Codis de bloc

Francesc Tiñena

Departament de Matemàtiques, UPC

Assignatura TCI (FIB), curs 2025-26q1

Exemple: el bit de paritat

- Si transmetem «tal qual» els possibles errors de transmissió que es cometin seràn indetectables per a nosaltres
- Habitualment hi ha errors $\Longrightarrow$ cal protegir la informació
  - Un mètode elemental consisteix, simplement, en dividir la informació en blocs de k bits i afegir, a cada un d'aquests blocs, un bit de paritat
  - Si elegim paritat parell el bit de paritat ha de ser 0 si en el bloc de k bits hi ha un nombre parell de 1's i el bit de paritat ha de ser 1 si en el bloc de k bits hi ha un nombre imparell de 1's.
  - La manera de protegir la informació enviada consisteix en afegir bits (afegir redundància controlada)
- El procés descrit consisteix en
  - dividir la informació a transmetre en blocs d'extensió k
  - afegir a cada un d'aquests blocs r símbols de redundància

Redundància

- Moltes fonts generen seqüències redundants
- Abans d'afegir la redundància controlada que ens permetrà detectar errros de transmissió, serà bo comprimir la informació a transmetre (per eliminar la redundància "descontrolada" de la font). Això es fa amb el codificador de font que ja hem estudiat a l'altra part del curs
- Les entrades al codificador de canal seràn blocs de k símbols presos d'un alfabet A i les sortides, blocs de n símbols del mateix alfabet ($n > k$). La redundància serà $r = n - k$. El procés de codificació és una aplicació de A^k (o d'una part de A^k) en A^n

Codificació binària (1)

- Exemple de codificació (binària):

$$\begin{aligned} 00 &\rightarrow 00000 \\ 01 &\rightarrow 01001 \\ 10 &\rightarrow 10110 \\ 11 &\rightarrow 11111 \end{aligned}$$

- El codi és $C = \{00000, 01001, 10110, 11111\}$. Cada paraula-codi té longitud 5 i la longitud dels misssatges a codificar és 2: es tracta d'un codi $[5, 2]$. En les codificacions no cal, encara que és bo fer-ho, respectar l'esquema "paraula-codi = missatge + redundància"

Codificació binària (2)

- Un altre exemple de codificació:

$$\begin{array}{lcllcl} 000 & \to & 110000 & 100 & \to & 100001 \\ 001 & \to & 101000 & 101 & \to & 010001 \\ 010 & \to & 100100 & 110 & \to & 001001 \\ 011 & \to & 100010 & 111 & \to & 000101 \end{array}$$

- En aquest cas el codi és

$$C = \{110000, 101000, 100100, 100010, 100001, 010001, 001001, 000101\}$$

Aquest codi té longitud 6 i els missatges tenen longitud 3: es tracta d'un codi $[6, 3]$

Taxa d'un codi

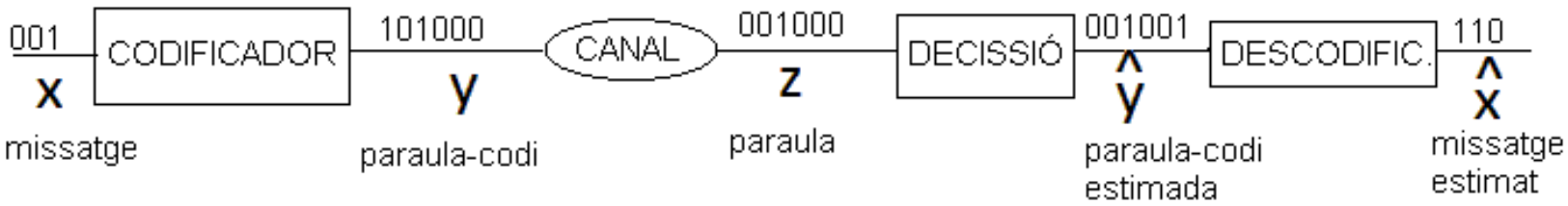
- Al codificador (de canal) li arriben *missatges* (blocs de k símbols) que el codificador transforma en *paraules-codi* (blocs de n símbols). Un paràmetre important d'un codi és la *taxa del codi* (o taxa d'informació del codi). Aquesta es defineix com la raó entre la longitud del missatge i la longitud de la paraula-codi:

$$R = \frac{k}{n}$$

A l'extrem receptor del canal, en general i degut als errors de transmissió, tindrem tires de símbols de longitud n que no són paraules-codi. Les anomenarem, simplement, *paraules*. Aquestes paraules han d'entrar a un mòdul de decissió on s'estimi la paraula-codi transmesa. Finalment, caldrà descodificar la paraula-codi estimada per obtenir el missatge estimat

Esquema codificador-descodificador

- Gràficament l'esquema és el següent:



- Com es veu, la paraula-codi estimada pot no coincidir amb la paraula-codi transmesa. En altres paraules, es poden cometre errors. El que es preten amb la codificació de canal és que la taxa d'error es mantingui en uns nivells acceptables

Distància de Hamming (1)

- En aquesta segona part del curs estudiarem com protegir la informació que s'envia
- Un paràmetre fonamental associat a un codi C és la seva distància de Hamming. Abans de definir la distància de Hamming d'un codi, definim la distància de Hamming entre paraules (tires de n símbols)

Definition

La distància de Hamming entre dues paraules z_1 i z_2 és el nombre de posicions en les quals difereixen.

- Per exemple, $d(00101, 01111) = 2$, $d(001100, 000100) = 1$. Amb alfabets no binaris la definició és la mateixa. Per exemple, si l'alfabet és $A = \{0, 1, 2, 3\}$ llavors $d(3323, 3123) = 1$

Distància de Hamming (2)

- La distància de Hamming té les propietats
  - $d(z_1, z_2) \geq 0$. $d(z_1, z_2) = 0$ si i només si $z_1 = z_2$
  - $d(z_1, z_2) = d(z_2, z_1)$
  - $d(z_1, z_2) \leq d(z_1, z) + d(z, z_2)$ (desigualtat triangular)
- Provem la tercera. Cada paraula de longitud n és la concatenació de n paraules de longitud 1 i la distància de Hamming entre dues paraules de longitud n és la suma de les distàncies de Hamming de cada component (de longitud 1). És suficient provar la proposició pel cas de longitud igual a 1:
  - Siguin u,v,w paraules de longitud 1 i veiem que

$$d(u, v) \leq d(u, w) + d(w, v)$$

  - Si $u = v$, la desigualtat és clara i si $u \neq v$ el membre esquerra de la desigualtat val 1 i el terme dret valdrà com a mínim 1 ja que w no pot ser simultàniament igual a u i a v

Distància de Hamming (3)

Definition

La distància de Hamming d'un codi C és

$$d = \min\{\, d(y_1, y_2) : y_1, y_2 \in C, \quad y_1 \neq y_2\}$$

- Per calcular-la cal fer, en principi, $\binom{M}{2} = \frac{1}{2}M(M-1)$ comparacions. En els codis lineals, que seran els que estudiarem, veurem que aquesta quantitat es pot reduïr molt.
- Hem parlat del codificador (converteix missatges a paraules-codi), hem parlat del canal (introdueix errors). El bloc que ve a continuació és el bloc de decissió. Allí cal estimar la paraula-codi transmesa en funció de la paraula rebuda. Per això ens caldrà algun "esquema de decisió"

Decisió per mínima distància

- Un de molt atractiu és l'esquema de mínima distància:
  - si la paraula rebuda, z, és paraula-codi, estimem que la paraula-codi transmesa coincideix amb la paraula rebuda: $\widehat{y} = z$
  - si la paraula rebuda, z, no és paraula-codi busquem, entre totes les paraules-codi y, aquella que més s'hi acosti en el sentit de fer mínima la distància $d(z, y)$
  - si hi ha més d'una paraula-codi que minimitzi la distància estimem que s'ha transmès qualsevol d'elles
- L'última decisió és discutible: podriem haver optar per no fer cap estimació de la paraula-codi transmesa
- Quan, per qualsevol paraula rebuda, farem una estimació de la paraula-codi transmesa, parlarem d'*esquema de descodificació complet*. Quan no prendrem cap decisió per algunes paraules rebudes parlarem d'*esquema de descodificació incomplet*

Decisió per màxima probabilitat

- El criteri de mínima distància és un criteri amb molt d'atractiu "geomètric" però, és un bon criteri? Per intentar respondre a aquesta qüestió preguntem-nos què és el que es preten amb la decisió
- Sembla clar que amb tota decisió el que es pretén és equivocar-se poc, cosa que sembla més relacionada amb conceptes probabilístics que no pas amb la distància de Hamming
- Si rebem z, hauriem de decidir que hem enviat $\widehat{y}$ si

$$p(\widehat{y} \mid z) = \max_{y} p(y \mid z)$$

Decisió per mínima distància i per màxima probabilitat

- Es pot demostrar (no ho farem) que, sota certes condicions, l'esquema de descodificació per mínima distància coincideix amb l'esquema de descodificació de màxima probabilitat
- En la resta de les diapositives utilitzarem només l'esquema de descodificació per mínima distància

Capacitat correctora d'un codi (1)

- Es diu que un codi corregeix e errors si el descodificador, amb l'esquema de decisió de mínima distància, és capaç de corregir qualsevol patró de e errors o menys

Theorem

Un codi amb distància mínima $d = 2e + 1$ corregeix e errors

Proof.

A la dispositiva següent □

Capacitat correctora d'un codi (2)

- Sigui A^n el conjunt de totes les paraules. Definim, per a cada paraula-codi y, l'esfera de centre y i radi e:

$$S(y, e) = \{z \in A^n : d(z, y) \leq e\}$$

- Veiem primer que si y_1 i y_2 són paraules-codi diferents llavors

$$S(y_1, e) \cap S(y_2, e) = \emptyset$$

  - Per això només cal suposar el contrari i arribar a una contradicció: si $z \in S(y_1, e) \cap S(y_2, e)$ llavors $d(z, y_1) \leq e$ i $d(z, y_2) \leq e$
  - Per la desigualtat triangular tindríem que

$$d(y_1, y_2) \leq d(y_1, z) + d(z, y_2) = d(z, y_1) + d(z, y_2) = 2e$$

cosa que no pot ser ja que la distància mínima del codi és $2e+1$

Capacitat detectora i correctora d'un codi (1)

- Observem que el mateix codi amb distància mínima $d = 2e+1$ pot ser utilitzat només per a detectar errors. En aquest cas, el codi amb distància mínima $d = 2e + 1$ pot detectar $2e$ errors
  - Per exemple, un codi amb distància mínima igual a 3 pot corregir un error o, si s'utilitza exclusivament per a detectar errors, en pot detectar 2. En general tenim el resultat següent:

Theorem

Un codi amb distància (mínima) igual a d pot corregir $\lfloor \frac{d-1}{2} \rfloor$ errors. Si s'utilitza només per a detecció, pot detectar $d-1$ errors

Capacitat detectora i correctora d'un codi (2)

- Els codis també poden ser utilitzats simultàniament per a corregir i detectar errors: per exemple si en el nostre sistema és relativament freqüent que es cometi un error per bloc (de n bits) però en canvi quasi mai es produeixin 2 errors en el mateix bloc
  - Per corregir 2 errors cal un codi amb distància igual a 5
  - Per corregir un error i detectar-ne dos (per demanar retransmissió del bloc, per exemple) en tindrem prou amb un codi amb distància igual a 4
  - I un codi amb distància igual a 4 necessita menys redundància que un codi amb distància igual a 5

Theorem

Un codi amb distància $d = 2k$ pot corregir $k - 1$ errors i, simultàniament, detectar-ne k

Codificacions lineals (1)

- Codificar és assignar a cada missatge (bloc de k dígits) una paraula-codi (bloc de n dígits)
- Una codificació $f : Z_2^k \longrightarrow Z_2^n$ és lineal si

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$

- Parlarem de codi (n, k) per referir-nos a una codificació com l'anterior. n és la longitud de cada paraula-codi (longitud del codi) i k és la longitud dels missatges ($n > k$). L'ús del parèntesi () voldrà dir que estem en presència d'una codificació lineal
- Com cal entendre la suma $(+)$?
  - Missatges i paraules-codi són tires de bits
  - la suma és bit a bit (sense cap tipus de carry)
  - Per a poder sumar paraules cal saber sumar bits individualment. La suma que cal prendre és la suma mòdul 2

Codificacions lineals (2)

- En una codificació lineal la codificació de qualsevol missatge es pot determinar a partir de les codificacions d'una base de Z_2^k
  - Per exemple, si

missatge	paraula-codi
100	1001
010	0101
001	0011

llavors:

missatge	paraula-codi
000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111

Matriu de codificació (1)

- L'operació de codificar es pot representar en forma matricial:

$$y = xG$$

x és el missatge a codificar (vector-fila de longitud k), y és la paraula-codi corresponent (vector-fila de longitud n) i G és la *matriu de codificació* o *matriu generadora del codi*. Les files de G són les paraules-codi associades als elements de la base canònica. En el nostre cas:

$$(y_3, y_2, y_1, y_0) = (x_2, x_1, x_0) \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Matriu de codificació (2)

- Per exemple, el missatge (101) es codificarà com

$$(101)\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = (1010)$$

- La *matriu generadora* G d'un codi (n, k) és una matriu $k \times n$. Observem que la linealitat de la codificació implica que el missatge 0 es codifica sempre amb la paraula-codi 0
- Una codificació ha d'assignar paraules-codi diferents a missatges diferents. I això vol dir que el procés de codificació és una aplicació injectiva o, el que és el mateix, que les files de la matriu G han de ser independents

Pes d'una paraula-codi

- Un concepte important per a codis lineals és el concepte de *pes* (o *norma*) d'una paraula-codi

Definition

El pes d'una paraula-codi és el nombre de components no nul.les

- Per exemple, el pes de la paraula 110000010 és 3:

$$w(110000010) = 3$$

- El pes mínim d'un codi C es defineix com el mínim dels pesos de totes les paraules-codi no nul.les:

$$w_{\min}(C) = \min\{w(y) : y \in C, \quad y \neq 0\}$$

Relació entre pes mínim i distància mínima

Theorem

Si C és un codi lineal llavors

$w(y) = d(y, 0)$

$d(y_1, y_2) = w(y_1 - y_2)$

- Una conseqüència immediata d'aquesta última proposició és que, en codis lineals,

$$\boxed{w_{\min} = d_{\min}}$$

Exemple1

- Suposem un codi amb matriu de codificació

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

- Calculem la longitud dels missatges i la longitud del codi. Escrivim totes les paraules-codi, codifiquem el missatge $x = (1110)$ i calculem la distància mínima del codi

Exemple2

- Veiem si les matrius

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

generen el mateix codi o no

Exemple3

- Diagonalitzem la matriu de codificació

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

i obtinguem una matriu G' (Gauss-Jordan)
Si és massa llarg procediu amb G_2

Codificacions sistemàtiques

- G i G' generen el mateix codi però la codificació donada per G' és més atractiva
- En G' codificar és afegir redundància
- Es diu que la codificació donada per G' és una *codificació sistemàtica*
- "Diagonalitzant" s'ha fet un intercanvi de paraules-codi de manera que
  - la nova codificació continua essent lineal
  - el codi generat (conjunt de totes les paraule-codi) és el mateix
  - la nova codificació és sistemàtica
- Intentarem usar sempre codificacions sistemàtiques. En aquestes la matriu de codificació G està particionada en dos blocs: la matriu identitat i una matriu de paritat

$$\text{Una codificació } G \text{ és sistemàtica} \iff G = (I \,|\, P)$$

Codis equivalents

- Per codis (n, k) les dimensions de les matrius G, I, P són:

$$\begin{aligned} G &\rightarrow k \times n \\ I &\rightarrow k \times k \\ P &\rightarrow k \times r, \qquad r = n - k \end{aligned}$$

- Si en un codi (conjunt de totes les paraules-codi) fem un intercanvi en l'ordre de les coordenades (de les paraules-codi) el que obtindrem serà un altre codi, diferent a l'anterior però amb les mateixes capacitats detectores/correctores que el codi inicial. Direm que els dos codis són *equivalents*. És fàcil veure que tot codi lineal és equivalent a un de sistemàtic: només cal permetre, en el procés de diagonalització de G, fer intercanvis de columnes. Els intercanvis de columnes es corresponen amb intercanvis de coordenades de les paraules-codi.

Exemple

- Considerem la codificació lineal

missatge	paraula-codi
100	00011
010	00101
001	11000

Trobeu un codi sistemàtic equivalent a l'anterior

Descodificació

- Situem-nos al receptor i suposem que ens arriba un paraula z. Per descodificar-la el primer que caldrà fer és mirar si z és una paraul-codi o no. En cas afirmatiu, interpretarem que no s'han comès errors i descodificarem $\widehat{y} = z$. Però, com "mirar" si z és una paraula-codi o no?
- Les paraules-codi són els elements del subespai generat per les files de G. El problema es redueix a mirar si un vector-fila pertany a no al subespai generat per altres vectors-fila
- Mirar si w pertany al subespai generat per els vectors $\{v_1, v_2, ..., v_k\}$ equival a veure si w és o no és ortogonal a tots els vectors d'una basse de l'espai ortogonal al conjunt $\{v_1, v_2, ..., v_k\}$ (espai dels vectors que són ortogonals a tots els v_i)

Matriu de comprovació

- La comprovació es redueix a veure si $(z_1, z_2, \ldots, z_n)$ satisfà un sistema (lineal, homogeni) d'equacions o no:

$$Hz^t = 0$$

- Les files de H són una base de l'espai ortogonal a les files de G
- H s'anomena «matriu de comprovació» i està formada pel màxim nombre de files independents de manera que $GH^t = 0$
- L'elecció de H no és única
- Per codificacions sistemàtiques és immediat obtenir una H:

Theorem

Si G és una codificació sistemàtica, $G = (I_k \mid P)$, llavors una matriu de comprovació per G és $H = (-P^t \mid I_r) = (P^t \mid I_r)$, en el cas de codis binaris. $r = n - k$

Matriu de codificació i matriu de comprovació

- És clar que si el codi forma un subespai de dimensió k de Z_2^n llavors l'espai ortogonal al codi serà de dimensió $n-k=r$. Vol dir això que la matriu H té el nombre de files que ha de tenir. Comprovem que $GH^t=0$:

$$GH^t=(I_k\mid P)(-P^t\mid I_r)^t=(I_k\mid P)\left(\begin{array}{c}-P\\\hline I_r\end{array}\right)=-I_kP+PI_r=-P+P=0$$

- G és una matriu $k\times n$ i H és matriu $r\times n$
  - n (nombre de columnes) és la longitud de les paraules (de les paraules-codi i de les paraules-no-codi)
  - k és la longitud dels missatges i
  - r és la redundància ($r=n-k$)

Exemple

- Trobeu una matriu de comprovació H per a la matriu de codificació

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

i mireu si les paraules rebudes $z_1 = (11011)$ i $z_2 = (10110)$ són paraules-codi o no

Matriu de comprovació en forma estàndard

- Sovint resulta més útil H que la pròpia G. De fet, és freqüent llegir coses de l'estil "considerem un codi amb matriu de comprovació H...". En aquest casos caldrà saber trobar una matriu de codificació G a partir de H. Si la matriu H, de dimensions $r \times n$, té la forma

$$H = (Q \mid I_r)$$

llavors direm que H està en *forma estàndar*. En aquest cas el codi sistemàtic associat és:

$$G = (I_k \mid -Q^t) = (I_k \mid Q^t), \qquad \text{si el codi és binari} \qquad (k = n-r)$$

Exemple1

- Considereu el codi amb matriu de comprovació

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

Calculeu els paràmetres n, k, r i codifiqueu el missatge que té totes les components iguals a 1

Exemple2

- (Matriu de comprovació en forma no estàndard). Trobeu una matriu generadora, en forma sistemàtica si és possible, del codi la matriu de comprovació del qual és

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

Relació entre la matriu H i la distància mínima

Theorem

Considerem un (n, k)-codi amb matriu de comprovació H

$$d_{\min} \geq s \iff \text{cada } s-1 \text{ columnes de } H \text{ són independents}$$

Proof.

