10
Eina-e

Matemàtica Discreta II

Aritmètica i teoria de la codificació

Maria Bras-Amorós
Josep Rifà Coma

[publicacions] urv

Matemàtica Discreta II

Eina-e, 10

Edita:
Publicacions URV

1a edició: Desembre de 2012
ISBN: 978-84-8424-207-9
Dipòsit legal: T-1464-2012

Publicacions de la Universitat Rovira i Virgili:
Av. Catalunya, 35 - 43002 Tarragona
Tel. 977 558 474
www.publicacionsurv.cat
publicacions@urv.cat

Matemàtica Discreta II

Aritmètica i teoria de la codificació

Maria Bras-Amorós
Josep Rifà Coma

[publicacions] urv

Tarragona, 2012

Índex

Prefaci

Aquest llibre pretén ser el suport de l'assignatura Matemàtica Discreta II impartida al grau d'Informàtica de la URV. Els dos blocs principals d'aquesta assignatura són l'aritmètica discreta i la teoria de la codificació per al tractament d'errors en les comunicacions digitals. El llibre està enfocat al planteig i la resolució de problemes. Inclou un primer capítol amb un resum de la teoria de l'assignatura i la resta de capítols estan dedicats als problemes de cadascun dels temes.

L'aritmètica (del grec $\alpha\rho\iota\theta\mu o\zeta$) és probablement la branca més elemental i antiga de les matemàtiques. Tracta els nombres i les seves combinacions. L'aritmètica discreta se centra en l'estudi dels nombres enters, la divisibilitat i els nombres primers i en determinats tipus d'equacions en aquest context, com les equacions diofàntiques o les equacions amb congruències. En l'era digital trobem operacions aritmètiques discretes en tots els protocols de tractament de dades, sigui de transmissió (codis de control d'errors), d'emmagatzematge (compressió de dades) o d'ocultació (criptografia).

Els codis de control d'errors s'utilitzen per poder detectar i corregir els errors que es poden produir en la trasmissió d'informació a través de canals defectuosos que distorsionin la informació que s'envia. Per exemple, els errors que produeix l'atmosfera en transmetre les fotos del satèl·lit Meteosat fins a la Terra, o els errors deguts a les diferents interferències produïdes en una comunicació per telèfon mòbil, o en la recepció del senyal de televisió digital (TDT) o la línia ADSL, o els possibles errors en la lectura d'un CD o DVD.

El funcionament d'aquests codis consisteix en l'enviament, junt amb la informació original, d'una mica de redundància de manera que a partir de tot el que es rep puguem deduir el que realment s'ha transmès. L'exemple més simple seria afegir, per cada bit que s'envia, dues còpies iguals del mateix bit. Així si el bit original o alguna de les còpies es rep malament, podem corregir-lo a partir dels altres dos. Observem que, en afegir redundància, d'una banda hi guanyem perquè millora la qualitat de la informació rebuda, però de l'altra hi perdem perquè hi ha un augment del cost d'enviament. En l'exemple de repetir bits, el cost es multiplica per tres.

La teoria de codis tracta el disseny i implementació de codis amb bona capacitat de corregir errors, però que suposin un baix cost d'enviar la informació codificada, així com dels seus algoritmes correctors que ens permetin recuperar la informació original.

Capítol 1
Resum de teoria

1.1 Estructures algebraiques: grup, anell, cos

Un **grup** és un conjunt A amb una operació $\oplus$ amb les següents propietats:

- **Propietat associativa**:
  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ per a tot $a, b, c \in A$.
- **Element neutre**:
  Existeix un element $\textcircled{0} \in A$ tal que $a \oplus \textcircled{0} = \textcircled{0} \oplus a = a$ per a tot $a \in A$.
- **Element invers**:
  Per a tot $a \in A$ existeix $(-a) \in A$ tal que $a \oplus (-a) = (-a) \oplus a = \textcircled{0}$.

El grup és **commutatiu** si, a més a més, $\oplus$ satisfà la

- **Propietat commutativa**:
  $a \oplus b = b \oplus a$ per a tot $a \in A$.

Exemple: Els enters $\mathbb{Z}$ amb la suma habitual són un grup (commutatiu). En canvi, els naturals $\mathbb{N}$ no ho són perquè no tots els elements tenen element invers. Els enters amb el producte habitual tampoc són grup perquè no sempre existeix l'element invers.

Un **anell** és un conjunt A amb dues operacions $\oplus$ i $\otimes$ tal que $\oplus$ li confereix estructura de grup commutatiu i $\otimes$ satisfà

- **Propietat associativa**:
  $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ per a tot $a, b, c \in A$.
- **Propietat distributiva respecte a $\oplus$**:
  $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ per a tot $a, b, c \in A$.

L'anell és **unitari** i **commutatiu** si $\otimes$ satisfà

- **Element neutre**:
  Existeix un element $\textcircled{1} \in A$ tal que $a \otimes \textcircled{1} = \textcircled{1} \otimes a = a$ per a tot $a \in A$.
- **Propietat commutativa**:
  $a \otimes b = b \otimes a$ per a tot $a \in A$.

Un **cos** és un anell unitari i commutatiu on $\otimes$ satisfà

- **Element invers**:
  Per a tot $a \in A$, tal que $a \neq \textcircled{0}$, existeix $a^{-1} \in A$ tal que $a \otimes a^{-1} = a^{-1} \otimes a = \textcircled{1}$.

Exemple: Els enters $\mathbb{Z}$, amb la suma i el producte habituals, són un anell. Però no són un cos perquè no tots els elements tenen element invers. Els racionals $\mathbb{Q}$ i els reals $\mathbb{R}$ sí que són cossos.

L'estructura algebraica pròpia de la teoria de codis és la dels cossos finits que presentarem en les següents seccions. El fet que es tracti d'estructures finites facilitarà les computacions. Les operacions $\oplus$ i $\ominus$ ens permetran codificar. L'existència d'element invers ens permetrà descodificar.

1.2 Aritmètica entera

1.2.1 Divisió euclidiana i identitat de Bézout

Divisió entera

Teorema 1. Per a tota parella d'enters a, b amb $b \neq 0$, existeixen enters q, r, únics amb $0 \leqslant r < |b|$ tals que

$$a = bq + r.$$

Donats a, b, q, r, com en el teorema, direm que q i r són, respectivament, el **quocient** i el **residu** de dividir a entre b. Si donats els enters a i b existeix un enter q tal que $a = qb$, aleshores diem que b **divideix** a, que b és un **divisor** d'a o que a és un **múltiple** de b. Es denota per $b \mid a$. Observem que si $b \mid a$, aleshores $-b \mid a$, $b \mid -a$ i $-b \mid -a$. Si $b \mid a$, aleshores $|b| \leqslant |a|$.

Donats dos enters qualssevol a i b denotem per $mcd(a, b)$ el màxim d'entre els divisors comuns d'a i b i l'anomenem **màxim comú divisor**. En particular, $mcd(a, 0) = |a|$ sempre que $a \neq 0$. Anàlogament es pot definir el màxim comú divisor d'un conjunt finit d'enters com el màxim dels seus divisors comuns. Diem que dos enters a i b són **coprimers** o **relativament primers** si $mcd(a, b) = 1$.

Algoritme d'Euclides

Teorema 2. [Teorema d'Euclides.] Donats a, b, q, r com en el teorema 1,

$$mcd(a, b) = mcd(b, r).$$

Prova: Com que $a = bq + r$, tots els divisors comuns de a, b divideixen r i tots els divisors comuns de b, r divideixen a. Per això, els divisors comuns de a, b coincideixen amb els divisors comuns de b, r i, en particular, el seu màxim comú divisor és el mateix. □

Donats dos enters a, b ens proposem calcular $mcd(a, b)$. Com que $mcd(a, b) = mcd(|a|, |b|)$, podem suposar que a i b són positius i $a \geqslant b$. Definim $r_{-2} = a$, $r_{-1} = b$ i, successivament, q_i i r_i com el quocient i el residu de dividir r_{i-2} entre r_{i-1} mentre r_{i-1} sigui diferent de 0. Així obtindrem una successió de

residus r_i, tots positius i que serà estrictament decreixent perquè, per definició, $r_i < r_{i-1}$. Per tant, arribarà un punt en què $r_{n+1} = 0$. Llavors tindrem

$$mcd(a,b) = mcd(b,r_0) = mcd(r_0,r_1) = mcd(r_1,r_2) = \cdots = mcd(r_n,0) = r_n.$$

Identitat de Bézout

Lema 3. Donats a, b i les successions de residus $\{r_i\}$ i de quocients $\{q_i\}$ com en l'apartat anterior, es té que per a tot enter $i \geqslant -2$ existeixen x_i i y_i tals que

$$x_i a + y_i b = r_i.$$

Prova: Podem suposar que a i b són positius ja que, altrament, n'hi ha prou de fer un canvi de signes dels enters x_i i y_i. Procedim per inducció sobre i. És fàcil comprovar el resultat per $i = -2$ prenent $x_{-2} = 1$ i $y_{-2} = 0$ i per $i = -1$ prenent $x_{-1} = 0$ i $y_{-1} = 1$.

Per $i \geqslant 0$ definim

$$\begin{aligned} x_i &= x_{i-2} - q_i x_{i-1} \\ y_i &= y_{i-2} - q_i y_{i-1} \end{aligned}$$

Aleshores,

$$\begin{aligned} x_i a + y_i b &= (x_{i-2} - q_i x_{i-1})a + (y_{i-2} - q_i y_{i-1})b \\ &= (x_{i-2}a + y_{i-2}b) - q_i(x_{i-1}a + y_{i-1}b) \\ &= r_{i-2} - q_i r_{i-1} = r_i. \end{aligned}$$

□

Teorema 4. [Identitat de Bézout.] Donats dos enters a i b, existeixen enters λ i μ tals que

$$\lambda a + \mu b = mcd(a,b).$$

Prova: És una conseqüència del lema 3. □

Per tal de trobar els coeficients de la identitat de Bézout utilitzarem la següent taula:

1	0	x_0	x_1	$\ldots$	x_i	$\ldots$	x_{n-1}	x_n	
0	1	y_0	y_1	$\ldots$	y_i	$\ldots$	y_{n-1}	y_n	
		q_0	q_1	$\ldots$	q_i	$\ldots$	q_{n-1}	q_n	q_{n+1}
a	b	r_0	r_1	$\ldots$	r_i	$\ldots$	r_{n-1}	r_n	0

Lema 5. Qualsevol expressió $\lambda a + \mu b$ amb a, b, λ, μ enters és un múltiple de $mcd(a,b)$.

Prova: $\lambda a + \mu b = mcd(a,b)\left(\lambda \frac{a}{mcd(a,b)} + \mu \frac{b}{mcd(a,b)}\right)$, on $\frac{a}{mcd(a,b)}$ i $\frac{b}{mcd(a,b)}$ són enters. □

Teorema 6. Els enters a i b són coprimers si i només si existeixen enters λ i μ tals que

$$\lambda a + \mu b = 1.$$

Prova: És una conseqüència del lema 5 i del teorema 4. □

Corol· lari 7. Per a tota parella d'enters a i b, els enters $\frac{a}{mcd(a,b)}$ i $\frac{b}{mcd(a,b)}$ són coprimers.

Prova: N'hi ha prou de dividir els dos costats de la identitat de Bézout entre $mcd(a,b)$. □

Corol· lari 8. Els enters λ i μ de la identitat de Bézout són coprimers.

Prova: N'hi ha prou de dividir els dos costats de la identitat de Bézout entre $mcd(a,b)$. □

Corol· lari 9. Si a, b, c són enters amb $mcd(a,b) = 1$ i $mcd(a,c) = 1$, aleshores $mcd(a,bc) = 1$.

Prova: Existiran $\lambda, \mu, \lambda', \mu'$ amb $\lambda a + \mu b = 1$ i $\lambda' a + \mu' c = 1$. N'hi ha prou de multiplicar les dues igualtats i obtenim que $\lambda'' a + \mu'' bc = 1$, on $\lambda'' = \lambda\lambda' a + \lambda\mu' c + \mu\lambda' b$ i $\mu'' = \mu\mu'$. □

Corol· lari 10. Si $a \mid bc$ i $mcd(a,b) = 1$, aleshores $a \mid c$.

Prova: Existeixen dos enters λ, μ tals que $1 = \lambda a + \mu b$. Multiplicant la igualtat per c obtenim $c = \lambda ac + \mu bc$, d'on $a \mid c$. □

Nombres primers i factorització

Diem que un nombre $a \geqslant 2$ és **primer** si els seus únics divisors són ± 1 i $\pm a$. Observem que 1 no és primer.

Lema 11. Si p és primer i $p \mid ab$, aleshores $p \mid a$ o $p \mid b$.

Prova: És una conseqüència de la definició de primer i del corol·lari 10. □

Teorema 12. [Teorema fonamental de l'aritmètica.] Qualsevol enter major o igual que 2 admet una descomposició en producte de primers. La descomposició és única, llevat de l'ordre dels factors.

Prova: L'existència de la descomposició és una conseqüència de la definició de primer. La unicitat és una conseqüència del lema 11. □

Teorema 13. Hi ha infinits nombres primers.

Prova: Procedim per reducció a l'absurd. Si $p_1 < \cdots < p_n$ són tots els primers, aleshores $p_1 \cdot \cdots \cdot p_n + 1$ també és primer (perquè no hi ha cap primer que el divideixi), però, en canvi, és major que p_n. □

Donats dos enters qualssevol a i b no nuls, denotem per $mcm(a, b)$ el mínim d'entre els múltiples positius comuns d'a i b i l'anomenem **mínim comú múltiple**. Anàlogament es pot definir el mínim comú múltiple d'un conjunt finit d'enters no nuls com el mínim dels seus múltiples positius comuns.

Lema 14. $mcd(a, b) \cdot mcm(a, b) = |a \cdot b|$.

Prova: Es pot comprovar a partir del teorema fonamental de l'aritmètica. □

Equacions diofàntiques lineals

Una **equació diofàntica lineal** és una equació de la forma

$$Ax + By = C$$

amb A, B, C enters. Diem que té solució si existeixen enters x i y que la compleixin.

Proposició 15. Sigui $Ax + By = C$ una equació diofàntica lineal.

(i) L'equació té solució si i només si $mcd(A, B) \mid C$.

(ii) Els enters x, y són solució de

$$Ax + By = C$$

si i només si ho són de

$$\frac{A}{mcd(A,B)}x + \frac{B}{mcd(A,B)}y = \frac{C}{mcd(A,B)}.$$

(iii) Si existeix una solució x_0, y_0, aleshores n'existeixen infinites i totes són de la forma

$$\begin{aligned} x &= x_0 + k\frac{B}{mcd(A,B)} \\ y &= y_0 - k\frac{A}{mcd(A,B)}, \end{aligned}$$

on $k \in \mathbb{Z}$.

Procediment per resoldre l'equació $Ax + By = C$:

- Si $mcd(A, B) \nmid C$, aleshores no hi ha solució.
- Si $mcd(A, B) \mid C$
  - Si $mcd(A, B) = 1$, aleshores
    - Calculem els coeficients λ i μ de la identitat de Bézout

$$\lambda A + \mu B = 1.$$

$*$ Les solucions són $x = C\lambda + Bk$, $y = C\mu - Ak$, on $k \in \mathbb{Z}$.

– Si $mcd(A, B) \neq 1$, aleshores resolem l'equació

$$\frac{A}{mcd(A,B)}x + \frac{B}{mcd(A,B)}y = \frac{C}{mcd(A,B)},$$

que compleix $mcd(\frac{A}{mcd(A,B)}, \frac{B}{mcd(a,b)}) = 1$

1.2.2 Congruències

Relació de congruència

Proposició 16. Donats enters a, b i $m > 0$ és equivalent:

- Els residus de dividir a i b entre m coincideixen.
- $a - b$ és un múltiple de m.

Prova: $a = q_a m + r$ i $b = q_b m + r$ implica que $a - b = (q_a - q_b)m$.

$a - b$ és un múltiple de m, $a = q_a m + r_a$ i $b = q_b m + r_b$ implica $(q_a - q_b)m + (r_a - r_b)$ és un múltiple de m i, per tant, $r_a - r_b$ és un múltiple de m. □

Dos enters a i b són **congruents mòdul** un enter m si es compleixen les condicions equivalents de la proposició 16. Escrivim $a \equiv b(mod\ m)$ o $a = b(mod\ m)$.

Proposició 17. Si $a \equiv b\ (mod\ m)$ i d divideix m, aleshores $a \equiv b\ (mod\ d)$.

Proposició 18. La relació de congruència és una relació d'equivalència (propietat reflexiva, propietat simètrica i propietat transitiva).

Proposició 19. [La suma i el producte de classes queden ben definits.] Si $a_1 \equiv a_2(mod\ m)$ i $b_1 \equiv b_2(mod\ m)$, aleshores $a_1 + b_1 \equiv a_2 + b_2(mod\ m)$ i $a_1 \cdot b_1 \equiv a_2 \cdot b_2(mod\ m)$.

Com a conseqüència, si $a \equiv b(mod\ m)$, aleshores $ka \equiv kb(mod\ m)$. Però el recíproc no és cert. **La simplificació no queda ben definida**. És a dir, pot ser que $ka \equiv kb(mod\ m)$, però, en canvi, $a \not\equiv b(mod\ m)$.

Per exemple, $2 \cdot 1 \equiv 2 \cdot 3(mod\ 4)$, però, en canvi, $1 \not\equiv 3(mod\ 4)$.

Proposició 20. $ka \equiv kb(mod\ m)$ si i només si $a \equiv b(mod\ \frac{m}{mcd(m,k)})$.

En el contraexemple anterior, $1 \equiv 3(mod\ \frac{4}{2})$.

Corol· lari 21. Es podrà simplificar sempre que $mcd(m, k) = 1$.

En el contraexemple no es pot simplificar perquè $mcd(k, m) = 2 \neq 1$.

Corol· lari 22. [Per simplificar, hem de simplificar també el mòdul.] Si $k \neq 0$, aleshores $ka \equiv kb(mod\ km)$ si i només si $a \equiv b(mod\ m)$.

Resolució de congruències

Una **congruència de grau n amb una incògnita** és una congruència de la forma

$$a_0 + a_1 x + \cdots + a_n x^n \equiv 0 (mod\ m),$$

amb m i $a_i \in \mathbb{Z}$, $m > 0$.

Diem que x_0 és una **solució** si, en substituir x per x_0, la congruència es compleix.

Lema 23. Si x_0 és solució i $x_0 \equiv x_1 (mod\ m)$, aleshores x_1 també és solució.

Com a solucions considerarem només un representant de cada classe.

Resolució directa Per substitució.
$x^2 - 1 \equiv 0 (mod\ 8)$ té solucions $1, 3, 5, 7$.

Resolució de congruències lineals Les congruències lineals són congruències de la forma $ax \equiv b (mod\ m)$.

Proposició 24. Considerem la congruència $ax \equiv b (mod\ m)$.

(i) Té solució si i només si $mcd(a, m) \mid b$.

(ii) L'enter x és solució de

$$ax \equiv b (mod\ m)$$

si i només si ho és de

$$\frac{a}{mcd(a,m)} x \equiv \frac{b}{mcd(a,m)} \left(mod\ \frac{m}{mcd(a,m)} \right).$$

(iii) Si existeix una solució x_0, aleshores n'existeixen $mcd(a, m)$ i el conjunt de solucions és donat per

$$x \equiv x_0 + k \frac{m}{mcd(a,m)} (mod\ m),$$

amb $k = 0, 1, \ldots, mcd(a, m) - 1$.

Procediment per resoldre la congruència $ax \equiv b (mod\ m)$:

- Si $mcd(a, m) \nmid b$, aleshores no hi ha solució.
- Si $mcd(a, m) \mid b$
  - Si $mcd(a, m) = 1$
    - Calculem els coeficients λ i μ de la identitat de Bézout

      $$\lambda a + \mu m = 1.$$

    - La solució és única i és $x \equiv \lambda b (mod\ m)$.
  - Si $mcd(a, m) \neq 1$

* Busquem la solució x_0 de la congruència

$$\frac{a}{mcd(a,m)}x \equiv \frac{b}{mcd(a,m)} \left(mod \ \frac{m}{mcd(a,m)} \right)$$

que compleix $mcd(\frac{a}{mcd(a,m)}, \frac{m}{mcd(a,m)}) = 1$.

* El conjunt de solucions serà

$$x \equiv x_0 + k\frac{m}{mcd(a,m)}(mod\ m),$$

amb $k = 0, \ldots, mcd(a,m) - 1$.

Exemple 1: $3x \equiv 4(mod\ 6)$ no té solució perquè $mcd(3,6) = 3 \not| 4$.

Exemple 2: $3x \equiv 4(mod\ 7)$ té solució perquè $mcd(3,7) = 1 \mid 4$.

La identitat de Bézout en aquest cas és donada per $7 \cdot 1 + 3 \cdot (-2) = 1$. Per tant, la solució a la congruència serà $x \equiv -2 \cdot 4 \equiv 6(mod\ 7)$.

Exemple 3: $34x \equiv 6(mod\ 38)$. Tenim $mcd(a,m) = 2 \mid b = 6$, $mcd(a,m) \not| 1$.

Resolem $17x \equiv 3(mod\ 19)$.

1	0	1	-8	
0	1	-1	9	
		1	8	2
19	17	2	1	0

La solució mòdul 19 és $x \equiv 9 \cdot 3 \equiv 8(mod\ 19)$

Les solucions mòdul 38 són $x \equiv 8(mod\ 38)$ i $x \equiv 27(mod\ 38)$.

Resolució de congruències quadràtiques Les congruències quadràtiques són de la forma

$$ax^2 + bx + c \equiv 0(mod\ m)$$

amb $a \not\equiv 0(mod\ m)$.

Si $m = 2$, aleshores les úniques equacions quadràtiques són les següents i les solucions es poden trobar per cerca exhaustiva.

$x^2 + x + 1 \equiv 0(mod\ 2)$	no té solució;
$x^2 + x \equiv 0(mod\ 2)$	té solució $x \equiv 0(mod\ 2)$ i $x \equiv 1(mod\ 2)$;
$x^2 + 1 \equiv 0(mod\ 2)$	té solució $x \equiv 1(mod\ 2)$;
$x^2 \equiv 0(mod\ 2)$	té solució $x \equiv 0(mod\ 2)$.

Si m és primer i diferent de dos, aleshores les solucions són determinades per

$$x \equiv \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}(mod\ m).$$

Sistemes de congruències lineals

Seran sistemes

$$\begin{cases} \hat{a}_1 x & \equiv & b_1 & (mod\, m_1) \\ \hat{a}_2 x & \equiv & b_2 & (mod\, m_2) \\ & & \vdots & \\ \hat{a}_k x & \equiv & b_k & (mod\, m_k) \end{cases}$$

amb $\hat{a}_i, b_i, m_i$ enters i $m_i > 0$.
Resolent cadascuna de les congruències, obtindrem un sistema de la forma

$$\begin{cases} x & \equiv & a_1 & (mod\, m_1) \\ x & \equiv & a_2 & (mod\, m_2) \\ & & \vdots & \\ x & \equiv & a_k & (mod\, m_k) \end{cases} \tag{1.1}$$

Per exemple, utilitzant les congruències dels exemples 2 i 3,

$$\begin{cases} 3x & \equiv & 4 & (mod\, 7) \\ 34x & \equiv & 6 & (mod\, 38) \end{cases}$$

és equivalent a

$$\begin{cases} x & \equiv & 6 & (mod\, 7) \\ x & \equiv & 8 & (mod\, 19) \end{cases}$$

Teorema 25. [Teorema xinès dels residus.] Si $m_1, m_2, \ldots, m_k$ són coprimers dos a dos, existeix una solució al sistema (1.1) mòdul $M = m_1 \cdot \cdots \cdot m_k$ i és única. La solució és donada per $x \equiv \sum_{i=1}^{k} a_i x_i M_i \ (mod\, M)$, on $M_i = \frac{M}{m_i}$ i x_i és solució de $M_i x \equiv 1 \ (mod\, m_i)$.

Exemple: El sistema $\begin{cases} x & \equiv & 3 & (mod\, 11) \\ x & \equiv & 6 & (mod\, 8) \end{cases}$ té solució $x \equiv 14 \ (mod\, 88)$.

Exemple: El sistema $\begin{cases} 3x & \equiv & 2 & (mod\, 5) \\ -x & \equiv & 1 & (mod\, 6) \\ 2x & \equiv & -1 & (mod\, 7) \end{cases}$ té solució $x \equiv 59 \ (mod\, 210)$.

1.2.3 Anells $\mathbb{Z}_m$

En la proposició 18 hem vist que la relació de congruència és una relació d'equivalència. Per això, podem dividir $\mathbb{Z}$ en m classes d'equivalència donades per la relació de congruència mòdul m. Definim $\mathbb{Z}_m$ com el conjunt de les m classes d'equivalència. Així,

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\},$$

on $[r]_m$ representa la classe de tots els enters que dividits entre m tenen residu r. Per extensió, escriurem $[a]_m = [r]_m$ si $a = qm + r$ amb $0 \leqslant r < m$.

Aritmètica modular

Per la proposició 19 sabem que dins de $\mathbb{Z}_m$ hi ha les dues operacions internes ben definides:

$$[r_1]_m + [r_2]_m = [r_1 + r_2]_m,$$
$$[r_1]_m \cdot [r_2]_m = [r_1 \cdot r_2]_m.$$

L'operació suma a $\mathbb{Z}_m$ és associativa i commutativa per ser-ho a $\mathbb{Z}$. El neutre per la suma és $[0]_m$ i l'invers per la suma està ben definit com

$$-[a]_m = [-a]_m.$$

La resta està ben definida, aleshores, com la suma de l'invers.

L'operació producte a $\mathbb{Z}_m$ és associativa i commutativa per ser-ho a $\mathbb{Z}$ i satisfà la propietat distributiva amb la suma. El neutre pel producte és $[1]_m$.

Per tot l'anterior, $\mathbb{Z}_m$ és un anell commutatiu amb unitat. En general, $\mathbb{Z}_m$ no és un cos perquè pot haver-hi elements que no tinguin invers. Per exemple, a $\mathbb{Z}_4$,

$$[2]_4 \cdot [0]_4 = [0]_4,$$
$$[2]_4 \cdot [1]_4 = [2]_4,$$
$$[2]_4 \cdot [2]_4 = [0]_4,$$
$$[2]_4 \cdot [3]_4 = [2]_4.$$

Per tant, no existeix cap classe $[a]_4$ tal que $[2]_4 \cdot [a]_4 = [1]_4$.

Invertibles i divisors de zero

Sigui $(A, +, \cdot)$ un anell amb neutre 0 respecte a $+$. Els elements d'A que tenen invers es diuen **invertibles**. Un element $a \in A$, $a \neq 0$ és un **divisor de zero** si existeix $b \in A$, $b \neq 0$ tal que $a \cdot b = b \cdot a = 0$.

Proposició 26. Considerem l'anell $\mathbb{Z}_m$ i un element $a \in \mathbb{Z}_m$, $a \neq 0$. Aleshores,

(i) a és invertible si i només si $mcd(a, m) = 1$.

(ii) a és un divisor de zero si i només si $mcd(a, m) \neq 1$.

Prova:

(i) $a \cdot b = 1 \iff ab - km = 1 \iff mcd(a, m) = 1$.

(ii) $\Longrightarrow$. Si $a \cdot b = 0$, aleshores $m \mid a \cdot b$. Si $mcd(m, a) = 1$, aleshores $m \mid b$ i, per tant, $b = 0$.

$\Longleftarrow$. Si $mcd(a, m) \neq 1$, aleshores $\frac{m}{mcd(a,m)} \neq 0$ i $a \cdot \frac{m}{mcd(a,m)} = \frac{a}{mcd(a,m)} \cdot m = 0$.

□

Proposició 27. $\mathbb{Z}_m$ és un cos si i només si m és primer.

Diem $\mathbb{Z}_m^*$ al conjunt d'elements invertibles de $\mathbb{Z}_m$.

Funció d'Euler

Definim, equivalentment,

$$\begin{aligned}\phi(m) &= \#\{a : 0 \leqslant a < m \text{ i } mcd(a,m) = 1\} \\ &= \#\mathbb{Z}_m^*\end{aligned}$$

Proposició 28.
- Si p és primer, aleshores $\phi(p) = p - 1$.
- Si $mcd(a,b) = 1$, aleshores $\phi(ab) = \phi(a)\phi(b)$.
- Si p és primer, aleshores $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

El primer punt es pot veure directament de la definició de ϕ. L'últim punt es pot comprovar veient que exactament 1 de cada p enters entre 0 i $p^k - 1$ és no coprimer amb p^k.

Com a conseqüència, si la descomposició d'un enter n en producte de primers és $n = p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$, aleshores

$$\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdot \cdots \cdot p_k^{n_k-1}(p_k - 1).$$

Teorema de Fermat i teorema d'Euler

Teorema 29. [Teorema de Fermat.] Si p és primer i $mcd(a,p) = 1$, aleshores

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Teorema 30. [Teorema d'Euler.] Si $mcd(a,m) = 1$, aleshores

$$a^{\phi(m)} \equiv 1 \ (mod\ m).$$

Els teoremes anteriors són útils per trobar elements inversos. En efecte, si a és no nul a $\mathbb{Z}_p$, aleshores

$$a^{-1} = a^{p-2} \ (mod\ p)$$

i si a és invertible a $\mathbb{Z}_m$, aleshores

$$a^{-1} = a^{\phi(m)-1} \ (mod\ m).$$

Ordre i elements primitius

L'**ordre** d'un element de $\mathbb{Z}_m$ és el mínim exponent diferent de 0 al qual l'hem d'elevar perquè ens doni 1. Un element de $\mathbb{Z}_m$ és **primitiu** si el seu ordre és $\phi(m)$.

Si $a^k = 1$ a $\mathbb{Z}_m$, aleshores l'ordre d'a divideix k. En particular, l'ordre de qualsevol element divideix $\phi(m)$.

No ha d'existir necessàriament un element primitiu. Per exemple, a $\mathbb{Z}_{24}$ no hi ha elements primitius (vegeu la secció 1.2.3). Si n'existeix un, β, aleshores les seves potències cobreixen tot $\mathbb{Z}_m^*$. Es té que β^j també és primitiu si i només si $mcd(j, \phi(m)) = 1$. Per això, si hi ha un element primitiu, aleshores n'hi ha $\phi(\phi(m))$.

Annex 1: Exponenciació modular ràpida

L'objectiu d'aquest apartat és calcular $a^N \ (mod\ m)$ de manera eficient.

Reducció de la base i de l'exponent

Proposició 31.
- Si $a = mq + r$ amb $0 \leqslant r < m$ i $mcd(a, m) = 1$, aleshores $a^N = r^N \ (mod\, m)$.
- Si $N = \phi(m)q + r$ amb $0 \leqslant r < \phi(m)$, aleshores $a^N = a^r \ (mod\, m)$.

Algoritme d'elevar i multiplicar

Si l'expressió de N amb base 2 és $n_k n_{k-1} \dots n_1 n_0$, aleshores N es pot obtenir pel següent algoritme:

```
N=0;
for(i=k;i>=0;i--)
  {
  N=N+N;
  if(n_i)
     N=N+1;
  }
```

Observem que el pas $N := N + N$ és equivalent a multiplicar N per 2 o, equivalentment, afegir un 0 a la dreta de la seva expressió en base 2. En canvi, el pas $N := N + 1$ després d'haver afegit un zero a la dreta és equivalent a canviar per 1 l'últim 0 de l'expressió en base 2 de N.

Prenem per exemple $13 = 1101_2$. En aquest cas $k = 3$. L'algoritme anterior ens donaria successivament els següents valors:

Inicialment, $N = 0$,

per $k = 3$, $\begin{cases} N := N + N = 0, \\ N := N + 1 = 1, \end{cases}$

per $k = 2$, $\begin{cases} N := N + N = 10_2 = 2, \\ N := N + 1 = 11_2 = 3, \end{cases}$

per $k = 1$, $\{ \ N := N + N = 110_2 = 6,$

per $k = 0$, $\begin{cases} N := N + N = 1100_2 = 12, \\ N := N + 1 = 1101_2 = 13. \end{cases}$

Observem que el pas $N \to N + N$ en l'exponent equival al pas $a^N \to a^{N+N} = a^N \cdot a^N$ en la potència. És el que en direm un pas d'elevar E. En canvi, el pas $N \to N + 1$ en l'exponent equival al pas $a^N \to a^{N+1} = a^N \cdot a$ en la potència. És el que en direm un pas de multiplicar M.

Així, l'algoritme d'elevar i multiplicar és el següent:

```
pot:=1;
for(i=k;i>=0;i--)
  {
  pot=pot*pot;
  if(n_i)
     pot=pot*a;
  }
```

Prenem per exemple $6^{13} \ (mod\, 55)$. L'algoritme anterior ens donaria successivament els següents valors:

Inicialment, $pot = 1$,

per $k=3$, $\begin{cases} pot := pot \cdot pot = 1, \\ pot := pot \cdot a = 6, \end{cases}$
per $k=2$, $\begin{cases} pot := pot \cdot pot = 36, \\ pot := pot \cdot a = 216 = 51, \end{cases}$
per $k=1$, $\{ \; pot := pot \cdot pot = 2585 = 16,$
per $k=0$, $\begin{cases} pot := pot \cdot pot = 256 = 36, \\ pot := pot \cdot a = 216 = 51. \end{cases}$
Per tant, $6^{13} = 51 \; (mod \; 55)$.

Annex 2: Criptosistema RSA

Proposició 32. Siguin

- p i q primers diferents,
- $n = p \cdot q$,
- $t \equiv 1 \; (mod \; \phi(n))$.

Aleshores, per a tot enter x amb $0 \leqslant x < n$ es té

$$x^t \equiv x \; (mod \; n).$$

Prova: N'hi ha prou si ho provem per x primer, ja que, altrament, si $x = p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$ i la congruència es compleix per a tot primer, aleshores $x^t = (p_1^t)^{n_1} \cdot \cdots \cdot (p_k^t)^{n_k} = p_1^{n_1} \cdot \cdots \cdot p_k^{n_k} = x$.

Suposem $t = k\phi(n) + 1$ i x primer.

Cas $x = p$: $p^{q-1} = 1 \; (mod \; q) \Longrightarrow p^{\phi(n)} = (p^{q-1})^{p-1} = 1 \; (mod \; q) \Longrightarrow p^{t-1} = p^{k\phi(n)} = 1 \; (mod \; q) \Longrightarrow p^t = p \; (mod \; n)$.

Cas $x = q$ equivalent al cas $x = p$.

Cas $x \neq p$ i $x \neq q$: Com que $mcd(x, n) = 1$, $x^{\phi(n)} = 1 \; (mod \; n) \Longrightarrow x^{t-1} = 1 \; (mod \; n) \Longrightarrow x^t = x \; (mod \; n)$. □

Criptosistema RSA (Rivest, Shamir, Adleman, 1977)

En Bob ha de rebre una informació confidencial de l'Alice.

En Bob escull arbitràriament:

- Dos primers *grans* p i q.
- Un enter e amb $1 \leqslant e < \phi(pq) = (p-1)(q-1)$ tal que $mcd(e, \phi(pq)) = 1$ o, equivalentment, un element de $\mathbb{Z}^*_{\phi(pq)}$.

Direm $n = pq$. En Bob calcula $d = e^{-1} \; (mod \; \phi(n))$ i obté així:
CLAU PÚBLICA: (n, e)
CLAU PRIVADA: d

Els valors $p, q, \phi(n)$ es guarden en secret, ja que faciliten el càlcul de d. La potència del criptosistema RSA rau en la dificultat de factoritzar n, és a dir, trobar p i q a partir de n.

Quan l'Alice ha d'enviar el missatge m amb $1 < m < n$, utilitza el **xifratge**:

$$c = m^e \; (mod \; n).$$

Quan en Bob ha de llegir el missatge enviat per l'Alice, utilitza el **desxifratge**:

$$c^d \ (mod\ n) = m^{ed} \ (mod\ n) = m \ (mod\ n).$$

Exemple: $p = 5$, $q = 11$, ($\Longrightarrow n = 5 \cdot 11 = 55$, $\phi(n) = (5-1)(11-1) = 40$), $e = 13$. La identitat de Bézout per a 40 i 13 és $40 \cdot 1 + 13 \cdot (-3) = 1$, d'on $13^{-1} = -3 = 37 \ (mod\ 40)$.

Suposem que el missatge que s'ha d'enviar és $m = 6$.

Xifratge: $c = 6^{13} \ (mod\ 55) = 51 \ (mod\ 55)$ (ho hem vist com a exemple de l'algoritme d'elevar i multiplicar).

Desxifratge: $51^{37} \ (mod\ 55)$.

Com que $37 = 100101_2$, utilitzant l'algoritme d'elevar i multiplicar,

$$1 \overset{E}{\longrightarrow} 1 \overset{M}{\longrightarrow} 51 \overset{E}{\longrightarrow} 51 \cdot 51 = 2601 = 16 \overset{E}{\longrightarrow} 16 \cdot 16 = 256 = 36 \overset{E}{\longrightarrow} 36 \cdot 36 = 1296 = 31 \overset{M}{\longrightarrow} 31 \cdot 51 = 1581 = 41 \overset{E}{\longrightarrow} 41 \cdot 41 = 1681 = 31 \overset{E}{\longrightarrow} 31 \cdot 31 = 961 = 26 \overset{M}{\longrightarrow} 26 \cdot 51 = 1326 = 6,$$

d'on $51^{37} = 6 \ (mod\ 55)$ i el text desxifrat és $6 \ (mod\ 55)$.

Exemple desconcertant: $p = 5$, $q = 7$, ($\Longrightarrow n = 5 \cdot 7 = 35$, $\phi(n) = (5-1)(7-1) = 24$), $e = 13$.

El desconcert: Per a qualsevol clau pública $(35, e)$ que escollim, la clau privada serà $d = e$. En efecte, els invertibles de $\mathbb{Z}_{24}$ són

$$\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

i els seus quadrats a $\mathbb{Z}_{24}$ són

$$1^2 = 1,\ 5^2 = 25 = 1,\ 7^2 = 49 = 1,\ 11^2 = 121 = 1,\ 13^2 = 169 = 1,$$

$$17^2 = 289 = 1,\ 19^2 = 361 = 1,\ 23^2 = 529 = 1.$$

Per tant, tots són inversos d'ells mateixos a $\mathbb{Z}_{24}$.

La maledicció del 13: A $\mathbb{Z}_{35}$ es compleix $a^{13} = a$ per a qualsevol $a \in \mathbb{Z}_{35}$. Això voldrà dir que, si en Bob escull com a clau pública $(35, e = 13)$, a part que la clau privada haurà de ser $d = e = 13$, es tindrà que qualsevol missatge xifrat serà igual al missatge en clar.

