Teoria de codis: codis lineals

Maria Bras-Amorós, Oriol Farràs Ventura

21 de desembre de 2023

Motivació

Codis lineals

Detecció i correcció d'errors

Solucions

Apèndix: Repàs d'àlgebra lineal i matrius

Motivació

Codis lineals

Detecció i correcció d'errors

Solucions

Apèndix: Repàs d'àlgebra lineal i matrius

Comunicació amb errors

Suposem que en una comunicació amb molt de soroll ambiental s'han de comunicar una de les paraules

CERT o **FALS**.

Comunicació amb errors

Suposem que en una comunicació amb molt de soroll ambiental s'han de comunicar una de les paraules

CERT o **FALS**.

Si el receptor rep la paraula

CART,

quina paraula deduiríeu que s'ha enviat?

Comunicació amb errors

Suposem que en una comunicació amb molt de soroll ambiental s'han de comunicar una de les paraules

CERT o **FALS**.

Si el receptor rep la paraula

CART,

quina paraula deduiríeu que s'ha enviat?

CERT $\rightarrow$**CART**.

En aquest cas podem dir que s'ha produït **un error**.

Teoria de codis

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

Teoria de codis

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

FALS →**??LS**

En aquest cas podem dir que s'han produït **dos esborralls**.

Teoria de codis

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

FALS →**??LS**

En aquest cas podem dir que s'han produït **dos esborralls**.

I si rebem

CALT,

podem deduir què s'ha enviat?

Teoria de codis

La teoria de codis gira al voltant d'aquesta problemàtica.

El conjunt

$$\{CERT, FALS\}$$

seria un codi que permetria transmetre dues paraules.

Podríem corregir un sol error en cada paraula i fins a tres esborralls.

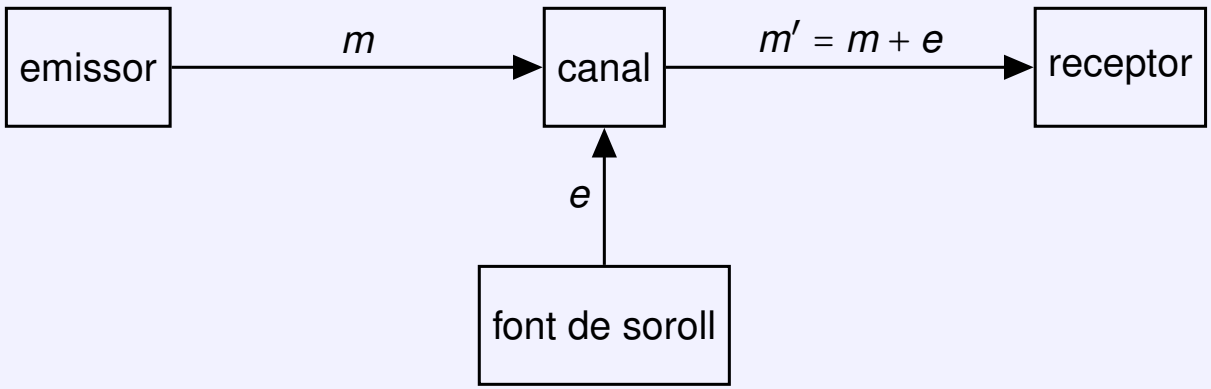
Veurem exemples més grans, però, sobretot, dotats d'estructures més potents.

Aquestes estructures ens permetran transmetre qualsevol seqüència de missatges a través d'un procés de codificació i ens permetran predir quants errors i quants esborralls es poden produir, de manera que es puguin corregir i, finalment, ens donaran eines per corregir i per tornar a descodificar i obtenir així la informació original.

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Model

En general, per abordar el problema de l'exemple, es pot considerar el model de la figura. Un **emissor** envia un missatge m a un **receptor** a través d'un **canal** de comunicació en el qual hi ha cert **soroll**. El receptor rep $m' = m + e$, on e és soroll.



m: missatge enviat, m': missatge rebut, e: soroll

Comunicacions

Perquè la comunicació sigui satisfactòria, el que volem és que el receptor pugui conèixer m.

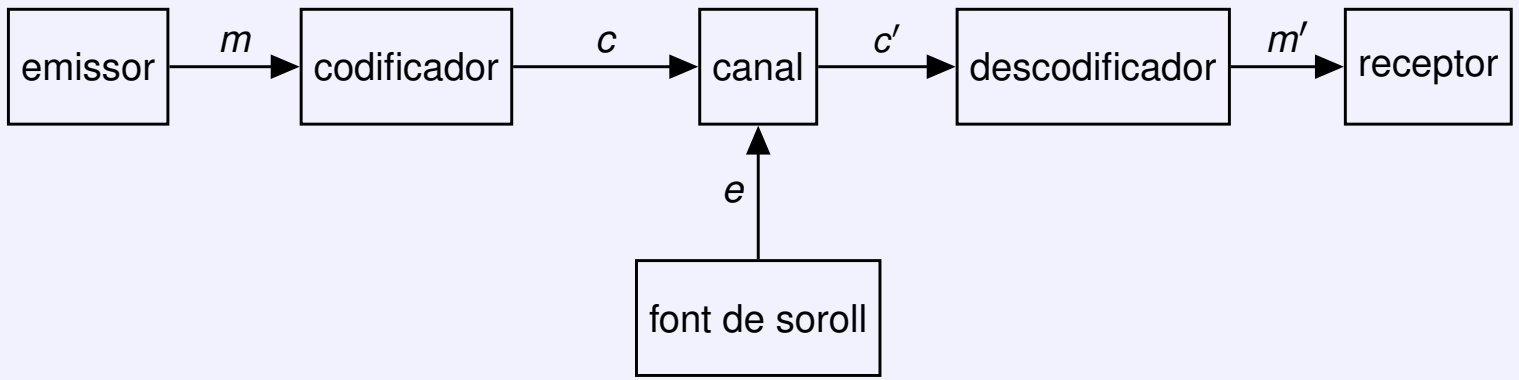
A l'exemple anterior, la informació que s'enviava era binària: cert o fals. De fet, era suficient enviar un bit: 1 (cert) o 0 (fals). Però si només s'envia el bit d'informació, si hi ha soroll, el missatge es pot perdre completament.

És per això que les llengües han evolucionat buscant un **codi** que intenta reduir els problemes ocasionats pel soroll ambiental, per comunicar-nos millor.

A les comunicacions digitals tenim el mateix problema. Aquest problema s'aborda formalment a la **teoria de codis**.

Model amb codificació

Per minimitzar els problemes causats pel soroll, s'incorporen mecanismes de **codificació** i **descodificació**. Ara, el que s'envia a través del canal és el missatge codificat.



m: missatge enviat, c: codificació del missatge, c': codificació rebuda, m': missatge obtingut, e: soroll

Objectiu de la teoria de codis

Afegint mecanismes de codificació, el que buscarem serà que la comunicació sigui

- **fiable**: Que el receptor obtingui $m' = m$ amb *alta* probabilitat,
- **eficient**: Que la proporció entre la llargada de c i de m sigui *petita*.

El que ens cal és trobar un compromís entre aquestes dues propietats. Això es pot veure al següent exemple.

Objectiu de la teoria de codis

Exemple

Suposem que el missatge és un bit b. Si volem una comunicació molt fiable, podem utilitzar un ***codi*** *de r-****repetició****: repetim r vegades el bit b.*
Amb un codi de 3-repetició, tindríem $c = bbb$. *És a dir, si* $b = 0$, $c = 000$, *i si* $b = 1$, $c = 111$. *Es descodificarà pel criteri de la majoria:*

- *Si el receptor rep* $c' = 000, 100, 010,$ *o* 001, *dirà que* $m' = 0$.
- *Si el receptor rep* $c' = 111, 011, 101,$ *o* 110, *dirà que* $m' = 1$.

Això es pot estendre a qualsevol r imparell. Com més gran sigui r, més ***fiable*** *serà. Però, com més gran sigui r, menor* ***eficiència*** *tindrem.*
En aquest curs veurem codis que permeten un millor compromís entre fiabilitat i eficiència.

Motivació

Codis lineals

Detecció i correcció d'errors

Solucions

Apèndix: Repàs d'àlgebra lineal i matrius

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Codis lineals

Un **codi lineal** C de **longitud** n sobre un alfabet $\mathbb{F}_q$ és un subespai vectorial de $\mathbb{F}_q^n$.

Exercici 1

Dins de $\mathbb{F}_2^3$ considerem el conjunt de paraules

$$C = \{(000), (111), (101), (010)\}.$$

Demostreu que C és un codi lineal.

Solució (p.88)

Codis lineals

Si $q = 2$, aleshores diem que el codi és **binari**, mentre que si $q = 3$, aleshores diem que el codi és **ternari**.

Exercici 2

Com és el codi $C = \{(000), (111), (101), (010)\}$ de l'exercici anterior?

Solució (p.89)

Codis lineals

La **dimensió** k del codi és la dimensió del subespai.

Exercici 3

Quina seria la dimensió del codi
$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$? Solució (p.90)

La **taxa de transmissió és** $\frac{k}{n}$. La **codimensió** és $n - k$.

Exercici 4

Quines serien la taxa de transmissió i la codimensió del codi
$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$? Solució (p.91)

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Matriu generadora

Si un codi C és un subespai vectorial de dimensió k, aleshores té una base formada per k vectors.

Podem col·locar els k vectors d'una base de C un damunt de l'altre en forma de matriu. Obtenim el que anomenem una matriu generadora.

> Diem que una matriu G de k files i n columnes és una **matriu generadora** del codi lineal C si les seves files són una base de C.

La matriu generadora no és única. Es poden intercanviar files, per exemple.

Matriu generadora

Exercici 5

Doneu una matriu generadora del codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

Solució (p.92)

Per **codificar** una paraula de k símbols de $\mathbb{F}_q$, la multipliquem per la matriu generadora.

