TCI - Exercicis Codificació

Exercici 1.1. Sigui C el codi binari format per totes les paraules de longitud 7 tals que el tercer bit és un bit de paritat dels dos primers, el sisè és un bit de paritat dels bits quart i cinquè i el darrer bit és un bit de paritat dels dos anteriors. Proveu que C és lineal. Descriviu aquest codi mitjançant equacions i determineu quants errors pot detectar i corregir

Exercici 1.2. Un codi lineal binari de longitud 8 està definit per les equacions següents:

$$\begin{aligned} x_5 &= x_2 + x_3 + x_4 \\ x_6 &= x_1 + x_2 + x_3 \\ x_7 &= x_1 + x_2 + x_4 \\ x_8 &= x_1 + x_3 + x_4 \end{aligned}$$

Trobeu la seva matriu de control, determineu el nombre de paraules de pes i, $(0 \leq i \leq 8)$ i proveu que la distància mínima d'aquest codi és 4

Exercici 1.3. Determineu totes les paraules, la distància mínima i una matriu de control del codi binari lineal $(5,3)$ definit per la matriu generadora

$$G := \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Exercici 1.4. Trobeu una matriu generadora del codi lineal que té per matriu de control la següent:

$$H := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Exercici 1.5. Un codi lineal té la següent matriu de paritat:

$$H := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & a_{1,6} \\ 1 & 1 & 0 & 0 & 0 & a_{2,6} \\ 1 & 0 & 1 & 0 & 0 & a_{3,6} \\ 0 & 1 & 1 & 1 & 0 & a_{4,6} \end{pmatrix}$$

(a) Doneu totes les paraules del codi quan $a_{1,6} = 0, a_{2,6} := 1, a_{3,6} := 1$ i $a_{4,6} := 0$

(b) Demostreu que es poden triar $a_{1,6}, a_{2,6}, a_{3,6}, a_{4,6}$ de manera que el codi corregeixi els errors simples i detecti els dobles, però que aquests no poden ser corregits

Exercici 1.6. Considerem el codi lineal que té per matriu generadora la matriu

$$G := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

(a) Comproveu que aquest codi no és sistemàtic

(b) Trobeu un codi sistemàtic equivalent a l'anterior

(c) Codifiqueu el missatge 101 amb el codi inicial i el que heu trobat a l'apartat anterior

Exercici 1. 7. Comproveu que els codis lineals definits per les matrius generadores següents són equivalents:

$$G_1 := \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad G_2 := \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Exercici 1.8. Considereu el codi descrit per la matriu de codificació següent:

$$G := \left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

(a) Doneu una matriu de control (H) del codi

(b) Trobeu la distància mínima del codi i expliqueu per a quines funcionalitats es pot utilitzar una tal distància

Exercici 1.9. Considerem el codi lineal que té per matriu de control

$$H := \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Descodifiqueu la paraula $z := (11111111)$. Quants errors conté? Quina és la capacitat correctora del codi? Feu un breu comentari

Exercici 1.10. Calculeu les síndromes i els líders del codi de repetició de longitud 5

Exercici 1.11. Un codificador transforma els parells de bits d'informació $00, 01, 10, 11$ respectivament en les successions $00000, 01101, 10111, 11010$

(a) Demostreu que aquest codi és lineal i expresseu cada dígit del codi en funció dels bits d'entrada

(b) Doneu una matriu generatriu i una matriu de paritat del codi

(c) Doneu els líders de les classes laterals del codi

Exercici 1.12. Un codi binari lineal C ve donat per la matriu de control següent:

$$H := \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Si s'ha rebut la paraula $y := 01001$, quin és, amb més probabilitat, el missatge enviat?

Exercici 1.13. Sigui C el codi binari de matriu generadora

$$G := \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

(a) Escriviu totes les paraules del codi

(b) Calculeu-ne la distància mínima i els errors que pot corregir

(c) Dins de la capacitat correctora del codi, trobeu els líders de les classes laterals i les corresponents síndromes

(d) Corregiu, si cal, el missatge 001100010001

Exercici 1.14. Considereu la matriu de codificació següent:

$$G := \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

(a) Doneu els paràmetres del codi (n, k, r)

(b) Trobeu una matriu de control H

(c) Trobeu la distància mínima del codi

Exercici 1.15. Considereu el codi descrit per la següent matriu de control

$$H := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

(a) Doneu els paràmetres del codi

(b) Doneu una matriu de codificació sistemàtica (si exiteix; si no, la doneu no sistemàtica)

(c) Amb l'anterior matriu codifiqueu el missatge format exclusivament per 1's: $(1, \ldots, 1)$

(d) Trobeu la distància mínima del codi

(e) Construïu una taula (per descodificar) per corregir patrons de fins 1 error

(f) Amb la taula de l'apartat anterior estimeu els errors que ha introduït el canal en les paraules següents: 011001, 111110, 111111

Exercici 1.16. Considerem el codi C que té per matriu de control associada

$$H := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

(a) Feu una taula de síndromes/errors estimats per a totes les síndromes corresponents a patrons d'un únic error i descodifiqueu les paraules (10011), (11110), (00101)