Podeu comprovar tots aquests resultats amb magma, a través de la calculadora online (http://magma.maths.usyd.edu.au/calc) i utilitzant el següent codi:

```
print "L'anell Z_24 es defineix per Integers(24):";
Integers(24);
[a: a in Integers(24)];

print " ";
print "De Integers(24) escollim aquells que siguin invertibles:";
[a: a in Integers(24) | IsInvertible(a)];

print " ";
print "Calculem els quadrats dels invertibles de Integers(24):";
[a^2: a in Integers(24) | IsInvertible(a)];
print "i comprovem que tots son 1.";
```

```
print " ";
print "Calculem els inversos dels invertibles de Integers(24):";
[a^(-1): a in Integers(24) | IsInvertible(a)];
print "i comprovem que tots els elements invertibles de Integers(24)
son inversos d'ells mateixos.";

print " ";
print "L'anell Z_35 es defineix per Integers(35):";
Integers(35);
[a: a in Integers(35)];

print " ";
print "Calculem a^13 per tots els elements de Integers(35):";
[a^13: a in Integers(35)];
print "i comprovem que tots els elements de Integers(35)
romanen inalterats en elevar-los a 13."
```

1.3 Aritmètica polinomial

1.3.0 Polinomis

Els **polinomis** sobre un cos K són els objectes de la forma

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0,$$

on $a_i \in K$ per a tot i. Els a_i s'anomenen **coeficients**. Denotem per $K[x]$ el conjunt de tots els **polinomis** amb coeficients a K. Diem que d és el **grau** del polinomi i que a_i és el coeficient de grau i. El grau d'un polinomi és 0 si i només si és una constant no nul·la. Un polinomi és zero si i només si tots els seus coeficients són zero. En aquest cas, diem que el grau és $-\infty$.

1.3.1 Divisió euclidiana i identitat de Bézout

Divisió de polinomis

Donats dos polinomis $f(x)$ i $g(x)$, existeix un únic polinomi $q(x)$ i un únic polinomi $r(x)$ tals que

$$f(x) = q(x)g(x) + r(x)$$

amb grau$(r(x)) <$ grau$(g(x))$. Diem que $q(x)$ és el **quocient** de la divisió i que $r(x)$ és el **residu** de la divisió.

Exemple: $f(x) = x^5 + 3x^3 - 8x^2 + 1$, $g(x) = x^3 - 2$. En aquest cas, $q(x) = x^2 + 3$ i $r(x) = -6x^2 + 7$.

Diem que $g(x)$ **divideix** $f(x)$ si $r(x)$ és 0. És a dir, si $f(x) = q(x)g(x)$.

Algoritme d'Euclides i identitat de Bézout

El màxim comú divisor, l'algoritme d'Euclides i la identitat de Bézout per a polinomis es poden definir de forma anàloga a com ho hem fet per als enters.

Exemple: Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$.

Utilitzem la mateixa taula que en l'apartat 1.2.1.

1	0	1	$x+2$	$\mathbf{2x^2+4x+1}$	
0	1	$4x^2+x+4$	$4x^3+4x^2+x+4$	$\mathbf{3x^4+3x^3+x^2+4x+4}$	
		x^2+4x+1	$4x+3$	$3x$	$3x+2$
x^5+x+1	x^3+x^2	$4x^2+x+1$	$3x+2$	$\mathbf{1}$	0

Deduïm que el màxim comú divisor és 1 i que els coeficients de la identitat de Bézout són $2x^2+4x+1$ i $3x^4+3x^3+x^2+4x+4$.

Per tant, la identitat de Bézout queda de la forma

$$(2x^2+4x+1)(x^5+x+1)+(3x^4+3x^3+x^2+4x+4)(x^3+x^2)=1.$$

Arrels de polinomis

Diem que α és arrel de $f(x)$ si $f(\alpha)=0$.

Lema 33. α és arrel de $f(x)$ si i només si $x-\alpha$ divideix $f(x)$.

Prova:

$\Rightarrow$ α arrel $\Rightarrow$ $f(\alpha)=0$. Fem la divisió de $f(x)$ per $x-\alpha$.

$$f(x)=q(x)(x-\alpha)+r(x)$$

$r(x)$ tindrà grau <1 $\Rightarrow r(x)$ ha de ser una constant $k\in K$.

$$f(\alpha)=q(\alpha)(\alpha-\alpha)+k=k=0$$

$\Rightarrow$ $r(x)=0$ $\Rightarrow$ $x-\alpha$ divideix $f(x)$.

$\Leftarrow$ Si $x-\alpha$ divideix $f(x)$, aleshores $f(x)=q(x)(x-\alpha)$, d'on és evident que $f(\alpha)=q(\alpha)(\alpha-\alpha)=0$.

□

Polinomis irreductibles i factorització

Un polinomi $f(x)\in K[x]$ no constant és **irreductible** si no es pot descompondre en producte de polinomis no constants. Es considera que els polinomis constants no són irreductibles.

Teorema 34. **(i)** Qualsevol polinomi no constant es pot expressar com a producte d'irreductibles.

(ii) Qualsevol polinomi no constant es pot expressar de manera única com a producte d'irreductibles mònics per una constant.

Corol· lari 35. El número d'arrels d'un polinomi és com a molt el seu grau.

Corol· lari 36. Si el polinomi $f(x)$ no té cap factor de grau menor o igual que $\frac{\text{grau}(f)}{2}$, aleshores és irreductible.

Corol· lari 37. Un polinomi de grau 2 o 3 és irreductible si i només si no té arrels.

El resultat no és cert en general per a polinomis de qualsevol grau. En efecte, $(x^2+1)^2$ no té arrels a $\mathbb{R}$, però no és irreductible a $\mathbb{R}$.

1.3.2 Congruències

Proposició 38. Donats polinomis $a(x), b(x)$ i $m(x) \neq 0$, és equivalent:

- Els residus de dividir $a(x)$ i $b(x)$ entre $m(x)$ coincideixen.
- $a(x) - b(x)$ és un múltiple de $m(x)$.

Dos polinomis $a(x)$ i $b(x)$ són **congruents mòdul** el polinomi no nul $m(x)$ si es compleixen les condicions equivalents de la proposicio 38. En aquest cas, escrivim $a(x) \equiv b(x)(mod\, m(x))$ o $a(x) = b(x)(mod\, m(x))$.

Proposició 39. Si $a(x) \equiv b(x)\ (mod\, m(x))$ i $d(x)$ divideix $m(x)$, aleshores $a(x) \equiv b(x)\ (mod\, d(x))$.

Proposició 40. La relació de congruència és una relació d'equivalència (propietat reflexiva, propietat simètrica i propietat transitiva).

Proposició 41. [La suma i el producte de classes queden ben definits.] Si $a_1(x) \equiv a_2(x)(mod\, m(x))$ i $b_1(x) \equiv b_2(x)(mod\, m(x))$, aleshores $a_1(x) + b_1(x) \equiv a_2(x) + b_2(x)(mod\, m(x))$ i $a_1(x) \cdot b_1(x) \equiv a_2(x) \cdot b_2(x)(mod\, m(x))$.

Com a conseqüència, si $a(x) \equiv b(x)(mod\, m(x))$, aleshores $k(x)a(x) \equiv k(x)b(x)(mod\, m(x))$. Però el recíproc no és cert. **La simplificació no queda ben definida**. És a dir, pot ser que $k(x)a(x) \equiv k(x)b(x)(mod\, m(x))$, però, en canvi, $a(x) \not\equiv b(x)(mod\, m(x))$.

Proposició 42. $k(x)a(x) \equiv k(x)b(x)(mod\, m(x))$ si i només si $a(x) \equiv b(x)(mod\, \frac{m(x)}{mcd(m(x),k(x))})$.

Corol· lari 43. Es podrà simplificar sempre que $mcd(m(x), k(x)) \in K$.

Corol· lari 44. [Per simplificar hem de simplificar també el mòdul.] Si $k(x) \neq 0$, aleshores $k(x)a(x) \equiv k(x)b(x)(mod\, k(x)m(x))$ si i només si $a(x) \equiv b(x)(mod\, m(x))$.

1.3.3 Anells $K[x]/(m(x))$

En la proposició 40 hem vist que, per a un polinomi no nul $m(x)$, la relació de congruència mòdul $m(x)$ és una relació d'equivalència. Per això, podem dividir $K[x]$ en les corresponents classes d'equivalència. La classe del polinomi $f(x)$ es representa per $[f(x)]_{m(x)}$. Definim $K[x]/(m(x))$ com el conjunt d'aquestes classes:

$$K[x]/(m(x)) = \{[f(x)]_{m(x)} : f(x) \in K[x]\}.$$

Per la proposició 41 sabem que dins de $K[x]/(m(x))$ hi ha les dues operacions internes ben definides:

$$[a(x)]_{m(x)} + [b(x)]_{m(x)} = [a(x) + b(x)]_{m(x)},$$

$$[a(x)]_{m(x)} \cdot [b(x)]_{m(x)} = [a(x) \cdot b(x)]_{m(x)}.$$

L'operació suma a $K[x]/(m(x))$ és associativa i commutativa per ser-ho a $K[x]$. El neutre per la suma és $[0]_{m(x)}$ i l'invers per la suma està ben definit com

$$-[a(x)]_{m(x)} = [-a(x)]_{m(x)}.$$

La resta està ben definida aleshores, com la suma de l'invers.

L'operació producte a $K[x]/(m(x))$ és associativa i commutativa per ser-ho a $K[x]$ i satisfà la propietat distributiva amb la suma. El neutre pel producte és $[1]_{m(x)}$.

Per tot l'anterior, $K[x]/(m(x))$ és un anell commutatiu amb unitat. En general $K[x]/(m(x))$ no és un cos perquè pot haver-hi elements que no tinguin invers.

Teorema 45. Si $m(x)$ és irreductible a $K[x]$, aleshores $K[x]/(m(x))$ és un cos.

1.4 Cossos finits

1.4.1 Construcció

Sigui $\mathbb{Z}_p[x]$ el conjunt de polinomis amb coeficients a $\mathbb{Z}_p$ i sigui $f(x)$ un polinomi irreductible de $\mathbb{Z}_p[x]$ de grau n.

Donat un polinomi qualsevol $g(x)$ de $\mathbb{Z}_p[x]$, tindrem que el residu de dividir $g(x)$ per $f(x)$ és un polinomi de grau menor que n. Per tant, els residus de dividir tots els polinomis de $\mathbb{Z}_p[x]$ per $f(x)$ seran tots els polinomis de grau menor que n.

Considerem ara el quocient $\mathbb{Z}_p[x]/(f(x))$. Aquest quocient és el conjunt de classes de polinomis de $\mathbb{Z}_p[x]$ mòdul $f(x)$. És a dir, cada polinomi s'identifica amb el residu de dividir-lo per $f(x)$.

Diguem α a la classe de x en el quocient $\mathbb{Z}_p[x]/(f(x))$. Tindrem que tots els elements de $\mathbb{Z}_p[x]/(f(x))$ es poden esciure de la forma

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0, \tag{1.2}$$

amb $a_i \in \mathbb{Z}_p$. És fàcil de comprovar que, d'aquests elements, n'hi ha p^n. A més com que $f(x)$ és irreductible, es té que tots aquests elements formen un cos. És el cos que anomenem $\mathbb{F}_{p^n}$ o $\boldsymbol{GF(p^n)}$. Diem que p és la **característica** de $\mathbb{F}_{p^n}$.

Si un element del cos finit $\mathbb{F}_{p^n}$ el tenim expressat com un polinomi en la classe de x, és a dir, com a (1.2), aleshores diem que està expressat en **notació polinòmica**. Aquesta notació és molt útil per **sumar i restar elements del cos finit**. No serà tan bona a l'hora de fer multiplicacions i divisions.

1.4.2 Ordre i elements primitius

L'**ordre d'un element** no nul $\gamma \in \mathbb{F}_q$ és el mínim enter r tal que $\gamma^r = 1$. Qualsevol element γ no nul de $\mathbb{F}_q$ compleix $\gamma^{q-1} = 1$ i $\gamma^q = \gamma$. L'ordre sempre divideix $q-1$.

Un element β no nul de $\mathbb{F}_q$ és un **element primitiu** si el seu ordre és $q-1$. Això significa que en el conjunt

$$\{0, 1, \beta, \beta^2, \beta^3, \ldots, \beta^{q-3}, \beta^{q-2}\}$$

tots els elements són diferents. Com que n'hi ha q i tots pertanyen a $\mathbb{F}_q$, són exactament tots els elements de $\mathbb{F}_q$.

Sempre existeix almenys un element primitiu. Això ens permet escriure qualsevol element no nul de $\mathbb{F}_q$ com una potència de l'element primitiu. És el que anomenem **notació potencial**. Amb aquesta notació ens serà molt fàcil **multiplicar i dividir elements del cos finit**.

Diem que el polinomi $f(x) \in \mathbb{Z}_p[x]$ és un **polinomi primitiu** si la classe de x és un element primitiu a $\mathbb{Z}_p[x]/(f(x))$. Per tot p i tot n, existeix almenys un polinomi primitiu a $\mathbb{Z}_p[x]$ de grau n.

1.4.3 Extensions de cossos finits

La mateixa construcció que hem fet en la secció 1.4.1 a partir d'un polinomi irreductible a $\mathbb{Z}_p[x]$ es pot fer a partir d'un polinomi irreductible a $\mathbb{F}_q[y]$ on q és una potència d'un primer ($q = p^n$).

Suposem que $g(y)$ és un polinomi irreductible de grau m de $\mathbb{F}_q[y]$. Aleshores, $\mathbb{F}_q[y]/(g(y))$ és un cos finit de q^m elements. Es diu que és una **extensió de $\mathbb{F}_q$**. Si β és la classe de y, llavors tots els elements de $\mathbb{F}_q[y]/(g(y))$ es poden escriure de la forma

$$b_{m-1}\beta^{m-1} + b_{m-2}\beta^{m-2} + \cdots + b_1\beta + b_0,$$

amb $b_i \in \mathbb{F}_q$.

En particular, $\mathbb{F}_q$ està inclòs en $\mathbb{F}_{q^m}$. Es diu que és un **subcòs**.

Es pot demostrar que totes aquestes extensions admeten una construcció com la de la secció 1.4.1. És a dir, existeix un polinomi irreductible $f(x) \in \mathbb{Z}_p[x]$ de grau $m \cdot n$ tal que

$$\mathbb{F}_q[y]/(g(y)) = \mathbb{Z}_p[x]/(f(x)).$$

Per tant, p és també la característica de $\mathbb{F}_{q^m}$.

1.4.4 Polinomi mínim

Observem que, si un element $\gamma \in \mathbb{F}_{p^n}$ té ordre r, aleshores anul·la els polinomis $x^r - 1$ i $x^{p^n-1} - 1$.

Anomenem **polinomi mínim respecte a $\mathbb{Z}_p$** de γ el polinomi de $\mathbb{Z}_p[x]$ mònic (i.e. amb coeficient de grau màxim igual a 1) de grau mínim d'entre tots els que s'anul·len quan els avaluem a γ. El denotem $m_\gamma(x)$. Es compleix que

$$m_\gamma(x) = (x-\gamma)(x-\gamma^p)(x-\gamma^{p^2}) \cdot \cdots \cdot (x-\gamma^{p^{s-1}}),$$

on s és el mínim enter positiu tal que $\gamma^{p^s} = \gamma$. En particular, $s \leqslant n$ i si γ és primitiu, aleshores $s = n$. L'exponent s coincideix amb el grau de $m_\gamma(x)$ i s'anomena **grau** de γ.

Si un polinomi s'anul·la quan l'avaluem a γ aleshores és divisible per $m_\gamma(x)$.

Si $\mathbb{F}_{q^m}$ és una extensió del cos finit $\mathbb{F}_q$ i $\gamma \in \mathbb{F}_{q^m}$, aleshores el **polinomi mínim respecte al subcòs $\mathbb{F}_q$** de γ és el polinomi de $\mathbb{F}_q[x]$ mònic de grau mínim d'entre tots els que s'anul·len quan els avaluem a γ. El denotem $m_{\gamma(\mathbb{F}_q)}(x)$.

Es compleix que

$$m_{\gamma(\mathbb{F}_q)}(x) = (x-\gamma)(x-\gamma^q)(x-\gamma^{q^2}) \cdot \cdots \cdot (x-\gamma^{q^{t-1}}),$$

on t és el mínim enter positiu tal que $q^t = 1$.

1.5 Codis lineals

Un **codi lineal** C de **longitud** n sobre un alfabet $\mathbb{F}_q$ és un subespai vectorial de $\mathbb{F}_q^n$. La **dimensió** k del codi és la dimensió del subespai i la **taxa de transmissió és** $\frac{k}{n}$. La **codimensió** és $n-k$.

Diem que una matriu G de k files i n columnes és una **matriu generadora** de C si les seves files són un conjunt de vectors generadors del codi. La matriu generadora no és única, es poden intercanviar files, per exemple. Per codificar una paraula de k símbols de $\mathbb{F}_q$, la multipliquem per la matriu generadora. Diem que una matriu generadora és **sistemàtica** en les primeres posicions (o en les darreres) si conté la identitat en les primeres posicions (o en les darreres). En codificar utilitzant una matriu generadora sistemàtica, la informació es repeteix en aquelles posicions on la matriu és sistemàtica.

El **codi dual** (o ortogonal) de C és $C^\perp = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ per a tot } c \in C\}$. És un codi lineal de la mateixa longitud que C i de dimensió $n-k$. Es pot definir a partir d'un sistema d'equacions lineals amb matriu G. Una matriu H generadora de $C^\perp$ es diu que és una **matriu de control** de C. Equivalentment, una matriu de control de C és una matriu tal que el codi C es pot redefinir com $C = \{c \in \mathbb{F}_q^n : c \cdot h = 0 \text{ per a tota fila } h \text{ de } H\}$. Si una matriu generadora és $G = (I|P)$, aleshores una matriu de control és $H = (-P^T|I)$ i, si una matriu generadora és $G = (P|I)$, aleshores una matriu de control és $H = (I|-P^T)$. Anàlogament, si una matriu de control és $H = (I|P)$, aleshores una matriu generadora és $G = (-P^T|I)$ i, si una matriu de control és $H = (P|I)$, aleshores una matriu generadora és $G = (I|-P^T)$.

La **distància de Hamming** entre dues paraules de la mateixa longitud és el número de posicions on difereixen. El **pes** d'una paraula és el número de posicions no nul·les o, equivalentment, la seva distància de Hamming al vector nul. La **distància mínima** d d'un codi lineal C es pot definir indistintament com

- La mínima distància de Hamming entre dues paraules de C.
- El mínim pes de les paraules no nul·les de C.
- El mínim número de columnes linealment dependents de H.

La **fita de Singleton** estableix que en un codi de longitud n i distància mínima d, la dimensió k satisfà $k \leqslant n - d + 1$.

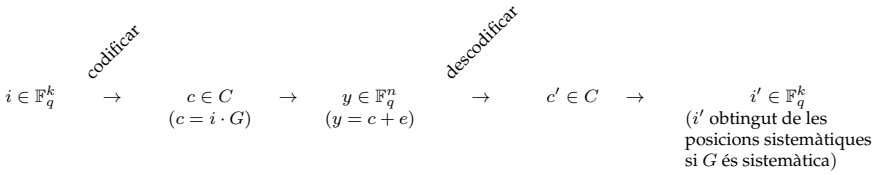
La **capacitat correctora** d'un codi de distància mínima d és $\lfloor \frac{d-1}{2} \rfloor$. Utilitzant un codi de distància mínima d, es podran detectar $d-1$ errors, corregir $d-1$ esborralls i corregir $\lfloor \frac{d-1}{2} \rfloor$ errors.

Detecció d'errors. Si la paraula rebuda y no satisfà $H \cdot y = 0$, aleshores podem afirmar que hi ha hagut error.

Correcció d'esborralls. Considerant els esborralls com a incògnites, a partir de $H \cdot c = 0$ obtenim un sitema lineal d'equacions. Si el número d'esborralls és com a màxim $d-1$ aleshores el sistema és compatible i determinat.

Correcció d'errors. La **síndrome** d'un vector v és $H \cdot v$. Una paraula c és de C si i només si la seva síndrome és zero. La síndrome d'una paraula amb error ($y = c + e$, $c \in C$) coincideix amb la síndrome del vector d'error ($H \cdot y = H \cdot (c+e) = H \cdot c + H \cdot e = H \cdot e$). **Quan la capacitat correctora és** 1**:** Si només es produeix un error, aleshores la paraula d'error ha de ser $(0, \ldots, 0, x_i, 0, \ldots, 0)$ i la síndrome $s = H^i x_i$, on H^i és la columna i-èssima de H. Buscant quina columna de H és un múltiple de s, tindrem la posició d'error; buscant l'únic valor x_i tal que $s = H^i x_i$, tindrem el valor de l'error. **Cas general:** La descodificació per **màxima versemblança** consisteix a descodificar y per $y - e'$ on e' és un vector de $\mathbb{F}_q^n$ amb mínim pes d'entre els que tenen la mateixa síndrome que y. La descodificació és única si el número d'errors és, com a màxim, la capacitat correctora.

Procés de codificació - descodificació:



El **codi de Hamming** de paràmetre t sobre $\mathbb{F}_q$ és el codi sobre $\mathbb{F}_q$ de màxima taxa de transmissió d'entre els que tenen codimensió t i capacitat correctora 1. Com que la taxa de transmissió és $\frac{k}{n} = \frac{n-t}{n} = 1 - \frac{t}{n}$ i, d'altra banda, $\frac{k}{n} = \frac{k}{t+k} = \frac{1}{1+\frac{t}{k}}$, això és equivalent al fet que la dimensió sigui màxima i també que la longitud sigui màxima. Per obtenir-lo, construirem una matriu de control de t files i el màxim número de columnes linealment independents dues a dues. Els seus paràmetres són $n = \frac{q^t-1}{q-1}$, $k = n - t$ i $d = 3$. El codi de Hamming de longitud n i dimensió k sobre $\mathbb{F}_q$ es denota $H_q(n, k)$. Així, el codi de Hamming de paràmetre t es denota $H(\frac{q^t-1}{q-1}, \frac{q^t-1}{q-1} - t)$. Els codis de Hamming són perfectes. Això significa que qualsevol paraula de $\mathbb{F}_q^n$ està a distància 1 d'una paraula del codi. En efecte, la descodificació explicada per al cas d'un error sempre tindrà una única solució, ja que, per construcció, qualsevol síndrome possible serà linealment dependent amb una i només una columna de H.

La **probabilitat residual d'error al símbol (al bit)** és la probabilitat d'error en la transmissió d'un símbol (d'un bit) que s'obté codificant, transmetent i descodificant. Si b és el número de bits per símbol,

$$(1 - p_{r_{simb}})^k = (1 - p_{r_{bit}})^{b \cdot k} = \begin{array}{l}\text{Prob. de les paraules}\\ \text{descodificables correctament.}\end{array}$$

El guany del codi és

$$10\log_{10}\left(\frac{p_{err_{bit}}}{p_{r_{bit}}}\right) dB$$

1.6 Codis cíclics

Diem que un codi lineal és **cíclic** si per a tota paraula $(c_0, c_1, \ldots, c_{n-1})$ del codi i per a tot $0 \leqslant i \leqslant n-1$ es té que $(c_i, c_{i+1}, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{i-1})$ també pertany al codi.

Per treballar amb codis cíclics, identifiquem els vectors amb polinomis

$$(v_0, v_1, \ldots, v_{n-1}) \leftrightarrow v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1}.$$

Per això, sovint indexarem dins de $0 \dots n-1$ en comptes de $1 \dots n$.

Tot codi cíclic C té un **polinomi generador** $g(x)$ tal que

$$v \in C \iff v(x) \text{ és divisible per } g(x).$$

El polinomi generador divideix $x^n - 1$ i té grau $n-k$. Si el codi està definit sobre $\mathbb{F}_q$ i $n = q-1$, aleshores diem que el codi és **primitiu**. En aquest cas és clar que $x - \beta$ divideix $x^n - 1$ per a tot $\beta \in \mathbb{F}_q^*$. Si el polinomi generador és $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{n-k} x^{n-k}$, aleshores com a matriu generadora podem prendre

$$\begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & & & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & & 0 \\ 0 & 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix}.$$

El **polinomi de control** de C es defineix per $h(x) = \frac{x^n-1}{g(x)}$ i compleix

$$v(x) \in \mathcal{C} \iff v(x)h(x) = 0 \bmod x^n - 1.$$

Una matriu de control del codi cíclic C es pot trobar per tres procediments diferents:

- A partir d'una matriu generadora sistemàtica,

$$G = (Id|P) \Longrightarrow H_1 = (-P^T|Id).$$

- A partir del polinomi $h^*(x)$ recíproc del de control (té els coeficients en ordre invers).

$$H_2 = \text{matriu generadora del codi cíclic generat per } h^*(x).$$

- Si totes les arrels $\beta_1, \beta_2, \dots, \beta_{n-k}$ de g són diferents,

$$H_3 = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \dots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \dots & \beta_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta_{n-k} & \beta_{n-k}^2 & \dots & \beta_{n-k}^{n-1} \end{pmatrix}.$$

  Cal tenir en compte que H_3 pot tenir files dependents.

  En aquest cas, les síndromes de $v(x)$ seran $v(\beta_1)$, $v(\beta_2)$, $v(\beta_3)$ ...

Per codificar sistemàticament una informació i de k símbols, podem fer-ho per dos procediments:

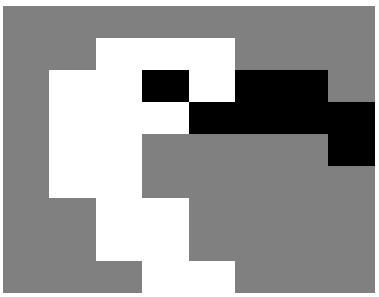
- Multipliquem i per una matriu generadora sistemàtica G. La codificació que obtenim és sistemàtica en les posicions on hi hagi la identitat dins de G.

- Suposem que $R(x)$ és el residu de dividir $i(x)x^{n-k}$ entre $g(x)$. Llavors $i(x)x^{n-k} - R(x)$ és múltiple de $g(x)$ i és una codificació de i sistemàtica en les últimes posicions.

La **distància mínima prevista** de C és el màxim enter d tal que hi ha $d-1$ arrels de g que són potències consecutives d'α ($\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2}$). Es compleix que, si δ és la distància mínima real del codi, aleshores $\delta \geqslant d$.

Exemple de codificació i descodificació amb un codi cíclic

Suposem una imatge digital.

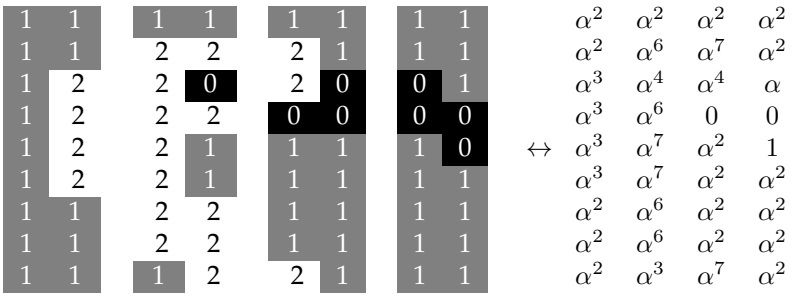


La representem amb símbols de $\mathbb{F}_3 = \mathbb{Z}_3$.

1	1	1	1	1	1	1	1
1	1	2	2	2	1	1	1
1	2	2	0	2	0	0	1
1	2	2	2	0	0	0	0
1	2	2	1	1	1	1	0
1	2	2	1	1	1	1	1
1	1	2	2	1	1	1	1
1	1	2	2	1	1	1	1
1	1	1	2	2	1	1	1

La podem pensar també com si els seus elements fossin de $\mathbb{F}_9 = \mathbb{Z}_3/(x^2 + 2x + 2)$. La representació vectorial dels elements d'aquest cos ve donada per la taula següent, on $\alpha = [x]$:

0	$(0,0)$
α^0	$(1,0)$
α^1	$(0,1)$
α^2	$(1,1)$
α^3	$(1,2)$
α^4	$(2,0)$
α^5	$(0,2)$
α^6	$(2,2)$
α^7	$(2,1)$



Considerem el codi cíclic sobre $\mathbb{F}_9$ primitiu amb polinomi generador $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2$.

Com que el codi és primitiu, té longitud $n = 9 - 1 = 8$. Com que el grau del polinomi generador és $n - k = 4$, aleshores la dimensió del codi és $k = 4$.

Això vol dir que en codificar agafem blocs de $k = 4$ símbols i els codifiquem, de manera que obtenim blocs de $n = 8$ símbols.

Codificació directa

Si fem codificació directa, aleshores simplement multipliquem els blocs de quatre símbols (polinomis de grau 3) pel polinomi generador (de grau 4), amb la qual cosa obtenim un bloc de 8 elements (corresponent a un polinomi de grau 7).

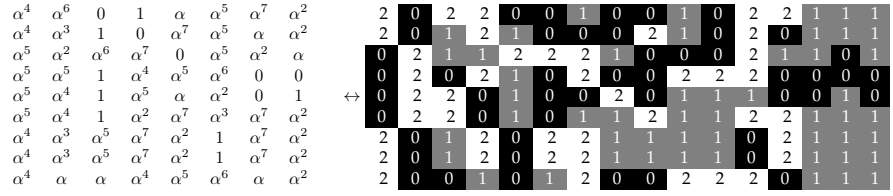
Els polinomis corresponents a la imatge són

$$\begin{array}{cccc} \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\ \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\ \alpha^3 & \alpha^6 & 0 & 0 \\ \alpha^3 & \alpha^7 & \alpha^2 & 1 \\ \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2 \end{array} \leftrightarrow \begin{array}{l} \alpha^2 + \alpha^2 x + \alpha^2 x^2 + \alpha^2 x^3 \\ \alpha^2 + \alpha^6 x + \alpha^7 x^2 + \alpha^2 x^3 \\ \alpha^3 + \alpha^4 x + \alpha^4 x^2 + \alpha x^3 \\ \alpha^3 + \alpha^6 x \\ \alpha^3 + \alpha^7 x + \alpha^2 x^2 + x^3 \\ \alpha^3 + \alpha^7 x + \alpha^2 x^2 + \alpha^2 x^3 \\ \alpha^2 + \alpha^6 x + \alpha^2 x^2 + \alpha^2 x^3 \\ \alpha^2 + \alpha^6 x + \alpha^2 x^2 + \alpha^2 x^3 \\ \alpha^2 + \alpha^3 x + \alpha^7 x^2 + \alpha^2 x^3 \end{array}$$

En multiplicar pel polinomi generador obtenim les paraules codificades.

Per exemple, per codificar la darrera fila $i(x) = \alpha^2 + \alpha^3 x + \alpha^7 x^2 + \alpha^2 x^3$, la multipliquem per $g(x)$ i ens queda $\alpha^4 + \alpha x + \alpha x^2 + \alpha^4 x^3 + \alpha^5 x^4 + \alpha^6 x^5 + \alpha x^6 + \alpha^2 x^7$.

Fem ara el mateix amb totes les files.



Codificació sistemàtica

Si apliquem la codificació sistemàtica, aleshores cada polinomi l'hem de multiplicar per x^{n-k} i restar-li el residu de dividir pel polinomi generador.

Per exemple, per codificar la darrera fila $i(x) = \alpha^2 + \alpha^3 x + \alpha^7 x^2 + \alpha^2 x^3$, la multipliquem per x^{8-4} i ens queda $\alpha^2 x^4 + \alpha^3 x^5 + \alpha^7 x^6 + \alpha^2 x^7$. En dividir aquest darrer polinomi per $g(x)$, ens queda residu $R(x) = \alpha^3 + \alpha^6 x + \alpha^2 x^3$. Aleshores

$$i(x)x^{n-k} - R(x) = \alpha^2 x^7 + \alpha^7 x^6 + \alpha^3 x^5 + \alpha^2 x^4 + \alpha^6 x^3 + \alpha^2 x + \alpha^7 \leftrightarrow (\alpha^7 \alpha^2 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 \alpha^2)$$

que correspon a 2 1 1 1 0 0 2 2 1 1 1 2 2 1 1 1

Fem ara el mateix amb totes les files.

α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2
α^2	α^7	α^4	α^3	α^2	α^6	α^7	α^2
α^3	α	α	α^4	α^3	α^4	α^4	α
1	α^2	α^4	α^3	α^3	α^6	0	0
α^5	α^4	0	α	α^3	α^7	α^2	1
1	α^2	α^5	α^6	α^3	α^7	α^2	α^2
0	α^6	0	0	α^2	α^6	α^2	α^2
0	α^6	0	0	α^2	α^6	α^2	α^2
α^7	α^2	0	α^6	α^2	α^3	α^7	α^2

$\leftrightarrow$

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	2	1	2	0	1	2	1	1	2	2	2	1	1	1
1	2	0	1	0	1	2	0	1	2	2	0	2	0	0	1
1	0	1	1	2	0	1	2	1	2	2	2	0	0	0	0
0	2	2	0	0	0	0	1	1	2	2	1	1	1	1	0
1	0	1	1	0	2	2	2	1	2	2	1	1	1	1	1
0	0	2	2	0	0	0	0	1	1	2	2	1	1	1	1
0	0	2	2	0	0	0	0	1	1	2	2	1	1	1	1
2	1	1	1	0	0	2	2	1	1	1	2	2	1	1	1

Correcció d'errors

Suposem que en la darrera paraula s'han produït errors de manera que es rep

2 1 2 2 0 0 2 2 1 1 1 2 2 1 1 0

corresponent a $\alpha^7 \quad \alpha^6 \quad 0 \quad \alpha^6 \quad \alpha^2 \quad \alpha^3 \quad \alpha^7 \quad 1.$

Observem que s'han produït tres errors de dígit però només dos de símbol.

El polinomi de control és $h(x) = \frac{x^n - 1}{g} = x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2$ i per tant podem prendre com a matriu de control

$$\begin{pmatrix} 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \end{pmatrix}$$

En multiplicar el corresponent vector rebut per la matriu de control, obtenim

$$\begin{pmatrix} 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \end{pmatrix} (\alpha^7 \alpha^6 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 1) = (\alpha^4, \alpha^2, 0, \alpha^7) = \alpha^2 H^2 + \alpha^5 H^8.$$

Per tant, l'error és $e = (0\alpha^2 00000\alpha^5)$. La paraula codi correcta és $(\alpha^7 \alpha^6 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 1) - (0\alpha^2 00000\alpha^5) = (\alpha^7 \alpha^2 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 \alpha^2)$.

Com que el codi és sistemàtic, sabem que la redundància és a l'esquerra i que la part d'informació correspon als símbols $\alpha^2 \alpha^3 \alpha^7 \alpha^2$.

1.7 Codis algebraics (RS i BCH)

Construcció

- Paràmetres
  - p primer, m, $\mathbb{F}_p$, $\mathbb{F}_{p^m}$.

  - n, α arrel n-èsima primitiva de la unitat.
    Si $n = p^m - 1$, aleshores α és un element primitiu de $\mathbb{F}_{p^m}$ i llavors parlem de **codis primitius**.

- Per definir els codis RS i BCH (cíclics per definició), imposem que entre les arrels dels seus polinomis generadors hi hagi

$$\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2}.$$

  Si $b = 1$, aleshores diem que els codis són en **sentit estricte**. En aquest cas, les arrels imposades són $\alpha, \alpha^2, \ldots, \alpha^{d-1}$.

- Les paraules d'un codi RS estaran dins de $(\mathbb{F}_{p^m})^n$ ($n \cdot m$ dígits de $\mathbb{F}_p$).
  Les paraules d'un codi BCH estaran dins de $(\mathbb{F}_p)^n$ (n dígits de $\mathbb{F}_p$).

- Per tant, prenem

$$\begin{aligned} g_{RS}(x) &= (x-\alpha^b)(x-\alpha^{b+1})\cdot\cdots\cdot(x-\alpha^{b+d-2}) \\ g_{BCH}(x) &= \text{mcm}\,(m_{\alpha^b}(x), m_{\alpha^{b+1}}(x), \ldots, m_{\alpha^{b+d-2}}(x)) \end{aligned}$$

Descodificació

Suposem que es rep u.

- Polinomi localitzador d'errors (σn són els errors)

$$\sigma(x) = \prod_{\substack{j \text{ pos. d'error} \\ 0 \leqslant j \leqslant n-1}} (1 - \alpha^j x)$$

$$j \text{ és posició d'error} \iff \sigma(\alpha^{-j}) = 0.$$

- Polinomi avaluador d'errors (ωalor dels errors)

$$e_j = -\frac{\omega(\alpha^{-j})}{\sigma'(\alpha^{-j})}.$$

- Polinomi de síndromes

$$S(x) = u(\alpha) + u(\alpha^2)x + u(\alpha^3)x^2 + \cdots + u(\alpha^{d-1})x^{d-2}$$

- Equació clau

$$\omega(x) = \sigma(x)S(x) \bmod x^{d-1}.$$

- Resolució

  Només esborralls

  (i) Calculem σ a partir de les posicions dels esboralls.
  (ii) Per poder calcular les síndromes, substituïm els esborralls per 0 (podríem substituir per un valor qualsevol).
  (iii) L'equació clau ens dóna la manera directa de calcular ω.

Només errors

$r_{-2} = S(x)$ $r_{-1} = x^{d-1}$ r_i residu de dividir r_{i-2} entre r_{i-1}	$Q_{-2} = 1$ $Q_{-1} = 0$ $Q_i = Q_{i-2} - q_i Q_{i-1}$ q_i quocient de dividir r_{i-2} entre r_{i-1}
Parem en arribar al primer r_i de grau $< \lfloor \frac{d-1}{2} \rfloor$.	
$\omega = r_i$	$\sigma = Q_i$

Errors i esborralls

(i) Considerem $\sigma = \sigma_{esb}\sigma_{err}$
- σ_{esb} localitza els esborralls (conegut),
- σ_{err} localitza els errors (desconegut).

(ii) Definim $T(x) = S(x)\sigma_{esb}(x)$

$r_{-2} = T(x)$ $r_{-1} = x^{d-1}$ r_i residu de dividir r_{i-2} entre r_{i-1}	$Q_{-2} = 1$ $Q_{-1} = 0$ $Q_i = Q_{i-2} - q_i Q_{i-1}$ q_i quocient de dividir r_{i-2} entre r_{i-1}
Parem en arribar a l'últim Q_i de grau $\leqslant \lfloor \frac{d-\#\text{esborralls}-1}{2} \rfloor$.	
$\omega = r_i$	$\sigma_{err} = Q_i$ $\sigma = \sigma_{err}\sigma_{esb}$

Exemple

(i) Comproveu que $x^2 + 2x + 2$ és un polinomi irreductible i primitiu de $\mathbb{Z}_3[x]$.

(ii) Construïu el codi BCH ternari primitiu en sentit estricte de longitud 8 i distància mínima prevista 5, tot donant-ne el polinomi generador.

