

Codis correctors d'errors: una aplicació dels cossos finits d'anada i tornada

Xevi Guitart

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
-
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
-
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
-
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
-
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
-
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
- $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
- $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
- ...i van trobar aplicacions inesperades al segle XX!

Cossos finits

- p un primer, $q := p^r$ i $f(x) \in \mathbb{F}_p[x]$ polinomi irreductible de grau r .
- $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ és un cos de q elements.

Exemple: $\mathbb{F}_{16}$

- $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \bar{x} \rightsquigarrow \alpha^4 + \alpha + 1 = 0$.
 - $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$
 - $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$
-
- Introduïts al segle XIX (Gauss, Galois, Jordan,...) com a objectes d'interès purament matemàtic...
 - ...i van trobar aplicacions inesperades al segle XX!

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:

- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - Ex: 0110 es codifica com 01101, mentre que 0100 com 01001
 - Ex: Si hi ha error en un bit es llegirà 1100 → hi ha hagut un error
- Hamming trobà una manera de codificar que pot corregir l'error

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:

- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - Ex: 0110 es troba bé, com 0110, mentre que 0100 com 0100
 - Ex: 0101 té error en un bit, es troba 1 1101, i té negat un error
- Hamming trobà una manera de codificar que pot corregir l'error

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:



- ▶ El codi s'entrava amb targetes perforades indicant un codi binari
- ▶ Un error en un bit (que era freqüent) parava el programa
- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - ▶ 0110 es codifica com 01100, mentre que 0100 com 01001
 - ▶ Si hi ha error en un bit i es llegeix 11100 $\rightsquigarrow$ hi ha hagut un error
- Hamming trobà una manera de codificar que pot **corregir** l'error

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:



- ▶ El codi s'entrava amb targetes perforades indicant un codi binari
- ▶ Un error en un bit (que era freqüent) parava el programa
- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - ▶ 0110 es codifica com 01100, mentre que 0100 com 01001
 - ▶ Si hi ha error en un bit i es llegeix 11100 $\rightsquigarrow$ hi ha hagut un error
- Hamming trobà una manera de codificar que pot **corregir** l'error

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:



- ▶ El codi s'entrava amb targetes perforades indicant un codi binari
- ▶ Un error en un bit (que era freqüent) parava el programa
- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - ▶ 0110 es codifica com 01100, mentre que 0100 com 01001
 - ▶ Si hi ha error en un bit i es llegeix 11100 $\rightsquigarrow$ hi ha hagut un error
- Hamming trobà una manera de codificar que pot **corregir** l'error

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:



- ▶ El codi s'entrava amb targetes perforades indicant un codi binari
- ▶ Un error en un bit (que era freqüent) parava el programa
- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - ▶ 0110 es codifica com 01100, mentre que 0100 com 01001
 - ▶ Si hi ha error en un bit i es llegeix 11100 $\rightsquigarrow$ hi ha hagut un error
- Hamming trobà una manera de codificar que pot **corregir** l'error

Richard Hamming (EUA, 1915-1998)



- Treballà al projecte Manhattan programant calculadores mecàniques
- Al 1946 passà als Bell Labs, per treballar en el Model V:



- ▶ El codi s'entrava amb targetes perforades indicant un codi binari
 - ▶ Un error en un bit (que era freqüent) parava el programa
- Es pot detectar un error en un bit afegint un “bit de paritat”:
 - ▶ 0110 es codifica com 01100, mentre que 0100 com 01001
 - ▶ Si hi ha error en un bit i es llegeix 11100 $\rightsquigarrow$ hi ha hagut un error
- Hamming trobà una manera de codificar que pot **corregir** l'error

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

El codi de Hamming (7,4,3)

- Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits
0000000, 0001011, 0010101, 0011110, 0100110, 0101101
0110011, 0111000, 1000111, 1001100, 1010010, 1011001
1100001, 1101010, 1110100, 1111111
- Propietat: dues paraules codi difereixen com a mínim en tres bits
- 0000 es codifica com 0000000
- 0001 es codifica com 0001011, etc.
- Si es produeix un error, per exemple 0001111
- Resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància ≥ 2 .
- Aquest és el naixement de la teoria de codis correctors d'errors
 - ▶ S'aplica a totes les formes de comunicació digital: transmissió digital de senyal, DVD, Disc durs,...
- Missatges: paraules de $\mathbb{F}_2^4$, Paraules codi: $\mathbb{F}_2^7$
 - ▶ En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$