(b) Trobeu un codificador sistemàtic per a C

Exercici 1.17. Siguin $K := \mathbb{F}_2[D]/(D^3 + D^2 + D)$ i α la classe de D. Calculeu els productes que s'indiquen a continuació i deduïu que K no és un cos:

(a) $(\alpha^2 + \alpha)(\alpha + 1)$

(b) $\alpha(\alpha^2 + \alpha + 1)$

Exercici 1.18. Proveu que el polinomi $D^4 + D^3 + D^2 + D + 1 \in \mathbb{F}_2[D]$ és irreductible però no és primitiu

Exercici 1.19. Comproveu que el polinomi $f(D) := D^3 + D^2 + 1$ és irreductible sobre $\mathbb{F}_2$. Sigui α la classe de D en el cos de 8 elements $\mathbb{F}_8 := \mathbb{F}_2[D]/(f(D))$

(a) Comproveu que α és un element primitiu de $\mathbb{F}_8$

(b) Representeu tots els elements no nuls de $\mathbb{F}_8$ com a potència de α

(c) Construïu la taula de la multiplicació d'aquest cos anomenant $\mathbb{F}_8 := \{0, 1, 2, 3, 4, 5, 6, 7\}$

Exercici 1.20. Siguin $f(D) := D^3 + D^2 + 1$, $\mathbb{F}_8 := \mathbb{F}_2[D]/(f(D))$ i α la classe de x (α és un element primitiu). Resoleu els sistemes d'equacions següents en les incògnites u, v i w i amb coeficients a $\mathbb{F}_8$:

$$\left.\begin{aligned} u + v + w &= 1 + \alpha \\ (1+\alpha)u + (1+\alpha^2)v + \alpha^3 w &= 0 \\ (1+\alpha)u + \alpha^2 v + \alpha w &= 1 + \alpha + \alpha^2 \end{aligned}\right\} \qquad \left.\begin{aligned} (1+\alpha)u + (1+\alpha^2)v + \alpha^3 w &= 0 \\ (1+\alpha)u + \alpha^2 v + \alpha w &= 0 \end{aligned}\right\}$$

Exercici 1. 21. Considerem el cos finit de 16 elements $\mathbb{F}_{16}$ construït amb el polinomi $f(D) := D^4 + D^3 + 1$ sobre $\mathbb{F}_2$

(a) Comproveu que el polinomi $f(D)$ és irreductible sobre $\mathbb{F}_2$

(b) Proveu que $\alpha := \overline{D} \in \mathbb{F}_{16}$ és un element primitiu d'aquest cos

Exercici 1.22. Proveu que el polinomi $f(D) := D^5 + D^2 + 1$ és irreductible i primitiu sobre $\mathbb{F}_2$ i considereu el cos $\mathbb{F}_{32}$ definit a partir d'aquest polinomi. Sigui α la classe de D en aquest cos

(a) Expresseu l'element $\beta := \alpha^5 + \alpha^{23} + \frac{\alpha^2+\alpha^4}{1+\alpha^{12}}$ com a potència de α

(b) Resoleu a $\mathbb{F}_{32}$ l'equació de segon grau: $\alpha^3 t^2 + \alpha^{18} t + 1 = 0$

Exercici 1.23. Demostreu que en $\mathbb{F}_{2^m}$ tots els elements són quadrats

Exercici 1.24. (El codi del DNI) El número del document nacional d'identitat (DNI) és un nombre decimal de 8 dígits al qual s'afegeix una lletra a efectes de control. Per decidir la lletra es calcula el residu del nombre mòdul 23 i s'afegeix la lletra que correspon segons la taula següent:

0	1	2	3	4	5	6	7	8	9	10	11
T	R	W	A	G	M	Y	F	P	D	X	B

12	13	14	15	16	17	18	19	20	21	22
N	J	Z	S	Q	V	H	L	C	K	E

Exemple: lletra que correspon al nombre 42.306.541. La divisió entre 23 dona 1.839.414 de quocient i 19 de residu. La lletra que correspon al 19 és L, de forma que el DNI complet és $42.306.541 - L$. Una forma còmoda d'obtenir el residu mòdul 23 és tenir calculades totes les potències de 10 mòdul 23:

i	0	1	2	3	4	5	6	7
$10^i \pmod{23}$	1	10	8	11	18	19	6	14

Així, el residu de

$$u = \underline{u_7u_6u_5u_4u_3u_2u_1u_0} = \sum_{i=0}^{7} u_i 10^i$$

mòdul 23 es pot calcular més fàcilment fent el producte matricial

$$\begin{pmatrix} u_7 & u_6 & u_5 & u_4 & u_3 & u_2 & u_1 & u_0 \end{pmatrix} \begin{pmatrix} 14 \\ 6 \\ 19 \\ 18 \\ 11 \\ 8 \\ 10 \\ 1 \end{pmatrix}$$

a $\mathbb{Z}_{23}$. Podem pensar en un DNI com en una paraula de longitud 9:

$$u := \begin{pmatrix} u_7 & u_6 & u_5 & u_4 & u_3 & u_2 & u_1 & u_0 & u_{-1} \end{pmatrix}$$

sobre l'alfabet $\mathbb{Z}_{23}$ on

- $0 \leq u_i \leq 9$ per $0 \leq i \leq 7$
- $u \cdot (14, 6, 19, 18, 11, 8, 10, 1, -1)^t = 0$