(iii) Corregiu els esborralls corresponents al primer bloc de la seqüència rebuda

$$0\,0\,1\,?\,?\,?\,?\,2\,0\,0\,1\,?\,?\,\ldots$$

(iv) Localitzeu i corregiu els errors de la primera paraula de la seqüència

$$1\,0\,1\,1\,2\,0\,0\,0\,0\,1\,2\,\ldots$$

(v) Corregiu la primera paraula de la següent seqüència, on s'han produït esborralls i errors

$$2\,2\,?\,?\,0\,1\,0\,0\,?\,?\,\ldots$$

(i)

α	$0\,1$
α^2	$1\,1$
α^3	$1\,2$
α^4	$2\,0$
α^5	$0\,2$
α^6	$2\,2$
α^7	$2\,1$
α^8	$1\,0$

(ii)

$$\begin{aligned} m_\alpha(x) &= (x-\alpha)(x-\alpha^3) = x^2 - x - 1 \\ m_{\alpha^2}(x) &= (x-\alpha^2)(x-\alpha^6) = x^2 + 1 \\ m_{\alpha^3}(x) &= m_\alpha^3(x) \\ m_{\alpha^4}(x) &= (x-\alpha^4) = x + 1 \end{aligned}$$

$g_{BCH} = m_\alpha m_{\alpha^2} m_{\alpha^4} = (x^2 - x - 1)(x^3 + x^2 + x + 1) = x^5 + 2x^3 + 2x^2 + x + 2$

(iii) $u = (0\,0\,1\,?\,?\,?\,?\,2)$

$$\begin{aligned}
u(x) &= x^2 + 2x^7 \\
\sigma &= (1-\alpha^3 x)(1-\alpha^4 x)(1-\alpha^5 x)(1-\alpha^6 x) \\
&= (1+\alpha x+\alpha^7 x^2)(1+\alpha^3 x+\alpha^3 x^2) = 1+x+\alpha^4 x^2+\alpha x^3+\alpha^2 x^4 \\
\sigma' &= 1+x+\alpha^2 x^3 \\
u(\alpha) &= \alpha^4 \\
u(\alpha^2) &= \alpha^4+\alpha^2 = \alpha \\
u(\alpha^3) &= \alpha^6+\alpha = \alpha^4 \\
u(\alpha^4) &= 1+1 = \alpha^4
\end{aligned}$$

$$\begin{aligned}
S &= u(\alpha)+u(\alpha^2)x+u(\alpha^3)x^2+u(\alpha^4)x^3 \\
&= \alpha^4+\alpha x+\alpha^4 x^2+\alpha^4 x^3
\end{aligned}$$

$$\omega = S\sigma \bmod x^4 = \alpha^2 x^3+\alpha x^2+\alpha^7 x+\alpha^4$$

$$\begin{aligned}
e_3 &= -\frac{\omega(\alpha^{-3})}{\sigma'(\alpha^{-3})} = 1 \\
e_4 &= -\frac{\omega(\alpha^{-4})}{\sigma'(\alpha^{-4})} = 2 \\
e_5 &= -\frac{\omega(\alpha^{-5})}{\sigma'(\alpha^{-5})} = 2 \\
e_6 &= -\frac{\omega(\alpha^{-6})}{\sigma'(\alpha^{-6})} = 0
\end{aligned}$$

$$c = u - e = (0,0,1,0,0,0,0,2) - (0,0,0,1,2,2,0,0) = (0,0,1,2,1,1,0,2).$$

(iv) $u = (1\,0\,1\,1\,2\,0\,0\,0)$

$$u(x) = 1+x^2+x^3+2x^4$$

$$\begin{aligned}
u(\alpha) &= 1+\alpha^2+\alpha^3+2\alpha^4 = 1 \\
u(\alpha^2) &= 1+\alpha^4+\alpha^6+2 = \alpha^3 \\
u(\alpha^3) &= 1+\alpha^6+\alpha+1 = 1 \\
u(\alpha^4) &= 1+1+\alpha^4+\alpha^4 = 0
\end{aligned}$$

$$\begin{aligned}
S &= u(\alpha)+u(\alpha^2)x+u(\alpha^3)x^2+u(\alpha^4)x^3 \\
&= x^2+\alpha^3 x+1
\end{aligned}$$

Divisions successives:

$r_{-2} = S$		$Q_{-2} = 1$
$r_{-1} = x^4$		$Q_{-1} = 0$
$r_0 = S$	$q_0 = 0$	$Q_0 = 1$
$r_1 = \alpha^4 x + \alpha^7$	$q_1 = x^2 + \alpha^7 x + \alpha^3$	$Q_1 = \alpha^4 x^2 + \alpha^3 x + \alpha^7$
r_1 té grau $< 2 = \lfloor \frac{d-1}{2} \rfloor$		

Parem a $i = 1$.

$$\begin{aligned} \omega &= r_i = \alpha^4 x + \alpha^7 \\ \sigma &= Q_i = \alpha^4 x^2 + \alpha^3 x + \alpha^7 \\ \sigma' &= x + \alpha^3 \end{aligned}$$

Busquem les arrels de σ:

$$\begin{aligned} \sigma(\alpha^{-0}) &= \sigma(\alpha^0) = \alpha^4 + \alpha^3 + \alpha^7 = \alpha^4 \\ \sigma(\alpha^{-1}) &= \sigma(\alpha^7) = \alpha^2 + \alpha^2 + \alpha^7 = 1 \\ \sigma(\alpha^{-2}) &= \sigma(\alpha^6) = 1 + \alpha + \alpha^7 = \alpha^5 \\ \sigma(\alpha^{-3}) &= \sigma(\alpha^5) = \alpha^6 + 1 + \alpha^7 = \alpha^4 \\ \sigma(\alpha^{-4}) &= \sigma(\alpha^4) = \alpha^4 + \alpha^7 + \alpha^7 = \alpha^5 \\ \sigma(\alpha^{-5}) &= \sigma(\alpha^3) = \alpha^2 + \alpha^6 + \alpha^7 = \alpha^7 \\ \sigma(\alpha^{-6}) &= \sigma(\alpha^2) = 1 + \alpha^5 + \alpha^7 = 0 \\ \sigma(\alpha^{-7}) &= \sigma(\alpha) = \alpha^6 + \alpha^4 + \alpha^7 = 0 \end{aligned}$$

Són exactament α^{-6} i α^{-7}.

$$\begin{aligned} e_6 &= -\frac{\omega(\alpha^{-6})}{\sigma'(\alpha^{-6})} = 1 \\ e_7 &= -\frac{\omega(\alpha^{-7})}{\sigma'(\alpha^{-7})} = 1 \end{aligned}$$

$c = u - e = (1,0,1,1,2,0,0,0) - (0,0,0,0,0,0,1,1) = (1,0,1,1,2,0,2,2)$.

(v) $u = (2\,2\,?\,?\,0\,1\,0\,0)$

$$\begin{aligned} u(x) &= 2 + 2x + x^5 \\ \sigma_{esb} &= (1 - \alpha^2 x)(1 - \alpha^3 x) = 1 + x + \alpha^5 x^2 \end{aligned}$$

$$\begin{aligned} u(\alpha) &= \alpha^4 + \alpha^5 + \alpha^5 = \alpha^7 \\ u(\alpha^2) &= \alpha^4 + \alpha^6 + \alpha^2 = \alpha^4 \\ u(\alpha^3) &= \alpha^4 + \alpha^7 + \alpha^7 = \alpha^5 \\ u(\alpha^4) &= \alpha^4 + 1 + \alpha^4 = \alpha^4 \end{aligned}$$

$$\begin{aligned} S &= u(\alpha) + u(\alpha^2)x + u(\alpha^3)x^2 + u(\alpha^4)x^3 \\ &= \alpha^4 x^3 + \alpha^5 x^2 + \alpha^4 x + \alpha^7 \end{aligned}$$

$$T = S\sigma_{esb} = \alpha x^5 + \alpha x^4 + \alpha^4 x^3 + \alpha^3 x^2 + \alpha^2 x + \alpha^7$$

Divisions successives:

$r_{-2} = T$		$Q_{-2} = 1$
$r_{-1} = x^4$		$Q_{-1} = 0$
$r_0 = \alpha^4 x^3 + \alpha^3 x^2 + \alpha^2 x + \alpha^7$	$q_0 = \alpha x + \alpha^5$	$Q_0 = 1$
$r_1 = \alpha^4 x + \alpha^2$	$q_1 = \alpha^4 x + \alpha^7$	$Q_1 = x + \alpha^3$
$r_2 = 1$	$q_2 = x^2 + \alpha^5 x + 1$	$Q_2 = Q_0 - q_2 Q_1$ tindrà grau $3 > \lfloor \frac{d-1}{2} \rfloor$

Parem a $i = 1$.

$$\begin{aligned} \omega &= r_i = \alpha^4 x + \alpha^2 \\ \sigma_{err} &= Q_i = x + \alpha^3 \end{aligned}$$

σ_{err} té com a arrel α^{-1}.

$$\begin{aligned} \sigma &= \sigma_{err}\sigma_{esb} = \alpha^5 x^3 + \alpha^4 x^2 + \alpha^6 x + \alpha^3 \\ \sigma' &= x + \alpha^6 \end{aligned}$$

$$\begin{aligned} e_1 &= -\frac{\omega(\alpha^{-1})}{\sigma'(\alpha^{-1})} = 1 \\ e_2 &= -\frac{\omega(\alpha^{-2})}{\sigma'(\alpha^{-2})} = 1 \\ e_3 &= -\frac{\omega(\alpha^{-3})}{\sigma'(\alpha^{-3})} = 1 \end{aligned}$$

$c = u - e = (2, 2, 0, 0, 0, 1, 0, 0) - (0, 1, 1, 1, 0, 0, 0, 0) = (2, 1, 2, 2, 0, 1, 0, 0).$

Capítol 2
Problemes d'aritmètica entera i polinomial

J. M. Basart, J. Rifà Coma, M. Villanueva[1]

2.1 Demostreu que no existeixen enters a i b tals que el seu màxim comú divisor és 7 i $a + b = 100$. D'altra banda, existeixen infinites parelles a, b tals que el seu màxim comú divisor és 5 i $a + b = 100$.

2.2 * Calculeu el màxim comú divisor de 365 i 70 i expresseu-lo com a combinació lineal de 365 i 70.

Resposta:

Construïm la taula de l'algoritme d'Euclides:

1	0	1	-4	5	
0	1	-5	21	-26	
		5	4	1	2
365	70	15	10	5	0

Deduïm que $mcd(365, 70) = 5$ i que $5 \cdot 365 + (-26) \cdot 70 = 5$.

2.3 Per a cadascun dels següents parells de nombres enters, calculeu el seu màxim comú divisor i escriviu-lo com a combinació lineal entera dels nombres donats:

(a) 26, 19

Sol.: $\mathbf{1 = 19 \cdot 11 - 8 \cdot 26}$

(b) 187, 34

Sol.: $\mathbf{17 = -5 \cdot 34 + 187 \cdot 1}$

(c) 841, 160

Sol.: $\mathbf{1 = 160 \cdot 205 - 841 \cdot 39}$

[1] Aquest capítol, a excepció dels problemes indicats amb *, ha estat extret íntegrament del llibre:

Josep M. Basart, Josep Rifà, Mercè Villanueva: *Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica*. Col·lecció Materials n. 36. Universitat Autònoma de Barcelona, 1999.

amb el consentiment dels seus autors. En el mencionat llibre conformen l'apartat d'exercicis dels capítols 5 i 6. Agraïm la col·laboració dels autors en el present projecte.

2.4 A l'anell dels enters demostreu

(a) Si $p^\alpha \mid a$ i $p^\beta \mid b$, llavors $p^{\alpha+\beta} \mid ab$

(b) Si $p^\alpha \mid a$; $p^\beta \mid b$ i $\alpha < \beta$, llavors $p^\alpha \mid a \pm b$

(c) Si $m|a$ i $n|a$, i m i n són primers entre ells, llavors $mn|a$

2.5 Demostreu que tot enter $n > 1$ no primer té un divisor positiu diferent d'1 i més petit o igual que $\sqrt{n}$. Aplicant aquest criteri descomponeu en producte de primers $3337, 3007$ i 7077.

Sol.: $3337 = 47 \cdot 71$, $3007 = 31 \cdot 97$ i 7077 és primer

2.6 Demostreu que, si x i y són dos elements senars de $\mathbb{Z}$, llavors $x^2 + y^2$ no és quadrat de cap enter.

2.7 Resoleu, si tenen solució, les equacions diofàntiques següents:

(a) $5x + 3y = 2$

Sol.: $\mathbf{x = -2 + 3\lambda}$, $\mathbf{y = 4 - 5\lambda}$, on $\lambda \in \mathbb{Z}$

(b) $97x + 23y = 10$

(c) $2x + 6y = 1$

Sol.: No té solució

(d) $2x + 3y = 1$

Sol.: $\mathbf{x = -1 + 3\lambda}$, $\mathbf{y = 1 - 2\lambda}$, on $\lambda \in \mathbb{Z}$

(e) $6x + 21y = 15$

Sol.: $\mathbf{x = -15 + 7\lambda}$, $\mathbf{y = 5 - 2\lambda}$, on $\lambda \in \mathbb{Z}$

(f) $11x - 12y = 3$

Sol.: $\mathbf{x = -3 - 12\lambda}$, $\mathbf{y = -3 - 11\lambda}$, on $\lambda \in \mathbb{Z}$

2.8 Si de la data de naixement d'una persona us donen el valor de la suma del dia del mes multiplicat per 12 més el nombre del mes multiplicat per 31, com podeu determinar quina fou la data? Quina és la data si la suma és 103?

Sol.: 6 de gener

2.9 Demostreu que, si $a \equiv b (mod\ m)$, llavors $mcd(a, m) = mcd(b, m)$.

2.10 Demostreu que, si $a \equiv b\ (mod\ m)$; $a \equiv b\ (mod\ n)$ i $mcd(m, n) = 1$, llavors $a \equiv b\ (mod\ m \cdot n)$.

2.11 Demostreu els criteris de divisibilitat per 3, per 4, per 5, per 9, per 11 i per 13.

2.12 Demostreu que $mcd(a, b) = mcd(a - b, b)$ per tota parella d'enters a i b.

2.13 Calculeu $mcd(28n + 5, 35n + 2)$ per a tot $n \geqslant 1$.

Sol.:

$$\mathbf{mcd(28n + 5, 35n + 2)} = \begin{cases} 17 & \mathbf{si\ n \equiv 15\ (mod\ 17)} \\ 1 & \mathbf{si\ n \not\equiv 15\ (mod\ 17)} \end{cases}$$

2.14 Demostreu que per a tot $n \geqslant 1$ es compleix

(a) $6 \mid n(n + 1)(n + 2)$

(b) $30 \mid n^5 - n$

(c) $13 \mid 4^{2n+1} + 3^{n+2}$

2.15 * Quantes solucions tenen aquestes equacions amb congruències? Doneu-ne les solucions.

(a) $26x \equiv 3 \; mod \; 13$

(b) $13x \equiv 3 \; mod \; 26$

(c) $26x \equiv 0 \; mod \; 13$

(d) $9x \equiv -3 \; mod \; 15$

(e) $5x \equiv 4 \; mod \; 7$

(f) $5x \equiv 7 \; mod \; 7$

Sol.: (a) 0 solucions, (b) 0 solucions, (c) 13 solucions, que són $x \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \; mod \; 13$**, (d) 3 solucions, que són** $x \equiv 3, 8, 13 \; mod \; 15$**, (e) 1 solució, que és** $x \equiv 5 \; mod \; 7$**, (f) 1 solució, que és** $x \equiv 0 \; mod \; 7$**.**

2.16 Resoleu les següents congruències:

(a) $4x \equiv 3 \, (mod \; 7)$

(b) $3x \equiv 2 \, (mod \; 4)$

(c) $2x - 1 \equiv 0 \, (mod \; 15)$

(d) $20x \equiv 60 \, (mod \; 80)$

(e) $158x \equiv -22 \, (mod \; 194)$

(f) $x^2 \equiv 1 \, (mod \; 12)$

Sol.: (a) $\mathbf{x \equiv 6 \; (mod \; 7)}$**, (b)** $\mathbf{x \equiv 2 \; (mod \; 4)}$**, (c)** $\mathbf{x \equiv 8 \; (mod \; 15)}$**, (d)** $\mathbf{x \equiv 3 \; (mod \; 4)}$**, o bé,** $\mathbf{x \equiv 3, 7, 11, \ldots, 79 \; (mod \; 80)}$ **(e)** $\mathbf{x \equiv 6 \; (mod \; 97)}$**, o bé,** $\mathbf{x \equiv 6 \text{ i } 103 \; (mod \; 194)}$ **(f)** $\mathbf{x \equiv 1, 5, 7 \text{ i } 11 \; (mod \; 12)}$

2.17 Descriviu les solucions de

(a) $27x \equiv 25 \; (mod \; 256)$

Sol.: $\mathbf{x \equiv 219 \; (mod \; 256)}$

(b) $103x \equiv 612 \; (mod \; 676)$

Sol.: $\mathbf{x \equiv 636 \; (mod \; 676)}$

2.18 Descriviu les solucions de

(a) $x^2 + 5x - 2 \equiv 0 \; (mod \; 11)$

Sol.: $\mathbf{x \equiv 3 \; (mod \; 11)}$

(b) $x^2 + 2x + 6 \equiv 0 \; (mod \; 7)$

Sol.: $\mathbf{x \equiv 2 \text{ i } 3 \; (mod \; 7)}$

2.19 Trobeu les solucions enteres comunes de

$$\begin{aligned} x &\equiv 2 \quad (mod \; 5) \\ x &\equiv 1 \quad (mod \; 3) \end{aligned}$$

Sol.: $\mathbf{x \equiv 7 \; (mod \; 15)}$

2.20 Apliqueu el teorema xinès dels residus pel cas de més de dues equacions i feu-lo servir per trobar la solució de

$$\begin{aligned} x &\equiv 2 \quad (mod \; 5) \\ x &\equiv 1 \quad (mod \; 3) \\ x &\equiv 2 \quad (mod \; 7) \end{aligned}$$

Sol.: $\mathbf{x \equiv 37 \; (mod \; 105)}$

2.21 Resoleu els sistemes de congruències següents:

$$\left.\begin{array}{l} 2x \equiv 3\,(mod\ 5) \\ 3x \equiv 2\,(mod\ 4) \end{array}\right\} \qquad \left.\begin{array}{l} x \equiv 7\,(mod\ 12) \\ x \equiv 5\,(mod\ 18) \end{array}\right\}$$

Sol.: el primer $\mathbf{x \equiv 14\ (mod\ 20)}$ i el segon no té solució

2.22 Resoleu els sistemes de congruències següents:

$$\left.\begin{array}{l} 2x \equiv 3\,(mod\ 5) \\ 3x \equiv 6\,(mod\ 7) \\ -7x \equiv 1\,(mod\ 13) \end{array}\right\} \qquad \left.\begin{array}{l} x \equiv 2\,(mod\ 3) \\ 9x \equiv -3\,(mod\ 15) \\ 5x \equiv 6\,(mod\ 7) \end{array}\right\}$$

Sol.: el primer $\mathbf{x \equiv 219\ (mod\ 455)}$ i el segon $\mathbf{x \equiv 53\ (mod\ 105)}$

2.23 (*Un problema xinès*) Tres pagesos xinesos cultiven arròs col·lectivament i, quan arriba l'època de la collita, ho fan tot junts. Després divideixen la collita en tres parts iguals i cadascun, amb la seva part, es dirigeix a un mercat diferent a vendre'l. A cada mercat hi ha unitats de mesura diferents; així, en el primer mercat la unitat de mesura és de 870 grams; en el segon, de 1.700 grams i, en el tercer, de 1.430 grams. Els tres pagesos venen totes les mesures possibles d'arròs, però retornen a la col·lectivitat amb 180 grams, 580 grams i 400 grams respectivament.

Quina quantitat d'arròs havien collit entre tots tres aquest any?

Sol.: $\mathbf{3.158.640gr.(mod\ 63.449.100)}$

2.24 (Brahmagupta, 700 a. de c.) Quan els ous d'un cistell es compten de dos en dos, tres en tres, quatre en quatre, cinc en cinc i sis en sis en sobren, respectivament, 1, 2, 3, 4 i 5. Si es fa de set en set, no en sobra cap.

Quants ous hi ha al cistell?

$\mathbf{x \equiv 119\ (mod\ 420)}$

2.25 Determineu tots els nombres enters acabats en 4 tals que el seu doble sigui múltiple de 3 i el seu triple múltiple de 7.

$\mathbf{84\ (mod\ 210)}$

2.26 Calculeu l'invers de 15 a $\mathbb{Z}_{23}$ i el de 156 a $\mathbb{Z}_{2671}$.

Sol.: 20 i 702

2.27 Trobeu els elements invertibles (donant el seu invers) i els divisors de zero a $\mathbb{Z}_{12}$.

Sol.: Invertibles: $\mathbf{1^{-1} = 1}$, $\mathbf{5^{-1} = 5}$, $\mathbf{7^{-1} = 7}$ i $\mathbf{11^{-1} = 11}$. Divisors de zero: 2,3,4,6,8,9 i 10

2.28 Sigui l'anell $\mathbb{Z}_{18}$

(a) És un cos?

(b) Quants elements invertibles té i quins són?

(c) Quants divisors de zero té?

(d) Busqueu un element primitiu.

(e) Quants elements primitius té?

Sol.: (a) No és un cos, (b) 6 invertibles, que són 1, 5, 7, 11, 13 i 17, (c) 11, (d) per exemple, el 5, (e) 2

2.29 * Sigui l'anell $\mathbb{Z}_{27}$.

(a) És un cos?

(b) Quants elements invertibles té i quins són?

(c) Quants divisors de zero té?

(d) Busqueu un element primitiu.

(e) Busqueu un element diferent de $0, 1$ que no sigui primitiu. Quin ordre té?

Sol.: (a) No és un cos, (b) $\phi(27) = 3^3 - 3^2 = 18$ **invertibles, que són** $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$ **(c) 8, (d) per exemple, el 2, (e) 4, que té ordre 9.**

2.30 Determineu en $M_2(\mathbb{Z}_7)$, l'anell de les matrius d'ordre 2 amb valors en $\mathbb{Z}_7$, la inversa de la matriu

$$\begin{pmatrix} 3 & 5 \\ 1 & 0 \end{pmatrix}$$

Sol.: $\begin{pmatrix} 0 & 1 \\ 3 & 5 \end{pmatrix}$

2.31 Resoleu l'equació 3x=-6 a $\mathbb{Z}_{15}$.

Sol.: $\mathbf{x = 3, 8 \text{ i } 13}$

2.32 (a) Resoleu l'equació $3x + 4 = 0$ en el cos $\mathbb{Z}_5$.

Sol.: $\mathbf{x = 2}$

(b) Digueu quant ha de valdre a per tal que l'equació $ax + 4 = 0$ es pugui resoldre a $\mathbb{Z}_6$. Resoleu l'equació per a cada valor possible de a.

Sol.: L'equació té solució per $\mathbf{a = 1, 2, 4}$ **i 5. Per** $\mathbf{a = 1, x = 2}$**; per** $\mathbf{a = 2, x = 1}$ **i 4; per** $\mathbf{a = 4, x = 2}$ **i 5; per** $\mathbf{a = 5, x = 4}$**.**

2.33 Resoleu, en el cos $\mathbb{Z}_5$, el sistema següent:

$$\begin{aligned} 3x + 2y &= 1 \\ x + y &= 4 \end{aligned}$$

Sol.: $\mathbf{x = 3}$ **i** $\mathbf{y = 1}$

2.34 Determineu el valor del paràmetre a de manera que el sistema següent tingui solució a $\mathbb{Z}_5$:

$$\begin{aligned} 3x + 2y &= 1 \\ ax + y &= 4 \end{aligned}$$

Sol.: $\mathbf{a = 0, 1, 2 \text{ o } 3}$

2.35 Determineu el valor del paràmetre a de manera que el sistema següent tingui solució a $\mathbb{Z}_{10}$:

$$\begin{aligned} 2x + 7y &= 6 \\ ax + 4y &= 9 \end{aligned}$$

Sol.: $\mathbf{a = 1, 3, 5 \text{ o } 7}$

2.36 Resoleu el següent sistema d'equacions a $\mathbb{Z}_7$:

$$\left\{\begin{array}{rcl} x+y-9z & = & 1 \\ 2x+3y-z & = & 8 \\ 7x-4y+25z & = & 0 \end{array}\right.$$

Sol.: x = 6, y = 5 i z = 5

2.37 Trobeu les solucions del sistema de congruències següent:

$$\left.\begin{array}{l} 7x+5y \equiv 2 \\ 5x+2y \equiv 0 \end{array}\right\} (mod\ 8)$$

(Penseu que teniu un sistema d'equacions a $\mathbb{Z}_8$).

Sol.: x = 4 i y = 6

2.38 Si p és primer i $\alpha^2 = \alpha \in \mathbb{Z}_p$, llavors $\alpha = 0$, o bé $\alpha = 1$.

Trobeu tots els α, tals que $\alpha^2 = \alpha \in \mathbb{Z}_{34}$.

Sol.: $\alpha = \mathbf{0, 1, 17}$ **i** 18

2.39 Calculeu $\phi(256)$, $\phi(3000)$, $\phi(97)$.

Sol.: 128, 800, 96

2.40 Si $n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}$, on p_i són primers diferents, doneu una fórmula per calcular $\phi(n)$.

Sol.: $\prod_{\mathbf{i=1}}^{\mathbf{r}} \mathbf{p_i^{n_i-1}(p_i-1)}$

2.41 Sigui $n = p \cdot q$ on p i q són primers. Demostreu que el coneixement de $\phi(n)$ és equivalent al coneixement de p i q.

2.42 Busqueu un element β de $\mathbb{Z}_{23}$ tal que tot altre element diferent de zero de $\mathbb{Z}_{23}$ es pot escriure com a potència de β.

Sol.: Per exemple, 7

2.43 Demostreu que, si p és primer, llavors $mcd(p, (p-1)!) = 1$. Demostreu que, si n no és primer i $n > 4$, llavors $(n-1)! \equiv 0(mod\ n)$.

2.44 Demostreu que, si 7 no divideix n, llavors 7 divideix $n^{12} - 1$.

2.45 Demostreu que $n^{13} - n$ és divisible per 2, 3, 5, 7 i 13, per tot $n \in \mathbb{Z}$.

2.46 Demostreu que $\dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7n}{15}$ sempre és un nombre enter, per tot $n \in \mathbb{Z}$.

2.47 Utilitzeu l'algorisme de multiplicar i elevar per contestar:

(a) Quines són les dues últimes xifres de 1993^{1992}?

Sol.: 01

(b) Quin és l'últim dígit de 7^{126}?

Sol.: 9

2.48 Trobeu el menor representant positiu de $2^{1000000}$ mod 77.

Sol.: 23

2.49 Calculeu la resta de dividir:

(a) 7457^{2748} entre 5

Sol.: 1

(b) $3752^{9784} + 274^{2780} - 4 \cdot 3^{158}$ entre 11

Sol.: 4

2.50 Calculeu 6^{41} a $\mathbb{Z}_{100}$.

Sol.: 56

2.51 Considerem el criptosistema RSA del qual coneixem el fitxer públic de claus:

(n_A, e_A)	$(133, 5)$
(n_B, e_B)	$(253, 7)$
$\cdots$	$\cdots$

Reproduïu el procés de xifrar-desxifrar el missatge 25, enviat d'A a B.

Sol.: Missatge xifrat, 174

2.52 Trobeu el quocient i el residu de la divisió de $f(x)$ per $g(x)$, on $f(x), g(x) \in \mathbb{Q}[x]$; $f(x) = x^5 - x^3 + x^2 + 7$ i $g(x) = x^3 + 3x^2 + x + 5$.

Sol.: $\mathbf{q(x) = x^2 - 3x + 7}$, $\mathbf{r(x) = -22x^2 + 8x - 28}$

2.53 Calculeu l'mcd i escriviu-lo com a combinació lineal amb coeficients polinomials dels polinomis inicials de $\mathbb{R}[x]$:

(a) $x^4 + x^2 + 1$ i $x^2 + 1$

Sol.: $\mathbf{1 = (x^4 + x^2 + 1) - x^2(x^2 + 1)}$

(b) $x^4 - 4x^3 + 6x^2 - 4x + 1$ i $x^3 - x^2 + x - 1$

Sol.: $\mathbf{x - 1 = \frac{1}{4}(x^2 - 4x + 5)(x^3 - x^2 + x - 1) - \frac{1}{4}(x - 1)(x^4 - 4x^3 + 6x^2 - 4x + 1)}$

(c) $x^3 + 1$ i $x^4 - 2x^3 + 2x^2 - 2x + 1$

Sol.: $\mathbf{1 = \frac{1}{8}(3x^2 + 5x + 3)(x^4 - 2x^3 + 2x^2 - 2x + 1) - \frac{1}{8}(3x^3 - x^2 - x - 5)(x^3 + 1)}$

(d) $3x^4 - 4x^3 + 1$ i $x^3 - 3x + 2$

Sol.: $\mathbf{x^2 - 2x + 1 = \frac{1}{9}(3x^4 - 4x^3 + 1) - \frac{1}{9}(3x - 4)(x^3 - 3x + 2)}$

2.54 Calculeu l'mcd i escriviu-lo com a combinació lineal polinomial dels polinomis inicials:

(a) $x^5 + x^2 + x + 1$ i $x^3 + 1$, a $\mathbb{Z}_2[x]$

Sol.: $\mathbf{x + 1 = (x^5 + x^2 + x + 1) + x^2(x^3 + 1)}$

(b) $x^5 + x^2 + x + 1$ i $x^2 + 1$, a $\mathbb{Z}_5[x]$

Sol.: $\mathbf{1 = (x^2 + 1)(3x^4 - 3x^2 + 3x + 1) + (-3x)(x^5 + x^2 + x + 1)}$

(c) $x^2 + 1$ i $x^3 - x^2 + 2x + 2$, a $\mathbb{Z}_5[x]$

Sol.: $\mathbf{x + 3 = (x^3 - x^2 + 2x + 2) - (x - 1)(x^2 + 1)}$

(d) $x^2 - x + 4$ i $x^3 + 2x^2 + 3x + 2$, a $\mathbb{Z}_3[x]$

Sol.: $\mathbf{x + 1 = x(x^2 - x + 4) - (x^3 + 2x^2 + 3x + 2)}$

(e) x^2+1 i x^5+1, a $\mathbb{Z}_2[x]$

Sol.: $\mathbf{x+1=(x^5+1)+(x^3+x)(x^2+1)}$

2.55 És $x-3$ un divisor de x^4+x^3+x+4 a $\mathbb{Z}_2[x]$?, a $\mathbb{Z}_3[x]$?, a $\mathbb{Z}_5[x]$?, a $\mathbb{Z}_7[x]$?

Sol.: no, no, sí, no

2.56 Calculeu els polinomis irreductibles de grau $\leqslant 3$ a $\mathbb{Z}_2[x]$ i tots els irreductibles de grau $\leqslant 2$ a $\mathbb{Z}_3[x]$.

Sol.: A $\mathbf{\mathbb{Z}_2[x]}$, $\mathbf{x}$, $\mathbf{x+1}$, $\mathbf{x^2+x+1}$, $\mathbf{x^3+x+1}$, $\mathbf{x^3+x^2+1}$. **A** $\mathbf{\mathbb{Z}_3[x]}$ **(llevat de multiplicar per constants)** $\mathbf{x}$, $\mathbf{x+1}$, $\mathbf{x+2}$, $\mathbf{x^2+1}$, $\mathbf{x^2+x+2}$, $\mathbf{x^2+2x+2}$

2.57 Sigui K un cos. Si $f,g,h\in K[x]$ i $mcd(f,g)=1$, llavors $mcd(fh,g)=mcd(h,g)$.

2.58 Factoritzeu completament a $\mathbb{Z}_3[x]$, a $\mathbb{Z}_5[x]$ i a $\mathbb{Z}_7[x]$ els polinomis x^4+1, x^4-1, x^4+4 i x^3-2.

Sol.: A $\mathbf{\mathbb{Z}_3[x]}$, $\mathbf{x^4+1=x^4+4=(x^2+2x+2)(x^2+x+2)}$, $\mathbf{x^4-1=(x-1)(x-2)(x^2+1)}$ **i** $\mathbf{x^3-2=(x+1)^3}$.

A $\mathbf{\mathbb{Z}_5[x]}$, $\mathbf{x^4+1=(x^2+2)(x^2+3)}$, $\mathbf{x^4-1=x^4+4=(x-1)(x-2)(x-3)(x-4)}$ **i** $\mathbf{x^3-2=(x-3)(x^2+3x+4)}$.

A $\mathbf{\mathbb{Z}_7[x]}$, $\mathbf{x^4+1=(x^2+3x+1)(x^2+4x+1)}$, $\mathbf{x^4-1=(x-1)(x-6)(x^2+1)}$ $\mathbf{x^4+4=(x^2+2x+2)(x^2+5x+2)}$ **i** $\mathbf{x^3-2}$ **és irreductible**

2.59 Per quins primers p, si n'hi ha algun, els dos polinomis x^6+2x^2+x i x^9+8x^3+x coincideixen com a funcions sobre $\mathbb{Z}_p$?

Sol.: $\mathbf{p=2}$ **i** $\mathbf{3}$

2.60 Descomponeu $x^5-x\in\mathbb{Z}_5[x]$ en producte de factors irreductibles.

Sol.: $\mathbf{x^5-x=x(x-1)(x-2)(x-3)(x-4)}$

2.61 Trobeu tots els polinomis irreductibles a $\mathbb{Z}_2[x]$ de grau 4.

Sol.: $\mathbf{x^4+x+1}$, $\mathbf{x^4+x^3+1}$ **i** $\mathbf{x^4+x^3+x^2+x+1}$

2.62 Descomponeu en factors irreductibles els següents polinomis de $\mathbb{Z}_2[x]$:

(a) $x^6+x^4+x^3+x^2+1$

Sol.: $\mathbf{x^6+x^4+x^3+x^2+1=(x^2+x+1)(x^4+x^3+x^2+x+1)}$

(b) $x^8+x^7+x^6+x^4+1$

Sol.: $\mathbf{x^8+x^7+x^6+x^4+1=(x^4+x^3+x^2+x+1)(x^4+x+1)}$

(c) $x^{16}-x$

Sol.: $\mathbf{x^{16}-x=x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)}$

(d) $x^7+x^6+x^4+1$

(e) $x^{10}+x^9+x^7+x^3+x^2+1$

Sol.: $\mathbf{x^{10}+x^9+x^7+x^3+x^2+1=(x+1)(x^3+x^2+1)(x^3+x+1)}$

(f) $x^{10}+x^7+x^4+x^3+x^2+x+1$

2.63 Factoritzeu:

(a) x^3+2x^2+5x+1 a $\mathbb{Z}_7[x]$

Sol.: és irreductible

(b) $x^3 + x^2 - 3x - 1$ a $\mathbb{Z}_5[x]$

Sol.: $\mathbf{x^3 + x^2 - 3x - 1 = (x + 3)(x^2 + 3x + 3)}$

2.64 Per a cada primer p, trobeu un polinomi no constant amb coeficients a $\mathbb{Z}_p$ que tingui derivada nul·la.

Sol.: $\mathbf{f(x) = x^p}$

2.65 Proveu el **Teorema de Wilson** (si p és un primer senar, llavors $(p-1)! \equiv -1(mod\ p)$) del següent mode:

(a) Proveu que a $\mathbb{Z}_p[x]$ el polinomi $f(x) = x^{p-1} - 1$ factoritza com $f(x) = (x-1)(x-2)\cdots(x-(p-1))$ (useu el teorema de Fermat i el teorema de l'arrel a $\mathbb{Z}_p[x]$.)

(b) Avalueu $f(0)$.

2.66 Demostreu que, si $p \equiv 1(mod\ 4)$, llavors $(\frac{p-1}{2})!^2 \equiv -1(mod\ p)$.

2.67 Demostreu que $x^5 + x^2 + 1$ és irreductible a $\mathbb{Z}_2[x]$.

2.68 Digueu si els polinomis x^5 i x^2-1 tenen invers a $\mathbb{Z}_3[x]/(x^2+2x+1)$ i calculeu-lo en cas afirmatiu.

Sol.: Invers de $\mathbf{[x^5]}$ **és** $\mathbf{[x]}$ **i** $\mathbf{[x^2 - 1]}$ **no té invers**

2.69 Trobeu els divisors de zero de $\mathbb{Z}_5[x]/(x^3 + 2x^2 + x + 2)$.

Sol.: $\mathbf{[(x + 3)(ax + b)]}$ **i** $\mathbf{[(x + 2)(ax + b)]}$, $\mathbf{\forall a, b \in \mathbb{Z}_5}$

2.70 Resoleu, si és possible:

(a) $(x^3 + x + 1)f(x) \equiv 1\ (mod\ x^4 + x + 1)$ a $\mathbb{Z}_2[x]$

Sol.: $\mathbf{f(x) \equiv (x^2 + 1)\ (mod\ x^4 + x + 1)}$

(b) $(2x + 1)f(x) \equiv 1\ (mod\ 2x^2 + 2x + 2)$ a $\mathbb{Z}_3[x]$

Sol.: No té solució

(c) $(x^2 + 1)f(x) \equiv x^2 + x + 1\ (mod\ x^4 + 1)$ a $\mathbb{Z}_2[x]$

Sol.: No té solució

(d) $(2x + 1)f(x) \equiv 1\ (mod\ 2x^2 + 2x + 1)$ a $\mathbb{Z}_3[x]$

Sol.: $\mathbf{f(x) \equiv (x + 2)\ (mod\ 2x^2 + 2x + 1)}$

Capítol 3
Problemes de cossos finits

3.1 Per quins polinomis $f(x)$ de $\mathbb{Z}_2[x]$ el quocient $\mathbb{Z}_2[x]/(f(x))$ és un cos de 4 elements? Doneu-ne un element primitiu i la taula d'equivalències potencial-vectorial-polinomial. Doneu també una taula per la suma i una taula pel producte.

Resposta:

Per tal que $\mathbb{Z}_2[x]/(f(x))$ sigui un cos de 4 elements, cal que el grau de $f(x)$ sigui 2. Els polinomis de grau 2 són

- x^2
- x^2+1
- x^2+x
- x^2+x+1

Cap dels tres primers polinomis és irreductible a $\mathbb{Z}_2[x]$. En efecte, $x^2 = x \cdot x$, $x^2+1 = (x+1)\cdot(x+1)$ i $x^2+x = x(x+1)$. El quart és irreductible ja que és de grau 3 i no té arrels ($0^2+0+1 \neq 0$ i $1^2+1+1 \neq 0$).

Comprovem que la classe de x és un element primitiu. Diguem $\alpha = [x]$. Tenim $\alpha^2 = \alpha^2 - (\alpha^2+\alpha+1) = -\alpha-1 = \alpha+1 \neq 1$ i, per tant, és un element primitiu.

La taula d'equivalències potencial-vectorial-polinomial és la següent:

0	$(0,0)$	0
α^0	$(1,0)$	1
α	$(0,1)$	α
α^2	$(1,1)$	$1+\alpha$

Les taules de la suma i del producte són

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

3.2 * Considerem $\mathbb{Z}_3[x]/(x^2+x+2)$

(a) Demostreu que és un cos.

(b) Quants elements té?

(c) És $\alpha = [x]$ un element primitiu? Per què?

(d) Doneu-ne una taula d'equivalències amb les notacions potencial, polinomial i vectorial.

(e) Calculeu $\alpha^2 \left(\frac{\alpha^{20}-\alpha^5+\alpha}{\alpha^3-\alpha}\right)$.

Resposta:

(a) Cal veure si x^2+x+2 és irreductible i ho és perquè té grau 2 i no té arrels ($f(0)=2\neq 0$, $f(1)=1\neq 0$ i $f(2)=2\neq 0$).

(b) $3^2=9$.

(c) Els únics ordres possibles dels elements de $\mathbb{Z}_3[x]/(x^2+x+2)$ són els divisors de $9-1=8$, és a dir, $\{1,2,4,8\}$. Però α^1 i α^2 són $\neq 1$ i $\alpha^4=(\alpha^2)^2=(2\alpha+1)^2=4\alpha^2+4\alpha+1=\alpha^2+\alpha+1=2\alpha+1+\alpha+1=2\neq 1$. Per tant, l'ordre d'$\alpha$ no és $1,2$ ni 4 i ha de ser 8.

