Teoria de codis: codis cíclics

Maria Bras-Amorós, Oriol Farràs Ventura

7 de gener de 2024

Matrius de Vandermonde I

Codis cíclics

L'exemple del faisà

Solucions

Apèndix: Repàs de determinants

Apèndix: Repàs de més nocions de matrius

Matrius de Vandermonde

- Les **matrius de Vandermonde** són una classe de matrius amb una estructura determinada que aporta propietats molt interessants.
- Tenen aplicacions en moltes àrees com les comunicacions digitals, el porcessat d'imatge i les antenes (MIMO), i s'empren en el càlcul de la Discrete Fourier Transform (DFT), la interpolació de funcions,...
- Nosaltres farem servir matrius de Vandermonde definides sobre un cos finit, però es poden definir sobre qualsevol cos.

Matrius de Vandermonde

Definició

Donats $v_1, v_2, \ldots, v_n \in \mathbb{F}_q$, la **matriu de Vandermonde** de $v_1, \ldots, v_n$ d'ordre r es defineix com

$$V_r(v_1, v_2, \ldots, v_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ v_1 & v_2 & \ldots & v_n \\ v_1^2 & v_2^2 & \ldots & v_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1^{r-1} & v_2^{r-1} & \ldots & v_n^{r-1} \end{pmatrix}$$

En aquest curs, només considerarem matrius de Vandermonde en les quals $v_i \neq v_j$ per tot $i \neq j$.

Matrius de Vandermonde

Exemple

1. *Calculem* $V_3(1,2,3)$ *per* $1,2,3 \in \mathbb{F}_5$*:*

$$V_3(1,2,3) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 4 \end{pmatrix}.$$

2. *Calculem* $V_3(0,1,2,3,4)$ *per* $0,1,2,3,4 \in \mathbb{F}_5$*:*

$$V_3(0,1,2,3,4) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{pmatrix}.$$

3. *Sigui* α *la classe de* x *a* $\mathbb{F}_9 = \mathbb{F}_3/(x^2+x+2)$*. Calculem* $V_4(1,\alpha,\alpha^3,\alpha^4,\alpha^6,\alpha^7)$ *a* $\mathbb{F}_9$*:*

$$V_4(1,\alpha,\alpha^3,\alpha^4,\alpha^6,\alpha^7) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^3 & \alpha^4 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^6 & 1 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha & \alpha^4 & \alpha^2 & \alpha^5 \end{pmatrix},$$

on hem fet servir la propietat que $\alpha^8 = 1$*.*

Determinant de matrius de Vandermonde

Lema 1

El determinant de la matriu de Vandermonde $V_n(v_1, v_2, \ldots, v_n)$ és igual a

$$\det(V_n(v_1, v_2, \ldots, v_n)) = \prod_{1 \leq i < j \leq n} (v_j - v_i)$$

Exemple

A $\mathbb{F}_5$*, la matriu* $V_3(0,1,2)$ *és* $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & 4 \end{pmatrix}$.

El determinant de $V_3(0,1,2)$ *és igual a* $4 - 2 = 2$.

Fent servir el lema, el determinant és $(2-0)(2-1)(1-0) = 2$.

Determinant de matrius de Vandermonde

Demostració

La prova es pot fer per inducció en n. Per n = 2, és senzill veure que $\begin{vmatrix} 1 & 1 \\ v_1 & v_2 \end{vmatrix} = v_2 - v_1 .$

Per n > 2, $|V_n(v_1, v_2, \ldots, v_n)| = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ v_1 & v_2 & \ldots & v_n \\ v_1^2 & v_2^2 & \ldots & v_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1^{n-1} & v_2^{n-1} & \ldots & v_n^{n-1} \end{vmatrix} .$

Per cada i ≥ 2, podem restar a la i-èssima fila l'anterior fila multiplicada per v_1 *i obtenir així*

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ 0 & v_2 - v_1 & \ldots & v_n - v_1 \\ 0 & v_2^2 - v_1 v_2 & \ldots & v_n^2 - v_1 v_n \\ \vdots & \vdots & \vdots & \vdots \\ 0 & v_2^{n-1} - v_1 v_2^{n-2} & \ldots & v_n^{n-1} - v_1 v_n^{n-2} \end{vmatrix} =$$

$$\begin{vmatrix} v_2 - v_1 & \ldots & v_n - v_1 \\ v_2(v_2 - v_1) & \ldots & v_n(v_n - v_1) \\ \vdots & \vdots & \vdots \\ v_2^{n-2}(v_2 - v_1) & \ldots & v_n^{n-2}(v_n - v_1) \end{vmatrix} .$$

Això és igual a $(v_2 - v_1) \cdot \cdots \cdot (v_n - v_1)\,|V_{n-1}(v_2, \ldots, v_n)|$ *. I, per la hipòtesis d'inducció, és igual a* $(v_2 - v_1) \cdot \cdots \cdot (v_n - v_1) \prod_{2 \le i < j \le n}(v_j - v_i) = \prod_{1 \le i < j \le n}(v_j - v_i)$.

□

Determinant de matrius de Vandermonde

Exercici 1

A $\mathbb{F}_7$,

1. Calculeu la matriu de Vandermonde de rang 4 de $6, 5, 4, 3$.
2. Calculeu el seu determinant per menors.
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

Solució (p.68)

Determinant de matrius de Vandermonde

Exercici 2

A $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2$, anomenem α a la classe de x.

1. Calculeu la matriu de Vandermonde de rang 4 de $\alpha, \alpha^3, \alpha^5, \alpha^7$.
2. Calculeu el seu determinant per menors .
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

Solució (p.69)

Exercici 3

Calculeu el determinant de $V_4(1, \alpha, \alpha^3, \alpha^4)$, on α és la classe de x de $\mathbb{F}_3[x]/x^2 + x + 2$.

- Per menors .
- Pel resultat del lema.

Solució (p.71)

Determinant de matrius de Vandermonde

- Recordem que, per tot cos $\mathbb{F}$ i tot $a, b \in \mathbb{F}$, $ab = 0$ si i només si $a = 0$ o $b = 0$.
- Per tant, $\det(V_n(v_1, v_2, \ldots, v_n)) = 0$ si i només si $v_i = v_j$ per algun $i \neq j$.
- Obtenim, així, el següent corol·lari:

Corol·lari 1

La matriu $V_n(v_1, v_2, \ldots, v_n)$ és invertible si i només si $v_i \neq v_j$ per tot $1 \leq i < j \leq n$.

- Així, agafant $v_i \neq v_j$ per tot $1 \leq i < j \leq n$, podem garantir que $V_n(v_1, v_2, \ldots, v_n)$ té rang n.

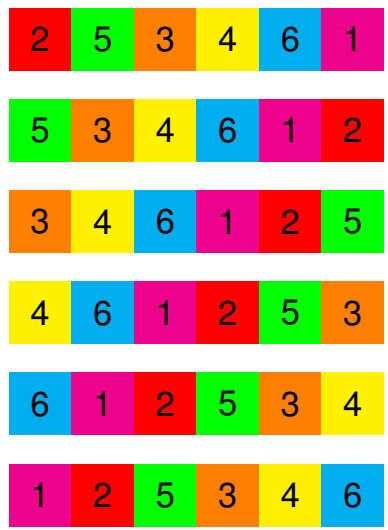
Desplaçaments circulars

Diem que els **desplaçaments circulars** d'una paraula $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ són totes les paraules $(c_i, c_{i+1}, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{i-1})$ amb $0 \leq i \leq n-1$.

Desplaçaments circulars

Exemple

Els desplaçaments circulars de 2 5 3 4 6 1 *seran*



Codis cíclics

Diem que un codi lineal és **cíclic** si conté tots els desplaçaments circulars de totes les seves paraules.

Exercici 4

Considerem el conjunt de paraules $\{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2^4$.

1. Demostreu que és un codi lineal.
2. Quina dimensió té?
3. Doneu-ne una matriu generadora.
4. Demostreu que és un codi cíclic.

Solució (p.73)

Codis cíclics

Exercici 5

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.

Solució (p.75)

Polinomi generador

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 $0 \ldots n-1$ en comptes de $1 \ldots n$.

Exemple

En l'exemple $C = \{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2^4$*, les paraules del codi les identificaríem amb polinomis de la manera següent:*

$$\begin{array}{lcl} 0000 & \longrightarrow & 0 + 0x + 0x^2 + 0x^3 = 0 \\ 0101 & \longrightarrow & 0 + 1x + 0x^2 + 1x^3 = x + x^3 \\ 1010 & \longrightarrow & 1 + 0x + 1x^2 + 0x^3 = 1 + x^2 \\ 1111 & \longrightarrow & 1 + 1x + 1x^2 + 1x^3 = 1 + x + x^2 + x^3 \end{array}$$

En un codi cíclic, diem que el **polinomi generador** és el polinomi que representa una paraula no nul·la del codi i que

- té grau mínim,
- és mònic (el coeficient de grau més gran és 1).