El conjunt C de les paraules de $\mathbb{Z}_{23}^9$ que compleixen aquestes dues condicions formen un codi de bloc, anomenat codi del DNI. Si H és la matriu (a $\mathbb{Z}_{23}$)

$$H := \begin{pmatrix} 14 & 6 & 19 & 18 & 11 & 8 & 10 & 1 & -1 \end{pmatrix}$$

i definim la síndrome d'una paraula $z \in \mathbb{Z}_{23}^9$ com el següent element de $\mathbb{Z}_{23}$:

$$s(z) := Hz^t$$

llavors per.a DNI's correctes la síndrome és zero; quan la síndrome no és zero, el DNI és incorrecte. Però si s'ha comès un únic error i sabem on... el podem corregir. Aquest exercici consisteix en veure quin dígit falta al següent DNI: 46.00?.002J

Exercici 1.25. (El codi ISBN) Cada llibre té un número associat anomenat International Standard Book Number o ISBN. Un ISBN és una paraula

$$u = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_8 & u_9 & u_{10} \end{pmatrix}$$

en l'alfabet $\mathbb{Z}_{11} := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$. Un parell d'exemples: $0 - 8218 - 0564 - 9$, $84 - 8301 - 216 - 2$. El primer grup de nombres és l'idioma: 0: anglès, 84: català i castellà; el segon grup és l'editorial: 8218: American Mathematical Society, 8301: Edicions UPC; el tercer grup és un nombre assignat al llibre per l'editor. L'últim dígit és redundant i es calcula per:

$$u_{10} := u_1 + 2u_2 + 3u_3 + \ldots + 9u_9 \pmod{11}$$

(Si el resultat és 10, es posa X). Els guions tenen com a única finalitat facilitar la lectura, però des d'un punt de vista formal són ignorats. Sigui H la matriu (a $\mathbb{Z}_{11}$)

$$H := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

La síndrome d'una paraula $z := (z_1, z_2, \ldots, z_{10})$ és $s(z) := Hz^t = z_1 + 2z_2 + \ldots + 10z_{10} \in \mathbb{Z}_{11}$. El conjunt de les paraules amb síndrome 0 tals que X no apareix a cap de les primeres 9 posicions és un codi sobre $\mathbb{Z}_{11}$ anomenat codi ISBN.Igual que per al DNI, per a ISBN's correctes la síndrome és zero i quan la síndrome no és zero, l'ISBN és incorrecte. Però si s'ha comès un únic error i sabem on... el podem corregir. Aquest exercici consisteix en detectar i/o corregir errors en els següents ISBN's:

(a) $84 - 7223 - 954 - 3$

(b) $84 - 7635 - 458 - X$

(c) $0 - 38? - 94599 - 7$

Exercici 1.26. Comproveu que el polinomi $m(D) := D^4 + D^3 + 1$ és irreductible sobre $\mathbb{Z}_2[D]$ i que l'element $\alpha := \bar{D}$ és primitiu en el cos $GF(16) := \mathbb{Z}_2[D]/(m(D))$. Resoleu, en aquest cos, l'equació $x^2 + \alpha^5 x + 1 = 0$. Observeu que:

(a) Una equació de segon grau no pot tenir més de dos zeros

(b) Encara que la «fórmula» per a resoldre equacions de segon grau sobre els reals no sigui d'aplicació, estem en un cos finit: podem anar provant els elements de un en un

(c) Per poder operar còmodament, construïu la taula de logaritmes de Zech

Exercici 1. 27. En el cos de Galois $GF(16)$ construit amb el polinomi de l'exercici anterior, ¿és primitiu l'element $\beta := \overline{D + 1}$?

Exercici 1.28. Considereu el codi de Hamming $Ham(7, 4)$ amb matriu de control

$$H := \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

on $\alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^3 + D + 1)$

(a) Doneu els paràmetres del codi n, k, r

(b) Doneu una matriu de codificació binària, no necessàriament sistemàtica (en aquest exercici no utilitzeu polinomis per a representar missatges, paraules, etc)

(c) Si les paraules que arriben a l'extrem receptor del canal són 0101100, 1110000, estimeu quines han estat les paraules transmeses

Nota.- Utilitzeu la taula de logaritmes de Zech; si no la teniu, construïu-la

Exercici 1.29. Considereu el codi de l'exercici anterior: $H := \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$. Si rebem la paraula ??11010, podem saber quins són els dígits que falten? En cas afirmatiu trobeu-los

Exercici 1.30. Considereu el codi de Hamming amb matriu de control $H := \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$ on $\alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^3 + D + 1)$

(a) Doneu els paràmetres del codi n, k, r

(b) Corregiu els errors que tenen (si en tenen) les paraules 1100110 i 0101100. Useu polinomis

(c) Codifiqueu sistemàticament els missatges 1100, 1001. Useu polinomis

Exercici 1.31. Considereu el codi de Hamming amb matriu de control $H := \begin{pmatrix} \alpha^{14} & \alpha^{13} & \alpha^{12} & \ldots & \alpha^2 & \alpha & 1 \end{pmatrix}$ on $\alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^4 + D + 1)$