Viatge d'anada: Teoria de codis

Distància de Hamming

$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n, \quad \text{dh}(u, v) = \#\{i: u_i \neq v_i\}$$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Viatge d'anada: Teoria de codis

Distància de Hamming

$u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n$, $\text{dh}(u, v) = \#\{i: u_i \neq v_i\}$

- És una distància: $d(u, v) \leq d(u, w) + d(w, v)$

Codi de bloc

Un codi de bloc q -ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$

- Distància mínima: $d_C = \min_{\substack{u, v \in C \\ u \neq v}} \text{dh}(u, v)$
- Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors

Problema fonamental de la teoria de codis (obert)

Donats n i d , trobar C de longitud n i distància d amb $\#C$ màxim

- Problema pràctic: trobar bons algorismes de descodificació
 - ▶ Ajuda: posar-hi estructura algebraica

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

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

$$C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis lineals

Codis lineals

Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$

- Si C té dimensió k i distància d , és un codi (n, k, d)
- Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n \rightsquigarrow$ taxa k/n
- C està completament determinat per una base
- Matriu generadora del codi: té per files una base de C
- $C = \{vG: v \in \mathbb{F}_q^k\}$

Hamming (7,4,3)

- $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- $C = \{(v_1, v_2, v_3, v_4)G: v_i \in \mathbb{F}_2\}$

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombroses aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombroses aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombroses aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombres aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombroses aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_i \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algoritme d'Euclides)
- Nombres aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombroses aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombres aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Codis de Reed–Solomon (1960)

- Prenem $n \in [1, 2, \dots, q]$ i $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elements diferents
- Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{ \text{polinomis de grau} < k \} \simeq \mathbb{F}_q^k$
- L'aplicació avaluació en $\alpha = (\alpha_1, \dots, \alpha_n)$ és injectiva:

$$\begin{aligned} \epsilon: \quad \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ f(x) &\longmapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \end{aligned}$$

ja que un polinomi té com a màxim $k - 1$ zeros i $n > k - 1$.

- $\text{RS}_\alpha(k) = \epsilon(\mathbb{F}_q[x]_k)$
- Dos polinomis diferents poden prendre el mateix valor en com a màxim $k - 1$ dels $\alpha_j \rightsquigarrow$ distància del codi $\geq n - (k - 1)$
- Matriu generadora: $V_k(\alpha_1, \dots, \alpha_n)$
- Bons algorismes de decodificació (basats en algorisme d'Euclides)
- Nombroses aplicacions:
 - ▶ CD, DVD, Codis QR
 - ▶ TV digital (RS(255, 239, 16) sobre $\mathbb{F}_{2^8}$)
 - ▶ Sondes del programa voyager: llançades el 1977, encara avui envien fotografies

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim

- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

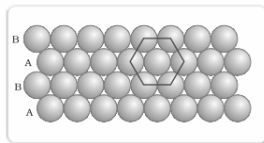
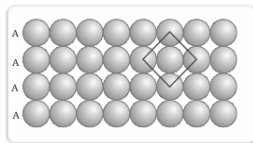
Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim



- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Viatge de tornada: empaquetament d'esferes

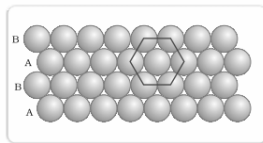
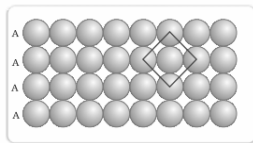
Empaquetament d'esferes a $\mathbb{R}^n$

- Sigui $S \subset \mathbb{R}^n$ una esfera oberta n -dimensional
- $c_1, c_2, \dots$ una seqüència infinita de punts a $\mathbb{R}^n$
- Empaquetament: si els traslladats $c_1 + S, c_2 + S, \dots$ són disjunts
- Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes

Problema

Seleccionar els centres per tal de maximitzar la densitat

- En dimensió 1 el problema és trivial: la densitat màxima és 1
- En dimensió 2 és fàcil trobar l'empaquetament òptim