El que es demostra és que

$$d_{\min} \leq s-1 \iff \text{existeixen } s-1 \text{ columnes de } H \text{ que són dependents}$$

□

Corollary

$d_{\min} = s$ *si*

- cada $s-1$ columnes de H són independents i
- existeix un conjunt de s columnes de H que són dependents

Estimació de l'error amb la taula de Slepian (1)

- Suposem que transmetem una paraula-codi y i que rebem la paraula z. El que ha fet el canal ha estat afegir errors: $z = y + e$
- El descodificador ha d'estimar l'error comès
  - Considerem la següent relació d'equivalència definida en $\mathbb{Z}_2^n$:

$$z \sim z' \iff z - z' \in C \quad (C \text{ és el codi})$$

  - Aquesta relació indueix una partició en el conjunt de les paraules
  - Les classes (classes laterals o cosets) són de la forma $z_i + C$
  - Com que cada coset té 2^k elements, en total hi haurà

$$L = \frac{2^n}{2^k} = 2^{n-k} = 2^r \text{ cosets}$$

Estimació de l'error amb la taula de Slepian (2)

- Si rebem la paraula $z = y + e$ llavors l'error $e = z - y$ pertany al mateix coset que z
- Rebuda z, els possibles errors comesos pertanyen tots ells al coset de z
- Si suposem que l'error comès és de pes mínim (és més probable cometre menys errors que més) estimarem l'error així:

  $\hat{e}$ serà la paraula de pes mínim del coset de z

- Aquesta paraula de pes mínim de cada classe (o una d'elles si n'hi ha més d'una) serà la que agafarem com a representant de la classe i l'anomenarem *líder* de la classe

Estimació de l'error amb la taula de Slepian (3)

- Per descodificar construirem una taula (anomenada taula de Slepian o standard array) de $L = 2^{n-k} = 2^r$ files (una per a cada coset) i 2^k columnes (una per a cada paraula-codi) amb els líders de cada classe situats a la primera columna de la taula
- La primera fila contindrà el codi C (paraula líder: 0)
- Com que les classes són traslacions del codi respecte dels líders, escriurem cada classe com la suma del líder amb els elements del codi
- Veiem com es descodifica amb l'ajut de la taula anterior:
  - Si rebem la paraula z... busquem la paraula z a la taula
  - L'error comès en la transmissió és una paraula de la mateixa fila i, d'entre tots els possibles errors comesos, el més probable és el líder: estimarem que la paraula transmesa és la suma de la paraula rebuda amb el líder del coset corresponent
  - Això és una descodificació "per bombolla": cada z es descodifica com la paraula codi de dalt de tot de la seva columna

Exemple (1)

- Considerem el codificador següent:

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

- El codi generat és un codi $(5, 2)$. Les paraules codi són:

$$C = \{00000, 10111, 01110, 11001\}$$

  i la distància mínima és

$$d_{\min} = w_{\min} = 3$$

- Aquest codi serà capaç de corregir 1 error. Taula de cosets:
- A la primera fila hi posarem el codi, amb la paraula 00000 a l'esquerra; l'ordre de les altres paraules-codi és irrellevant

00000	10111	01110	11001

Exemple (2)

- Les files 2 a 8 són pels altres cosets. Per construir la segona fila triarem una paraula que encara no hagi sortit a la taula, per exemple 11111, la possarem a la primera posició (de moment) i farem les sumes de la paraula 11111 amb les paraules-codi de la primera columna:

00000	10111	01110	11001
11111	01000	10001	00110

- Ja hem calculat el segon coset. El líder 01000, però, no està al lloc que li toca. Repetim la construcció però posant el líder bé:

00000	10111	01110	11001
01000	11111	00110	10001

Exemple (3)

- Construïm la tercera fila. Aquesta vegada la farem bé directament. Com que el pes de qualsevol paraula no nula és, com a mínim, 1, agafem com a líder una paraula que ho hagi sortir anteriorment i que contingui exactament un 1:

00000	10111	01110	11001
01000	11111	00110	10001
10000	00111	11110	01001

Exemple (4)

- Continuem construint cosets amb líders de pes 1:

00000	10111	01110	11001
01000	11111	00110	10001
10000	00111	11110	01001
00100	10011	01010	11101
00010	10101	01100	11011
00001	10110	01111	11000

Exemple (5)

- Encara falten dues files. Construïm la propera amb un líder de pes 2 que no hagi aparegut amb anterioritat: el 00011, per exemple:

00000	10111	01110	11001
01000	11111	00110	10001
10000	00111	11110	01001
00100	10011	01010	11101
00010	10101	01100	11011
00001	10110	01111	11000
00011	10100	01101	11010

Exemple (6)

- Última fila. Com que hi ha paraules de pes 2 que encara no han sortit, elegim-ne una d'elles com a líder de l'últim coset:

00000	10111	01110	11001
01000	11111	00110	10001
10000	00111	11110	01001
00100	10011	01010	11101
00010	10101	01100	11011
00001	10110	01111	11000
00011	10100	01101	11010
10010	00101	11100	01011

Exemple (7)

- Fem uns quants exemples de descodificació en aquesta diapositiva i en la següent:
  - $z = 11101$. La busquem a la taula: està la posició (4,4). Vol dir això que l'error comès a la transmissió és una paraula de la mateixa fila i, d'entre tots els possibles errors comesos, el més probable és el líder: $\widehat{e} = 00100$. Estimarem que la paraula rebuda és $\widehat{y} = z + \widehat{e} = 11101 + 00100 = 11001$. La paraula descodificada és la suma de la paraula rebuda amb el líder del coset corresponent. Hem dit que això és una descodificació "per bombolla": cada z rebuda es descodificarà com la paraula codi que apareix a dalt de tot de la seva columna
  - $z = 00111$. La localitzem: està a la posició (2,2) i descodifiquem per bombolla: $\widehat{y} = 10111$

Exemple (8)

- $z = 11100$. Posició (8,3). Per tant, $\widehat{y} = 01110$. Fixem-nos que això equival a dir que l'error comès és el lider de classe: $\widehat{e} = 10010$. En el mateix coset, però, hi ha una altra paraula de pes 2: 00101. Vol dir això que és igualment probable que l'error sigui l'estimat com que l'error sigui $\widehat{e_1} = 00101$. Observem que el nostre codi només tenia capacitat de corregir 1 error i que, en la paraula rebuda, hi ha un mínim de dos errors: hem excedit la capacitat correctora del codi. Una alternativa a la descodificació per bombolla, en el cas de que s'hagi excedit la capacitat del codi, consisteix, simplement, en no descodificar. En un cas com el presentat el codificador actuaria comunicant que s'han comès dos errors o més i no faria cap estimació de la paraula-codi transmesa, estariem en presència d'un esquema de descodificació *incomplet*. De fet és una postura força raonable el pretendre descodificar només dins del límits de les capacitats del codi

Les taules de Slepian són massa grans

- A l'any 1972 la sonda Mariner va prendre fotografies del planeta Mart, fotografies que, digitalment, es vàren enviar a la Terra. Per evitar que l'activitat solar i les condicions atmosfèriques introduïssin errors en les fotografies es va utilitzar una codificació binària (32,6). La taula de Slepian necessària per a descodificar les fotografies seria una taula amb 2^{32} caselles, cada una d'elles amb una paraula de 32 bits (4 bytes) en el seu interior. Això requereix una memòria de $2^{32} \times 4$ bytes, més de 17 Gbytes. Sembla clar que vàren descodificar d'una altra manera
- Com reduir les dimensions de la taula? Si només descodificarem quan el nombre estimat d'errors és corregible amb el nostre codi, com que de la taula de Slepian només s'utilitzen els líders dels cosets, si tinguéssim alguna manera d'identificar-los, sembla que podríem quedar-nos únicament amb la primera columna

Síndromes (1)

- La síndrome d'una paraula z és $s(z) := Hz^t$. Per tant,

Theorem

Dues paraules estan al mateix coset si i només si tenen la mateixa síndrome, és a dir

$$z \sim z' \iff s(z) = s(z')$$

Proof.

$$z \sim z' \iff z - z' \in C \iff H(z - z')^t = 0 \iff$$
$$\iff Hz^t = H(z')^t \iff s(z) = s(z')$$

Síndromes (2)

- A la diapositiva anterior hem vist que els cosets venen caracteritzats per les síndromes
- Per altra part, si $z = y + e$ llavors

$$s(z) = Hz^t = H(y + e)^t = Hy^t + he^t = 0 + He^t = s(e)$$

- Podem substituir la taula de Slepian per una taula amb només dues columnes: una pels errors estimats i l'altra per les síndromes corresponents
- Per descodificar una paraula z calcularem la seva síndrome i veurem quin error li toca

Exemple (1)

- Agafem el codi $(5, 2)$ de l'exemple anterior i completem la taula allí construïda amb la columna de síndromes
- Necessitem les síndromes de cada coset. Però primer necessitarem la matriu de comprovació H
- Com que G és sistemàtic,

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

Exemple (2)

$$s(10000) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$s(01000) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Exemple (3)

$$s(00100) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$s(00010) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Exemple (4)

$$s(00001) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

- No calculem més síndromes ja que només descodificarem aquelles paraules que estimem que només contenen un error. La taula de Slepian amb la columna de síndromes afegida com a primera columna està a la diapositiva següent

Exemple (5)

s^t				
000	00000	10111	01110	11001
110	01000	11111	00110	10001
111	10000	00111	11110	01001
100	00100	10011	01010	11101
010	00010	10101	01100	11011
001	00001	10110	01111	11000
⋮	00011	10100	01101	11010
⋮	10010	00101	11100	01011

Exemple (6)

- Les dues primeres columnes de la taula:

s^t	error
000	00000
110	01000
111	10000
100	00100
010	00010
001	00001

- Descodificació de la paraula $z := 11111$ (diapositiva següent)

Exemple (7)

- Per descodificar $z := 11111$ primer calculem la síndrome:

$$s(11111) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

- Ara mirem a quin error correspon la síndrome i descodifiqiem: $\widehat{e} = 01000$ i $\hat{y} = z + \widehat{e} = 11111 + 01000 = 10111$

Exemple (8)

- Descodifiquem $z' := 10001$:

$$s(10001) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

- En aquest cas la paraula rebuda ja és paraula-codi. Estimarem que no hi ha errors (també ens podem equivocar, és clar): $\widehat{y} = 10001$

Exemple (9)

- Descodifiquem $z'' := 11100$:

$$s(11100) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

- En aquest cas la síndrome no es correspon a cap paraula-codi amb un (o zero) errors. Comuniquem que a la paraula z'' hi ha més d'un error i acabem (no descodifiquem)

Nombres amb la sonda Mariner i taula només amb síndromes i errors

- Refem els nombres amb l'exemple de la sonda Mariner. El codi corregia 7 errors. Nombre d'error-patterns:

$$\binom{32}{1}+\binom{32}{2}+\binom{32}{3}+\binom{32}{4}+\binom{32}{5}+\binom{32}{6}+\binom{32}{7} \simeq 4.5\times 10^6$$

- La taula amb les dues columnes síndromes/errors tindrà una extensió mínima d'unes 4.5×10^6 files, a $32 + 26 = 58$ bits/fila, és a dir, més de 32.6 Mbytes. Això va ser a l'any 1972 $\Longrightarrow$ van descodificar d'una altra manera
- La descodificació mitjançant taules només pot ser útil per codis "molt curts"
- Cal evitar taules i usar mètodes basat en *càlculs*

Codis de Hamming

- Són codis amb capacitat de corregir 1 error
- Els codis de Hamming de paràmetre r són codis (n, k) on

$$n = 2^r - 1, \qquad k = n - r, \qquad d_{\min} = 3$$

(r és la redundància)

- La matriu H tindrà r files i $n = 2^r - 1$ columnes
- Perquè $d_{\min} \geq 3$ cada dues columnes de H han de ser independents (diferents i no nul.les)
- La matriu de comprovació pels codis de Hamming de paràmetre r està formada exactament per les $2^r - 1$ columnes no nules
- Hi ha conjunts de 3 columnes dependents $\implies$ $d_{\min} = 3$
- Elegirem matrius de comprovació en forma estàndar

$Ham(7,4)$ o $H(7,4)$

- Per $r = 3$ tindrem un codi amb $n = 2^r - 1 = 7$ i $k = n - r = 4$: el codi de Hamming $Ham(7,4)$ (o $H(7,4)$)
- La matriu de comprovació per a $H(7,4)$ serà una matriu de 3 files i 7 columnes: totes les que es poden fer amb 3 bits, llevat de la columna 0:

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

o també:

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

entre d'altres

$H(15, 11)$ (1)

- Per $r = 4$ tindrem un codi de Hamming amb paràmetres $n = 2^r - 1 = 15$ i $k = n - r = 11$: el codi de Hamming $H(15, 11)$
- La matriu de comprovació per $H(15, 11)$ serà una matriu de 4 files i 15 columnes: totes les que es poden fer amb 4 bits, llevat de la columna 0. Per exemple:

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

$H(31,26)$, $H(3,1)$

- Per $r = 5$, tindríem $n = 2^5 - 1 = 31$ i $k = n - r = 31 - 5 = 26$, el codi $H(31,26)$
- Cada vegada ens surten codis més llargs però amb millor taxa $R = k/n$
- Per $r = 2$ és $n = 2^2 - 1 = 3$ i $k = n - r = 3 - 2 = 1$. Això és un codi $(3,1)$
- No és gaire difícil comprovar que es tracta d'un codi de repetició (un codi que codifica el missatge x com la paraula-codi xxx)

$H(15, 11)$ (2)

- Practiquem amb $H(15, 11)$ amb H donada anteriorment
- Mirem si $z = (111111111100000)$ és paraula-codi:

$$Hz^t = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

- $Hz^t \neq 0 \implies z = (111111111100000)$ no és paraula-codi

Simplificació de la notació (1)

- Els càlculs són una mica voluminosos (i això que no hem calculat la matriu generadora ni hem codificat res)
- Seria interessant poder simplificar la notació:
  - Podem llegir la matriu de comprovació del codi $H(15, 11)$ per columnes interpretant que cada columna és l'expressió binària d'un dígit hexadecimal. Els dígits hexadecimals són:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$$

  - Suposarem que el bit més significatiu és el de la part superior. Amb aquest conveni, la matriu H s'escriuria com:

$$H = (F\ E\ D\ C\ B\ A\ 9\ 7\ 6\ 5\ 3\ 8\ 4\ 2\ 1)$$

  - Bastant més curta, no?

