Pràctica 2: Codis Cíclics

1. Primer repassarem com treballar amb paraules-codi i polinomis sobre $GF(2)$. Executeu les següents instruccions i observeu el resultat obtingut.

   (a) Necessitem definir un cos base: `F2=GF(2); F2`.

   (b) Es pot definir una paraula-codi com un vector: `v=vector(GF(2),[1,0,1,1]); v`

   (c) I convertir un vector a una llista: `v.list()`.

   (d) Podem definir una matriu,
   `G = matrix(F2, [(0,1,0,1,0),(0,1,1,1,0),(0,0,1,0,1),(0,1,0,0,1)]); G`

   (e) I el codi lineal amb aquesta matriu generadora: `C=LinearCode(G); C`

   (f) Construcció de l'anell de polinomis sobre $GF(2)$: `Z2X.<x>=PolynomialRing(F2); Z2X`.

   (g) Definir un polinomi amb coeficients a $GF(2)$: `pX=Z2X(1+x^2+x^3), pX`.

   (h) Alternativament: `pX=Z2X([1,0,1,1])`.

   (i) Desplaçament dels coeficients d'un polinomi (multiplicar per `x^2`): `pX.shift(2)`.

   (j) També en l'altre sentit (dividir per `x`), `pX.shift(-1)`.

   (k) Operar amb polinomis: `qX=pX*(x+1); qX`.

   (l) Comprovar si un polinomi és irreductible: `pX.is_irreducible(), qX.is_irreducible()`.

   (m) I si no ho és, descomposar-lo en factors: `qX.factor()`.

   (n) Construir un codi cíclic de longitud 3 i polinomi generador `x+1`: `C=CyclicCode(x+1,3); C`.

   (o) Veure el conjunt de paraules d'un codi: `S = set(C.list()); S`.

2. a) Considereu la paraula-codi determinada per la llista de bits: `[1,0,1,1]`. Definiu la funció `UAB_right_shift(n,L)` que permeti obtenir un cíclic shift de n ($n \geq 0$) posicions de la llista `L`. Per exemple, `UAB_right_shift(1,[1,0,1,1])=[1,1,0,1]`. (**1 punt**)

   b) A partir d'aquesta funció construïu el codi lineal generat pels desplaçaments cíclics del vector `v=(0,0,1,1,0,1,0)` i comproveu que el conjunt amb les paraules generades per aquest codi lineal és equivalent al conjunt amb les paraules generades pel codi cíclic de longitud 7 generat pel polinomi `1+x+x^3`. Calculeu també la longitud, la dimensió i la distància mínima d'aquest codi. (**1 punt**)

3. Existeix un codi binari cíclic de longitud 15 amb polinomi generador `g(x)=1+x+x^4`? i amb polinomi generador `g(x)=1+x^2+x^3`? Justifiqueu la resposta. (**1 punt**)

4. Quants codis cíclics binaris de longitud 15 hi ha? Feu en Sage el càlculs necessaris per trobar aquest nombre. (**1 punt**)

5. Quin és el menor codi cíclic de longitud 15 que conté la paraula codi
   `v=(1,1,0,1,1,0,0,0,0,0,0,0,0,0,0)`? (**1 punt**)

6. Considereu el codi binari cíclic de longitud 15 generat pel polinomi `g(x)=1+x+x^4`. Calculeu el polinomi de control de `g(x)`, `h(x)`, i el polinomi recíproc de `h(x)`, `h*(x)`. (**1 punt**)

7. a) Dissenyeu una funció `UAB_gen_matrix(g,n)` que, a partir del polinomi generador `g` d'un codi cíclic i la seva longitud `n`, calculi la seva matriu generadora. (**1 punt**)

   b) Doneu la matriu generadora dels codis cíclics de longitud 15 i polinomis generadors $g_1(x) = 1 + x + x^4$ i $g_2(x) = x^6 + x^5 + x^4 + x^3 + 1$. (**1 punt**)

8. a) Dissenyeu una funció `UAB_con_matrix(g,n)` que, a partir del polinomi generador `g` d'un codi cíclic i la seva longitud `n`, calculi la seva matriu de control. (**1 punt**)

   b) Trobeu la matriu de control dels codis cíclics de longitud 15 de l'exercici anterior. (**1 punt**)