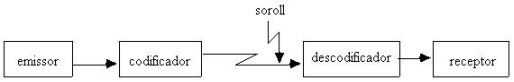
Biblioteca per a la simulació de la codificació i la descodificació amb codis BCH i RS

Juan Gabriel Gomila Salas
Llicenciatura en Matemàtiques

I. Introducció

Considerem el diagrama de transmissió d'informació representat per la figura:



A causa del soroll que subsisteix sempre en qualsevol canal de transmissió, és gairebé inevitable que el receptor obtingui el missatge enviat havent sofert algunes alteracions dels seus símbols (en el cas binari, canvis de 0 per 1 i viceversa). L'única possibilitat de detectar aquests errors és enviar la informació juntament amb dígits suplementaris, anomenats de control, mitjançant una certa regla (codi) coneguda tant per l'emisor com pel receptor.

Una manera de garantitzar la fiabilitat en la transmisió d'informació per canals, com per exemple, una imatge que ens arribi des d'un satèlit geoestacionari, una cançó en format mp3 és amb els codis codificadors i correctors d'errors. En particular, s'empren dos tipus de codis, coneguts amb el nom de BCH i RS, el fonament dels quals es basa en la teoria de cossos finits. Per aprofundir més dins aquest camp cal esmentar el llibre [1], en el qual ens hem basat per desenvolupar aquests exemples.

En aquest article es presenta la implementació d'una biblioteca en *Mathematica 6.0* [2] per fer una simulació completa per poder veure i treballar, en detall, la codificació i correcció d'errors amb aquests dos tipus de codis . Si algú està interessat en provar, per si mateix, exemples amb dita biblioteca, només cal que us poseu amb contacte amb algun de nosaltres, qui us podrà dir com accedir-hi de manera gratuïta. A més, pensant en la facilitat que haurien de tenir els usuaris per poder emprar una biblioteca implementada per una altra persona, s'hi ha incorporat una ajuda interactiva, on fer preguntes sobre com explotar-la al 100 %

II. Construcció d'un cos finit, o de Galois

- $(F[x]/(f(x)), +_{\bmod f(x)}, \cdot_{\bmod f(x)})$ és un *cos* si i només si $f(x)$ és un polinomi irreductible sobre $F[x]$, essent F un cos.

- Si $F = F_p = (Z_p, +_{\bmod p}, \cdot_{\bmod p})$ i $f(x)$ és un polinomi irreductible de grau n sobre F_p, aleshores

$$(F[x]/(f(x)), +_{\bmod f(x)}, \cdot_{\bmod f(x)})$$

és un cos amb p^n elements.

Els elements del cos són els diferents residus mòdul $f(x)$ i per tant es poden representar com polinomis de grau menor o igual a n amb coeficients dins F_p.

És a dir: $\forall a(x) \in F_p[x]/(f(x)),\quad a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0;\ a_i \in F_p$.

Pels codis que construirem posteriorment, utilitzarem el cos de Galois sobre F_2 amb el polinomi irreductible $f(x) = x^4 + x^3 + 1$. Aleshores podem considerar l'isomorfisme $GF(2^4) \approx F_2[x]/(f(x))$ agafant una arrel α de $f(x)$; és a dir $f(\alpha) = 0 \Longrightarrow \alpha^4 = \alpha^3 + 1$ i $\alpha^1 5 = 1$:

$$\begin{pmatrix} GF(2^4) & F_2[x]/(1+x^3+x^4) \\ -\infty & 0 \\ 0 & 1 \\ \alpha & x \\ \alpha^2 & x^2 \\ \alpha^3 & x^3 \\ \alpha^4 & x^3+1 \\ \alpha^5 & x^3+x+1 \\ \alpha^6 & x^3+x^2+x+1 \\ \alpha^7 & x^2+x+1 \\ \alpha^8 & x^3+x^2+x \\ \alpha^9 & x^2+1 \\ \alpha^{10} & x^3+x \\ \alpha^{11} & x^3+x^2+1 \\ \alpha^{12} & x+1 \\ \alpha^{13} & x^2+x \\ \alpha^{14} & x^3+x^2 \end{pmatrix} \tag{1}$$

III. Codis binaris, lineais i cíclics: BCH

Un codi binari, lineal i cíclic $C(n,k)$ pot ser considerat com l'ideal principal de $Z_2[x]/x^n - 1$ generat per un polinomi mònic $g(x)$, divisor de $x^n - 1$. Si el grau de $g(x)$ és r, aleshores es satisfà la relació $k = n - r$, essent k la dimensió de C, com a subespai vectorial de F_2^n.

