TRENTO, A.A. 2020/21
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 10

Esercizio 10.1. Definite la distanza di Hamming d su $\mathbf{F}_2^n$, e mostrate che soddisfa, per $a, b, c \in \mathbf{F}_2^n$,

(1) $d(a, b) = 0$ se e solo se $a = b$.
(2) $d(a, b) = d(b, a)$.
(3) $d(a, b) \leq d(a, c) + d(c, b)$.
(4) $d(a, b) = d(a - b, 0)$.

Esercizio 10.2. Sia $\mathcal{C}$ un codice lineare binario, e si definisca la sua distanza minima come

$$d(\mathcal{C}) = \min \{ d(a, b) : a, b \in \mathcal{C}, a \neq b \} .$$

Si mostri che

$$d(\mathcal{C}) = \min \{ d(a, 0) : a \in \mathcal{C}, a \neq 0 \} .$$

Esercizio 10.3. Per un codice lineare, si dica cos'è una matrice del codice, cos'è una matrice di controllo della parità.

Esercizio 10.4. Si diano matrici del codice e matrici di controllo di parità per i seguenti codici lineari binari.

(1) Il codice a ripetizione due volte.
(2) Il codice a ripetizione tre volte.
(3) Il codice a controllo di parità in generale. Dunque per $n \geq 1$ la codifica è la funzione lineare

$$\begin{aligned} \mathbf{F}_2^n &\to \mathbf{F}_2^{n+1} \\ [x_1, \dots, x_n] &\mapsto [x_1, \dots, x_n, x_1 + \cdots + x_n] \end{aligned}$$

Notate in particolare che per $n = 1$ si ha il codice a ripetizione due volte.

Esercizio 10.5. Sia $\mathcal{C}$ un codice lineare binario, e sia $\mathcal{H}$ la sua matrice di controllo di parità.

(1) Mostrate che $\mathcal{C}$ rivela un errore (cioè il ricevente si accorge se c'è stato un errore) se e solo se
   (a) $d(\mathcal{C}) > 1$, ovvero
   (b) le colonne di $\mathcal{H}$ sono tutte diverse da zero.
(2) Mostrate che $\mathcal{C}$ corregge un errore (cioè il ricevente si accorge se c'è stato un errore, ed è in grado di individuare il bit in cui è avvenuto, e dunque di correggerlo) se e solo se
   (a) $d(\mathcal{C}) > 2$, ovvero
   (b) le colonne di $\mathcal{H}$ sono tutte diverse da zero, e distinte fra loro.