Simplificació de la notació (2)

- Amb aquesta notació apareix un petit problema. Suposem que rebem la paraula $z = (111111111100000)$. Per saber si z és una paraula-codi o no hem de calcular Hz^t, és a dir

$$(F\,E\,D\,C\,B\,A\,9\,7\,6\,5\,3\,8\,4\,2\,1) \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = F + E + D + C + B + A + 9 + 7 + 6 + 5$$

Simplificació de la notació (3)

- Com se suma tot això?
- I si en lloc de codis binaris usem codis hexadecimals?
- És a dir si els missatges són tires de k dígits hexadecimals i les paraules codi, tires de n dígits hexadecimals?
- Com es calcula la síndrome del missatge $z := 2A090D101B050F0$?

$$s(z) = (F\ E\ D\ C\ B\ A\ 9\ 7\ 6\ 5\ 3\ 8\ 4\ 2\ 1) \begin{pmatrix} 2 \\ A \\ 0 \\ 9 \\ 0 \\ D \\ 1 \\ 0 \\ 1 \\ B \\ 0 \\ 5 \\ 0 \\ F \\ 0 \end{pmatrix} = 2 \cdot F + A \cdot E + 9 \cdot C + D \cdot A + 9 + 7 + B \cdot 6 + 5 \cdot 4 + F \cdot 2$$

Simplificació de la notació (4)

- Comencem amb un exemple més "petit": decidim, pel motiu que sigui, agrupar els bits de dos en dos i agafar com a lletres individuals les combinacions $00, 01, 10, 11$
- El nostre alfabet tindrà quatre símbols: $0, 1, 2, 3$ i, per treballar amb codis lineals, cal saber operar amb aquests símbols
- Com es sumen, com es multipliquen? La suma i la multiplicació ens han de servir per poder fer les típiques manipulacions lineals, bàsicament la resolució de sistemes (lineals)
- Vol dir això que la suma i la multiplicació han de tenir "bones propietats" (propietats anàlogues a les propietats de la suma i multiplicació de nombres reals)

Simplificació de la notació (5)

- Els dígits representen tires (vectors) de bits. La suma ha de ser, per tant, la suma bit a bit (component a component), sense cap tipus de carry:

$$\begin{aligned} 1+2 &= (01)+(10)=(11)=3 \\ 1+3 &= (01)+(11)=(10)=2 \\ 2+3 &= (10)+(11)=(01)=1 \\ x+x &= 0 \end{aligned}$$

- La taula de la suma és:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Simplificació de la notació (6)

- Anem per el producte. $2 \cdot 3$ ha de ser $0, 1, 2$ o 3. No pot ser 0 ja que cap dels factors és zero; no pot ser 2 ja que si $2 \cdot 3 = 2 = 2 \cdot 1$ llavors $3 = 1$
- Per la mateixa raó tampoc pot ser 3. Així doncs $2 \cdot 3 = 1$.
- I $2 \cdot 2$? No pot valer 0 ja que $2 \neq 0$. No pot valer 1 ja que si $2 \cdot 2 = 1 = 2 \cdot 3$ llavors $2 = 3$ i tampoc pot valer 2 ja que en cas de que així fos tindríem $2 = 1$. Per tant, $2 \cdot 2 = 3$. Anàlogament, $3 \cdot 3 = 1$. Taula de la multiplicació:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Exemple

- Resolem una equació lineal sobre $\{0, 1, 2, 3\}$: $2x + 3 = 0$
- "Fem fora el 3". Per a això sumem 3 als dos costats:

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

- "Traiem el 2". Per això multiplicarem els dos membres de l'equació per l'invers del 2. L'invers del 2 és aquell "nombre" que multiplicat per 2 dóna 1. Si mirem la taula de la multiplicació veurem que l'invers del 2 (s'escriu: 2^{-1}) és 3. Així,

$$\begin{aligned} 3 \cdot 2 \cdot x &= 3 \cdot 3 \\ x &= 2 \end{aligned}$$

- Cal anar amb les taules, taules que primer s'han de construir
- Abandonarem la codificació i farem les matemàtiques necessàries per entendre millor aquestes sumes i multiplicacions

Els anells $(\mathbb{Z}_m, +, \cdot, 0, 1)$, m enter, $m > 1(1)$

- Ja es van estudiar a FM (quadrimestre 1) els $\mathbb{Z}_m$
- El conjunt $\mathbb{Z}_m$ és el conjunt de classes de residus mòdul m
  - Per exemple, si $m = 4$, $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ on

$$\overline{0} := \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\} = \overline{4} = \overline{8} = \ldots$$

$$\overline{1} := \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\} = \overline{-3} = \overline{-7} = \ldots$$

$$\overline{2} := \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\} = \overline{6} = \overline{-2} = \ldots$$

$$\overline{3} := \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\} = \overline{-5} = \overline{15} = \ldots$$

Els anells $(\mathbb{Z}_m, +, \cdot, 0, 1)$, m enter, $m > 1$ (2)

- El conjunt $\mathbb{Z}_m$ s'anomena «conjunt dels enters modulars mòdul m», encara que els seus elements no són enters sinó classes d'enters (el conjunt $\mathbb{Z}_m$ és un conjunt quocient)
- Per simplicitat escriurem $0, 1, 2, 3$ en lloc de $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ (o en lloc de $\overline{4}, \overline{-3}, \overline{6}, \overline{-5}$, per exemple)
- En $\mathbb{Z}_m$ es pot definir una suma i un producte (sumant i multiplicant els representats). Seguint amb $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Els anells $(\mathbb{Z}_m, +, \cdot, 0, 1)$, m enter, $m > 1$ (3)

- Ja sabem que la suma i el producte de $\mathbb{Z}_m$ estan ben definits i tenen bones propietats, és a dir per a qualssevol $a, b, c \in \mathbb{Z}_m$:
  - $(a + b) + c = a + (b + c)$
  - $a + b = b + a$
  - $a + 0 = a$
  - $\forall a \exists b\, a + b = 0$ (b, que és únic, és l'«oposat de a»; $b := -a$)
  - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - $a \cdot b = b \cdot a$
  - $1 \cdot a = a$
  - $a \cdot (b + c) = a \cdot b + a \cdot c$
- Un conjunt que contingui un 0 i un 1 ($0 \neq 1$) i en el qual hi hagi definides una suma i un producte que compleixi les anteriors propietats s'anomena «anell». De fet: anell commutatiu (perquè el producte és commutatiu) amb unitat (1)

Els anells $(\mathbb{Z}_m, +, \cdot, 0, 1)$, m enter, $m > 1$ (4)

- A l'anell $\mathbb{Z}_m$ el que NO és cert, en general, és que $\forall a \neq 0 \, \exists b$: $a \cdot b = 1$ (en $\mathbb{Z}_4$ no hi ha cap element que multiplicat per 2 doni 1)
- Si $m = p$ és un nombre primer sí que és cert, en $\mathbb{Z}_p$, que $\forall a \neq 0 \, \exists b$: $a \cdot b = 1$
- Aquest b, que és únic, s'anomena «invers de a»: $b := a^{-1}$
- Un COS és un anell (amb unitat) on tot element no nul és invertible
- Exemples de cossos:
  - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (infinits)
  - $\mathbb{Z}_2 := \{0, 1\}, \mathbb{Z}_p$ (p primer)

Cossos de Galois (cossos finits)

- Es pot demostrar que si un cos té un nombre finit d'elements aquest és p^m on p és un nombre primer i m un enter positiu
- Per aplicacions a la codificació només ens interessarà el cas $p = 2$ (el que agruparem seran bits, de m en m)
- Ens limitarem a estudiar, per tant, els cossos de 2^m elements
- Es pot demostrar que tots els cossos de 2^m elements són isomorfs (llevat de com etiquetem els seus elements, «són el mateix») entre sí
- Al cos de 2^m elements se l'anomena cos de Galois de 2^m elements i se'l representa per $GF(2^m)$ (també se l'anomena cos finit de 2^m elements i es representa per $\mathbb{F}_{2^m}$
- Els elements de $GF(2^m)$ són «tires» de m dígits binaris i se sumen bit a bit (sense carry)

Exemple: el cos $GF(2^2) \equiv GF(4) \equiv \mathbb{F}_4$ (1)

- Ja sabem que els elements de $GF(4)$ (o $\mathbb{F}_4$) són «tires» de 2 digits binaris:

$$\mathbb{F}_4 := \{0, 1, 2, 3\} = \{00, 01, 10, 11\}$$

i ja sabem com se sumen: bit a bit (en $\mathbb{Z}_2$) sense carry:

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

El problema estarà en la multiplicació. Però aquest problema ja l'hem resolt

Exemple: el cos $GF(2^2) \equiv GF(4) \equiv \mathbb{F}_4$ (2)

- Taula de la multiplicació en $GF(4)$:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Exemple: el cos $GF(2^2) \equiv GF(4) \equiv \mathbb{F}_4$ (3)

- Igual que hem trobat la taula de multiplicar del cos $\mathbb{F}_4$, també (amb una mica més de feina) podem trobar la del cos $\mathbb{F}_8$
- Però... i la del cos $\mathbb{F}_{16}$? Aquesta és poc probable que surti d'aquesta manera
- Veurem una manera sistemàtica de construir els cossos $\mathbb{F}_{2^m}$
- El cos $\mathbb{F}_{2^m}$ conté el 0 i el 1. És per tant, una extensió del cos $\mathbb{F}_2 := \{0, 1\}$
- Veiem con s'estén un cos
- I per això millor «recordar» (o «explicar») com es fa per passar del cos dels reals $\mathbb{R}$ al cos dels complexes

Extensions Algebraiques d'un Cos (1)

- Suposem $\mathbb{Q}$ i considerem $p(x) := x^2 - 2$
- $p(x)$ no té cap zero racional, però sí té zeros reals: $\pm\sqrt{2}$
- I com que $\mathbb{Q} \subseteq \mathbb{R}$ i $\sqrt{2} \in \mathbb{R}$, $p(x)$ sí que descompon a $\mathbb{R}$: $p(x) = (x - \sqrt{2})(x + \sqrt{2})$
- $p(x)$ no té cap zero a $\mathbb{Q}$ però sí a $\mathbb{R}$. De fet, en el mínim cos que conté $\mathbb{Q}$ i $\sqrt{2}$, cos que es designa per $\mathbb{Q}(\sqrt{2})$
- Si suposem que només tenim $\mathbb{Q}$ i no tenim $\mathbb{R}$, què és $\sqrt{2}$? Una cosa estranya, no? Una cosa que elevada al quadrat dona 2. Però en $\mathbb{Q}$ no hi ha cap cosa que elevada al quadrat doni 2
- Suposo que el fet de disposar de $\mathbb{R}$ ens ha tranquilitzat molt, sabem què és $\sqrt{2}$ (la diagonal del quadrat unitari, per exemple). Però si no disposésim de $\mathbb{R}$, $\sqrt{2}$ seria una cosa molt rara (cosa –inexistent– que elevada al quadrat dona 2)

Extensions Algebraiques d'un Cos (2)

- Suposem ara el cos dels nombres reals $\mathbb{R}$ i considerem el polinomi a coeficients reals $p(x) := x^2 + 1$
- Aquest polinomi no té cap zero real: $x^2 + 1 = 0 \implies x = \pm\sqrt{-1}$, que no existeix (a $\mathbb{R}$). Suposem ara un cos més gran $\mathbb{K}$ tal que $\mathbb{R} \subseteq \mathbb{K}$ i $\sqrt{-1} \in \mathbb{K}$. En aquest cos més gran sí que tindrà zeros el polinomi $p(x)$. I, de fet, no caldrà agafar aquest «cos més gran», serà suficient agafar el mínim cos que contingui $\mathbb{R}$ i $\sqrt{-1}$. Què és $\sqrt{-1}$? Una cosa rara, no? Donem-li un nom: i: i és la cosa que elevada al quadrat dona -1 (inexistent a $\mathbb{R}$).
- Fixem-nos que estem fent el mateix d'abans, només que ara no tenim una referència com abans
- Veurem com estendre un cos perquè l'extensió contingui les arrels d'un polinomi que no té arrels en el cos original

Extensions Algebraiques d'un Cos (3)

- Si $p(x) \in K[x]$ és un polinomi que no té zeros a K, quina és l'extensió «mínima» de K que conté els zeros de $p(x)$?
- Agafem l'exemple usat. $\mathbb{Q}(\sqrt{2})$ és el mínim cos que conté $\mathbb{Q}$ i $\sqrt{2}$. Aquest serà un subcos de $\mathbb{R}$ però si no volem la referència canviem lleugerament la pregunta: com es pot construir el mínim cos que conté $\mathbb{Q}$ i les arrels del polinomi (irreductible en $\mathbb{Q}[x]$) $x^2 - 2$?
- Resposta usant $\mathbb{R}$: $\mathbb{Q}(\sqrt{2}) := \left\{ a\sqrt{2} + b \ : \ a, b \in \mathbb{Q} \right\} \subseteq \mathbb{R}$

Extensions Algebraiques d'un Cos (4)

- Resposta sense usar $\mathbb{R}$: agafem la «lletra» $\sqrt{2}$, (recordem que no tenim $\mathbb{R}$, només tenim $\mathbb{Q}$ i que $\sqrt{2}$ no és res) que té la propietat que elevada al quadrat és 2 i considerem tots els elements que tenen la forma $a\sqrt{2}+b$, $a,b \in \mathbb{Q}$. Aquests elements són polinomis de primer grau en la lletra $\sqrt{2}$. La suma de dos «nombres» d'aquests és una suma component a component
- Però el producte és més complicat ja que el producte de dos polinomis de grau 1 és un polinomi de grau 2.
- Per assimilar un producte d'aquests a un polinomi de grau 1 cal convenir que cada vegada que tinguem $(\sqrt{2})^2$ ho substituirem pel polinomi 2
- Identificarem el polinomi $(\sqrt{2})^2$ amb el polinomi 2 (identificarem el polinomi $(\sqrt{2})^2-2$ amb el polinomi 0)

Extensions Algebraiques d'un Cos (5)

- Identificar elements és fer un conjunt quocient
- Els conjunts quocient es fan respecte d'una relació d'equivalència: la que identifica amb zero el polinomi $(\sqrt{2})^2 - 2$
- $\mathbb{Q}(\sqrt{2})$ és el conjunt quocient dels polinomis a coeficients racionals en $\sqrt{2}$ mòdul la relació d'equivalència que identifica amb zero el polinomi $(\sqrt{2})^2 - 2$:

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \,/\, \left((\sqrt{2})^2 - 2\right)$$

Extensions Algebraiques d'un Cos (6)

- Tot polinomi $\ell(x)$ es pot dividir entre $x^2 - 2$:

$$\ell(x) = (x^2 - 2) \cdot q(x) + (ax + b)$$
$$0 \equiv (x^2 - 2) \cdot q(x) \implies \ell(x) \equiv ax + b$$

- $\mathbb{Q}[x]/(x^2 - 2)$ té com a elements els de la forma $\overline{ax + b} = \overline{a} \cdot \overline{x} + \overline{b}$. Anomenant $\sqrt{2} = \overline{x}$ els elements de $\mathbb{Q}[x]/(x^2 - 2)$ són

$$a\sqrt{2} + b$$

perquè és clar que $\overline{a} \cdot \overline{x} + \overline{b} \equiv \overline{a_1} \cdot \overline{x} + \overline{b_1} \iff a = a_1$ i $b = b_1$

Extensions Algebraiques d'un Cos (7)

- I això és exactament el mateix que es fa quan es passa dels reals als complexes: $\mathbb{C} = \mathbb{R}(i)$:
- i és la «cosa» que elevada al quadrat dona -1
- $\mathbb{C}$ és el mínim cos que conté $\mathbb{R}$ i i
- $\mathbb{C}$ s'obté identificant, al conjunt de polinomis en i, el polinomi $i^2 + 1$ amb el polinomi 0:

$$\mathbb{C} = \mathbb{R}[i] / (i^2 + 1)$$

Els cossos $GF(2^m)$

- $\mathbb{F}_{2^m}$ pot considerar-se una extensió de $\mathbb{F}_2 := \{0, 1\}$
- Hem vist com construir extensions d'un cos K adjuntant les arrels d'un polinomi irreductible en $K[x]$
- En el nostre cas construirem els cossos de Galois de 2^m elements com a extensions de $\mathbb{F}_2$
- Només necessitem un polinomi irreductible en $\mathbb{F}_2[D]$
- Es senzill demostrar que si $f(D) \in \mathbb{F}_2[D]$ és un polinomi irreductible de grau m llavors el cos

$$\mathbb{F}_2[D]/(f(D))$$

té 2^m elements

- I els polinomis irreductibles $f(D)$ estan tabulats!

Construcció del cos $\mathbb{F}_4$ com a conjunt quocient

- $\mathbb{F}_4$ té com a elements les tires de bits de longitud 2, és a dir $(00), (01), (10), (11)$. Podem pensar en aquests símbols com a polinomis en D: $0, 1, D, D+1$ (respectivament)
- La suma és component a component (en $\mathbb{F}_2$) i per fer el producte necessitem identificar un polinomi (irreductible) de grau 2 amb 0. El polinomi és $D^2 + D + 1$
- És a dir cada vegada que fent un producte en quedi una D^2 la substituirem per $-D-1$, que és el mateix que $D+1$:

$\cdot$	0	1	$2 = (10) = D$	$3 = (11) = D+1$
0	0	0	0	0
1	0	1	2	3
$2 = (10) = D$	0	2	$D^2 = D+1 = (11) = 3$	$D^2 + D = D+1+D = 1$
$3 = (11) = D+1$	0	3	$D^2 + D = D+1+D = 1$	$D^2 + 1 = D+1+1 = D = (10) = 2$

Construcció del cos $\mathbb{F}_8$ com a conjunt quocient (1)

- $\mathbb{F}_8 := \{0, 1, 2, 3, 4, 5, 6, 7\}$. Polinomi que identificarem amb 0: $D^3 + D + 1$

·	0	1	2	3	4	5	6	7
0=(000)	0	0	0	0	0	0	0	0
1 = (001)	0	1	2	3	4	5	6	7
2 = (010)	0	2	4	6	3	1	7	5
3 = (011)	0	3	6	5	7	4	1	2
4 = (100)	0	4	3	7	6	2	5	1
5 = (101)	0	5	1	4	2	7	3	6
6 = (110)	0	6	7	1	5	3	2	4
7 = (111)	0	7	5	2	1	6	4	3

Construcció del cos $\mathbb{F}_8$ com a conjunt quocient (2)

- Calculem, per exemple, $3 \cdot 7$ i $5 \cdot 6$:

$$\begin{aligned} 3 \cdot 7 &= (011) \cdot (111) = (D+1) \cdot (D^2+D+1) = D^3+D^2+D+D^2+D+1 = \\ &= D^3+1 = D+1+1 = D = (010) = 2 \end{aligned}$$

$$\begin{aligned} 5 \cdot 6 &= (101) \cdot (110) = (D^2+1) \cdot (D^2+D) = D^4+D^3+D^2+D = \\ &= D \cdot (D+1) + (D+1) + D^2 + D = D^2+D+D+1+D^2+D = \\ &= D+1 = (011) = 3 \end{aligned}$$

Polinomis irreductibles i cossos (1)

- Hem vist com operar sobre els conjunts $\{0, 1, 2, ..., 2^m - 1\}$. Es tracta d'escriure els elements en binari i pensar cada un d'ells com un polinomi en D. Per poder-los multiplicar cal identificar el polinomi D^m amb algun polinomi, convenientment elegit, de grau inferior o, el que és el mateix, cal identificar amb zero un polinomi $f(D) = D^m + ...$

$$\{0, 1, 2, ..., 2^m - 1\} = Z_2[D] \,/\, (f(D))$$

Polinomis irreductibles i cossos (2)

- Sobre l'elecció del polinomi $f(D) = D^m + \ldots$: l'objectiu és produir cossos i el punt més important a vigilar és que el producte de dos elements diferents de zero no doni zero
- No podem elegir un polinomi qualsevol. Si, a l'exemple anterior, haguéssim elegit $f(D) = D^3 + D^2 + D + 1$, llavors

$$3 \cdot 5 = (011) \cdot (101) = (D+1) \cdot (D^2+1) = D^3 + D + D^2 + 1 = 0$$

- Cal elegir polinomis que no descomposin com a producte de dos, és a dir polinomis irreductibles
- Un polinomi és irreductible si no factoritza com a producte de polinomis de grau inferior

$$Z_2[D]/\ (f(D)) \quad \text{cos} \quad \Longleftrightarrow \quad f(D) \quad \text{irreductible}$$

Polinomis irreductibles i cossos (3)

- Per construïr l'anterior taula de multiplicació hem elegit un polinomi irreductible: $f(D) = D^3 + D + 1$. Com podem veure que aquest polinomi és irreductible?
- Si $f(D)$ descomposés com a producte de 2 factors, un d'ells seria de grau 1 i l'altre de grau 2. I si $f(D)$ admetés un factor de grau 1 llavors $f(D)$ tindria un zero en $Z_2 = \{0, 1\}$. Veiem que $f(D)$ no admet cap zero en Z_2:

$$\begin{aligned} f(0) &= 0^3 + 0 + 1 = 1 \neq 0 \\ f(1) &= 1^3 + 1 + 1 = 1 \neq 0 \end{aligned}$$

- És clar que hi pot haver altres polinomis de grau 3, sobre Z_2, que també són irreductibles

Polinomis irreductibles i cossos (4)

- Com a exercici, calculem-los tots. El llistat de tots els polinomis de grau 3 a coeficients binaris és

$$(1000) = D^3 \qquad (1001) = D^3 + 1$$
$$(1010) = D^3 + D \qquad (1011) = D^3 + D + 1$$
$$(1100) = D^3 + D^2 \qquad (1101) = D^3 + D^2 + 1$$
$$(1110) = D^3 + D^2 + D \qquad (1111) = D^3 + D^2 + D + 1$$

- Cap polinomi de la primera columna és irreductible ja que en tots ells es pot treure D factor comú. D^3+1 i D^3+D^2+D+1 tampoc són irreductibles ja que admeten el zero $D = 1$

Polinomis irreductibles i cossos (5)

- Els irreductibles són $D^3 + D + 1$ i $D^3 + D^2 + 1$
- Podríem haver triat qualsevol dels dos per a la construcció del cos finit de 8 elements. Quan volguem construir un cos finit amb molts elements (2^m elements, m gran) el trobar un polinomi irreductible de grau m pot ser una tasca força complicada
- A efectes pràctics, aquests polinomis estàn tabulats: només cal consultar la taula corresponent
- En general, a més, hi haurà molts polinomis irreductibles per escollir. Quin criteri haurem de seguir per fer una bona elecció? Obtindrem el mateix cos utilitzant un polinomi o un altra?