Polinomi generador

Lema 2: Lema fonamental dels codis cíclics

Suposem que C és un codi cíclic de longitud n i dimensió k.
Sigui $g(x)$ un polinomi generador de C, aleshores

1. $g(x)$ és únic amb aquesta propietat.
2. $v \in C \iff v(x)$ és divisible per $g(x)$
   és a dir, les paraules del codi són els múltiples de $g(x)$.
3. $g(x)$ és un divisor de $x^n - 1$.
4. Si el polinomi generador és $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$,
   aleshores com a matriu generadora podem agafar

$$\begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & & & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & & 0 \\ 0 & 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_r \end{pmatrix}.$$

5. $g(x)$ té grau $n - k$.

Polinomi generador

Demostració

1. *Si $g(x)$ i $g'(x)$ són tots dos mònics i de grau mínim, aleshores $g(x) - g'(x)$ és un polinomi que representa una paraula del codi de grau més petit que el mínim d'entre els que representen paraules no nul·les.*
   Per tant, $g(x) - g'(x)$ ha de ser nul.

2. *D'una banda, si multipliquem $g(x)$ per un monomi x^i amb $i + \text{grau}(g) < n$, el resultat correspon a una paraula del codi.*
   D'aquí és fàcil deduir que qualsevol polinomi de la forma $g(x) \cdot f(x)$ amb grau total més petit que n pertany a C.
   Per tant, si $v(x)$, amb grau total més petit que n, és divisible per $g(x)$, aleshores $v \in C$.
   D'altra banda, suposem que v pertany al codi i que el polinomi corresponent té quocient $q(x)$ i residu $r(x)$ en dividir-lo per $g(x)$.
   Aleshores $r(x) = v(x) - q(x)g(x)$ representa una paraula del codi però té el grau més petit que $g(x)$. Per tant, ha de ser nul.
   Això vol dir que $v(x)$ és múltiple de $g(x)$.

3. *Suposem que la paraula corresponent a $g(x)$ és $(g_0, g_1, \ldots, g_{n-1})$.*
   Com que C és cíclic, $(g_{n-1}, g_0, g_1, \ldots, g_{n-2})$ ha de pertànyer a C.
   Però $g_{n-1} + g_0 x + g_1 x^2 \cdots + g_{n-2} x^{n-1} = x \cdot g(x) - g_{n-1} x^n + g_{n-1} = x \cdot g(x) - g_{n-1}(x^n - 1)$.
   Pel punt anterior sabem que $g(x)$ ha de dividir $x \cdot g(x) - g_{n-1}(x^n - 1)$ i, per tant, $g(x)$ ha de dividir $x^n - 1$.

4. *Es dedueix del punt 2.*

5. *Es dedueix del punt anterior.*

□

Polinomi generador

Recíprocament, es pot demostrar el següent:

> Qualsevol polinomi $g(x) \in \mathbb{F}_q[x]$ que divideixi $x^n - 1$ genera un codi cíclic de $\mathbb{F}_q^n$.

És a dir, si per alguns enters n i q, existeix un polinomi $g(x) = g_r x^r + g_{r-1} x^{r-1} + \cdots + g_1 x + g_0 \in \mathbb{F}_q[x]$ que divideixi $x^n - 1$, aleshores, equivalentment,

- La matriu de n columnes

$$\begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & & & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & & 0 \\ 0 & 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_r \end{pmatrix}$$

  genera un codi cíclic de $\mathbb{F}_q^n$ de dimensió $n - r$,

- El conjunt de paraules correponent al conjunt de polinomis $\{a(x)g(x) : a(x) \in \mathbb{F}_q[x], \text{ amb } \text{grau}(a(x)) < n - r\}$ és un codi cíclic de dimensió $n - r$.

Polinomi generador

Exercici 6

Considerem el codi cíclic format per les paraules $\{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2^4$.

1. Quina és la seva longitud n?
2. Doneu-ne el polinomi generador.
3. Comproveu que és un divisor de $x^n - 1$.
4. Comproveu que el seu grau és $n - k$.

Solució (p.77)

Caracterització de matrius generadores de codis cíclics

Una matriu té **forma de cascada** (de grau r) si és de la forma

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_r & 0 & & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_r & 0 & & 0 \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 & 0 \\ \vdots & & \ddots & & & & \ddots & 0 \\ 0 & \dots & & 0 & a_0 & a_1 & \dots & a_r \end{pmatrix}$$

amb $a_0 \neq 0$, $a_r \neq 0$.

Exemple

Les següents matrius de $\mathbb{Z}_7$ tenen forma de cascada.

$$\begin{pmatrix} 4 & 2 & 0 & 3 & 5 & 1 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 & 3 & 5 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 0 & 3 & 5 & 1 & 0 \\ 0 & 0 & 0 & 4 & 2 & 0 & 3 & 5 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 6 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 6 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 6 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 6 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 6 & 1 \end{pmatrix}$$

Caracterització de matrius generadores de codis cíclics

Observem que en una matriu cascada, el grau r coincideix amb la diferència entre el nombre de columnes i el nombre de files.

Observem també que, si A és una matriu cascada, aleshores $A = (Q|P)$, on

(1) Q és una matriu quadrada, triangular superior i tal que els valors dins de cada súper-diagonal coincideixen entre ells. A més, són no nuls el valor corresponent a la diagonal principal i a la r-èssima súper-diagonal, i és zero el valor de les súper-diagonals més enllà de la r-èssima.

(2) Si k és el nombre de files de A, aleshores la concatenació de a_0 amb la fila inferior de la matriu P d'una banda i la primera fila de A d'una altra banda, coincideixen en les primeres $\min(r+1, k)$ posicions.

Una matriu té **forma de precascada** si és de la forma $(Q|P)$ on Q i P satisfan les propietats (1) i (2).

En aquest cas,

$$A = \left(\begin{array}{ccccccc|ccc} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 & * & * & * \\ 0 & a_0 & a_1 & \dots & a_r & \ddots & \vdots & * & & * \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 & \vdots & & \vdots \\ \vdots & & \ddots & a_0 & & & a_r & & & \\ \vdots & & & \ddots & a_0 & & a_{r-1} & \vdots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots & * & * & * \\ 0 & \dots & \dots & \dots & & 0 & a_0 & a_1 & \dots & a_r \end{array}\right) \text{ si } r < k$$

o bé

$$A = \left(\begin{array}{ccccccc|cccc} a_0 & a_1 & \dots & & & & a_{k-1} & * & * & * & * \\ 0 & a_0 & a_1 & \dots & & & a_{k-2} & * & & & * \\ 0 & 0 & a_0 & a_1 & \dots & & a_{k-3} & \vdots & & & \vdots \\ \vdots & & \ddots & a_0 & & & & & & & \\ \vdots & & & \ddots & a_0 & & & \vdots & & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots & * & * & * & * \\ 0 & \dots & \dots & \dots & & 0 & a_0 & a_1 & \dots & \dots & a_r \end{array}\right) \text{ si } r \geq k$$

amb $a_0 \neq 0$, $a_r \neq 0$.

Si $a_0 = 1$ diem que la matriu té forma de **precascada normalitzada**.

Caracterització de matrius generadores de codis cíclics

Exemple

Vegem com podem convertir una matriu com ara $A = \begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}$ *definida sobre* $\mathbb{F}_7$*, en una matriu equivalent en forma de precascada normalitzada.*

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim \begin{matrix} \\ f_1' = f_1 + 3f_2 \\ \\ \end{matrix} \begin{pmatrix} 1 & 3 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 5 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim \begin{matrix} f_1' = f_1 + 4f_3 \\ f_2' = f_2 + 3f_3 \\ \\ \end{matrix} \begin{pmatrix} 1 & 3 & 4 & 6 & 4 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}$$

Caracterització de matrius generadores de codis cíclics

Qualsevol matriu que sigui equivalent a una matriu de la forma $(I|P)$, serà també equivalent a una *única* matriu en forma de precascada normalitzada.
En efecte, diguem $a_0 = 1$ i sigui $a_1, \ldots, a_r$ la darrera fila de P. Definim

$$Q = \begin{pmatrix} a_0 & a_1 & \ldots & a_r & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_r & \ddots & \vdots \\ 0 & 0 & a_0 & a_1 & \ldots & a_r & 0 \\ \vdots & & \ddots & a_0 & & & a_r \\ \vdots & & & \ddots & a_0 & & a_{r-1} \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & \ldots & & 0 & a_0 \end{pmatrix} \text{ si } r < k \qquad \text{o bé} \qquad Q = \begin{pmatrix} a_0 & a_1 & \ldots & & & a_{k-1} \\ 0 & a_0 & a_1 & \ldots & & a_{k-2} \\ 0 & 0 & a_0 & a_1 & \ldots & a_{k-3} \\ \vdots & & \ddots & a_0 & & \\ \vdots & & & \ddots & a_0 & \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & \ldots & & 0 & a_0 \end{pmatrix} \text{ si } r \geq k$$

El producte de matrius $Q(I \mid P)$ és equivalent també a $(I \mid P)$ i té forma de precascada normalitzada.