(a) Doneu els paràmetres del codi (n, k, r)

(b) Corregiu els errors de la paraula $1100\ldots0$ (les dues primeres components són 1, les altres 0). Useu polinomis

(c) Codifiqueu sistemàticament els missatges $1\ldots1$ (tot uns). Useu polinomis

Exercici 1.32. Considerem el codi de Hamming $H(7, 4)$ definit per la matriu de control

$$H := \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

$\alpha := \overline{D}$ és l'element primitiu del cos de Galois $GF(8)$ construït amb el mòdul $m(D) := D^3 + D^2 + 1$

(a) Descodifiqueu la paraula (1110001)

(b) Codifiqueu, de manera sistemàtica, el missatge (1011)

Exercici 1.33. Considerem el codi de Hamming $H(15, 11)$ definit per la matriu de control

$$H := \begin{pmatrix} \alpha^{14} & \alpha^{13} & \alpha^{12} & \alpha^{11} & \alpha^{10} & \alpha^9 & \alpha^8 & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

on $\alpha := \overline{D}$ és l'element primitiu del cos de Galois $GF(16)$ construït amb el mòdul $m(D) := D^4 + D^3 + 1$

(a) Feu la taula de logaritmes de Zech

(b) Descodifiqueu la paraula (000 101 000 101 000)

Exercici 1.34. Trobeu el màxim comú divisor dels polinomis a coeficients binaris que s'indiquen a continuació:

(a) $f(x) := x^7 + 1$, $g(x) := x^5 + x^3 + x + 1$

(b) $f(x) := x^5 + x + 1$, $g(x) := x^6 + x^5 + x^4 + 1$

Exercici 1.35. Resoleu la congruència

$$\left(x^4 + x^3 + x^2 + 1\right) \cdot f(x) \equiv \left(x^2 + 1\right) \quad \left(mod\ \ x^3 + 1\right)$$

Exercici 1.36. Com és el codi BCH de paràmetre $m := 3$ i distància de disseny $\delta := 5$?

Exercici 1.37. Considereu el codi BCH de longitud 15 corrector de 2 errors, amb matriu de control

$$H := \begin{pmatrix} \alpha^{12} & \alpha^9 & \alpha^6 & \dots & \alpha^6 & \alpha^3 & 1 \\ \alpha^{14} & \alpha^{13} & \alpha^{12} & \dots & \alpha^2 & \alpha & 1 \end{pmatrix} \quad \alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^4 + D + 1)$$

Corregiu els errors de les paraules: 100001010000000, 000100010000110, 100101010000010, 100001000100101, 100101010000110

Exercici 1.38. Considerem un codi RS de longitud 7 corrector de 2 errors

(a) Descodifiqueu la paraula $(0\alpha 0\alpha^3\alpha^6 11)$. Treballeu amb el cos de Galois $GF(8)$ construit amb $m(D) := D^3 + D + 1$

(b) Si l'emissor ha codificat de manera sistemàtica, quin ha estat el missatge transmès?

Exercici 1.39. Considerem un codi RS de longitud 7 corrector de 2 errors

(a) Calculeu el polinomi generador del codi. Quina és la dimensió del codi?

(b) Codifiqueu, de manera sistemàtica, el missatge format exclusivament per 1's

(c) Descodifiqueu la paraula $(0\alpha 00\alpha 01)$

Treballeu amb el cos de Galois $GF(8)$ construit amb $m(D) := D^3 + D + 1$. Taula de logaritmes de Zech i polinomis mínims per $GF(8)$ construit amb $m(D) := D^3 + D + 1$ ($\alpha := \overline{D}$):

i	1	2	3	4	5	6
$Z(i)$	3	6	1	5	4	2

$$m_1(x) = x^3 + x + 1 \qquad m_3(x) = x^3 + x^2 + 1$$

Exercici 1. 40. Calculeu els paràmetres (n, k, r) del codi BCH de longitud 31 amb distància de disseny $\delta := 7$

Exercici 1. 41. Calculeu els paràmetres (n, k, r) del codi BCH de longitud 63 amb distància de disseny $\delta := 11$

Exercici 1.42. Considereu el codi BCH de longitud 15 corrector de 2 errors, amb matriu de control

$$H := \begin{pmatrix} \alpha^{12} & \alpha^9 & \alpha^6 & \dots & \alpha^6 & \alpha^3 & 1 \\ \alpha^{14} & \alpha^{13} & \alpha^{12} & \dots & \alpha^2 & \alpha & 1 \end{pmatrix} \quad \alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^4 + D + 1)$$

(a) Calculeu el polinomi generador del codi $g(x)$

(b) Calculeu els paràmetres del codi (n, k, r)