Polinomis irreductibles i cossos (6)

- Es pot demostrar que per a cada valor de m existeix essencialment un únic cos de 2^m elements, l'anomenat *cos de Galois* $GF(2^m)$
- Com que, en general, es poden fer moltes construccions diferents de $GF(2^m)$ —es poden elegir molts $f(D)$ diferents—, caldria concretar què vol dir el terme "essencialment". Es pot demostrar que totes les construccions del cos $GF(2^m)$ són equivalents en el sentit de que produeixen *cossos isomorfs*, això és, cossos que, llevat dels noms dels elements, són el mateix

Multiplicacions en $\mathbb{F}_q \quad -q = 2^m - (1)$

- Ja sembla resolt el problema de treballar amb alfabets de 2^m elements
- Però aquest problema està resolt només en part: a la pràctica és difícil fer multiplicacions, caldria simplificar-les
- Per això podem tornar a pensar en els nombres complexos. Ja sabem que un mateix nombre complex el podem escriure en forma binòmica o en forma polar. Quan s'utilitza la forma polar la multiplicació esdevé molt senzilla. El que farem a continuació és una mena d'anàlog però amb cossos finits. En concret buscarem una "forma" alternativa per als elements del cos de manera que la multiplicació quedi senzilla. Per això ens basarem en el teorema de la diapositiva següent

Multiplicacions en $\mathbb{F}_q \quad - q = 2^m - (2)$

Theorem

En tot cos finit hi ha un element, diem-ne α*, tal que tots els elements del cos, llevat del* 0*, són potències de* α*:*

$$GF(q) = \{0, \alpha, \alpha^2, \alpha^3, ..., \alpha^{q-1} = 1\}$$

(nosaltres utilitzarem $q = 2^m$)

- Un tal element (α) s'anomena *element primitiu* (del cos)
- Si representem els elements no nuls del cos com a potències d'un element primitiu, haurem resolt el problema de la multiplicació. Per exemple, si

$$GF(8) = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1\}$$

llavors $\alpha^2\alpha^4 = \alpha^6$ o $\alpha^5\alpha^4 = \alpha^9 = \alpha^7\alpha^2 = 1\alpha^2 = \alpha^2$

Multiplicacions en $\mathbb{F}_q \quad -q = 2^m- \ (3)$

- La multiplicació ha deixat de ser un problema! I la suma? Quan val, per exemple, $\alpha^2 + \alpha^5$? L'única cosa que és clara és que

$$\alpha^2 + \alpha^5 = \alpha^2(1 + \alpha^3)$$

- Amb aquesta senzilla igualtat ja hem aconseguit simplificar força la suma: en lloc de necessitar totes les sumes $\alpha^i + \alpha^j$ veiem que només ens calen les sumes $1 + \alpha^i$
- En lloc de necessitar una taula de sumar de dimensions $(q-1) \times (q-1)$, només ens cal un array de longitud $(q-1)$
- Aquest array l'haurem de construir nosaltres a partir de la construcció del cos. Això és el que farem a continuació per el cos $GF(8)$, construit amb el polinomi $f(D) = D^3 + D + 1$

Logaritmes de Zech (1)

Theorem

Sigui $q = 2^m$, $f_m(D) \in Z_2[D]$ *un polinomi irreductible de grau* m *i* $GF(q) = Z_2[D] \,/\, (f_m(D))$ *el cos de Galois de* q *elements. Si*

$$GF(q) = \{0, 1, \alpha, \alpha^2, ..., \alpha^{q-2}\}$$

llavors per cada $i \in \{1, 2, ..., q-2\}$ existeix un únic $Z(i) \in \{1, 2, ..., q-2\}$ tal que

$$1 + \alpha^i = \alpha^{Z(i)}$$

- $Z(i)$ és el *logaritme de Zech* de i

Logaritmes de Zech (2)

- Construïrem la taula de logaritmes de Zech per al cos $GF(8)$, construït amb $f(D) = D^3 + D + 1$ i agafant com a α (la classe d'equivalència d') el polinomi D
- Escrivim els elements del cos com a tires de bits, com a classes de polinomis en D i com a potències de α:

tira de bits	c. de polinomi	potència de α
000	$\overline{0}$	α^∞
001	$\overline{1}$	$\alpha^7 = 1$
010	$\overline{D}$	α
011	$\overline{D+1}$	α^3
100	$\overline{D^2}$	α^2
101	$\overline{D^2+1}$	α^6
110	$\overline{D^2+D}$	α^4
111	$\overline{D^2+D+1}$	α^5

Logaritmes de Zech (3)

- Per construir la columna de la dreta s'han d'anar fent les potències de α i veient amb quin polinomi es corresponen:

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

- Ja podem construir la taula de logaritmes de Zech:

i	$1+\alpha^i$	$Z(i)$
1	α^3	3
2	α^6	6
3	α	1
4	α^5	5
5	α^4	4
6	α^2	2

Logaritmes de Zech (4)

- La columna del mig només és un ajut per fer la construcció, en podem prescindir:

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

- També es pot definir el logaritme de Zech de 0:
  - Com que

$$1 + \alpha^0 = 1 + 1 = 0$$

si introduim un nou símbol ∞ i definim $\alpha^\infty = 0$, resultarà que

$$1 + \alpha^0 = 1 + 1 = 0 = \alpha^\infty$$

  - Per tant $Z(0) = \infty$

Exemple (mirant la taula de logaritmes de Zech)

Example

Calculem $\alpha^2+\alpha^5+1+\alpha^3$ i $\alpha^2+\alpha^{-5}+\alpha^{27}$

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

Per calcular l'altra suma observem, en primer lloc, que $27=7\cdot 3+6$ i, per tant,

$$\alpha^{27}=\alpha^{7\cdot 3+6}=\alpha^{7\cdot 3}\alpha^6=\left(\alpha^7\right)^3\alpha^6=1^3\alpha^6=\alpha^6$$

α^{-5} és l'invers de α^5, per tant $\alpha^{-5}=\alpha^2$
Finalment,

$$\alpha^2+\alpha^{-5}+\alpha^{27}=\alpha^2+\alpha^2+\alpha^6=(\alpha^2+\alpha^2)+\alpha^6=0+\alpha^6=\alpha^6$$

Logaritmes de Zech (5)

- Els logaritmes de Zech depenen de quin element agafem com a α. $\alpha = \overline{D}$ ha funcionat (no ens ha sortit 1 fins la potència α^7). En general però ni $\alpha = \overline{D}$ és primitiu ni és l'únic primitiu. Si en lloc d'agafar $\alpha = \overline{D}$ haguéssim près, per exemple, $\alpha = \overline{D^2 + 1}$, la taula de logaritmes de Zech s'hauria modificat
- Potències de $\alpha = \overline{D^2 + 1}$ i elements del cos:

$$
\begin{aligned}
\alpha^2 &= \overline{\left(D^2+1\right)^2} = \overline{D^4+1} = \overline{DD^3+1} = \overline{D(D+1)+1} = \overline{D^2+D+1} \\
\alpha^3 &= \alpha\alpha^2 = \overline{D^2+1D^2+D+1} = \overline{D^4+D^3+D^2+D^2+D+1} = \\
&= \overline{D(D+1)+(D+1)+D+1} = \overline{D^2+D} \\
\alpha^4 &= \alpha\alpha^3 = \overline{D^2+1D^2+D} = \overline{D^4+D^3+D^2+D} = \\
&= \overline{D(D+1)+(D+1)+D^2+D} = \overline{(D^2+D)+(D+1)+(D^2+D)} = \overline{D+1} \\
\alpha^5 &= \alpha\alpha^4 = \overline{D^2+1}\,\overline{D+1} = \overline{D^3+D^2+D+1} = \overline{(D+1)+D^2+(D+1)} = \overline{D^2} \\
\alpha^6 &= \alpha\alpha^5 = \overline{D^2+1D^2} = \overline{D^4+D^2} = \overline{D(D+1)+D^2} = \overline{D^2+D+D^2} = \overline{D} \\
\alpha^7 &= \alpha\alpha^6 = \overline{D^2+1}\,\overline{D} = \overline{D^3+D} = \overline{D+1+D} = \overline{1}
\end{aligned}
$$

Logaritmes de Zech (6)

- Elements del cos:

tira de bits	c. del polinomi	potència de α
000	0	α^{∞}
001	1	$\alpha^7 = 1$
010	D	α^6
011	$D+1$	α^4
100	D^2	α^5
101	D^2+1	α
110	D^2+D	α^3
111	D^2+D+1	α^2

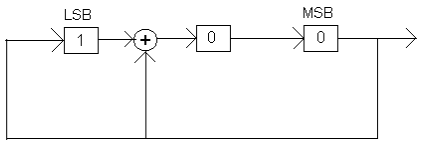
Logaritmes de Zech (7)

- Taula de logaritmes de Zech:

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

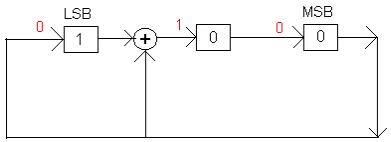
Sobre l'elecció de l'element primitiu (1)

- Ara hem tingut més feina per calcular els logaritmes de Zech
- Una vegada els tenim tabulats ja no s'han de tornar a calcular
- A la pràctica, però, una operació que haurà de fer moltes vegades el nostre maquinari serà calcular potències de α
  - Si $\alpha = \overline{D}$, calcular potències de α serà una feina senzilla
  - Caldrà disposar d'un registre de desplaçament amb les connexions necessàries per implementar la identificació $f(D) = 0$
  - En el cos $GF(8) = Z_2[D] / (D^3+D+1)$ amb $\alpha = \overline{D}$, el maquinari necessari per a calcular potències de α és el dibuixat a continuació. En el dibuix, el contingut actual del registre és 001

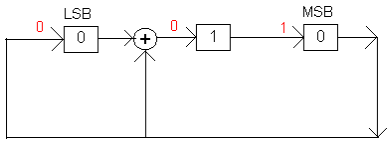


Sobre l'elecció de l'element primitiu (2)

- A cada clock de rellotge el contingut del registre quedarà multiplicat per α:

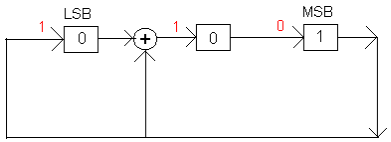


contingut del registre: $001 = 1$ (en vermell, el que entrarà en el següent flanc de pujada del rellotge)

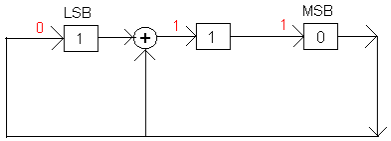


contingut del registre: $010 = \overline{D} = \alpha$

Sobre l'elecció de l'element primitiu (3)

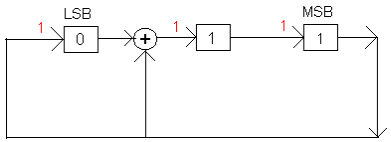


contingut del registre: $100 = \overline{D^2} = \alpha^2$

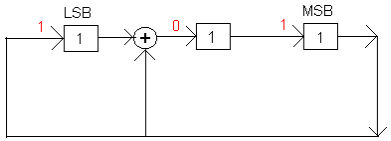


contingut del registre: $011 = \overline{D+1} = \alpha^3$

Sobre l'elecció de l'element primitiu (4)

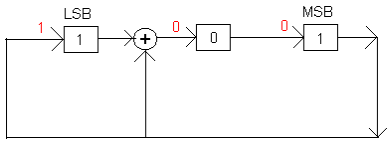


contingut del registre: $110 = \overline{D^2 + D} = \alpha^4$

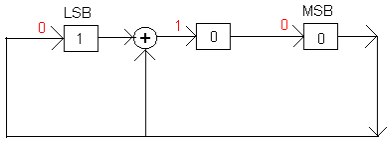


contingut del registre: $111 = \overline{D + D + 1} = \alpha^5$

Sobre l'elecció de l'element primitiu (5)



contingut del registre: $101 = \overline{D^2 + 1} = \alpha^6$



contingut del registre: $001 = \overline{1} = \alpha^7$

Sobre l'elecció de l'element primitiu (6)

- El millor que es pot fer (des d'un punt de vista pràctic) és agafar $\alpha = \overline{D}$
- I si $\alpha = \overline{D}$ no és un element primitiu? En aquest cas elegim un polinomi $f(D)$ de manera que $\alpha = \overline{D}$ sigui primitiu
- Aquests polinomis s'anomenen *polinomis primitius*. Són tipus especial de polinomis irreductibles i també estàn tabulats
- Elegirem $f(D)$ primitiu de grau m —per construir el cos $GF(2^m)$—
- α serà $\overline{D}$
- I si hi ha m és d'un polinomi primitiu de grau m?
- Elegim-ne un de pes mínim (menor nombre possible de 1's)
- Així estalviarem connexions al registre de desplaçament que implementarà la multiplicació per α

Taula de polinomis binaris primitius de grau ≤ 8

D^2+D+1
D^3+D+1
D^3+D^2+1
D^4+D+1
D^4+D^3+1
D^5+D^2+1
D^5+D^3+1
$D^5+D^3+D^2+D+1$
$D^5+D^4+D^2+D+1$
$D^5+D^4+D^3+D+1$
$D^5+D^4+D^3+D^2+1$
D^6+D+1
$D^6+D^4+D^3+D+1$
D^6+D^5+1
$D^6+D^5+D^2+D+1$
$D^6+D^5+D^3+D^2+1$
$D^6+D^5+D^4+D+1$

D^7+D+1
D^7+D^3+1
$D^7+D^3+D^2+D+1$
D^7+D^4+1
$D^7+D^4+D^3+D^2+1$
$D^7+D^5+D^2+D+1$
$D^7+D^5+D^3+D+1$
$D^7+D^5+D^4+D^3+1$
$D^7+D^5+D^4+D^3+D^2+D+1$
D^7+D^6+1
$D^7+D^6+D^3+D+1$
$D^7+D^6+D^4+D+1$
$D^7+D^6+D^4+D^2+1$
$D^7+D^6+D^5+D^2+1$
$D^7+D^6+D^5+D^3+D^2+D+1$
$D^7+D^6+D^5+D^4+1$
$D^7+D^6+D^5+D^4+D^2+D+1$
$D^7+D^6+D^5+D^4+D^3+D^2+1$

$D^8+D^4+D^3+D^2+1$
$D^8+D^5+D^3+D+1$
$D^8+D^5+D^3+D^2+1$
$D^8+D^6+D^3+D^2+1$
$D^8+D^6+D^4+D^3+D^2+D+1$
$D^8+D^6+D^5+D+1$
$D^8+D^6+D^5+D^2+1$
$D^8+D^6+D^5+D^3+1$
$D^8+D^6+D^5+D^4+1$
$D^8+D^7+D^2+D+1$
$D^8+D^7+D^3+D^2+1$
$D^8+D^7+D^5+D^3+1$
$D^8+D^7+D^6+D+1$
$D^8+D^7+D^6+D^3+D^2+D+1$
$D^8+D^7+D^6+D^5+D^2+D+1$
$D^8+D^7+D^6+D^5+D^4+D^2+1$

Codis de Hamming (1)

- Els codis de Hamming $Ham(n,k)$ o $H(n,k)$ són codis lineals amb $n = 2^r - 1$ i $k = n - r$, la matriu de comprovació dels quals té per columnes les expressions binàries dels enters compresos entre 1 i 2^r (cada columna té r components). El codi $H(7,4)$, per exemple, té com a matriu de comprovació:

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

- (La matriu ja està en forma estàndar). Els codis de Hamming tenen $d_{\min} = 3$ i són capaços de corregir un error
- Podem pensar les columnes de la matriu H com elements del cos $GF(2^r)$

Codis de Hamming (2)

- I si en lloc de notar els elements del cos en format "tira de bits" ho fem en el format "potències de α" ($\alpha = \overline{D}$ és un element primitiu; cal suposar que, en la construcció del cos, ja hem triat un polinomi primitiu), la matriu de comprovació per a un $H(n,k)$, $n = 2^r - 1$, és:

$$H = (\alpha^{n-1}, \alpha^{n-2}, ..., \alpha^3, \alpha^2, \alpha, 1)$$

  - H ja està en forma estàndar (les últimes r columnes és la matriu identitat)
  - L'ordre en que estan les $n - r$ primeres columnes sembla el més "natural"
- Ens quedarem amb aquesta forma per a H

Codis de Hamming (3)

- Comencem amb el problema de la descodificació
- Suposem que, per a protegir la informació enviada pel canal, hem utilitzat una codificació $H(n, k)$
- Si el missatge a codificar és x (x és un bloc de k bits), la paraula-codi corresponent és y (y és un bloc de n bits) i la paraula rebuda a l'extrem receptor és z (z també és un bloc de n bits), la condició perquè z sigui paraula-codi és que $Hz^t = 0$:

$$(\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha^2, \alpha, 1) \begin{pmatrix} z_1 \\ z_2 \\ \\ \vdots \\ \\ z_{n-2} \\ z_{n-1} \\ z_n \end{pmatrix} = z_1\alpha^{n-1} + z_2\alpha^{n-2} + \ldots + z_{n-2}\alpha^2 + z_{n-1}\alpha + z_n = 0$$

Codis de Hamming (4)

- Hz^t és un vector-columna binari de dimensió r o, equivalentment, un element de $GF(2^r)$
- Hz^t és la *síndrome* de z
  - Si la síndrome de la paraula rebuda és zero llavors la paraula rebuda és una paraula-codi. En aquest cas interpretarem que no s'ha produit cap error i descodificarem $\widehat{y} = z$
  - Si la síndrome no és zero llavors la síndrome és alguna potència de α. Veiem que, si no hem sobrepassat la capacitat correctora del codi, la síndrome ens permet localitzar l'error.