- En el segon $\delta = \pi/\sqrt{12} \simeq 0.906$, i és òptim (Thue, 1892)

Dimensió 3

- En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$:



- Té $\delta = \frac{\pi/3}{\sqrt{2}} \simeq 0.74$, però és difícil provar aquest δ és òptim
- Conjecturat per Kepler el 1611
- Provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
- En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden
- Fins fa poc, no se sabia el δ òptim per cap $n > 3$

Dimensió 3

- En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$:



- Té $\delta = \frac{\pi/3}{\sqrt{2}} \simeq 0.74$, però és difícil provar aquest δ és òptim
- Conjecturat per Kepler el 1611
- Provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
- En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden
- Fins fa poc, no se sabia el δ òptim per cap $n > 3$

Dimensió 3

- En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$:



- Té $\delta = \frac{\pi/3}{\sqrt{2}} \simeq 0.74$, però és difícil provar aquest δ és òptim
- Conjecturat per Kepler el 1611
- Provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
- En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden
- Fins fa poc, no se sabia el δ òptim per cap $n > 3$

Dimensió 3

- En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$:



- Té $\delta = \frac{\pi/3}{\sqrt{2}} \simeq 0.74$, però és difícil provar aquest δ és òptim
- Conjecturat per Kepler el 1611
- Provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
- En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden
- Fins fa poc, no se sabia el δ òptim per cap $n > 3$

Dimensió 3

- En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$:



- Té $\delta = \frac{\pi/3}{\sqrt{2}} \simeq 0.74$, però és difícil provar aquest δ és òptim
- Conjecturat per Kepler el 1611
- Provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
- En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden
- Fins fa poc, no se sabia el δ òptim per cap $n > 3$

Dimensió 3

- En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$:



- Té $\delta = \frac{\pi/3}{\sqrt{2}} \simeq 0.74$, però és difícil provar aquest δ és òptim
- Conjecturat per Kepler el 1611
- Provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
- En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden
- Fins fa poc, no se sabia el δ òptim per cap $n > 3$

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions 8 i 24: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions 8 i 24: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions 8 i 24: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
 - Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
 - Col·lecció de centres amb bones propietats d'empaquetament
-
- Dimensions 8 i 24: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
 - En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions **8** i **24**: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions **8** i **24**: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions **8** i **24**: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Empaquetaments i codis

Construcció fonamental

- Morfisme de reducció mòdul p : $\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$
- Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$
- Col·lecció de centres amb bones propietats d'empaquetament
- Dimensions **8** i **24**: dos empaquetaments E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis:
 - ▶ Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat)
 - ▶ Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$
- En els dos casos $\pi^{-1}(C)$ té “forats” molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la drete té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la drete té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:

▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:

$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$

- ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
- ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

Codis cíclics

- Isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$
- L'espai de la dreta té una estructura d'anell

Codi cíclic

El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$

- Obs: si $(a_0, a_1, \dots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1x + \dots + a_{n-1}x^{n-1})$ és del codi i per tant $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$
- Tot codi cíclic és generat per un polinomi $f \mid x^n - 1$
- Codi de Golay binari:
 - ▶ A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:
$$(x+1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$
 - ▶ És el generat per un dels factors de grau 11, és un codi (23, 12, 7)
 - ▶ El codi estès (24, 12, 8) s'obté afegint un bit de paritat

El reticle de Leech

- El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat.
- El 1968 va calcular el grup d'automorfismes de Λ_{24} , que té cardinal $2^{22}3^95^47^211 \cdot 13 \cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.
- El reticle E_8 té densitat $\pi^2/384 \simeq 0.2536695079010480$
- El reticle de Leech Λ_{24} té densitat $\pi^{12}/12! \simeq 0.0019295743094039$
- No és gens evident que aquests reticles donin la densitat òptima...

El reticle de Leech

- El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat.
- El 1968 va calcular el grup d'automorfismes de Λ_{24} , que té cardinal $2^{22}3^95^47^211 \cdot 13 \cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.
- El reticle E_8 té densitat $\pi^2/384 \simeq 0.2536695079010480$
- El reticle de Leech Λ_{24} té densitat $\pi^{12}/12! \simeq 0.0019295743094039$
- No és gens evident que aquests reticles donin la densitat òptima...