(c) Codifiqueu sistemàticament el missatge format per dos 1's i la resta 0's

Exercici 1.43. Considereu el codi BCH de longitud 15 corrector de 3 errors, amb matriu de control

$$H := \begin{pmatrix} \alpha^{10} & \alpha^5 & 1 & \dots & \alpha^{10} & \alpha^5 & 1 \\ \alpha^{12} & \alpha^9 & \alpha^6 & \dots & \alpha^6 & \alpha^3 & 1 \\ \alpha^{14} & \alpha^{13} & \alpha^{12} & \dots & \alpha^2 & \alpha & 1 \end{pmatrix} \quad \alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^4 + D + 1)$$

(a) Calculeu el polinomi generador del codi $g(x)$

(b) Calculeu els paràmetres del codi (n, k, r)

(c) Codifiqueu sistemàticament el missatge format per dos 1's i la resta 0's

Exercici 1. 44. A partir de l'equació fonamental trobeu els coeficients del polinomi localitzador d'errors pel codi de l'exercici anterior quan la paraula rebuda és $w := 101010100000001$ i estimeu la paraula-codi transmesa

Exercici 1.45. Considereu el codi BCH de longitud 31 amb distància de disseny $\delta := 7$ i matriu de control la habitual, amb $\alpha := \overline{D} \in \mathbb{Z}_2[D]/(D^5 + D^2 + 1) \equiv GF(32)$. Estimeu la paraula-codi transmesa quan la paraula rebuda és $w :=$ 0000|0000|0000|0000|1000|1011|0001|001. La taula de logaritmes de Zech és:

i	1	2	3	4	6	7	8	9	11	12	13	15	17	21	26
$Z(i)$	18	5	29	10	27	22	20	16	19	23	14	24	30	25	28

Exercici 1.46. Considerem un codi BCH de longitud 15 corrector de 3 errors

(a) Descodifiqueu la paraula (001 000 111 001 011). Treballeu amb el cos de Galois $GF(16)$ construit amb $m(D) := D^4 + D + 1$

(b) Si l'emissor ha codificat de manera sistemàtica, quin ha estat el missatge transmès?

Exercici 1.47. Considerem un codi BCH de longitud 15 corrector de 3 errors

(a) Calculeu el polinomi generador del codi. Quina és la dimensió del codi?

(b) Codifiqueu, de manera sistemàtica, el missatge format exclusivament per 1's

(c) Descodifiqueu la paraula (011 000 111 111 001)

Treballeu amb el cos de Galois $GF(16)$ construit amb $m(D) := D^4 + D + 1$. Taula de logaritmes de Zech i polinomis mínims per $GF(16)$ construit amb $m(D) := D^4 + D + 1$ ($\alpha := \overline{D}$):

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$Z(i)$	4	8	14	1	10	13	9	2	7	5	12	11	6	3

$$m_1(x) = x^4 + x + 1 \qquad m_3(x) = x^4 + x^3 + x^2 + x + 1$$
$$m_5(x) = x^2 + x + 1 \qquad m_7(x) = x^4 + x^3 + 1$$

TCI - Solucions Codificació

Solució 1. 1. Si suposem paritat parell, el bit de paritat associat als bits a, b és $a+b$ (suma en $\mathbb{Z}_2$) i si suposem paritat senar el bit de paritat és $a+b+1$. Per fixar idees suposem paritat parell. El bit de paritat associat a dos bits d'una suma de dues paraules és la suma dels bits de paritat de cada paraula (associada a les dues posicions amb les que estem treballant). Per tant, el codi és lineal. I la distància mínima és 2 ja que no hi ha cap columna de zeros i les dues primeres columnes (per exenple) són dependents. Un codi (lineal) amb distància mínima igual a 2 no pot corregir cap error, però en pot detectar un

Solució 1.2.

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- Paraules de pes 0: només hi ha la 00000000
- Paraules de pes 1: no pot ser que a les quatre primeres posicions només hi hagi un 1 (en aquest cas hi hauria tres 1's a les posicions 5 a 8); per altra part, si a les primeres 4 posicions no hi ha cap 1 llavors estem davant de la paraula 00000000. Per tant, no hi ha cap paraula-codi de pes 1
- Paraules de pes 2: a les 4 primeres posicions hi ha d'haver algun 1; si només n'hi ha un ja sabem que a les 4 últimes posicions n'hi haurà tres. Per tant els dos 1's han d'estar a les 4 primeres posicions. Però en aquest cas hi hauria dos 1's més a les posicions 4 a 8. Per tant no hi ha paraules-codi de pes 2
- Paraules de pes 3: de manera anàloga es veu que no hi ha paraules-codi de pes 3
- Paraules de pes no inferior a 4: hi ha d'haver algun 1 a les 4 primeres posicions
  - 1000|0111, 0100|1110, 0010|1101, 0001|1011 $\rightarrow$ pes 4
  - 1100|1001, 1010|1010, 1001|1100, 0110|0011, 00101|0101, 0011|0110 $\rightarrow$ pes 4
  - 1110|0100, 1101|0010, 1011|0001, 0111|1000 $\rightarrow$ pes 4
  - 1111|1111 $\rightarrow$ pes 8
- Per tant la distància mínima d'aquest codi és 4