Codis de Hamming (5)

Theorem

Considerem una codificació de Hamming $H(n,k)$, $n = 2^r - 1$. *Sigui* y *la paraula-codi transmesa i* z *la paraula rebuda*

$$z = y + e$$

Si la paraula d'error, e, *té pes igual a* 1 *i la síndrome de* z *és* $s = Hz^t = \alpha^i$, $i \in \{0, ..., n-1\}$ *llavors l'error està en la posició* $n - i$*:*

$$e = (0, ..., 0, \overset{n-i)}{1}, ..., 0)$$

Codis de Hamming (6)

Proof.

Nomes cal observar que les afirmacions

- l'error està a la component j-èssima, $j \in \{1, \ldots, n\}$
- la síndrome és $s = \alpha^{n-j}$

són equivalents: □

$$Hz^t = H(y+e)^t = Hy^t + He^t = 0 + He^t = (\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha^2, \alpha, 1) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \longleftarrow j)$$

Exemple de descodificació amb $H(7,4)$ (1)

- Recordem que $r = 3$ i recordem també la taula de logaritmes de Zech del $GF(8)$:

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

- Descodifiquem la paraula (1100010):

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

- La síndrome és zero. Això vol dir que (1100010) ja és una paraula-codi

Exemple de descodificació amb $H(7,4)$ (2)

- Descodifiquem la paraula (1101011):

$$s = (\alpha^6, \alpha^5, \alpha^4, \alpha^3, \alpha^2, \alpha, 1) \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1 = (\alpha^6 + \alpha^5) + (\alpha^3 + \alpha) + 1 =$$

$$= \alpha^8 + \alpha^7 + 1 = \alpha + \alpha^7 + 1 = (\alpha + \alpha^7) + 1 = \alpha^3 + 1 = \alpha$$

- La síndrome és $s = \alpha^1$. Això vol dir que s'han comès errors; si només se n'ha comès un, llavors aquest està en la component $7 - 1 = 6$. Estimarem que hem transmès $\widehat{y} = (1101001)$

Els codis de Hamming com a codis perfectes

- Amb els codis de Hamming, qualsevol paraula z està a distància 0 o 1 d'una paraula-codi
- Rebem el que rebem, sempre podem interpretar que s'ha comès un error com a màxim (cosa que no té per què ser certa)
- Els codis amb capacitat de corregir e errors que tenen la propietat de que qualsevol paraula z està a distància no superior a e d'una paraula-codi s'anomen *codis perfectes*
- Els codis de Hamming són codis perfectes. Hi ha altres famílies de codis que són perfectes, no gaires però

Codificació amb codis de Hamming (1)

- Cal trobar a partir de H una matriu G tal que $HG^t = 0$:

$$H := \begin{pmatrix} h_{11} & \dots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{r1} & \dots & h_{rn} \end{pmatrix} \qquad G := \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}$$

$$\forall j = 1, \dots, r \; \forall i = 1, \dots, k \quad h_{j1}g_{i1} + h_{j2}g_{i2} + \cdots + h_{jn}g_{in} = 0$$

- Equivalentment, $\forall i = 1, \dots, k$ cal resoldre els sistemes

$$\left.\begin{array}{c} h_{11}g_{i1} + h_{12}g_{i2} + \cdots + h_{1n}g_{in} = 0 \\ \dots \\ h_{r1}g_{i1} + h_{r2}g_{i2} + \cdots + h_{rn}g_{in} = 0 \end{array}\right\}$$

  sistemes que tenen solució no trivial en ser homogenis i tenir menys equacions (r) que incògnites (n)

- Això és massa complicat, seguirem un altre camí

Un parèntesi: multiplicacions de matrius de bloc

Prop1: Si B és una matriu $n \times k$ que té per columnes $B_1, B_2, \ldots, B_k$, cosa que representarem per

$$B = (B_1|B_2|\ldots|B_k)$$

i A és una matriu $r \times n$ llavors

$$A \cdot B = A \cdot (B_1|B_2|\ldots|B_k) = (AB_1|AB_2|\ldots|AB_k)$$

Prop2: Si A és una matriu $r \times n$ que té per columnes $A_1, A_2, \ldots, A_n$ ($A = (A_1|A_2|\ldots|A_n)$ i v és un vector de dimensió n

$$Av = (A_1|A_2|\ldots|A_n) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = v_1A_1 + v_2A_2 + \cdots + v_nA_n$$

Codificació amb codis de Hamming (2)

- Continuem intentant trobar G en funció de H:

$$HG^t = \begin{pmatrix} h_{11} & \dots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{r1} & \dots & h_{rn} \end{pmatrix} \left(\begin{array}{c|c|c} g_{11} & \dots & g_{k1} \\ \vdots & \vdots & \vdots \\ g_{1n} & \dots & g_{kn} \end{array} \right) =$$

$$\left(\begin{pmatrix} h_{11} & \dots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{r1} & \dots & h_{rn} \end{pmatrix} \begin{pmatrix} g_{11} \\ \vdots \\ g_{1n} \end{pmatrix} \middle| \dots \middle| \begin{pmatrix} h_{11} & \dots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{r1} & \dots & h_{rn} \end{pmatrix} \begin{pmatrix} g_{k1} \\ \vdots \\ g_{kn} \end{pmatrix} \right) =$$

$$= \left(g_{11} \begin{pmatrix} h_{11} \\ \vdots \\ h_{r1} \end{pmatrix} + \dots + g_{1n} \begin{pmatrix} h_{1n} \\ \vdots \\ h_{rn} \end{pmatrix} \middle| \dots \middle| g_{k1} \begin{pmatrix} h_{11} \\ \vdots \\ h_{r1} \end{pmatrix} + \dots + g_{kn} \begin{pmatrix} h_{1n} \\ \vdots \\ h_{rn} \end{pmatrix} \right)$$

Codificació amb codis de Hamming (3)

- El problema es redueix al càlcul dels

$$g_{i1}\begin{pmatrix} h_{11} \\ \vdots \\ h_{r1} \end{pmatrix} + g_{i2}\begin{pmatrix} h_{12} \\ \vdots \\ h_{r2} \end{pmatrix} + \cdots + g_{in-1}\begin{pmatrix} h_{1n-1} \\ \vdots \\ h_{rn-1} \end{pmatrix} + g_{in}\begin{pmatrix} h_{1n} \\ \vdots \\ h_{rn} \end{pmatrix}$$

és a dir al càlcul dels

$$g_{i1} \cdot \alpha^{n-1} + g_{i2} \cdot \alpha^{n-2} + \cdots + g_{in-1} \cdot \alpha + g_{in} \cdot 1$$

- Si pensem en les files de G com a polinomis,

$$(g_{i1}, g_{i2}, ..., g_{i,n-1}, g_{i,n}) = g_{i1}x^{n-1} + g_{i2}x^{n-2} + ... + g_{i,n-1}x + g_{i,n}1 = g_i(x)$$

llavors l'anterior producte s'escriu com a $g_i(\alpha)$

Codificació amb codis de Hamming (4)

- Resum: si pensem en les files de G com a polinomis (coeficient principal a l'esquerra)

$$g_i(x) = g_{i1}x^{n-1} + g_{i2}x^{n-2} + \ldots + g_{i,n-1}x + g_{i,n}1$$

llavors la condició $HG^t = 0$ s'escriu com

$$\forall i = 1, \ldots, k \quad g_i(\alpha) = 0$$

- La matriu generadora del codi serà una G amb files independents i que compleixin $g_i(\alpha) = 0$. Una elecció senzilla és:

$$G = \begin{pmatrix} x^{k-1}f(x) \\ \vdots \\ x^2 f(x) \\ xf(x) \\ f(x) \end{pmatrix}$$

($f(D)$ és el polinomi utilitzat per a construir el cos $GF(2^r)$)

Codificació amb codis de Hamming (5)

- Si posem

$$f(D) = D^r + f_{r-1}D^{r-1} + ... + f_2D^2 + f_1D + 1$$

veiem com es codifica el missatge $x = (x_1, ..., x_k)$:

$$(y_1, y_2, ..., y_n) = (x_1, x_2, ..., x_{k-1}, x_k) \begin{pmatrix} x^{k-1}f(x) \\ x^{k-2}f(x) \\ \vdots \\ xf(x) \\ f(x) \end{pmatrix} =$$

$$= x_1x^{k-1}f(x) + x_2x^{k-2}f(x) + \cdots + x_{k-1}xf(x) + x_kf(x) =$$

$$= (x_1x^{k-1} + x_2x^{k-2} + \cdots + x_{k-1}x + x_k)f(x)$$

Codificació amb codis de Hamming (6)

- Si pensem en el missatge com a polinomi, la codificació amb G es redueix a multiplicar el missatge per $f(x)$
- Si hem de pensar missatges i paraules-codi com a polinomis, és més còmode canviar de notació (hi ha massa x's):
- Anomenarem $u(x)$ al missatge a codificar

$$u(x) = u_{k-1}x^{k-1} + ... + u_1x + u_0$$

és a dir el missatge que codificarem és

$$(u_{k-1}, ..., u_0)$$

- Anàlogament, a la paraula-codi resultant l'anomenarem

$$v(x) = v_{n-1}x^{n-1} + ... + v_1x + v_0$$

és a dir la paraula codificada serà

$$(v_{n-1}, ..., v_1, v_0)$$

Codificació amb codis de Hamming (7)

- Codificar un missatge $u(x)$ equival a multiplicar-lo per $f(x)$:

$$v(x) = u(x)f(x)$$

- El codi (conjunt de totes les paraules-codi) està format per

$$C = \{u(x)f(x) : u(x) \text{ de grau} \leq k-1\}$$

- D'aquesta manera no cal explicitar cap matriu. Però aquesta codificació no és sistemàtica

Codificació sistemàtica amb codis de Hamming

- Solucionem la no sistematicitat del codi anterior:
- Si fem la divisió de $x^r u(x)$ entre $f(x)$

$$x^r u(x) = f(x)q(x) + r(x)$$

i passem el residu a l'altre membre:

$$x^r u(x) + r(x) = f(x)q(x)$$

tindrem 2^k polinomis (tots els $x^r u(x) + r(x)$) del codi
- Per tant formen el codi i la codificació

$$v(x) = x^r u(x) + r(x)$$

és sistemàtica (la redundància afegida coincideix amb el residu de la divisió de $x^r u(x)$ entre $f(x)$)

Exemple (1)

- Codifiquem, amb un $H(15, 11)$, el missatge (10010100011)
- Pels codis de Hamming de paràmetre r és $n = 2^r - 1$ i $k = n - r$. Així, $r = 4$
- Necessitem el polinomi $f(x)$ amb el qual ha estat construit el cos $GF(2^r)$. Aquest polinomi és $f(x) = x^4 + x + 1$
- Per codificar, interpretem el missatge com a polinomi:

$$(10010100011) = x^{10} + x^7 + x^5 + x + 1$$

i calculem la redundància com el residu de la divisió del «missatge corregut»

$$x^r u(x) = x^4(x^{10} + x^7 + x^5 + x + 1) = x^{14} + x^{11} + x^9 + x^5 + x^4$$

- entre $f(x) = x^4 + x + 1$. La divisió a la diapositiva següent

Exemple (2)

$$
\begin{array}{llllllll}
x^{14} & x^{11} & & x^{9} & & & x^{5} & x^{4} \\
x^{14} & x^{11} & x^{10} & & & & & \\
\hline
/ & / & x^{10} & x^{9} & & & & \\
 & & x^{10} & & x^{7} & x^{6} & & \\
\hline
 & & / & x^{9} & x^{7} & x^{6} & x^{5} & \\
 & & & x^{9} & & x^{6} & x^{5} & \\
\hline
 & & & / & x^{7} & / & / & x^{4} \\
 & & & & x^{7} & & & x^{4} \quad x^{3} \\
\hline
 & & & & / & & & / \quad x^{3}
\end{array}
$$

$$
\begin{array}{l|lllll}
 & x^{4} & & & x & 1 \\
\hline
x^{10} & x^{6} & x^{5} & x^{3} & &
\end{array}
$$

Exemple (3)

- La redundància és $x^3 = (1000)$ i la paraula-codi resultant:

$$v = (100101000111000)$$

- Podem fer la divisió posant només els coeficients dels polinomis:

```
1 0 0 1 0 1 0 0 0 1 1 0 0 0 0 | 1 0 0 1 1
1 0 0 1 1                     | 1 0 0 0 1 1 0 1 0 0 0
/ 0 0 0 1 1
      1 0 0 1 1
    / 1 0 1 1 1
      1 0 0 1 1
    / 0 1 0 0 1 0
        1 0 0 1 1
      / 0 0 0 1 0 0 0
```

Exemple (4)

- El residu, és a dir la redundància a afegir és (1000)
- La paraula-codi corresponent és $v = (100101000111000)$
- Suposem que a recepció apareix un error a la cinquena component (això no ho sap el receptor) i descodifiquem la paraula rebuda $w = (100111000111000)$:
- La síndrome és la paraula rebuda, pensada com a polinomi i avaluada en α. Reproduim la taula de logaritmes de Zech pel cos $\mathbb{F}_{16}$

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

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

Exemple (5)

per a calcular la síndrome de la paraula rebuda:

$$s = (\alpha^{14}+\alpha^{11})+(\alpha^{10}+\alpha^{9})+(\alpha^{5}+\alpha^{4})+\alpha^{3} = (\alpha^{10}+\alpha^{13})+(\alpha^{8}+\alpha^{3}) = \alpha^{9}+\alpha^{13} = \alpha^{10}$$

- Com que $s = \alpha^{10} = \alpha^{-5} \neq 0$ sabem que s'han produit errors i que si només s'ha produit un error (és a dir, si no s'ha excedit la capacitat del codi) llavors aquest està a la posició 5 (posició d'usuari, començant per l'esquerra)

Codis correctors de 2 errors (1)

- Els codis de Hamming tenen capacitat de corregir un error
- Els codis que generalitzen els de Hamming, en el sentit que corregeixen t errors, són els codis BCH (Bose-Chaudhuri-Hocquenghem)
- El codi de Hamming de longitud $n = 2^m - 1$ necessita m bits de paritat per a corregir un error. Sembla, per tant, que amb $2m$ bits de paritat podrem corregir dos errors
- Intentem construir la matriu de comprovació H pel codi corrector de dos errors afegint una fila d'elements de $GF(2^m)$ a la matriu de comprovació del codi de Hamming:

$$H = \begin{pmatrix} h(\alpha^{n-1}) & h(\alpha^{n-2}) & \cdots & h(\alpha^2) & h(\alpha) & h(1) \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix}$$

Codis correctors de 2 errors (2)

- Només falta elegir, de manera adequada, la funció h
- Per això, suposem que a la paraula rebuda, w, hi ha dos errors, a les posicions x_1 i x_2, $1 \leq x_1 < x_2 \leq n$.

$$\begin{aligned} w &= v + e \\ (w_{n-1}, w_{n-2}, ..., w_1, w_0) &= (v_{n-1}, v_{n-2}, ..., v_1, v_0) + (..., 0, \overset{x_1}{1}, ..., 0, \overset{x_2}{1}, ..) \end{aligned}$$

- Com que la síndrome de w i la síndrome de e són el mateix:
  $s = Hw^t = H(v+e)^t = H(v^t + e^t) = Hv^t + He^t = 0 + He^t = He^t$
  podem escriure l'equació $He^t = s$ (diapositiva següent):

Codis correctors de 2 errors (3)

$$\begin{pmatrix} h(\alpha^{n-1}) & h(\alpha^{n-2}) & \cdots & h(\alpha^2) & h(\alpha) & h(1) \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix} \begin{pmatrix} \vdots \\ 0 \\ 1 \\ \vdots \\ 0 \\ 1 \\ \vdots \end{pmatrix} \begin{matrix} \\ \\ \leftarrow x_1 \\ \\ \\ \leftarrow x_2 \\ \\ \end{matrix} = \begin{pmatrix} s_1' \\ s_0' \end{pmatrix}$$

$$\begin{pmatrix} h(\alpha^{n-x_1}) + h(\alpha^{n-x_2}) \\ \alpha^{n-x_1} + \alpha^{n-x_2} \end{pmatrix} = \begin{pmatrix} s_1' \\ s_0' \end{pmatrix}$$

