ESERCIZI

1) Determinare la probabilità che in una sequenza di bit compaia:
   esattamente 1 errore
   esattamente 2 errori
   almeno 2 errori
   (5|10|05)

2) Contare i sottospazi di dimensione 0 e 1 di $\mathbb{F}_2^5$
   Contare i sottoinsiemi con 0 e 1 elementi in $\mathbb{F}_2^5$
   $A = \mathbb{F}_q$, determinare il numero di sottospazi di dimensione k in A^m
   (5|10|05)

3) Rep $(m, \mathbb{F}_2)$
   $C = \{\underline{0}, \underline{1}\} \subseteq \mathbb{F}_2^m$
   Dimostrare che C è un codice lineare
   Determinare la dimensione di C.
   (5|10|05)

4) Dimostrare che la dimensione del codice di controllo della parità C è $m-1$ anche mediante la Teoria dei codici
   Più in generale provare che se $C \leq A^m$, A campo, $|A| = m$, allora $\dim_A C = \log_{|A|} |C|$
   (19|10|05)

5) C codice di controllo della parità
   Dimostrare che $d_{min}(C) = 2$
   a) facendo vedere che $d_H(x,y) = d_H(x-z, y-z)$
   b) esibendo 2 vettori T.c. $d_H(x,y) = 2$
   c) $\nexists\, x \in C$ T.c. $d_H(x,0) = 1$
   (19|10|05)

6) Dimostrare che la relazione:
   $v \sim w \iff \exists \lambda \in K \setminus \{0\} : v = \lambda w$, $v, w \in V \setminus \{0\}$
   è di equivalenza
   (20|10|05)

7) Dimostrare che $m \leq \dfrac{p^m - 1}{p-1}$ è vera $\forall p \geq 2$, $m \in \mathbb{N}$
   (20|10|05)

8) Dimostrare che $d_{min}(Ham(2,3)) = 3$
(20/10/05)

9) $C = Ham(2,3)$
$H \in (\mathbb{F}_2)_{7\times 3}$
C è un $(7,4,3)$-codice
Dimostrare che $d_{min}(C) = 3$ e provare che C è un 1-error correcting code perfetto
(26/10/05)

10) $^- : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ (riduzione modulo 3)
Se $v \in \mathbb{Z}^{13} \Rightarrow \bar{v} \in Ker(H^t)$
Dimostrare che non è vero il viceversa
$w = (\bar{w}_1, \dots, \bar{w}_{13})$
$v = (w_1, \dots, w_{13})$ $w_i \in \mathbb{Z}$
Mostrare che $v \notin Ker A^t$
(3/11/05)

11) Calcolare $P_x(A)$ (= probabilità che usando l'algoritmo A il simbolo $x \in C$ venga decodificato in modo errato) quando $A = SS_p$ (algoritmo di decodifica) usando un canale m-ario simmetrico
$mSC(p)$, p = prob. che $x_i \to x_j$ $i \neq j$
(2/11/05)

12) a) Dimostrare che $w_{min}(C) = d_{min}(C)$
b) Calcolare $d_{min}(Rep(m, \Delta))$
c) Calcolare $d_{min}(Ham(2,3))$
(2/11/05)

13) Dimostrare che $\mathbb{C}$ e $\mathbb{R}$ sono $\mathbb{C}$-spazio vettoriale e $\mathbb{R}$-spazio vettoriale e trovare le dimensioni
(9/11/05)

14) Trovare tutte le scelte per le 4 variabili libere nel sistema che descrive $Ham(2,3)$ e determinare esplicitamente le soluzioni in 1 caso
(9/11/05)

15) Dimostrare che

$C = \{(x,y,z) \in \mathbb{F}_2^3 : x+y=0 \,,\, y+z=0\} \leq \mathbb{F}_2^3$

C è il nucleo di una particolare matrice H, $C = \ker(H)$

$$(x\ y\ z)\underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}}_{H} = (0\ 0)$$

(16/11/05)

16) • Dimostrare che esistono tante G (matrici generatrici) quante sono le basi ordinate di C

• Se $q = |\mathbb{F}|$, $k = \dim(C)$, dimostrare che

$$q^{\binom{k}{2}} = \prod_{i=1}^{k} (q^i - 1) = \prod_{i=0}^{k-1} (q^k - q^i)$$

(16/11/05)

17) $C \longrightarrow G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in (\mathbb{F}_3)_{3\times 4}$ matrice generatrice

a) Trasformare G in forma a scala (senza mutare C)

b) Trovare $\pi \in \mathrm{Sym}(4)$ t.c. $\pi(C)$ ammetta G' in forma standard

(16/11/05)

18) Dimostrare che ogni codice di Hamming $C = \mathrm{Ham}(q,m)$ è un

$$\left[\frac{q^m-1}{q-1}\,,\ \frac{q^m-1}{q-1} - m\,,\ 3\right] - \text{codice}$$

(17/11/05)

19) Contare $S_i = \{S : S \text{ insieme di righe di } H \text{ lin. dip.}, |S| = i\}$

(23/11/05)

20) a) Dimostrare che $C = \mathrm{Rep}(m,F)$ è MDS

b) Cosa succede se prendo $C = \mathrm{Ham}(2,3)$?