Exemple

En l'exemple anterior tindríem $Q = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$

i $QA = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 & 6 & 4 \\ 0 & 1 & 3 & 2 & 5 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}.$

Caracterització de matrius generadores de codis cíclics

Lema 3

El codi lineal generat per una matriu G de k files i n columnes és cíclic si i només si es compleixen les tres condicions següents:

- G és sistematitzable en les primeres posicions (és a dir, $G \sim (I \mid P)$ per una (única) matriu P, de mida $k \times (n-k)$).
- La matriu en forma de precascada normalitzada equivalent a G és una matriu cascada.
- Si $a_1, \ldots, a_{n-k}$ és la darrera fila de P, el polinomi $1 + a_1 x + \cdots + a_{n-k} x^{n-k}$ divideix $x^n - 1$.

En aquest cas, el polinomi generador del codi és $a_{n-k}^{-1}(1 + a_1 x + \cdots + a_{n-k} x^{n-k})$.

Caracterització de matrius generadores de codis cíclics

Exercici 7

Quina o quines de les següents matrius sobre $\mathbb{F}_7$ generen un codi cíclic?

1. $G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

2. $G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

3. $G_3 = \begin{pmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

Solució (p.78)

Codis cíclics primitius

Si un codi està definit sobre $\mathbb{F}_q$ i la seva longitud és $n = q-1$, aleshores diem que el codi és **primitiu**.

Exercici 8

Demostreu que en aquest cas $x - \beta$ divideix $x^n - 1$ per a tot $\beta \in \mathbb{F}_q^*$.

Solució (p.81)

Exercici 9

Demostreu que si $\alpha_1, \ldots, \alpha_r$ són elements de $\mathbb{F}_q \setminus \{0\}$ diferents entre ells, aleshores $(x-\alpha_1)\cdots\cdots(x-\alpha_r)$ és el polinomi generador d'un codi cíclic primitiu definit a $\mathbb{F}_q$.

Solució (p.82)

Codis cíclics primitius

L'interès dels codis primitius és precisament una conseqüència del darrer exercici.

Per construir un codi cíclic sobre $\mathbb{F}_q$, podem agafar $n = q - 1$, i uns quants elements diferents de $\mathbb{F}_q$, que anomenem $\alpha_1, \alpha_2, \ldots, \alpha_r$. Aleshores el polinomi $(x - \alpha_1) \cdot (x - \alpha_2) \cdot \cdots \cdot (x - \alpha_r)$ sabem que és el polinomi generador d'un codi cíclic.

Exemple

Per construir un codi cíclic sobre $\mathbb{F}_{11} = \mathbb{Z}_{11}$, podem agafar el polinomi

$$\begin{aligned}(x-3)(x-6)(x-10) &= x^3 + (-3-6-10)x^2 + \\ &\quad ((-3)(-6) + (-3)(-10) + (-6)(-10))x + (-3)(-6)(-10) \\ &= x^3 + 3x^2 + (7+8+5)x + 7 \\ &= x^3 + 3x^2 + 9x + 7,\end{aligned}$$

que dividirà $x^{10} - 1$ per l'exercici anterior. Per tant, és el polinomi generador d'un codi cíclic.
Quina serà la seva matriu generadora?

$$\begin{pmatrix} 7 & 9 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 7 & 9 & 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 7 & 9 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 9 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 7 & 9 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 7 & 9 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 & 9 & 3 & 1 \end{pmatrix}$$

Codis cíclics primitius

Exemple

Per construir un codi cíclic sobre $\mathbb{F}_9 = \mathbb{Z}_3/(x^2+2x+2)$*, considerem que* α *sigui la classe de* x*. Tindrem*

$$\begin{aligned}
\alpha^2 &= \alpha + 1 \\
\alpha^3 &= \alpha^2 + \alpha = 2\alpha + 1 \\
\alpha^4 &= 2\alpha^2 + \alpha = 2 \\
\alpha^5 &= 2\alpha \\
\alpha^6 &= 2\alpha^2 = 2\alpha + 2 \\
\alpha^7 &= 2\alpha^2 + 2\alpha = \alpha + 2 \\
\alpha^8 &= \alpha^2 + 2\alpha = 1
\end{aligned}$$

Com que $\alpha, \alpha^2, \alpha^3$ *són tots diferents, considerem el polinomi*

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

Sabem segur (per l'exercici) que aquest polinomi dividirà $x^8 - 1$ *i, per tant, serà el polinomi generador d'un codi cíclic. Quina serà la seva matriu generadora?*

$$\begin{pmatrix}
\alpha^2 & \alpha & \alpha^3 & 1 & 0 & 0 & 0 & 0 \\
0 & \alpha^2 & \alpha & \alpha^3 & 1 & 0 & 0 & 0 \\
0 & 0 & \alpha^2 & \alpha & \alpha^3 & 1 & 0 & 0 \\
0 & 0 & 0 & \alpha^2 & \alpha & \alpha^3 & 1 & 0 \\
0 & 0 & 0 & 0 & \alpha^2 & \alpha & \alpha^3 & 1
\end{pmatrix}$$

Polinomi de control

Si C és un codi cíclic de longitud n i polinomi generador $g(x)$, aleshores el **polinomi de control** de C es defineix com

$$h(x) = \frac{x^n - 1}{g(x)}.$$

El polinomi de control compleix que

$$v(x) \in C \iff v(x)h(x) = 0 \mod x^n - 1.$$

Polinomi de control

Exercici 10

1. Demostreu que $g = x^4 + 4x^3 + 6x + 3$ genera un codi cíclic primitiu sobre $\mathbb{F}_7 = \mathbb{Z}_7$.
2. Doneu-ne el polinomi de control.
3. Quina longitud i quina dimensió té aquest codi?
4. Doneu-ne una matriu generadora.
5. Es pot deduir la distància mínima a partir de la matriu generadora?
6. Corregiu la paraula següent amb esborralls: $(???235)$.
7. Comproveu si la paraula obtinguda en l'apartat anterior pertany al codi mitjançant el polinomi de control.

Solució (p.83)

Polinomi de control

Exercici 11

Sobre $\mathbb{F}_2$ considerem la matriu

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

1. Demostreu que el codi generat per G és cíclic.
2. Trobeu els polinomis generador i de control.

Solució (p.88)

Matriu de control d'un codi cíclic

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

1. A partir d'una matriu generadora sistemàtica, $G = (I|P)$,

$$H_1 = (-P^T|I).$$

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

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

3 Si g té $n-k$ arrels $\beta_1, \beta_2, \ldots, \beta_{n-k}$, totes elles diferents,

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

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

Matriu de control d'un codi cíclic

Justificació de la segona matriu de control

Suposem que $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$ *i* $h(x) = h_0 + h_1 x + \cdots + h_k x^k$.

Sabem que $c(x)$ *és una paraula del codi si i només si* $c(x)h(x) = 0 \mod x^n - 1$.

Com que el grau de $c(x)h(x)$ *és com a molt* $n + k - 1$, *alsehores* $c(x)h(x)$ *serà un producte* $(x^n - 1)p(x)$ *amb* $p(x)$ *un polinomi de grau com a molt* $k - 1$.

Però en aquest cas, $(x^n - 1)p(x)$ *és la suma de* $-p(x)$ *que només té coeficients de graus entre* 0 *i* $k - 1$ *i de* $x^n p(x)$ *que només té coeficients de graus entre* n *i* $n + k - 1$.

Per això els coeficients de $c(x)h(x)$ *de graus entre* k *i* $n - 1$ *seran tots nuls. Ara només queda observar que el coeficients de graus* k *fins a* $n - 1$ *són, respectivament,*

$$\text{grau } k: \quad c_0 h_k + c_1 h_{k-1} + \cdots + c_k h_0 = \begin{pmatrix} h_k & \ldots & h_0 & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$\text{grau } k+1: \quad c_1 h_k + c_2 h_{k-1} + \cdots + c_{k+1} h_0 = \begin{pmatrix} 0 & h_k & \ldots & h_0 & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$\vdots$$

$$\text{grau } n-1: \quad c_{n-k-1} h_k + c_{n-k} h_{k-1} + \cdots + c_{n-1} h_0 = \begin{pmatrix} 0 & \ldots & 0 & h_k & \ldots & h_0 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

Matriu de control d'un codi cíclic

Justificació de la tercera matriu de control

Suposem que $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$.

Sabem que $c(x)$ *és una paraula del codi si i només si és divisibl per* $g(x)$.

Per això, si $g(x) = (x - \beta_1) \cdot \cdots \cdot (x - \beta_{n-k})$, *aleshores* $\beta_1, \ldots, \beta_{n-k}$ *han de ser arrels de* $c(x)$.

I, per això, $c(\beta_1) = c(\beta_2) = \cdots = c(\beta_{n-k}) = 0$.

Però resulta que

$$
\begin{aligned}
c(\beta_1) &= c_0 + c_1\beta_1 + \cdots + c_{n-1}\beta_1^{n-1} = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \ldots & \beta_1^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\
c(\beta_2) &= c_0 + c_1\beta_2 + \cdots + c_{n-1}\beta_2^{n-1} = \begin{pmatrix} 1 & \beta_2 & \beta_2^2 & \ldots & \beta_2^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\
&\vdots \\
c(\beta_{n-k}) &= c_0 + c_1\beta_{n-k} + \cdots + c_{n-1}\beta_{n-k}^{n-1} = \begin{pmatrix} 1 & \beta_{n-k} & \beta_{n-k}^2 & \ldots & \beta_{n-k}^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}
\end{aligned}
$$

Quedaria justificar que la matriu és de rang màxim. Això es dedueix de les propietats de les matrius de Vandermonde.