(d)

pot.	pol.	vect.
0	0	(0,0)
α	α	$(0,1)$
α^2	$2\alpha+1$	$(1,2)$
α^3	$2\alpha+2$	$(2,2)$
α^4	2	$(2,0)$
α^5	2α	$(0,2)$
α^6	$\alpha+2$	$(2,1)$
α^7	$\alpha+1$	$(1,1)$
α^8	1	$(1,0)$

(e) $\alpha^2\left(\frac{\alpha^{20}-\alpha^5+\alpha}{\alpha^3-\alpha}\right)=\alpha^2\left(\frac{\alpha^4-\alpha^5+\alpha}{\alpha^3-\alpha}\right)=\alpha^2\left(\frac{2-2\alpha+\alpha}{2\alpha+2-\alpha}\right)=\alpha^2\left(\frac{2+2\alpha}{\alpha+2}\right)=\alpha^2\left(\frac{\alpha^3}{\alpha^6}\right)=\frac{\alpha^5}{\alpha^6}=\frac{\alpha^{13}}{\alpha^6}=\alpha^7$.

3.3 Demostreu que x^3+x^2+1 és irreductible a $\mathbb{Z}_2[x]$ i, a partir d'aquí, construïu un cos finit de vuit elements.

Resposta:

Si $p(x)=x^3+x^2+1$ no fos irreductible a $\mathbb{Z}_2[x]$, podríem expressar-lo com a producte de polinomis (tres de grau 1 o un de grau 1 i un de grau 2). Per tant, intentarem descompondre $p(x)$ en $(x-0)\cdot g(x)$ o $(x-1)\cdot h(x)$.

Substituint x per 0 a $p(x)$ dóna 1, i substituint x per 1, també. Llavors, $p(x)$ és irreductible.

Construïm ara el cos $\mathbb{Z}_2[x]/x^3+x^2+1$ com:

$$\{[0],[1],[x],[1+x],[x^2],[1+x^2],[x+x^2],[1+x+x^2]\}$$

Agafem $\alpha = [x+1]$ i trobem les potències de α (recordeu que en els càlculs hem d'anar fent mòdul $x^3 + x^2 + 1$).

L'element que hem triat és primitiu, perquè anem trobant tots els elements diferents del cos, fins que fem α^7 i veiem que és el mateix que α^0:

$$\alpha = [x+1]$$

$$\alpha^2 = [x^2+1]$$

$$\alpha^3 = [x]$$

$$\alpha^4 = [x^2+x]$$

$$\alpha^5 = [x^2+x+1]$$

$$\alpha^6 = [x^2]$$

$$\alpha^7 = [1] = \alpha^0$$

Ara podem escriure la taula d'equivalències potencial-polinomial-vectorial:

Pot.	Pol.	Vec.
$\alpha^{-\infty}$	0	(0,0,0)
α^0	1	(1,0,0)
α^1	$x+1$	(1,1,0)
α^2	x^2+1	(1,0,1)
α^3	x	(0,1,0)
α^4	x^2+x	(0,1,1)
α^5	x^2+x+1	(1,1,1)
α^6	x^2	(0,0,1)

3.4 Hom pensa que la quantitat de solucions d'una equació polinòmica de grau m és, com a màxim, m. Fixeu-vos en l'equació polinòmica: $x^2 - 1 = 0$, i observeu que té quatre solucions a $\mathbb{Z}_8$; $x = 1, x = 3, x = 5, x = 7$. Quin és el problema?

Resposta:

Podem veure que l'equació $x^2 - 1 = 0$ té quatre solucions: $1, 3, 5$ i 7 a $\mathbb{Z}/8$. L'enunciat del problema es refereix al fet que una equació polinòmica de grau n, a coeficients en un cos, té, com a màxim, n solucions.

En el nostre problema, els coeficients ho són a $\mathbb{Z}/8$, que no és un cos.

3.5 Escriviu la taula d'equivalències per al cos finit $\mathbb{F}_{2^4}$, amb generador α.

(a) Determineu δ com a potència de α, on $\delta = \alpha^{10} + \dfrac{\alpha^7 + \alpha^{23}}{1 + \alpha^{12}} + 1$

(b) Trobeu totes les arrels de l'equació:

$$\alpha^7 x^2 + (\alpha^2 + \alpha^9)x + \frac{1+\alpha}{\alpha^4} = 0$$

Resposta:

Treballarem amb el cos $\mathbb{F}_{2^4} = \mathbb{Z}_2[x]/f(x)$, on $f(x)$ és un polinomi irreductible de grau 4 i coeficients a $\mathbb{Z}_2$.

Primerament, hem de trobar un polinomi irreductible i primitiu de quart grau. Trobem, primer, tots els polinomis irreductibles:

De grau 1 $\longrightarrow x,\ x+1$.
De grau 2 $\longrightarrow x^2+x+1$.
De grau 3 $\longrightarrow x^3+x^2+1,\ x^3+x+1$.
De grau 4 $\longrightarrow x^4+x^3+x^2+x+1,\ x^4+x^3+1,\ x^4+x+1$.

D'aquests últims polinomis de quart grau, en cercarem un que sigui primitiu, és a dir, que les seves arrels tinguin ordre $p^n-1=15$.

Comprovem el polinomi $x^4+x^3+x^2+x+1$:

Sigui α una arrel, llavors

$$\begin{aligned}\alpha^4 &= \alpha^3+\alpha^2+\alpha+1\ ,\\ \alpha^5 &= \alpha^4+\alpha^3+\alpha^2+\alpha=1\ ,\end{aligned}$$

$\alpha^5=1 \Longrightarrow \alpha$ no és d'ordre 15; per tant, el polinomi no és primitiu.

Comprovem ara el polinomi x^4+x^3+1:

Sigui α una arrel, llavors

$$\begin{aligned}\alpha^4 &= \alpha^3+1\\ \alpha^5 &= \alpha^4+\alpha=\alpha^3+\alpha+1\\ \alpha^6 &= \alpha^4+\alpha^2+\alpha=\alpha^3+\alpha^2+\alpha+1\\ \alpha^7 &= \alpha^4+\alpha^3+\alpha^3+\alpha=\alpha^2+\alpha+1\\ \alpha^8 &= \alpha^3+\alpha^2+\alpha\\ \alpha^9 &= \alpha^4+\alpha^3+\alpha^2=\alpha^2+1\\ \alpha^{10} &= \alpha^3+\alpha\\ \alpha^{11} &= \alpha^4+\alpha^2=\alpha^3+\alpha^2+1\\ \alpha^{12} &= \alpha^9+\alpha^6+\alpha^3+1=\alpha+1\\ \alpha^{13} &= \alpha^2+\alpha\\ \alpha^{14} &= \alpha^3+\alpha^2\\ \alpha^{15} &= 1\\ \alpha^{16} &= \alpha^3+\alpha^2+\alpha+1+\alpha^3+1+\alpha^2=\alpha\end{aligned}$$

Per tant, **el polinomi** x^4+x^3+1 **és primitiu.**

Així, doncs, utilitzarem el polinomi primitiu x^4+x^3+1 i $\mathbb{F}_{2^4}=\mathbb{Z}_2[x]/x^4+x^3+1$.

La taula d'equivalències potencial-vectorial és, doncs,

0	(0000)
α^0	(1000)
α^1	(0100)
α^2	(0010)
α^3	(0001)
α^4	(1001)
α^5	(1101)
α^6	(1111)
α^7	(1110)
α^8	(0111)
α^9	(1010)
α^{10}	(0101)
α^{11}	(1011)
α^{12}	(1100)
α^{13}	(0110)
α^{14}	(0011)

(a) Per determinar δ com a potència de α, calcularem:

$$\delta = \alpha^{10} + \frac{\alpha^7 + \alpha^{23}}{1 + \alpha^{12}} + 1 = \alpha^{10} + \frac{\alpha^7 + \alpha^8}{\alpha} + 1 = \alpha^{10} + \frac{\alpha^4}{\alpha} + 1 = \alpha^{10} + \alpha^3 + 1 = \alpha^{12}.$$

(b) Per trobar les arrels de l'equació, hem de resoldre:

$$\alpha^7 x^2 + (\alpha^2 + \alpha^9)x + \frac{1+\alpha}{\alpha^4} = 0,$$

o sigui: $\alpha^7 x^2 + x + \alpha^8$.
Per recerca exhaustiva sobre aquesta equació, trobem les arrels α^3 i α^{13}.

3.6 * (a) Per què per comprovar que un polinomi de grau menor o igual que 3 és irreductible n'hi ha prou de veure que no té arrels?

(b) Considerem el conjunt P de polinomis amb coeficients a $\mathbb{Z}_3$ que tenen exactament un monomi de grau senar i coeficient 1 i la resta de monomis de grau parell. Doneu-ne un exemple.

(c) Demostreu que un polinomi $p \in P$ que sigui irreductible ha de complir:
   (a) La suma dels seus coeficients no és múltiple de 3.
   (b) La suma dels seus coeficients no és congruent amb 2 mòdul 3.

(d) Doneu una altra condició que ha de complir un polinomi de P que sigui irreductible.

(e) Utilitzeu els apartats anteriors per donar un polinomi que generi $\mathbb{F}_{27}$.

Resposta:

(a) Perquè si té grau 2 només es pot descompondre en producte de dos polinomis de grau 1, mentre que si té grau 3 només es pot descompondre en producte d'un polinomi de grau 1 per un altre de grau 2 o bé en producte de tres polinomis de grau 1. En tots els casos es necessita un factor de grau 1. Però si no té arrels, aleshores no té factors de grau 1 i, per tant, no es descompon i és irreductible.

(b) $x^3 + x^2 + 2 \in P$

(c) (a) La suma dels coeficients de p és $p(1)$. Si $p(1)$ és un múltiple de 3, aleshores s'anul·la a $\mathbb{Z}_3$ i 1 és una arrel de p. Per tant, p no és irreductible.

(b) Tenim que $2^2 = 4 = 1$ a $\mathbb{Z}_3$. Per tant, $2^r = \begin{cases} 1 \text{ si } r \text{ és parell,} \\ 2 \text{ si } r \text{ és senar.} \end{cases}$

Tenim que $p(2)$ és la suma de coeficients més 1 i, per tant, $p(2)$ no s'anul·la a $\mathbb{Z}_3$ si i només si la suma de coeficients és congruent amb 2 mòdul 3.

(d) El coeficient constant, com que és $p(0)$, no ha de ser nul.

(e) $x^3 + 2x^2 + 1$ o bé $x^3 + x^2 + 2$.

3.7 Considerem els següents polinomis de $\mathbb{Z}_3[x]$.

- $f(x) = x^3 + x^2 + 2$,
- $g(x) = x^3 + 2x + 1$,
- $h(x) = x^3 + 2x^2 + 2$.

Sabem que

- $x^{11} \bmod f(x) = x + 1$,
- $x^{11} \bmod g(x) = x^2 + x + 2$,
- $x^{11} \bmod h(x) = 2x^2 + x + 1$.

(a) Quins d'aquests polinomis són irreductibles?

(b) Quins dels polinomis irreductibles són primitius?

(c) Per quins polinomis, en fer quocient a $\mathbb{Z}_3[x]$ s'obté un cos? De quants elements?

(d) Per quins dels polinomis anteriors que, en fer quocient, ens donen un cos, podem expressar qualsevol element del cos com a potència de la classe de x en el quocient?

3.8 Sigui $\mathbb{F}_{27} = \mathbb{F}_3/(x^3 + 2x + 1)$. Diguem $\alpha = [x]$. Siguin $f = x^7 - 1$ i $g = x^4 + \alpha x^2 + \alpha^2 x + 2$.

(a) Doneu una taula exponencial-vectorial de $\mathbb{F}_{27}$.

(b) Doneu el quocient i el residu de dividir f entre g.

(c) Calculeu la derivada de g.

(d) Avalueu el quocient $-\frac{f}{g'}$ en α^3.

Resposta:

(b) $x^3 + \alpha^{14}x + \alpha^{15}$ i $\alpha^{21}x^3 + \alpha^{16}x^2 + \alpha^{10}x + \alpha^8$.

(c) $x^3 + \alpha^{14}x + \alpha^2$.

(d) α^{25}.

3.9 (a) Comproveu que el polinomi $x^3 + x^2 + 1$ és irreductible i primitiu sobre $\mathbb{F}_2$.

(b) Construïu $\mathbb{F}_8$ utilitzant aquest polinomi, denotant α la classe de x. Doneu-ne una taula exponencial-vectorial.

(c) Calculeu el polinomi $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$.

(d) Considerem el polinomi $u(x) = \alpha x + \alpha^3 x^3 + x^4 + \alpha^2 x^6$. Calculeu

- $s_1 = u(\alpha)$.
- $s_2 = u(\alpha^2)$.
- $s_3 = u(\alpha^3)$.

(e) Considerem els polinomis $\sigma(x) = 1 + x$ i $S(x) = s_1 + s_2 x + s_3 x^2$. Calculeu $T(x) = S(x)\sigma(x)$.

(f) Calculeu el quocient q_0 i el residu r_0 de dividir $T(x)$ entre x^3.

(g) Calculeu el quocient q_1 i el residu r_1 de dividir x^3 entre r_0.

(h) Calculeu les arrels i la derivada del producte $\sigma(x)q_1(x)$.

3.10 Trobeu tots els polinomis irreductibles de grau 5 definits sobre $\mathbb{Z}_2$. Digueu quins d'aquests són primitius.

Resposta:

Hem de trobar tots els polinomis irreductibles de grau 5 sobre $\mathbb{Z}_2$.

De grau 1 $\longrightarrow x,\ x+1$.

De grau 2 $\longrightarrow x^2 + x + 1$.

De grau 3 $\longrightarrow x^3 + x^2 + 1,\ x^3 + x + 1$.

De grau 4 $\longrightarrow x^4 + x^3 + x^2 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x + 1$.

Els polinomis irreductibles de grau 5 han de tenir sempre terme independent (si no, serien divisibles per x) i un nombre senar de termes (si no serien divisibles per $(x+1)$).

Així, doncs, tenim vuit possibles candidats a ser polinomis irreductibles; però, descartant els dos que són productes de polinomis de grau 2 i 3, ens quedem amb els polinomis irreductibles següents:

$$\begin{array}{l} x^5 + x^3 + 1 \\ x^5 + x^2 + 1 \\ x^5 + x^3 + x^2 + x + 1 \\ x^5 + x^4 + x^2 + x + 1 \\ x^5 + x^4 + x^3 + x + 1 \\ x^5 + x^4 + x^3 + x^2 + 1 \end{array}$$

En total, tenim sis polinomis irreductibles de grau 5 sobre $\mathbb{Z}_2$.

Sigui $\mathbb{F}_{2^5} = \mathbb{Z}_2[x]/f(x)$ el cos generat a partir del polinomi primitiu $f(x)$, llavors l'ordre de α ($\alpha = [x]$) haurà de ser divisor de $2^5 - 1 = 31$.

Com que 31 és un nombre primer, els únics divisors de 31 seran 1 i 31.

Sabem que $\alpha^1 = \alpha \neq 1$ ja que $f(x)$ és irreductible i, per tant, tots els polinomis irreductibles de grau 5 seran primitius.

3.11 Trobeu els valors de m per als quals $x^2 + mx + 2$ és un polinomi irreductible primitiu a $\mathbb{Z}_{11}[x]$.

Resposta:

Hem de trobar tots els m tals que el polinomi $p(x) = x^2 + mx + 2$ sigui irreductible i primitiu a $\mathbb{Z}/11[x]$.

Primer trobarem els valors de m per als quals $p(x)$ és irreductible. Per fer-ho, suposarem que $x^2 + mx + 2 = (x - a)(x - b)$.

$$x^2 + mx + 2 = (x - a)(x - b) =$$

$$= x^2 - bx - ax + ab =$$

$$= x^2 - (a + b)x + ab$$

Llavors veiem que s'han de complir les equacions:

$$-(a + b) = m$$

$$ab = 2$$

I trobem les solucions:

$$a = 1 \quad b = 2 \quad m = 8$$

$$a = 2 \quad b = 1 \quad m = 8$$

$$a = 3 \quad b = 8 \quad m = 0$$

$$a = 4 \quad b = 6 \quad m = 1$$

$$a = 5 \quad b = 7 \quad m = 10$$

$$a = 6 \quad b = 4 \quad m = 1$$

$$a = 7 \quad b = 5 \quad m = 10$$

$$a = 8 \quad b = 3 \quad m = 0$$

$$a = 9 \quad b = 10 \quad m = 3$$

$$a = 10 \quad b = 9 \quad m = 3$$

La conclusió és que els possibles valors de m perquè $p(x)$ sigui irreductible són $2, 4, 5, 6, 7$ i 9.

Finalment, hem de substituir m per aquests valors i mirar que $p(x)$ sigui primitiu. Per veure que un polinomi és primitiu, hem de comprovar que les seves arrels tinguin ordre $p^n - 1$, o sigui, ordre 120. Un element α té ordre i si $\alpha^i = \alpha^0 = 1$ dins el cos en el qual estem treballant. Llavors, hauríem d'agafar $\alpha = [x]$ com a arrel i anar fent potències d'aquest element fins a arribar a un i tal que $\alpha^i = 1$. Si aquest i és 120 (ordre màxim), podem dir que aquest element és primitiu.

(Recordeu que no cal calcular totes les potències de α fins a 120. N'hi ha prou fent α^i amb i divisor de 120).

Fent això, ens queden com a valors que fan que $p(x)$ sigui primitiu $m = 4, 5, 6$ i 7.

3.12 Per a quins valors de p ($p = 3, 5, 7, 11, 13, 19, 23$) es pot construir un cos d'ordre p^2 usant el polinomi $x^2 + 1$?

Resposta:

Hem d'esbrinar per a quins valors de p es pot construir un cos amb p^2 elements a partir del polinomi **irreductible** $x^2 + 1$, és a dir, hem de construir un cos $\mathbb{F}_{p^2} = \mathbb{Z}_p[x]/x^2 + 1$.

Si $f(x) = x^2 + 1$ no és irreductible, podrà ser descompost de la forma $(x - a)(x - b)$. Aleshores, si existeixen valors $x = a$ o $x = b$ tals que $f(x) = 0 \bmod p$, $f(x)$ no serà irreductible i, per tant, $\mathbb{Z}_p[x]/x^2 + 1$ no serà un cos.

Suposem $f(x) = 0$; llavors, tindríem $x^2 + 1 = 0$ i $x^2 = -1 = p - 1 \bmod p$.

Així, doncs, comprovarem si $p-1$ té arrel quadrada mòdul p i, en cas afirmatiu, $f(x)$ no serà irreductible.

- Per $p = 3$**:** $x^2 = 2$ no té solució $\Longrightarrow f(x)$ és **irreductible**.
- Per $p = 5$**:** $x^2 = 4$ té solució $x = 2,\ x = -2 \Longrightarrow f(x)$ **no és irreductible**.
- Per $p = 7$**:** $x^2 = 6$ no té solució $\Longrightarrow f(x)$ **és irreductible**.
- Per $p = 11$**:** $x^2 = 10$ no té solució $\Longrightarrow f(x)$ **és irreductible**.
- Per $p = 13$**:** $x^2 = 12$ té solució $x = 5$ $(5^2 = 25 = 12 \bmod p) \Longrightarrow f(x)$ **no és irreductible**.
- Per $p = 19$**:** $x^2 = 18$ no té solució $\Longrightarrow f(x)$ **és irreductible**.
- Per $p = 23$**:** $x^2 = 22$ no té solució $\Longrightarrow f(x)$ **és irreductible**.

Els valors de p que compleixen que $\mathbb{F}_{p^2} = \mathbb{Z}_p[x]/x^2 + 1$ és un cos són: $3, 7, 11, 19$ i 23.

3.13 El polinomi $x^4 + x^3 + 1$ és irreductible i primitiu a $\mathbb{Z}_2[x]$. Diguem α a la classe de x. Dins el problema 3.5 teniu una taula d'equivalències vectorial-potencial pel cos $\mathbb{Z}_2[x]/x^4 + x^3 + 1$.

(a) Doneu l'expressió vectorial, polinòmica i potencial de l'element

$$\beta = \alpha^{12} \frac{\alpha^6 + \alpha}{\alpha^{13} - \alpha^8}.$$

(b) Quin és el polinomi mínim d'α? I de β?

(c) Doneu la matriu inversa de

$$\begin{pmatrix} \alpha^2 & \alpha^4 + \alpha^6 \\ \alpha^{11}\alpha^{13} & \alpha^7 \end{pmatrix}.$$

Resposta:

(a) vectorial: $(1, 1, 0, 1)$, polinòmica: $\alpha^3 + \alpha + 1$, potencial: α^5

(b) $x^4 + x^3 + 1$, $x^2 + x + 1$.

(c) $\begin{pmatrix} \alpha^6 & \alpha^{12} \\ \alpha^8 & \alpha \end{pmatrix}$.

3.14 Considerem el cos finit $\mathbb{F}_{25}$, generat per $x^2 - 2 \bmod 5$. És irreductible aquest polinomi? Per què? Diguem α l'element del cos que correspon a la classe de $x \bmod (x^2 - 2)$.

(a) Quin és l'ordre de α?

(b) Trobeu una arrel primitiva, diguem-ne β, i expresseu α com una potència d'aquesta.

(c) Calculeu el polinomi mínim de β.

(d) Calculeu el polinomi mínim de les cinc primeres potències de β.

Resposta:

Tenim el cos finit $\mathbb{F}_{25} = \mathbb{Z}_5[x] \,/\, f(x)$ on $f(x) = x^2 - 2$.

Comprovem si $f(x)$ és irreductible:

Si $f(x)$ no fos irreductible, tindríem:

$$x^2 - 2 = (x - a) \cdot (x - b) = x^2 - (a + b)x + a \cdot b$$

Llavors,

$$\begin{array}{ll} a + b = 0 & \Longrightarrow \quad a = -b \\ a \cdot b = -2 & \Longrightarrow \quad -b^2 = -2 = b^2 = 2 \end{array}$$

No existeix cap b tal que $b^2 = 2 \bmod 5$; per tant, podem deduir que el polinomi $f(x) = x^2 - 2$ **és irreductible**.

Per trobar l'ordre de α, hem de trobar l'exponent mínim e que compleixi: $\alpha^e = 1$.

$$\begin{array}{rcl} \alpha^1 & = & \alpha \neq 1 \\ \alpha^2 & = & 2 \neq 1 \\ \alpha^3 & = & 2\alpha \neq 1 \\ \alpha^4 & = & 4 \neq 1 \\ \alpha^5 & = & 4\alpha \neq 1 \\ \alpha^6 & = & 4\alpha^2 = 8 = 3 \neq 1 \\ \alpha^8 & = & 1 \end{array}$$

L'ordre de α és 8.

Per tal de trobar els elements de $\mathbb{F}_{25}$, utilitzarem una arrel primitiva $\beta \in \mathbb{F}_{25}$ tal que:

$$\mathbb{F}_{25} = \{0, \beta, \beta^2, \cdots, \beta^{p^n - 1}\},$$

β serà de la forma $a + b \cdot \alpha$, ja que $\mathbb{F}_{25}$ és un espai vectorial de dimensió 2 sobre $\mathbb{F}_5$ i els elements $1, \alpha$ en són una base.

Agafem, per exemple, $\beta = 2 + \alpha$.

Comprovem si $\beta = 2 + \alpha$ és un element primitiu. L'ordre de β serà un dels següents: 24, 12, 6, 8, 4, 3, 2, 1.

$$\begin{aligned}
&\beta = 2 + \alpha \\
&\beta^2 = 4 + 4\alpha + \alpha^2 = 4\alpha + 1 \\
&\beta^3 = 4\alpha^2 + 9\alpha + 2 = 4\alpha \\
&\beta^4 = 8\alpha + 4\alpha^2 = 3\alpha + 3 \\
&\beta^5 = 16\alpha^2 + 4\alpha = 4\alpha + 2 \\
&\beta^6 = 12\alpha^2 + 15\alpha + 3 = 2 \\
&\beta^7 = 16\alpha^2 + 12\alpha + 2 = 2\alpha + 4 \\
&\beta^8 = 3\alpha + 2 \\
&\beta^9 = 3\alpha \\
&\beta^{10} = \alpha + 1 \\
&\beta^{11} = 3\alpha + 4 \\
&\beta^{12} = 9\alpha^2 + 15\alpha + 6 = 4 \\
&\beta^{13} = 4\alpha + 3 \\
&\beta^{14} = \alpha + 4 \\
&\beta^{15} = \alpha \\
&\dots \quad \dots \\
&\beta^{24} = 16 = 1
\end{aligned}$$

Per tant, l'ordre de β val vint-i-quatre i β és primitiu. A més, tenim que $\beta^{15} = \alpha$.

Calculem ara el polinomi mínim de les cinc primeres potències de β:

Si β és un element primitiu, aleshores

$$m_\beta(x) = (x - \beta) \cdot (x - \beta^5) \in \mathbb{Z}_5[x].$$

Així, doncs,

- $m_\beta(x) = (x - \beta) \cdot (x - \beta^5) = x^2 - 4x + 2$;
- $m_{\beta^2}(x) = (x - \beta^2) \cdot (x - \beta^{10}) = x^2 - 2x + 4$;
- $m_{\beta^3}(x) = (x - \beta^3)(x - \beta^{15}) = x^2 + 3$;
- $m_{\beta^4}(x)) = x^2 - x + 1$;
- $m_{\beta^5}(x) = x^2 - 4x + 2$.

3.15 Considerem el cos finit generat per x^2+1 a $\mathbb{Z}_3$. És irreductible aquest polinomi? Per què? Quants elements té el cos generat? Diguem α l'element del cos que correspon a la classe de $x \bmod (x^2 + 1)$.

(a) Quin és l'ordre d'α?

(b) Trobeu una arrel primitiva, diguem-ne β, i expresseu α com una potència d'aquesta.

(c) Calculeu el polinomi mínim d'α i de β.

(d) Calculeu el polinomi mínim de les cinc primeres potències de β.

3.16 Sigui $\gamma \in \mathbb{F}_{p^m}$. Proveu que, si $\gamma \in \mathbb{Z}_p$, aleshores el seu polinomi mínim és $x - \gamma$, mentre que, si $\gamma \notin \mathbb{Z}_p$, aleshores γ té grau més gran que 1.

3.17 (a) Quins polinomis $x^2 - a$ són irreductibles sobre el cos $\mathbb{F}_5$?

(b) Descomponeu en factors els polinomis anteriors que no siguin irreductibles.

(c) A partir dels dos polinomis irreductibles trobats, construïu, en cada cas, el cos $\mathbb{F}_{25}$ i doneu l'isomorfisme que passa d'un cos a l'altre.

Resposta:

(a) Si el polinomi x^2-a no és irreductible, es descompondrà en dos polinomis $(x-b)$ i $(x-c)$. Substituint x per $0,1,2,3,4 \in \mathbb{F}_5$ i igualant a zero, obtenim $a = \pm 1$ o $a = 0$.

Per tant, el polinomi $x^2 - a$ és irreductible quan $a = \pm 2$.

(b)

$$x^2 - 0 = x \cdot x$$

$$x^2 - 1 = (x-1) \cdot (x+1) = (x-4) \cdot (x+4)$$

$$x^2 - 4 = (x-2) \cdot (x+2) = (x-3) \cdot (x+3)$$

(c) Podem construir $\mathbb{F}_{5^2}$ com $\mathbb{F}_{5^2} = \mathbb{Z}_5[x]/x^2-2$ o, també, com $\mathbb{F}_{5^2} = \mathbb{Z}_5[x]/x^2-3$.

Comencem per $\mathbb{F}_{5^2} = \mathbb{Z}_5[x]/x^2 - 2$.

Observem que $\alpha = [x]$ no té ordre màxim, ja que $\alpha^8 = \alpha^0$. Volem trobar un α amb ordre $p^n - 1 = 5^2 - 1 = 24$ que ens generi tot el cos.

Considerem $\alpha = [x+2]$ i donem la taula d'equivalències:

Pot.	Pol.	Vect.	Pot.	Pol.	Vect.
$\alpha^{-\infty}$	0	$(0,0)$	α^{12}	4	$(4,0)$
α^0	1	$(1,0)$	α^{13}	$3+4x$	$(3,4)$
α^1	$2+x$	$(2,1)$	α^{14}	$4+x$	$(4,1)$
α^2	$1+4x$	$(1,4)$	α^{15}	x	$(0,1)$
α^3	$4x$	$(0,4)$	α^{16}	$2+2x$	$(2,2)$
α^4	$3+3x$	$(3,3)$	α^{17}	$3+x$	$(3,1)$
α^5	$2+4x$	$(2,4)$	α^{18}	3	$(3,0)$
α^6	2	$(2,0)$	α^{19}	$1+3x$	$(1,3)$
α^7	$4+2x$	$(4,2)$	α^{20}	$3+2x$	$(3,2)$
α^8	$2+3x$	$(2,3)$	α^{21}	$2x$	$(0,2)$
α^9	$3x$	$(0,3)$	α^{22}	$4+4x$	$(4,4)$
α^{10}	$1+x$	$(1,1)$	α^{23}	$1+2x$	$(1,2)$
α^{11}	$4+3x$	$(4,3)$			

Ara hem de fer el mateix per a $\mathbb{F}_{5^2} = \mathbb{Z}_5[x]/x^2 - 3$.

Observem que un element primitiu és $\beta = [1+x]$.

En aquest cas, la taula d'equivalències és:

Pot.	Pol.	Vect.	Pot.	Pol.	Vect.
$\beta^{-\infty}$	0	$(0,0)$	β^{12}	4	$(4,0)$
β^0	1	$(1,0)$	β^{13}	$4+4x$	$(4,4)$
β^1	$1+x$	$(1,1)$	β^{14}	$1+3x$	$(1,3)$
β^2	$4+2x$	$(4,2)$	β^{15}	$4x$	$(0,4)$
β^3	x	$(0,1)$	β^{16}	$2+4x$	$(2,4)$
β^4	$3+x$	$(3,1)$	β^{17}	$4+x$	$(4,1)$
β^5	$1+4x$	$(1,4)$	β^{18}	2	$(2,0)$
β^6	3	$(3,0)$	β^{19}	$2+2x$	$(2,2)$
β^7	$3+3x$	$(3,3)$	β^{20}	$3+4x$	$(3,4)$
β^8	$2+x$	$(2,1)$	β^{21}	$2x$	$(0,2)$
β^9	$3x$	$(0,3)$	β^{22}	$1+2x$	$(1,2)$
β^{10}	$4+3x$	$(4,3)$	β^{23}	$2+3x$	$(2,3)$
β^{11}	$3+2x$	$(3,2)$			

Per trobar l'isomorfisme entre les dues construccions hauríem d'associar a $\alpha \in \mathbb{F}_{5^2}$ un element de $\mathbb{Z}_5/x^2-3$ que tingués el mateix polinomi mínim. L'isomorfisme serà $\phi(\alpha)=\beta^i$.
Calculem el polinomi mínim de α i busquem l'element β^i a l'altre cos que tingui el mateix polinomi mínim.
$m_\alpha(x)=(x-\alpha)(x-\alpha^5)=x^2+x+2$
$m_\beta(x)=(x-\beta)(x-\beta^5)=x^2-2x+3$
$m_{\beta^2}(x)=(x-\beta^2)(x-\beta^{10})=x^2+2x+4$
etc.
$m_{\beta^{19}}(x)=(x-\beta 19)(x-\beta^{23})=x^2+x+2$
L'isomorfisme serà $\phi(\alpha)=\beta^{19}$.

3.18 Utilitzeu l'algorisme de les divisions successives per calcular:

(a) L'invers de 43 en el cos $\mathbb{Z}_{101}$

(b) L'invers de $(1,2)$ en el cos $\mathbb{F}_{3^2}$ (genereu $\mathbb{F}_{3^2}$ a partir del polinomi irreductible $f(x)=x^2+1$)

Resposta:

(a) L'invers de 43 a $\mathbb{Z}_{101}$ serà un x tal que $43\cdot x = 1 \bmod 101$. Per tant, $43x=1+101y$.
Apliquem l'algorisme de les divisions successives amb:

$$r_{-2}=101$$
$$r_{-1}=43$$

Q_i	1	0	1	-2	3	-20	
P_i	0	1	-2	5	-7	47	
q_i			2	2	1	6	
r_i	101	43	15	13	2	1	0

$$1=101\cdot(-20)+43\cdot 47 \Longrightarrow 1=43\cdot \mathbf{47} \bmod 101.$$

Per tant, $43^{-1}=47 \bmod 101$.

(b) Anem a calcular l'invers de $(1,2)$ a $\mathbb{F}_{3^2}$, on $\mathbb{F}_{3^2}$ s'ha generat a partir de $f(x) = x^2 + 1$.
L'element $(1,2)$, en forma polinòmica, està representat per $1+2\alpha = 1+2x$, on $\alpha = [x] \in \mathbb{Z}_3[x]/x^2+1$.
Fem l'algorisme de les divisions successives entre x^2+1 i $2x+1$:

Q_i	1	0	1	
P_i	0	1	$x+1$	
q_i			$2x+2$	
r_i	x^2+1	$2x+1$	2	0

obtenim $1 \cdot (x^2+1) + (x+1) \cdot (2x+1) = 2$, o sigui:

$$(2x+2) \cdot (2x+1) = 1 \bmod x^2+1$$

Per tant, $(1,2)^{-1} = (2,2)$.

3.19 Donats els polinomis $S(x)$, $g(x) \in \mathbb{F}_{2^4}$:

$$S(x) = \alpha^{14} + \alpha^{13}x + \alpha x^2 + \alpha^4 x^3 + \alpha^5 x^4 + \alpha^2 x^5;\ g(x) = x^6,$$

trobeu els polinomis $\sigma(x)$ i $\omega(x)$ tals que:

$$\omega(x) = S(x)\sigma(x) \bmod g(x)$$

$$0 < grau(\sigma) \leqslant \frac{grau(g)}{2};\ 0 < grau(\omega) < \frac{grau(g)}{2}$$

Resposta:

El primer que hem de fer és construir el cos $\mathbb{F}_{2^4}$.

Agafem el polinomi primitiu $f(x) = x^4 + x^3 + 1$ i considerem el cos $\mathbb{F}_{2^4} = \mathbb{Z}_2[x]/f(x)$:

α^0	1	(1000)
α	x	(0100)
α^2	x^2	(0010)
α^3	x^3	(0001)
α^4	x^3+1	(1001)
α^5	x^3+x+1	(1101)
α^6	x^3+x^2+x+1	(1111)
α^7	x^2+x+1	(1110)
α^8	x^3+x^2+x	(0111)
α^9	x^2+1	(1010)
α^{10}	x^3+x	(0101)
α^{11}	x^3+x^2+1	(1011)
α^{12}	$x+1$	(1100)
α^{13}	x^2+x	(0110)
α^{14}	x^3+x^2	(0011)

Ara aplicarem l'algorisme de les divisions successives entre els polinomis

$$S(x) = \alpha^{14} + \alpha^{13}x + \alpha x^2 + \alpha^4 x^3 + \alpha^5 x^4 + \alpha^2 x^5$$

$$g(x) = x^6$$

Pararem l'algorisme quan trobem el primer residu de grau estrictament més petit que 3.

	1	0	1	$\alpha\alpha^{13}$	$\alpha\alpha^{12}\alpha^{10}$	$\alpha^5\alpha\alpha^{11}\alpha^3$
	0	1	0	1	$\alpha^{11}\alpha^{12}$	
q_i			0	$\alpha\alpha^{13}$	$\alpha^{11}\alpha^{12}$	$\alpha^3\alpha^8$
r_i	$S(x)$	$g(x)$	$S(x)$	$1\alpha^6\alpha^4\alpha^7\alpha^5$	$1\,1\,\alpha^5\alpha^{12}$	$\alpha^4\alpha^4\alpha^4$

Finalment, $\sigma(x) = \alpha^5 + \alpha x + \alpha^{11}x^2 + \alpha^3x^3$ i $w(x) = \alpha^4 + \alpha^4 x + \alpha^4 x^2$.

3.20 Descomponeu $x^{16} - x$ en factors irreductibles a $\mathbb{Z}_2[x]$.

Resposta:

$x^{16} - x = x^{2^4} - x$, que coincideix amb el producte de tots els polinomis a coeficients a $\mathbb{Z}_2$ irreductibles de grau divisor de 4.

Així, doncs, el problema serà trobar els polinomis irreductibles a $\mathbb{Z}_2[x]$ de grau 1, 2 i 4.

De grau 1 $\longrightarrow x,\ x+1$.

De grau 2 $\longrightarrow x^2 + x + 1$.

De grau 4 $\longrightarrow x^4 + x^3 + x^2 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x + 1$.

Per tant,

$$x^{16} - x = x \cdot (x+1) \cdot (x^2+x+1) \cdot (x^4+x^3+x^2+x+1) \cdot (x^4+x^3+1) \cdot (x^4+x+1)$$

3.21 Feu la descomposició factorial de $x^{24} - 1$, respectivament, sobre $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$ i $\mathbb{F}_7$.