$C = \mathrm{Ham}(q,2)$?

(23/11/05)

21) T = Trasversa. Dimostrare che # Trasverse $= |C|^{|T|}$

(23/11/05)

22) $\varphi: \mathbb{Z} \to F$ $\qquad \varphi(\mathbb{Z}) \cong \mathbb{Z}/\ker(\varphi)$

$a + \ker(\varphi) \mapsto \varphi(a)$

Dimostrare che è un isomorfismo di anelli

(30/11/05)

23) Dimostrare che $\left(A/I, +, \cdot\right)$ è un anello commutativo con $1_{A/I}$

Per esempio $A = \mathbb{Z}$, $I = m\mathbb{Z}$

(30/11/05)

24) $I \trianglelefteq A$, $I < J \trianglelefteq A$, $\bar{A} = A/I$

Dimostrare che $\bar{J} \trianglelefteq \bar{A}$ provando che se $a \in J \Rightarrow$

$a + i \in J \quad \forall i \in I$ (chiusura rispetto alla somma)

$\bar{J} = \{a + I : a \in J\}$

(30/11/05)

25) Costruire la Tabella rispetto alla somma e al prodotto di $\mathbb{F}_4$

Dimostrare che $\mathbb{F}_4 \not\cong \mathbb{Z}/4\mathbb{Z}$

(30/11/05)

26) Determinare Tutti i generatori di $\mathbb{F}_4^*$, $\mathbb{F}_{27}^*$ e stabilire come è fatto $\mathbb{F}_8^*$

(1/12/05)

27) a) Determinare la probabilità che un generico polinomio monico di grado m su $\mathbb{F}_p$ sia irriducibile

b) Stabilire per quali valori di (p, m) Tale probabilità sia $> \frac{1}{2}$

(13/12/05)

28) $F = \mathbb{F}_3[X]/\langle X^2 + 1 \rangle$

a) Costruire la Tabella additiva di $(F, +)$

b) Dimostrare che è isomorfo (come gruppo abeliano additivo)

$(F, +) \cong \mathbb{F}_3 \oplus \mathbb{F}_3 = \mathbb{F}_3^2$

In particolare $3\beta = 0 \quad \forall \beta \in F$

(13/12/05)

29) Dimostrare che $\forall g \in G$, $|g| = m$ e $d \mid m \Rightarrow |g^d| = \frac{m}{d}$

(13/12/05)

30) Dimostrare che l'insieme delle matrici $aI + bA$, $a, b \in \mathbb{F}_3$ è isomorfo al campo $F = \mathbb{F}_3[x]/\langle x^2+1 \rangle$

(13|12|05)

31) L'insieme dei numeri complessi $\mathbb{R}[i]$ si possono leggere come:

$\mathbb{R}[x]/\langle x^2+1 \rangle$, $a+bi$, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$

(13|12|05)

32) $F = \mathbb{F}_3[x]/\langle x^2+1 \rangle = I$, $F' = \mathbb{F}_3[x]/\langle x^2+x-1 \rangle = J$

$\alpha = x + I$ $\quad$ $\beta = x + J$

$|\alpha + 1| = |\beta| = 8$

$\alpha + 1 \xrightarrow{\varphi} \beta$

a) φ è univocamente determinato dalla condizione che è un isomorfismo e che $\varphi(\alpha+1) = \beta$

b) Determinare se questa unica mappa è un isomorfismo

c) Cosa accade per le altre scelte: $2\alpha+1$, $2\alpha+2$, $\alpha+2$?

(Un elemento di questi di ordine 8 deve andare in β)

(13|12|05)

33) Dimostrare in generale questo Teorema: $\mu(m) = \mu_{(\alpha, \bar{\alpha})}(m, 1)$

(15|12|05)

34) a) Dimostrare che $\frac{m(m-1)}{2} \in \mathbb{N}$ sempre

b) Dimostrare che $\frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d \in \mathbb{N}$ senza usare il fatto che è uguale a $N_m(p)$

(15|12|05)

35) Dimostrare che la probabilità che un polinomio scelto a caso di grado m su $\mathbb{F}_p$, al variare di p, $\longrightarrow \frac{1}{m!}$

$\text{Prob}(\deg(g) = m) \longrightarrow \frac{1}{m}$

(15|12|05)

36) $\delta : V \to V$

$(e_1, \dots, e_m)$ base per V

$$J = \begin{pmatrix} \delta(e_1) \\ | \\ | \\ \delta(e_m) \end{pmatrix} = \begin{pmatrix} 0 & 1 & & * \\ | & & \ddots & \\ | & & & 1 \\ 0 & & & 0 \end{pmatrix}$$

matrice associata a δ

Determinare il polinomio caratteristico e il polinomio minimo di
(21/12/05)

37) $W = F[x]/\langle x^m - 1 \rangle = I$

Dimostrare che $\{1, x, \dots, x^{m-1}\}$ sono linearmente indipendenti in W
(21/12/05)

