TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 9

Esercizio 9.1. Per un codice lineare, si dica cos'è una matrice del codice, cos'è una matrice di controllo della parità.

Esercizio 9.2. 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

$$\mathbf{F}_2^n \to \mathbf{F}_2^{n+1}$$
$$[x_1, \ldots, x_n] \mapsto [x_1, \ldots, x_n, x_1 + \cdots + x_n]$$

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

Esercizio 9.3. 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.

Esercizio 9.4. Si costruisca il codice di Hamming sul campo con 8 elementi, usando prima uno poi l'altro dei due polinomi irriducibili di grado 3 su $\mathbf{F}_2$.

Si mostri come avviene la codifica, e si dia un paio di esempi di codifica e di decodifica.

Si mostri che questi codici sono ciclici, nel senso che se $\mathcal{C}$ è uno di essi, allora

$$[a_6, a_5, a_4, a_3, a_2, a_1, a_0] \in \mathcal{C} \quad \text{implica} \quad [a_5, a_4, a_3, a_2, a_1, a_0, a_6] \in \mathcal{C}.$$

Che legame c'è fra i due codici ottenuti?

Esercizio 9.5 (Questo è del tutto opzionale). Si costruisca il codice di Hamming sul campo con 16 elementi, usando prima l'uno e poi l'altro dei due polinomi irriducibili primitivi di grado 4 su $\mathbf{F}_2$. (Dunque i polinomi sono $x^4 + x + 1$ e $x^4 + x^3 + 1$.)

Si mostri come avviene la codifica, e si dia un paio di esempi di decodifica.

Esercizio 9.6. Si mostri che il codice di Hamming sul campo con 4 elementi, ovvero quello basato sull'unico polinomio irriducibile di grado 2 in $\mathbf{F}_2[x]$ (ovvero su un elemento α tale che $\alpha^2 + \alpha + 1$) è il codice a ripetizione 3 volte.