Teoria de la Informació GCED-UPC curs 2019/20
Problemes; full número 6

26 de novembre de 2019

6.1. Demostreu la *fita de Singleton*: tot codi q-ari $\mathcal{C}$ de longitud n i distància mínima d conté un nombre de paraules M que satisfà la desigualtat

$$M \leqslant q^{n-d+1},$$

i deduïu que si el codi és lineal de dimensió k aquesta fita equival a $d \leqslant n - k + 1$.
INDICACIÓ: Considereu el conjunt de paraules obtingudes traient les $d - 1$ últimes lletres de la paraula del codi. En el cas de codis lineals es pot demostrar usant àlgebra lineal.

6.2. Considereu el codi binari lineal amb base `11011,11100,11111`.

1. Doneu els seus paràmetres: longitud, dimensió i distància mínima.
2. Quina és la seva capacitat correctora i detectora?
3. Doneu la matriu generadora corresponent a aquesta base i calculeu la matriu de control associada.
4. Codifiqueu les paraules `000` i `111` amb la matriu generadora anterior i descodifiqueu les paraules del codi `00100` i `11111`.
5. Digueu quines són les síndromes i trobeu els errors de probabilitat màxima corresponents a cadascuna (coset leaders).
6. Si es reben les paraules amb errors `00001` i `01110`, quines són les paraules del codi amb probabilitat més alta d'haver estat enviades?
7. Doneu una matriu generadora sistemàtica d'un codi equivalent i la matriu de control corresponent.

6.3. Trobeu una matriu generadora sistemàtica del codi de Hamming de longitud 15.

6.4. Doneu la matriu de control d'un codi de Hamming que permet descodificar canviant el bit que indica la seva síndrome, interpretada com un enter escrit en base 2.

6.5. Sigui $\mathcal{C} \subseteq \{0,1\}^n$ un codi binari lineal de longitud n, dimensió k i distància mínima d. S'anomena *extensió parell* de $\mathcal{C}$ el codi que s'obté afegint a cada paraula del codi $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ un bit de paritat $c_{n+1} = \sum_{i=1}^{n} c_i$.

Comproveu que aquesta extensió és un codi lineal i determineu la seva longitud, dimensió i distància mínima en funció de les de $\mathcal{C}$.

6.6. Sigui $\mathcal{C} \subseteq \{0,1\}^7$ el codi lineal format pels vectors que són solució del sistema lineal

$$X_2 + X_4 + X_6 = X_1 + X_2 + X_4 = X_5 + X_6 + X_7 = 0.$$

Calculeu la seva dimensió i distància mínima i calculeu també la dimensió i la distància mínima del seu codi ortogonal $\mathcal{C}^\perp$.

6.7. Sigui $\mathcal{C} \subseteq \{0,1\}^n$ un codi binari lineal de longitud n, dimensió k i distància mínima d. Es consideren els codis de longitud n següents:

1. les paraules parells del codi $\mathcal{C}_{\text{ev}} = \{\boldsymbol{x} = (x_i) \in \mathcal{C} : \sum x_i = 0\}$;
2. les paraules senars del codi $\mathcal{C}_{\text{odd}} = \{\boldsymbol{x} = (x_i) \in \mathcal{C} : \sum x_i = 1\}$;
3. les paraules complementaries de les del codi $\mathcal{C}_{\text{comp}} = \{\overline{\boldsymbol{x}} = (1 - x_i) : \boldsymbol{x} = (x_i) \in \mathcal{C}\}$.

Discutiu, per a cadascun d'aquests tres codis si són o no lineals, el nombre de paraules que contenen en funció del nombre de paraules de $\mathcal{C}$ i què es pot dir de la seva distància mínima en funció de la de $\mathcal{C}$.

6.8. Sigui $\mathbb{F}$ un cos finit de q elements. Per a cada enter $m \geqslant 2$ es defineix el codi de Hamming amb paràmetre m com un codi que té matriu de control de paritat amb columnes que siguin generadors de tots els subespais de dimensió 1 de l'espai $\mathbb{F}^m$ (rectes que passen per l'origen).

1. Doneu els paràmetres d'aquest codi: longitud, dimensió i distància mínima.
2. Trobeu una matriu generadora d'un codi de Hamming sobre $\mathbb{Z}_3$ amb paràmetre $m = 2$.

6.9. Feu les taules de sumar i de multiplicar del cos finit $GF(7)$ de 7 elements.

6.10. Considereu el cos finit $\mathbb{F} = GF(2)$ de 2 elements. A l'anell de polinomis $\mathbb{F}[X]$ (polinomis binaris) es considera el polinomi $P(X) = X^3 + X + 1$ i es consideren les operacions de sumar i multiplicar mòdul P, definides exactament igual que amb les congruències de nombres enters.

- Comproveu que el polinomi P és primer.
- Feu una taula amb les operacions de sumar i multiplicar al conjunt de les classes de congruència mòdul P, que es poden representar com els 8 polinomis de grau $\leqslant 2$:

$$\mathbb{F}_8 = \{0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1\}.$$