Resposta:

- $\mathbb{F}_2$:
  Veiem que la factorització de $x^{24} - 1$ serà $(x^2 + x + 1)^8 \cdot (x + 1)^8$, ja que el cos és de característica 2, i podem fer:

  $$x^{24} - 1 = x^{24} - 1^{24} = (x^3)^8 - (1^3)^8 = (x^3 - 1^3)^8 = (x^2 + x + 1)^8 \cdot (x + 1)^8.$$

- $\mathbb{F}_3$:
  El cos és de característica 3:

  $$x^{24} - 1^{24} = (x^8 - 1^8)^3.$$

  Fent la descomposició de $x^8 - 1$, trobem:

  $$x^8 - 1 = (x - 1) \cdot (x - 2) \cdot (x^2 + x + 2) \cdot (x^2 + 1) \cdot (x^2 + 2 \cdot x + 2).$$

- $\mathbb{F}_4$:
  Agafem els elements $\{0, 1, \alpha, \alpha^2\}$, trobats fent la construcció del cos $\mathbb{F}_4 = \mathbb{Z}_2[x]/x^2 + x + 1$.
  El cos és de característica 2. Per tant, arribem a la mateixa expressió que a $\mathbb{F}_2$:
  $$x^{24} - 1 = (x^3 - 1)^8$$
  Però ara canvia la forma de descompondre: a $\mathbb{F}_2$ ens ha quedat un producte de dos polinomis, un de primer grau i un de segon grau. Ara, operant sobre $\mathbb{F}_4$, la descomposició queda:
  $$x^3 + 1 = (x + 1) \cdot (x^2 + x + 1) = (x + 1)(x + \alpha)(x + \alpha^2)$$
  Llavors $x^{24} - 1 = (x + 1)^8 \cdot (x + \alpha)^8 \cdot (x + \alpha^2)^8$.
- $\mathbb{F}_5$:
  $x^{24} - 1 = (x - 1) \cdot (x - 2) \cdot (x - 3) \cdot (x - 4) \cdot \ldots$, on els punts suspensius representen 10 polinomis irreductibles de grau 2:
  $$\begin{gathered} x^2 + 2 \\ x^2 + 3 \\ x^2 + x + 1 \\ x^2 + x + 2 \\ x^2 + 2x + 3 \\ x^2 + 2x + 4 \\ x^2 + 3x + 3 \\ x^2 + 3x + 4 \\ x^2 + 4x + 1 \\ x^2 + 4x + 2 \end{gathered}$$
  Aquests polinomis els hem trobat escrivint tots els polinomis de grau 2, bo i separant els irreductibles de grau 2, que són els que tenen la forma $(x - a) \cdot (x - b)$ per a algun a i $b \in \mathbb{F}_5$.
- $\mathbb{F}_7$
  Sabem que $x^{48} - 1$ és el producte de tots els polinomis irreductibles a coeficients a $\mathbb{F}_7$ de grau un divisor de 2.
  Però $x^6 - 1 | x^{12} - 1 | x^{24} - 1) | x^{48} - 1$; per tant, $x^{24} - 1$ descompondrà en producte de polinomis de grau 1 o 2.
  També sabem que:
  $x^{24} - 1 = (x^{12} + 1)(x^{12} - 1)$;
  $x^{12} - 1 = (x^6 + 1)(x^6 - 1)$;
  $x^6 - 1 = (x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6)$.
  El problema és descompondre $x^6 + 1$ i $x^{12} + 1$ com a producte de polinomis irreductibles a $\mathbb{Z}_7[x]$ de grau 2.
  Fem $y = x^2$ i considerem $y^3 + 1 = (y + 1)(y^2 + y + 1 = (y + 1)(y - 5)(y - 3)$, llavors $x^6 + 1 = (x^2 + 1)(x^2 + 2)(x^2 + 4)$.
  Fem ara $y = x^4$ i aprofitem el resultat anterior per escriure $x^{12} + 1 = (x^4 + 1)(x^4 + 2)(x^4 + 4)$.
  D'altra banda, els polinomis irreductibles de grau 2 a coeficients a $\mathbb{Z}_7$ són de la forma $x^2 + ax + b$. Multiplicant entre ells aquests polinomis $x^2 + ax + b$,

$x^2+a'x+b'$ de tal manera que $a+a'=0 \in \mathbb{Z}_7$, ja que volem que el resultat del producte doni x^4+1, x^4+2 o x^4+4, obtenim:

$$x^4+1=(x^2+3x+6)(x^2+4x+6)$$

$$x^4+2=(x^2+x+3)(x^2+6x+3)$$

$$x^4+4=(x^2+2x+5)(x^2+5x+5).$$

Finalment,
$x^{24}-1=(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)(x^2+1)(x^2+2)(x^2+4)(x^2+3x+6)(x^2+4x+6)(x^2+x+3)(x^2+6x+3)(x^2+2x+5)(x^2+5x+5)$

3.22 És possible que $f(x)$ sigui un divisor de $g(x)$? (Sí o no i, en tot cas, per què?)
$f(x)=x^5+x^2+3x+1 \in \mathbb{F}_7[x]$
$g(x)=x^{49}-x \in \mathbb{F}_7[x]$

Resposta:

Sabem que $(x^{p^n}-x)$ és el producte de tots els polinomis irreductibles diferents de $\mathbb{Z}_p[x]$, de grau k, on $k|n$.

$x^{49}-x=x^{7^2}-x$ i els polinomis irreductibles que ens interessen són de grau 1 i de grau 2.

$f(x)$ no té cap arrel a $\mathbb{Z}_7$, i ho veiem substituint $f(x)$ per tots els elements del cos $\mathbb{Z}_7$: $f(0)=1$, $f(1)=6$, $f(2)=1$, $f(3)=3$, $f(4)=3$, $f(5)=2$, $f(6)=5$.

Per tant, si $f(x)$ fos un divisor de $g(x)$, seria producte de polinomis de grau 2, i això no és possible ja que el seu grau és 5.

3.23 Proveu que, en un cos de característica p,

$$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p.$$

3.24 Demostreu que, en el cos $\mathbb{F}_q$, on q és una potència d'un nombre primer imparell, el producte de tots els elements no nuls és -1.

Resposta:

Els cos $\mathbb{F}_{p^n}$ està format pels elements que compleixen $x^{p^n}-x=0$. Anomenarem aquests elements com $\{0,a_1,a_2,\cdots,a_{p^n-1}\}$.

Llavors: $x^{p^n-1}-1=(x-a_1)(x-a_2)\cdots(x-a_{p^n-1})$.

Fent operacions:

$$x^{p^n-1}-1=x^{p^n-1}-\underbrace{(a_1+a_2+\cdots+a_{p^n-1})}_{=0}x^{p^n-2}+\cdots+(-1)^{p^n-1}\prod a_i$$

Si p és senar, p^n-1 és parell. Llavors el productori és igual a -1.

3.25 Demostreu que, en un cos finit de característica p,

(a) si $p=2$, cada element és un quadrat;

(b) si p és imparell, exactament la meitat dels elements són quadrats.

Resposta:

(a) Si $p = 2 \longrightarrow \mathbb{F}_{2^n} = \{0, \alpha^1, \alpha^2, \cdots, \alpha^{2^n-1}\}$, on α és un element primitiu.
Cal veure si α té arrel quadrada:

$$\alpha^0 = \alpha^{2^n-1} \Longrightarrow \alpha = \alpha^{2^n} \Longrightarrow \sqrt{\alpha} = \alpha^{2^{n-1}}$$

Com que α té arrel quadrada, tots els elements de $\mathbb{F}_{2^n}$ en tindran també.

(b) Si $p = 2k+1 \longrightarrow \mathbb{F}_{p^n} = \{0, \alpha^1, \alpha^2, \cdots, \alpha^{p^n-1}\}$, on α és un element primitiu i $\alpha^{p^n-1} = \alpha^0$.
Evidentment, α^{2k} té arrel quadrada, així com el zero. Per tant, els elements que podem assegurar que tenen arrel quadrada seran:

$$\{0, \alpha^0, \alpha^2, \cdots, \alpha^{p^n-1}\}$$

que són exactament la meitat dels elements no nuls de $\mathbb{F}_{p^n}$ i, a més a més, el zero.
Anem a veure que no hi ha cap més element a $\mathbb{F}_{p^n}$, a banda dels anteriors, que tingui arrel quadrada i, per això, veurem que $\phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$, tal que $\phi(x) = x^2$, és una aplicació que, llevat del zero, totes les imatges tenen exactament dues antiimatges.
Suposem que dos elements $x, y \in \mathbb{F}_{p^n}, x \neq y$ tenen un mateix quadrat, és a dir, $x^2 = y^2$. Llavors

$$x^2 = y^2 \Longrightarrow x^2 - y^2 = 0 \Longrightarrow (x+y) \cdot (x-y) = 0$$

Aquesta equació té dues possibles solucions: $x = y$ i $x = -y$. Com que p és imparell, sempre existiran valors diferents $x, y \in \mathbb{F}_{p^n}$ tals que $x = -y$, excepte en el cas del zero.

3.26 Proveu que, en un cos finit de q elements, hi ha $\phi(q-1)$ elements primitius.

3.27 Quins membres de $\mathbb{F}_9$ es poden agafar com a generadors del seu grup multiplicactiu?

Quins membres de $\mathbb{F}_9$ tenen arrel quadrada en aquest cos?

Resposta:

$$\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2 = \{0, \alpha^0, \alpha, \cdots, \alpha^7\} \text{ , on } \alpha = [x]$$

- Hi ha $\phi(8)$ generadors del grup multiplicatiu d'aquest cos. $\phi(8) = \phi(2^3) = 2^2 \cdot 1 = 4$.
  Els generadors del cos seran de la forma α^i, on $m.c.d.(i, 8) = 1$; per tant, $i = 1, 3, 5$ i 7.
  Així, doncs, els generadors seran $\{\alpha, \alpha^3, \alpha^5, \alpha^7\}$.
- Els elements que tenen arrel quadrada seran els d'exponent parell, és a dir, $\{0, \alpha^0, \alpha^2, \alpha^4, \alpha^6\}$.

3.28 Si F és el cos finit $\mathbb{F}_{p^m}$, demostreu que qualsevol funció

$$f : F \longrightarrow F$$

és una funció polinòmica de grau, com a màxim, $p^m - 1$.

Resposta:

Sigui $F = \mathbb{F}_{p^m}$ i $f : F \to F$ una funció polinòmica de grau menor o igual a $p^m - 1$, o sigui, $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_r x^r$, on $a_i \in F$ i $r \leqslant p^m - 1$.

Agafem un element qualsevol de F (diguem-li z) i mirem el valor de $f(z)$. Això ens donarà una equació lineal amb $r + 1$ incògnites. Si podem calcular totes les incògnites, haurem escrit la funció f com a polinomi.

Calculem $f(z)$ per a tots els elements de F: obtenim p^m equacions, amb les $r + 1$ incògnites.

Escrivim la matriu del sistema lineal obtingut:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^r \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2r} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^r & \alpha^{2r} & \cdots & \alpha^{rr} \end{pmatrix}$$

Aquesta matriu és quadrada de la forma de VanderMonde (aquestes matrius tenen la propietat que el determinant és no nul). Per tant, el sistema d'equacions té solució i és única.

3.29 Feu un gràfic del reticle de subcossos de $\mathbb{F}_{p^{16}}$, $\mathbb{F}_{p^{20}}$ i $\mathbb{F}_{p^{24}}$.

Resposta:

Observeu les figures 1.1, 1.2 i 1.3.

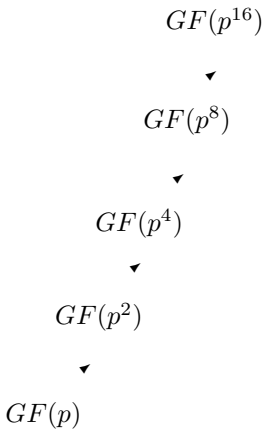


Figura 3.1: Reticle de subcossos per a $\mathbb{F}_{p^{16}}$

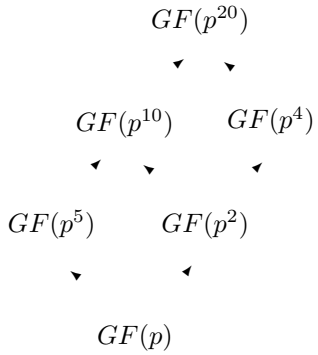


Figura 3.2: Reticle de subcossos per a $\mathbb{F}_{p^{20}}$

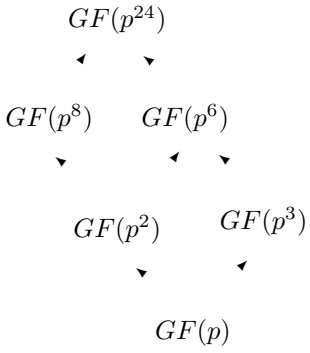


Figura 3.3: Reticle de subcossos per a $\mathbb{F}_{p^{24}}$

Capítol 4
Problemes de codis correctors

4.1 Considerem l'espai vectorial $\mathbb{F}_2^6$. Anomenem $d(x, y)$ la distància de Hamming entre dos elements de $\mathbb{F}_2^6$. Quants elements hi ha a cada esfera de radi 1? És possible trobar un conjunt C de 9 vectors de $\mathbb{F}_2^6$ tals que per a qualssevol $x, y \in C$, on $x \neq y$, resulti $d(x, y) \geqslant 3$?

Resposta:

Diguem $F = \mathbb{F}_2^6$. La distància de Hamming $d(x, y)$ es defineix com el nombre de coordenades diferents entre els vectors x i y.

El nombre d'elements que hi ha dins una esfera de radi unitat serà el cardinal de $B(v, 1)$ on

$$B(v, 1) = \{x \in F \mid d(x, v) \leq 1\}$$

$$\|B(v, 1)\| = 1 + \binom{6}{1} \cdot (q - 1) = 1 + 6 = 7.$$

Tenim que a cada esfera de radi 1 hi ha 7 elements de F.

En el centre de cada esfera hi haurà una paraula codi, per tant, com que el nombre total d'elements de F és $2^6 = 64$, i com que $9 \cdot 7 \leq 64$, llavors hi haurà com a molt nou paraules codi i, per tant, nou esferes de radi 1 diferents.

Anem a veure si podem fer-ne una construcció efectiva. Suposem els nou vectors ja construïts i considerem-ne les dues últimes coordenades. Poden ser $(00), (01), (10), (11)$ i, per això, hi haurà, com a mínim, tres vectors d'entre els nou que tindran les mateixes dues últimes coordenades. Aquests tres vectors tindrien distància 3 entre ells, considerant només les primeres quatre coordenades.

El problema que tenim ara és el següent:

Podem construir tres vectors de quatre coordenades binàries tals que la distància de Hamming entre ells sigui, com a mínim, 3?

La resposta, per recerca exhaustiva, és negativa.

Per tant, tornant al problema inicial, **no** és possible trobar un conjunt C de nou vectors a F, tals que $d(x,y) \geqslant 3$, per a tot $x, y \in C$.

4.2 Demostreu que en un codi ternari $C(M, n=3, d=2)$ es compleix $M \leqslant 9$.

Demostreu que existeix un codi ternari $C(M=9, n=3, d=2)$.

Generalitzeu els resultats anteriors al cas de codis q-aris de paràmetres $(M, n=3, d=2)$.

Resposta:

- Llistem les M paraules codi i, en cadascuna, suprimim l'última coordenada. Com que en el codi original C la distància mínima és 2, resultarà que observant les dues primeres coordenades no poden haver-hi vectors repetits. Per tant, com a màxim, n'hi haurà nou de diferents. Llavors $M \leqslant 9$.
- Per fer la construcció d'un codi C que tingui exactament nou paraules codi, podem agafar les nou possibles parelles (a,b) $((00), (10), (20), \cdots, (22))$ i, a cadascuna, afegir-hi una tercera coordenada x tal que $x = a+b \bmod 3$. Hem obtingut un codi C de nou vectors que entre ells tenen distància mínima 2. Aquest codi és

$$C = \{(000), (011), (022), (101), (112), (120), (202), (210), (221)\}$$

- Generalitzant a codis q-aris tindríem $M \leqslant q^2$ i podríem construir, fent consideracions semblants a les d'abans, efectivament un codi on $M = q^2$.

4.3 Després de mostrejar un senyal el volem transmetre a 20 Kbits/seg i s'està utilitzant un ample de banda de 2.500 Hz. Digues de quants bits et sembla que haurien de ser les mostres de manera que no hi hagi pèrdues en la transmissió.

Resposta:

Segons el teorema de Nyquist, hauríem de mostrejar el senyal al doble de la freqüència màxima que, en el nostre cas, serà de 2.500 Hz. Això ens dóna una proporció de 5.000 mostres/segon i, si cada mostra és de x bits, obtindrem una transmissió a $5.000 \cdot x$ bits/segpn o, el que és el mateix, $5 \cdot x$ Kbits/seg. Perquè no hi hagi pèrdues en la transmissió s'hauria de complir: $5x > 20$ i, per tant, $x > 4$.

4.4 (R. Balcells, A. Martín, J. Oliveras)

No podem enviar informació per un canal continu, ja que la taxa E_b/N no supera el valor límit.

(a) Quines característiques hauríem de modificar (i com) per poder utilitzar aquest canal per transmetre informació?

(b) Si el paràmetre E_b/N no supera la fita de Shannon, és un bon mètode la utilització de codis correctors d'errors per aconseguir transmetre informació pel canal?

Resposta:

(a) Sabem que:

$$\frac{E_b}{N_0} \geqslant 10 \log \frac{2^r - 1}{r}$$

Per tant, per fer possible una comunicació, hauríem d'augmentar l'energia al bit E_b, disminuir la potència del soroll N_0 o disminuir r. Per altra banda, $r = \dfrac{R_b}{B}$ i, per tant, disminuir r equival a disminuir la taxa de transmissió R_b o augmentar l'amplitud de banda B.

Si $\dfrac{E_b}{N_0}$ no supera la fita de Shannon, o sigui, $\dfrac{E_b}{N_0} < \ln 2 \leqslant 10 \log \dfrac{2^r - 1}{r}$, encara que variem r, no aconseguirem superar el límit de Shannon, per tant, en aquest cas, només podem actuar sobre l'energia al bit o la potència del soroll.

(b) No. Si el paràmetre E_b/N no supera la fita de Shannon, encara que s'utilitzin codis correctors d'errors, no aconseguirem enviar informació fiable pel canal, ja que el que fan els codis correctors d'errors és disminuir la taxa de transmissió, o sigui, disminuir r i, amb això, el valor de $\dfrac{E_b}{N_0}$ no varia.

4.5 Volem transmetre informació a través d'un canal binari i simètric amb probabilitat d'error al bit de $0,05$. Per fer-ho utilitzarem un codi de Hamming sobre $\mathbb{F}_{2^2}$, de paràmetre $t = 2$.

Calculeu la probabilitat d'error residual i el guany de la codificació.

Resposta:

El codi té longitud $n = \dfrac{4^2 - 1}{4 - 1} = 5$ i dimensió $k = n - t = 5 - 2 = 3$. Això significa que hem de fer blocs de 6 bits que es convertiran en 10 després de la codificació i que seran els que passaran pel canal.

La probabilitat d'error en la paraula enviada és de:

$P_e = 1 - ((1-p)^{10} + 10p(1-p)^9 + 5p^2(1-p)^8)$,

i la probabilitat residual es pot calcular com p_r, de manera que:

$1 - (1 - p_r)^6 = P_e$.

Fent operacions resulta $p_{r1} = 0,01$.

En decibels, la codificació aporta un guany de $10 \log_{10}(\dfrac{0,01}{0,05}) = 5,71 dB$.

4.6 Utilitzem un codi de Hamming binari paràmetre $t = 3$ en un canal binari i simètric amb probabilitat d'error al bit d'1%.

Calculeu la probabilitat residual d'error al bit després d'utilitzar aquest codi i el guany en decibels.

Resposta:

El codi és 1-corrector, la dimensió és 4 i la longitud 7, o sigui, un codi $C(7, 4)$.

Hi haurà errors residuals a la transmissió quan, en una trama de 7 bits, es produeixin dos o més errors en el canal. La probabilitat que no hi hagi cap error o que només n'hi hagi un és:

$pc = (1-p)^7 + 7(1-p)^6 p = 0.9979689584$,

on $p = 0.01$ és la probabilitat d'error al bit del canal.

Després de la utilització del codi de Hamming, és com si tinguéssim un canal virtual amb una probabilitat d'error al bit P (que és la probabilitat residual que ens demana el problema).

Utilitzant un codi $C(7,4)$ tenim 4 bits d'informació en cada trama de 7 bits i la probabilitat que quatre bits d'informació es transmetin correctament és $(1-P)^4$. Aquest últim valor ha de coincidir amb pc. O sigui, $(1-P)^4 = pc$ i, d'aquí, $P = 0.0005081476$.

El guany del codi és: $10\log_{10}(\frac{p}{P}) = 12.94010121$.

4.7 Per un canal binari i simètric de probabilitat d'error al bit $p = 0.01$, transmetem informació codificada utilitzant el codi de Hamming $\mathcal{H}(5,3)$, sobre $\mathbb{F}_{2^2}$. Calculeu la probabilitat residual d'error al símbol del canal.

4.8 Suposem que C és un codi t-corrector, lineal i binari (n,k). Suposem que usem un canal BSC de probabilitat d'error, p, molt petita. Demostreu que la probabilitat d'error a la paraula tramesa es pot calcular, aproximadament, per:

$$\left(\binom{n}{t+1} - \alpha_{t+1}\right) \cdot p^{t+1}$$

on α_{t+1} és la quantitat de cossets-líders de pes $(t+1)$ de C.

Resposta:

La probabilitat d'error a la paraula tramesa consisteix en la probabilitat que hi hagi més de t errors en una paraula donada:

$$p = \binom{n}{t+1} p^{t+1}(1-p)^{n-t-1} + \binom{n}{t+2} p^{t+2}(1-p)^{n-t-2} + \cdots$$

Ara bé, si α_{t+1} és la quantitat de cossets-líders de pes $(t+1)$ de C, en el cas que l'error sigui exactament un d'ells el corregirem bé. Llavors la probabilitat anterior seria:

$$p = \left(\binom{n}{t+1} - \alpha_{t+1}\right) p^{t+1}(1-p)^{n-t-1} + \ldots$$

i es pot aproximar per:

$$\left(\binom{n}{t+1} - \alpha_{t+1}\right) \cdot p^{t+1}.$$

4.9 Sigui C un codi lineal i binari de tipus (n,k), que té per enumerador de pesos el polinomi $A(z)$.

Fem servir el codi anterior en un canal BSC de probabilitat d'error p, amb el propòsit de detectar errors i no de corregir-los.

Quina és la probabilitat de rebre una paraula incorrecta i que no es detecti l'error?

Resposta:

Si el codi $C(n,k)$ és de distància mínima d, podrem detectar, com a màxim, fins a $d-1$ errors.

Que no detectem un error significa que l'error és tan gran que fa canviar una paraula codi per una altra.

El canal és BSC amb probabilitat d'error p.

Comencem calculant la probabilitat de no detectar un error quan aquest és una paraula codi $\overrightarrow{v_1}$ de pes i:

$$P(\overrightarrow{e} = \overrightarrow{v_1}) = (1-p)^{n-i} \cdot p^i.$$

Llavors:

$$P(\overrightarrow{e} = \text{ paraula codi de pes } i) = A_i \cdot (1-p)^{n-i} \cdot p^i,$$

on A_i és la quantitat de paraules codi de pes i, és a dir, el coeficient de x_i del polinomi enumerador de pesos:

$$A(x) = \sum_{i=0}^{n} A_i \cdot x^i.$$

La probabilitat que ens demana el problema és:

$$P = \sum_{i=0}^{n} A_i \cdot (1-p)^{n-i} \cdot p^i = \sum_{i=0}^{n} A_i \cdot \frac{p^i}{(1-p)^i} \cdot (1-p)^n =$$

$$(1-p)^n \cdot \sum_{i=0}^{n} A_i \cdot \left(\frac{p}{1-p}\right)^i = A(x) \Big| \; x = \tfrac{p}{1-p} \quad .$$

Capítol 5
Problemes de codis lineals

5.1 * Dins de $\mathbb{F}_2^3$ considerem el conjunt de paraules $C = \{(000), (111), (101), (010)\}$.

(a) Demostreu que C és un codi lineal.

(b) Doneu una matriu generadora, G, de C.

(c) Comproveu que totes les paraules de C estan generades per G.

(d) Doneu una matriu de control de C.

(e) Justifiqueu quina és la distància mínima de C.

(f) Comproveu que totes les paraules del codi, quan les multipliquem per la matriu de control, donen 0.

(g) Doneu el codi dual $C^{\perp}$.

(h) Comproveu que les paraules del codi dual, quan les multipliquem per la matriu G, donen 0.

Resposta:

(a) Podem comprovar que és un espai vectorial perquè les combinacions lineals de dos vectors qualssevol de C és dins de C. En efecte,

$$\begin{array}{lcllcl}
(000) & + & (000) & = & (000) & \in & C \\
(000) & + & (111) & = & (111) & \in & C \\
(000) & + & (101) & = & (101) & \in & C \\
(000) & + & (010) & = & (010) & \in & C \\
(111) & + & (111) & = & (000) & \in & C \\
(111) & + & (101) & = & (010) & \in & C \\
(111) & + & (010) & = & (101) & \in & C \\
(101) & + & (101) & = & (000) & \in & C \\
(101) & + & (010) & = & (111) & \in & C \\
(010) & + & (010) & = & (000) & \in & C
\end{array}$$

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

(c) Vegem com la matriu G genera tot C:

$$\begin{array}{ll}
\begin{pmatrix} 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \\
\begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}
\end{array}$$

(d) Com que G té la forma $(I|P)$, podem construir H com $(-P^T|I)$. Ens queda $H = (101)$.

(e) $d = 1$. Es pot veure per la matriu de control o perquè hi ha una paraula de pes 1 o perquè podem trobar dues paraules a distància 1.

(f) Podem comprovar que totes les paraules de C, quan les multipliquem per H, ens donen 0. En efecte,

$$\begin{array}{lll}
\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & = & 0 \\
\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} & = & 0 \\
\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} & = & 0 \\
\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} & = & 0
\end{array}$$

(g) El codi dual és el que està generat per H. En el nostre cas és $\{0H, 1H\} = \{(000), (101)\}$.

(h)

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

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

5.2 Els llibres tenen assignat un número que correspon a l'International Standard Book Number (ISBN). Aquest número és un element d'un codi de longitud 10, sobre l'alfabet decimal. Els nou primers dígits donen informació sobre l'idioma, l'editorial i el número dins l'editorial. L'últim dígit és tal que $\sum_{i=1}^{10} i \cdot x_i \equiv 0 \bmod 11$.

Demostreu:

(a) Que el codi ISBN és capaç de detectar un error.

(b) Que el codi ISBN és capaç de detectar dos errors, si aquests consisteixen en la transposició de dos dígits.

(c) Que el codi ISBN és capaç de corregir un esborrall.

(d) Quín és el dígit que falta al codi ISBN $0131 * 91399$?

Resposta:

Cada número ISBN conté 10 dígits decimals, és a dir:

$$x = x_1, x_2, x_3, \cdots, x_{10} \text{ on cada } x_j \in \{0, 1, \cdots, 9\}$$

L'últim dígit és tal que:

$$\sum_{i=1}^{10} i \cdot x_i = 0 \bmod 11 \Longrightarrow \left(\sum_{i=1}^{9} i \cdot x_i\right) + 10 \cdot x_{10} = 0 \bmod 11 \Longrightarrow$$

$$\sum_{i=1}^{9} i \cdot x_i = -10 \cdot x_{10} \bmod 11 \Longrightarrow x_{10} = \sum_{i=1}^{9} i \cdot x_i \bmod 11$$

Demostrem que:

(a) El codi ISBN pot detectar un error.

Suposem $x = x_1, x_2, x_3, \cdots, x_{10}$ amb un error; per tant, x'_j és de la forma $x_j + e \bmod 11$, on e és l'error a detectar.

$$\sum_{i=1}^{10} i \cdot x_i = 0 \bmod 11 \Longrightarrow \left(\sum_{i=1}^{10} i \cdot x_i\right) + j \cdot e = 0 \bmod 11$$

Tenim que $j \cdot e = 0 \bmod 11$, però $e \neq 0$ i $j \geq 1$; per tant, això no pot ser.
Queda demostrat, doncs, que el codi ISBN detecta un error.

(b) El codi ISBN detecta dos errors, si aquests consisteixen en la transposició de dos dígits.

Suposem que x_j es transposa amb x_k, on $x_j \neq x_k$.
Podem considerar aquesta transposició com

$$x'_j = x_k$$
$$x'_k = x_j$$

Així, doncs, no detectarem el problema si

$$\sum_{i=1}^{10} i \cdot x'_i \; = \; 0$$

O sigui:

$$0 = \sum_{i=1}^{10} i \cdot x'_i = \left(\sum_{i=1}^{10} i \cdot x_i\right) + j \cdot x'_j + k x'_k - j x_j - k x_k =$$
$$j x_k + k x_j - j x_j - k x_k = j(x_k - x_j) - k(x_k - x_j) = (j-k)(x_k - x_j)$$

però $e = x_k - x_j$ té invers mòdul 11, ja que $e \neq 0$; per tant, $j - k = 0 \bmod 11$ i $j = k$.
Això vol dir que, si suposem $j \neq k$, sempre detectarem els dos errors.

Així, doncs, queda demostrat que qualsevol transposició de dos dígits diferents és detectable.

(c) El codi ISBN pot corregir un esborrall.

Suposem un esborrall a la posició j:

$$j \cdot x_j + \sum_{i=1,\, i\neq j}^{10} i \cdot x_i = 0 \Longrightarrow j \cdot x_j = - \sum_{i=1,\, i\neq j}^{10} i \cdot x_i \Longrightarrow$$

$$x_j = - \sum_{i=1,\, i\neq j}^{10} \frac{i \cdot x_i}{j} \quad \text{ja que } j \text{ té invers.}$$

(d) Trobarem el dígit que falta al codi ISBN 0131$*$91399.

La posició de l'esborrall és $j = 5$. Segons l'expressió de l'apartat anterior:

$$x_5 = \frac{-(1 \cdot 0 + 2 \cdot 1 + 3 \cdot 3 + \cdots + 9 \cdot 9 + 10 \cdot 9)}{5} = \frac{-7}{5} = \frac{4}{5};$$

com que $4 \cdot 5^{-1} = 4 \cdot 9 = 36 = \mathbf{3}$, tenim $x_5 = 3$.

El codi ISBN original és 0131391399.

5.3 A l'Estat espanyol s'assigna a cada persona un número de NIF que consisteix en el número de DNI (8 dígits decimals) seguit d'una lletra que s'assigna a la classe del DNI a $\mathbb{F}_{23}$. Aquesta assignació *lletra-classe* es fa de la manera següent:

A=3; B=11; C=20; D=9; E=22; F=7; G=4; H=18; J=13; K=21; L=19; M=5; N=12; P=8; Q=16; R=1; S=15; T=0; V=17; W=2; X=10; Y=6; Z=14.

Descriviu les capacitats correctores i/o detectores d'errors d'aquest codi NIF, i compareu-les amb les del codi ISBN del problema 2.

Resposta:

Quan detectem un error, pot ser al número o a la lletra (en aquest últim cas, la correcció és directa).

Les paraules codi són de la forma $(x_0, x_1, \cdots x_8)$, on $x_i \in \{0..9\}$ per a $0 \leqslant i \leqslant 7$ i $x_8 \in \{A..Z\}$, $x_8 = \phi\left(\sum_{i=0}^{7} x_i 10^{7-i}\right)$, i ϕ és la correspondència donada a l'enunciat.

- **Detecció d'un error:**

  Suposem que tenim un error a la coordenada x_j: ${x_j}^* = x_j + e$, on $e \in \{0..9\}$ i $j \neq 8$.

  $$\sum_{i=0}^{7} 10^{7-i} \cdot x_i^* = \sum_{i=0}^{7} 10^{7-i} \cdot x_i + 10^{7-j} \cdot e$$

  i $\phi(\sum_{i=0}^{7} 10^{7-i} \cdot x_i^*)$ serà diferent de $\phi(\sum_{i=0}^{7} 10^{7-i} \cdot x_i)$.

  Anem a veure ara que també podem detectar dos errors quan aquests es produeixen com a transposició de dos dígits numèrics consecutius.

  Suposem que $x_j^* = x_k$ i $x_k^* = x_j$.

  Llavors:

  $\sum_{i=0}^{7} 10^{7-i} \cdot x_i^* = \sum_{i=0}^{7} 10^{7-i} \cdot x_i - 10^{7-j} x_j - 10^{7-k} x_k + 10^{7-j} x_k + 10^{7-k} x_j =$

  $\sum_{i=0}^{7} 10^{7-i} \cdot x_i + 10^{7-j}(x_k - x_j) - 10^{7-k}(x_k - x_j) = \sum_{i=0}^{7} 10^{7-i} \cdot x_i + (10^{7-j} - 10^{7-k})(x_k - x_j)$

  Però $k \neq j$ i $10^{7-j} \neq 10^{7-k} \bmod 23$. Llavors $\sum_{i=0}^{7} 10^{7-i} \cdot x_i^* \neq \sum_{i=0}^{7} 10^{7-i} \cdot x_i$.

- **Correcció d'un esborrall:**

  Si l'esborrall és la lletra x_8, només cal recalcular $\phi(\sum_{i=0}^{7} 10^{7-i} \cdot x_i)$ per corregir-lo.

  Si l'esborrall és un dígit numèric, per exemple x_a, llavors:

  $\phi(\sum_{i=0}^{7} 10^{7-i} \cdot x_i) = x_8 = \phi(\sum_{i=0, i\neq a}^{7} 10^{7-i} \cdot x_i + x_a 10^{7-a})$ ens permet recalcular x_a fent:

  $$x_a 10^{7-a} = \phi^{-1}\left(x_8 - \phi(\sum_{i=0, i\neq a}^{7} 10^{7-i} \cdot x_i)\right)$$

  $$= \phi^{-1}(x_8) - \sum_{i=0, i\neq a}^{7} 10^{7-i} \cdot x_i$$

  Per exemple, anem a corregir l'esborrall produït a $1234567?S$:

  $$\sum_{i=0, i\neq 7}^{7} 10^{7-i} \cdot x_i + x_7 10^{7-7} = \phi^{-1}(S) = 15 \bmod 23$$

  O sigui, $x_7 10^{7-7} = 15 - \sum_{i=0, i\neq 7}^{7} 10^{7-i} \cdot x_i = 15 - 6 = 9 \bmod 23$.

  El NIF correcte és: $12345679S$.

5.4 Donat el codi binari i lineal que té per matriu generadora:

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

(a) codifiqueu la informació (1101);

(b) descodifiqueu les paraules rebudes següents: (1101010), (0110111), (0111000).

Resposta:

(a) Volem codificar la informació $v = (1101)$. Per fer això només hem de multiplicar el vector $v \cdot G$, on G és la matriu que ens donen a l'enunciat.

$$(1101) \cdot G = (1011101).$$

(b) Passem ara la matriu G a la forma $(Id|P)$ (mètode dels pivots o de Gauss).

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

permutem la segona i la cinquena columnes

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & \boxed{1} & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Volem descodificar els vectors següents: (1101010), (0111000) i (0011110). Per poder descodificar-los hem de trobar primer la matriu H; l'únic que hem de fer a partir de la matriu G sistemàtica és $(-P^\top|Id)$

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

Hem de desfer les permutacions de columnes realitzades a l'hora de passar la matriu G a sistemàtica. Hem permutat la segona columna amb la cinquena, així la H quedarà:

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

Observem que H té dues columnes iguals. Això vol dir que la distància mínima del codi serà $d = 2$, i no podem, en general, corregir cap error!

- Descodificació del vector (1101010):
  $H \cdot (1101010) = (001)$. Error a la setena columna, llavors el vector descodificat serà (1101011).
- Descodificació del vector (0111000):
  $H \cdot (0111000) = (100)$. Error a la segona o a la primera columnes. Llavors el vector descodificat serà (0011000) o (1111000) i la descodificació no serà única.
- Descodificació del vector (0011110):
  $H \cdot (0011110) = (111)$. Hi ha un error a la primera i tercera coordenades, o primera i quarta, o segona i tercera, o segona i quarta, o cinquena i sisena. La descodificació no és única i hem de decidir entre (1001110), (1010110), (0101110) o (0110110).

5.5 Sigui C el codi ternari de matriu generadora

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix},$$

(a) trobeu la matriu generadora del codi sitemàtic equivalent al donat;

(b) trobeu la matriu de control;

(c) useu la síndrome per descodificar els vectors rebuts, 2121, 1201, 2222.

Resposta:

A partir de la matriu generadora

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix},$$

permutant columnes (la primera amb la segona i, llavors, la segona amb la quarta) obtenim:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} = G',$$

on ara G' és la matriu generadora d'un codi sistemàtic.

Matriu de control del codi sistemàtic:

$$H' = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$$

Desfent les permutacions anteriors, obtindrem la matriu de control H del codi inicial:

$$\begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 2 & 1 & 2 \\ 1 & 2 & 0 & 1 \end{pmatrix} = H$$

Observem que el codi és sistemàtic i que la informació es recull en les coordenades 2 i 4 del vector tramès.

Observem, també, que el mínim grup de vectors dependents entre les columnes de la matriu H té cardinal 3. Llavors el codi és 1-corrector.

Descodifiquem els vectors rebuts:

- $H \cdot (2121) = (02) = 2 \cdot (01) \Longrightarrow$ S'ha produït un error (amb valor 2) a la primera columna.
  Així, doncs, el vector correcte serà (0121) i la informació, (11).
- $H \cdot (1201) = (00) \Longrightarrow$ No s'ha produït cap error.
  El vector correcte és (1201) i la informació (21).
- $H \cdot (2222) = (12) = 2 \cdot (21) \Longrightarrow$ S'ha produït un error (amb valor 2) a la quarta coordenada. El vector correcte és (2220) i la informació, (20).

5.6 Un codi ternari està generat per les paraules (00210) i (01002) i totes les combinacions lineals d'ambdues.

(a) Doneu-ne una matriu generadora i una matriu de control.

(b) Quina és la seva dimensió?

(c) Quina és la seva distància mínima?

(d) Quants errors es poden corregir?

(e) Quants esborralls es poden corregir?

(f) Quants errors es poden detectar?

(g) Com ha de ser un error per a poder-se corregir?

Resposta:

(a) Matriu generadora:

$$G = \begin{pmatrix} 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 2 \end{pmatrix}.$$

Permutant la primera i quarta columnes de G, obtenim

$$G' = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 \end{pmatrix}.$$

Una matriu ortogonal de G' és

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

Tornant a permutar les columnes primera i quarta de H', obtenim una matriu ortogonal de G:

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

(b) La seva dimensió és 2 perquè els dos vectors que generen el codi són independents.

(c) La distància mínima és $\delta = 2$ perquè és el mínim número de columnes dependents de la matriu H.

(d) No es pot corregir cap error ja que el número d'errors que es poden corregir és $\left\lfloor \frac{\delta - 1}{2} \right\rfloor = 0$.

(e) Es pot corregir $\delta - 1 = 1$ esborrall.

(f) Es pot detectar $\delta - 1 = 1$ error.

(g) Ha de ser a la primera coordenada.

5.7 Un codi binari té per matriu de control

$$H = (00001)$$

(a) Descriviu, a través d'alguna propietat, com són les paraules-codi.

(b) Quina és la dimensió del codi?

(c) Quina és la distància mínima del codi?

(d) Afegiu una nova fila a H i obtingueu una nova matriu de control H' de manera que el codi que tingui per matriu de control la matriu H' pugui detectar almenys un error.

(e) Doneu una matriu generadora del nou codi.

Resposta:

(a) Són les paraules tals que la seva última coordenada és 0.

(b) Si k és la dimensió del codi, la dimensió de la matriu H és $5 - k = 1$. Per tant, $k = 4$.

(c) La distància mínima del codi és 1, ja que existeixen columnes a H nul·les i, per tant, dependents. Observem, per exemple, que la paraula $v = (10000)$ pertany al codi i té pes 1.

(d) Perquè es pugui detectar un error, cal que la distància mínima del codi sigui almenys 2. Per tant, cal que totes les columnes de H' no siguin nul·les. Podem prendre

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

(e) Ara permutem les dues últimes columnes de H' i obtenim

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

Com que H'' és de la forma $(P \mid I)$ podem prendre com a matriu ortogonal de H'' la matriu $(I \mid -P^T)$:

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

Per obtenir la matriu generadora del nou codi, hem de tornar a permutar les dues darreres columnes:

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

5.8 Considerem el codi C definit sobre $\mathbb{F}_5$ format per les solucions del sistema

$$\begin{aligned} x_1 + 3x_2 + 2x_4 + 4x_5 &= 0 \\ x_2 + 3x_3 + x_4 + x_5 &= 0 \end{aligned}$$

(a) Quina és la seva dimensió?

(b) Quina és la seva distància mínima?

(c) Corregiu el missatge 1132321231.

Resposta:

(a) 3.

(b) 3

(c) 1132321031.

5.9 Sigui C el codi sobre F_2 amb matriu generadora

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

(a) Calculeu una matriu de control de C.

(b) Quins són els paràmetres d'aquest codi?

(c) Quants errors corregeix?

(d) Calculeu la síndrome de $v = (00111101)$.

(e) Corregiu v.

(f) Si hem emprat G per codificar, quin era la paraula transmesa?

(g) Quin era el missatge enviat?

Resposta:

(f) 01110101

(g) 01

5.10 Un codi sobre $\mathbb{F}_5$ té matriu generadora

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

(a) Doneu-ne una matriu de control.

(b) Quina és la distància mínima?

(c) Transmetem una paraula del codi per un canal on només es produeixen esborralls i rebem $(3\ ?\ 2\ ?\ 1)$. Quina és la paraula que s'ha enviat?