Codificació sistemàtica de codis cíclics

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.

Codificació sistemàtica de codis cíclics

Exercici 12

Considerem el codi cíclic generat per $g = x^4 + 4x^3 + 6x + 3$ sobre $\mathbb{F}_7 = \mathbb{Z}_7$. Codifiqueu de forma sistemàtica la informació (11) mitjançant el polinomi generador.

Solució (p.90)

Distància mínima prevista

Sigui α un element primitiu de $\mathbb{F}_q$. Sigui C un codi de $\mathbb{F}_q^n$.
La **distància mínima prevista** de C és el màxim enter δ tal que hi ha $\delta - 1$ arrels de g que són potències consecutives de α ($\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$).

Lema 4

Es compleix que, si d és la distància mínima real del codi, aleshores $d \geq \delta$.

Distància mínima prevista

Demostració

Considerem la matriu

$$\begin{pmatrix} 1 & \alpha^b & (\alpha^b)^2 & (\alpha^b)^3 & \dots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & (\alpha^{b+1})^3 & \dots & (\alpha^{b+1})^{n-1} \\ \vdots & & & & & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & (\alpha^{b+\delta-2})^3 & \dots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix}$$

Les seves primeres $\delta - 1$ columnes formen una matriu de Vandermonde transposada. Les seves files són per tant, linealment independents i, a més, són del codi dual. Per àlgebra lineal sabem que podem completar el conjunt d'aquestes files obtenint una base del codi dual o, equivalentment, les files d'una matriu de control de C.

Acabarem la demostració veient que qualsevol conjunt de $\delta - 1$ columnes d'aquesta matriu de control són linealment independents. Suposem que prenem les columnes corresponents als exponents $i_1, \dots, i_{\delta-1}$, amb tots aquests exponents entre 0 i $n-1$. Les primeres $\delta - 1$ files de la matriu formada per aquest subconjunt de $\delta - 1$ columnes és de la forma

$$\begin{pmatrix} (\alpha^b)^{i_1} & (\alpha^b)^{i_2} & \dots & (\alpha^b)^{i_{\delta-1}} \\ (\alpha^{b+1})^{i_1} & (\alpha^{b+1})^{i_2} & \dots & (\alpha^{b+1})^{i_{\delta-1}} \\ \vdots & & & \vdots \\ (\alpha^{b+\delta-2})^{i_1} & (\alpha^{b+\delta-2})^{i_2} & \dots & (\alpha^{b+\delta-2})^{i_{\delta-1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \vdots & & & \vdots \\ \alpha^{i_1(\delta-2)} & \alpha^{i_2(\delta-2)} & \dots & \alpha^{i_{\delta-1}(\delta-2)} \end{pmatrix} \begin{pmatrix} \alpha^{bi_1} & 0 & \dots & 0 \\ 0 & \alpha^{bi_2} & \ddots & \vdots \\ \vdots & \ddots & & 0 \\ 0 & \dots & 0 & \alpha^{bi_{\delta-1}} \end{pmatrix},$$

que és de rang $\delta - 1$ si α és primitiu, ja que la primera matriu és Vandermonde amb totes les arrels diferents, mentres que la segona és diagonal sense zeros a la diagonal.

□

Exercici 13

Considerem el codi sobre $\mathbb{F}_2$ generat per la matriu

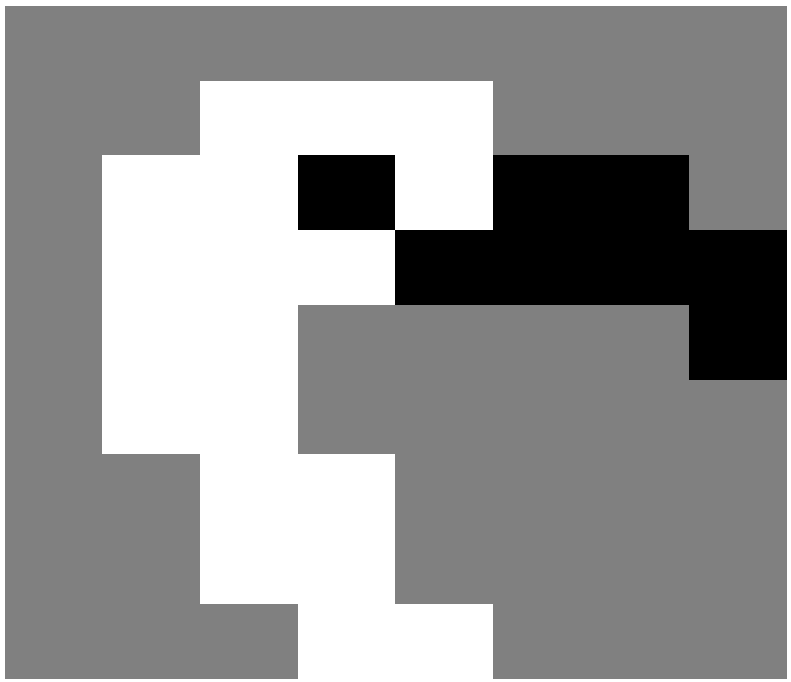
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

1. Trobeu una matriu de control de dues maneres diferents.
2. Quina és la distància mínima?
3. Codifiqueu de manera sistemàtica la informació 10110 mitjançant divisió de polinomis.

Solució (p.91)

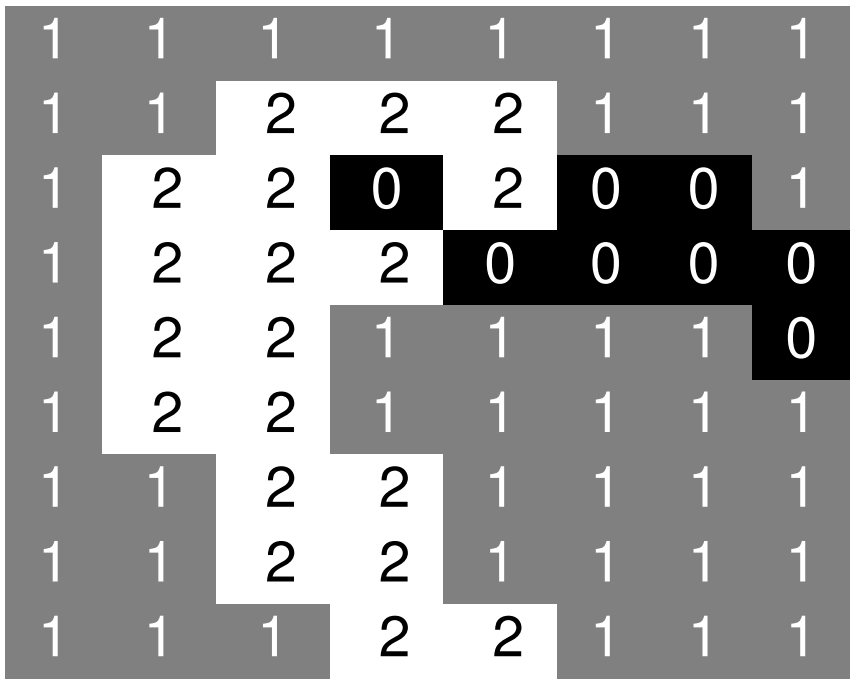
Exemple de codificació i descodificació amb un codi cíclic

Suposem una imatge digital.



Exemple de codificació i descodificació amb un codi cíclic

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

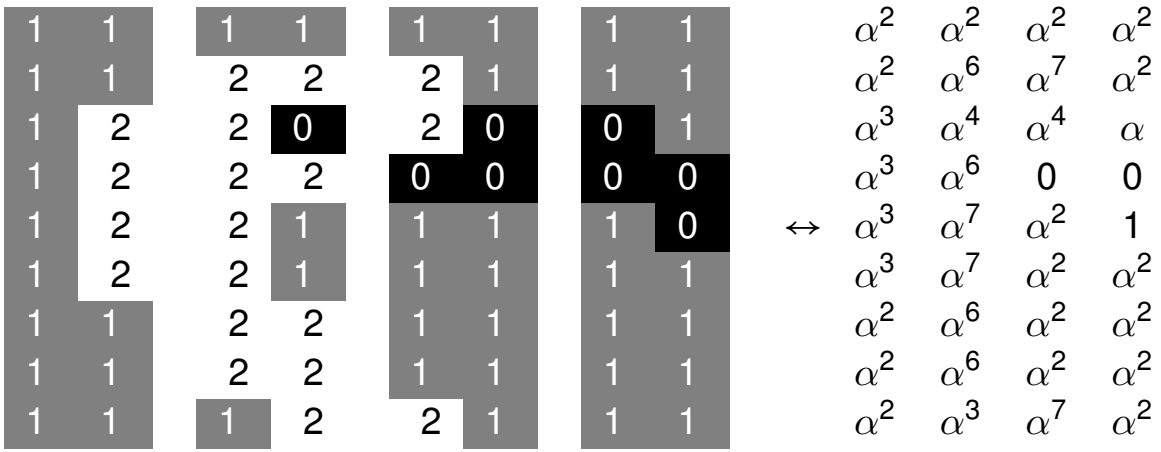


Exemple de codificació i descodificació amb un codi cíclic

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	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

Exemple de codificació i descodificació amb un codi cíclic



Exemple de codificació i descodificació amb un codi cíclic

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.