Solució 1.3. Paraules-codi:

$$00000, 10011, 00101, 10110, 01001, 11010, 01100, 11111$$

Distància mínima: 2. H (per exemple):

$$H := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Solució 1.4.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Solució 1.5. Si $a_{1,6} = 0, a_{2,6} := 1, a_{3,6} := 1 i a_{4,6} := 0$ llavors el codi és

$$000000, 011001, 100011, 111010$$

En general, hi ha 4paraules-codi, que són $x_1x_2x_3x_4x_5x_6$ amb

$$\begin{cases} x_1 = x_5 + a_{1,6}x_6 \\ x_2 = x_5 + (a_{1,6} + a_{2,6})x_6 \\ x_3 = x_5 + (a_{1,6} + a_{3,6})x_6 \\ x_4 = (a_{2,6} + a_{3,6} + a_{4,6})x_6 \end{cases}$$

Si $x_6 := 0$ llavors les paraules-codi que acaben en 0 són de la forma: $(x_5, x_5, x_5, 0, x_5, 0)$; en particular, per $x_5 := 1$ tenim la paraula-codi 111010, la qual té pes 4. La distància mínima és doncs ≤ 4 i això no permet corregir dos errors. Ja coneixem dues paraules del codi: 000000 i 111010. Només falten les altres dues. Que acabaran en 1. Les que acaben en 01 són:

$$a_{1,6}, a_{1,6} + a_{2,6}, a_{1,6} + a_{3,6}, a_{2,6} + a_{3,6} + a_{4,6}, 0, 1$$

Per $a_{1,6} := 0$ tenim

$$0, a_{2,6}, a_{3,6}, a_{2,6} + a_{3,6} + a_{4,6}, 0, 1$$

I si volem que $d_{\min} \geq 4$ ha de ser $a_{2,6} = a_{3,6} = a_{4,6} = 1$. I aquesta elecció ja va bé. Les paraules-codi en aquest cas són: $(x_1, x_2, x_3, x_4, x_5, x_6) = (x_5, x_5 + x_6, x_5 + x_6, x_6, x_5, x_6)$ és a dir:

$$000000 \quad 011101 \quad 111010 \quad 100111$$

La distància mínima és 4 i, per tant aquest codi pot corregir un error i detectar-ne dos

Solució 1.6.

(a) És clar que el codi no és sistemàtic

(b) Per exemple: $G' := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

(c) Codificació de 101 amb G i amb G':

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} G' = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Solució 1.7. Si intercanviem les posicions 1 i 3 de les paraules-codi del codi G_1 s'obté el codi G_2

Solució 1.8.

1.

$$H = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right)$$

2. $d_{\min} = 2$. Amb això només es pot detectar 1 error

Solució 1. 9. A H no hi ha la columna nul · la però hi ha columnes repetides (la segona i la sisena); per tant $d_{\min} = 2$. Amb això només es pot detectar 1 error. Ara bé, si llistem totes les paraules-codi (calculant primer una G, sistemàtica) veurem que hi ha una única paraula-codi que és la més propera a 11111111, que és la paraula-codi 11110110 i aquesta es descodifica com 1111

Solució 1. 10. Estem parlant del codi que a cada missatge (binari) x li assigna la paraula-codi $xxxxx$. És a dir estem parlant del codi que té com a matriu de codificació

$$G := \left(\begin{array}{c|cccc} 1 & 1 & 1 & 1 & 1 \end{array} \right)$$

Per tant una matriu de control és

$$H := \left(\begin{array}{c|cccc} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array} \right)$$

És a dir la síndrome de la paraula $z := z_1 z_2 z_3 z_4 z_5$ és

$$s(z) := Hz^t = \begin{pmatrix} z_1 + z_2 & z_1 + z_3 & z_1 + z_4 & z_1 + z_5 \end{pmatrix}^t$$

Com que $d_{\min} = 5$, aquest codi pot corregir dos errors. Llistem els patrons de dos errors (líders) juntament amb les síndromes corresponents:

líders	s^t
00000	0000
10000	1111
01000	1000
00100	0100
00010	0010
00001	0001
11000	0111
10100	1011
10010	1101
10001	1110
01100	1100
01010	1010
01001	1001
00110	0110
00101	0101
00011	0011

Solució 1.11.

(a) Un codi és lineal si transforma el missatge «suma» en la suma de missatges. Com que el 00 es transforma en 00000, només falta veure que $01 + 10$ es transforma en $01101 + 10111$, que $01 + 11$ es transforma en $01101 + 11010$ i que $10 + 11$ es transforma en $10111 + 11010$, cosa que es comprova. $x_1 x_2$ es codifica com $x_1, x_2, x_1 + x_2, x_1, x_1 + x_2$

(b)

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(c) El pes mínim és 3; per tant la distància mínima és 3. I això només permet corregir un error. Donem els líders de pes no superior a 1 de les classes laterals del codi, juntament amb les síndromes que identifiquen les classes:

líders	s^t
00000	000
10000	111
01000	101
00100	100
00010	010
00001	001

Solució 1.12. Com que H és una matriu 3×5, la redundància d'aquest codi és $r := 3$ i la longitud del codi és $n := 5$; per tant la longitud dels missatges és $k := 2$. Vol dir això que només hi ha 4 missatges: 00, 01, 10 i 11 que es codifiquen respectivament com 00000, 01111, 10010, 11101. El pes mínim és 2 i això no permet corregir cap error. I les paraules-codi més properes a 01001 són les que estan a distància $d := 2$. I n'hi ha tres! Per tant no podem saber què s'ha transmès.