Matriu generadora

Exemple

Podem representar els elements de $\mathbb{Z}_7$ de la següent manera:

$\mathbb{Z}_7 = \{$ 0 , 1 , 2 , 3 , 4 , 5 , 6 $\}$

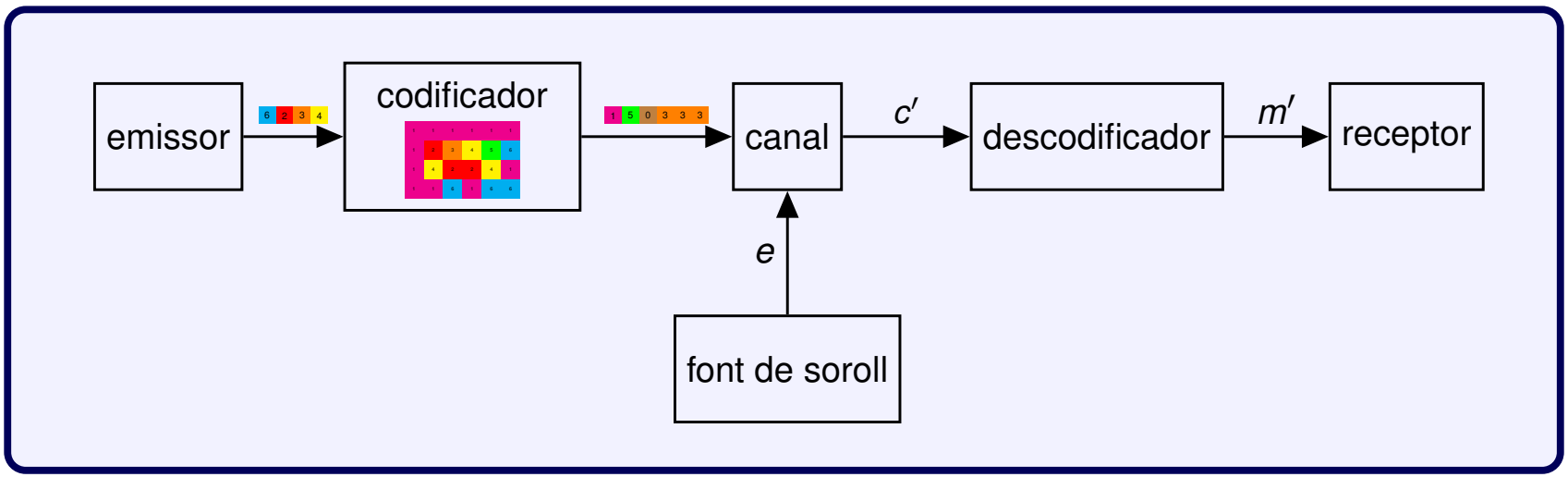
Considerem el codi generat per la matriu

$$G = \begin{array}{|cccccc|}\hline 1&1&1&1&1&1\\ 1&2&3&4&5&6\\ 1&4&2&2&4&1\\ 1&1&6&1&6&6\\ \hline\end{array}$$

Per codificar una paraula com 6 2 3 4 *amb la matriu G, la multipliquem per G.*

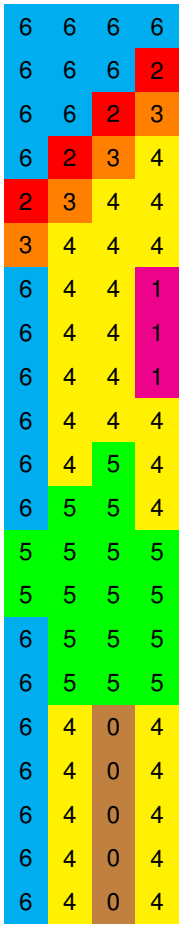
$$\begin{array}{|cccc|}\hline 6&2&3&4\\ \hline\end{array} \cdot \begin{array}{|cccccc|}\hline 1&1&1&1&1&1\\ 1&2&3&4&5&6\\ 1&4&2&2&4&1\\ 1&1&6&1&6&6\\ \hline\end{array} = \begin{array}{|cccccc|}\hline 1&5&0&3&3&3\\ \hline\end{array}$$

Matriu generadora



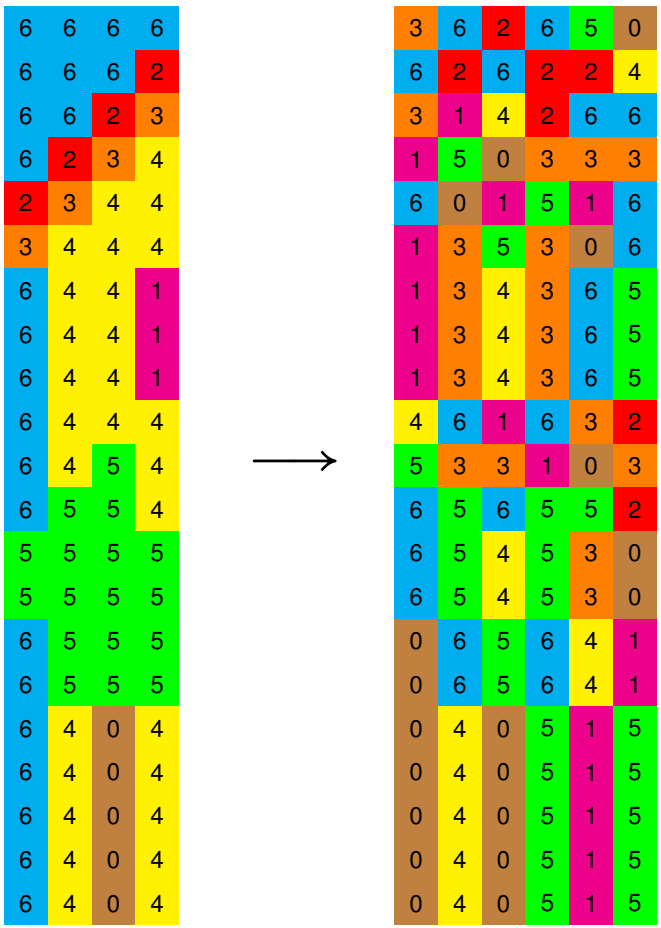
Matriu generadora

Suposem que ara volem codificar la imatge següent.

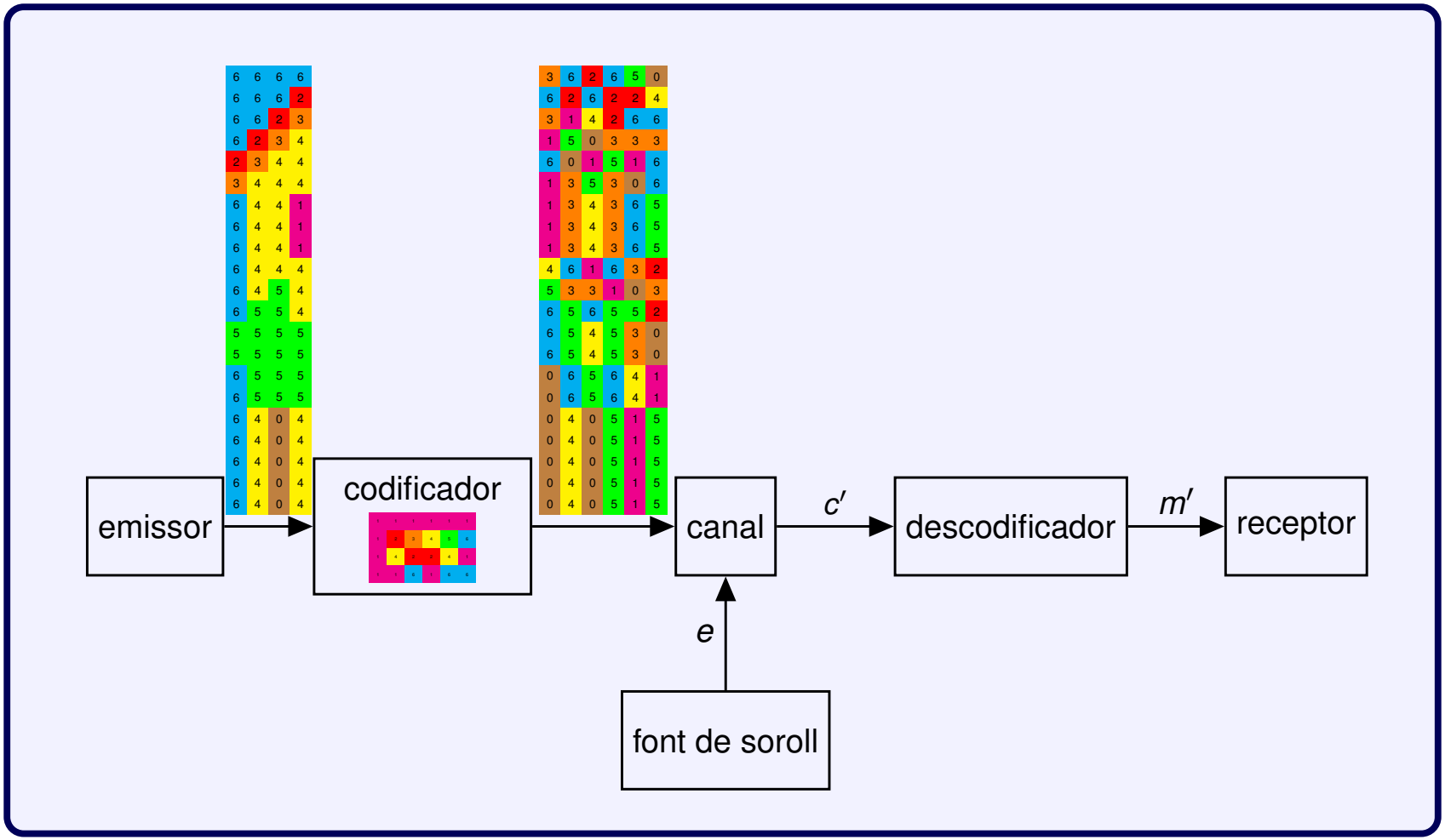


Matriu generadora

Codificarem cadascuna de les seves files.



Matriu generadora



Matriu generadora

Exercici 6

Comproveu que les paraules del codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$ són totes les codificacions possibles amb la matriu

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

Solució (p.93)

Matriu generadora sistemàtica

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.

Vegeu més sobre l'existència de matrius sistemàtiques (p.118)

Matriu generadora sistemàtica

Exemple

Recordem l'exemple de codi sobre $\mathbb{Z}_7$.
Una alternativa per codificar és fer servir la següent matriu sistemàtica equivalent a G:

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

Matriu generadora sistemàtica

Exemple

Recordem l'exemple de codi sobre $\mathbb{Z}_7$.
Una alternativa per codificar és fer servir la següent matriu sistemàtica equivalent a G:

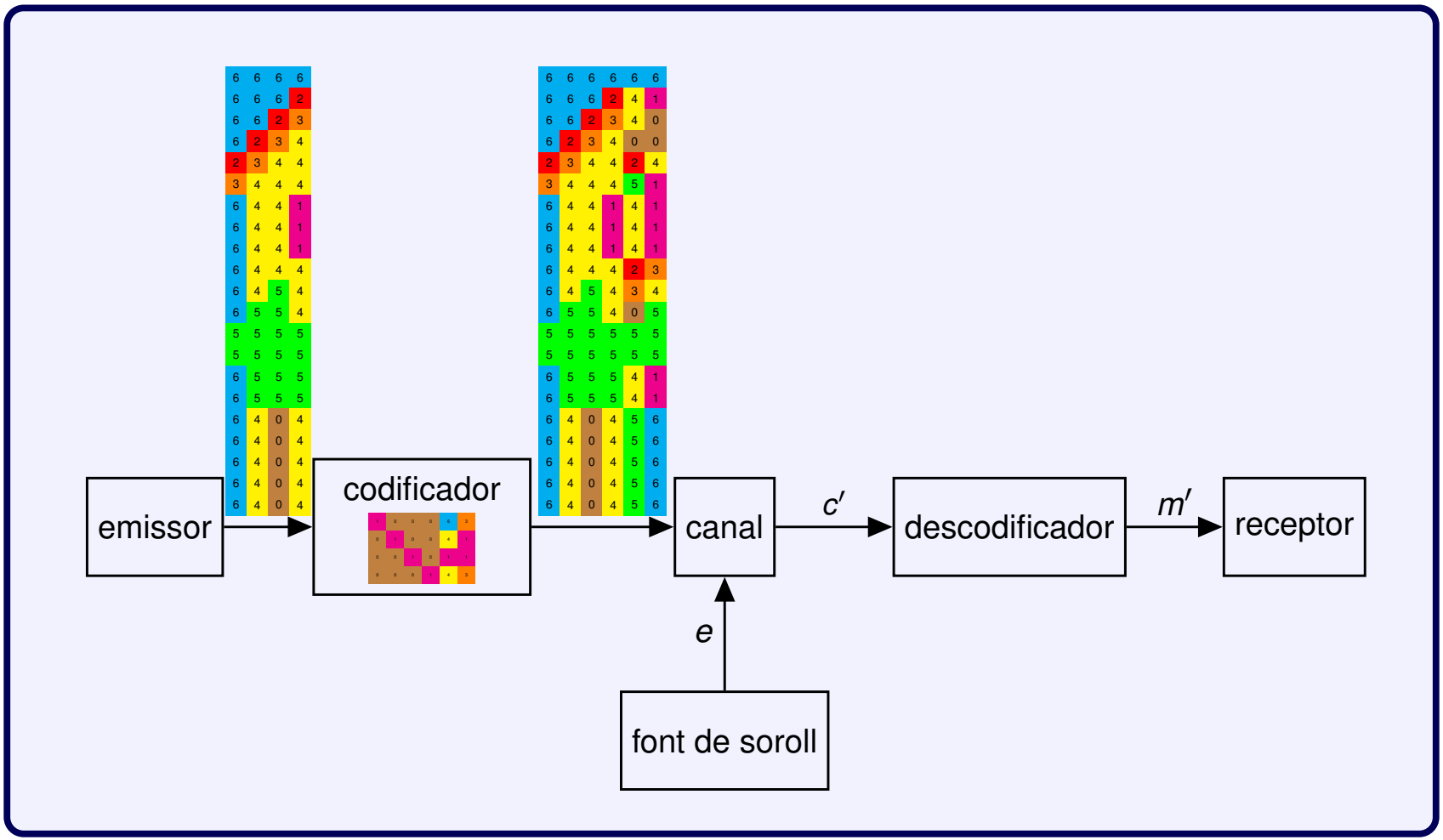
$$G_s = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}$$

Així, codificar una paraula com $(6\ 2\ 3\ 4)$ *serà*

$$(6\ 2\ 3\ 4) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix} = (6\ 2\ 3\ 4\ 0\ 0)$$

Matriu generadora sistemàtica

Ara, en codificar la imatge, què observem?



Més endavant utilitzarem aquest exemple per a la detecció d'errors (p.63) i per a la error correction (p.74).

Matriu generadora sistemàtica

Exercici 7

Considerem un codi ternari amb matriu generadora

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix}$$

Codifiqueu sistemàticament a l'esquerra la informació

- $(1,0,2)$
- $(2,2,1)$

Solució (p.94)

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Codificació en símbols i en dígits

En un cos finit de p^m elements distingim

- **dígits**: són els elements de $\mathbb{Z}_p$,
- **símbols**: són els elements de $\mathbb{F}_{p^m}$.

Cada símbol es pot representar amb m dígits mitjançant la notació vectorial.

Els dígits de $\mathbb{Z}_2$ també s'anomenen **bits**. Els dígits de $\mathbb{Z}_3$ també s'anomenen **trits**.

Exemple

Suposem que volem utilitzar un codi sobre $\mathbb{F}_9 = \mathbb{Z}_3/x^2 + 2x + 2$. Si diem α a la classe de x, tenim la taula d'equivalències següent:

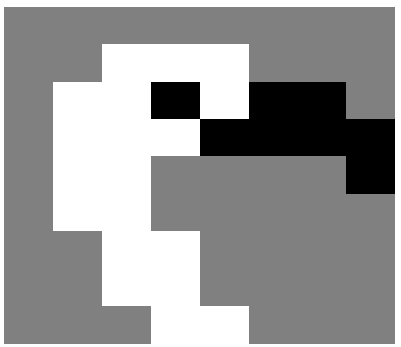
exp.	*vect.*
0	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21
↑	↑
símbols	***parelles de dígits***

Codificació en símbols i en dígits I

Considerem el codi que té matriu generadora

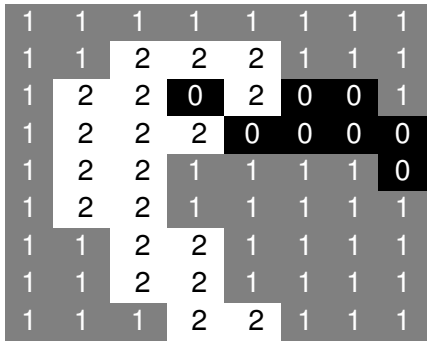
$$\begin{pmatrix} \alpha^2 & \alpha^3 & 1 & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^4 & 1 & \alpha^4 & \alpha^4 & 0 & 1 & 0 & 0 \\ \alpha^2 & \alpha^5 & \alpha^4 & \alpha^3 & 0 & 0 & 1 & 0 \\ \alpha & \alpha^6 & \alpha^4 & \alpha^6 & 0 & 0 & 0 & 1 \end{pmatrix}$$

i suposem que volem codificar la imatge digital següent:



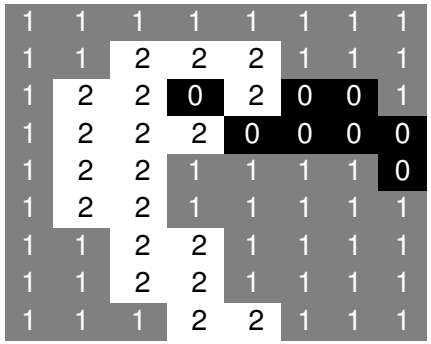
Codificació en símbols i en dígits

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

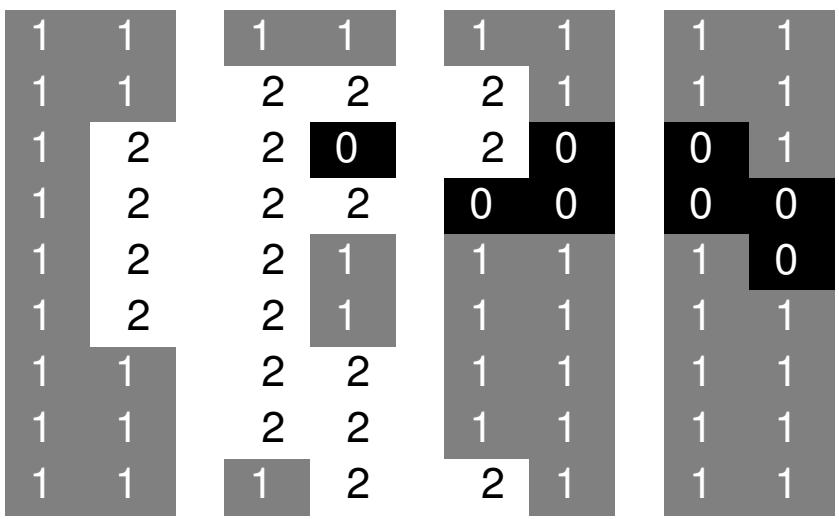


Codificació en símbols i en dígits

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



I agrupem cada $m = 2$ dígits per formar un símbol, mitjançant la taula d'equivalències anterior.



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

Codificació en símbols i en dígits

Ara ja podem multiplicar cada fila per la matriu generadora

$$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\ \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\ \alpha^3 & \alpha^6 & 0 & 0 \\ \alpha^3 & \alpha^7 & \alpha^2 & 1 \\ \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2 \end{pmatrix} \begin{pmatrix} \alpha^2 & \alpha^3 & 1 & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^4 & 1 & \alpha^4 & \alpha^4 & 0 & 1 & 0 & 0 \\ \alpha^2 & \alpha^5 & \alpha^4 & \alpha^3 & 0 & 0 & 1 & 0 \\ \alpha & \alpha^6 & \alpha^4 & \alpha^6 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^7 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\ \alpha^3 & \alpha & \alpha & \alpha^4 & \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\ 1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 & \alpha^6 & 0 & 0 \\ \alpha^5 & \alpha^4 & 0 & \alpha & \alpha^3 & \alpha^7 & \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\ 0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\ \alpha^7 & \alpha^2 & 0 & \alpha^6 & \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2 \end{pmatrix}$$

Codificació en símbols i en dígits

I ara podem tornar a convertir cada símbol en la parella de dígits que li correspon i obtenim la imatge codificada.

$$\begin{pmatrix} \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ \alpha^2 & \alpha^7 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\ \alpha^3 & \alpha & \alpha & \alpha^4 & \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\ 1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 & \alpha^6 & 0 & 0 \\ \alpha^5 & \alpha^4 & 0 & \alpha & \alpha^3 & \alpha^7 & \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\ 0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\ \alpha^7 & \alpha^2 & 0 & \alpha^6 & \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2 \end{pmatrix} \rightarrow$$

1	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

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Codi dual

El **codi dual** (o ortogonal) de C és

$$C^{\perp} = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ per a tot } c \in C\}.$$

El codi dual d'un codi és, per tant, el complement ortogonal (p.121) del codi.

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 de coeficients G.

Exemple

El codi ternari amb matriu generadora

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix}$$

té com a codi dual el conjunt de vectors $(x_1, \ldots, x_6)$ *que són solucions de*

$$\begin{array}{rrrrrrr} 2x_1 & +2x_2 & & +2x_4 & +x_5 & +x_6 & = 0 \\ 2x_1 & & +x_3 & +x_4 & +2x_5 & +2x_6 & = 0 \\ x_1 & +2x_2 & & +2x_4 & +x_5 & & = 0 \end{array}$$

Matriu de control

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

$$C = \{c \in \mathbb{F}_q^n : c \cdot h = 0 \text{ per a tota fila } h \text{ de } H\}.$$

Matriu de control

Si una matriu generadora és de la forma

$$G = (I|P),$$

aleshores una matriu de control és

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

I si una matriu generadora és de la forma

$$G = (P|I),$$

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

Vegeu una justificació de l'àlgebra lineal (p.120)

Matriu de control

Exercici 8

Considerem el codi ternari de l'Exercici 7 amb matriu generadora

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix}$$

Doneu-ne una matriu de control.