El reticle de Leech

- El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat.
- El 1968 va calcular el grup d'automorfismes de Λ_{24} , que té cardinal $2^{22}3^95^47^211 \cdot 13 \cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.
- El reticle E_8 té densitat $\pi^2/384 \simeq 0.2536695079010480$
- El reticle de Leech Λ_{24} té densitat $\pi^{12}/12! \simeq 0.0019295743094039$
- No és gens evident que aquests reticles donin la densitat òptima...

El reticle de Leech

- El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat.
- El 1968 va calcular el grup d'automorfismes de Λ_{24} , que té cardinal $2^{22}3^95^47^211 \cdot 13 \cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.
- El reticle E_8 té densitat $\pi^2/384 \simeq 0.2536695079010480$
- El reticle de Leech Λ_{24} té densitat $\pi^{12}/12! \simeq 0.0019295743094039$
- No és gens evident que aquests reticles donin la densitat òptima...

El reticle de Leech

- El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat.
- El 1968 va calcular el grup d'automorfismes de Λ_{24} , que té cardinal $2^{22}3^95^47^211 \cdot 13 \cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.
- El reticle E_8 té densitat $\pi^2/384 \simeq 0.2536695079010480$
- El reticle de Leech Λ_{24} té densitat $\pi^{12}/12! \simeq 0.0019295743094039$
- No és gens evident que aquests reticles donin la densitat òptima...

El reticle de Leech

- El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat.
- El 1968 va calcular el grup d'automorfismes de Λ_{24} , que té cardinal $2^{22}3^95^47^211 \cdot 13 \cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.
- El reticle E_8 té densitat $\pi^2/384 \simeq 0.2536695079010480$
- El reticle de Leech Λ_{24} té densitat $\pi^{12}/12! \simeq 0.0019295743094039$
- No és gens evident que aquests reticles donin la densitat òptima...

Maryna Viazovska (Ucraïna, 1984)



- L'any 2017 va provar que E_8 dona la densitat òptima
- Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dona la densitat òptima
- Va rebre la Medalla Fields el 2022
- Elkies i Cohn havien provat que si existeix una funció $f: \mathbb{R}^n \rightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims
- Viazovska va trobar aquesta funció màgia fent servir la teoria de formes modulars

Maryna Viazovska (Ucraïna, 1984)



- L'any 2017 va provar que E_8 dona la densitat òptima
- Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dona la densitat òptima
- Va rebre la Medalla Fields el 2022
- Elkies i Cohn havien provat que si existeix una funció $f: \mathbb{R}^n \rightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims
- Viazovska va trobar aquesta funció màgia fent servir la teoria de formes modulars

Maryna Viazovska (Ucraïna, 1984)



- L'any 2017 va provar que E_8 dona la densitat òptima
- Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dona la densitat òptima
- Va rebre la Medalla Fields el 2022
- Elkies i Cohn havien provat que si existeix una funció $f: \mathbb{R}^n \rightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims
- Viazovska va trobar aquesta funció màgia fent servir la teoria de formes modulars

Maryna Viazovska (Ucraïna, 1984)



- L'any 2017 va provar que E_8 dona la densitat òptima
- Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dona la densitat òptima
- Va rebre la Medalla Fields el 2022
- Elkies i Cohn havien provat que si existeix una funció $f: \mathbb{R}^n \rightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims
- Viazovska va trobar aquesta funció màgia fent servir la teoria de formes modulars

Maryna Viazovska (Ucraïna, 1984)



- L'any 2017 va provar que E_8 dona la densitat òptima
- Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dona la densitat òptima
- Va rebre la Medalla Fields el 2022
- Elkies i Cohn havien provat que si existeix una funció $f: \mathbb{R}^n \rightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims
- Viazovska va trobar aquesta funció màgia fent servir la teoria de formes modulars

Maryna Viazovska (Ucraïna, 1984)



- L'any 2017 va provar que E_8 dona la densitat òptima
- Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dona la densitat òptima
- Va rebre la Medalla Fields el 2022
- Elkies i Cohn havien provat que si existeix una funció $f: \mathbb{R}^n \rightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims
- Viazovska va trobar aquesta funció màgia fent servir la teoria de formes modulars