La distància mínima prevista és 5. D'acord amb la fita de Singleton, podem concloure que aquest codi té distància mínima 5.

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 (que correspon a un polinomi de grau 7).

Els polinomis corresponents a la imatge són

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

Codificació directa I

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 $\alpha^4+\alpha x+\alpha x^2+\alpha^4 x^3+\alpha^5 x^4+\alpha^6 x^5+\alpha x^6+\alpha^2 x^7$.

Codificació directa II - detalls dels càlculs

$$i(x)g(x) = \alpha^2 g(x) + \alpha^3 x g(x) + \alpha^7 x^2 g(x) + \alpha^2 x^3 g(x)$$

$$\begin{aligned}
\alpha^2 g(x) &= \alpha^2 x^4 + \alpha^8 x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4 \\
&= \alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4 \\
\alpha^3 x g(x) &= \alpha^3 x^5 + \alpha^9 x^4 + \alpha^3 x^3 + \alpha^6 x^2 + \alpha^5 x \\
&= \alpha^3 x^5 + \alpha x^4 + \alpha^3 x^3 + \alpha^6 x^2 + \alpha^5 x \\
\alpha^7 x^2 g(x) &= \alpha^7 x^6 + \alpha^{13} x^5 + \alpha^7 x^4 + \alpha^{10} x^3 + \alpha^9 x^2 \\
&= \alpha^7 x^6 + \alpha^5 x^5 + \alpha^7 x^4 + \alpha^2 x^3 + \alpha x^2 \\
\alpha^2 x^3 g(x) &= \alpha^2 x^7 + \alpha^8 x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha^4 x^3 \\
&= \alpha^2 x^7 + x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha^4 x^3
\end{aligned}$$

Codificació directa III - detalls dels càlculs

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

Ara, fent servir la taula de correspondència, escrivim cada potència de α en notació vectorial i fem la suma. Per exemple, el coeficient de x^6 es correspon a

$$1 + \alpha^7 \to (1,0) + (2,1) = (0,1) \to \alpha$$

El resultat és

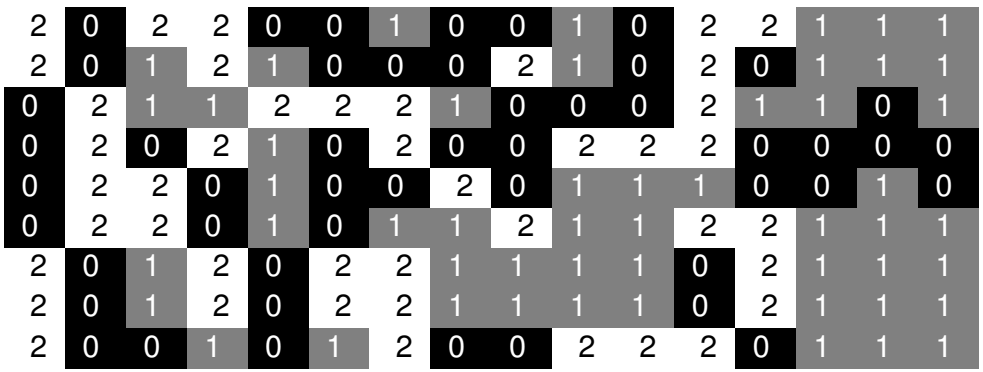
$$\alpha^4+\alpha x+\alpha x^2+\alpha^4 x^3+\alpha^5 x^4+\alpha^6 x^5+\alpha x^6+\alpha^2 x^7.$$

Codificació directa IV

Fem ara el mateix amb totes les files:

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

$\leftrightarrow$



Codificació sistemàtica I

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

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

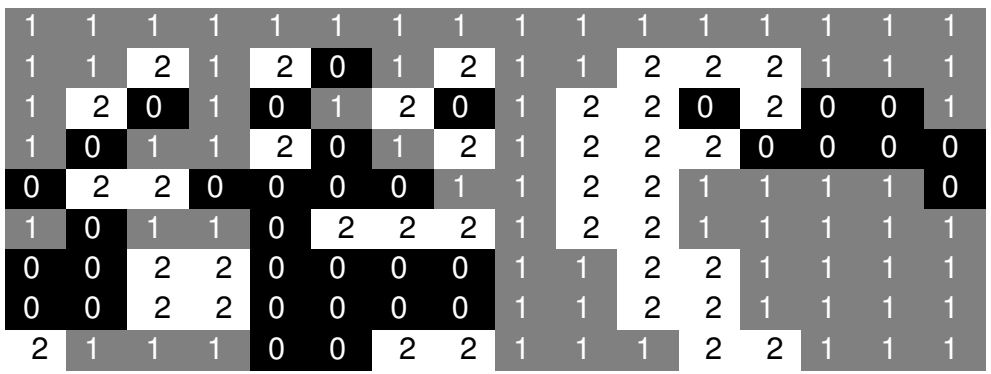
que correspon a la imatge

Codificació sistemàtica II

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

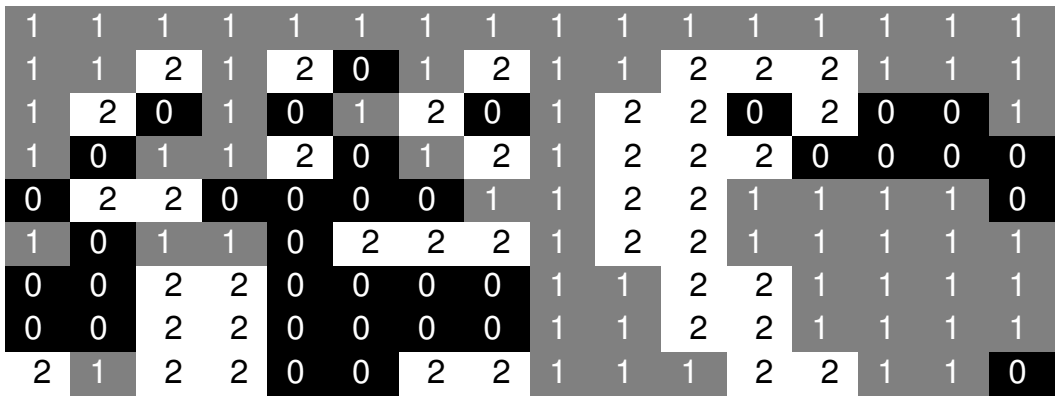
$\leftrightarrow$



Observem que, en aquest cas, la imatge original queda replicada en les darreres posicions.

Correcció d'errors I

Suposem ara que aquesta imatge s'ha enviat i que el canal de transmissió ha generat certs errors.



El receptor genera una matriu de control per verificar si hi ha hagut errors. El polinomi de control és
$h(x) = \frac{x^n-1}{g} = x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2$.

Correcció d'errors II

Per tant, podem agafar com a matriu de control

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

En multiplicar les primeres 8 paraules per H, s'obté el vector nul.
Però, en multiplicar la darrera per H, obtenim

$$\begin{pmatrix} 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \end{pmatrix} \begin{pmatrix} \alpha^7 \\ \alpha^6 \\ 0 \\ \alpha^6 \\ \alpha^2 \\ \alpha^3 \\ \alpha^7 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ \alpha^2 \\ 0 \\ \alpha^7 \end{pmatrix}.$$

Correcció d'errors III

Si fos associat a un vector d'error de pes 1, la síndrome seria múltiple d'una columna. Comprovem que no és així. Busquem una combinació lineal de dues columnes que doni aquesta síndrome. Observem que

$$\begin{pmatrix} \alpha^4 \\ \alpha^2 \\ 0 \\ \alpha^7 \end{pmatrix} = \alpha^2 H^2 + \alpha^5 H^8.$$

Per tant, considerarem que 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 $\alpha^2\alpha^3\alpha^7\alpha^2$.

