

## Problemes: Codis II. Codis cíclics.

**VI.1.** Considerem el conjunt  $C$  de paraules binàries de longitud  $n$  i pes parell.

- (a) Demostreu que  $C$  és un codi lineal.
- (b) Quina és la distància mínima de  $C$ ? Per què?
- (c) Quants errors pot corregir  $C$ ? I quants esborralls?
- (d) Si es rep la paraula  $000 \dots 001?10$ , podríeu dir justificadament quin dígit correspon a l'esborrall?
- (e) Demostreu que  $C$  és un codi cíclic.
- (f) Doneu-ne el polinomi generador i una matriu generadora.
- (g) Doneu-ne el polinomi de control i una matriu de control.
- (h) Quin és el codi dual?

**VI.2.** Sigui  $\alpha$  un element primitiu del cos  $\mathbb{F}_{2^m}$ .

Considerem el codi binari cíclic de longitud  $n$ , on  $n = 2^m - 1$ , que té per polinomi generador  $g(x)$ , el qual s'anul·la sobre  $\alpha$  i també sobre  $\alpha^{-1}$ .

Demostreu que la distància mínima del codi anterior és 5 (com a mínim).

- VI.3.**
- (a) Descomponeu  $x^7 - 1$  en factors irreductibles sobre el cos  $\mathbb{F}_2$  i determineu tots els codis cíclics binaris de longitud 7.
  - (b) Quants codis cíclics ternaris hi ha de longitud 8?
  - (c) Suposem que  $x^n - 1$  és el producte de  $t$  polinomis irreductibles diferents sobre  $\mathbb{F}_q$ . Quants codis cíclics de longitud  $n$  hi ha sobre  $\mathbb{F}_q$ ?

- VI.4.**
- (a) Demostreu que  $(x + y)^p = x^p + y^p$  a  $\mathbb{F}_{p^n}$ .
  - (b) Quants codis cíclics 5-aris de longitud 10 hi ha? Descriviu detalladament de quina forma són els seus polinomis generadors.
  - (c) Quants codis cíclics 5-aris de longitud 10 i dimensió 6 hi ha? Justifiqueu-ho.

- VI.5.**
- (a) Demostreu que  $\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + 1$ .
  - (b) Quins són els codis cíclics binaris de dimensió 1? I els de codimensió 1?

**VI.6.** Considerem un codi cíclic  $C$  de longitud  $n$ , dimensió  $k$  i distància mínima  $d$ , i amb polinomi generador  $g(x)$ .

- (a) Suposem que existeixen  $m$  posicions seguides d'una paraula no nul·la de  $C$  fora de les qual tots els valors són 0. Demostreu que necessàriament  $m \geq n - k + 1$ .
- (b) Demostreu que una paraula no nul·la de  $C$  tindrà, com a màxim,  $k - 1$  posicions nul·les seguides.
- (c) Suposem que existeixen  $n - k + 1$  posicions seguides d'una paraula no nul·la fora de les quals tots els valors són 0. Demostreu que en aquest cas els valors en aquestes posicions són els coeficients d'un polinomi que és un múltiple escalar de  $g(x)$ .
- (d) Doneu una demostració alternativa de la fita de Singleton per codis cíclics.

- (e) Demostreu que, en una matriu generadora sistemàtica en les primeres posicions, l'última fila conté els coeficients del polinomi  $g(x)/g_0$ , on  $g_0$  és el coeficient constant de  $g(x)$ .
- (f) En una matriu generadora sistemàtica en les últimes posicions, la primera fila conté els coeficients del polinomi  $g(x)$ . Demostreu-ho de tres maneres diferents: pel mètode dels pivots, pel sistema de codificació sistemàtica a través de la divisió de polinomis i pels primers apartats.
- (g) \* Demostreu que els únics codis cíclics binaris separables a màxima distància són el codi de repetició i el de paritat.

**VI.7.** Descriviu tots els codis ternaris cíclics de longitud 18.

- VI.8.**
- (a) És la intersecció de dos codis cíclics (de la mateixa longitud i definits sobre el mateix alfabet) un codi cíclic? I la unió?
  - (b) Donats dos codis cíclics de longitud  $n$  amb polinomis generadors  $g_1(x)$  i  $g_2(x)$ , descriuiu el màxim codi cíclic contingut pels dos.
  - (c) Donats dos codis cíclics de longitud  $n$  amb polinomis generadors  $g_1(x)$  i  $g_2(x)$ , descriuiu el mínim codi cíclic que els conté tots dos.
  - (d) Concreteu els dos apartats anteriors pel cas de codis ternaris cíclics de longitud 18.

**VI.9.** Sabem que el polinomi  $x - 1$  divideix  $x^{q-1} - 1$  a  $\mathbb{F}_q$  per tot  $q$ . Per tant, ha de ser el polinomi generador d'un codi cíclic primitiu de  $\mathbb{F}_q$ .

- (a) Doneu-ne una matriu generadora en forma de cascada i una de control.
- (b) Quin és el seu codi dual?