Resposta:

(a)
$$\begin{pmatrix} 4 & 3 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 4 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

(b) Com que les columnes de la matriu de control són linealment independents dues a dues i en podem trobar tres que són linealment dependents, deduïm que la distància mínima és 3.

(c) Suposem que la paraula enviada és $(3\ x\ 2\ y\ 1)$. Com que la seva síndrome ha de ser 0, tenim

$$\begin{aligned} 3x &= 1 \\ 2x + y &= 0 \\ x &= 2 \end{aligned}$$

D'on es dedueix que $x = 2$ i $y = 1$.

5.11 * Considerem el codi ternari C generat per la matriu

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$$

(a) Quantes paraules té aquest codi?

(b) Doneu totes les paraules del codi.

(c) Doneu la distància mínima del codi.

(d) Quina dimensió té el codi dual?

(e) Doneu dues paraules (no múltiples una de l'altra) del codi dual.

(f) Quina relació hi ha entre C i $C^{\perp}$?

(g) Trobeu una matriu de control del codi.

(h) Corregiu el missatge rebut 212112012222.

Resposta:

(a) La dimensió del codi és el nombre de files linealment independents de la matriu generadora, que és 2. Aleshores el codi té 9 paraules perquè té dimensió 2 i és sobre $\mathbb{Z}_3$.

(b) Les paraules s'obtenen multiplicant la matriu generadora per tots els possibles vectors de dues coordenades de $\mathbb{Z}_3$:

$$(00)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (0000) \quad (10)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (1110) \quad (20)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (2220)$$
$$(01)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (2011) \quad (11)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (0121) \quad (21)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (1201)$$
$$(02)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (1022) \quad (12)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (2102) \quad (22)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (0212)$$

(c) La distància mínima és 3 perquè totes les paraules, excepte la nul·la, tenen pes 3.

(d) El codi dual, com que està generat per la matriu de control, té com a dimensió el nombre de files de la matriu de control que és $n - k = 2$.

(e) Observem que les dues files de la matriu generadora, quan les multipliquem per la matriu generadora, ens donen 0. Per tant, podem donar les paraules 1110 i 2011.

(f) C i $C^\perp$ són iguals, ja que $C^\perp$ té dimensió 2 i, per tant, està generat per la mateixa matriu generadora de C.

(g) Com que C i $C^\perp$ són iguals, la mateixa matriu generadora és matriu de control.

(h) Podem corregir per síndrome o per observació de les paraules del codi. Com que la distància mínima és 3, només es pot corregir un error. Per cada bloc, si trobem una paraula del codi a distància 1 (o 0), aquesta és la paraula corregida. Així doncs, la seqüència corregida ens queda com 0121 1201 2220.

5.12 * (a) Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$.

(b) Doneu una taula exponencial-vectorial de $\mathbb{F}_4$.

(c) Diguem α a la classe de x dins de $\mathbb{F}_4$. Considerem el codi C amb matriu generadora

$$G = \begin{pmatrix} 1 & \alpha & \alpha & 1 \\ 0 & \alpha^2 & 0 & \alpha^2 \end{pmatrix}.$$

Codifiqueu la cadena de bits 011001001111 donant el resultat també en bits.

(d) Doneu una matriu de control del codi.

(e) Quina és la distància mínima del codi C?

(f) Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?

(g) Detecteu si hi ha errors en la cadena codificada de bits

$$011111010011001000000000.$$

(h) * En quina posició ha de ser un error per tal de poder-lo corregir?

Resposta:

(a) Els polinomis irreductibles de grau 2 de $\mathbb{Z}_2[x]$ seran aquells que no s'anul·lin a 0 (coef. constant 1) ni a 1 (nombre senar de termes no nuls). L'únic polinomi amb aquestes característiques és $x^2 + x + 1$.

(b)

0	00
1	10
α	01
α^2	11

(c) La cadena de bits representa la cadena de símbols $\alpha 1 \alpha 0 \alpha^2 \alpha^2$. Multipliquem cada parell de símbols per la matriu generadora:

$$\alpha 0 \alpha^2 1 \quad \alpha\alpha^2\alpha^2\alpha \quad \alpha^2\alpha^2 11$$

(d) La matriu generadora sistemàtica serà:

$$\begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Per tant, com a matriu de control podem prendre

$$\begin{pmatrix} \alpha & 0 & 1 & 0 \\ \alpha^2 & 1 & 0 & 1 \end{pmatrix}.$$

(e) Com que hi ha dues columnes iguals i no hi ha cap columna nul·la, la distància mínima és 2.

(f) No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.

(g) De les tres paraules codificades només té error la paraula del mig (multiplicada per la matriu de control dóna $\neq 0$).

5.13 Considerem el codi binari i lineal definit per les paraules codi:

$(a_1, a_2, a_3, a_4, a_5, a_1 + a_2 + a_4 + a_5, a_1 + a_3 + a_4 + a_5, a_1 + a_2 + a_3 + a_5, a_1 + a_2 + a_3 + a_4)$

(a) Doneu la matriu de control i la matriu generadora d'aquest codi. Trobeu els valors de n, k, d.

(b) Afegiu a la matriu de control trobada una columna desena i una nova equació, donada per:

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} = 0$$

Trobeu la nova matriu generadora. Quant val ara la nova distància mínima?

(c) Doneu les taules de descodificació via síndrome per aquest segon codi.

Resposta:

Com que hi ha nou coordenades, $n = 9$.

Hi ha cinc paràmetres independents; per tant, $k = 5$.

Matriu generadora $G = (Id|P)$:

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

Matriu de control $H = (-P^T|Id)$:

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

A la matriu de control H hi ha tres columnes linealment dependents (per exemple, la primera, la cinquena i la novena); per tant, la distància mínima d'aquest codi serà $d = 3$, i la capacitat correctora serà $c = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$.

Ampliem H amb una nova columna (i una nova fila) per tal d'afegir la nova equació:

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

De fet, aquesta nova equació proporciona al codi un control de paritat (paritat parella).

La nova matriu de control H' correspon a un codi $C(10, 5)$ i, per tant, la matriu generadora tindrà també deu columnes i cinc files i, en aquest nou codi, $n = 10$ i $k = 5$.

Observem que, a causa del control de paritat, ara $d = 4$, però la capacitat correctora encara és $c = 1$.

Per tal de trobar la nova matriu generadora G', passarem la matriu de control H' a una matriu sistemàtica sumant la primera fila amb tota la resta i realitzant després una sèrie de transposicions entre les columnes $6, 7, 8, 9$ i 10:

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

Trobem ara la matriu generadora d'aquest codi sistemàtic:

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

Desfem ara les anteriors transposicions de columnes per tal d'obtenir la matriu generadora del codi original:

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

Atès que la capacitat correctora d'aquest codi és $c = 1$, llavors obtenim a partir de H' la següent taula de descodificació via síndrome, on hem escrit només les síndromes que corresponen a "cosets"amb líder únic:

Vector d'error	$H(\overrightarrow{v})$
(0 0 0 0 0 0 0 0 0 0)	(0 0 0 0 0)
(1 0 0 0 0 0 0 0 0 0)	(1 1 1 1 1)
(0 1 0 0 0 0 0 0 0 0)	(1 1 0 1 1)
(0 0 1 0 0 0 0 0 0 0)	(1 0 1 1 1)
(0 0 0 1 0 0 0 0 0 0)	(1 1 1 0 1)
(0 0 0 0 1 0 0 0 0 0)	(1 1 1 1 0)
(0 0 0 0 0 1 0 0 0 0)	(1 1 0 0 0)
(0 0 0 0 0 0 1 0 0 0)	(1 0 1 0 0)
(0 0 0 0 0 0 0 1 0 0)	(1 0 0 1 0)
(0 0 0 0 0 0 0 0 1 0)	(1 0 0 0 1)
(0 0 0 0 0 0 0 0 0 1)	(1 0 0 0 0)

5.14 Construïu la taula estàndard del codi que té la matriu generadora següent:

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

(a) Descodifiqueu els vectors rebuts 11111 i 01011

(b) Doneu exemples d'una paraula en què hi hagi dos errors que siguin corregits en descodificar-la, i d'una altra en què hi hagi dos errors que no siguin corregits en descodificar-la.

(c) Suposeu que el canal és binari i simètric amb probabilitat d'error al bit de l'1 per mil. Calculeu la probabilitat de detectar errors, és a dir, que la paraula rebuda no sigui igual que la paraula enviada i que ens n'adonem.

Resposta:

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

Aquest codi té paràmetres $n = 5$, $k = 2$ i $d = 3$. Construïm la taula estàndard:

	00	01	10	11
00000	00000	01011	10110	11101
10000	10000	11011	00110	01101
01000	01000	00011	11110	10101
00100	00100	01111	10010	11001
00010	00010	01001	10100	11111
00001	00001	01010	10111	11100
11000	11000	10011	01110	00101
10001	10001	11010	00111	01100
01100	01100	00111	11010	10001
⋮	⋮	⋮	⋮	⋮

(a) Per descodificar els vectors rebuts, els busquem a la taula estàndard i mirem a quina columna d'error pertanyen:

El primer vector rebut és 11111. El trobem a la fila amb l'error 00010. Llavors, si restem l'error de la paraula rebuda, traurem els errors: $11111 -$

$00010 = 11101$. El codi és sistemàtic. Per tant, el vector descodificat seran les dues primeres posicions del vector, o sigui 11.

El segon vector rebut és 01011. El trobem a la fila amb error 00000. Per tant, no hi ha errors i descodifiquem per 01.

(b) Si es produeixen dos errors, pot passar que $\overline{e}$ sigui el líder de la seva classe o no. $\overline{e} = (11000)$ el corregirem i, en canvi, $\overline{e} = (00101)$ no el corregirem bé, ja que a la taula estàndard n'hem agafat com a líder de la seva classe només un.

Si rebem la paraula 01110 i mirem la taula estàndard, veurem que la trobem a la fila amb l'error 11000 i descodificarem correctament.

En canvi, si codifiquem la paraula 01 (obtenim 01011) i afegim el vector d'error 10100, rebem la paraula 11111. Si descodifiquem, trobarem aquesta paraula a la fila amb error 00010, i descodificarem errròniament per 11.

(c) En el codi hi ha un vector de pes 0, dos de pes 3 i un de pes 4. Detectarem errors si el vector d'error és qualsevol cosa menys un d'ells: $p_{det} = 1 - 2p^3(1-p)^2 - p^4(1-p) = -2 \cdot 0.001^3 \cdot 0.999^2 - 0.001^4 \cdot 0.999 \approx 1$.

5.15 Donat un codi ternari lineal $C(5,2)$ que té per matriu generadora:

$$G = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & a & 2 \end{pmatrix}$$

(a) Calcula el valor de a de manera que el codi tingui la màxima capacitat correctora.

(b) Calcula el valor de a pel qual es compleixi que el vector $v = (2,1,1,1,1)$ sigui una paraula-codi.

(c) Fes la taula de síndromes per poder portar a terme una descodificació incompleta i digues, pels diferents valors de a, quina és la informació associada al vector rebut $w = (10212)$.

Resposta:

El codi donat és sistemàtic i, per tant, la matriu de control és fàcil d'escriure:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & -a & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(a) Per $a = 0$, hi ha dues columnes a la matriu H linealment dependents. La distància mínima del codi és 2 i la capacitat correctora val zero.

Per $a = 1$ i $a = 2$, hi ha tres columnes a la matriu H linealment dependents. La distància mínima del codi és 3 i la capacitat correctora val 1.

(b) El vector $v = (2,1,1,1,1)$ pertanyerà al codi si la seva síndrome val zero: $H(v) = 0 \Rightarrow a = 1$

(c) Per $a = 0$, no hi ha taula de síndromes, ja que el codi no corregeix cap error.

Per $a = 1$ i $a = 2$, les taules de síndromes (descodificació incompleta) són:

error	**síndrome**	
	$a=1$	$a=2$
00000	000	000
00001	001	001
00010	010	010
00100	100	100
01000	021	011
10000	102	102

La síndrome del vector rebut val: $H(v) = H(10212) = 011$.

Per $a = 1$, no podem descodificar el vector rebut, però per $a = 2$, segons la taula de síndromes, decidim que s'ha comès l'error 01000 i, per tant, el vector enviat és: $v = w - (01000) = (10212) - (01000) = (12212)$.

La informació enviada és (12), ja que el codi era sistemàtic en les dues primeres coordenades.

5.16 Considerem el codi lineal $(10, 8)$ sobre $\mathbb{F}_{11}$, definit a partir de la seva matriu de control:

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

Diguem C al codi format a partir del codi anterior ometent totes les paraules en què alguna coordenada valgui 10.

(a) Demostreu que la distància mínima d'aquest codi és 3.

(b) Descriviu un algorisme de descodificació incompleta, que no usi taules, que sigui capaç de corregir qualsevol error simple.

(c) Descodifiqueu el vector rebut 0617960587.

Resposta:

Tenim el codi lineal $(10, 8)$ sobre $\mathbb{F}_{11}$ amb una matriu de control:

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

Anomenem C el codi anterior eliminant les paraules en què alguna coordenada val 10.

(a) La distància mínima és, efectivament, 3, ja que, si multipliquem la primera columna per 6 i li sumem la segona també per 6, obtenim la setena columna. Llavors 3 és el mínim nombre de columnes dependents de la matriu H (no hi ha la columna tot zeros ni cap columna múltipla d'una altra).

(b) Per fer això, utilitzarem la definició de síndrome: sabem que, si $\overrightarrow{v} \in C$, llavors $H \cdot \overrightarrow{v} = \overrightarrow{0}$. Per a la construcció del codi sabem:

$$\sum v_i = 0 \quad mod\ 11$$

$$\sum i \cdot v_i = 0 \quad mod\ 11.$$

Si ens arriba una paraula $\overrightarrow{w} = \overrightarrow{v} + \overrightarrow{e}$, amb un error simple $e = (0, 0, \ldots, 1, 0, \ldots, 0)$, obtenim l'error

$$\sum w_i = \sum v_i + e_k \Rightarrow e_k = \sum w_i \mod 11,$$

i la seva posició:

$$\sum i \cdot w_i = \sum i \cdot v_i + k \cdot e_k$$

$$k \cdot e_k = \sum i \cdot w_i$$

(c) Descodifiquem $w = 0617960587$:

$$\sum w_i = 5 \Rightarrow e_i = 5;$$

$$\sum i \cdot w_i = 9 \Rightarrow i = \frac{\sum i \cdot w_i}{e_i} = \frac{9}{5} = \frac{2}{6} = 4.$$

Ara sabem que l'error és 5 a la posició 4. Corregim l'error, i trobem $v = 0612960587$. Calculant la síndrome veiem que dóna zero; per tant, aquest altre vector sí que pertany al codi.

5.17 Sigui C un codi lineal i binari de matriu generadora:

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

Demostreu que C és descodificable de manera única (és a dir, per a cada paraula rebuda w, existeix una única paraula codi, v, tal que $d(w, v)$ sigui mínima).

Resposta:

Descodificar $v \in C$ de manera única vol dir que $\forall \omega, \exists\, !\ \ v$ tal que $d(v, \omega)$ és mínima.

Si $d(v, \omega)$ mínima $\Rightarrow$ pes$(v - \omega)$ mínim $= d(v - \omega, 0)$ sigui mínima.

Trobem la matriu H de la manera habitual.

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

Si observem la matriu H, podem fer una reordenació en les seves columnes i posar la primera a la columna vuitena, i la sisena i la setena a les posicions novena i desena, respectivament; així, ens quedarà :

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & H_2 \\ H_1 & 0 \end{pmatrix}$$

La nova matriu H reordenada està formada per dues caixes de zeros i dues caixes més H_1 i H_2. H_1 és una caixa formada per tres files i set columnes, amb la matriu identitat inclosa. H_1 és la matriu de control d'un codi binari de Hamming C_1, amb $t = 3$. La caixa H_2 és una matriu amb dues files i tres columnes, és la matriu de control d'un codi binari de Hamming C_2, amb $t = 2$.

Per a tot $w \in F^{10}$, existeixen $a \in F^7$, $b \in F^3$ tals que $w = a + b$.

A partir de $a \in F^7$, podem assegurar l'existència d'una única paraula $a' \in C_1$ a distància mínima de a: $d(a, a') \leqslant 1$.

A partir de $b \in F^3$, podem assegurar l'existència d'una única paraula $b' \in C_2$ a distància mínima de b: $d(b, b') \leqslant 1$.

Fem $v = a' + b'$. Tenim $v \in C$, $d(v, w) \leqslant 2$ i $v \in C$ és l'única paraula que està a distància mínima de w.

5.18 Suposem un cert canal binari que accepta paraules de longitud 7 i que només produeix errors d'un cert tipus.

L'error del canal és additiu i el vector d'error és un dels següents:

0000000, 0000001, 0000011, 0000111, 0001111, 0011111, 0111111, 1111111.

Dissenyeu un codi binari lineal $(7, k)$ que sigui capaç de corregir aquests tipus d'errors i feu per manera que el codi cercat tingui la més alta possible taxa de transmissió.

Resposta:

Suposant que el canal és binari i l'error és additiu, hem de construir un codi que sigui capaç de detectar els vectors d'error següents:

(0000000),(0000001),(0000011),(0000111)
(0001111),(0011111),(0111111),(1111111)

Aprofitant que aquests vectors d'error tenen un format definit (a partir d'una posició, tots 1), hem de construir una matriu de control amb una taula de síndromes associada, amb les quals es pugui reconèixer el vector d'error que ha afectat la paraula codi transmesa.

Per poder reconèixer el vector d'error, haurem de crear una taula de síndromes en què cada error estigui en una classe diferent. Com que hi ha vuit vectors d'error diferents, necessitarem vuit classes, com a mínim.

Per fer que la taxa de transmissió $R = \dfrac{k}{n}$ sigui màxima, k haurà de ser com més gran millor. La matriu de control retornarà 2^{n-k} valors diferents i, com que

necessitem diferenciar vuit (2^3) vectors d'error i $n = 7$, obtenim que $2^{7-k} \geq 2^3$ i, per tant, $k \leq 4$.

Per tal d'aconseguir, doncs, una taxa de transmissió R com més alta millor, la matriu de control H hauria de tenir només $n - k = 7 - 4 = 3$ files.

Per poder controlar i diferenciar els diferents vectors d'error, podríem construir un sistema de paritat entre les diferents coordenades de les paraules codi, de forma que una sèrie de coordenades de cada paraula codi hauria de tenir sempre el mateix valor.

Per exemple, podríem utilitzar paraules codi amb el format:

$$\overrightarrow{v} = (\text{a b a 0 a b a}),$$

on, en funció dels valors de a i de b, podríem formar les quatre paraules codi següents:

a	b	paraula codi
0	0	(0 0 0 0 0 0 0)
0	1	(0 1 0 0 0 1 0)
1	0	(1 0 1 0 1 0 1)
1	1	(1 1 1 0 1 1 1)

.

Observem que la quarta coordenada de cada paraula codi sempre ha de tenir valor zero, per tal de poder reconèixer el vector d'error (1111111), el qual, a causa de la seva simetria, no es detectaria amb els controls de paritat.

La matriu de control H, doncs, serà:

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

La taula síndrome associada a aquest codi serà:

Vector d'error	$H(\overrightarrow{v})$
(0 0 0 0 0 0 0)	(0 0 0)
(0 0 0 0 0 0 1)	(0 0 1)
(0 0 0 0 0 1 1)	(0 1 1)
(0 0 0 0 1 1 1)	(0 1 0)
(0 0 0 1 1 1 1)	(1 1 0)
(0 0 1 1 1 1 1)	(1 1 1)
(0 1 1 1 1 1 1)	(1 0 1)
(1 1 1 1 1 1 1)	(1 0 0)

5.19 Tenim la possibilitat d'utilitzar un codi de Hamming sobre $\mathbb{F}_{3^2}$. El canal de comunicacions sobre el qual circularà la informació és ternari i no s'hi produeixen errors, només esborralls. Els esborralls es produeixen sempre en ràfegues de tres.

Analitzeu el problema (prestacions, paràmetres, taxes, etc.) i decidiu quin és el millor paràmetre t a utilitzar, si entre dues ràfegues observem que, com a mínim, sempre hi ha

(a) 20 dígits correctes;

(b) 100 dígits correctes.

Resposta:

Utilitzarem un codi de Hamming sobre $\mathbb{F}_{3^2}$ sobre un canal ternari sense errors, només esborralls, sempre en ràfegues de 3.

$$n = \frac{q^t - 1}{q - 1} = \frac{9^t - 1}{8}$$
$$\mathbb{F}_{3^2} = \mathbb{Z}_3[x]/x^2 + x + 2.$$

Abans de començar a resoldre el problema, construïm el cos finit $\mathbb{F}_{3^2} = \mathbb{Z}_3[x]/x^2 + x + 2$.

- En forma polinòmica: $\mathbb{F}_{3^2} = \{0, 1, 2, x, 1 + x, 2 + x, 2x, 1 + 2x, 2 + 2x\}$.

- En forma vectorial:
  $\mathbb{F}_{3^2} = \{(00), (10), (20), (01), (11), (21), (02), (12), (22)\}$.

- En forma potencial:
  $\alpha^2 = 2\alpha + 1$
  $\alpha^3 = 2\alpha^2 + \alpha = 2\alpha + 2$
  $\alpha^4 = 2\alpha^2 + 2\alpha = 2$
  $\alpha^5 = 2\alpha$
  $\alpha^6 = 2\alpha^2 = \alpha + 2$
  $\alpha^7 = \alpha^2 + 2\alpha = 1 + \alpha$
  $\alpha^8 = \alpha^2 + \alpha = 1$.

  $$\mathbb{F}_{3^2} = \{\alpha^{-\infty}, \alpha^8, \alpha^4, \alpha, \alpha^7, \alpha^6, \alpha^5, \alpha^2, \alpha^3\}.$$

  Sabem que els codis de Hamming són 1-correctors i $d = 3$. $2t + \delta < d \Rightarrow \delta = 0$, $t = 1$ o bé $\delta = 2$, $t = 0$. Podem corregir dos esborralls cada n elements de $\mathbb{F}_{3^2}$ que circulin pel canal.

  En tenir un codi ternari, els elements de $\mathbb{F}_{3^2}$ estan formats per dos dígits ternaris.

- Ràfegues de tres esborralls cada vint dígits correctes:
  Hem de calcular la t més adient per utilitzar un codi en aquest cas.
  Sabem que la taxa de transmissió és de

$$R = \frac{k}{n} = \frac{n-t}{n} = 1 - \frac{t}{n} \text{ i } n = \frac{q^t - 1}{q-1} = \frac{9^t - 1}{8}.$$

Per a $t = 1$, tenim $n = 1, k = 0, R = 0$.

Per a $t = 2 \Rightarrow n = 10, k = 8, R = \frac{4}{5} = 0.8$. Podem corregir quatre esborralls de $\mathbb{Z}_3$ cada bloc de vint dígits ternaris.

Per a $t = 3 \Rightarrow n = 91, k = 88, R = \frac{88}{91} > 0.8$. Podem corregir quatre esborralls de $\mathbb{Z}_3$ cada bloc de cent vuitanta-dos dígits ternaris.

El primer cas no té cap interès. El segon cas resol el nostre problema i, per a $t > 2$, ja no podem resoldre'l.

La solució és, doncs, $t = 2$.

- En el cas de les ràfegues cada cent dígits correctes, el raonament a fer és el mateix que abans, i la conclusió és, també, $t = 2$, ja que per a valors més grans de t no podem corregir tots els esborralls que es presentin.

5.20 Anomenem $\alpha \in \mathbb{F}_{2^4}$ un element primitiu.

(a) Resoleu el sistema d'equacions següent:

$$\begin{array}{rcl} x + y + z & = & 1 \\ \alpha x + y + \alpha z & = & 0 \\ x + \alpha z & = & \alpha^2 \end{array}$$

(b) Trobeu l'invers de l'element $(1001) \in \mathbb{F}_{2^4}$

(c) S'utilitza el codi de Hamming sobre $\mathbb{F}_2$, de paràmetre $t = 4$, per transmetre informació binària, sobre un canal binari.

A la sortida del canal, rebem $011\,011\,011\,011\,011\,011\,011\,\ldots$.

Seleccioneu el primer bloc rebut, descodifiqueu-lo corregint errors, si en trobeu, i doneu-ne la informació associada corresponent.

Resposta:

Abans de resoldre el sistema, hem de construir $\mathbb{F}_{2^4}$. Agafem $x^4 + x^3 + 1$, que és un polinomi irreductible de $\mathbb{Z}_2[x]$, i fem $\mathbb{F}_{2^4} = \mathbb{Z}_2[x]/x^4 + x^3 + 1$.

$\alpha^4 = \alpha^3 + 1$
$\alpha^5 = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$
$\alpha^6 = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^7 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1$
$\alpha^8 = \alpha^3 + \alpha^2 + \alpha$
$\alpha^9 = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^2 + 1$
$\alpha^{10} = \alpha^3 + \alpha$
$\alpha^{11} = \alpha^4 + \alpha^2 = \alpha^3 + \alpha^2 + 1$
$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha = \alpha + 1$
$\alpha^{13} = \alpha^2 + \alpha$
$\alpha^{14} = \alpha^3 + \alpha^2$
$\alpha^{15} = \alpha^4 + \alpha^3 = 1$

0	α	α^2	α^3	α^4	α^5	α^6	α^7
(0000)	(0100)	(0010)	(0001)	(1001)	(1101)	(1111)	(1110)
α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}
(0111)	(1010)	(0101)	(1011)	(1100)	(0110)	(0011)	(1000)

La matriu del sistema proposat és:

$$\begin{pmatrix} 1 & 1 & 1 \\ \alpha & 1 & \alpha \\ 1 & 0 & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \alpha^2 \end{pmatrix}$$

(a) Calculem el determinant:

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha & 1 & \alpha \\ 1 & 0 & \alpha \end{vmatrix} = \alpha^9.$$

El sistema és de Cramer i les solucions són:

$$x = \frac{\begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & \alpha \\ \alpha^2 & 0 & \alpha \end{vmatrix}}{\alpha^9} = \frac{\alpha + \alpha^3 + \alpha^2}{\alpha^9} = \frac{\alpha^8}{\alpha^9} = \alpha^{-1} = \alpha^{14},$$

$$y = \frac{\begin{vmatrix} 1 & 1 & 1 \\ \alpha & 0 & \alpha \\ 1 & \alpha^2 & \alpha \end{vmatrix}}{\alpha^9} = \frac{\alpha^3 + \alpha + \alpha^3 + \alpha^2}{\alpha^9} = \frac{\alpha^{13}}{\alpha^9} = \alpha^4,$$

$$z = \frac{\begin{vmatrix} 1 & 1 & 1 \\ \alpha & 1 & 0 \\ 1 & 0 & \alpha^2 \end{vmatrix}}{\alpha^9} = \frac{\alpha^2 + 1 + \alpha^3}{\alpha^9} = \frac{\alpha^{11}}{\alpha^9} = \alpha^2.$$

(b) Calculem l'invers de 1001:

El passem a forma potencial, ja que és més fàcil fer l'invers d'aquesta manera.

$$1001 = 1 + \alpha^3 = \alpha^4$$
$$\alpha^4 \alpha^x = 1 = \alpha^{15} \Rightarrow x = 11.$$

Aleshores, l'invers de (1001) és (1011).

(c) Utilitzarem ara el codi de Hamming sobre $\mathbb{F}_2$, de paràmetre $t = 4$, en un canal binari.

Escriurem la matriu H, que té per dimensions n i k, amb els valors següents:

$n = \dfrac{q^t - 1}{q - 1} = \dfrac{2^4 - 1}{2 - 1} = 15$; $k = n - t = 11$.

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

Rebem la paraula codi següent i la partim en blocs de 15 bits, ja que $n = 15$:

$$\underbrace{011011011011011}_{v1}\underbrace{0110110\cdots}_{v2}.$$

El primer bloc rebut és v_1 i, per descodificar-lo, calculem la seva síndrome: $H \cdot (v1) = (0001)$. O sigui, hi ha un error a la quarta coordenada.

$$e = (000100000000000)$$

La paraula corregida serà:

$$v_1 - e = (011011011011011) - (000100000000000) = (011111011011011).$$

La informació associada correspon a les onze últimes coordenades, ja que la matriu generadora té la matriu identitat en les onze últimes posicions. El vector d'informació demanat és:

$$(11011011011).$$

5.21 Demostreu que, en un codi binari lineal, o bé totes les paraules-codi tenen un **0** a la primera coordenada, o bé la meitat tenen un **0** i l'altra meitat un **1**.

Resposta:

Un codi lineal binari té totes les paraules-codi generades linealment a partir d'una colla de vectors (les files de la matriu generadora) que formen base de l'espai vectorial, que és el codi.

Si tots els vectors que formen base tenen un zero a la primera coordenada, resultarà que tots els vectors del codi tindran un zero a la primera coordenada, ja que els obtindrem fent combinacions lineals d'aquells.

Si algun vector de la matriu generadora, diguem-li v_1, té un **1** a la primera coordenada, podem obtenir una altra base fent operacions agafant com a pivot la primera coordenada del vector v_1. Això ens porta a una altra base del codi en la qual tots els vectors, v_2, v_3, ..., v_k, tenen un zero a la primera coordenada, menys el vector v_1, que hi té un **1**. Els vectors del codi són totes les possibles combinacions lineals de v_1, v_2, ..., v_n i, per tant, en la meitat figurarà el vector v_1 (i les paraules-codi corresponents tindran un **1** a la primera coordenada) i en l'altra meitat no figurarà el vector v_1 (i les paraules-codi corresponents tindran un **0** a la primera coordenada).

5.22 Si C és un codi de longitud n sobre un alfabet binari, definim el codi estès C' com:

$$C' = \{(c_1, c_2, ..., c_n, c_{n+1})/(c_1, c_2, ..., c_n) \in C, \sum c_i = 0\}$$

Si C és un codi lineal de matriu generadora G i matriu de control H, trobeu, en funció d'aquestes, la matriu generadora i de control del codi C'. Si C té distància mínima $2e + 1$, trobeu la distància mínima de C'.

Anomenem $A(z)$ l'enumerador de pesos del codi C. Quin és l'enumerador de pesos del codi estès C'?

Resposta:

- Tenim un codi $C(n,k)$ sobre $\mathbb{F}_2$. Definim el codi estès C' com:

$$C' = \{(\underbrace{c_1, c_2, c_3, \cdots c_n}_{\in C}, c_{n+1} | \sum_{i=1}^{n+1} c_i = 0\}.$$

  Si tenim la matriu generadora G de $n \times k$ i la matriu de control H de $n \times n-k$, les matrius G' ' H' seran:

  G' tindrà k files i $n+1$ columnes. Aquesta columna afegida serà $c_{n+1} = -\sum_{i=1}^{n} c_i$.

  A H' hi afegirem una fila al davant tota plena d'uns i una columna de zeros al final. Això ens donarà unes dimenisons de $(n+1) \times (n-k+1)$.

- La distància mínima de C és $\delta = 2 \cdot e + 1$, que consisteix en la mínima quantitat de columnes dependents de H. Mirem les variacions de la matriu H: hem afegit una fila, que fa independents les δ columnes dependents de H. Per tant, la distància mínima a C' serà: $\delta' = \delta + 1$

- Sigui $A(z) = A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n$ l'enumerador de pesos del codi C i

  $\bar{A}(z) = \bar{A_0} + \bar{A_1} z + \cdots \bar{A_n} z^n + \bar{A_{n+1}} z^{n+1}$ l'enumerador de pesos del codi C'.

  Sabem que $\bar{A_i} = 0$ si i és senar. Els elements de per $2r$ a C continuen amb pes $2r$. Els que a C tenien pes $2r+1$ ara es converteixen en elements de pes $2r+2$.

  Llavors:

$$\bar{A_{2r}} = A_{2r} + A_{2r-1}$$

$$\bar{A}(z) = A_0 + A_2 z^2 + A_4 z^4 + \cdots + z(A_1 z + A_3 z^3 + A_5 z^5 + \cdots) =$$

$$= \frac{A(z) + A(-z)}{2} + z\frac{A(z) - A(-z)}{2} =$$

$$= \frac{(1+z)A(z) + (1-z)A(-z)}{2}.$$

5.23 Sigui $C(2k+1, k)$ un codi lineal i binari tal que $C \subset C^{\perp}$.

Descriviu el codi $C^{\perp}$.

Resposta:

Sabem que $dim(C^{\perp}) = n - dim(C) = 2k + 1 - k = k + 1$.

Sabem que $C \subset C^{\perp}$ i, per tant, podem concloure que $C^{\perp}/C$ és un espai vectorial de dimensió 1.

Sabem que per a tots els elements $c \in C$ és $c \cdot c = 0$, o sigui que el pes de tots els elements $c \in C$ és parell. Si fem $J = (1, 1, 1, \ldots, 1)$, podem escriure aquesta última propietat com $c \cdot J = 0$, que ens assegura que $J \in C^{\perp}$. També podem observar que $J \notin C$, ja que el seu pes no és parell.

La conclusió de totes aquestes observacions és que:

$$C^{\perp} = C \oplus \langle J \rangle.$$

5.24 Sigui $C(n,k)$ un codi lineal i binari. Si C té una paraula codi de pes imparell, llavors les paraules codi de pes parell formen un altre codi de tipus $(n, k-1)$.

Resposta:

Sigui $C(n,k)$ un codi lineal i binari amb una paraula de pes senar.

Per ser un codi lineal, ha de complir-se

$$c = \sum_{i=1}^{k} \lambda_i \cdot V_i,$$

on les λ_i són elements de $\mathbb{F}_2$ i els V_i són els vectors del codi que formen la matriu generadora G.

Farem que un d'aquests V_i (per exemple, V_k) sigui una paraula codi de pes senar, i la resta $V_1, V_2, \cdots, V_{k-1}$ siguin paraules codi de pes parell.

Això sempre serà possible fer-ho, ja que si alguna V_j amb $i \neq j$ fos també de pes senar, una combinació lineal de V_k amb V_j ens donaria una paraula codi de pes parell. Així, doncs, podem considerar una base del codi amb una única paraula codi de pes senar i totes les altres de pes parell.

Aleshores, un vector del codi amb $\lambda_k = 0$ serà de pes parell i, si $\lambda_k = 1$, serà de pes senar.

Per tant, de les 2^k combinacions (paraules codi) possibles, només la meitat (2^{k-1}) són de pes parell, i l'altra meitat, de pes senar.

Aleshores, agafant G' amb $V_1, V_2, \cdots, V_{k-1}$ (amb dimensió $k-1$) generarem totes aquestes paraules de pes parell, que pertanyeran al codi $C'(n, k-1)$.

5.25 Sigui $C(n,k)$ un codi lineal sobre $\mathbb{F}_q$, amb matriu generadora G. Si G no té cap columna tot zeros, llavors la suma de tots els pesos de totes les paraules codi és: $n \cdot (q-1) \cdot q^{k-1}$.

Resposta:

Ens demanen calcular la suma dels pesos de totes les paraules codi. Posem totes les paraules del codi en columna, una a sota de l'altra, i sumem coordenada a coordenada (sumem la primera coordenada de cada paraula, després la segona, i així successivament fins a arribar a la coordenada n).

El total de pesos aportat per la primera coordenada és $q^k - q^{k-1} = q^{k-1}(q-1)$, ja que hi ha tots els possibles vectors que es poden fer amb totes les combinacions lineals possibles entre els vectors de la matriu generadora, que la podíem haver simplificat agafant un "pivot"a la primera fila, primera columna.

Totes les coordenades aporten el mateix pes total.

Finalment, doncs, el resultat serà:

$$n \cdot (q-1) \cdot q^{k-1}.$$

Capítol 6
Problemes de codis cíclics

6.1 Creieu que és cíclic el codi del problema 5.9?

6.2 * (a) Demostreu que $g = x^4 + 4x^3 + 6x + 3$ genera un codi cíclic primitiu sobre $\mathbb{F}_7 = \mathbb{Z}_7$.

(b) Quina longitud i quina dimensió té aquest codi?

(c) Doneu-ne una matriu generadora.

(d) Es pot deduir la distància mínima a partir de la matriu generadora?

(e) Corregiu la paraula següent amb esborralls: $(???235)$.

(f) Comproveu si la paraula obtinguda en l'apartat anterior pertany al codi utilitzant el polinomi de control.

(g) Codifiqueu de forma sistemàtica la informació (11) utilitzant el polinomi generador.

Resposta:

(a) Cal demostrar que g divideix $x^6 - 1$. I, en efecte, $(x^6 - 1)/g = x^2 + 3x + 2$.

(b) $n = 6$, $k = 2$.

(c) $G = \begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix}$

(d) Les paraules del codi seran combinacions lineals de les dues files de G. Observem que totes dues files tenen pes 4 i que qualsevol combinació lineal d'ambdues tindrà com a mínim quatre components no nul·les.

(e) (542235)

(f) $(5 + 4x + 2x^2 + 2x^3 + 3x^4 + 5x^5)(x^2 + 3x + 2) = 5x^7 + 4x^6 + 2x + 3$. Si ara dividim $5x^7 + 4x^6 + 2x + 3$ entre $x^6 - 1$ ens dóna quocient $5x + 4$ i residu 0.

(g) El residu de dividir $i(x)x^{n-k} = x^4 + x^5$ entre g és $R(x) = 5x^3 + x^2 + x + 2$. Aleshores $x(x)x^{n-k} - R(x)$ correspon a la paraula codi 566211.

6.3 Suposem que tenim un codi sobre $\mathbb{F}_{11}$ cíclic de longitud 12 i dimensió 7. La codificació sistemàtica en les darreres posicions d'un vector d'informació i és

$$10\ 1\ 10\ 0\ 1\ 10\ 0\ 2\ 8\ 3\ 9\ 1.$$

Doneu la codificació sistemàtica en les primeres posicions del mateix vector d'informació. Justifiqueu la resposta.

6.4 Sigui $\alpha = [x]$ a $\mathbb{F} = \mathbb{F}_{3^2} = \mathbb{Z}_3[x]/x^2 + 2x + 2$. Sigui C un codi cíclic ternari primitiu de polinomi generador $g(x)$.

(a) Construïu el polinomi $g(x) \in \mathbb{Z}_3[x]$ de manera que es pugui assegurar que té coeficients al cos $\mathbb{Z}_3$ i, com a mínim, les arrels α i α^2.

(b) Doneu la longitud, dimensió i capacitat correctora de C.

(c) Construïu per tres procediments diferents (via matriu generadora, via polinomi de control i via arrels de $g(x)$) una matriu de control del codi C.

Resposta:

(a) $g(x) = m_\alpha(x)m_{\alpha^2}(x) = x^4 + 2x^3 + 2x + 2$.

(b) $n = 8, k = 4$. $d \geqslant 4$ perquè el polinomi generador té 3 arrels consecutives. $d \leqslant 4$ perquè la paraula corresponent a $g(x)$ té pes 3. Capacitat correctora $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{4-1}{2} \rfloor = 1$.

(c) En primer lloc, $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 2 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 \end{pmatrix}$

d'on $H_1 = \begin{pmatrix} 1 & 1 & 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 2 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$.

En segon lloc, $h(x) = \frac{x^8+2}{g(x)} = x^4 + x^3 + x^2 + 2x + 1$,

d'on $H_2 = \begin{pmatrix} 1 & 1 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 \end{pmatrix}$.

