Coduri Reed-Solomon

Codurile Reed-Solomon (RS) reprezintă o subclasă specială de coduri BCH *q*-are care au simboluri în câmpul Galois GF(q). În cazul codurilor *q*-are , biții sunt înlocuiți cu caractere.

Un cod *q*-ar corector de *t* erori şi cu simboluri în GF(q) este un cod BCH *q*-ar cu următorii parametri:

- lungimea blocului $n = q - 1$;
- numărul digiților de informație k;
- numărul digiților de control $m = n - k = 2t$;
- distanța minimă $d_{\min} = 2t + 1$.

În definirea codului RS se folosesc drept simboluri *n* elemente x_i care reprezintă *n* puteri diferite ale unui singur element *z* de ordinul *n*.

Fie $z^n = 1,\ z^i \neq 1$, pentru $0 < i < n,\ z \in GF(q)$. Un cod RS de lungime *n* şi distanță minimă *d* este definit , în sensul restrâns , ca mulțimea vectorilor $v = [a_0, a_1, \ldots, a_{n-1}],\ a_i = V\left(x = z^i\right)$, unde *V(x)* este un polinom peste GF(q) de $grad \leq n - d$.

Transformarea Fourier discretă în câmpul Galois (GF-DFT)

Codurile bloc corectoare de erori pot fi reprezentate cu ajutorul unei transformări asemănătoare transformării Fourier discrete DFT (Discret Fourier Transform), definite de această data în câmpul Galois GF(Q). Domeniul frecvență oferă, mai ales la decodare, unele avantaje de calcul sau de implementare , cum ar fi utilizarea unor algoritmi rapizi de calcul ai transformatei Fourier, utilizarea procesoarelor digitale de semnal şi altele. Dacă interesează procesul de codare, furnizor al cuvintelor de cod , informația primară este conținută în *reprezentarea frecvențială.*

Fie vectorul *v* corespunzător unui cuvânt în domeniul timp

$$v = [a_0, a_1, \ldots, a_{n-1}],$$

constituit din coeficienții polinomului,

$$v(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},\ a_i \in GF(q)\ .$$

Fie, de asemenea, vectorul *V* în domeniul frecvență

$$V = [A_0, A_1, \ldots, A_{N-1}],$$

constituit din coeficienții polinomului

$$V(x) = A_0 + A_1 x + \cdots + A_{n-1} x^{n-1},\ A_i \in GF(q).$$

Fie *z* un element de ordinul *n* al lui GF(q), adică

$$z^n = 1, \quad z^i \neq 0, \quad i < n.$$

Transformata GF-DFT a vectorului *v* este vectorul *V*

$$V = \mathrm{GF}\{v\},$$

cu

$$A_j = n^{-1} v(z^{-j}),\ j = \overline{0, n-1}.$$

Transformata GF-DFT inversă (GF-DFTI) a vectorului *V* este vectorul *v*

$$v = GF^{-1}\{V\},$$

cu

$$a_i = V(z^i),\ i = \overline{0, n-1}.$$

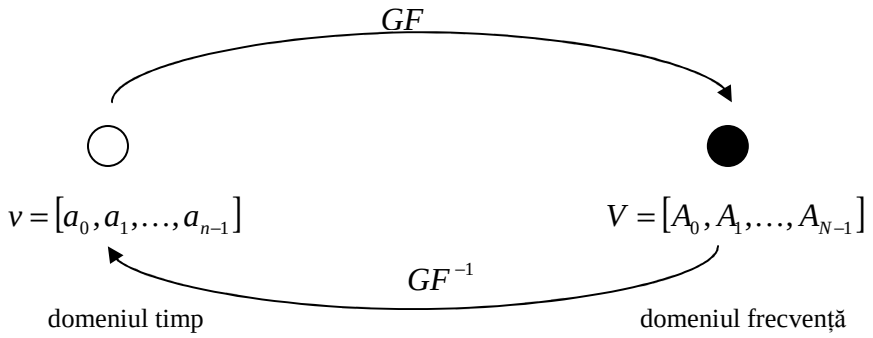


Fig. 3.9. Corespondența domeniul timp – domeniul frecvență.

Codarea şi decodarea prin metoda Reed şi Solomon

Metoda de codare şi decodare Reed şi Solomon are anumite avantaje practice, cu toate că decodarea nu poate fi aplicată decât în cazul codurilor Reed-Solomon de lungime mică.

● *Codarea prin metoda Reed şi Solomon*

Fie $i=[i_0,i_1,\ldots,i_{k-1}]$, $i_i \in GF(q)$ simbolurile de informație care urmează a fi codate şi fie

$$i(z)=\sum_{i=0}^{k-1} i_i z_i \ .$$

Atunci cuvântul de cod corespunzând lui *i* se alege a fi vectorul al cărui *polinom Mattson-Solomon* este *ni(z)*, unde *n=q-1*.