Codificar una informació $a = (a_0, a_1, .., a_{k-1}), a_i \in Z_2$, esdevé en trobar la paraula-codi $v = (v_0, v_1, ..., v_{n-1})$, de manera que els polinomis associats respectius compleixen: $v(x) = a(x) \cdot g(x)$.

Els codis BCH van ser introduïts per Hocquenghem (1959) i Bose, Chaudhuri (1960), com a generalització dels codis de Hamming, però amb capacitat correctora $t \geq 1$. Aquest tipus de codis venen definits per dos paràmetres m i t, que verifiquen el següent teorema:

Teorema
Per a tot sencer n de la forma $n = 2^m - 1$, $m \geq 3$, i per a tot

sencer t tal que $n - t \cdot m > 0$, existeix un codi binari, lineal i cíclic t-corrector, de llargària n, dimensió $k \geq n - t \cdot m$ i distància mínima $d \geq 2t+1$, que té per polinomi generador:

$$g(x) = \text{m.c.m. } (m_1(x), m_3(x), ..., m_{2t-1}(x))$$

essent $m_i(x)$ el polinomi mínim de α^i i α un element primitiu de $GF(2^m)$.

Construcció del codi BCH de paràmetres $m = 4$, $t = 3$

En la figura 1 veim com s'ha resolt amb els algoritmes de la nostra biblioteca.
El codi BCH sobre $GF(2^4)$ que construirem tindrà una longitud 15, una dimensió 5, capacitat correctora 3 i distància mínima entre les paraules-codi 7. Els passos seguits són:

1. Construcció del cos $GF(2^4)$ (matriu (II)).
2. Cerca d'un element $\alpha \in GF(2^4)$ primitiu i agafar com a longitud del codi $n = 2^4 - 1 = 15$.
3. Calcular el polinomi generador:

$$\begin{aligned} g(x) &= \text{m.c.m. } (m_1(x), m_3(x), m_5(x)) \\ &= 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10} \end{aligned}$$

Suposem doncs, que volem trasmetre el vector d'informació $\underline{a} = (1, 0, 1, 0, 0)$, que té per polinomi associat $a(x) = 1 + x^2$. La informació codificada és, aleshores,

$$v(x) = g(x) \cdot a(x) = 1 + x^4 + x^5 + x^6 + x^7 + x^9 + x^{11} + x^{12}$$

Suposem ara que trasmitim la paraula codi $\underline{v}$ per un cert canal, on s'ens introdueix un error a les coordenades $1, 3$ i 5

$$\underline{v} = (10001111010110)$$

$$\underline{u} = \underline{v} + \underline{e} = (11011011010110)$$

(és a dir, el vector d'error és $e(x) = x + x^3 + x^5$). En aquest cas, el polinomi associat al vector $\underline{u}$ que es rebrà a la sortida del canal serà

$$u(x) = v(x) + e(x) = 1 + x + x^3 + x^4 + x^6 + x^7 + x^9 + x^{11} + x^{12}$$

IV. Codis binaris, lineals i cíclics: RS

Els codis RS van ser introduïts per Reed i Solomon (MIT, 1960), i tenen la propietat que pels paràmetres, n i k , tenen la capacitat correctora més gran possible: $d - 1 = n - k$ (codis de màxima distància separable).

Un *codi binari, lineal i cíclic de Reed-Solomon* (RS) és un codi sobre $GF(2^4)$, de llargària $n = 2^4 - 1$ i dimensió k, tal que la seva distància mínima és $d = n - k + 1$, i té per polinomi generador:

$$g(x) = (x - \alpha)(x - \alpha^1)...(x - \alpha^{d-1})$$

on α és un element primitiu de $GF(2^4)$.

Construcció del codi RS amb $m = 4$, $t = 3$

En la figura 2 veim com s'ha resolt amb els algoritmes de la nostra biblioteca. El codi RS que construirem tendrà una longitud 15, una dimensió 9, capacitat correctora 3 i distància mínima entre les paraules 7.