Solució de l'Exercici 1

1. A $\mathbb{F}_7$,

$$V_4(6,5,4,3) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 6 & 5 & 4 & 3 \\ 6^2 & 5^2 & 4^2 & 3^2 \\ 6^3 & 5^3 & 4^3 & 3^3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 6 & 5 & 4 & 3 \\ 1 & 4 & 2 & 2 \\ 6 & 6 & 1 & 6 \end{pmatrix}.$$

2. Anomenem $A = V_4(6,5,4,3)$. Els seus menors corresponents a la primera fila seran

$$A_{11} = \det\begin{pmatrix} 5 & 4 & 3 \\ 4 & 2 & 2 \\ 6 & 1 & 6 \end{pmatrix} = 60 + 12 + 48 - 36 - 10 - 96 = 4 + 5 + 6 - 1 - 3 - 5 = 6$$

$$A_{12} = \det\begin{pmatrix} 6 & 4 & 3 \\ 1 & 2 & 2 \\ 6 & 1 & 6 \end{pmatrix} = 72 + 3 + 48 - 36 - 12 - 24 = 2 + 3 + 6 - 1 - 5 - 3 = 2$$

$$A_{13} = \det\begin{pmatrix} 6 & 5 & 3 \\ 1 & 4 & 2 \\ 6 & 6 & 6 \end{pmatrix} = 144 + 18 + 60 - 72 - 72 - 30 = 4 + 4 + 4 - 2 - 2 - 2 = 6$$

$$A_{14} = \det\begin{pmatrix} 6 & 5 & 4 \\ 1 & 4 & 2 \\ 6 & 6 & 1 \end{pmatrix} = 24 + 24 + 60 - 96 - 72 - 5 = 3 + 3 + 4 - 5 - 2 - 5 = 5.$$

Per tant, $\det(A) = 1 \cdot A_{11} - 1 \cdot A_{12} + 1 \cdot A_{13} - 1 \cdot A_{14} = 6 - 2 + 6 - 5 = 5$.

3. Fent servir el lema,

$$\det(A) = (3-4)(3-5)(3-6)(4-5)(4-6)(5-6) == (-1)(-2)(-3)(-1)(-2)(-1) = 12 = 5.$$

Corroborem, per tant, que coincideixen.

Torna a l'exercici (p.10)

Solució de l'Exercici 2

0	0
1	1
α	α
α^2	$\alpha+1$
α^3	$\alpha^2+\alpha=2\alpha+1$
α^4	$2\alpha^2+\alpha=2$
α^5	2α
α^6	$2\alpha^2=2\alpha+2$
α^7	$2\alpha^2+2\alpha=\alpha+2$
α^8	$\alpha^2+2\alpha=1$

1. $V_4(\alpha,\alpha^3,\alpha^5,\alpha^7)=\begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^5 & \alpha^7 \\ (\alpha)^2 & (\alpha^3)^2 & (\alpha^5)^2 & (\alpha^7)^2 \\ (\alpha)^3 & (\alpha^3)^3 & (\alpha^5)^3 & (\alpha^7)^3 \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^5 & \alpha^7 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha & \alpha^7 & \alpha^5 \end{pmatrix}.$
2. Anomenem $A=V_4(\alpha,\alpha^3,\alpha^5,\alpha^7)$. Els seus menors corresponents a la primera fila seran

$$\begin{aligned} A_{11} &= \det\begin{pmatrix} \alpha^3 & \alpha^5 & \alpha^7 \\ \alpha^6 & \alpha^2 & \alpha^6 \\ \alpha & \alpha^7 & \alpha^5 \end{pmatrix} \\ &= \alpha^{3+2+5}+\alpha^{5+6+1}+\alpha^{6+7+7}-\alpha^{7+2+1}-\alpha^{6+7+3}-\alpha^{6+5+5} \\ &= \alpha^2+\alpha^4+\alpha^6-\alpha^2-\alpha^2-\alpha^2 \\ &= \alpha^4+\alpha^6+\alpha^2 \\ &= (2)+(2\alpha+2)+(\alpha+1)=2 \end{aligned}$$

Solució de l'Exercici 2

i, de manera anàloga,

$$A_{12} = \det\begin{pmatrix} \alpha & \alpha^5 & \alpha^7 \\ \alpha^2 & \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^7 & \alpha^5 \end{pmatrix} = 1 + \alpha^6 + 1 - \alpha^4 - \alpha^4 - \alpha^6 = -\alpha^4 = 1,$$

$$A_{13} = \det\begin{pmatrix} \alpha & \alpha^3 & \alpha^7 \\ \alpha^2 & \alpha^6 & \alpha^6 \\ \alpha^3 & \alpha & \alpha^5 \end{pmatrix} = \alpha^4 + \alpha^4 + \alpha^2 - 1 - 1 - \alpha^2 = \alpha^4 = 2,$$

$$A_{14} = \det\begin{pmatrix} \alpha & \alpha^3 & \alpha^5 \\ \alpha^2 & \alpha^6 & \alpha^2 \\ \alpha^3 & \alpha & \alpha^7 \end{pmatrix} = \alpha^6 + 1 + 1 - \alpha^6 - \alpha^4 - \alpha^4 = -\alpha^4 = 1.$$

Per tant, $\det(A) = 1 \cdot A_{11} - 1 \cdot A_{12} + 1 \cdot A_{13} - 1 \cdot A_{14} = 2 - 1 + 2 - 1 = 2$.

3. Fent servir el lema,

$$\begin{aligned} \det(A) &= (\alpha^7 - \alpha^5)(\alpha^7 - \alpha^3)(\alpha^7 - \alpha)(\alpha^5 - \alpha^3)(\alpha^5 - \alpha)(\alpha^3 - \alpha) \\ &= (\alpha + 2 - 2\alpha)(\alpha + 2 - 2\alpha - 1)(\alpha + 2 - \alpha)(2\alpha - 2\alpha - 1)(2\alpha - \alpha)(2\alpha + 1 - \alpha) \\ &= (-\alpha + 2)(-\alpha + 1)(2)(-1)(\alpha)(\alpha + 1) \\ &= (2\alpha + 2)(2\alpha + 1)(2)(2)(\alpha)(\alpha + 1) \\ &= \alpha^6\alpha^3\alpha^4\alpha^4\alpha\alpha^2 = \alpha^{6+3+4+4+1+2} = \alpha^{20} = \alpha^4 = 2 \end{aligned}$$

Corroborem, per tant, que coincideixen.

Torna a l'exercici (p.11)

Solució de l'Exercici 3

Utilitzarem la taula

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha+1$	12
α^3	$2\alpha+2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha+2$	21
α^7	$\alpha+1$	11

Calculem el determinant per menors:

$$\det(V_4(1,\alpha,\alpha^3,\alpha^4)) = \det\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^6 & 1 \\ 1 & \alpha^3 & \alpha & \alpha^4 \end{pmatrix} =$$

$$\det\begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} - \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} + \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^4 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} - \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^6 & 1 \end{pmatrix} =$$

$$= (\alpha^3+\alpha^6+\alpha^7-\alpha^5-\alpha-\alpha^2)-(\alpha^2+\alpha^3+\alpha^3-\alpha-\alpha-\alpha^6)+(\alpha^7+\alpha^7+\alpha^2-\alpha^6-\alpha^5-\alpha^5)-(\alpha^3+\alpha^6+\alpha^7-\alpha^5-\alpha-\alpha^2) =$$

Solució de l'Exercici 3

$$= (\cancel{\alpha^3}+\cancel{\alpha^6}+\cancel{\alpha^7}-\cancel{\alpha^5}-\cancel{\alpha}-\cancel{\alpha^2})-(\cancel{\alpha^2}+\cancel{\alpha^3}+\alpha^3-\cancel{\alpha}-\alpha-\cancel{\alpha^6})+(\alpha^7+\alpha^7+\cancel{\alpha^2}-\cancel{\alpha^6}-\alpha^5-\alpha^5)-(\alpha^3+\cancel{\alpha^6}+\cancel{\alpha^7}-\cancel{\alpha^5}-\alpha-\cancel{\alpha^2}) =$$

$$= -\alpha^3+\alpha+\alpha^7+\alpha^7-\alpha^5-\alpha^5-\alpha^3+\alpha = (\alpha+\alpha)+(\alpha^7+\alpha^7)-(\alpha^3+\alpha^3)-(\alpha^5+\alpha^5) = \alpha^4\alpha+\alpha^4\alpha^7+\alpha^3+\alpha^5 =$$

$$= \alpha^5+\alpha^3+\alpha^3+\alpha^5 = (\alpha^5+\alpha^5)+(\alpha^3+\alpha^3) = \alpha+\alpha^7$$

veiem que el determinant és α^2.

Calculem el determinant pel lema:

$$(1-\alpha)(1-\alpha^3)(1-\alpha^4)(\alpha-\alpha^3)(\alpha-\alpha^4)(\alpha^3-\alpha^4) = \alpha^2\alpha^6\alpha^4\alpha^2\alpha^7\alpha^5 = \alpha^2.$$

Observem com els dos càlculs coincideixen.

Torna a l'exercici (p.11)

Solució de l'Exercici 4

1. És un subespai vectorial perquè totes les combinacions lineals de dues de les quatre paraules pertanyen al codi:

$$
\begin{array}{ccccc}
0000 & + & 0000 & = & 0000 \\
0000 & + & 0101 & = & 0101 \\
0000 & + & 1010 & = & 1010 \\
0101 & + & 0101 & = & 0000 \\
0101 & + & 1010 & = & 1111 \\
0101 & + & 1111 & = & 1010 \\
1010 & + & 1010 & = & 0000 \\
1010 & + & 1111 & = & 0101 \\
1111 & + & 1111 & = & 0000
\end{array}
$$

   Per tant, és un codi lineal.

2. La dimensió és 2 perquè és el màxim nombre de paraules linealment independents.

3. Qualsevol de les tres matrius següents és matriu generadora

$$
\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},
$$

Solució de l'Exercici 4

i també qualsevol de les anteriors intercanviant les dues files.