Solució (p.95)

Matriu de control

Exercici 9

Considerem el codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

1. Doneu una matriu de control de C.
2. Comproveu que totes les paraules del codi, quan les multipliquem per la matriu de control, donen 0.
3. Doneu el codi dual $C^\perp$.
4. Comproveu que les paraules del codi dual, quan les multipliquem per la matriu G, donen 0.

Solució (p.96)

Motivació

Codis lineals

Detecció i correcció d'errors

Solucions

Apèndix: Repàs d'àlgebra lineal i matrius

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Distància de Hamming

La **distància de Hamming** entre dues paraules de la mateixa longitud és el nombre de posicions on difereixen.
Anomenem $d_H(u, v)$ a la distància de Hamming entre les paraules u i v.

Exemple

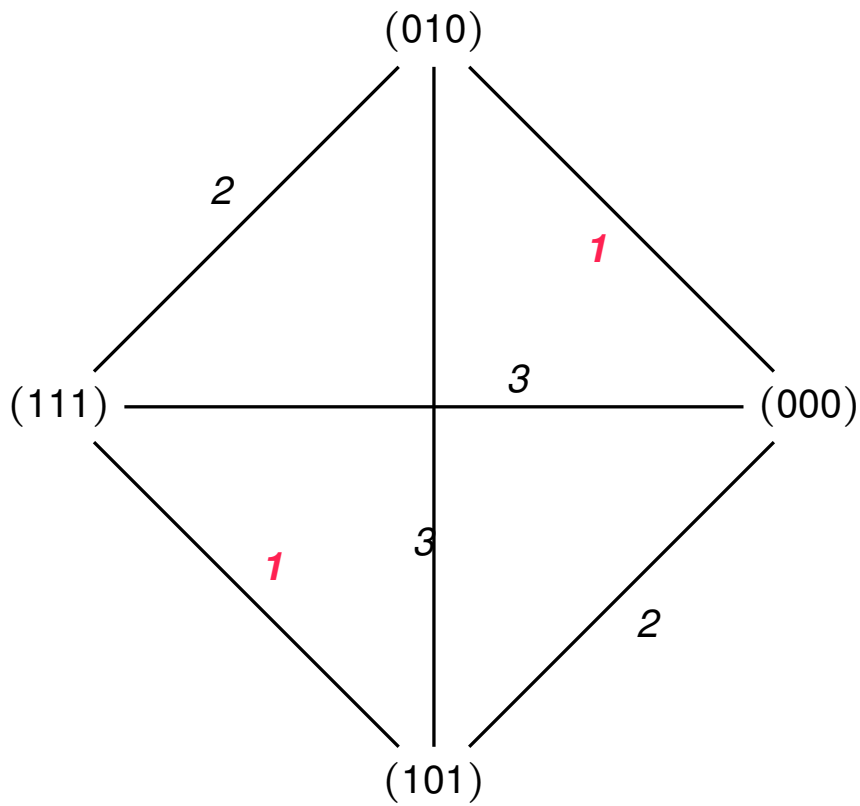
$$\begin{aligned} d_H(CERT, CART) &= 1 \\ d_H(FALS, CART) &= 3 \\ d_H(CERT, CALT) &= 2 \\ d_H(FALS, CALT) &= 2 \end{aligned}$$

Distància de Hamming

En un codi ens interessarà considerar la distància de Hamming entre cada parella de paraules i determinar la mínima d'aquestes distàncies.

Exemple

Les distàncies entre les paraules del codi
$C = \{(000), (111), (101), (010)\}$ *són les següents:*



Pes

El **pes** d'una paraula és el nombre de posicions no nul·les. Anomenem $w(u)$ al pes de u.

Exemple

Els pesos de les paraules del codi anterior són:

$$\begin{aligned} w(000) &= 0 \\ w(010) &= 1 \\ w(101) &= 2 \\ w(111) &= 3 \end{aligned}$$

Si $u, v \in \mathbb{F}_q^n$ i diem $\vec{0}$ al vector nul de $\mathbb{F}_q^n$, aleshores,

- $d(u, \vec{0}) = w(u)$,
- $d(u, v) = d(u - v, \vec{0}) = w(u - v)$.

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Distància mínima

La **distància mínima** 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 nombre de columnes linealment dependents de H.

Justificació de l'equivalència

Les dues primeres definicions són equivalents pel fet que C és un espai vectorial i pel fet que $d(u, v) = w(u - v)$.

La darrera definició es dedueix del fet que si una paraula c té pes w amb coordenades no nul·les en les posicions $i_1, \ldots, i_w$, aleshores el producte de la matriu de control per c és una combinació lineal nul·la de les columnes en posició $i_1, \ldots, i_w$ de la matriu de control. En aquest cas, les columnes de H en les posicions $i_1, \ldots, i_w$ són linealment dependents.

Distància mínima

Exemple

Volem determinar la distància mínima del codi C de $\mathbb{Z}_5^5$ que té matriu de control

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

- *Perquè d fos 1 caldria que hi hagués una columna linealment dependent a H. Una sola columna és linealment dependent si i només si és nul·la. Com que no hi ha cap columna nul·la descartem $d = 1$.*
- *Perquè d fos 2 caldria que hi hagués dues columnes linealment dependents a H. Dues columnes són linealment dependents si una és un múltiple de l'altra. Com que això no es dona per cap parella de columnes, descartem $d = 2$.*
- *Perquè d fos 3 caldria que hi hagués tres columnes linealment dependents a H. Tres columnes són linealment dependents si una és una combinació lineal de les altres dues. Observem, per exemple, que la tercera columna és la suma de la segona i la quarta. Deduïm que $d = 3$.*

Fita de Singleton

La **fita de Singleton** estableix que, en un codi de longitud n i distància mínima d, la dimensió k satisfà

$$k \leq n - d + 1.$$

Demostració

Com que una matriu de control té $n - k$ files, sabem que qualsevol conjunt de $n - k + 1$ columnes de la matriu de control seran linealment dependents. La fita es dedueix pel fet que la distància mínima és el mínim nombre de columnes linealment dependents d'una matriu de control. □

Fita de Singleton

Exercici 10

Considerem el codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

1. Quina és la seva distància mínima?
2. Verifiqueu la fita de Singleton pel codi C.

Solució (p.98)

Capacitat correctora

Utilitzant un codi de distància mínima d, es podran

- detectar $d-1$ errors,
- corregir $d-1$ esborralls,
- corregir $\lfloor \frac{d-1}{2} \rfloor$ errors.

La **capacitat correctora** d'un codi de distància mínima d és

$$\left\lfloor \frac{d-1}{2} \right\rfloor$$

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Detecció d'errors

Suposem que rebem una paraula u i volem verificar si és del codi ($u \in C$) o, en cas contrari, **detectar** que conté **errors** ($u \notin C$).

> Anomenem **síndrome** de u respecte d'una matriu de control H de C al resultat del producte $H \cdot u$.

Observem que la síndrome depèn de la matriu de control emprada.

Una paraula c és de C si i només si la seva síndrome és zero.

Tot i que la síndrome depèn de la matriu de control emprada, si per a alguna matriu de control H es compleix $H \cdot u = 0$, aleshores es complirà per a totes les matrius de control.

> Si la síndrome de u és nul·la, deduïm que $u \in C$.
> Si no, aleshores **detectem error**.

Detecció d'errors

Exemple

A $\mathbb{Z}_5$ considerem el codi C que té matriu de control

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

Volem detectar si en les paraules (11111) *i* (01234) *hi ha errors.*
Multipliquem les paraules per la matriu H.

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow \textit{paraula de C}$$

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow \textbf{\textit{error detectat}}$$

Detecció d'errors

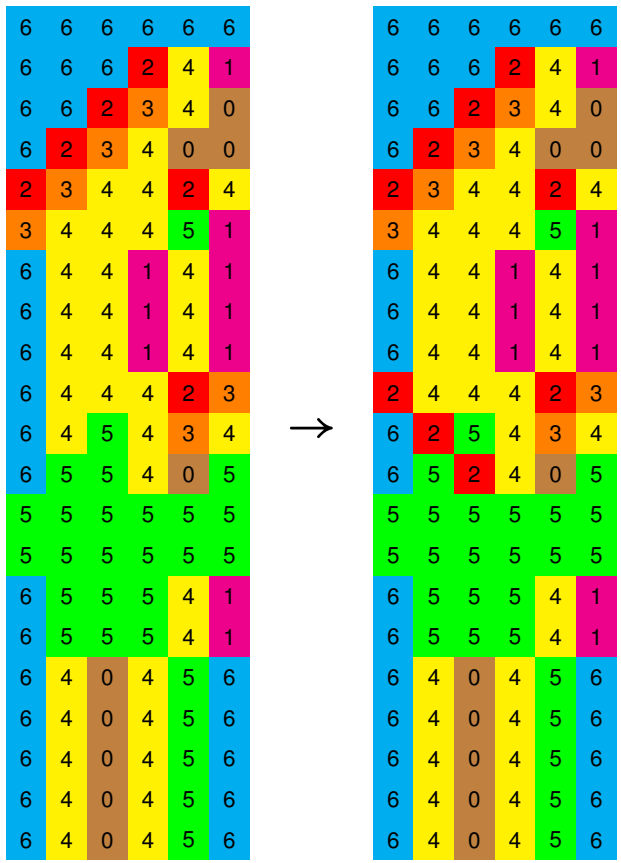
Exemple

Una martriu de control del codi que havíem vist és

$$H = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 4 & 2 & 2 & 4 & 1 \\ \hline \end{array}$$

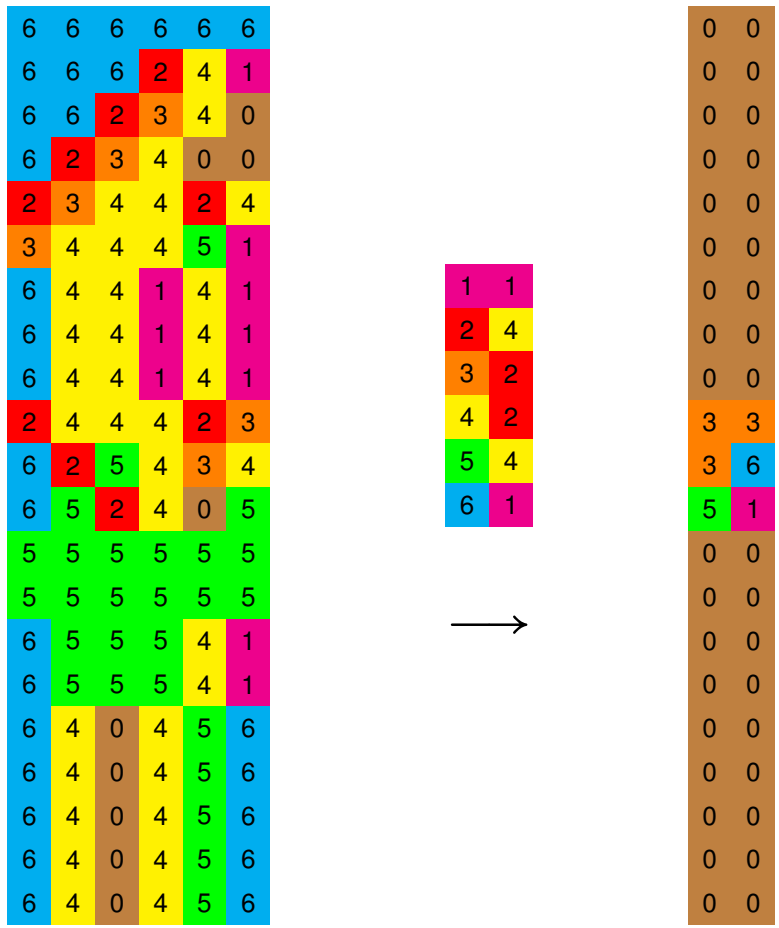
Detecció d'errors

Suposem que se'ns embruta la imatge codificada:



Detecció d'errors

Per identificar on s'han produït els errors, multiplicarem cada fila per H^T (transposem H, ja que uH^T és una transposició de Hu).