Codis correctors de 2 errors (4)

- Ens queda un sistema de 2 equacions amb dues incògnites

$$\begin{cases} h(\alpha^{n-x_1}) + h(\alpha^{n-x_2}) = s_1' \\ \alpha^{n-x_1} + \alpha^{n-x_2} = s_0' \end{cases} \qquad \begin{cases} h(z) + h(t) = s_1' \\ z + t = s_0' \end{cases}$$

  sistema en el cos $GF(2^m)$ (anomenem $z := \alpha^{n-x_1}$, $t := \alpha^{n-x_2}$)
- Cal elegir h de manera que el descodificador pugui resoldre aquest sistema
- Una elecció dolenta de h és: $h(x) = cx \quad \forall x \in GF(2^m)$, ($c$ constant). En aquest cas el sistema anterior prendria la forma

$$\begin{cases} c(z+t) = s_1' \\ z + t = s_0' \end{cases}$$

  És clar que aquest sistema, en general, no tindrà solucions

Codis correctors de 2 errors (5)

- Una altra elecció, també dolenta, per a la funció h és: $h(x) = x^2 \quad \forall x \in GF(2^m)$
- Amb aquesta elecció, l'anterior sistema quedaria com

$$\begin{cases} z^2 + t^2 = s_1' \\ z + t = s_0' \end{cases}$$

- Observem que $z^2 + t^2 = (z + t)^2$, és a dir, el membre esquerra de l'equació de dalt és el quadrat del membre esquerra de l'equació de baix. Aquest sistema, per tant, tampoc tindrà, en general, solució

Codis correctors de 2 errors (6)

- Provem amb
$$h(x) = x^3 \quad \forall x \in GF(2^m)$$
- En aquest cas, el sistema a resoldre serà:
$$\begin{cases} z^3 + t^3 = s_1^{'} \\ z + t = s_0^{'} \end{cases}$$
- Aquests sistemes sí que es poden resoldre
- Per tant, l'elecció $h(x) = x^3$ és una bona elecció

Codis correctors de 2 errors (7)

- Despejem, del sistema anterior, zt:

$$z^3 + t^3 = (z+t)(z^2 + zt + t^2)$$
$$s_1^{'} = s_0^{'}(z^2 + zt + t^2)$$

Observem que si $s_0^{'} = 0$ llavors $s_1^{'} = 0$ i, per tant, $z = t$, cosa que, si s'han comès dos errors, no és. En cas contrari ($s_0^{'} \neq 0$),

$$\frac{s_1^{'}}{s_0^{'}} = (z+t)^2 + zt = (s_0^{'})^2 + zt \Rightarrow zt = \frac{s_1^{'}}{s_0^{'}} + (s_0^{'})^2$$

- De z i t coneixem la seva suma i el seu producte:

$$z + t = s_0^{'}$$
$$zt = \frac{s_1^{'}}{s_0^{'}} + (s_0^{'})^2$$

Codis correctors de 2 errors (8)

- Recordem que $z := \alpha^{n-x_1}$ i $t := \alpha^{n-x_2}$, és a dir

$$z^{-1} = \alpha^{x_1} \qquad t^{-1} = \alpha^{x_2}$$

on x_1 i x_2 són les posicions dels errors. Per altra part, z^{-1} i t^{-1} són els zeros del polinomi

$$L(x) = (1 + zx)(1 + tx) = 1 + (z + t)x + ztx^2 = 1 + s_0' x + \left(\frac{s_1'}{s_0'} + (s_0')^2 \right) x^2$$

- Aquest és el *polinomi localitzador d'errors* ja que els seus zeros ens donen les posicions dels errors: si els zeros estan a les posicions α^{x_1} i α^{x_2} els errors estan a les posicions x_1 i x_2
- En $GF(2^m)$ no és d'aplicació la fórmula habitual per a calcular els zeros d'un polinomi de segon grau. Però $GF(2^m)$ és un cos finit: podem anar provant un a un amb tots els elements del cos!

Codis correctors de 2 errors (9)

- Calculem les síndromes de la paraula rebuda (canviem una mica els noms):

$$\begin{pmatrix} s_3 \\ s_1 \end{pmatrix} = \begin{pmatrix} (\alpha^{n-1})^3 & (\alpha^{n-2})^3 & \cdots & (\alpha^2)^3 & \alpha^3 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix} \begin{pmatrix} w_{n-1} \\ w_{n-2} \\ \vdots \\ w_2 \\ w_1 \\ w_0 \end{pmatrix}$$

- El motiu d'aquest canvi de nom és que si pensem en la paraula rebuda com un polinomi:

$$w = (w_{n-1}, w_{n-2}, ..., w_1, w_0) = w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_1 x + w_0 = w(x)$$

llavors

$$\begin{aligned} s_1 &= w(\alpha) \\ s_3 &= w(\alpha^3) \end{aligned}$$

Codis correctors de 2 errors (10)

- Per descodificar la paraula rebuda $w(x)$ calculem les síndromes:

$$\begin{aligned} s_1 &= w(\alpha) \\ s_3 &= w(\alpha^3) \end{aligned}$$

- Si $s_1 = 0$ (i per tant $s_3 = 0$) llavors $w(x)$ ja és una paraula-codi; en cas contrari es calcula el polinomi localitzador d'errors:

$$\begin{aligned} L(x) &= 1 + L_1 x + L_2 x^2 \\ L_1 &= s_1 \\ L_2 &= \frac{s_3}{s_1} + s_1^2 \end{aligned}$$

- Resolem $L(x) = 0$ (provant). Si els zeros són α^{x_1} i α^{x_2}, els errors estan a les posicions x_1 i x_2
- Si $L(x)$ no té zeros és que hem sobrepassat la capacitat correctora del codi (s'han comès més de dos errors)
- Si $L(x)$ només té un zero, α^{x_1}, només s'ha comès un error

Exemple (1)

- Suposem un codi BCH de longitud $15 = 2^4 - 1$, corrector de 2 errors i descodifiquem la paraula

$$(100101110000010) = x^{14} + x^{11} + x^9 + x^8 + x^7 + x = w(x)$$

- Càlcul de les síndromes:

$$\begin{aligned} s_1 &= w(\alpha) = \alpha^{14} + \alpha^{11} + \alpha^9 + \alpha^8 + \alpha^7 + \alpha \\ s_3 &= w(\alpha^3) = \alpha^{42} + \alpha^{33} + \alpha^{27} + \alpha^{24} + \alpha^{21} + \alpha^3 = \alpha^{12} + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 \end{aligned}$$

- Per fer aquests càlculs necessitem la taula de logaritmes de Zech de $GF(2^4)$. Reproduim-la:

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

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

Exemple (2)

- Ara, els càlculs:

$$\begin{aligned} s_1 &= w(\alpha) = (\alpha^{14} + \alpha^{11}) + (\alpha^9 + \alpha^8) + (\alpha^7 + \alpha) = (\alpha^{10} + \alpha^{12}) + \alpha^{14} = \alpha^3 + \alpha^{14} = 1 \\ s_3 &= w(\alpha^3) = (\alpha^{12} + \alpha^3) + (\alpha^{12} + \alpha^9) + (\alpha^6 + \alpha^3) = (\alpha^{10} + \alpha^8) + \alpha^2 = \alpha + \alpha^2 = \alpha^5 \end{aligned}$$

- Càlcul del polinomi localitzador d'errors: $L(x) = 1 + L_1 x + L_2 x^2$

$$\begin{aligned} L_1 &= s_1 = 1 \\ L_2 &= \frac{s_3}{s_1} + s_1^2 = \alpha^5 + 1 = \alpha^{10} \end{aligned}$$

- Per tant: $L(x) := 1 + x + \alpha^{10} x^2$

Exemple (3)

- Zeros del polinomi localitzador d'errors $L(x) = 1 + x + \alpha^{10}x^2$. Provem, un a un, amb tots els elements del cos $GF(16)$:

i	$L(\alpha^i)$
0	$1 + 1 + \alpha^{10} \neq 0$
1	$1 + \alpha + \alpha^{10}\alpha^2 = \alpha^4 + \alpha^{12} \neq 0$
2	$1 + \alpha^2 + \alpha^{10}\alpha^4 = \alpha^8 + \alpha^{14} \neq 0$
3	$1 + \alpha^3 + \alpha^{10}\alpha^6 = \alpha^{14} + \alpha \neq 0$
4	$1 + \alpha^4 + \alpha^{10}\alpha^8 = \alpha + \alpha^3 \neq 0$
5	$1 + \alpha^5 + \alpha^{10}\alpha^{10} = \alpha^{10} + \alpha^5 \neq 0$
6	$1 + \alpha^6 + \alpha^{10}\alpha^{12} = \alpha^{13} + \alpha^7 \neq 0$
7	$1 + \alpha^7 + \alpha^{10}\alpha^{14} = \alpha^9 + \alpha^9 = 0$

i	$L(\alpha^i)$
8	$1 + \alpha^8 + \alpha^{10}\alpha = \alpha^2 + \alpha^{11} \neq 0$
9	$1 + \alpha^9 + \alpha^{10}\alpha^3 = \alpha^7 + \alpha^{13} \neq 0$
10	$1 + \alpha^{10} + \alpha^{10}\alpha^5 = \alpha^5 + \alpha \neq 0$
11	$1 + \alpha^{11} + \alpha^{10}\alpha^7 = \alpha^{12} + \alpha^2 \neq 0$
12	$1 + \alpha^{12} + \alpha^{10}\alpha^9 = \alpha^{11} + \alpha^4 \neq 0$
13	$1 + \alpha^{13} + \alpha^{10}\alpha^{11} = \alpha^6 + \alpha^6 = 0$
14	$1 + \alpha^{14} + \alpha^{10}\alpha^{13} = \alpha^3 + \alpha^8 \neq 0$

  Els zeros de $L(x)$ són: α^7 i α^{13}
- Si hi ha dos errors, aquests estan a les posicions 7 i 13. Paraula descodificada:

$$v = (100101110000010) + (000000100000100) = (100101010000110)$$

- Observació: el càlcul de $L(\alpha^{14})$ era innecessari

Idea dels codis BCH correctors de 3 errors (1)

- Si volguéssim un codi, de longitud n, amb capacitat de corregir 3 errors agafariem una matriu de comprovació del tipus:

$$H = \begin{pmatrix} (\alpha^{n-1})^5 & (\alpha^{n-2})^5 & \cdots & (\alpha^2)^5 & \alpha^5 & 1 \\ (\alpha^{n-1})^3 & (\alpha^{n-2})^3 & \cdots & (\alpha^2)^3 & \alpha^3 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix}$$

- Si la paraula rebuda, $w(x)$, té errors a les posicions x_1, x_2, x_3 $0 \leq x_1 < x_2 < x_3 \leq n$ (observem que les posicions dels errors es corresponen amb les columnes de $\alpha^{n-x_1}, \alpha^{n-x_2}, \alpha^{n-x_3}$) i les síndromes de w, que recordem que coincideixen amb les síndromes de l'error, són

$$\begin{pmatrix} s_5 \\ s_3 \\ s_1 \end{pmatrix} = \begin{pmatrix} (\alpha^{n-1})^5 & (\alpha^{n-2})^5 & \cdots & (\alpha^2)^5 & \alpha^5 & 1 \\ (\alpha^{n-1})^3 & (\alpha^{n-2})^3 & \cdots & (\alpha^2)^3 & \alpha^3 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix} \begin{pmatrix} w_{n-1} \\ w_{n-2} \\ \\ \vdots \\ w_2 \\ w_1 \\ w_0 \end{pmatrix}$$

Idea dels codis BCH correctors de 3 errors (2)

- Per trobar els errors buscariem el polinomi localitzador d'errors per a aquest problema,

$$L(x) := 1 + L_1 x + L_2 x^2 + L_3 x^3$$

  i les seves arrels, $\alpha^{x_1}, \alpha^{x_2}$ i α^{x_3} ens indicarien les posicions dels errors
- Els coeficients del polinomi localitzador d'errors es troben, mitjançant algun algorisme, a partir de les síndromes s_1, s_3, s_5

Idea dels codis BCH correctors de 3 errors (3)

- Si, per exemple, $n = 2^4 - 1 = 15$, cada α^i representa una columna de 4 bits
- La matriu de comprovació H és una matriu binària de 12 files i 15 columnes. Amb l'ajut de la taula del cos $GF(16)$,

bits	c. del polinomi	α^i
0000	0	α^∞
0001	1	$\alpha^{15} = 1$
0010	D	α
0011	$D+1$	α^4
0100	D^2	α^2
0101	D^2+1	α^8
0110	D^2+D	α^5
0111	D^2+D+1	α^{10}

bits	c: del polinomi	α^i
1000	D^3	α^3
1001	D^3+1	α^{14}
1010	D^3+D	α^9
1011	D^3+D+1	α^7
1100	D^3+D^2	α^6
1101	D^3+D^2+1	α^{13}
1110	D^3+D^2+D	α^{11}
1111	D^3+D^2+D+1	α^{12}

(recordem que el mòdul és $f(D) = D^4 + D + 1$)

Idea dels codis BCH correctors de 3 errors (4)

(continuació) escrivim la matriu H en forma binària:

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

Idea dels codis BCH correctors de 3 errors (5)

- Les files de H representen equacions. Són independents? Mirant la matriu veurem que la primera fila és de zeros i que la segona i la tercera fila coincideixen. I, de manera immediata, no es veu res més. De fet, es pot demostrar que les files 3 a 12 són independents. La nostra matriu H es compón, per tant, de 10 equacions efectives, és a dir, la redundància del nostre codi és $r = 10$ (i no $r = 12$). Com que $n = 15$, $k = n - r = 5$. Es tracta d'un codi $(15, 5)$. Amb aquest exemple es pot veure que, per corregir t errors (en el cas $t := 3$) en un codi de longitud $n = 2^m - 1$, la redundància, en general, només estarà fitada per mt:

$$r \leq mt$$

Codis BCH (1)

- Els codis BCH correctors de t errors tindràn una distància mínima de la qual només podrem afirmar que no és inferior a $\delta = 2t + 1$
- δ és la distància mínima *de disseny*

Codis BCH (2)

- Codi BCH de paràmetre m corrector de t errors

Codi de longitud $n = 2^m - 1$, $r \leq mt$ i matriu de comprovació

$$H = \begin{pmatrix} (\alpha^{n-1})^{2t-1} & (\alpha^{n-2})^{2t-1} & \cdots & (\alpha^2)^{2t-1} & \alpha^{2t-1} & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ (\alpha^{n-1})^3 & (\alpha^{n-2})^3 & \cdots & (\alpha^2)^3 & \alpha^3 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix}$$

$\alpha = \overline{D}$ és un element primitiu del cos $GF(2^m)$

- Es pot demostrar que la distància mínima d'aquests codis és igual o més gran que $\delta := 2t + 1$.

Introducció als codis de Reed-Solomon

- Les operacions pròpies de la descodificació dels BCH (càlcul de síndromes i del polinomi localitzador d'errors, càlcul de les arrels) es fan totes en el cos $GF(2^m)$
- Per què no considerar un codi anàleg al BCH però on les lletres de l'alfabet siguin elements de $GF(2^m)$?
- Si fem això obtindrem els codis de Reed-Solomon (RS)
- Els codis RS de paràmetre m són codis de longitud $n = 2^m - 1$ sobre l'alfabet $GF(2^m)$ i constitueixen els exemples més importants de codis BCH no binaris
- Hem vist (BCH binaris de paràmetre m, correctors de t errors) que la redundància només està fitada per mt (en general no coincideix amb mt)
- Per codis lineals generals la redundància compleix una desigualtat en l'altra sentit (diapositiva següent)

Fita de Singleton

Theorem

(Fita de Singleton). En qualsevol codi lineal (n, k) corrector de t errors, la redundància, $r = n - k$, satisfà:

$$r \geq 2t$$

Proof.