1. Construcció del cos $GF(2^4)$ (figura II).

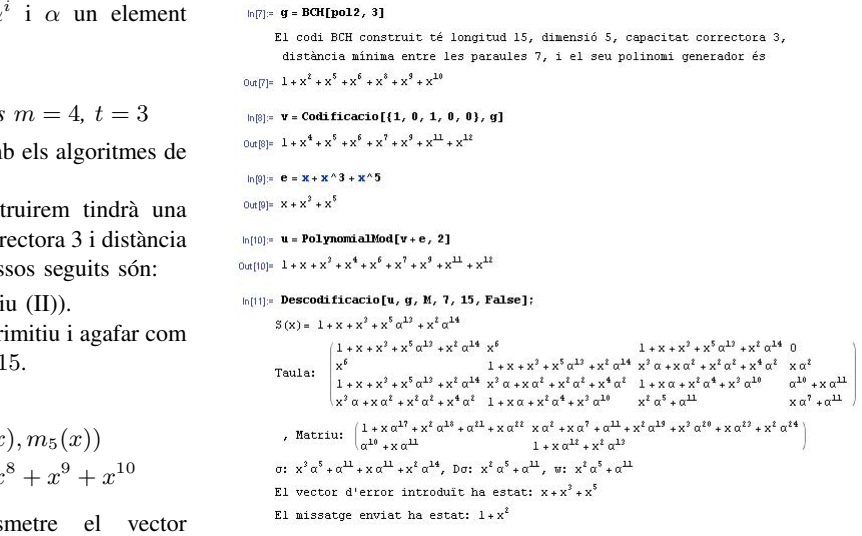


Figura 1. Exemple de la simulació d'un codi BCH.

2. Cercar un element $\alpha \in GF(2^4)$ primitiu i agafar com a longitud del codi $n = 2^4 - 1 = 15$.
3. Calcular el polinomi generador:

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^1)...(x - \alpha^6) \\ &= \alpha^6 + \alpha^{11}x + \alpha^7 x^2 + \alpha^2 x^3 + x^4 + \alpha^{12} x^5 + x^6 \end{aligned}$$

Per a la codificació, suposem que volem trasmetre el vector d'informació $a = (\alpha^5, \alpha^1 1, 0, 0, 0, \alpha^3, 0)$, que té per polinomi associat $a(x) = \alpha^3 x^5 + \alpha^{11} x + 1$.

Aquí consideram la *codificació sistemàtica*:

$$v(x) = a(x) \cdot x^r - p(x), \text{ on } p(x) = a(x) \cdot x^r \bmod g(x);$$
$$\text{i } r = grau\ g(x) = d - 1$$

és a dir, que en el nostre cas, resulta:

$$\begin{aligned} v(x) = \quad & \alpha^5 + x\alpha + x^2\alpha^{11} + x^4\alpha^{14} + x^3\alpha^6 + \\ & + x^5\alpha^6 + x^6\alpha^5 + x^7\alpha^{11} + x^{11}\alpha^3 \end{aligned}$$

Suposem que introduïm un error α la coordenada 1, α^4 en la coordenada 2 i α^6 en la coordenada 5.

Com abans, el polinomi d'error serà $e(x) = x\alpha + x^2\alpha^4 + x^5\alpha^6$, i per tant pel canal es rebrà el vector $\underline{u}$ que té per polinomi:

$$\begin{aligned} & u(x) = v(x) + e(x) = \\ & \alpha^5 + x^2\alpha^2 + x^3\alpha^6 + x^4\alpha^{14} + x^6\alpha^5 + x^7\alpha^{11} + x^{11}\alpha^3 \end{aligned}$$

V. Descodificació: Algoritme de Berlekamp-Massey

L'algoritme de descodificació que descriurem aquí és de l'any 1969, i és útil tant pels codis BCH com pels RS.

Sigui $u(x) = u_0 + u_1 x + ... + u_{n-1} x^{n-1}$ el polinomi associat al vector rebut a la sortida del canal de comunicació,