Allà on el resultat és diferent de zero és on hi ha errors.

Exercici 11

1. Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$.
2. Doneu una taula exponencial-vectorial de $\mathbb{F}_4$.
3. Anomenem 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 i doneu el resultat també en bits.
4. Doneu una matriu de control del codi.
5. Quina és la distància mínima del codi C?
6. Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?
7. Detecteu si hi ha errors en la cadena codificada de bits

   011111010011001000000000.

Solució (p.99)

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Correcció d'esborralls

Suposem que rebem una paraula on s'han esborrat alguns dels símbols i s'han convertit en **esborralls**.

Considerant els esborralls com a incògnites, a partir de

$$H \cdot u = 0$$

obtenim un sitema lineal d'equacions.

Si el nombre d'esborralls és com a màxim $d - 1$, aleshores el sistema és compatible i determinat.

La substitució de les incògnites per la solució del sistema ens dona la **correcció d'esborralls**.

Correcció d'esborralls

Exemple

A $\mathbb{Z}_5$ considerem el codi C que té matriu de control

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

Volem corregir els esborralls de la paraula $(324??)$ *i donar-ne la paraula corregida.*
Substiuïm els esborralls per incògnites: $(324xy)$ *i resolem el sistema*

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 4 \\ x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

equivalent a

$$\begin{array}{rcl} 3 + 2x + y & = & 0 \\ 4 + 4x + y & = & 0 \\ 1 + 3y & = & 0 \end{array} \quad \Longrightarrow \quad y = 3 \qquad \Longrightarrow \quad 2x + 1 = 0 \quad \Longrightarrow \quad x = 2$$

que té solució $x = 2$ *i* $y = 3$*. Per tant, la paraula corregida és* (32423)*.*

Correcció d'esborralls

Exercici 12

1. Comproveu que el polinomi $x^2 + 2x + 2$ és irreductible i primitiu a $\mathbb{Z}_3[x]$.
2. Doneu una taula exponencial-vectorial de $\mathbb{Z}_3[x]/x^2 + 2x + 2$, utilitzant $\alpha = [x]$.
3. Considerem el codi C amb matriu generadora

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

   Codifiqueu la cadena de trits 01211022. Doneu el resultat també com a cadena de trits.
4. Doneu una matriu de control del codi.
5. Quina és la distància mínima de C?
6. Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?
7. Corregiu els esborralls de la cadena de trits 0112??22. Doneu el resultat en trits.

Solució (p.101)

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Correcció d'errors

Ara suposem que s'ha enviat una paraula de codi $c \in C$, que eventualment s'han produït errors i s'ha convertit en u.

Anomenem $e = u - c$. Suposarem que s'han produït pocs errors i que, per tant, e és nul gairebé en totes les coordenades excepte en unes poques.

Diem que c és la **paraula codi**, u és la **paraula rebuda** i e és el **vector d'errors**.

Si $e = (0, \ldots, 0, e_{i_1}, 0, \ldots, 0, e_{i_2}, 0, \ldots, 0, \ldots, e_{i_t})$ amb $e_{i_1}, e_{i_2}, \ldots, e_{i_t} \neq 0$, aleshores diem que $i_1, i_2, \ldots, i_t$ són les **posicions d'error**, mentre que $e_{i_1}, \ldots, e_{i_t}$ són els **valors dels errors**.

Per corregir errors utilitzarem que la **síndrome** de la paraula rebuda satisfà

$$H \cdot u = H \cdot e$$

Anomenarem $s = H \cdot u$.

Correcció d'errors

Per corregir 1 **error:**

Si només es produeix un error, aleshores

- $e = (0, \ldots, 0, e_i, 0, \ldots, 0)$,
- $s = H \cdot u = h_i e_i$, on h_i és la columna i-èssima de H.

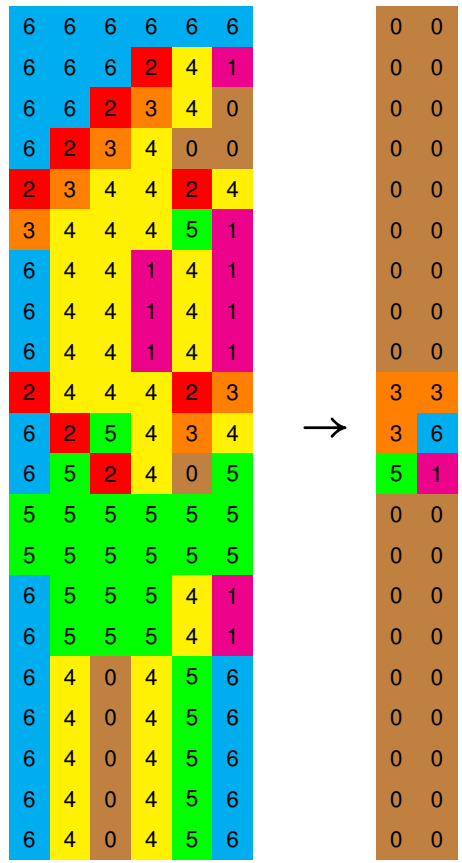
Aleshores

- buscant quina columna de H és un múltiple de s, tindrem la **posició d'error**,
- buscant l'únic valor e_i tal que $s = h_i e_i$, tindrem el **valor de l'error**.

Correcció d'errors

Exemple

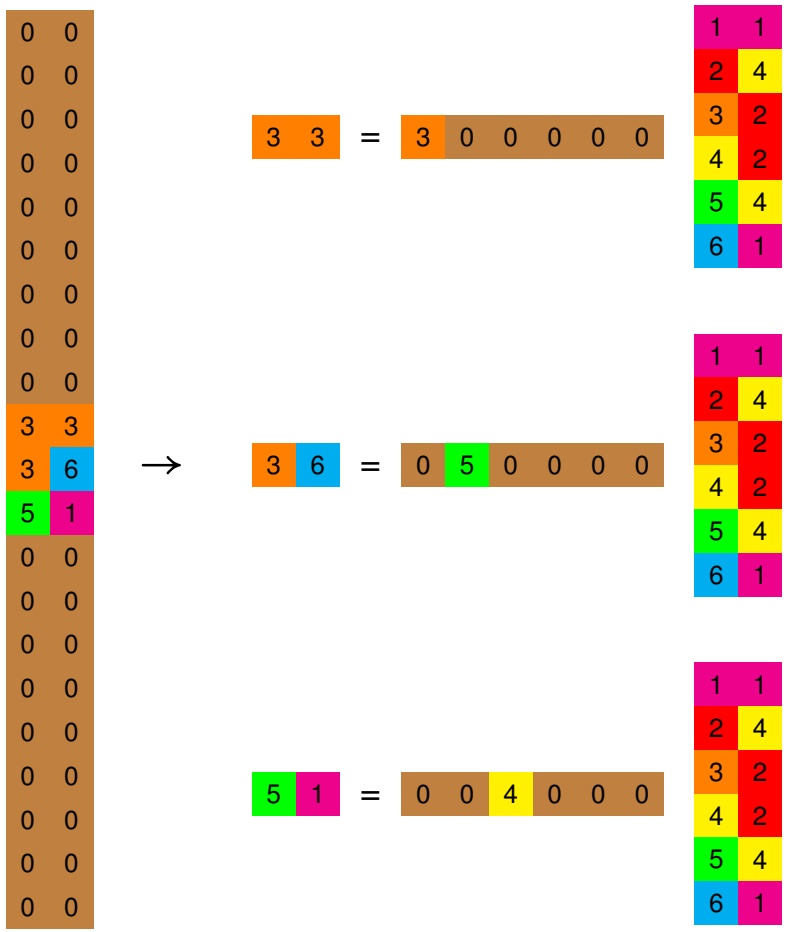
Continuem amb el codi que havíem vist.



Havíem calculat les síndromes.

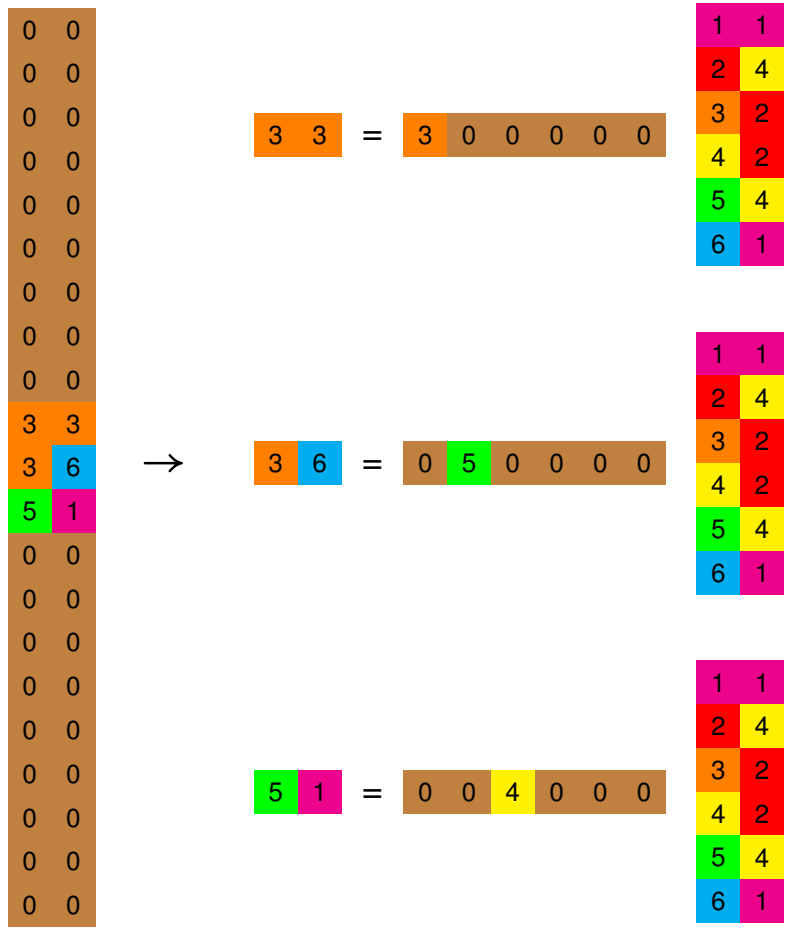
Correcció d'errors

Per trobar el valor dels errors, vegem que les síndromes són múltiples de columnes de H:



Correcció d'errors

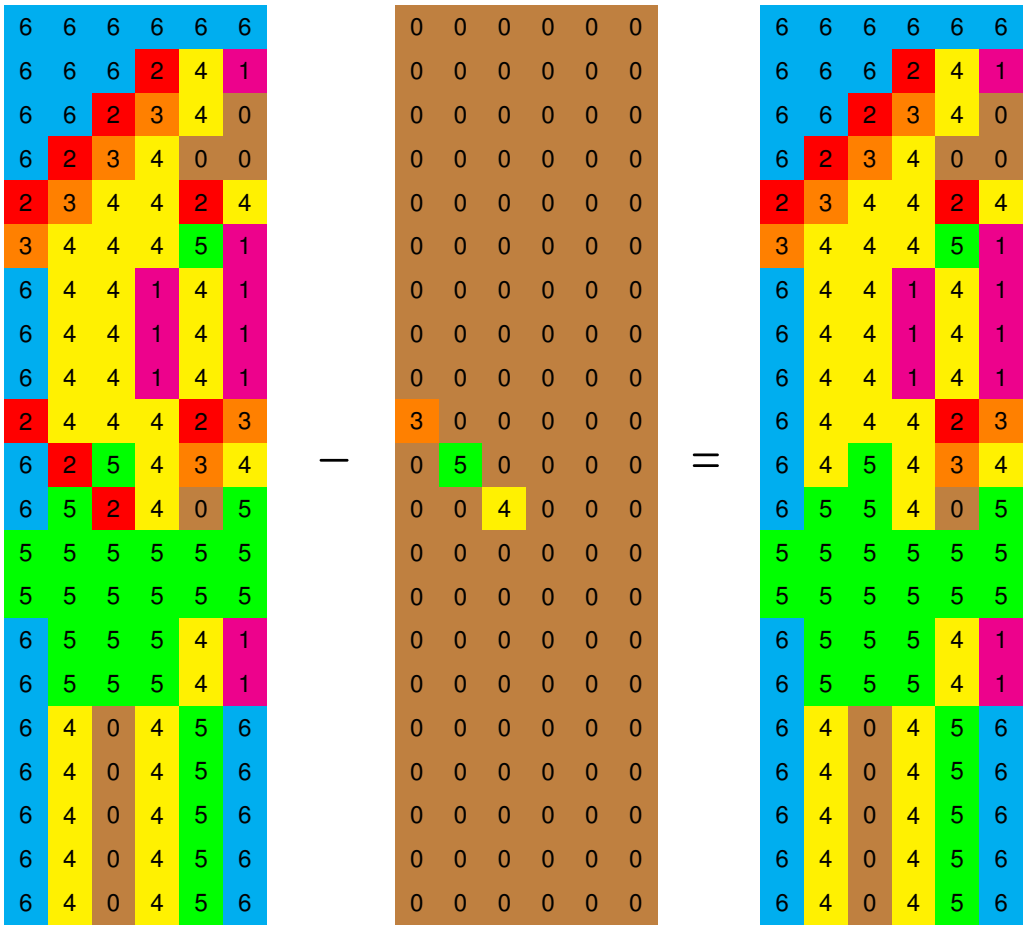
Per trobar el valor dels errors, vegem que les síndromes són múltiples de columnes de H:



Deduïm que les paraules d'error són

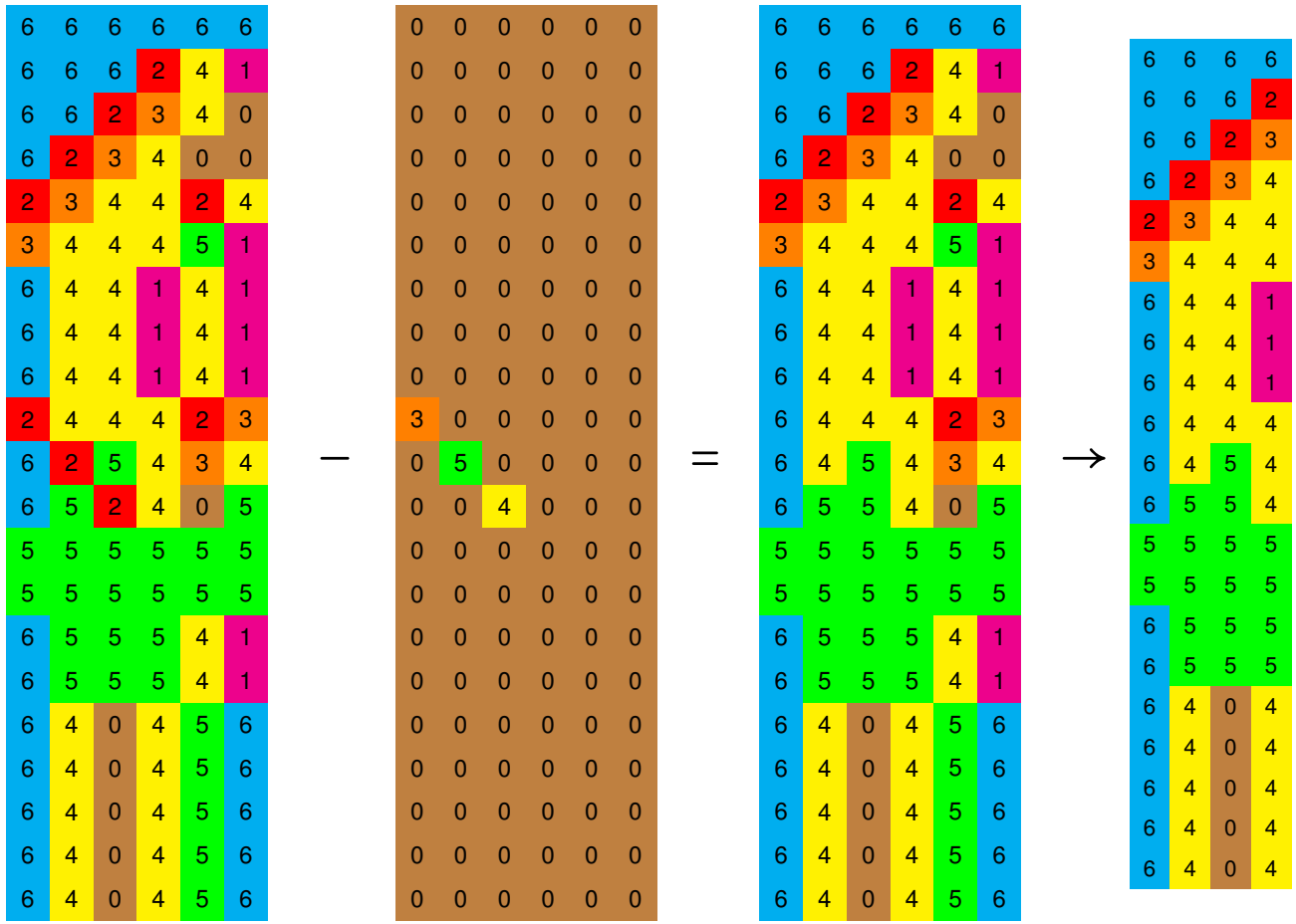
Correcció d'errors

Restem les paraules d'error de les paraules rebudes



Correcció d'errors

Restem les paraules d'error de les paraules rebudes



I descodifiquem per la part sistemàtica.

Correcció d'errors

Exercici 13

Utilitzem el codi dels Exercicis 7 i 8.
Useu la síndrome per descodificar el vector rebut 212121.

Solució (p.105)

Correcció d'errors

Cas general:

La descodificació per **màxima versemblança** consisteix a descodificar u per $u - e'$, on e' és un vector de $\mathbb{F}_q^n$ amb mínim pes d'entre els que tenen la mateixa síndrome que u.

Per fer-ho busquem una combinació lineal mínima de columnes de H que sigui igual a la síndrome. És a dir, si la representació d'H en columnes és $(h_1, h_2, \ldots, h_n)$, busquem una combinació $\alpha_{i_1} h_{i_1} + \cdots + \alpha_{i_r} h_{i_r}$ que utilitzi el mínim possible de columnes d'H i que sigui igual a la síndrome $H \cdot u$. Aleshores prenem $e' = (0, \ldots, 0, \alpha_{i_1}^{(i_1}, 0, \ldots 0, \alpha_{i_r}^{(i_r}, 0, \ldots, 0)$.

La descodificació és única si el nombre d'errors és, com a màxim, la capacitat correctora.

Principi de màxima versemblança

Exemple

Codi de repetició 3:

1. *Quan rebem la seqüència* 001*, sabem que hi ha hagut algun error. Podríem pensar que la paraula era* 000 *i s'ha produït l'error* 001*, o que la paraula era* 111 *i l'error ha estat el* 110*.*
2. *La probabilitat d'error del canal p_c ens informa de la probabilitat que un bit canviï en ser transmès per un canal determinat.*
3. *La probabilitat que l'error sigui* 001 *és $(1-p_c)^2 p_c$, mentre que la probabilitat que l'error sigui* 110 *és $(1-p_c)p_c^2$.*
4. *Si $p_c = 0.01$, $(1-p_c)^2 p_c = 0.0098$, i $(1-p_c)p_c^2 = 0.000099$.*
5. *Si $p_c < 1/2$, el primer cas és més probable que el segon.*

Sota el principi de màxima versemblança, sempre assumirem que la paraula enviada ha estat la que correspon al cas més probable.

