TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 11

Esercizio 11.1. Sia $V = F^n$ lo spazio delle n-ple sul campo $F = \mathbf{Z}/2\mathbf{Z}$. Per $a, b \in V$, si ponga la distanza (di Hamming) fra a e b pari a

$$d(a,b) = |\{\, i : a_i \neq b_i \,\}|$$

(Sto usando la solita convenzione che $a = [a_0, a_1, \ldots, a_{n-1}]$, cioè che la componente i-sima di un vettore a è a_i.)

Si mostri che valgono le proprietà seguenti, per $a, b, c \in V$.

(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) $d(a,b) = d(a-b, 0)$.

In realtà tutto quanto vale qualunque sia il campo F.

Esercizio 11.2. Il *codice a controllo di parità* generale funziona cosí. Il mittente vuole trasmettere una successione arbitraria di bit. La spezza in una successione di vettori lunghi $n-1$, dunque elementi di $\mathbf{F}_2^{n-1}$. (Qui $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z} = \{\, 0, 1 \,\}$.) Poi aggiunge un bit di controllo, usando la funzione

$$\mathbf{F}_2^{n-1} \to \mathbf{F}_2^n$$
$$a = [a_1, \ldots, a_{n-1}] \mapsto [a_1, \ldots, a_{n-1}, a_1 + \cdots + a_{-1n}].$$

Come nel caso particolare $n = 3$ visto a lezione, l'immagine $\mathcal{C}$ di questa funzione lineare consiste dei vettori di $\mathbf{F}_2^n$ che hanno un numero pari di 1.

Si mostri che il codice a controllo di parità $\mathcal{C}$ *rivela un errore*, nel senso che se $a \in \mathcal{C}$, e cambio *una* componente di a, ottenendo un vettore b, allora $b \notin \mathcal{C}$

Esercizio 11.3. Si scrivano matrici del codice, e matrici a controllo di parità per

(1) il codice a ripetizione 2 volte,
(2) il codice a ripetizione 3 volte,
(3) il codice a controllo di parità $\mathbf{F}_2^{n-1} \to \mathbf{F}_2^n$ per $n = 2, 3$, e per n generico.

Esercizio 11.4. Sia $\mathcal{C} \subseteq \mathbf{F}_2^n$ un codice lineare.

Si mostri che

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

Questo numero si chiama la *distanza minima* del codice.

Esercizio 11.5. Sia $\mathcal{C} \subseteq \mathbf{F}_2^n$ un codice lineare.

(1) Si mostri che sono equivalenti
- $\mathcal{C}$ rivela un errore, e
- la distanza minima di $\mathcal{C}$ è > 1.

(2) Si mostri che sono equivalenti
- $\mathcal{C}$ corregge un errore, e
- la distanza minima di $\mathcal{C}$ è > 2.

Esercizio 11.6. Il codice ISBN-10 era usato fino a tutto il 2006 per identificare i libri pubblicati. Consiste di 10 cifre decimali (l'ultima può anche essere una `X`). Le prime 9

$$a_1, a_2, \ldots, a_9$$

identificano il libro. La decima è calcolata come il resto della divisione per 11 di

$$\sum_{i=1}^{9} i \cdot a_i = 1 \cdot a_1 + 2 \cdot a_2 + \cdots + 9 \cdot a_9.$$

(Se il resto è 10, si scrive `X`.)

Si mostri che il codice ISBN-10 rivela un errore (cioè se cambio una cifra di un codice valido, ottengo un codice non valido), e rivela anche lo scambio di due cifre.