38) $b = \{1, x, \dots, x^{m-1}\}$

$\mu_x : W \to W$

$\overline{v} \longmapsto \overline{xv}$

Dimostrare che μ_x è una mappa lineare invertibile.
Trovare la matrice rappresentativa rispetto a b.
$\gamma(x_1, \dots, x_m) = (x_2, x_1, x_3, \dots, x_m)$
Determinare codici C t.c. $\sigma(C) = \gamma(C) = C$
$\sigma(x_1, \dots, x_m) = (x_m, x_1, \dots, x_{m-1})$
(21/12/05)

39) $C' = \gamma(C)$

$p(x) = p_0 + \dots + p_{m-1} x^{m-1}$
Dimostrare che $p(x) C' = C'$ se $p(x) \perp x^m - 1$
(22/12/05)

40) Determinare esplicitamente $\phi_m(x)$ a partire dai polinomi $x^d - 1$, $d \mid m$
(22/12/05)

41) Dimostrare che se $E \geq \mathbb{F}_q$ è un campo finito che contiene $\mathbb{F}_q$ allora $E = \mathbb{F}_{q^t}$ per qualche intero t
Dimostrare che in realtà $t = \dim_{\mathbb{F}_q} E$
(11/01/06)

42) Sia Ω un anello commutativo e sia $I \trianglelefteq \Omega$, ideale
Dimostrare che $I = \ker(\pi)$, dove $\pi : \Omega \to \Omega/I$

$r \longmapsto r + I$

Viceversa sia $\pi : \Omega \to S$ omomorfismo di anelli commutativi allora $\ker(\pi) \trianglelefteq \Omega$
(11/01/06)

(43) Sia G ciclico, $|G| = n$ e sia $d \mid n \Rightarrow \exists! H \leq G$ t.c. $|H| = d$
(Suggerimento: $G = \langle g \rangle$, $H = \langle g^{n/d} \rangle$)
(12/01/06)

(44) Sia $t = \mathrm{ord}_n(q)$, $|Z| = n \Rightarrow Z, Z^q, Z^{q^2}, \ldots, Z^{q^{t-1}}$ sono tutte distinte. Per cui $\mathrm{minim}_{\mathbb{F}_q}(Z) = \prod_{j=0}^{t-1} (x - Z^{q^j})$
(12/01/06)

(45) Perché gli unici 2 polinomi irriducibili: $Z = N_3(Z)$ compaiono nella fattorizzazione in $x^7 - 1$
(18/01/06)

ESERCIZI (MAPLE)

1) Scrivere in Java e in Maple un programma che data una cinta conta il numero di occorrenze di 1 e 0.
Due procedure:
- Contare l'occorrenza prima di 0 e poi di 1
- Contare l'occorrenza di un solo bit e poi sottrarla dal totale di bit per trovare il numero di occorrenze dell'altro bit.

Determinare quale è il tempo di esecuzione più veloce.
(6|10|05)

2) Scrivere una funzione che data una cinta e mi fornisce la prima posizione in cui compare un dato simbolo a_i
(e se non compare?)
INPUT: $c = [a_1, \dots, a_m]$
(13|10|05)

3) Scrivere un programma che mi restituisce la matrice H del codice di controllo della parità
(20|10|05)

4) Scrivere un programma che costruisce H.
Ottenere il nucleo di H. (Maple usa le righe o le colonne?)
Determinare l'insieme: $\{ d_H(\underline{x}, \underline{0}) : x \in C \}$
(27|10|05)

5) Modificare il codice di Hamming, lavorando in $\mathbb{F}_p$, cioè non lavorando con la matrice A ma direttamente con la matrice H
(3|11|05)

6) Quale ordine viene usato nella costruzione del prodotto cartesiano $A \times B$, A, B cinte ordinate?
(10|11|05)

7) Si può modificare l'istruzione: cod := [op(cod), v] ?
(10|11|05)

8) per i := [1,2,6,3,5,4];
P := proc(i,j)
if per[i] = j then return 1;
else return 0;
Pi;
end;
P := Hod(p, Matrix(m,m,P), integer[]);

a) Generalizzare ad ogni caso la costruzione di per
per $\rightarrow$ P

b) Si può usare P per ottenere la matrice di controllo per C?
(17111105)

9) Modificare il codice che prende un vettore, lo Trasla, e calcola il peso minimo del vettore Traslato, in modo che funzioni qualunque sia il livello del codice di Hamming e il primo
(24111105)

10) a) Modificare il codice per la costruzione dei Coset Leaders in modo che si possa applicare ad ogni $C \leq \mathbb{F}_p^m$

b) Dimostrare che se C = Ham(2,3) ed esiste $t \in e + C$ con $w_H(t) = 1 \Rightarrow t$ è l'unico elemento con questa proprietà in $e + C$

c) Far variare e in modo casuale e costruire Coset Leaders per ottenere $t : w_H(t) = \min\{w_H(e+c) : c \in C\}$
Avviene sempre che $w_H(t) = \begin{cases} 1 \\ 0 \end{cases}$?

d) Come faccio a costruire una Trasversa di C in V?
(24111105)