Solució 1.13.

(a) $000000, 100011, 101101, 001110, 010111, 110111, 111010, 011001$

(b) $d_{\min} = 3 \implies$ pot corregir 1 error

(c)

líders	s^t
000000	000
100000	011
010000	111
001000	110
000100	100
000010	010
000001	001

(d) $s(001100) = (010)^t$, $s(010001) = (110)^t$. La paraula corregida és 000010 001000

Solució 1.14.

(a) $k := 4$, $n := 7$, $r := 3$

(b)

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c) $d_{\min} = 2$

Solució 1.15.

(a) $r := 3, n := 6, k := 3$

(b)

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(c) $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$

(d) $d_{\min} = 3$

(e)

líders	s^t
000000	000
100000	110
010000	001
001000	101
000100	010
000010	011
000001	100

(f) A la paraula 011001 no hi ha cap error; a la paraula 111110 hi ha un error en el penúltim dígit; a la paraula 111111 hi ha més d'un error

Solució 1.16.

(a) $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

(b) Només hi ha 4 paraules-codi: podem fer el que calgui. $d_{\min} = 3$. Taula per a descodificar patrons d'un error:

líders	s^t
00000	000
10000	100
01000	010
00100	001
00010	011
00001	111

Descodificacions: $10011 \mapsto 10011, 11110 \mapsto 01110, 00101 \mapsto$ més d'un error

Solució 1.17.

(a) $(\alpha^2 + \alpha)(\alpha + 1) = \alpha^3 + \alpha + \alpha^2 + \alpha = \alpha^2 + \alpha + \alpha + \alpha^2 = 0$

(b) $\alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + \alpha^2 + \alpha = 0$

Tenim (tan en un cas com en l'altre) el producte de dos elements no nuls que dona 0.

Solució 1.18. Si no fos irreductible seria el producte de dos polinomis de grau 2 o d'un polinomi de grau 3 per un polinomi de grau 1. Aquest últim cas implica que el polinomi tindria una arrel en $\mathbb{F}_2$, cosa que no és, ja que ni en 0 ni en 1 el polinomi dona 0. I si $D^4 + D^3 + D^2 + D + 1$ és producte de dos polinomis de segon grau aquests han de ser $(D^2 + aD + 1)$ i $(D^2 + bD + 1)$. Però si $D^4 + D^3 + D^2 + D + 1 = (D^2 + aD + 1) \cdot (D^2 + bD + 1)$ llavors $a + b = a \cdot b = 1$, cosa que no pot ser (recordem $a, b \in \mathbb{F}_2$). Per tant $\mathbb{F}_2[D]/\big(D^4 + D^3 + D^2 + D + 1\big)$ és un cos. Si anomenem $\alpha := \overline{D}$ llavors $\alpha^5 = 1$ (feu-ho). Per tant el polinomi inicial no és primitiu

Solució 1.19.

(a) Comproveu vosaltres mateixos que 1 no surt fins α^7

(b) $1 = \alpha^7$, $2 = \alpha$, $3 = \alpha^5$, $4 = \alpha^2$, $5 = \alpha^3$, $6 = \alpha^6$, $7 = \alpha^4$

(c)

$*$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	5	7	1	3
3	0	3	6	5	1	2	7	4
4	0	4	5	1	7	3	2	6
5	0	5	7	2	3	6	4	1
6	0	6	1	7	2	4	3	5
7	0	7	3	4	6	1	5	2

Solució 1.20. Com que

$$\begin{vmatrix} 1 & 1 & 1 \\ 1+\alpha & 1+\alpha^2 & \alpha^3 \\ 1+\alpha & \alpha^2 & \alpha \end{vmatrix} \neq 0,$$

el primer sistema té solució única: $u = \alpha^2, v = \alpha^4, w = 0$. Segon sistema: és un sistema homogeni, amb 1 grau de llibertat: $u = v = \alpha^4 w$, w lliure

Solució 1.21.

(a) Si el polinomi $f(D)$ descomposés ho faria en producte de dos polinomis de grau 2 o en producte d'un polinomi de grau 3 per un polinomi de grau 1. Aquesta última opció implicaria que $f(D)$ té alguna arrel en $\mathbb{F}_2 := \{0, 1\}$ i no és el cas. I si $f(D)$ descomposa com a producte de dos polinomis de grau 2 ha de ser

$$D^4 + D^3 + 1 = (D^2 + aD + 1) \cdot (D^2 + bD + 1)$$

però això implicaria que $a + b = 1$ i $a + b = 0$, cosa que tampoc pot ser.