4. És un codi cíclic perquè qualsevol desplaçament circular de les seves paraules dona una altra paraula del codi. En efecte,
   - tots els desplaçaments circulars de 0000 donen la mateixa paraula 0000,
   - tots els desplaçaments circulars de 0101 donen la mateixa paraula 0101 o bé la paraula 1010,
   - tots els desplaçaments circulars de 1010 donen la mateixa paraula 1010 o bé la paraula 0101,
   - tots els desplaçaments circulars de 1111 donen la mateixa paraula 1111.

Torna a l'exercici (p.17)

Solució de l'Exercici 5

Com que és un codi de dimensió 7 sistemàtic en les darreres posicions, deduïm que el bloc d'informació corresponent a la paraula codi

$$\overbrace{10\ \ 1\ \ 10\ \ 0\ \ 1}^{n-k=5}\ \ \overbrace{10\ \ 0\ \ 2\ \ 8\ \ 3\ \ 9\ \ 1}^{k=7}$$

és

$$10\ \ 0\ \ 2\ \ 8\ \ 3\ \ 9\ \ 1.$$

Si volem la codificació sistemàtica de 10 0 2 8 3 9 1 en les primeres posicions, estem buscant un vector que sigui del codi i que sigui de la forma

$$(10\ 0\ 2\ 8\ 3\ 9\ 1\ r_1\ r_2\ r_3\ r_4\ r_5),$$

on r_1, r_2, r_3, r_4, r_5 ens venen donats de manera únivoca pel bloc d'informació.

Però, d'altra banda, com que el codi és cíclic, sabem que la paraula següent també és del codi: $(10\ 0\ 2\ 8\ 3\ 9\ 1\ 10\ 1\ 10\ 0\ 1)$.

Com que la codidificació del bloc d'informació és única, per força hem de tenir

$$r_1 = 10\ r_2 = 1\ r_3 = 10\ r_4 = 0\ r_5 = 1.$$

Solució de l'Exercici 5

Per tant, la paraula codi demanada ha de ser

$$(10\ 0\ 2\ 8\ 3\ 9\ 1\ 10\ 1\ 10\ 0\ 1).$$

Torna a l'exercici (p.18)

Solució de l'Exercici 6

1. La longitud és $n = 4$.
2. Els polinomis que representen les 4 paraules del codi són
   - 0,
   - $x + x^3$,
   - $1 + x^2$,
   - $1 + x + x^2 + x^3$,

   dels quals el de grau mínim sense comptar el 0 és $x^2 + 1$. Per tant, aquest és el polinomi generador del codi.
3. $$\begin{array}{rl} x^4 \quad +1 & \left| \begin{array}{l} x^2+1 \\ \hline x^2+1 \end{array} \right. \\ \underline{-(x^4+x^2\quad)} & \\ x^2+1 & \\ \underline{-(x^2+1)} & \\ 0 & \end{array}$$

   Veiem que la divisió és exacta.
4. $\text{grau}(g) = 2$ i $n - k = 4 - 2 = 2$.

Torna a l'exercici (p.24)

Solució de l'Exercici 7

1. Per analitzar G_1 i G_2, considerem $Q = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

   Observem que la forma de precascada de G_1 és

$$Q \cdot G_1 = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 0 & 5 & 2 \\ 0 & 1 & 2 & 4 & 6 & 1 \\ 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$$

   Com que la forma de precascada de G_1 no té forma de cascada, G_1 no genera un codi cíclic.

2. De la seva banda, la forma de precascada de G_2 és

$$Q \cdot G_2 = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 0 & 0 & 0 \\ 0 & 1 & 2 & 4 & 0 & 0 \\ 0 & 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$$

   En aquest cas, la forma de precascada de G_2 té forma de cascada. Per veure si G_2 genera un codi cíclic, quedarà veure si $1 + 2x + 4x^2$ divideix $x^6 - 1$.

$$\begin{array}{r} x^6 \qquad\qquad\qquad\qquad\qquad\qquad +6 \\ -(\,x^6 + 4x^5 + 2x^4 \qquad\qquad\qquad\quad) \\ \hline 3x^5 + 5x^4 \qquad\qquad\qquad\quad +6 \\ -(\,3x^5 + 5x^4 + 6x^3 \qquad\quad) \\ \hline x^3 \qquad\qquad +6 \\ -(\,x^3 + 4x^2 + 2x \qquad) \\ \hline 3x^2 + 5x + 6 \\ -(\,3x^2 + 5x + 6\,) \\ \hline 0 \end{array} \qquad \begin{array}{l|l} 4x^2 + 2x + 1 & \\ \hline 2x^4 + 6x^3 \qquad +2x + 6 & \end{array}$$

Solució de l'Exercici 7

Com que la divisió és exacta, concloem que G_2 genera un codi cíclic.

3. Consider $Q_3 = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

Observem que la forma de precascada de G_3 és

$$Q_3 \cdot G_3 = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 0 & 0 \\ 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}$$

Tornem a tenir el cas en què la forma de precascada de G_3 té forma de cascada. Per veure si G_3 genera un codi cíclic, quedarà veure si $1 + 2x + 4x^2$ divideix $x^5 - 1$.

$$\begin{array}{rl|l} x^5 & +6 & 4x^2 + 2x + 1 \\ \cline{3-3} -(x^5 + 4x^4 + 2x^3 &) & 2x^3 + 6x^2 + 2 \\ \cline{1-2} 3x^4 + 5x^3 & +6 & \\ -(3x^4 + 5x^3 + 6x^2 &) & \\ \cline{1-2} x^2 & +6 & \\ -(x^2 + 4x + 2) & & \\ \cline{1-2} 3x + 4 & & \end{array}$$

Com que en aquest cas la divisió no és exacta, G_3 tampoc generarà un codi cíclic.
Podem veure, per exemple, que la paraula (40012), que és desplaçament circular de (12400), no pertany al codi i, per tant, efectivament, el codi no pot ser cíclic.
Perquè (40012) fos paraula del codi, hauria de ser de la forma

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 & 0 & 0 \\ 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} x & 2x + y & 4x + 2y + z & 4y + 2z & 4z \end{pmatrix},$$

Solució de l'Exercici 7

és a dir, s'hauria de complir

$$\begin{aligned} x &= 4 \\ 2x + y &= 0 \\ 4x + 2y + z &= 0 \\ 4y + 2z &= 1 \\ 4z &= 2 \end{aligned}$$

que no té solució, perquè per satisfer les tres primeres igualtats ens caldria $x = 4$, $y = 6$, $z = 0$, però aleshores les altres igualtats no se satisfarien.

Torna a l'exercici (p.31)

Solució de l'Exercici 8

Si el codi és primitiu, aleshores $n = q - 1$.

Que $x - \beta$ divideixi $x^n - 1 = x^{q-1} - 1$ és equivalent al fet que β sigui una arrel de $x^{q-1} - 1$. I sabem que qualsevol element β del cos finit de q elements satisfà $\beta^{q-1} = 1$. Per tant β és arrel de $x^{q-1} - 1$.

Torna a l'exercici (p.33)

Solució de l'Exercici 9

Es dedueix de l'exercici anterior i del fet que $(x-\alpha_1),\ldots,(x-\alpha_r)$ són tots irreductibles. Torna a l'exercici (p.33)

Solució de l'Exercici 10

1. Cal demostrar que g divideix $x^6 - 1$.

$$
\begin{array}{rl}
x^6 \qquad\qquad\qquad\qquad\qquad\qquad +6 & \big| \; x^4+4x^3 \qquad +6x+3 \\
\hline
-(x^6 + 4x^5 \qquad +6x^3+3x^2 \qquad\quad) & x^2+3x+2 \\
\hline
3x^5 \qquad + x^3 +4x^2 \qquad +6 & \\
-(3x^5 + 5x^4 \qquad +4x^2+2x \quad) & \\
\hline
2x^4 + x^3 \qquad +5x+6 & \\
-(2x^4 + x^3 \qquad +5x+6) & \\
\hline
0 &
\end{array}
$$

2. El polinomi de control serà $h(x) = (x^6 - 1)/g = x^2 + 3x + 2$.
3. La longitud és $n = 6$, perquè és un codi primitiu. La dimensió la podem deduir del fet que el grau del polinomi generador, que en el nostre cas és grau$(x^4 + 4x^3 + 6x + 3) = 4$, ha de ser $n - k = 6 - k$. Per tant, $k = 2$.

Solució de l'Exercici 10

4. El polinomi generador

$$x^4 + 4x^3 + 6x + 3 = 3 + 6x + 0x^2 + 4x^3 + x^4$$

correspon a la paraula

$$(360410).$$

Pel lema fonamental dels codis cíclics, deduïm que

$$G = \begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix}$$

Solució de l'Exercici 10

5. Les paraules del codi seran combinacions lineals de les dues files de G, és a dir, tindran la forma

$$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3a & 6a+3b & 6b & 4a & a+4b & b \end{pmatrix}.$$

   - Si $a = 0$ i $b \neq 0$, aleshores el pes és 4.
   - Si $a \neq 0$ i $b = 0$, aleshores el pes és 4.
   - Si $a \neq 0$ i $b \neq 0$, aleshores el pes serà com a mínim 4, ja que $3a \neq 0$, $6b \neq 0$, $4a \neq 0$, $b \neq 0$.