En tercer lloc,

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \\ 1 & \alpha^6 & \alpha^4 & \alpha^2 & 1 & \alpha^6 & \alpha^4 & \alpha^2 \end{pmatrix} \approx \left(\begin{array}{cccccccc} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ \hline 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \\ \hline \cancel{1} & \cancel{1} & \cancel{2} & \cancel{0} & \cancel{2} & \cancel{2} & \cancel{1} & \cancel{0} \\ \cancel{0} & \cancel{2} & \cancel{2} & \cancel{1} & \cancel{0} & \cancel{1} & \cancel{1} & \cancel{2} \\ \hline \cancel{1} & \cancel{2} & \cancel{2} & \cancel{1} & \cancel{1} & \cancel{2} & \cancel{2} & \cancel{1} \\ \cancel{0} & \cancel{2} & \cancel{0} & \cancel{1} & \cancel{0} & \cancel{2} & \cancel{0} & \cancel{1} \end{array}\right. \begin{array}{l} \\ \\ \\ \\ (f_1 + f_2) \\ (2f_2) \\ \\ (f_3 + f_4) \\ (2f_4) \end{array} \approx$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \end{pmatrix} = H_3.$$

6.5 Sigui α 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 α i també sobre α^{-1}.

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

Resposta:

Si $g(x)$ té com a arrels α i α^{-1}, també tindrà com a arrels α^2, α^{-2}, $\alpha^4 \cdots$.

Construïm un nou codi amb $g'(x) = g(x) \cdot (x - \alpha^0)$. Aquest nou codi té dimensió una menys que l'original; per tant, a la matriu de control hi trobarem el mateix nombre de columnes i una fila més que al codi inicial. També veiem que el polinomi generador tindrà les mateixes arrels que $g(x)$ i, a més, α^0; tot plegat ens dóna cinc arrels consecutives. Aquest nou codi té, doncs, distància mínima prevista $d' = 6$ i, com que la matriu de control té exactament una fila més que l'original, podem concloure que la distància mínima prevista del codi original és $d \geqslant 5$ (tingueu en compte la relació entre la distància mínima i el mínim grup de columnes dependents de la matriu de control).

6.6 Sobre $\mathbb{F}_2$ considerem la matriu

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

(a) Demostreu que el codi generat per G és cíclic.

(b) Trobeu els polinomis generador i de control.

(c) Trobeu una matriu de control de dues maneres diferents.

(d) Quina és la distància mínima?

(e) Codifiqueu de manera sistemàtica la informació 10110 utilitzant divisió de polinomis.

Resposta:

(b) $x^3 + x^2 + x + 1$ i $x^5 + x^4 + x + 1$.

(d) La distància mínima és 2 perquè hi ha dues columnes dependents a la matriu de control.

(e) 10010110.

6.7 (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 $\mathbb{F}_q$?

Resposta:

Sabem que els elements de K_q, un cos finit, són les solucions de l'equació

$$x^q - x = 0.$$

O bé

$$(x^q - x) = \prod_{\alpha \in K_q} (x - \alpha).$$

Els elements de $\mathbb{F}_{2^3}$ són aquells que $x^8 - x = x^{2^3} - x = 0$.

D'altra banda, també sabem que $x^{p^n} - x$ és el producte de tots els polinomis irreductibles a coeficients a $\mathbb{F}_p$ de grau $k|n$.

Podem descompondre $x^8 - x = x^{2^3} - x$ en polinomis de grau 1 i 3.

És a dir, $x^7 - 1$ es pot descompondre en tres polinomis irreductibles.

$$x^7 - 1 = (x-1) \cdot (x^3 + x^2 + 1) \cdot (x^3 + x + 1)$$

Els codis cíclics binaris de longitud 7 corresponen a codis de polinomi generador un divisor de $x^7 - 1$.

A banda dels trivials $g(x) = 1$, $g(x) = x^7 - 1$, podem trobar tots aquests polinomis divisors de $x^7 - 1$:

$$\begin{array}{rcl} g(x) & = & (x-1) \\ g(x) & = & (x^3 + x^2 + 1) \\ g(x) & = & (x^3 + x + 1) \\ g(x) & = & (x-1) \cdot (x^3 + x^2 + 1) \\ g(x) & = & (x-1) \cdot (x^3 + x + 1) \\ g(x) & = & (x^3 + x^2 + 1) \cdot (x^3 + x + 1) \end{array}$$

Ara estudiarem els codis cíclics ternaris de longitud 8. Aquests són els que tenen per polinomi generador un divisor de $x^8 - 1 \in \mathbb{Z}_3[x]$.

$x^{3^2} - x$ es descompon en tres polinomis irreductibles de grau 1 i tres polinomis de grau 2.

$x^8 - 1$ es descompon en cinc polinomis irreductibles, dos de grau 1 i tres de grau 2. Si fem totes les possibles combinacions de polinomis en què es descompon $x^8 - 1$, obtindrem $2^5 = 32$ possibles polinomis generadors.

Finalment, si $x^n - 1$ és producte de t polinomis a $\mathbb{F}_q$ irreductibles i diferents, llavors hi ha 2^t codis cíclics a $\mathbb{F}_q$.

6.8 (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.

Resposta:

(a) Pel binomi de Newton sabem que $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$. Tots els nombres binomials $\binom{p}{i}$, amb i entre 0 i p, són múltiples de p, excepte $\binom{p}{0} = 1$ i $\binom{p}{p} = 1$. Per tant, $(x+y)^p = x^p + y^p$ a $\mathbb{Z}_p$ i, per tant, també a $\mathbb{F}_{p^n}$.

(b) El polinomi generador d'un codi cíclic 5-ari de longitud 10 ha de dividir $x^{10} - 1$. Com que a $\mathbb{F}_5$ es compleix $x^{10} - 1 = (x^2 - 1)^5$, es té $x^{10} - 1 = ((x+1)(x-1))^5 = (x+1)^5 (x-1)^5$. Aleshores tot codi cíclic tindrà com a polinomi generador un polinomi de la forma $(x+1)^i (x-1)^j$ amb $0 \leqslant i \leqslant 5$ i $0 \leqslant j \leqslant 5$. D'aquests polinomis n'hi ha 36 i, per tant, hi ha 36 codis cíclics 5-aris de longitud 10.

(c) La dimensió d'un codi cíclic és la longitud del codi menys el grau del polinomi generador. Per tal que el nostre codi tingui dimensió 6, caldrà que el polinomi generador tingui grau 4. Per tant, haurà de ser de la forma $(x+1)^i(x-1)^j$ amb $i+j=4$ i $0 \leqslant i \leqslant 5$ i $0 \leqslant j \leqslant 5$. Això es pot donar de 5 maneres diferents. Per tant, hi ha 5 codis cíclics 5-aris de longitud 10 i dimensió 6.

6.9 (a) Demostreu que $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + 1$.

(b) Quins són els codis cíclics binaris de dimensió 1? I els de codimensió 1?

6.10 Considerem un codi cíclic $\mathcal{C}$ 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 $\mathcal{C}$ fora de les qual tots els valors són 0. Demostreu que necessàriament $m \geqslant n-k+1$.

(b) Demostreu que una paraula no nul·la de $\mathcal{C}$ 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.

6.11 Descriviu tots els codis ternaris cíclics de longitud 18.

6.12 (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 $g_2(x)$, descriviu el màxim codi cíclic contingut pels dos.

(c) Donats dos codis cíclics de longitud n amb polinomis generadors $g_1(x)$ i $g_2(x)$, descriviu el mínim codi cíclic que els conté tots dos.

(d) Concreteu els dos apartats anteriors pel cas de codis ternaris cíclics de longitud 18.

Capítol 7
Problemes de codis algebraics

7.1 (a) Construcció d'un cos finit.

- Comproveu que el polinomi $x^3 + x + 1$ és irreductible i primitiu sobre $\mathbb{F}_2$.
- Construïu $\mathbb{F}_8$ utilitzant aquest polinomi i doneu-ne una taula exponencial-vectorial.

(b) Definiu els codis RS i BCH primitius i en sentit estricte, capaços de detectar dos errors.

- Doneu-ne la longitud i la dimensió.
- Doneu-ne el polinomi generador.
- Doneu-ne una matriu generadora i una matriu de control.
- Quants errors podem garantir que podran corregir?

(c) Suposem que s'ha utilitat el codi de RS. Descodifiqueu:

- $(\alpha^3, 0, \alpha^4, \alpha^5, 1, \alpha, 1)$.
- $(\alpha^3, 0, \alpha^4, 0, ?, ?, 1)$.

(d) Suposem que s'ha utilitat el codi BCH. Descodifiqueu:

- $(0, 0, 1, 0, 0, 1, 0)$.
- $(?, ?, 1, 0, 0, 1, 0)$.

7.2 * (a) Comproveu que el polinomi $x^4 + x + 1$ sobre $\mathbb{Z}_2$

(a) És irreductible.

(b) És primitiu.

(b) Quants elements té el cos $\mathbb{F}$ que obtenim fent mòdul $x^4 + x + 1$ a $\mathbb{Z}_2[x]$? Per què?

(c) Doneu una taula potencial-vectorial de $\mathbb{F}$.

(d) Doneu el polinomi generador d'un codi C de Reed-Solomon sobre $\mathbb{F}$ primitiu en sentit estricte capaç de corregir dos esborralls.

(e) Doneu els paràmetres (longitud, dimensió i distància mínima) de C.

(f) Demostreu que la paraula $(\alpha^3\alpha^5 1000 \alpha^3\alpha^5 1000 \alpha^3\alpha^5 1)$ pertany al codi.

(g) Amb quina cadena de bits la passaríem pel canal?

(h) Corregiu els esborralls de la següent cadena de bits rebuda per un canal que afegeix només esborralls si s'ha emprat C per codificar la informació.

$$????????0000000000000000000000000000000000000000000000000001$$

Resposta:

(a) (a) Com que avaluat a 0 i a 1 dóna diferent de zero, no té arrels. Per tant, no té factors de grau 1. Tampoc no és un múltiple de l'únic irreductible de grau 2. Per tant, és irreductible.

(b) Si fem totes les potències de $\alpha = [x]$ veiem que no obtenim 1 fins a arribar a l'exponent 15. Vegeu l'apartat amb la taula d'equivalències potencial vectorial.

(b) El cos té 16 elements, ja que el polinomi està definit sobre $\mathbb{Z}_p$ amb $p = 2$ i el grau del polinomi és $m = 4$. Per tant, el cos obtingut té $p^m = 16$ elements. És a dir, $\mathbb{F} = \mathbb{F}_{16}$.

(c) La taula d'equivalència vectorial-potencial és:

$vect.$	(1000)	(0100)	(0010)	(0001)	(1100)	(0110)	(0011)
$pot.$	α^0	α	α^2	α^3	α^4	α^5	α^6

(1101)	(1010)	(0101)	(1110)	(0111)	(1111)	(1011)	(1001)
α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}

(d) Per corregir dos esborralls necessitem distància mínima més gran o igual que 3. Prenem com a polinomi generador $g(x) = (x - \alpha)(x - \alpha^2) = x^2 + \alpha^5 x + \alpha^3$.

(e) longitud$= n = 15$, dimensió$= k = n - grau(g) = 15 - 2 = 13$. Com que és un codi RS, $d = n - k + 1 = 15 - 13 + 1 = 3$.

(f) La paraula donada és la forma vectorial del polinomi $g + x^6 g + x^{12} g = (1 + x^6 + x^{12})g$. Com que és un múltiple del polinomi generador, pertany al codi.

(g) $0001\ 0110\ 1000\ 0000\ 0000\ 0000\ 0001\ 0110\ 1000\ 0000\ 0000\ 0000\ 0001\ 0110\ 1000$

(h) La paraula correspon al vector de símbols $??000000000000\alpha^3$. Per tant, el polinomi corresponent a la paraula rebuda és $u(x) = \alpha^3 x^{14}$. Tenim $\sigma = (1 - x)(1 - \alpha x) = \alpha x^2 + \alpha^4 x + 1$ i $\sigma'(x) = \alpha^4$. D'altra banda, les síndromes són $u(\alpha) = \alpha^{3+14} = \alpha^2$, $u(\alpha^2) = \alpha^{3+2\cdot 14} = \alpha$ i, per tant, el polinomi de síndromes és $\alpha x + \alpha^2$.

$$\begin{aligned}\omega &= \sigma S \ mod\ x^2 \\ &= (x^2 + \alpha^4 x + 1)(\alpha x + \alpha^2)\ mod\ x^2 \\ &= (\alpha^4 x + 1)(\alpha x + \alpha^2)\ mod\ x^2 \\ &= \alpha^{11} x + \alpha^2\ mod\ x^2\end{aligned}$$

Els valors dels errors són

$$e_0 = -\frac{\omega(\alpha^{-0})}{\sigma'(\alpha^{-0})} = \frac{\alpha^{11} + \alpha^2}{\alpha^4} = \frac{\alpha^9}{\alpha^4} = \alpha^5$$

$$e_1 = -\frac{\omega(\alpha^{-1})}{\sigma'(\alpha^{-1})} = \frac{\alpha^{10}+\alpha^2}{\alpha^4} = \frac{\alpha^4}{\alpha^4} = 1$$

Per tant, la paraula corregida és $000000000000000\alpha^3 - \alpha^5 10000000000000 = \alpha^5 1000000000000\alpha^3$. Observem que correspon al polinomi $x^{14}g$ i que hauríem pogut deduir el resultat per la forma de la paraula rebuda.

7.3 * (a) Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$ i doneu una taula exponencial-vectorial de $\mathbb{F}_4$.

(b) Construïu un codi C de Reed-Solomon primitiu en sentit estricte sobre $\mathbb{F}_4$ capaç de corregir un esborrall, tot donant-ne el polinomi generador g.

(c) Quant valen la longitud i la dimensió de C?

(d) Codifiqueu de manera sistemàtica la informació corresponent al polinomi x. Doneu el resultat en bits.

(e) Doneu una matriu generadora de C.

(f) Doneu una matriu de control de C.

(g) Corregiu els esborralls de totes les paraules de la seqüència codificada de bits

$$0011????0100.$$

Doneu el resultat en bits.

(h) Comproveu que la seqüència obtinguda pertany al codi.

(i) Quin polinomi generador tindrà el codi dual de C?

(j) Construïu un codi $\tilde{C}$ BCH primitiu en sentit estricte sobre $\mathbb{F}_4$ capaç de corregir un error, tot donant-ne el polinomi generador.

(k) Quant valen la longitud i la dimensió de $\tilde{C}$?

(l) Doneu una matriu generadora de $\tilde{C}$.

(m) Doneu una paraula c de $\tilde{C}$.

(n) Afegiu un error en una posició de la paraula c i doneu el vector amb error obtingut.

(o) Corregiu aquest vector explicant tots els passos.

Resposta:

(a) Els polinomis irreductibles de grau 2 de $\mathbb{Z}_2[x]$ són aquells que no s'anul·len a 0 (coef. constant 1) ni a 1 (nombre senar de termes no nuls). L'únic polinomi amb aquestes característiques és x^2+x+1.

0	00
1	10
α	01
α^2	11

(b) Hem de considerar com a distància prevista 2 i polinomi generador $x-\alpha$.

(c) $n=3$ i $k=2$.

(d) $x\cdot x^{n-k} - (x\cdot x^{n-k} \bmod g) = x^2+\alpha^2$. Correspon a la paraula $\alpha^2 01 \equiv 110010$.

(e)
$$\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{pmatrix}.$$

(f)
$$(1\alpha\alpha^2)$$

(g) Tenim dues paraules amb un esborrall cadascuna:
- $(0\alpha^2?)$: Tindrem $\sigma(x) = 1 + \alpha^2 x$ i $S(x) = 1$, d'on, per l'equació clau, $\omega(x) = 1$. Ara, $e_2 = -\frac{\omega(\alpha^{-2})}{\sigma'(\alpha^{-2})} = \alpha$. Per tant, la primera paraula corregida és $(0\alpha^2\alpha) \equiv 001101$.
- $(?\alpha 0)$: Ara $\sigma(x) = 1 + x$ i $S(x) = \alpha^2$, d'on, per l'equació clau, $\omega(x) = \alpha^2$. Per tant, $e_0 = -\frac{\omega(\alpha^0)}{\sigma'(\alpha^0)} = \alpha^2$ i la segona paraula corregida és $(\alpha^2\alpha 0) \equiv 110100$.

(h) Veiem que la segona paraula és la mateixa que la primera paraula desplaçada. Com que és un codi cíclic, n'hi ha prou de comprovar que una de les dues pertany al codi. I, en efecte, la segona paraula correspon al polinomi generador multiplicat per α.

(i) El polinomi de control és $h(x) = (x^3 - 1)/(x - \alpha) = x^2 + \alpha x + \alpha^2$. El seu recíproc és $\alpha^2 x^2 + \alpha x + 1$. Si el que volem és un generador mònic, hem de prendre $x^2 + \alpha^2 x + \alpha$.

(j) Considerem com a distància mínima prevista $d = 3$. El polinomi generador de $\tilde{C}$ és $(x - \alpha)(x - \alpha^2) = x^2 + x + 1$.

(k) $n = 3, k = 1$

(l) (111)

(m) (111) o bé (000).

(n) Per exemple, en el primer cas, (101).

(o) Es pot corregir directament perquè la paraula a distància mínima és (111). O bé es pot corregir veient que
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$
és una matriu de control i que
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$
que és la segona columna de H.
Altrament, $u(x) = 1 + x^2$, $u(\alpha) = 1 + \alpha^2 = \alpha$, $u(\alpha^2) = 1 + \alpha^4 = \alpha^2$. Per tant, $S = \alpha + \alpha^2 x$.
L'equació clau és $w = \sigma S \ mod\ x^2$ i la resolem per divisions successives:

1	0	1	$\alpha x + 1$
		0	$\alpha x + 1$
S	x^2	$\alpha^2 x + \alpha$	α

Deduïm que $\omega = \alpha$ i $\sigma = \alpha x + 1$. Per tant, tindrem error en la posició d'índex 1 (ja que $\sigma(\alpha^{-1}) = 0$), és a dir, en la segona posició. També, $\sigma' = \alpha$, d'on, per la fórmula dels errors, $e_1 = -\frac{\omega(\alpha^{-1})}{\sigma'(\alpha^{-1})} = -\frac{\alpha}{\alpha} = 1$.

7.4 (a) Comproveu que x^2+2x+2 és un polinomi irreductible i primitiu de $\mathbb{Z}_3[x]$.

(b) Construïu el codi BCH ternari primitiu en sentit estricte de longitud 8 i distància mínima prevista 5, tot donant-ne el polinomi generador.

(c) Corregiu els esborralls corresponents al primer bloc de la seqüència rebuda

$$0\,0\,1\,?\,?\,?\,?\,2\,0\,0\,1\,?\,?\,\ldots$$

(d) Localitzeu i corregiu els errors de la primera paraula de la seqüència

$$1\,0\,1\,1\,2\,0\,0\,0\,0\,1\,2\,\ldots$$

(e) Corregiu la primera paraula de la següent seqüència, on s'han produït esborralls i errors

$$2\,2\,?\,?\,0\,1\,0\,0\,?\,?\,\ldots$$

Resposta:

(b) $2x^2 + x + 2$.

(c) 00121102.

(d) 10112022.

(e) 21220100.

7.5 Quina és la distància mínima real d'un codi BCH sobre $\mathbb{F}_{2^3}$ amb distància mínima prevista 2?

Resposta:

La distància mínima real és 3. En efecte, el polinomi generador té arrels $\alpha, \alpha^2, \alpha^4$ ($\Longrightarrow$ n'hi ha dues de consecutives $\Longrightarrow d \geqslant 3$) i és igual a $x^3 + x^2 + 1$ (té tres coeficients no nuls $\Longrightarrow d \leqslant 3$).

7.6 Anomenarem C un codi en sentit estricte, primitiu, de Reed-Solomon, capaç de corregir dos errors, construït sobre el cos $\mathbb{F}_{3^2}$.

(a) Comproveu que el polinomi $x^2 + x + 2 \in \mathbb{F}_3$ és irreductible, i utilitzeu-lo per construir $\mathbb{F}_{3^2}$.

(b) Doneu l'equivalència vectorial-exponencial per a cada element de $\mathbb{F}_{3^2}$.

(c) Doneu el polinomi generador del codi C.

(d) Doneu la matriu de control del codi C.

(e) Procés de codificació-descodificació:
Codificarem el mot **PEP**; seguidament l'introduirem en un canal ternari amb soroll additiu i, després, el descodificarem.

- Usant el codi ASCII, escriviu **PEP** en el sistema ternari (cada caràcter alfabètic s'ha d'escriure utilitzant cinc dígits ternaris).

- Amb la tècnica de codificació sistemàtica per a codis cíclics, codifiqueu l'anterior informació usant el codi C.
- El canal pel qual circularà la paraula codificada és un canal ternari en què hi ha un soroll additiu que ens donarà el vector d'error següent: $e = (12121212000000000000000000000000\ldots)$.
  Calculeu la paraula que trobarem a la sortida del canal.
- Descodifiqueu el vector rebut utilitzant la tècnica de descodificació algebraica. Calculeu el polinomi síndrome i els polinomis localitzador i avaluador d'errors.
- Doneu els tres caràcters, després de la descodificació, que corresponen al mot **PEP** que hem enviat pel canal.

(f) Torneu a fer el problema, però ara suposant que el canal només introdueix esborralls i no errors. És a dir, que el vector d'errors és: $e = (???????? \; 00000000 \cdots)$.

Resposta:

(a) El polinomi donat és irreductible perquè és de grau 2 i no té arrels.

(b) $\mathbb{Z}_3[x]/x^2+x+2$

Vec.	$(0,0)$	$(0,1)$	$(1,2)$	$(2,2)$	$(2,0)$	$(0,2)$	$(2,1)$	$(1,1)$	$(1,0)$
Pot.	0	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8

(c) El polinomi generador $g(x)$ pot ser construït sabent que α, α^2, α^3 i α^4 en són arrels i que $g(x) \in \mathbb{F}_{3^2}[x]$.
$g(x) = \prod_{i=1,2,3,4}(x-\alpha^i) = \alpha^2 + \alpha^4 x + \alpha^2 x^2 + \alpha^7 x^3 + x^4$.
El codi que estem construint té longitud $n = 8$, dimensió $k = 4$ i distància mínima real $\delta = d = 5$.

(d) La matriu de control es pot construir

- a partir de la matriu generadora (i aquesta es pot escriure a partir del polinomi generador);
- a partir del polinomi recíproc del polinomi de control;
- directament com

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \\ 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 \end{pmatrix}$$

(e) Codificarem la seqüència **02222 02120 02222**; seguidament la introduirem en un canal ternari amb soroll additiu i, després, el descodificarem.
Farem blocs de dos dígits per obtenir elements de $\mathbb{F}_{3^2}$:

$$02\,22\,20\,21\,20\,02\,22\,2\cdots$$
$$\alpha^5, \alpha^3, \alpha^4, \alpha^6, \alpha^4, \alpha^5, \alpha^3, \alpha^4, \cdots .$$

Ara considerarem blocs de quatre elements (ja sabem que el codi té dimensió 4).

$$m_1 = \alpha^5\alpha^3\alpha^4\alpha^6$$
$$m_2 = \alpha^4\alpha^5\alpha^3\alpha^4$$

$$m_3 = \cdots$$

O en forma polinòmica:

$$m_1(x) = \alpha^5 + \alpha^3 x + \alpha^4 x^2 + \alpha^6 x^3$$
$$m_2 = \alpha^4 + \alpha^5 x + \alpha^3 x^2 + \alpha^4 x^3$$
$$m_3 = \cdots$$

La codificació consisteix a calcular el vector $v_i(x)$ a partir de cada vector d'informació $m_i(x)$:
$v_i(x) = m_i(x)x^4 - R_i(x)$, on $R_i(x)$ és el residu de la divisió entre $m_i(x)x^4$ i $g(x)$:
$v_1(x) = \alpha^7 + x + \alpha^7 x^2 + \alpha^6 x^3 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7$;
$v_2(x) = \alpha^5 + \alpha^2 x + \alpha^6 x^2 + \alpha x^3 + \alpha^4 x^4 + \alpha^5 x^5 + \alpha^3 x^6 + \alpha^4 x^7$.
Considerant només els coeficients i "passant-los"a ternari, finalment, tindrem els símbols que travessaran el canal:
11 10 11 21 02 22 20 21 02 12 21 01 20 02 22 20 $\cdots$.
El canal pel qual circula la paraula codificada és un canal ternari en què hi ha un soroll additiu que ens dóna el vector d'error següent:
$e = (12121212000000000000000000000000\ldots)$.
Els símbols ternaris que apareixeran a la sortida del canal, i que són aquells amb els quals haurem de fer les operacions de descodificació, seran:
20 22 20 00 02 22 20 21 02 12 21 22 20 02 22 20 $\cdots$.
Anem a la descodificació:
La longitud del codi és 8, sobre $\mathbb{F}_{3^2}$; per tant, el primer vector rebut consistirà en els 16 primers símbols ternaris rebuts, el segon en els altres 16, etc.
$u_1 = \alpha^4 + \alpha^3 x + \alpha^4 x^2 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7$.
El polinomi síndrome tindrà per coeficients:
$s_1 = u_1(\alpha) = \alpha^4$
$s_2 = u_1(\alpha^2) = 0$
$s_3 = u_1(\alpha^3) = 1$
$s_4 = u_1(\alpha^4) = 0$
i valdrà: $S(x) = \alpha^4 + x^2$.
L'equació clau: $w(x) = \sigma(x)S(x) \bmod x^4$ la resoldrem via l'algorisme de les divisions successives, a partir de $S(x)$ i x^4. L'algorisme el pararem en trobar el primer residu de grau estrictament més petit que 2.
En el moment de parar l'algorisme, tenim:
$r_1(x) = 1$
$Q_1(x) = \alpha^4 x^2 + \alpha^4$.
Per tant:
$w(x) = r_1(x) = 1$
$\sigma(x) = \alpha^4 x^2 + \alpha^4$
$\sigma'(x) = x$

Resoldrem el polinomi localitzador d'errors $\sigma(x)$. Les seves arrels són: α^2, α^6.

Els errors estan localitzats a les coordenades $x_1 = \dfrac{1}{\alpha^2} = \alpha^6$ (setena coordenada) i $x_2 = \dfrac{1}{\alpha^6} = \alpha^2$ (tercera coordenada).

El valor de l'error en la coordenada x_1 és

$e_6 = -\dfrac{w(\alpha^2)}{\sigma'(\alpha^2)} = -\alpha^6 = \alpha^2$ i, en la coordenada x_2, és

$e_2 = -\dfrac{w(\alpha^6)}{\sigma'(\alpha^6)} = -\alpha^2 = \alpha^6$.

El vector d'error serà:

$e = (0, 0, \alpha^6, 0, 0, 0, \alpha^2, 0)$,

i el vector descodificat serà:

$u_1 - e = (\alpha^4 + \alpha^3 x + \alpha^4 x^2 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7) - (\alpha^6 x^2 + \alpha^2 x^6) =$
$\alpha^4 + \alpha^3 x + \alpha^5 x^2 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^7 x^6 + \alpha^6 x^7$.

I la informació associada (el codi era sistemàtic i la informació són les quatre últimes coordenades) serà:

$\alpha^5\, \alpha^3\, \alpha^7\, \alpha^6$.

Nota: El segon bloc no té problemes, i la informació associada serà la mateixa de partida, és a dir:

$\alpha^4\, \alpha^5\, \alpha^3\, \alpha^4$.

Els dígits d'informació, després de la descodificació, que corresponen als dígits enviats són:

$\alpha^5\, \alpha^3\, \alpha^7\, \alpha^6\ \ \alpha^4\, \alpha^5\, \alpha^3\, \alpha^4 = 02\,22\,11\,21\,20\,02\,22\,20\cdots$.

Nota: Observeu que no hem pogut corregir els errors introduïts pel canal.

(f) Ara tornarem a fer el problema, però suposant que el canal només introdueix esborralls i no errors. És a dir, que el vector d'errors és: $e = (????????\,00000000\cdots)$.

Els dígits que trobarem a la sortida del canal seran:

$??\,??\,??\,??\,02\,22\,20\,21\,02\,12\,21\,22\,20\,02\,22\,20\ \cdots$.

La longitud del codi és 8, sobre $\mathbb{F}_{3^2}$; per tant, el primer vector rebut consistirà en els 16 primers símbols ternaris rebuts, el segon en els altres 16, etc.

Com que hi ha hagut esborralls, posarem qualsevol valor en les coordenades d'esborralls i deduirem el polinomi localitzador d'errors, que serà:

$\sigma(x) = (1 - \alpha^0 x)(1 - \alpha x)(1 - \alpha^2 x)(1 - \alpha^3 x) =$
$1 + \alpha^6 x + x^2 + \alpha x^3 + \alpha^6 x^4$.

A més, el codi pot corregir quatre esborralls (si és que no hi ha errors) i, per tant, es pot esperar que puguem corregir els esborralls produïts.

El vector (o polinomi rebut) és:

$u_1(x) = \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7$.

Noteu que hem substituït els esborralls per zeros.

El polinomi síndrome tindrà per coeficients:

$s_1 = u_1(\alpha) = \alpha^3$

$s_2 = u_1(\alpha^2) = \alpha$

$s_3 = u_1(\alpha^3) = \alpha^4$
$s_4 = u_1(\alpha^4) = \alpha^2$,
i valdrà: $S(x) = \alpha^3 + \alpha x + \alpha^4 x^2 + \alpha^2 x^3$.
L'equació clau: $w(x) = \sigma(x)S(x) \bmod x^4$ la resoldrem sense cap problema, només fent operacions:
Obtenim $w(x) = \sigma(x)S(x) = \alpha^3 + \alpha^5 x + \alpha^4 x^2 + \alpha^2 x^3 \bmod x^4$,
i el valor dels esborralls és:

- primera coordenada (substituïm $x = \alpha^0$),
  $e = -\dfrac{w(\alpha^0)}{\sigma'(\alpha^0)} = \alpha^3$;
- segona coordenada (substituïm $x = \alpha^7$),
  $e = -\dfrac{w(\alpha^7)}{\sigma'(\alpha^7)} = \alpha^4$;
- tercera coordenada (substituïm $x = \alpha^6$),
  $e = -\dfrac{w(\alpha^6)}{\sigma'(\alpha^6)} = \alpha^3$;
- quarta coordenada (substituïm $x = \alpha^5$),
  $e = -\dfrac{w(\alpha^5)}{\sigma'(\alpha^5)} = \alpha^2$.

El vector d'errors és:
$e = (\alpha^3, \alpha^4, \alpha^3, \alpha^2, 0, 0, 0, 0)$,
i el vector descodificat serà:
$u_1(x) - e(x) = (\alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7) - (\alpha^3 + \alpha^4 x + \alpha^3 x^2 + \alpha^2 x^3) =$
$\alpha^7 + x + \alpha^7 x^2 + \alpha^6 x^3 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7$,
que coincideix amb el vector enviat.

7.7 Amb les mateixes condicions que el problema anterior, ara corregirem errors i esborralls simultàniament. A més, usarem la tècnica de parar l'algorisme de les divisions successives controlant el polinomi $Q_i(x)$ i no el residu $r_i(x)$.

(a) Feu el problema en el cas que el canal afegeixi el vector d'error $e = (00\,00\,00\,00\,00\,00\,22\,00)$.

(b) Feu el problema en el cas que el canal afegeixi el vector d'error $e = (0?\,?0\,11\,00\,00\,00\,00\,00)$.

Resposta:

Suposarem el codi C, ternari Reed-Solomon, capaç de corregir dos errors, amb paràmetre $m = 2$

El missatge a codificar en caràcters ternaris és $02\,22\,20\,21$, que, en termes del nostre cos $\mathbb{F}_{3^2}$ a partir del polinomi irreductible $x^2 + x + 2$, és

$$m_1(x) = \alpha^5 + \alpha^3 x + \alpha^4 x^2 + \alpha^6 x^3.$$

Un cop realitzada la codificació sistemàtica, ens queda

$$v_1(x) = \alpha^7 + x + \alpha^7 x^2 + \alpha^6 x^3 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7$$

que serà transmès pel canal com

$$11\,10\,11\,21\,02\,22\,20\,21.$$

CORRECCIÓ D'ERRORS

El canal pel qual circularà la paraula codificada és un canal ternari en què un soroll additiu afegirà el vector d'error: $e = (0000000000002200)$.

Els símbols ternaris que apareixeran a la sortida del canal seran:

$$11\,10\,11\,21\,02\,22\,12\,21.$$

El polinomi u_1 rebut serà:

$$u_1(x) = \alpha^7 + \alpha^0 x + \alpha^7 x^2 + \alpha^6 x^3 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^2 x^6 + \alpha^6 x^7$$

Com sempre, en rebre un polinomi, s'ha de calcular la síndrome associada $S(x)$, que tindrà per coeficients:

$s_1 = u_1(\alpha) = \alpha$

$s_2 = u_1(\alpha^2) = \alpha^7$

$s_3 = u_1(\alpha^3) = \alpha^5$

$s_4 = u_1(\alpha^4) = \alpha^3$,

i valdrà:

$$S(x) = \alpha + \alpha^7 x + \alpha^5 x^2 + \alpha^3 x^3.$$

Equació clau

Atès que $2c+t < \delta$ i el codi té $\delta = 5$, podrà corregir un màxim de dos errors; per tant, el polinomi localitzador dels errors $\sigma(x) = \prod_{\alpha^i \in E}(1 - \alpha^i x)$ tindrà grau inferior a 3:

$$w(x) = \sigma(x)S(x) \bmod x^{d-1}$$

que es pot resoldre via l'algorisme de les divisions successives, a partir de $S(x)$ i $x^{d-1} = x^4$ i que pararem just en trobar el polinomi Q_i de grau més gran inferior a 3.

Q_i	1	0	1	$\alpha^7\alpha$	$0\alpha^7001$
q_i			0	$\alpha^3\alpha^5$	$\alpha\alpha^7\alpha^5\alpha^3$
r_i	$S(x)$	x^4	$S(x)$	1	0

Com que el darrer Q_i és de grau 4 ($0\alpha^7001$), el localitzador dels errors és: $\sigma(x) = \alpha^7 + \alpha x$ i $\omega(x) = 1$.

$\sigma(x)$ és de grau 1 (un error) i té com a arrel α^2; per tant, la situació de l'error és $1/\alpha^2 = \alpha^6$, la setena coordenada.

La derivada del localitzador és $\sigma'(x) = \alpha$, i el valor de l'error,

$$e_1 = -\frac{w(\alpha^0)}{\sigma'(\alpha^0)} = -\frac{1}{\alpha} = \alpha^3 = 22.$$

Per recuperar el missatge original haurem de restar el vector d'error $e = (0000000000002200)$ al vector rebut.

CORRECCIÓ D'ERRORS I ESBORRALLS

Suposem que el canal afegeix el vector d'error següent:

$e = (0??0110000000000)$.

Els símbols ternaris que apareixeran a la sortida del canal seran:

$$1?\ ?0\,22\,21\,02\,22\,20\,21.$$

Malgrat que hi hagi dos esborralls i dos errors ternaris, com que estem a $\mathbb{F}_{3^2}$ hem de bloquejar els símbols ternaris de dos en dos, per la qual cosa tenim dos esborralls i un error a corregir.

Donant valor zero als esborralls, el vector u_1 rebut serà:

$$u_1(x) = \alpha^3x^2 + \alpha^6x^3 + \alpha^5x^4 + \alpha^3x^5 + \alpha^4x^6 + \alpha^6x^7.$$

La síndrome associada $S(x)$ tindrà per coeficients:

$s_1 = u_1(\alpha) = \alpha^3$

$s_2 = u_1(\alpha^2) = \alpha^5$

$s_3 = u_1(\alpha^3) = \alpha^5$

$s_4 = u_1(\alpha^4) = 1$,

i valdrà:

$$S(x) = \alpha^3 + \alpha^5x + \alpha^5x^2 + x^3.$$

Polinomi localitzador d'errors

$$\sigma(x) = \prod_{\alpha^i \in E} (1 - \alpha^i x)$$

Aquest polinomi es pot considerar constituït pel producte d'altres dos

$$\sigma(x) = \sigma_{err}(x)\sigma_{esb}(x),$$

on $\sigma_{esb}(x)$ és el polinomi localitzador dels esborralls (errors de posició coneguda)

$$\sigma_{esb}(x) = (1 - \alpha^0x)(1 - \alpha^1x) = 1 + \alpha^3x + \alpha x^2$$

i $\sigma_{err}(x)$ el polinomi localitzador dels errors de posició desconeguda del qual sabem que és un polinomi de grau igual al nombre d'errors corregibles comesos, en el nostre cas el grau és estrictament inferior a 2 (un codi amb distància δ té capacitat per corregir c errors i t esborralls sempre que s'acompleixi $2c + t < \delta$, aquí $2c + t = 4 < \delta$).

L'equació clau: $w(x) = \sigma(x)S(x) \bmod x^{d-1}$ queda convertida en

$$w(x) = \sigma_{err}(x)\sigma_{esb}(x)S(x) \bmod x^{d-1}.$$

Si anomenem $T(x) = \sigma_{esb}(x)S(x)$, llavors

$$w(x) = \sigma_{err}(x)T(x) \bmod x^{d-1},$$

que pot resoldre's via l'algorisme de les divisions successives, a partir de $T(x) = \alpha^3 + \alpha^4 x + \alpha^5 x^2 + \alpha^7 x^3 + \alpha^0 x^4 + \alpha x^5$ i $x^{d-1} = x^4$ i que pararem just en Q_i de grau més gran inferior a 2 ($\sigma_{err}(x)$ de grau < 2).

Q_i	1	0	1	$\alpha^7\alpha^5$
q_i			$\alpha^0\alpha$	$\alpha^3\alpha$
r_i	$T(x)$	x^4	$\alpha^3\alpha^4\alpha^5\alpha^7$	$\alpha^2\alpha^5\alpha^6$

Per tant,

$$w(x) = \alpha^2 + \alpha^5 x + \alpha^6 x^2$$

i

$$\sigma_{err}(x) = \alpha^7 + \alpha^5 x.$$

L'arrel de $\alpha^3 + \alpha x$ és α^6 i, per tant, la situació de l'error $x_3 = 1/\alpha^6 = \alpha^2$, la tercera coordenada. Tenim localitzats els errors a α^0, α i α^2, i el polinomi localitzador complet és

$$\sigma(x) = \sigma_{err}(x)\sigma_{esb}(x) = \alpha^7 + \alpha^7 x + \alpha^4 x^2 + \alpha^6 x^3,$$

i la seva derivada:

$$\sigma'(x) = \alpha^7 + x.$$

Per esbrinar el valor del polinomi error:

- primera coordenada (substituïm $x = \alpha^0$, invers d'α^0),
  $e_1 = -\dfrac{w(\alpha^0)}{\sigma'(\alpha^0)} = -\dfrac{\alpha^5}{\alpha^6} = \alpha^3$;
- segona coordenada (substituïm $x = \alpha^7$, invers d'α),
  $e_2 = -\dfrac{w(\alpha^7)}{\sigma'(\alpha^7)} = -\dfrac{\alpha^3}{\alpha^3} = \alpha^4$;
- tercera coordenada (substituïm $x = \alpha^6$),
  $e_3 = -\dfrac{w(\alpha^6)}{\sigma'(\alpha^6)} = -\dfrac{1}{\alpha^5} = \alpha^7$.