Correcció d'errors

Exercici 14

Utilitzem el codi dels Exercicis 7 i 8.
Useu la síndrome per corregir els vectors rebuts

(a) 120102, Solució (p.106)

(b) 222222. Solució (p.107)

Correcció d'errors

Exercici 15

Considerem el codi C definit sobre $\mathbb{F}_5$ format per les solucions del sistema

$$\begin{aligned} x_1 + 3x_2 + 2x_4 + 4x_5 &= 0 \\ x_2 + 3x_3 + x_4 + x_5 &= 0 \end{aligned}$$

1. Quina és la seva dimensió?
2. Quina és la seva distància mínima?
3. Corregiu el missatge 1132321231.

Solució (p.108)

Correcció d'errors

Exercici 16

Sigui C el codi sobre $\mathbb{F}_2$ amb matriu generadora

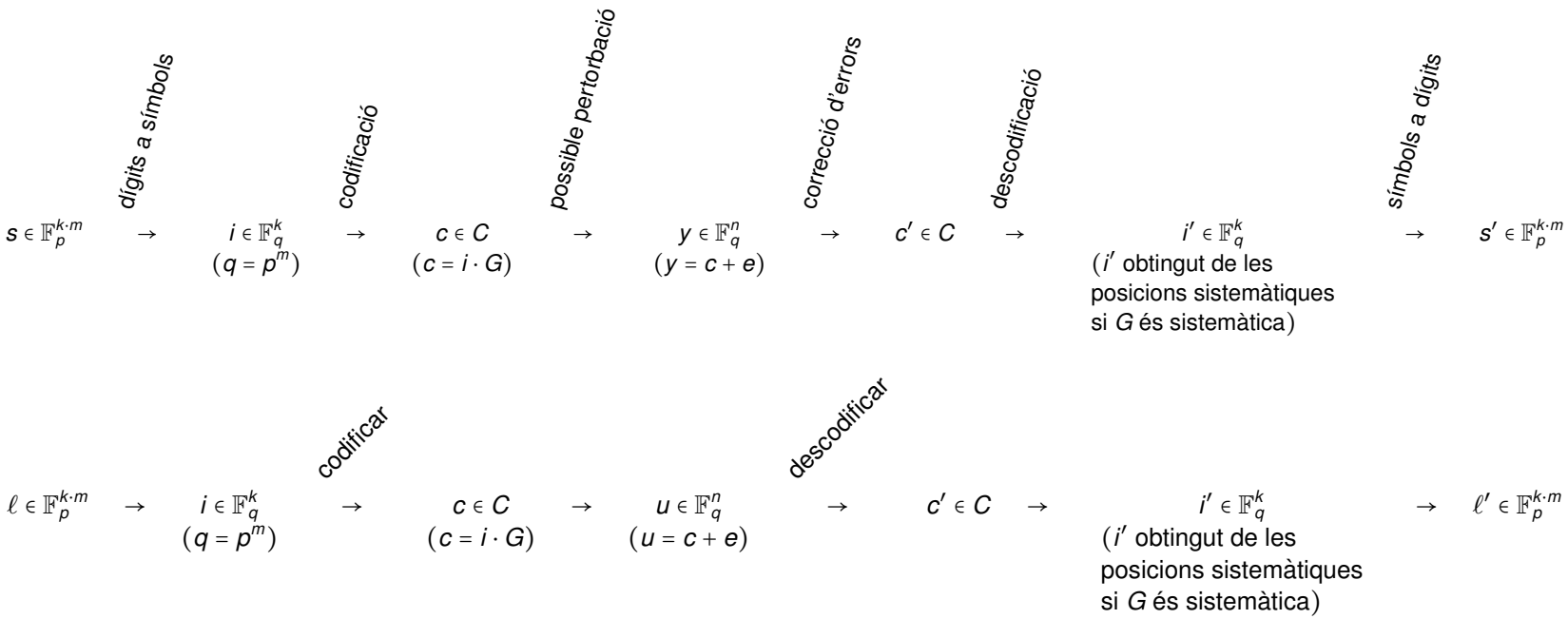
$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

1. Calculeu una matriu de control de C.
2. Quins són els paràmetres d'aquest codi?
3. Quants errors corregeix?
4. Calculeu la síndrome de $v = (00111101)$.
5. Corregiu v.
6. Si hem emprat G per codificar, quina era la paraula transmesa?
7. Quin era el missatge enviat?

Solució (p.109)

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Procés de codificació-descodificació



Motivació

Codis lineals

Detecció i correcció d'errors

Solucions

Apèndix: Repàs d'àlgebra lineal i matrius

Solució de l'Exercici 1

Com que C és un subespai de $\mathbb{F}_2^3$, els escalars són únicament 0 i 1. Així els vectors de C multiplicats per escalars són o bé el vector nul o bé els mateixos vectors.

Queda comprovar que les sumes de dos vectors de C són vectors de C. I, en efecte,

$$
\begin{array}{lcllcl}
(000) & + & (000) & = & (000) & \in C \\
(000) & + & (111) & = & (111) & \in C \\
(000) & + & (101) & = & (101) & \in C \\
(000) & + & (010) & = & (010) & \in C \\
(111) & + & (111) & = & (000) & \in C \\
(111) & + & (101) & = & (010) & \in C \\
(111) & + & (010) & = & (101) & \in C \\
(101) & + & (101) & = & (000) & \in C \\
(101) & + & (010) & = & (111) & \in C \\
(010) & + & (010) & = & (000) & \in C
\end{array}
$$

Torna a l'exercici (p.19)

Solució de l'Exercici 2

Es tracta d'un codi binari.

Torna a l'exercici (p.20)

Solució de l'Exercici 3

$k = 2$

Torna a l'exercici (p.21)

Solució de l'Exercici 4

$$\frac{k}{n} = 0.666,\ n - k = 1$$

Torna a l'exercici (p.21)

Solució de l'Exercici 5

Per exemple,

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

però també $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \dots$

Torna a l'exercici (p.24)

Solució de l'Exercici 6

Vegem com la matriu G genera tot C:

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

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

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

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

Torna a l'exercici (p.30)

Solució de l'Exercici 7

Busquem la matriu equivalent sistemàtica per l'esquerra:

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

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

La codificació demanada és

$$\begin{pmatrix} 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Torna a l'exercici (p.35)

Solució de l'Exercici 8

En la resolució de l'Exercici 7 (p.94) hem vist que la matriu generadora donada és equivalent a la matriu sistemàtica

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}$$

que és de la forma $(I|P)$ amb

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ i } P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

Ara tindrem $P^T = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 2 \\ 1 & 1 & 0 \end{pmatrix}$ i $-P^T = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix}$

Una matriu de control serà, doncs,

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

Torna a l'exercici (p.47)

Solució de l'Exercici 9

1. Com que la matriu generadora

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

té la forma $(I|P)$, podem construir H com $(-P^T|I)$.
En aquest cas $P = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, per tant, $P^T = \begin{pmatrix} 1 & 0 \end{pmatrix}$, que és igual a $-P^T$. Ens queda

$$H = (101).$$

2. Podem comprovar que totes les paraules de C, quan les multipliquem per H, ens donen 0. En efecte,

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

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

Solució de l'Exercici 9

3. El codi dual és el que està generat per H. En el nostre cas és $\{0H, 1H\} = \{(000), (101)\}$.
4.

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

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

Torna a l'exercici (p.48)

Solució de l'Exercici 10

1. La distància mínima és $d = 1$. Es pot veure de tres maneres diferents:
   - per la matriu de control, que en l'exercici anterior havíem vist que era (101) i, per tant, té una columna linealment dependent;
   - perquè hi ha una paraula de pes 1;
   - perquè podem trobar dues paraules a distància 1.
2. Pel codi C tenim paràmetres $n = 3$, $k = 2$, $d = 1$. La fita de Singleton estableix $k \leq n - d + 1$, que en el cas de C correspon a

$$2 \leq 3 - 1 + 1 = 3.$$

Torna a l'exercici (p.58)

Solució de l'Exercici 11

1. 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 $x^2 + x + 1$.
2.

0	00
1	10
α	01
α^2	11

3. 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:

$$\alpha 0 \alpha^2 1 \quad \alpha\alpha^2\alpha^2\alpha \quad \alpha^2\alpha^2 11$$

El resultat en bits serà

$$01001110 \;\; 01111101 \;\; 11111010$$

Solució de l'Exercici 11

4. 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 agafar

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

5. Com que a la matriu de control hi ha dues columnes iguals i no hi ha cap columna nul·la, la distància mínima és 2.
6. No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.
7. De les tres paraules codificades només té error la paraula del mig (multiplicada per la matriu de control dona $\neq 0$).

Torna a l'exercici (p.66)

Solució de l'Exercici 12

1. El polinomi és irreductible perquè té grau 2 i no té arrels ($f(0) = 2$, $f(1) = 2$ i $f(2) = 1$). Si fem totes les potències de $\alpha = [x]$ veiem que són diferents fins que arribem a $\alpha^8 = 1$. Per això el polinomi és primitiu.

2.

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

Solució de l'Exercici 12

3. Com que els elements de $\mathbb{Z}_3[x]/x^2 + 2x + 2$ representen per dos trits cadascun, per poder passar la cadena de trits a cadena de símbols haurem d'agrupar els trits de 2 en 2. Així, la cadena de trits 01211022 la separem com

$$(01)(21)(10)(22).$$

A cada parella de trits li fem correspondre un símbol seguint la taula de l'apartat anterior. Obtenim la cadena de símbols

$$\alpha\alpha^7 1\alpha^6.$$

Ara, per poder codificar la cadena de símbols, la separem en blocs de $k = 2$ símbols:

$$(\alpha\alpha^7)(1\alpha^6).$$

Multipliquem cada bloc per la matriu generadora:

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

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

i obtenim la cadena de símbols

$$\alpha, 2, \alpha^3, \alpha^2 \quad 1, \alpha^3, \alpha^2\alpha$$

que correspon a la cadena de trits

$$01201211 \quad 10121101.$$

Solució de l'Exercici 12

4. La matriu generadora és equivalent a

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

que és equivalent a

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

Per tant, com a matriu de control podem agafar

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

5. Com que hi ha dues columnes linealment dependents i no hi ha cap columna nul·la, la distància mínima és 2.

Solució de l'Exercici 12

6. No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.

   La cadena de trits representa el vector $\alpha\alpha^3 x\alpha^6$. Perquè aquest vector sigui del codi, cal que en multiplicar-lo per H ens doni el vector nul.

$$H \cdot \begin{pmatrix} \alpha \\ \alpha^3 \\ x \\ \alpha^6 \end{pmatrix} = \begin{pmatrix} \alpha^7 + x \\ 0 \end{pmatrix}.$$

   Deduïm que

$$x + \alpha^7 = 0.$$

   Per tant, $x = -\alpha^7 = \alpha^3$. La paraula codi corregida és $\alpha\alpha^3\alpha^3\alpha^6$, que correspon a la cadena de trits

$$01121222.$$

Torna a l'exercici (p.70)

Solució de l'Exercici 13

Hem vist que una matriu de control era

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

La síndrome del vector rebut serà

$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 2 \\ 1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} = 2h_2$$

Deduïm que s'ha produït un error a la segona posició de valor 2 i que la paraula enviada era

$$\begin{pmatrix} 2 & 1 & 2 & 1 & 2 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}$$

Torna a l'exercici (p.79)

Solució de l'Exercici 14(a)

En el primer cas, la síndrome és

$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}$$

Aquesta síndrome no és múltiple de cap columna de H, per tant, deduïm que s'ha produït més d'un error. Però sí que es pot escriure de manera única com a combinació lineal de dues columnes com $h_2 + h_5$. Per tant, deduïm que s'ha produït un error a la segona posició de valor 1 i un error a la cinquena posició de valor 1, i que la paraula enviada era

$$\begin{pmatrix} 1 & 2 & 0 & 1 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 2 & 2 \end{pmatrix}$$

Torna a l'exercici (p.82)

Solució de l'Exercici 14(b)

En el segon cas, la síndrome és

$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Aquesta síndrome no és ni nul·la ni múltiple de cap columna de H. Però sí que es pot escriure com a combinació lineal de dues columnes, tot i que es pot fer de dues maneres diferents: $h_4 + h_6$ o bé $2h_2 + h_5$. Per tant, deduïm que s'han produït dos errors i que la paraula enviada era

$$\begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}$$

o bé

$$\begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 2 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 2 & 2 & 1 & 2 \end{pmatrix}$$

Torna a l'exercici (p.82)

Solució de l'Exercici 15

1. 3.
2. 3.
3. 1132321031.