   Per tant, la distància mínima ha de ser 4.

Solució de l'Exercici 10

6. La paraula $\begin{pmatrix} x & y & z & 2 & 3 & 5 \end{pmatrix}$ ha de ser de la forma

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3a & 6a+3b & 6b & 4a & a+4b & b \end{pmatrix}.$$

De la darrera posició deduïm que $b = 5$.
De la penúltima posició deduïm que

$$a + 4b = 3 \Longrightarrow a + 20 = 3 \Longrightarrow a = -17 = 21 - 17 = 4.$$

La paraula del codi serà, doncs,

$$\begin{pmatrix} 4 & 5 \end{pmatrix} \begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 4 & 2 & 2 & 3 & 5 \end{pmatrix}.$$

Solució de l'Exercici 10

7. Multipliquem el polinomi corresponent a la paraula (542235) pel polinomi de control i comprovem si ens dona 0 mod $x^n - 1$.
   D'una banda,

$$(5 + 4x + 2x^2 + 2x^3 + 3x^4 + 5x^5)(x^2 + 3x + 2) = 5x^7 + 4x^6 + 2x + 3.$$

   Si ara dividim $5x^7 + 4x^6 + 2x + 3$ entre $x^6 - 1$ ens dona quocient $5x + 4$ i residu 0:

$$\begin{array}{rl|l} 5x^7 + 4x^6 + 2x + 3 & & x^6 + 6 \\ \cline{3-3} -(5x^7 + 2x) & & 5x + 4 \\ \cline{1-1} 4x^6 + 3 & & \\ -(4x^6 + 3) & & \\ \cline{1-1} 0 & & \end{array}$$

Torna a l'exercici (p.38)

Solució de l'Exercici 11

1. Es pot veure que

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \sim \begin{array}{l} f_1' = f_1 + f_2 + f_3 + f_4 \\ f_2' = f_2 + f_3 + f_4 + f_5 \\ f_3' = f_3 + f_4 + f_5 \\ f_4' = f_4 + f_5 \\ f_5' = f_5 \end{array}$$

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

Observem que aquesta matriu té forma de cascada i correspon al polinomi $x^3 + x^2 + x + 1$. Si veiem que aquest polinomi divideix $x^n - 1$, aleshores haurem demostrat que es tracta d'un codi cíclic.

$$\begin{array}{rl|l} x^8 & +1 & x^3 + x^2 + x + 1 \\ \cline{3-3} -(x^8 + x^7 + x^6 + x^5 &) & x^5 + x^4 + x + 1 \\ \cline{1-2} x^7 + x^6 + x^5 & +1 & \\ -(x^7 + x^6 + x^5 + x^4 &) & \\ \cline{1-2} x^4 & +1 & \\ -(x^4 + x^3 + x^2 + x &) & \\ \cline{1-2} x^3 + x^2 + x + 1 & & \\ -(x^3 + x^2 + x + 1) & & \\ \cline{1-2} 0 & & \end{array}$$

En efecte, la divisió és exacta.

Solució de l'Exercici 11

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

Torna a l'exercici (p.39)

Solució de l'Exercici 12

El residu de dividir $i(x)x^{n-k} = x^4 + x^5$ entre g és $R(x) = 5x^3 + x^2 + x + 2$:

$$\begin{array}{rl|l} x^5 + x^4 & & x^4+4x^3+6x+3 \\ \cline{3-3} -(x^5 + 4x^4 + 6x^2+3x) & & x + 4 \\ \cline{1-1} 4x^4 + x^2 + 4x & & \\ -(4x^4+2x^3 + 3x+5) & & \\ \cline{1-1} 5x^3 + x^2 + x + 2 & & \end{array}$$

Aleshores $i(x)x^{n-k} - R(x)$ correspon a la paraula codi 566211.

Torna a l'exercici (p.46)

Solució de l'Exercici 13

1. A la solució de l'exercici 11 hem vist que aquest és un codi cíclic i generat per $g(x) = 1 + x + x^4 + x^5$. Per tant, podem trobar una matriu de control fent la transformació genèrica de les matrius generadores del tipus $G = (I|P)$ (com aquesta), i fent servir el polinomi de control $h(x) = x^5 + x^4 + x + 1$. En el primer cas obtenim la matriu de control

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

En el segon cas, com que $h^*(x) = 1 + x + x^4 + x^5$, obtenim la matriu de control

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

Solució de l'Exercici 13

2. La distància mínima és 2 perquè a H hi ha dues columnes dependents.
3. La informació que cal codificar és $i = 10110$, que es correspon al polinomi $i(x) = 1 + x^2 + x^3$. Com que $n - k = 3$, $i(x)x^{n-k} = x^6 + x^5 + x^3$. Dividim aquest polinomi per $g(x)$ i obtenim quocient $x^3 + x + 1$ i residu 1. Per tant, $i(x)x^{n-k} - R(x) = x^6 + x^5 + x^3 + 1$, que es correspon amb la paraula 10010110.

Torna a l'exercici (p.50)

Apèndix: Repàs de determinants

El **determinant** és una valor que associem a una matriu quadrada A i que denotem per $\det(A)$ o $|A|$. En els casos en què el nombre de files sigui com a molt 3 tenim les fórmules següents:

$$\det\begin{pmatrix} a_{11} \end{pmatrix} = a_{11},$$

$$\det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{12}a_{23}a_{31} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}.$$

Per exemple,

$$\det\begin{pmatrix} 4 \end{pmatrix} = 4,$$

$$\det\begin{pmatrix} 4 & 5 \\ 2 & 7 \end{pmatrix} = 28 - 10 = 18,$$

$$\det\begin{pmatrix} 4 & 5 & 0 \\ 2 & 7 & 9 \\ 8 & 6 & 1 \end{pmatrix} = 28 + 0 + 360 - 216 - 0 - 10 = 162.$$

Apèndix: Repàs de determinants

Per a casos més grans, definim el **menor** complementari d'a_{ij}, que denotem A_{ij}, com el determinant de la matriu que obtenim eliminant la fila i-èssima i la columna j-èssima de A. Aleshores podem calcular el determinant de A per alguna de les fórmules equivalents següents.
Desenvolupament de menors per files:

$$\begin{aligned}
\det(A) &= a_{11}A_{11} - a_{12}A_{12} + a_{13}A_{13} - a_{14}A_{14} + \dots \\
&= -a_{21}A_{21} + a_{22}A_{22} - a_{23}A_{23} + a_{24}A_{24} - \dots \\
&= a_{31}A_{31} - a_{32}A_{32} + a_{33}A_{33} - a_{34}A_{34} + \dots \\
&= -a_{41}A_{41} + a_{42}A_{42} - a_{43}A_{43} + a_{44}A_{44} - \dots \\
&\vdots
\end{aligned}$$

O bé desenvolupament de menors per columnes:

$$\begin{aligned}
\det(A) &= a_{11}A_{11} - a_{21}A_{21} + a_{31}A_{31} - a_{41}A_{41} + \dots \\
&= -a_{12}A_{12} + a_{22}A_{22} - a_{32}A_{32} + a_{42}A_{42} - \dots \\
&= a_{13}A_{13} - a_{23}A_{23} + a_{33}A_{33} - a_{43}A_{43} + \dots \\
&= -a_{14}A_{14} + a_{24}A_{24} - a_{34}A_{34} + a_{44}A_{44} - \dots \\
&\vdots
\end{aligned}$$

Relacionat: determinant d'una matriu Vandermonde (p.8)

Apèndix: Repàs de determinants

Una matriu quadrada és invertible si i només si el seu determinant és diferent de zero.

Així, un sistema d'equacions on la matriu del sistema sigui una matriu quadrada amb determinant diferent de zero, tindrà solució i la solució serà única.

Apèndix: Repàs de més nocions de matrius

Una matriu és **quadrada** si té tantes files com columnes. La **diagonal principal** d'una matriu quadrada està formada pel primer element de la primera fila, el segon element de la segona fila, el tercer element de la tercera fila, i així fins al darrer element de la darrera fila. Una matriu quadrada és **triangular superior (o inferior)** si tots els elements que es troben per sota (o per sobre) de la diagonal principal són nuls. La primera súper-diagonal (o sub-diagonal) d'una matriu quadrada són els elements que es troben just a sobre (sota) de la diagonal principal. La segona súper-diagonal (o sub-diagonal) d'una matriu quadrada són els elements que es troben just a sobre (sota) de la primera súper-diagonal (sub-diagonal). I així es defineixen successivament totes les **súper-diagonals (o sub-diagonals)**. Per exemple, la matriu següent és triangular superior, la seva primera súper-diagonal és $1,9$ i la seva segona súper-diagonal és 4:

$$\begin{pmatrix} 8 & 1 & 4 \\ 0 & 7 & 9 \\ 0 & 0 & 1 \end{pmatrix}.$$

Relacionat: matrius precascada (p.27)