservazione: matrice di parità e pesi

3.8 Teorema: Criterio per il calcolo del peso minimo

3.9 Esempio: $\mathcal{H}_3$ ha peso minimo 3, il tetracodice ha peso minimo 3

§4. Correzione di errori

4.1 Sfera $B_r(y)$ di raggio r intorno a y

4.2 Lemma su $\mid B_r(y) \mid$

4.3 Teorema: Sfere disgiunte intorno a parole distinte

4.4 Corollario: Un codice lineare di peso minimo $d \in \{2t+1, 2t+2\}$ corregge t, ma non $t+1$, errori

4.5 Sindrome

4.6 Algoritmo SDA (syndrome decoding algorithm)

4.7 Esempio

§5. Codici di Hamming

5.1 Codice di Hamming $\mathcal{H}_r$ di lunghezza $n = 2^r - 1$

5.2 Esempio $r = 3$

5.3 Teorema: Ogni codice lineare binario $[n, n-r, 3]$ con $n = 2^r - 1$ è equivalente a $\mathcal{H}_r$

5.4 Algoritmo SDA per i codici di Hamming

§6. Il Teorema di Shannon

6.1 Esempio

6.2 Esempio

6.3 Ipotesi e notazione

6.4 Teorema (Shannon)

Bibliografia:

[1] W. C. Huffman-V.Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press

[2] J.H. van Lint, Introduction to Coding Theory, Springer (Graduate Texts in Mathematics)