Torna a l'exercici (p.83)

Solució de l'Exercici 16

6. 01110101.
7. 01.

Torna a l'exercici (p.84)

Motivació

Codis lineals

Detecció i correcció d'errors

Solucions

Apèndix: Repàs d'àlgebra lineal i matrius

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Repàs d'espais vectorials I

Un **espai vectorial** sobre $\mathbb{F}$ és un conjunt V amb dues operacions suma '+' i producte '$\cdot$' que satisfan les condicions de la llista. Els elements de V s'anomenen **vectors**, i els de $\mathbb{F}$ s'anomenen **escalars**.

1. El conjunt V és **tancat per la suma**:
   $\mathbf{x} + \mathbf{y} \in V$ per tot $\mathbf{x}, \mathbf{y}, \in V$.
2. La suma és **commutativa**:
   $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ per tot $\mathbf{x}, \mathbf{y} \in V$.
3. La suma és **associativa:**
   $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$ per tot $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.
4. Existeix un **element neure** $\mathbf{0} \in V$ tal que $\mathbf{x} + \mathbf{0} = \mathbf{x}$ per tot $\mathbf{x} \in V$.
5. Per tot $\mathbf{x} \in V$ existeix un **element oposat** $-\mathbf{x}$ pel qual $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$.

Repàs d'espais vectorials II

6. El conjunt V és **tancat** per la multiplicació per escalars: $\alpha \cdot \mathbf{x} \in V$ per tot $\mathbf{x} \in V$.
7. El producte és **distributiu** sobre la suma d'escalars: $(\alpha + \beta) \cdot \mathbf{x} = \alpha \cdot \mathbf{x} + \beta \cdot \mathbf{x}$ per tot $\alpha, \beta \in \mathbb{F}$ i $\mathbf{x} \in V$.
8. El producte és **distributiu** sobre la suma de vectors: $\alpha \cdot (\mathbf{x} + \mathbf{y}) = \alpha \cdot \mathbf{x} + \alpha \cdot \mathbf{y}$ per tot $\alpha, \beta \in \mathbb{F}$ i $\mathbf{x}, \mathbf{y} \in V$.
9. El producte per escalars i el producte a $\mathbb{F}$ són **compatibles**: $(\alpha\beta) \cdot \mathbf{x} = \alpha \cdot (\beta \cdot \mathbf{x})$ per tot $\alpha, \beta \in \mathbb{F}$ i $\mathbf{x} \in V$.
10. La **unitat** $1 \in \mathbb{F}$ satisfà $1 \cdot \mathbf{x} = \mathbf{x}$ per tot $\mathbf{x} \in V$

Repàs d'espais vectorials III

Definició

Un **subespai vectorial** de V és un conjunt tancat per la suma i el producte per escalars. És a dir,

- Si $\alpha \in \mathbb{F}$ i $v \in V$, aleshores $\alpha v \in V$.
- Si $v_1, v_2 \in V$, aleshores $v_1 + v_2 \in V$.

Relacionat: codi lineal (p.19)

Repàs d'espais vectorials IV

Definició

Sigui V un espai vectorial i $\mathbf{x}_1, \ldots, \mathbf{x}_n \in V$. Diem que $\mathbf{x}_1, \ldots, \mathbf{x}_n$ són **linealment dependents** si existeixen $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ no tots nuls pels quals

$$\alpha_1 \mathbf{x}_1 + \ldots + \alpha_n \mathbf{x}_n = \mathbf{0}.$$

Altrament, direm que són **linealment independents**.

En particular, un únic vector és linealment dependent si i només si és el vector nul. Dos vectors són linealment dependents si i només si són proporcionals, és a dir, un vector és el producte de l'altre per un escalar.

Relacionat: distància mínima (p.55)

Repàs d'espais vectorials V

Definició

Un conjunt $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\} \subseteq V$ és un **sistema de generadors** d'un subespai vectorial S si tot element de S es pot escriure com a combinació lineal de $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

Definició

Un conjunt $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\} \subseteq V$ és una **base** del subespai vectorial S si és un sistema de generadors que és linealment indepedent.

Relacionat: matriu generadora (p.23)

Proposició 1

Totes les bases d'un subespai vectorial tenen el mateix nombre d'elements.

Repàs d'espais vectorials VI

Definició

La **dimensió** d'un subespai vectorial $S \subseteq V$ és el nombre d'elements que té qualsevol de les seves bases.

Relacionat: dimensió d'un codi lineal (p.21)

Repàs d'espais vectorials VII

Definició

Si E és un K-subespai vectorial de F i $\dim F = n$, aleshores un **sistema d'equacions impícites** de E és un sistema homogeni d'equacions de K^n les solucions del qual són els (vectors de coordenades dels) elements de E.

Base sistemàtica: Si E és un subespai vectorial de F, $\dim F = n$, $\dim E = k$ i B és una base de F, aleshores una **base sistemàtica** de E en les posicions $\{j_1, \ldots, j_k\}$ (posicions sistemàtiques) és una base $S = \{s_1, \ldots, s_k\}$ on

- $(coord_B(s_i))_{j_r} = 0$ per tot $r \neq i$
- $(coord_B(s_i))_{j_i} = 1$.

Sempre existeix un conjunt de posicions sistemàtiques i una base sistemàtica en aquestes posicions. El conjunt de posicions sistemàtiques i la base sistemàtica són únics si afegim la condició $(coord_B(s_i))_l = 0$ for all $l < j_i$. Aquesta base s'obté per transformacions gaussianes.

Relacionat: matriu generadora sistemàtica (p.31)

Repàs d'espais vectorials VIII

Diem G a la matriu $k \times n$ següent:

$$\begin{pmatrix} \leftarrow & coord_B(s_1) & \rightarrow \\ & \vdots & \\ \leftarrow & coord_B(s_k) & \rightarrow \end{pmatrix}.$$

La submatriu de G formada per les columnes en les posicions sistemàtiques és la matriu identitat $k \times k$ i la submatriu de G formada per les columnes en les posicions no sistemàtiques és una matriu $k \times (n-k)$, que podem anaomenar $\tilde{G}$, que té l'element de la fila r i columna "corresponent a" l igual a $(coord_B(s_r))_l$.

Repàs d'espais vectorials IX

Els elements de E seran combinacions lineals dels elements de S i tindran la forma $u = \lambda_1 s_1, \ldots, \lambda_k s_k = (\lambda_1 \ \ldots \ \lambda_k)G$. Si diem $(x_1, \ldots, x_n) = coord_B(u)$, aleshores, $x_{j_i} = \lambda_i$, per tota posició sistemàtica j_i, mentres que per les posicions no sistemàtiques, $x_l = \sum_i \lambda_i (coord_B(s_i))_l = \sum_i (coord_B(s_i))_l x_{j_i}$. Això ens permet obtenir un sistema de $n-k$ equacions implícites d'un subespai a partir de la base sistemàtica on les equacions són $-\sum_i (coord_B(s_i))_l x_{j_i} + x_l = 0$ per tot $l \notin \{j_1, \ldots, j_k\}$. Diem H a la matriu d'aquest sistema d'equacions. La submatriu de H formada per les columnes en les posicions no sistemàtiques és la matriu identitat $(n-k) \times (n-k)$ i la submatriu de H formada per les columnes en les posicions sistemàtiques és una matriu $(n-k) \times k$ que té l'element de la fila l i columna r igual a $-(coord_B(s_r))_l$, és a dir, la submatriu és $-\tilde{G}^T$.

Relacionat: matrius generadores i de control sistemàtiques (p.46)

Repàs d'espais vectorials X

Definició

El **complement ortogonal** d'un subespai E, que denotem $E^\perp$, és l'espai generat per les files d'una matriu d'un sistema d'equacions implícites de E.

Relacionat: codi dual (p.44)

És independent de la matriu seleccionada.

Té dimensió $n - k$.

$(E^\perp)^\perp = E$

Motivació
Model de comunicació
Codis lineals
Definició
Matriu generadora i codificació
Codificació en símbols i en dígits
Codi dual i matriu de control
Detecció i correcció d'errors
Distància de Hamming i pes
Distància mínima i capacitat correctora
Detecció d'errors
Correcció d'esborralls
Correcció d'errors
Procés de codificació-descodificació
Solucions
Apèndix: Repàs d'àlgebra lineal i matrius
Repàs d'espais vectorials
Repàs de matrius

Repàs de matrius I

Una **matriu** $m \times n$ és un conjunt de $m \cdot n$ elements organitzats en m **files** horitzontals i n **columnes** verticals.

La matriu $n \times m$ que conté com a files les columnes de la matriu anterior i que conté com a columnes les files de la matriu anterior s'anomena la seva **transposada**.

Per exemple, la primera de les matrius següents és una matriu 2×3 mentre que la segona matriu és la seva transposada.

$$A = \begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix}, \quad A^T = \begin{pmatrix} 5 & 9 \\ 1 & 8 \\ 3 & 2 \end{pmatrix}.$$

Anomenem a_{ij} l'element d'A que es troba a la i-èssima fila i a la j-èssima columna.

Repàs de matrius II

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.

Per exemple, la matriu següent és quadrada i la seva diagonal principal és $4, 7, 1$:

$$\begin{pmatrix} 4 & 5 & 0 \\ 2 & 7 & 9 \\ 8 & 6 & 1 \end{pmatrix}$$

La **matriu identitat** d'ordre i és la matriu quadrada amb 1 a la diagonal principal i 0 a la resta de posicions. Per exemple, la matriu identitat d'ordre 3 és

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

Repàs de matrius III

Per multiplicar una matriu per un vector (vertical), multipliquem cadascuna de les files de la matriu pel vector i deixem el resultat a la mateixa altura que ocupa la fila. Per exemple,

$$\begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 41 \\ 94 \end{pmatrix}.$$

En canvi, per multiplicar un vector (horitzontal) per una matriu, multipliquem el vector per cadascuna de les columnes de la matriu i deixem el resultat a la mateixa posició que ocupa la columna. Per exemple,

$$\begin{pmatrix} 3 & 7 \end{pmatrix}\begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix} = \begin{pmatrix} 78 & 59 & 23 \end{pmatrix}.$$

Repàs de matrius IV

Per multiplicar dues matrius, multipliquem la matriu de l'esquerra per cadascuna de les columnes de la matriu de la dreta. Per exemple,

$$\begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 6 & 3 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 41 & 14 \\ 94 & 37 \end{pmatrix}.$$