El polinomi d'error és

$$e(x) = \alpha^3 + \alpha^4 x + \alpha^7 x^2,$$

que s'ha de restar a $u_1(x)$ per recuperar el missatge emès:

$$u_1(x) - e_1(x) = v_1(x) = \alpha^7 + x + \alpha^7 x^2 + \alpha^6 x^3 + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^4 x^6 + \alpha^6 x^7.$$

Com que la codificació era sistemàtica i $v_1 = 11\,10\,11\,21\,02\,22\,20\,21$, resulta

$$m_1 = 02\,22\,20\,21,$$

i s'han corregit errors i esborralls correctament.

7.8 Anomenem C el codi binari RS, en sentit estricte, primitiu, de paràmetres $m = 3$; $d = 5$.

Utilitzant aquest codi volem transmetre els elements de $\mathbb{F}_2$,

$100110010000\ldots$ per un canal binari en el qual es produirà un error additiu donat pel vector $e = (111111000\ldots)$.

Reproduïu tot el procés de codificació-descodificació.

Resposta:

Anomenem C el codi de Reed-Solomon, 2-corrector, construït sobre el cos $\mathbb{F}_{2^3}$.

El codi C té com a paràmetres $m = 3$ i $d = 5$.

El codi C és cíclic, de longitud $n = 2^3 - 1 = 7$, i la seva dimensió és $k = n - (d-1) = 7 - (5-1) = 3$.

El seu polinomi generador té coeficients en $\mathbb{F}_{2^3}$ i és el polinomi mínim de $\alpha, \alpha^2, \alpha^3, \alpha^4$, on α és un element primitiu de $\mathbb{F}_{2^3}$. El cos finit $\mathbb{F}_{2^3}$ el podem construir com $\mathbb{Z}_2[x]/f(x)$, on $f(x) = x^3 + x + 1$, és un polinomi primitiu, amb α com a arrel.

$f(x) = x^3 + x + 1$, és primitiu ja que no el podem descompondre en factors de grau 1 que, en aquest cas, serien: $x - 0$ o $x - 1$ i, si substituïm $x = 0$ o $x = 1$ al polinomi, aquest no s'anul·la.

El polinomi generador és $g(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$.

Agafem α com a generador de $\mathbb{F}_{2^3}$, i busquem les representacions polinòmica, vectorial i potencial:

0	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1
(000)	(010)	(001)	(110)	(011)	(111)	(101)	(100)
0	α	α^2	α^3	α^4	α^5	α^6	1

Codifiquem la informació **100110010000** mitjançant la tècnica de codificació sistemàtica per a codis cíclics, utilitzant el codi C:

Fem blocs de m $(m = 3)$ dígits per obtenir elements de $\mathbb{F}_{2^3}$:

$$\{100\ 110\ 010\ 000\}.$$

Utilitzant la taula vectorial-potencial, passem els blocs anteriors a forma potencial:

$$1, \alpha^3, \alpha, 0.$$

Com que el codi és un espai vectorial de dimensió 3 sobre $\mathbb{F}_{2^3}$, fem blocs de 3 dígits.

$$1\alpha^3\alpha\ 000.$$

Passem a forma polinòmica:

$$i_1(x) = 1 + \alpha^3 \cdot x + \alpha \cdot x^2$$

$$i_2(x) = 0.$$

Ara fem la codificació, que consisteix a calcular

$$i(x) = x^4 \cdot i(x) - R(x),$$

on $R(x)$ és el residu de dividir $x^4 \cdot i(x)$ per $g(x)$.

$$v_1(x) = \alpha + x + x^3 \cdot \alpha^3 + x^4 + x^5 \cdot \alpha^3 + x^6 \cdot \alpha$$

$$v_2(x) = 0.$$

La paraula codi que obtenim és:

$$\{\alpha, 1, 0, \alpha^3, 1, \alpha^3, \alpha\}.$$

Passant aquests elements a notació vectorial, tenim:

$$\{0101000001101001100100000000000000000000000\}.$$

que són els bits que passen pel canal.
En el canal s'afegeixen errors als sis primers dígits del missatge i en resulta:

$$\{1010110001101001100100000000000000000000000\}.$$

Comencem a fer la descodificació.
Trenquem la cadena de bits rebuda en blocs de tres.

$$\{101\ 011\ 000\ 110\ 100\ 110\ 010\ 000\ 000\ 000\ 000\ 000\ 000\ 000\}.$$

En forma potencial:

$$\{\alpha^6, \alpha^4, 0, \alpha^3, 1, \alpha^3, \alpha, 0, 0, 0, 0, 0, 0, 0\}.$$

A partir del vector rebut, en forma potencial, calculem el seu polinomi associat:

$$u(x) = \alpha^6 + \alpha^4 \cdot x + \alpha^3 \cdot x^3 + x^4 + \alpha^3 \cdot x^5 + \alpha \cdot x^6.$$

I ara calculem el polinomi síndrome $S(x)$, els coeficients del qual són $s_i = u(\alpha^i)$:

$$\begin{aligned} s_1 &= u(\alpha) = \alpha \\ s_2 &= u(\alpha^2) = \alpha^4 \\ s_3 &= u(\alpha^3) = \alpha^6 \\ s_4 &= u(\alpha^4) = \alpha^3. \end{aligned}$$

Així, el polinomi síndrome tindrà la forma :

$$S(x) = \alpha + \alpha^4 x + \alpha^6 x^2 + \alpha^3 x^3.$$

Ara, mitjançant l'algorisme de la descodificació algebraica, podem calcular el polinomi localitzador d'errors $\sigma(x)$ i el polinomi avaluador d'errors $w(x)$.

Cal notar que, en aplicar l'algorisme de les divisions successives, $r_{-2}(x) = S(x)$ i $r_{-1}(x) = x^{d-1} = x^4$ i que l'algorisme s'atura quan troba el primer residu de grau estrictament menor que $\dfrac{d-1}{2} = 2$.

$$\sigma(x) = \alpha^2 \cdot x^2 + \alpha^4 \cdot x + \alpha$$
$$w(x) = \alpha^2.$$

Llavors $\sigma'(x) = \alpha^4$.

Les arrels de $\sigma(x)$ es busquen de forma exhaustiva i resulten ser α^0 i α^6.

Els errors estan localitzats, respectivament, a les coordenades $x_1 = \dfrac{1}{\alpha^0} = \alpha^0$ i $x_2 = \dfrac{1}{\alpha^6} = \alpha$.

El valor dels errors resulta ser:

- $e_1 = \dfrac{w(\alpha^0)}{\sigma'(\alpha^0)} = \dfrac{\alpha^2}{\alpha^4} = \alpha^5$;
- $e_2 = \dfrac{w(\alpha^6)}{\sigma'(\alpha^6)} = \dfrac{\alpha^2}{\alpha^4} = \alpha^5$.

El vector d'errors és: $e = (\alpha^5\alpha^5 00000)$, i el missatge descodificat, en forma potencial, serà

$$\{\alpha, 1, 0, \alpha^3, 1, \alpha^3, \alpha, 0, 0, 0, 0, 0, 0, 0\}.$$

La informació associada a cada vector, una vegada corregits els errors, és $100110010\ldots$.

7.9 Sigui C el codi *BCH*, primitiu, en sentit estricte, de distància mínima prevista $d = 5$, sobre $\mathbb{F}_{3^2}$. Utilitzarem aquest codi en un canal ternari en què sabem que es produiran esborralls, però no errors.

(a) Codifiqueu el primer bloc de la informació ternària següent:

$$120120120120\cdots.$$

(b) Suposant que el missatge rebut a la sortida del canal és:

$$***110\,120\,120\,120\cdots,$$

on $*$ significa un esborrall, descodifiqueu el primer bloc rebut i doneu-ne, si s'escau, la informació associada.

Resposta:

Sigui C el codi BCH, primitiu en sentit estricte, amb $d = 5$, sobre $\mathbb{F}_{3^2}$. Utilitzarem aquest codi en un canal ternari en què sabem que es produiran esborralls, però no errors.

La construcció de $\mathbb{F}_{3^2}$ s'ha fet a partir del polinomi irreductible, primitiu, $x^2 + x + 2$. Diguem α una arrel d'aquest polinomi, llavors α és un element primitiu del cos $\mathbb{F}_{3^2}$.

La longitud del codi serà $n = 3^2 - 1 = 8$. Per donar el valor de la dimensió, primer calcularem el polinomi generador $g(x)$, que és el polinomi mínim, sobre $\mathbb{F}_{3^2}$, de α, α^2, α^3 i α^4. Calculem aquest polinomi mínim:

$$\begin{aligned} m_\alpha &= 2 + x + x^2 \\ m_{\alpha^2} &= 1 + x^2 \\ m_{\alpha^3} &= 2 + x + x^2 \\ m_{\alpha^4} &= 1 + x. \end{aligned}$$

Per tant,

$$\begin{aligned} g(x) = mcm(m_{\alpha^i}(x)) = m_\alpha(x) \cdot m_{\alpha^2}(x) \cdot m_{\alpha^4(x)} = \\ = 2 + x^2 + x^3 + 2x^4 + x^5. \end{aligned}$$

Una vegada calculat el polinomi generador del codi, podem calcular la dimensió exacta: $k = n - grau(g) = 8 - 5 = 3$.

Codifiquem, ara, el primer bloc de la informació ternària següent:

$$120120120120\ldots$$

Com que la dimensió del codi és $k = 3$, aleshores el primer bloc a codificar és 120.

Passant-ho a forma polinòmica:

$$i_1(x) = 1 + 2x.$$

Codificarem $i(x) \to x^5 \cdot i(x) - R(x)$, on $R(x)$ és el residu de dividir $x^5 \cdot i(x)$ per $g(x)$.

$$i_1(x) \to 2x^6 + x^5 - R(x) \ = \ x + 2x^3 + 2x^4 + x^5 + 2x^6.$$

Els bits codificats són:

$$01022120.$$

Suposem que el missatge rebut a la sortida del canal és:

$$***110120120120\ldots$$

on $*$ significa un esborrall. Ara descodificarem el primer bloc rebut.

$$u(x) = * + *x + *x^2 + x^3 + x^4 + x^6 + 2x^7$$

Donem valors arbitraris (per exemple, zeros) als llocs on s'han produït els esborralls:

$$u(x) = x^3 + x^4 + x^6 + 2x^7.$$

El polinomi síndrome és:

$$S(x) = \alpha^3 + \alpha x^2 + 2x^3.$$

Càlcul del polinomi localitzador d'esborralls $\sigma(x)$:

$$\sigma(x) = (1 - \alpha^0 x)(1 - \alpha^1 x)(1 - \alpha^2 x) = 1 + x + \alpha^5 x^2 + \alpha^7 x^3.$$

Aleshores, utilitzant l'equació clau: $\omega(x) = \sigma(x)S(x)\ mod\ x^4$, obtenim:

$$\omega = \sigma(x)S(x) = (1 + x + \alpha^5 x^2 + \alpha^7 x^3)(\alpha^3 + \alpha x^2 + 2x^3)$$
$$= \alpha^3 + \alpha^3 x + \alpha^7 x^2\ mod\ x^4$$
$$\sigma'(x) = 1 + \alpha x,$$

i el valor dels esborralls és:

- primera coordenada (substituïm per $x = 1$):

$$e = -\frac{w(1)}{\alpha'(1)} = 1;$$

- segona coordenada (substituïm per $x = \alpha^7$):

$$e = -\frac{w(\alpha^7)}{\alpha'(\alpha^7)} = 0;$$

- tercera coordenada (substituïm per $x = \alpha^6$):

$$e = -\frac{w(\alpha^6)}{\alpha'(\alpha^6)} = 1.$$

El vector d'errors és:

$$e = (1, 0, 1, 0, 0, 0, 0, 0).$$

Aleshores tenim:

$$u(x) - e(x) = 2 + 2x^2 + x^3 + x^4 + x^6 + 2x^7;$$

i, finalment,

$$202\,110\,12\ldots$$

7.10 Digueu quins són els paràmetres (dimensió, longitud i capacitat correctora) d'un codi ternari BCH, primitiu i en sentit estricte, amb $m = 2$ i distància mínima prevista 5.

Resposta:

El codi s'ha de construir sobre el cos finit $\mathbb{F}_{3^2}$, per tant, la seva longitud serà $3^2 - 1 = 8$.

Diguem $\alpha = [x]$ un element primitiu del cos finit $\mathbb{F}_{3^2}$.

La distància mínima prevista ens diu que el polinomi generador està construït a partir dels polinomis mínims de α, α^2, α^3 i α^4.

El polinomi mínim de α té com a arrels α i α^3. Per tant, el grau de $m_\alpha(x)$ és 2.

El polinomi mínim de α^2 té com a arrels α^2 i α^6. Per tant, el grau de $m_{\alpha^2}(x)$ és 2.

El polinomi mínim de α^4 té com a arrels α^4. Per tant, el grau de $m_{\alpha^4}(x)$ és 1.

El polinomi generador del codi serà: $g(x) = m_\alpha(x)m_{\alpha^2}(x)m_{\alpha^4}(x)$ i tindrà grau 5.

La dimensió del codi és $n - t$, on $t = 5$ és el grau del polinomi generador. Per tant, $k = 8 - 5 = 3$.

La distància mínima del codi δ està afitada inferiorment per la distància mínima prevista ($5 \leqslant \delta$) i, a més, compleix la fita de Singleton, $\delta \leqslant n - k + 1$. Tenim, doncs, $5 \leqslant \delta \leqslant 6$.

Podem assegurar que el codi serà 2 corrector.

7.11 Doneu els paràmetres d'un codi binari BCH (longitud, dimensió, distància mínima prevista i grau del polinomi generador) que sigui comparable en taxa de transmissió a un codi $C(30, 23)$.

Resposta:

Agafarem un codi binari construït sobre $\mathbb{F}_{2^5}$. Tindrà longitud $2^5 - 1 = 31$. La dimensió del codi hauria de ser al voltant de 23.8 per poder tenir la mateixa taxa de transmissió que el codi donat. Per tant, el grau del polinomi generador hauria d'estar al voltant de $r = n - k = 31 - 23.8 = 7.2$.

El polinomi generador tindrà com a arrels:

- α (i llavors també, α^2, α^4, α^8 i α^{16}).
- α^3 (i llavors també, α^6, α^{12}, α^{24} i α^{17}).

Així, el polinomi contindrà les arrels consecutives: α, α^2, α^3 i α^4 i el seu grau valdrà 10.

Els paràmetres demanats són: $n = 31$, $k = 31 - 10 = 21$, $d = 5$, $r = 8$.

7.12 Per un canal binari i simètric transmetem informació codificada utilitzant el codi binari, BCH, primitiu de longitud 7 i de distància mínima prevista 3.

(a) Calculeu la dimensió del codi.

(b) Calculeu la matriu de control per tres procediments diferents.

Resposta:

Calculem primer la taula d'equivalències del cos finit $\mathbb{F}_{2^3}$. El polinomi irreductible i primitiu utilitzat és $f(x) = x^3 + x^2 + 1$. Definim $\alpha = [x]$ i tenim $\alpha^3 + \alpha^2 + 1 = 0$. D'aquí surt que:

(000)	(100)	(010)	(001)	(101)	(111)	(110)	(011)
α^∞	α^0	α^1	α^2	α^3	α^4	α^5	α^6

En segon lloc, calculem el polinomi generador del codi. Ha de tenir dues arrels consecutives:

El polinomi mínim de α: $m_\alpha(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4) = x^3+x^2+1$

Observem que aquest polinomi ja té les arrels α, α^2 i α^4. Llavors, el polinomi generador:

$g(x) = m_\alpha(x) = (x^3+x^2+1)$

El polinomi generador és de grau 3, o sigui, que la dimensió del codi serà $n-3=4$.

Per calcular la matriu de control del codi, podem fer-ho per tres procediments:

La matriu de control es pot construir:

- a partir de la matriu generadora (i aquesta es pot escriure a partir del polinomi generador).
  La matriu generadora és:

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

  i d'aquí surt la matriu de control:

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

- a partir del polinomi recíproc del polinomi de control.
  El polinomi de control és $\dfrac{x^7-1}{x^3+x^2+1} = x^4+x^3+x^2+1$ i el polinomi recíproc és x^4+x^2+x+1.
  Llavors la matriu cercada és:

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

- directament com:

$$\begin{aligned} H &= \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{aligned}$$

7.13 (a) Comproveu que el polinomi x^3+x^2+1 és irreductible i primitiu sobre $\mathbb{F}_2$.

(b) Construïu $\mathbb{F}_8$ utilitzant aquest polinomi i doneu-ne una taula exponencial-vectorial.

(c) Definiu el codi RS primitiu i en sentit estricte sobre $\mathbb{F}_8$ capaç de corregir un error i un esborrall a la vegada.

(d) Doneu-ne el polinomi generador.

(e) Doneu-ne la dimensió.

(f) Doneu-ne una matriu generadora i una de control.

(g) Suposem que s'ha utilitzat la codificació sistemàtica habitual. Descodifiqueu la primera paraula de la seqüència

$$?1101000010110000000100001011 1\ldots$$

(h) En el mateix supòsit que l'apartat anterior, quina és la informació que s'ha enviat?

Resposta:

(a) Diguem $f(x) = x^3+x^2+1$. Per comprovar que el polinomi és irreductible, com que és de grau 3 n'hi ha prou de veure que no s'anul·la en cap dels elements de $\mathbb{F}_2$. Com que $f(0) = 1 \neq 0$ i $f(1) = 1 \neq 0$, podem concloure que $f(x)$ és irreductible sobre $\mathbb{F}_2$. Per veure que és primitiu, hem de veure que tots els elements no nuls de $\mathbb{F}_{2^3}$ són una potència de la classe de x, que anomenem α. Això ho podem veure en la taula exponencial-vectorial de l'apartat següent.

(b)

α	α^2	α^3	α^4	α^5	α^6	α^7	0
$(0,1,0)$	$(0,0,1)$	$(1,0,1)$	$(1,1,1)$	$(1,1,0)$	$(0,1,1)$	$(1,0,0)$	$(0,0,0)$

(c) Si volem un codi RS que corregeixi un error i un esborrall a la vegada, cal que la distància mínima δ satisfaci $2+1 < \delta$. Ho podem imposar prenent com a distància de disseny $d = 4$.

(d) El polinomi generador serà el producte de tots els monomis $x - \alpha^i$ amb i entre 1 i $d-1 = 3$. Per tant, $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3) = x^3 + \alpha^5 x^2 + x + \alpha^6$.

(e) Si el codi és primitiu, aleshores la longitud és $n = 8-1 = 7$. Si k és la dimensió del codi, el grau del polinomi $g(x)$ serà $n-k = 3$. Per tant, $k = 4$.

(f) Podem prendre com a matriu generadora,

$$\begin{pmatrix} \alpha^6 & 1 & \alpha^5 & 1 & 0 & 0 & 0 \\ 0 & \alpha^6 & 1 & \alpha^5 & 1 & 0 & 0 \\ 0 & 0 & \alpha^6 & 1 & \alpha^5 & 1 & 0 \\ 0 & 0 & 0 & \alpha^6 & 1 & \alpha^5 & 1 \end{pmatrix}.$$

I, com a matriu de control, tenint en compte que les arrels del polinomi generador són $\alpha, \alpha^2, \alpha^3$:

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

(g) La primera paraula de la seqüència és

$$?11\ 010\ 000\ 101\ 100\ 000\ 001$$

corresponent a

$$?\alpha 0\alpha^3 10\alpha^2.$$

Si ara convertim l'esborrall en 0, obtenim

$$0\alpha 0\alpha^3 10\alpha^2.$$

Per aplicar l'algoritme de les divisions successives, necessitem avaluar el polinomi corresponent, $u(x) = \alpha x + \alpha^3 x^3 + x^4 + \alpha^2 x^6$ en $\alpha, \alpha^2, \alpha^3$ i n'obtenim així les síndromes: $s_1 = u(\alpha) = \alpha^4$, $s_2 = u(\alpha^2) = \alpha$, $s_3 = u(\alpha^3) = 1$. Per tant, $S(x) = x^2 + \alpha x + \alpha^4$.

Ara, el localitzador d'esborralls és $\sigma_{esb}(x) = 1 - x = 1 + x$. Per aplicar l'algoritme de les divisions successives, utilitzarem $T(x) = S(x)\sigma_{esb}(x) = x^3 + \alpha^5 x^2 + \alpha^3 x + \alpha^4$.

Els diferents residus que anem obtenint són $r_{-2} = T(x)$, $r_{-1} = x^3$, $r_0 = \alpha^5 x^2 + \alpha^3 x + \alpha^4$, $r_1 = \alpha^5 x + \alpha^4$ i els polinomis Q, són $Q_{-2} = 1$, $Q_{-1} = 0$, $Q_0 = 1$, $Q_1 = \alpha^2 x + 1$. Parem a Q_1, ja que és l'últim polinomi de grau inferior o igual que el número d'errors (no esborralls) que pretenem corregir (1).

Deduïm $\sigma_{err}(x) = Q_1$, $\sigma(x) = \sigma_{err}(x)\sigma_{esb}(x) = \alpha^2 x^2 + \alpha^3 x + 1$, $\sigma'(x) = \alpha^3$, $\omega(x) = r_1$. I, finalment, les posicions d'error són 1 i 3, ja que 1 correspon a l'esborrall i $\sigma_{err}(\alpha^{-2}) = \sigma_{err}(\alpha^5) = 0$, mentre que els valors dels errors són $e_1 = -\dfrac{\omega(\alpha^0)}{\sigma'(\alpha^0)} = \alpha^6$ i $e_3 = -\dfrac{\omega(\alpha^5)}{\sigma'(\alpha^5)} = \alpha^5$.

Per tant, la paraula transmesa ha estat:

$$\alpha^6\alpha\alpha^5\alpha^3 10\alpha^2.$$

(h) Si s'ha utilitzat codificació sistemàtica habitual, la informació que s'ha enviat és a les últimes k coordenades. És a dir,

$$\alpha^3 10\alpha^2.$$

7.14 Problema relacionat amb el 6.4.

(a) Comproveu que el polinomi $x^2 + 2x + 2$ és irreductible i primitiu sobre $\mathbb{F}_3$.

(b) Construïu $\mathbb{F}_9$ utilitzant aquest polinomi i doneu-ne una taula exponencial-vectorial.

(c) Definiu el codi BCH primitiu i en sentit estricte sobre $\mathbb{F}_9$, capaç de corregir almenys 3 esborralls.

(d) Doneu-ne el polinomi generador.

(e) Doneu-ne la dimensió.

(f) Doneu-ne una matriu generadora i una de control.

(g) Descodifiqueu la primera paraula de la seqüència

$$???22200011012001212\ldots$$

(h) Descodifiqueu la primera paraula de la seqüència

$$01202122101120010220\ldots$$

(i) Descodifiqueu la primera paraula de la seqüència

$$?01021210102210221 01\ldots$$

(j) Suposem que s'ha utilitzat la codificació sistemàtica habitual. Quina és la informació que s'ha enviat en els tres casos dels apartats anteriors?

Resposta:

(a) Diguem $f(x) = x^2+2x+2$. Per comprovar que el polinomi és irreductible, com que és de grau 3 n'hi ha prou de veure que no s'anul·la en cap dels elements de $\mathbb{F}_3$. Com que $f(0) = 2 \neq 0$, $f(1) = 2 \neq 0$ i $f(2) = 1 \neq 0$, podem concloure que $f(x)$ és irreductible sobre $\mathbb{F}_3$. Per veure que és primitiu, hem de veure que tots els elements no nuls de $\mathbb{F}_{3^2}$ són una potència de la classe de x, que anomenem α. Això ho podem veure en la taula exponencial-vectorial de l'apartat següent.

(b)

α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	0
$(0,1)$	$(1,1)$	$(1,2)$	$(2,0)$	$(0,2)$	$(2,2)$	$(2,1)$	$(1,0)$	$(0,0)$

(c) Si volem un codi BCH que corregeixi tres esborralls, cal que la distància mínima δ satisfaci $3 < \delta$. Ho podem imposar prenent com a distància de disseny $d = 4$.

(d) El polinomi generador serà el mínim comú múltiple dels polinomis mínims de α, α^2 i α^3. Com que $m_\alpha(x) = m_{\alpha^3}(x) = x^2 + 2x + 2$ i $m_{\alpha^2}(x) = x^2 + 1$, aleshores $g(x) = m_\alpha(x)m_{\alpha^2}(x) = x^4 + 2x^3 + 2x + 2$.

(e) Si el codi és primitiu, aleshores la longitud és $n = 9 - 1 = 8$. Si k és la dimensió del codi, el grau del polinomi $g(x)$ serà $n - k = 4$. Per tant, $k = 4$.

(f) Podem prendre com a matriu generadora:

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 2 & 1 \end{pmatrix}.$$

I, com a matriu de control, tenint en compte que les arrels consecutives del polinomi generador són $\alpha, \alpha^2, \alpha^3$:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^1 & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \end{pmatrix}.$$

(g) La primera paraula de la seqüència és

$$???22200.$$

Si ara convertim els esborralls en 0, obtenim

$$00022200.$$

Per calcular el polinomi de síndromes, necessitem avaluar el polinomi corresponent, $u(x) = 2x^3 + 2x^4 + 2x^5$ en $\alpha, \alpha^2, \alpha^3$ i n'obtenim així les síndromes: $s_1 = u(\alpha) = \alpha^5$, $s_2 = u(\alpha^2) = \alpha^4$, $s_3 = u(\alpha^3) = \alpha^7$. Per tant, $S(x) = \alpha^7 x^2 + \alpha^4 x + \alpha^5$.
El localitzador d'errors és igual al localitzador d'esborralls i és igual a $\sigma(x) = (1-x)(1-\alpha x)(1-\alpha^2 x) = \alpha^7 x^3 + \alpha^7 x^2 + \alpha^2 x + 1$. La seva derivada és $\sigma'(x) = \alpha^3 x + \alpha^2$. I l'avaluador d'errors $\omega(x)$, el podem calcular així:

$$\omega(x) = S(x)\sigma(x) \mod x^3 = \alpha^2 x + \alpha^5 \mod x^3.$$

Finalment, els valors dels errors són $e_1 = -\dfrac{\omega(\alpha^8)}{\sigma'(\alpha^8)} = 1$, $e_2 = -\dfrac{\omega(\alpha^{8-1})}{\sigma'(\alpha^{8-1})} = 0$ i $e_3 = -\dfrac{\omega(\alpha^{8-2})}{\sigma'(\alpha^{8-2})} = 2$.
Per tant, la paraula transmesa ha estat

$$20122200.$$

(h) La primera paraula de la seqüència és

$$01202122.$$

Per aplicar l'algoritme de les divisions successives, necessitem avaluar el polinomi corresponent, $u(x) = x + 2x^2 + 2x^4 + x^5 + 2x^6 + 2x^7$ en $\alpha, \alpha^2, \alpha^3$ i n'obtenim així les síndromes: $s_1 = u(\alpha) = \alpha^6$, $s_2 = u(\alpha^2) = 1$, $s_3 = u(\alpha^3) = \alpha^2$. Per tant, $S(x) = \alpha^2 x^2 + x + \alpha^6$.
Apliquem l'algoritme de les divisions successives. Els diferents residus que anem obtenint són $r_{-2} = S(x)$, $r_{-1} = x^3$, $r_0 = \alpha^2 x^2 + x + \alpha^6$, $r_1 = \alpha^2$ i els polinomis Q, són $Q_{-2} = 1$, $Q_{-1} = 0$, $Q_0 = 1$, $Q_1 = \alpha^2 x + \alpha^4$. Parem a r_1, ja que és el primer residu de grau estrictament inferior a la capacitat correctora.
Deduïm $\sigma(x) = Q_1$, $\sigma'(x) = \alpha^2$, $\omega(x) = r_1$. I, finalment, la posició d'error és 3, ja que $\sigma(\alpha^{-2}) = 0$, mentre que el valor de l'error és $e_3 = -\dfrac{\omega(\alpha^{-2})}{\sigma'(\alpha^{-2})} = 2$.
Per tant, la paraula transmesa ha estat

$$01002122.$$

(i) La primera paraula de la seqüència és

$$?0102121.$$

Si ara convertim l'esborrall en 0, obtenim

$$00102121.$$

Per aplicar l'algoritme de les divisions successives, necessitem avaluar el polinomi corresponent, $u(x) = x^2 + 2x^4 + x^5 + 2x^6 + x^7$ en $\alpha, \alpha^2, \alpha^3$ i n'obtenim així les síndromes: $s_1 = u(\alpha) = \alpha^6$, $s_2 = u(\alpha^2) = \alpha^4 = 2$, $s_3 = u(\alpha^3) = \alpha^2$. Per tant, $S(x) = \alpha^2 x^2 + 2x + \alpha^6$.

Ara, el localitzador d'esborralls és $\sigma_{esb}(x) = 1 - x = 1 + 2x$. Per aplicar l'algoritme de les divisions successives utilitzarem $T(x) = S(x)\sigma_{esb}(x) = \alpha^6 x^3 + \alpha^7 x^2 + \alpha x + \alpha^6$.

Els diferents residus que anem obtenint són $r_{-2} = T(x)$, $r_{-1} = x^3$, $r_0 = \alpha^7 x^2 + \alpha x + \alpha^6$, $r_1 = \alpha^5 x + \alpha$ i els polinomis Q són $Q_{-2} = 1$, $Q_{-1} = 0$, $Q_0 = 1$, $Q_1 = \alpha^5 x + \alpha^3$. Parem a Q_1, ja que és l'últim polinomi de grau inferior o igual que el número d'errors (no esborralls) que pretenem corregir (1).

Deduïm $\sigma_{err}(x) = Q_1$, $\sigma(x) = \sigma_{err}(x)\sigma_{esb}(x) = \alpha x^2 + \alpha^4 x + \alpha^3$, $\sigma'(x) = \alpha^5 x + \alpha^4$, $\omega(x) = r_1$. I, finalment, les posicions d'error són 1 i 7, ja que 1 correspon a l'esborrall i $\sigma_{err}(\alpha^{-6}) = \sigma_{err}(\alpha^2) = 0$, mentre que els valors dels errors són $e_1 = -\dfrac{\omega(\alpha^0)}{\sigma'(\alpha^0)} = 0$ i $e_7 = -\dfrac{\omega(\alpha^2)}{\sigma'(\alpha^2)} = 1$.

Per tant, la paraula transmesa ha estat

$$00102111.$$

(j) Si s'ha utilitzat codificació sistemàtica habitual, la informació que s'ha enviat és a les últimes k coordenades. És a dir, 2200 per al primer cas, 0100 per al segon cas i 0010 per a l'últim cas.

7.15 Sigui D el codi RS sobre $\mathbb{F}_{3^2}$, primitiu, en sentit estricte, capaç de corregir, com a mínim, dos errors.

A la sortida del canal hem rebut la seqüència:

$$????010021????202201010120000021$$

Descodifiqueu el primer bloc de la seqüència rebuda i doneu-ne, si s'escau, la informació associada.

Nota: Considereu el polinomi $x^2 + 2x + 2$ per a la construcció del cos finit.

Resposta:

$\mathbb{Z}_3[x]/x^2 + 2x + 2$

Vec.	$(0,0)$	$(0,1)$	$(1,1)$	$(1,2)$	$(2,0)$	$(0,2)$	$(2,2)$	$(2,1)$	$(1,0)$
Pot.	0	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8

El polinomi generador $g(x)$ pot ser construït sabent que α, α^2, α^3 i α^4 en són arrels i que $g(x) \in \mathbb{F}_{3^2}[x]$.

$g(x) = \prod_{i=1,2,3,4}(x - \alpha^i) = x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2$

El codi que estem construint té longitud $n = 8$, dimensió $k = 4$ i distància mínima real $\delta = d = 5$.

El primer bloc de la seqüència rebuda és ????010021????20. Substituint els esborralls per zeros i escrivint la seqüència utilitzant elements de $\mathbb{F}_{3^2}$, resulta: $u = (00\alpha 0\alpha^7 00\alpha^4)$ o, en forma polinomial, $u(x) = \alpha x^2 + \alpha^7 x^4 + \alpha^4 x^7$.

Els esborralls ens han provocat errors en les coordenades $0, 1, 5, 6$ i el polinomi localitzador d'errors és: $\sigma(x) = (1 - \alpha^0 x)(1 - \alpha^1 x)(1 - \alpha^5 x)(1 - \alpha^6 x) = 2x^4 + \alpha^7 x^3 + \alpha^2 x^2 + \alpha x + 1$

També podem calcular la derivada, $\sigma'(x) = 2x^3 + 2\alpha^2 x + \alpha$

El polinomi síndrome és $S(x) = s_1 + s_2 x + s_3 x^2 + s_4 x^3$, on: $s_1 = u(\alpha) = 0$; $s_2 = u(\alpha^2) = \alpha$; $s_3 = \alpha$; $s_4 = \alpha^5$.

$$S(x) = \alpha x + \alpha x^2 + \alpha^5 x^3$$

Segons l'equació clau: $w(x) = S(x)\sigma(x) \bmod x^4 = \alpha^2 x^3$

Podem avaluar els esborralls:

$e_0 = -\frac{w(x=\alpha^0)}{\sigma'(x=\alpha^0)} = \alpha^6$

$e_1 = -\frac{w(x=\alpha^7)}{\sigma'(x=\alpha^7)} = \alpha^2$

$e_5 = -\frac{w(x=\alpha^3)}{\sigma'(x=\alpha^3)} = \alpha^6$

$e_6 = -\frac{w(x=\alpha^2)}{\sigma'(x=\alpha^2)} = \alpha^6$

Per tant, deduïm que el vector enviat és: $v = (00\alpha 0\alpha^7 00\alpha^4) - (\alpha^6\alpha^2 000\alpha^6\alpha^6 0) = (\alpha^2\alpha^2\alpha 0\alpha^7\alpha^2\alpha^2\alpha^4) = (1111100021111120)$ i la informació associada és: (21111120).

7.16 En un canal binari, on només es produeixen esborralls, s'ha utilitzat la codificació sistemàtica donada per un codi C de Reed-Solomon, binari, primitiu i en sentit estricte, de paràmetres $m = 3$ i distància mínima prevista $d = 5$.

De la següent seqüència de bits rebuda, descodifiqueu la primera paraula-codi i doneu la informació associada.

$$??????????\ \ ??01010101\ \ 1010101010\ \ 000\cdots$$

Nota: Utilitzeu el polinomi $1 + x + x^3$ per a la construcció del cos finit.

Resposta:

El cos finit $\mathbb{F}_8$ té la següent taula d'equivalències:

vect	(000)	(100)	(010)	(001)	(110)	(011)	(111)	(101)
pot	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6

El codi C té longitud $n = 2^3 - 1 = 7$ i dimensió $k = n - d + 1 = 7 - 5 + 1 = 3$.

Cada paraula-codi té una longitud de $7 \cdot 3 = 21$ bits i, per tant, la primera paraula-codi rebuda a la sortida del canal (substituint els esborralls per zeros) és: 0000000000 0001010101 1, o sigui: $0\,0\,0\,0\,\alpha^1\alpha^6\alpha^4$. En forma polinomial: $u(x) = \alpha^1 x^4 + \alpha^6 x^5 + \alpha^4 x^6$.

Polinomi síndrome:

$$S(x) = \alpha + \alpha^2 x + \alpha^4 x^2 + \alpha^6 x^3.$$

Polinomi localitzador d'errors: $\sigma(x) = (1-x)(1-\alpha x)(1-\alpha^2 x)(1-\alpha^3 x)$.

Segons l'equació clau:

$$\omega(x) = \sigma(x)S(x) = \alpha + \alpha^5 x + \alpha^6 x^2 + \alpha^2 x^3 \bmod x^4.$$

El valor dels esborralls, el calcularem com:

$$e_0 = -\frac{w(\alpha^0)}{\sigma'(\alpha^0)} = \alpha^6$$

$$e_1 = -\frac{w(\alpha^6)}{\sigma'(\alpha^6)} = \alpha^0$$

$$e_2 = -\frac{w(\alpha^5)}{\sigma'(\alpha^5)} = \alpha^0$$

$$e_3 = -\frac{w(\alpha^4)}{\sigma'(\alpha^4)} = \alpha^4$$

El vector d'error és $e = (101\,100\,100\,011\,000\,000\,000)$ i el vector rebut, una vegada corregits els errors:

$v = u - e = (101\,100\,100\,011\,010\,101\,011$.

La informació associada és: $010\,101\,011$.

7.17 Per un canal binari i simètric transmetem informació codificada utilitzant el codi binari, BCH, primitiu de longitud 15 i de distància mínima prevista 5. Calculeu la dimensió del codi i la síndrome del primer bloc de la seqüència rebuda $11110\,00000\,00000\,00000\,\ldots$

Nota: Construïu el cos finit $\mathbb{F}_{2^4}$ utilitzant el polinomi primitiu $x^4 + x + 1$.

Resposta:

Les operacions per treballar en aquest codi s'han de fer sobre el cos finit $\mathbb{F}_{2^4}$, ja que la dimensió és $n = 15 = 2^4 - 1$.

Si $\alpha = [x] \in \mathbb{F}_{2^4}$, el polinomi generador del codi ha de tenir, com a mínim, 4 arrels consecutives i:

$$g(x) = m_\alpha(x) m_{\alpha^3}(x)$$

Les arrels de $m_\alpha(x)$ són α, α^2, α^4 i α^8. Les de $m_{\alpha^3}(x)$ són α^3, α^6, α^{12} i α^9.

El polinomi generador té grau 8 i $n - k = 8$. La dimensió del codi és, doncs, $k = n - 8 = 15 - 8 = 7$.

La taula d'equivalència vectorial-potencial per al cos finit $\mathbb{F}_{2^4}$ és:

vect.	(1000)	(0100)	(0010)	(0001)	(1100)	(0110)	(0011)
pot.	α^0	α	α^2	α^3	α^4	α^5	α^6

(1101)	(1010)	(0101)	(1110)	(0111)	(1111)	(1011)	(1001)
α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}

El vector rebut a la sortida del canal és: $u(x) = 1 + x + x^2 + x^3$ i el seu polinomi síndrome resulta de donar valors:

$u(\alpha) = \alpha^{12}$

$u(\alpha^2) = \alpha^9$
$u(\alpha^3) = \alpha 12$
$u(\alpha^4) = \alpha^3$
$S(x) = \alpha^{12} + \alpha^9 x + \alpha^{12} x^2 + \alpha^3 x^3$

Relació de cossos finits

$\mathbb{F}_4$	Problema 3.1 (x^2+x+1)
$\mathbb{F}_8$	Problema 7.8 (x^3+x+1) Problema 7.12 (x^3+x^2+1)
$\mathbb{F}_9$	Problema 5.19 (x^2+x+2) Problema 6.4 (x^2+2x+2)
$\mathbb{F}_{16}$	Problema 3.5 (x^4+x^3+1) Problema 7.17 (x^4+x+1)
$\mathbb{F}_{25}$	Problema 3.17 (x^2-2) Problema 3.17 (x^2-3)
$\mathbb{F}_{27}$	Problema 3.8 (x^3+2x+1)

Aquest llibre pretén ser el suport de l'assignatura Matemàtica Discreta II, impartida al grau d'Informàtica de la URV. Els dos blocs principals d'aquesta assignatura són l'aritmètica discreta i la teoria de la codificació per al tractament d'errors en les comunicacions digitals. El llibre està enfocat a plantejar i resoldre problemes. El primer capítol és un resum de la teoria de l'assignatura; la resta de capítols estan dedicats als problemes de cadascun dels temes.