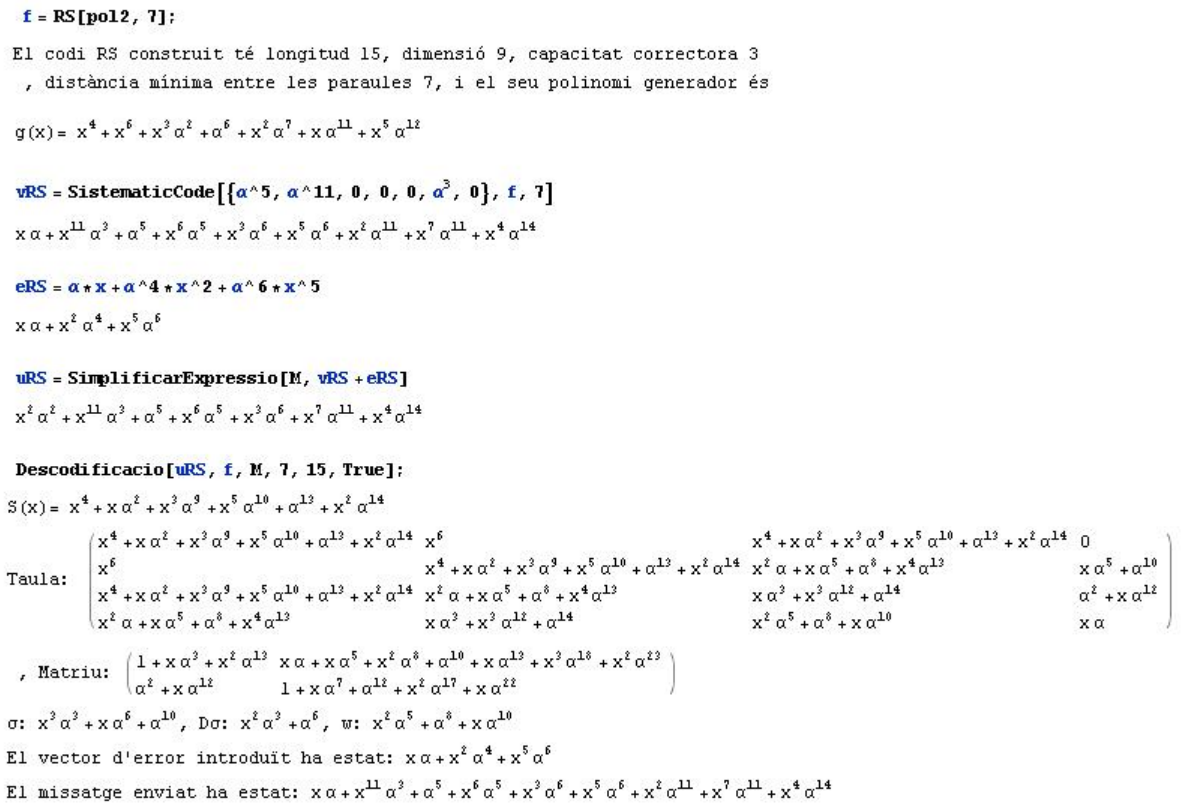


Figura 2. Exemple de simulació d'un codi RS.

on s'ha utilitzat un codi BCH o RS, construït sobre un cos finit $GF(2^m)$, on α és l'element primitiu ($a^{2^{m-1}} = 1$). Les passes a seguir, que poden veure's en les figures 1 i 2 són:

- Calcular el seu polinomi síndrome $S(x) = \sum_{i=0}^{d-2} u(\alpha^i) \cdot x^i$. El seu grau és sempre $\leq d-1$. Els polinomis síndrome obtinguits respectivament en cada exemple anterior són:

$$S_{BCH}(x) = 1 + x + x^2\alpha^{14} + x^3 + x^5\alpha^{13}$$

$$S_{RS}(x) = \alpha^{13} + x\alpha^2 + x^2\alpha^{14} + x^3\alpha^9 + x^4 + x^5\alpha^{10}$$

- Es realitzen una sèrie de divisions successives, donades per l'algoritme d'Euclides extès, que pot consultar-se en [1] i que ens dóna una matriu de la forma:

$$\begin{pmatrix} P_k & Q_k \\ P_{k-1} & Q_{k-1} \end{pmatrix} = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Calculam, pel teorema de Dirichlet:
  i) El polinomi localitzador d'errors, que és: $\sigma(x) = Q_k$. En els nostres exemples resulten, respectivament:

$$\sigma_{BCH} : \alpha^{11} + x\alpha^{11} + x^2\alpha^{14} + x^3\alpha^5$$

$$\sigma_{RS} : \alpha^{10} + x\alpha^6 + x^3\alpha^3$$

  ii) El polinomi avaluador d'errors, que és: $w(x) = (-1)^k r_k(x)$. En els nostres casos:

$$w_{BCH}(x) = x^2\alpha^5 + \alpha^{11}$$

$$w_{RS} = x^2\alpha^5 + \alpha^8 + x\alpha^{10}$$

- Calcular els zeros de $\sigma(x)$. Si els errors estan localitzats a les coordenades $E = \{k_1, k_2, ..., k_c\}$, aleshores els zeros del polinomi localitzador $\sigma(x)$ són $\frac{1}{\alpha^i}$ on $i \in E$. Així, obtindríem les coordenades on tenim un cert error (1, 3 i 5 en el primer cas i 1, 2 i 5 en el segón)

- Calcular els valors dels errors per: $w(\alpha^j)/\sigma'(\alpha^j) = -e_i$ on $\alpha^j = \frac{1}{\alpha^i}$ pels $i \in E$ i $\sigma'(\alpha^j)$ indica la derivada del polinomi localitzador $\sigma(x)$ avaluada a α^j. Així, tendríem finalment quin vector d'error se'ns havía introduït. Simplement sabent el tipus de codificació usada, es pot fer el procediment invers, i descodificar, obtenint la informació que inicialment havíem enviat.

REFERENCIAS

[1] J. Rifa L. Huguet. *Comunicación digital: Teoria de la Información. Codificación algebraica. Criptografia.* Masson, Barcelona, Septiembre 1991.

[2] Mathematica 6.0 i posteriors. www.wolfram.com.