(b) Per justificar que $\alpha := \overline{D} \in \mathbb{F}_{16}$ és un element primitiu d'aquest cos només cal fer la construcció corresponent i veure que la primera potència de α que dona 1 és α^{15}

Solució 1. 22. Si $f(D)$ no fos irreductible seria el producte d'un polinomi de grau 3 per un polinomi de grau 2 o el producte d'un polinomi de grau 4 per un polinomi de grau 1. Aquest últim cas implicaria que el polinomi tindria una arrel en $\mathbb{F}_2$, cosa que no és, ja que ni en 0 ni en 1 el polinomi dona 0. I si

$$D^5 + D^2 + 1 = (D^3 + aD^2 + bD + 1) \cdot (D^2 + cD + 1)$$

llavors $a = b = c$ i això contradiu el fet que $1 + ac + b = 0$. El polinomi, per tant, és irreductibe. I si feu les potències de α veureu que 1 no surt fins α^{31}. Per tant, el polinomi és primitiu

(a) $\beta = \alpha^{22}$

(b) $t = \alpha^6, \alpha^{22}$

Solució 1.23. Si α és un element primitiu de $\mathbb{F}_{2^m}$ llavors $\mathbb{F}_{2^m} = \left\{0, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^m-1} = 1\right\}$. És clar que que 0 és un quadrat, només falta veure que ho són els demés elements. α^{parell} és clar que és un quadrat i $\alpha^{\text{senar}} = \alpha^{\text{senar}} \cdot \alpha^{2^m-1}$, és a dir $\alpha^{\text{senar}} = \alpha^{\text{senar}+2^m-1}$ i senar $+ 2^m - 1$ és parell

Solució 1.24. $? = 1$

Solució 1.25.

(a) Correcta

(b) Incorrecta (té errors)

(c) $? = 7$

Solució 1.26. El comprovar que un polionomi és primitiu ja ho sabeu fer. Solucions de l'equació $x^2 + \alpha^5 x + 1 = 0$: $x = \alpha^3, \alpha^{12}$

Solució 1.27. No

Solució 1.28.

(a) $n = 7, r = 3, k = 4$

(b)

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(c) $0101100 \mapsto 0101100$, $1110000 \mapsto 1110100$

Solució 1.29. $??11010 \mapsto 1011010$

Solució 1.30.

(a) $n = 7$, $r = 3$, $k = 4$

(b) $1100110 \mapsto 1100010$, $0101100 \mapsto 0101100$

(c) $1100 \mapsto 1100010$, $1001 \mapsto 1001110$

Solució 1.31.

(a) $n = 15$, $r = 4$, $k = 11$

(b) $1100\ldots0 \mapsto 110\ldots0100$

(c) $11111111111 \mapsto 111111111110000$

Solució 1.32.

(a) Descodificació: $(1110001) \mapsto (1010001)$

(b) Codificació: $(1011) \mapsto (1011100)$

Solució 1.33.

(a)

i	$Z(i)$
1	12
2	9
3	4
5	10
6	8
7	13
11	14

(b) Descodificació: $000\,101\,000\,101\,000 \mapsto 000\,101\,000\,001\,000$

Solució 1.34.

(a) $x + 1$

(b) 1

Solució 1.35. $f(x) = (x+1)^2 = x^2 + 1$

Solució 1.36. És el codi de repetició ($k = 1$) que codifica

$$\begin{aligned} 0 &\mapsto 0000000 \\ 1 &\mapsto 1111111 \end{aligned}$$

Solució 1.37. Correccions: $100001010000000 \mapsto$ excedida capacitat correctora del codi, $000100010000110 \mapsto 100101010000110$, $100101010000010 \mapsto 100101010000110$, $100001000100101 \mapsto$ excedida capacitat correctora del codi, $100101010000110 \mapsto 100101010000110$

Solució 1.38.

(a) $0\alpha0\alpha^3\alpha^6 11 \mapsto 0\alpha0\alpha^3\alpha 11$.

(b) Missatge transmès estimat: $0\alpha0$

Solució 1.39.

(a) $g(x) := x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$. Dimensió del codi: $k = 3$

(b) $111 \mapsto 1111111$

(c) Descodificació: $0\alpha00\alpha01 \mapsto 0\alpha0\alpha^3\alpha11$

Solució 1.40. $n = 31, k = 16, r = 15$

Solució 1.41. $n = 63, k = 36, r = 27$

Solució 1.42.

(a) $g(x) = x^8 + x^7 + x^6 + x^4 + 1$

(b) $n = 15, k = 7, r = 8$

(c) Codificació: $1100000 \mapsto 110000010011100$

Solució 1.43.

(a) $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$

(b) $n = 15, k = 5, r = 10$

(c) $11000 \mapsto 110000101001101$

Solució 1.44. $L(x) = 1+\alpha^8 x+\alpha^6 x^2+\alpha^9 x^3$. Descodificació: $101010100000001 \mapsto 111010110010001$

Solució 1.45. Descodificació: 0000|0000|0000|0000|1000|1011|0001|001 $\mapsto$ 0000|0000|0100|0000|1000|1011|0001|101

Solució 1.46.

(a) Descodificació: $001\,000\,111\,001\,011 \mapsto 001\,000\,111\,101\,011$

(b) Missatge estimat: 00100

Solució 1.47.

(a) $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$, dimensió: 32 ($k = 5$)

(b) Codifiqueu, de manera sistemàtica, el missatge format exclusivament per 1's Codificació: $11111 \mapsto 111111111111111$

(c) Descodificació: $011\,000\,111\,111\,001 \mapsto 001\,000\,111\,101\,011$