Si el codi és capaç de corregir t errors, llavors la seva distància mínima ha de complir $d_{\min} \geq 2t + 1$. Veiem que $r \geq d_{\min} - 1$. Per això suposem el missatge format per un u i $k - 1$ zeros:

$$u = (10 \ldots 0)$$

La paraula-codi corresponent (codificació sistemàtica) tindrà un pes no nul i no superior a $r + 1$. Per tant, $d_{\min} \leq r + 1$, és a dir, $r \geq d_{\min} - 1 \geq 2t$

Codis RS (1)

- La fita de Singleton mostra la mínima quantitat de redundància per corregir t errors. Els codis RS assoleixen aquesta fita
- Codi RS de paràmetre m corrector de t errors

Alfabet: $GF(2^m)$, longitud del codi: $n = 2^m - 1$, redundància: $r = 2t$, longitud dels missatges: $k = n - r$. Matriu de comprovació:

$$H = \begin{pmatrix} (\alpha^{n-1})^{2t} & (\alpha^{n-2})^{2t} & \cdots & (\alpha^2)^{2t} & \alpha^{2t} & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ (\alpha^{n-1})^2 & (\alpha^{n-2})^2 & \cdots & (\alpha^2)^2 & \alpha^2 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix}$$

$\alpha = \overline{D}$ és un element primitiu del cos $GF(2^m)$

Codis RS (2)

- Recordem la notació que estem usant:
  - els polinomis en D (les classes de polinomis en D) són els elements del cos $GF(2^m)$
  - tots els demés polinomis són polinomis en x (la paraula w a descodificar, per exemple)
- Comparant les matrius de control dels codis RS i BCH (codis, en ambdós casos, de paràmetre m i dissenyats per a corregir t errors), veiem una diferència: a la matriu de comprovació del BCH falten, en relació a la matriu de comprovació del RS, les files parells. Analitzem aquestes síndromes que "falten"

Codis RS (3)

- Si

$$w = (w_{n-1}, w_{n-2}, ..., w_1, w_0) = w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_1 x + w_0 = w(x)$$

com que els w_i són 0 ó 1, llavors $w_i^2 = w_i$ i

$$s_2 = w(\alpha^2) = w_{n-1}^2(\alpha^{n-1})^2 + w_{n-2}^2(\alpha^{n-2})^2 + \cdots + w_1^2(\alpha)^2 + w_0^2 =$$
$$= (w_{n-1}\alpha^{n-1} + w_{n-2}\alpha^{n-2} + \cdots + w_1\alpha + w_0)^2 = w^2(\alpha)$$

és a dir

$$s_2 = s_1^2$$

- De la mateixa manera,

$$s_4 = w(\alpha^4) = w^2(\alpha^2) = w^4(\alpha) = s_1^4$$
$$s_6 = w(\alpha^6) = w^2(\alpha^3) = s_3^2$$
$$\cdots\cdots\cdots$$

- Les equacions que falten en la matriu de comprovació del codi BCH (respecte del codi RS) són *redundants*

Descodificació RS (1)

- Continuem amb l'estudi dels codis de RS ja que els desenvolupaments seran aprofitables pels BCH
- La descodificació d'un RS serà una mica més complicada que la descodificació d'un BCH: en els BCH n'hi ha prou localitzant els errors; en els RS, primer s'hauran de localitzar i després avaluar la seva magnitud
- Per descodificar els RS primer es calculen les síndromes de la paraula rebuda w:

$$\begin{pmatrix} s_{2t} \\ \vdots \\ s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} (\alpha^{n-1})^{2t} & (\alpha^{n-2})^{2t} & \cdots & (\alpha^2)^{2t} & \alpha^{2t} & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ (\alpha^{n-1})^2 & (\alpha^{n-2})^2 & \cdots & (\alpha^2)^2 & \alpha^2 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix} \begin{pmatrix} w_{n-1} \\ w_{n-2} \\ \vdots \\ w_2 \\ w_1 \\ w_0 \end{pmatrix}$$

Descodificació RS (2)

- Si el vector de síndromes no és el vector nul (en aquest cas la paraula rebuda ja és paraula-codi), es calcula el polinomi localitzador d'errors. Aquest és un polinomi de grau ν (nombre d'errors comesos, $\nu \leq t$) amb terme independent igual a 1 i que admet com a zeros α^{n_1}, α^{n_2},..., α^{n_ν}. si els errors estan a les posicions $n_1, n_2, \ldots, n_\nu$. És a dir

$$L(x) = \prod_{i=1}^{\nu} \left(1 + \alpha^{n-n_i} x\right) = 1 + L_1 x + \ldots + L_{\nu-1} x^{\nu-1} + L_\nu x^\nu$$

- Es resol l'equació $L(x) = 0$ i si asquesta admet com a solucions $\alpha^{n_1}, \alpha^{n_2}, \ldots, \alpha^{n_\nu}$ és que els errors estan a les posicions $n_1, n_2, ..., n_\nu$
- Finalment caldrà avaluar les magnituds dels errors $e_1, e_2, ..., e_\nu$

Descodificació RS (3)

- Per a descodificar un RS necessitarem el polinomi localitzador d'errors $L(x)$, polinomi que es calcula a partir de les síndromes (de la paraula rebuda):

$$\begin{pmatrix} s_{2t} \\ s_{2t-1} \\ \vdots \\ s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} w(\alpha^{2t}) \\ w(\alpha^{2t-1}) \\ \vdots \\ w(\alpha^2) \\ w(\alpha) \end{pmatrix}$$

- Si pensem en les síndromes com en un polinomi:

$$s(x) = (s_{2t}, s_{2t-1}, ..., s_2, s_1) = s_{2t}x^{2t-1} + s_{2t-1}x^{2t-2} + \cdots + s_2x + s_1$$

Descodificació RS (4)

- Es pot demostrar (no ho farem) que la relació que hi ha entre el polinomi de síndromes $s(x)$ i el polinomi localitzador d'errors $L(x)$ ve donada per l'equació fonamental

Theorem

Equació fonamental (the key-equation)

$$\varepsilon_{\nu-1}(x) \equiv L_{\nu}(x) s_{2t-1}(x) \pmod{x^{2t}}$$

(els subíndexs indiquen els graus dels polinomis corresponents; $\nu \leq t$ és el nombre d'errors comesos)

- $\varepsilon_{\nu-1}(x)$ és l'anomenat polinomi avaluador d'errors; l'usarem

Descodificació RS (5)

- L'equació fonamental *caracteritza* el polinomi localitzador d'errors (i el polinomi avaluador d'errors) en el sentit que si $\hat{\varepsilon}_{\nu-1}(x)$ i $\hat{L}_\nu(x)$ $(\nu \leq t)$ són polinomis arbitraris de graus respectius $\nu-1$ «menor que t» i ν que satisfan l'equació fonamental

$$\hat{\varepsilon}_{\nu-1}(x) \equiv \hat{L}_\nu(x) s_{2t-1}(x) \quad (\mathrm{mod} x^{2t})$$

llavors

$$L(x) = k\hat{L}_\nu(x) \quad \text{i} \quad \varepsilon(x) = k\,\hat{\varepsilon}(x)$$

- I com que només volem els zeros de $L(x)$ ens podem quedar amb $\hat{L}(x)$
- Veiem com trobar un $\hat{L}(x)$ que satisfaci l'equació fonamental

Descodificació RS (6)

- La congruència

$$\hat{\varepsilon}_{\nu-1}(x) \equiv \hat{L}_{\nu}(x) \cdot s_{2t-1}(x) \pmod{x^{2t}}$$

equival a les igualtats

$$\begin{aligned} \hat{\varepsilon}_{\nu-1}(x) + \hat{L}_{\nu}(x) \cdot s_{2t-1}(x) &= c(x)x^{2t} \\ \hat{L}_{\nu}(x) \cdot s_{2t-1}(x) + c(x)x^{2t} &= \hat{\varepsilon}_{\nu-1}(x) \end{aligned}$$

$\hat{L}(x)$ i $\hat{\omega}(x)$ es poden trobar amb l'algorisme d'Euclides estès!

- Repassem l'algorisme d'Euclides

Algorisme d'Euclides per a nombres (1)

- Ja coneixem l'algorisme d'Euclides per a nombres:
- si $a > b > 0$ llavors el $mcd(a, b) := d$ es pot obtenir aplicant iteradament el Teorema d'Euclides que diu que si fem la divisió entera de a entre b, és a dir si

$$a = bq + r, \qquad 0 \leq r < b$$

llavors $mcd(a, b) = mcd(b, r)$.Tornant a dividir b entre r:

$$b = rq_1 + r_1 \qquad 0 \leq r_1 < r$$

tindrem $mcd(a, b) = mcd(b, r) = mcd(r, r_1)$. Si continuem:

$$r = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1$$

es complirà

$$mcd(a, b) = mcd(b, r) = mcd(r, r_1) = mcd(r_1, r_2)$$

Algorisme d'Euclides per a nombres (2)

I així successivament. D'aquesta manera s'obtenen residus

$$r > r_1 > r_2 > \ldots$$

Per tant, hi ha un primer residu nul:

$$r_n > 0, \quad r_{n+1} = 0$$

i, pel teorema d'Euclides,

$$mcd(a, b) = mcd(b, r) = mcd(r, r_1) = \cdots = mcd(r_{n-1}, r_n) = mcd(r_n, 0) = r_n$$

És a dir, $mcd(a, b)$ és l'últim residu no nul

Algorisme d'Euclides per a nombres (3)

- Ja sabeu (FM) que tots aquests càlculs es poden presentar en una taula (algorisme d'Euclides)
- Per evitar posar massa lletres fem un exemple: $mcd(4999, 1109)$:

Q		4	1	1	32	8	2	
R	4999	1109	563	546	17	2	1	0

$$mcd(4999, 1109) = 1$$

Identitat de Bézout per a nombres

- Ja sabeu que si $mcd(a, b) = d$ llavors existeixen enters x, y (no únics) tals que $d = xa + yb$. I aquesta és la identitat de Bézout per a aquests nombres
- Una manera d'obtenir uns coeficients per a la identitat de Bézout és a partir de l'algorisme d'Euclides estès:
  - Primer es fa l'algorisme d'Euclides
  - i després s'estén amb dues files, una que s'etiqueta com a X i l'altra que s'etiqueta com a Y
- Continuem amb l'exemple d'abans (diapositiva següent)

Algorisme d'Euclides estès per a nombres (1)

- Exemple anterior:

X	**1**	**0**	1	-1	2	-65	522	
Y	**0**	**1**	-4	5	-9	293	-2353	
Q		4	1	1	32	8	2	
R	4999	1109	563	546	17	2	1	0

$$4999 \cdot 522 + 1109 \cdot (-2353) = 1$$

Algorisme d'Euclides estès per a nombres (2)

- Per a la identitat de Bézout només s'usen els dos «pesos» finals, els que hi han damunt del mcd
- Però tots els pesos són útils: el de la fila X és el pes del nombre més gran dels dos dels que busquem el seu mcd (el primer, vaja) i el coeficient de la fila Y és el pes del nombre més petit (el segon): ponderats els dos nombres amb els pesos indicats s'obté el residu de sota
- Per exemple:

$$2 * 4999 + (-9) * 1109 = 17$$

Algorisme d'Euclides estès per a polinomis (1)

- El concepte de *mcd* també es pot definir per a polinomis
- Es diu que $d(x)$ és el $mcd(a(x), b(x))$ si
  - $d(x)|a(x)$
  - $d(x)|b(x)$
  - $\forall d'(x)\,(d'(x)|a(x) \wedge d'(x)|b(x) \implies d'(x)|d(x))$
- Es pot demostrar que el *mcd* de dos polinomis $a(x)$ i $b(x) \neq 0$ sempre existeix i és únic en el sentit que si n'hi ha dos, un és múltiple escalar de l'altre. Per això se sol agafar com a *mcd* un polinomi amb el coeficient del terme de grau màxim igual a 1 (polinomi mònic)
- Si $b(x) \equiv b$ és una constant no nul·la llavors $mcd(a(x), b) = 1$

Algorisme d'Euclides estès per a polinomis (2)

- Si $a(x)$ i $b(x)$ són polinomis a coeficients en un cos K tals que
  - $grau(a(x)) \geq grau(b(x))$
  - $b(x) \neq 0$

  el $mcd(a(x), b(x))$ es pot obtenir igual que en el cas numèric
- Exemple a $\mathbb{R}[x]$: $mcd(x^3 + x^2, x + 1)$

Q	$x^2 - 2x + 2$		
R	$x^3 - x^2$	$x + 1$	-2

  $mcd(x^3 - x^2, x + 1) = 1$
- El «mateix» exemple $\mathbb{F}_2[x]$:

Q	x^2		
R	$x^3 + x^2$	$x + 1$	0

  $mcd(x^3 - x^2, x + 1) = x + 1$

Coeficients per a la identitat de Bézout (polinomis)

- $\mathbb{R}[x]$:

X	1	0	1
Y	0	1	$-x^2+2x-2$
Q		x^2-2x+2	
R	x^3-x^2	$x+1$	-2

$$1\cdot(x^3-x^2)+(-x^2+2x-2)\cdot(x+1)=-2$$

$$-\frac{1}{2}\cdot(x^3-x^2)-\left(\frac{1}{2}\cdot(-x^2+2x-2)\right)\cdot(x+1)=1$$

- $\mathbb{F}_2[x]$:

X	1	0
Y	0	1
Q		x^2
R	x^3+x^2	$x+1$

$$0\cdot(x^3-x^2)+1\cdot(x+1)=x+1$$

Codificació sistemàtica dels codis RS (1)

- Recordem que $w(x)$ és paraula-codi sii $w(\alpha) = w(\alpha^2) = w(\alpha^3) = \ldots = w(\alpha^{2t}) = 0$, és a dir, si $w(x)$ és múltiple dels polinomis $(x+\alpha)$, $(x+\alpha^2)$,$(x+\alpha^3)$,$\ldots$, $(x+\alpha^{2t})$
- Com que en els codis RS és $2t = r < n$, els anteriors polinomis són primers entre sí dos a dos
- $w(x)$ és paraula-codi sii $w(x)$ és múltiple del polinomi $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)\cdots(x+\alpha^{2t})$
- Al polinomi $g(x)$ se l'anomena «polinomi generador del codi»
- I se l'anomena d'aquesta manera perquè el codi (el conjunt de totes les paraules-codi) és

$$C = \{u(x)g(x) : u(x) \text{ de grau } \leq k-1\}$$

Codificació sistemàtica dels codis RS (2)

- La codificació $u(x) \mapsto u(x)g(x)$ no és sistemàtica
- Per trobar un codificador sistemàtic procedirem igual que amb els Hamming: dividim el polinomi $x^r u(x)$ entre $g(x)$:

$$x^r u(x) = g(x)q(x) + res(x)$$

($q(x)$ és el quocient i $res(x)$ el residu de la divisió)

- Per tant,

$$g(x)q(x) = x^r u(x) + res(x)$$

cosa que mostra que les $x^r u(x) + res(x)$ són paraules-codi. Agafem-les per a codificar $u(x)$:

$$u(x) \to x^r u(x) + res(x)$$

Exemple de RS, codificació i localització dels errors (1)

- Cos $\mathbb{F}_{16}$ construit amb el polinomi primitiu $D^4 + D + 1$:

0000	0		1000	D^3	α^3
0001	1	α^{15}	1001	$D^3 + 1$	α^{14}
0010	D	α	1010	$D^3 + D$	α^9
0011	$D + 1$	α^4	1011	$D^3 + D + 1$	α^7
0100	D^2	α^2	1100	$D^3 + D^2$	α^6
0101	$D^2 + 1$	α^8	1101	$D^3 + D^2 + 1$	α^{13}
0110	$D^2 + D$	α^5	1110	$D^3 + D^2 + D$	α^{11}
0111	$D^2 + D + 1$	α^{10}	1111	$D^3 + D^2 + D + 1$	α^{12}

Exemple de RS, codificació i localització dels errors (2)

- Taula de logaritmes de Zech:

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

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

Exemple de RS, codificació i localització dels errors (3)

- Suposem sobre el cos anterior un RS capaç de corregir tres errors, és a dir, un RS de longitud 15 i redundància 6 (per tant els missatges tindran longitud 9)
- Codifiquem (sistemàticament) el missatge
$$(\alpha^3 1000 \alpha^7 00 \alpha)$$
- Pensat com a polinomi el missatge és: $u(x) := \alpha^3 x^8 + x^7 + \alpha^7 x^3 + \alpha$
- La paraula-codi corresponent és $x^6 \cdot u(x) + res$ on res és el residu de la divisió de $x^6 \cdot u(x)$ entre $g(x)$,
$$g(x) := (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$$
- Fent els càlculs,
$$g(x) := x^6 + \alpha^{10} x^5 + \alpha^{14} x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6$$
$$res := \alpha^{12} x^5 + \alpha x^4 + \alpha^{11} x^3 + \alpha^{12} x^2 + \alpha^{14} x + \alpha^4$$

Exemple de RS, codificació i localització dels errors (4)

- $(\alpha^3 1000 \alpha^7 00 \alpha)$ es codificarà com $(\alpha^3 1000 \alpha^7 00 \alpha \alpha^{12} \alpha \alpha^{11} \alpha^{12} \alpha^{14} \alpha^4)$
- Afegim dos errors i descodifiquem $(\alpha^3 \alpha 000 \alpha^7 00 \alpha \alpha^{12} \alpha \alpha^{11} 1 \alpha^{14} \alpha^4)$
- La paraula rebuda és

$$w := \alpha^3 x^{14} + \alpha x^{13} + \alpha^7 x^9 + \alpha x^6 + \alpha^{12} x^5 + \alpha x^4 + \alpha^{11} x^3 + x^2 + \alpha^{14} x + \alpha^4$$

- Calculem les síndromes:

$$\begin{pmatrix} s_6 \\ s_5 \\ s_4 \\ s_3 \\ s_2 \\ s_1 \end{pmatrix} := \begin{pmatrix} w(\alpha^6) \\ w(\alpha^5) \\ w(\alpha^4) \\ w(\alpha^3) \\ w(\alpha^2) \\ w(\alpha) \end{pmatrix} = \begin{pmatrix} \alpha^{11} \\ \alpha^5 \\ \alpha^{13} \\ \alpha^{14} \\ 0 \\ \alpha^{14} \end{pmatrix}$$

Exemple de RS, codificació i localització dels errors (5)

- Alternativament, es poden calcular les síndromes sense usar polinomis. Però és més llarg:

$$\begin{pmatrix} s_6 \\ s_5 \\ s_4 \\ s_3 \\ s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} \alpha^9 & \alpha^3 & \alpha^{12} & \alpha^6 & 1 & \alpha^9 & \alpha^3 & \alpha^{12} & \alpha^6 & 1 & \alpha^9 & \alpha^3 & \alpha^{12} & \alpha^6 & 1 \\ \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & \alpha^5 & 1 & \alpha^{10} & \alpha^5 & 1 \\ \alpha^{11} & \alpha^7 & \alpha^3 & \alpha^{14} & \alpha^{10} & \alpha^6 & \alpha^2 & \alpha^{13} & \alpha^9 & \alpha^5 & \alpha & \alpha^{12} & \alpha^8 & \alpha^4 & 1 \\ \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 \\ \alpha^{13} & \alpha^{11} & \alpha^9 & \alpha^7 & \alpha^5 & \alpha^3 & \alpha & \alpha^{14} & \alpha^{12} & \alpha^{10} & \alpha^8 & \alpha^6 & \alpha^4 & \alpha^2 & 1 \\ \alpha^{14} & \alpha^{13} & \alpha^{12} & \alpha^{11} & \alpha^{10} & \alpha^9 & \alpha^8 & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix} \begin{pmatrix} \alpha^3 \\ \alpha \\ 0 \\ 0 \\ 0 \\ \alpha^7 \\ 0 \\ 0 \\ \alpha \\ \alpha^{12} \\ \alpha \\ \alpha^{11} \\ 1 \\ \alpha^{14} \\ \alpha^4 \end{pmatrix} = \begin{pmatrix} \alpha^{11} \\ \alpha^5 \\ \alpha^{13} \\ \alpha^{14} \\ 0 \\ \alpha^{14} \end{pmatrix}$$

Exemple de RS, codificació i localització dels errors (6)

- Busquem el polinomi $\hat{L}(x)$. Per això aplicarem l'algorisme d'Euclides a x^6 i $s(x) := \alpha^{11}x^5 + \alpha^5x^4 + \alpha^{13}x^3 + \alpha^{14}x^2 + \alpha^{14}$ fins arribar a un residu de grau estrictament inferior a 3:

Y	0	1	$\alpha^4x + \alpha^{13}$	$\alpha^9x^2 + \alpha^8x + \alpha^9$
Q		$\alpha^4x + \alpha^{13}$	$\alpha^5x + \alpha^9$	
R	x^6	$\alpha^{11}x^5 + \alpha^5x^4 + \alpha^{13}x^3 + \alpha^{14}x^2 + \alpha^{14}$	$\alpha^6x^4 + \alpha^5x^3 + \alpha^{12}x^2 + \alpha^3x + \alpha^{12}$	$\alpha^7x + \alpha^8$

$$\hat{L}(x) := \alpha^9x^2 + \alpha^8x + \alpha^9$$

$$\hat{L}(x) = 0 \implies x = \alpha^2, \alpha^{13} \text{ (provant)}$$

- Per tant els errors estan a les posicions $n_1 := 2$ i $n_2 := 13$

Avaluació dels errors, primer mètode (1)

- Per avaluar la magnitud dels errors fixem notació:
  - ν és el nombre d'errors ($\nu \leq t$)
  - $e_1, \ldots, e_\nu$ són les magnituds dels errors comesos a les posicions respectives $n_1, \ldots, n_\nu$ ($n_1 < \ldots < n_\nu$)
- Com que les síndromes de la paraula rebuda coincideixen amb les síndromes dels errors, si

$$e = (\ldots \overset{n_1)}{0} \ldots e_1 \ldots 0 \ldots \overset{n_\nu)}{e_\nu} \ldots 0 \ldots)$$

llavors

$$s(w) = s(e) := H \cdot e^t = \begin{pmatrix} (\alpha^{n-1})^{2t} & (\alpha^{n-2})^{2t} & \cdots & (\alpha^2)^{2t} & \alpha^{2t} & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ (\alpha^{n-1})^2 & (\alpha^{n-2})^2 & \cdots & (\alpha^2)^2 & \alpha^2 & 1 \\ \alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha & 1 \end{pmatrix} \begin{pmatrix} \vdots \\ 0 \\ e_1 \\ \vdots \\ 0 \\ e_\nu \\ \vdots \end{pmatrix} \begin{matrix} \\ \\ \leftarrow n_1 \\ \\ \\ \leftarrow n_\nu \\ \\ \end{matrix}$$

Avaluació dels errors, primer mètode (2)

- Com que l'anterior producte matriu per vector és

$$\begin{pmatrix} \left(\alpha^{n-n_1}\right)^{2t} & \cdots & \left(\alpha^{n-n_\nu}\right)^{2t} \\ \cdots & \cdots & \cdots \\ \left(\alpha^{n-n_1}\right)^{1} & \cdots & \left(\alpha^{n-n_\nu}\right)^{1} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_\nu \end{pmatrix}$$

- ens queda el sistema

$$\begin{pmatrix} \left(\alpha^{n-n_1}\right)^{2t} & \cdots & \left(\alpha^{n-n_\nu}\right)^{2t} \\ \cdots & \cdots & \cdots \\ \left(\alpha^{n-n_1}\right)^{1} & \cdots & \left(\alpha^{n-n_\nu}\right)^{1} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_\nu \end{pmatrix} = \begin{pmatrix} s_{2t} \\ \vdots \\ s_1 \end{pmatrix}$$

Avaluació dels errors, primer mètode (3)

- Es pot demostrar que

$$\begin{vmatrix} \left(\alpha^{n-n_1}\right)^{\nu} & \cdots & \left(\alpha^{n-n_\nu}\right)^{\nu} \\ \cdots & \cdots & \cdots \\ \left(\alpha^{n-n_1}\right)^{1} & \cdots & \left(\alpha^{n-n_\nu}\right)^{1} \end{vmatrix} \neq 0$$

- Per tant, per trobar els errors ens podem limitar a resoldre el sistema format per les últimes ν equacions:

$$\begin{pmatrix} \left(\alpha^{n-n_1}\right)^{\nu} & \cdots & \left(\alpha^{n-n_\nu}\right)^{\nu} \\ \cdots & \cdots & \cdots \\ \left(\alpha^{n-n_1}\right)^{1} & \cdots & \left(\alpha^{n-n_\nu}\right)^{1} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_\nu \end{pmatrix} = \begin{pmatrix} s_\nu \\ \vdots \\ s_1 \end{pmatrix}$$

Continuació amb l'exemple de RS (1)

- En el nostre exemple hem trobat $\nu = 2$, $n_1 = 2$ i $n_2 = 13$; només falta avaluar la magnitud dels errors. Per a això cal resoldre el sistema

$$\begin{pmatrix} \left(\alpha^{n-n_1}\right)^{\nu} & \cdots & \left(\alpha^{n-n_\nu}\right)^{\nu} \\ \cdots & \cdots & \cdots \\ \left(\alpha^{n-n_1}\right)^{1} & \cdots & \left(\alpha^{n-n_\nu}\right)^{1} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_\nu \end{pmatrix} = \begin{pmatrix} s_\nu \\ \vdots \\ s_1 \end{pmatrix}$$

  sistema que, en el nostre cas, és:

$$\begin{pmatrix} \alpha^{11} & \alpha^{4} \\ \alpha^{13} & \alpha^{2} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} s_2 \\ s_1 \end{pmatrix}$$

- Com que $s_1 = w(\alpha) = \alpha^{14}$ i $s_2 = w(\alpha^2) = 0$, el sistema que ens donarà els error és el de la diapositiva següent

Continuació amb l'exemple de RS (2)

$$\begin{pmatrix} \alpha^{11} & \alpha^4 \\ \alpha^{13} & \alpha^2 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha^{14} \end{pmatrix}$$

sistema que té per solució $e_1 = \alpha^4$, $e_2 = \alpha^{11}$

- Per tant,

$$e = (0, \alpha^4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha^{11}, 0, 0)$$

$$\hat{w} = (\alpha^3, \alpha, 0, 0, 0, \alpha^7, 0, 0, \alpha, \alpha^{12}, \alpha, \alpha^{11}, 1, \alpha^{14}, \alpha^4) + (0, \alpha^4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha^{11}, 0, 0)$$

$$\hat{w} = (\alpha^3, 1, 0, 0, 0, \alpha^7, 0, 0, \alpha, \alpha^{12}, \alpha, \alpha^{11}, \alpha^{12}, \alpha^{14}, \alpha^4)$$

Avaluació dels errors (RS), segon mètode (1)

- Hem trobat el nombre ν i les posicions $n_1 < n_2 < \ldots n_\nu$ dels errors (a partir del polinomi localitzador d'errors $L(x)$)
- Per avaluar la seva magnitud usarem el polinomi avaluador d'errors $\varepsilon(x)$. Aquest polinomi es defineix com

$$\varepsilon(x) := \sum_{j=1}^{\nu} \alpha^{-n_j} e_j \ell_j(x) \quad \text{on} \quad \ell_j(x) := \prod_{\substack{i=1 \\ i \neq j}}^{\nu} \left(1 + \alpha^{-n_i} x\right)$$

- Observem que $\ell_j(\alpha^{n_i}) = 0$ si $i \neq j$. Per tant,

$$\varepsilon(\alpha^{n_i}) = \alpha^{-n_i} e_i \ell_i(\alpha^{n_k})$$

Avaluació dels errors (RS), segon mètode (2)

- Recordem que

$$L(x) := \prod_{i=1}^{\nu} (1 + \alpha^{-n_i} x)$$

Per tant,

$$L'(x) = \sum_{j=1}^{\nu} \alpha^{-n_j} \prod_{\substack{i=1 \\ i \neq j}}^{\nu} (1 + \alpha^{-n_i} x) = \sum_{j=1}^{\nu} \alpha^{-n_j} \cdot \ell_j(x)$$

En particular,

$$L'(\alpha^{n_i}) = \sum_{j=1}^{\nu} \alpha^{-n_j} \cdot \ell_j(\alpha^{n_i}) = \alpha^{-n_i} \cdot \ell_i(\alpha^{n_i})$$

Avaluació dels errors (RS), segon mètode (3)

Com que

$$\varepsilon\left(\alpha^{n_i}\right) = \sum_{j=1}^{\nu} \alpha^{-n_j} e_j \ell_j\left(\alpha^{n_i}\right) = \alpha^{-n_i} e_i \ell_i\left(\alpha^{n_i}\right)$$

tenim que

$$e_i = \frac{\varepsilon\left(\alpha^{n_i}\right)}{L'\left(\alpha^{n_i}\right)} \qquad i = 1, \ldots, \nu$$

Avaluació dels errors (RS), segon mètode (4)

- Com que els polinomis que es troben amb l'algorisme d'Euclides són

$$\hat{L}(x) = c \cdot L(x) \quad \text{i} \quad \hat{\varepsilon}(x) = c \cdot \varepsilon(x)$$

  - els zeros de $\hat{L}(x)$ ens indiquen les posicions dels errors (si els zeros són $\alpha^{n_1}, \ldots, , \alpha^{n_\nu}$ els errors estan a les posicions $n_1, \ldots, n_\nu$)
  - les magnituds dels errors $e_1, \ldots, e_\nu$ venen donades per

$$e_i = \frac{\hat{\varepsilon}\left(\alpha^{n_i}\right)}{\hat{L}'\left(\alpha^{n_i}\right)} \quad i = 1, \ldots, , \nu$$

- Podem comprovar (exercici) que aquest segon mètode de descodificació dóna el mateix que el primer amb l'exemple anterior

Aquest ha estat un curs per a no-matemàtics

He fet el curs d'aquesta manera perquè aquest curs no va destinat a matemàtics:

- hem començat amb 0's i 1's, hem introduït els cossos finits i hem acabat amb polinomis a coeficients en un cos finit
- si aquest curs hagués anat destinat a matemàtics hauríem començat amb codis polinòmics
  - si pensem en les paraules-codi com a polinomis, un codi és un conjunt de polinomis de grau inferior a n
  - un codi s'anomena polinòmic si aquest codi consisteix en tots els múltiples (polinòmics) de grau inferior a n d'un cert polinomi $g(x)$ –polinomi generador del codi–
- també hauria parlat de codis cíclis
- Tornem als BCH (binaris) amb aquest enfocament «polinòmic»

Pol mínim d'un element $\gamma \in K$ $(K := \mathbb{F}_2[x]/f(D))$ (1)

- Considerem un cos finit $\mathbb{F}_{2^m}$ de 2^m elements, és a dir: $\mathbb{F}_{2^m} \approx \mathbb{F}_2[x]/(f(D))$ on $f(D)$ és un polinomi irreductibe (nosaltres l'agafem primitiu) de grau m
- Si $\gamma \in K$, $\gamma \neq 0, 1$ es defineix el polinomi mínim de γ com el polinomi de grau mínim (a coeficients binaris) que anula γ:

$$m_\gamma(\gamma) = 0$$

$m_\gamma(x) \in \mathbb{F}_2[x]$ de grau mínim entre tots els que compleixen l'anterior condició

- És clar que si un polinomi $w(x) \in \mathbb{F}_2[x]$ compleix $w(\gamma) = 0$, també complirà $w(\gamma^2) = w(\gamma^4) = w(\gamma^8) = \ldots = 0$
- Com que el conjunt $\{\gamma, \gamma^2, \gamma^4, \gamma^8, \ldots\}$ és finit, hi haurà un primer exponent 2^s tal que $\gamma^{2^s} \in \left\{\gamma, \gamma^{2^1}, \gamma^{2^2}, \ldots., \gamma^{2^{s-1}}\right\}$
- Per a aquest exponent es compleix que $\gamma^{2^s} = \gamma$. Demostració:

Pol mínim d'un element $\gamma \in K$ $(K := \mathbb{F}_2[x]/f(D))$ (2)

Lema

Si x, y són elements d'un cos finit tals que $x^2 = y^2$ llavors $x = y$.

Demostració.

$x^2 = y^2 \implies (x+y)(x+y) = (x+y)^2 = x^2 + y^2 = 0 \implies$
$x + y = 0 \implies x = y$ □

- $s \neq 1$: $s = 1 \implies \gamma^2 = \gamma \implies \gamma \in \{0, 1\}$. Per tant $s > 1$
- I si $\gamma^{2^s} \neq \gamma$ llavors $\gamma^{2^s} = \gamma^{2^i}$ per un cert $i > 0$
- I si $\gamma^{2^s} = \gamma^{2^i}$ llavors $\left(\gamma^{2^{s-1}}\right)^2 = \left(\gamma^{2^{i-1}}\right)^2$. I pel lema, $\gamma^{2^{s-1}} = \gamma^{2^{i-1}}$, és a dir que 2^s no seria el primer exponent tal que $\gamma^{2^s} \in \left\{\gamma, \gamma^{2^1}, \ldots., \gamma^{2^{s-1}}\right\}$
- $m_\gamma(x) := (x+\gamma)\left(x+\gamma^2\right)\left(x+\gamma^4\right)\cdots\left(x+\gamma^{2^{s-1}}\right)$

Pol mínim d'un element $\gamma \in K$ $(K := \mathbb{F}_2[x]/f(D))$ (3)

- Veiem que els coeficients de $m_\gamma(x)$ són binaris:

$$m_\gamma(x) = (x+\gamma)\left(x+\gamma^2\right)\left(x+\gamma^4\right)\cdots\left(x+\gamma^{2^{s-1}}\right)$$
$$\Downarrow$$
$$m_\gamma^2(x) = (x+\gamma)^2\left(x+\gamma^2\right)^2\left(x+\gamma^4\right)^2\cdots\left(x+\gamma^{2^{s-1}}\right)^2$$
$$\Downarrow$$
$$m_\gamma^2(x) = \left(x^2+\gamma^2\right)\left(x^2+\gamma^4\right)\left(x^2+\gamma^8\right)\cdots\left(x^2+\gamma^{2^s}\right)$$
$$\Downarrow$$
$$m_\gamma^2(x) = \left(x^2+\gamma\right)\left(x^2+\gamma^2\right)\left(x^2+\gamma^4\right)\cdots\left(x^2+\gamma^{2^{s-1}}\right)$$

és a dir $m_\gamma^2(x) = m_\gamma(x^2)$

Pol mínim d'un element $\gamma \in K$ $(K := \mathbb{F}_2[x]/f(D))$ (4)

- Si escrivim

$$m_\gamma(x) = m_s x^s + m_{s-1} x^{s-1} + \ldots + m_1 x + m_0$$

llavors

$$m_s^2 x^{2s} + m_{s-1}^2 x^{2(s-1)} + \ldots + m_1^2 x^2 + m_0^2 =$$
$$= m_s x^{2s} + m_{s-1} x^{2(s-1)} + \ldots + m_1 x^2 + m_0$$
$$\Downarrow$$
$$\forall i = 0, \ldots, s,\ m_i^2 = m_i$$
$$\Downarrow$$
$$\forall i = 0, \ldots, s,\ m_i \in \{0, 1\}$$

- Els polinomis mínim són irreductibles

Més sobre polinomis mínims

- Hi ha elements diferents que tenen el mateix polinomi mínim
- Per exemple: en $\mathbb{F}_8$ construit amb el polinomi $f(D) := D^3 + D + 1$, el polinomi mínim de α^5 i α^6 és el mateix:

$$m_{\alpha^5}(x) := \left(x + \alpha^5\right)\left(x + \alpha^{10}\right)\left(x + \alpha^{20}\right) =$$
$$= \left(x + \alpha^5\right)\left(x + \alpha^3\right)\left(x + \alpha^6\right) = x^3 + x^2 + 1$$

$$m_{\alpha^6}(x) := \left(x + \alpha^6\right)\left(x + \alpha^{12}\right)\left(x + \alpha^{24}\right) =$$
$$= \left(x + \alpha^6\right)\left(x + \alpha^5\right)\left(x + \alpha^3\right) = x^3 + x^2 + 1$$

- Però si els elements $\gamma_1, \gamma_2, \ldots, \gamma_\ell$ tenen polinomis mínims diferents dos a dos, llavors

$$mcm(m_{\gamma_1}(x), m_{\gamma_2}(x), \ldots, m_{\gamma_\ell}(x)) = m_{\gamma_1}(x) \cdot m_{\gamma_2}(x) \cdot \ldots \cdot m_{\gamma_\ell}(x)$$

Polinomi generador d'un BCH i codi generat (1)

- Es pot demostrar que el polinomi generador d'un BCH de paràmetre m corretor de t errors és

$$g(x) := mcm(m_\alpha(x), m_{\alpha^3}(x), \ldots, m_{\alpha^{2t-1}}(x)) = m_\alpha(x) \cdot m_{\alpha^3}(x) \cdot \ldots \cdot m_{\alpha^{2t-1}}(x))$$

- Posem un exemple per no seguir amb tantes lletres: BCH de paràmetre $m := 4$ i corrector de 3 errors:

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

$$g(x) = mcm\left(m_\alpha(x), m_{\alpha^3}(x), m_{\alpha^5}(x)\right) = m_\alpha(x) \cdot m_{\alpha^3}(x) \cdot m_{\alpha^5}(x)$$
$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

Polinomi generador d'un BCH i codi generat (2)

- Llista de totes les paraules-codi:

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	1	0	1	1	1	0	0	0	0
0	0	0	0	1	0	1	0	0	1	1	0	1	1	1	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0
0	0	0	1	0	1	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0
0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	1	0	1	1	0	0	1	0	0	0	1	1	1	1	0
0	0	1	0	1	0	0	1	1	0	1	1	1	0	0	1	0	1	0	1	1	0	0	1	0	0	0	1	1	1
0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	1	1	0	1	1	1	0	0	0	1	0	1	0	0	0
0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	1	1	1	0	0	0	0	1	0	1	1	0	0	1	0
0	0	1	1	0	1	1	1	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	0	0	1	1	0	1	1	1	0	0	0	0	1	0
0	1	0	1	1	0	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1	0	1	0	0	1	1	0	1	1
0	1	0	0	0	1	1	1	1	0	1	0	1	1	0	1	0	1	1	1	0	0	0	0	1	0	1	0	0	1
0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	1	1	0	0	0	1	1	1	1	0	1	0	1	1	0
0	1	1	1	0	0	0	0	1	0	1	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1
0	1	1	0	1	1	1	0	0	0	0	1	0	1	0	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1
0	1	0	0	1	1	0	1	1	1	0	0	0	0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	1	1	0	0	0	0	0	1	0	1	0	0	1	1	0	1