Fie $\alpha \in GF(q^m)$ un element primitiv. Polinomul Mattson-Solomon asociat unui vector $a=[a_0,a_1,\ldots,a_{n-1}]$, $a_i \in GF(q^m)$, este următorul polinom cu coeficienți în $GF(q^m)$

$$A(z)=\sum A_j z^{n-j} \ ,$$

unde

$$A_j = a(\alpha^j)=\sum_{i=0}^{n-1} a_i \alpha^{ij}, \ \ i=0,\pm 1,\pm 2,\ldots \ .$$

Forme alternative pentru *A(z)* sunt:

$$A(z)=\sum_{j=0}^{n-1} A_{-j} z^j = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \left(\alpha^{-i} z\right)^j \ .$$

Deci

$$v=[i(1),i(\alpha),\ldots,i(\alpha^{n-1})].$$

Se poate arăta că *v* este în codul Reed-Solomon verificând că

$$v(x)=\sum_{i=0}^{n-1} v_i x^i$$

are ca rădăcini pe $1,\alpha,\alpha^2,\ldots,\alpha^{d-1}$. De fapt polinomul Mattson-Solomon al lui *v*, *ni(z)* este egal cu

$$\sum_{j=0}^{n-1} A_{-j} z^j ,$$

unde $A_{-j} = v(\alpha^{-j})$. Aşadar , identificând coeficienţii şi luând n = -1 în GF(q), rezultă

$$v(1) = -i_0,\ v(\alpha^{-1}) = -i_1,\ \ldots v(\alpha^{-k+1}) = -i_{k-1}$$

şi $v(\alpha^j) = 0$ pentru $1 \le j \le n-k = d-1$.

● *Decodarea prin metoda Reed şi Solomon*

Se presupune că a fost transmis cuvântul de cod *v*, apare un vector eroare $e = [e_0, e_1, \ldots, e_{n-1}]$, iar $r = [r_0, r_1, \ldots, r_{n-1}]$ este cuvântul recepționat. Deci decodorul cunoaşte

$$r_0 = e_0 + i_0 + i_1 + i_2 + \cdots + i_{k-1},$$

$$r_1 = e_1 + i_0 + i_1\alpha + i_2\alpha^2 + \cdots + i_{k-1}\alpha^{k-1},$$

...

$$r_{n-1} = e_{n-1} + i_0 + i_1\alpha^{n-1} + i_2\alpha^{2(n-1)} + \cdots + i_{k-1}\alpha^{(k-1)(n-1)}.$$

Dacă nu există erori, *e=0*, şi oricare *k* dintre aceste ecuații pot fi rezolvate pentru a determina mesajul $i = [i_0, i_1, \ldots, i_{k-1}]$, deoarece matricea coeficienților este de tip Vandermonde. Deci există C_n^k nedeterminări, sau voturi, pentru vectorul *i* corect.

Dacă există erori, unele seturi de *k* ecuații vor da un *i* greşit. Dar nici un *i* incorect nu poate să primească prea multe voturi.

Dacă apar *t* erori, un *i* incorect va primi cel mult C_{t+k-1}^k voturi, iar vectorul *i* corect va primi cel puțin C_{n-t}^k voturi.

Deci mesajul *i* va fi obținut corect dacă $C_{n-t}^k > C_{t+k-1}^k$, adică dacă *n - t > t+ + k - 1*, sau *d = n – k + 1 > 2t*. Aşa vectorii eroare de pondere mai mică decât jumătate din distanța minimă pot fi corectați.

Coduri derivate din codurile Reed-Solomon

Considerând un element β al câmpului Galois $GF(2^m)$, acesta poate fi exprimat, în mod unic, ca o combinație liniară între puterile elementului primitiv α:

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}.$$

Fie un cod Reed-Solomon corector de *t* erori. Fiecare simbol va fi reprezentat prin m-tuplu corespunzător. Astfel se va obține un cod binar echivalent având lungimea $n = m(2^m - 1)$, iar numărul de simboluri de control va fi *n-k=2mt*. Acest cod va putea corecta orice structură de eroare care va afecta cel mult *t* simboluri a câte *m* biți fiecare. La ieşirea canalului, vectorul recepționat este împărțit în $2^m - 1$ simboluri. Acest cod va fi un *cod corector de pachete fazate multiple* de erori.

Codurile binare derivate din codurile Reed-Solomon sunt foarte eficiente pentru corecția erorilor în pachete multiple deoarece acest tip de erori implică mai multe erori într-un simbol şi relativ puține simboluri eronate.

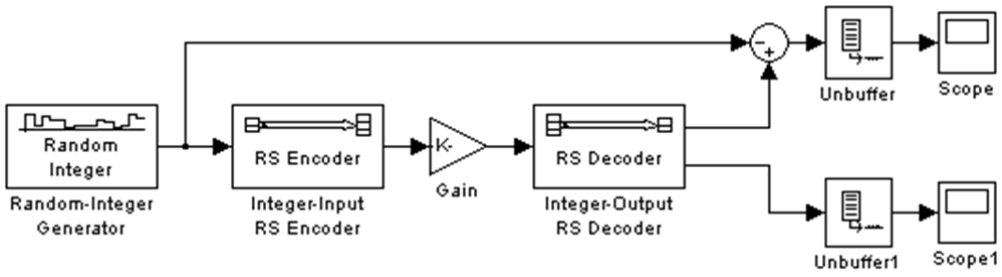
Un cod binar derivat dintr-un cod Reed-Solomon corector de *t* simboluri va fi capabil să corecteze orice combinație de cel mult *v* pachete de erori de lungime *l*, unde

$$v = \frac{t}{1 + \left\lfloor \frac{l + m - 2}{m} \right\rfloor},$$

sau să corecteze orice pachet de erori de lungime *l=(t-1)m+1*. Simultan poate corecta orice combinație de cel mult *t* erori aleatoare.

Implementarea codului Reed-Solomon

Se va implementa codul Reed-Solomon în format întreg. Se realizează schema de mai jos:

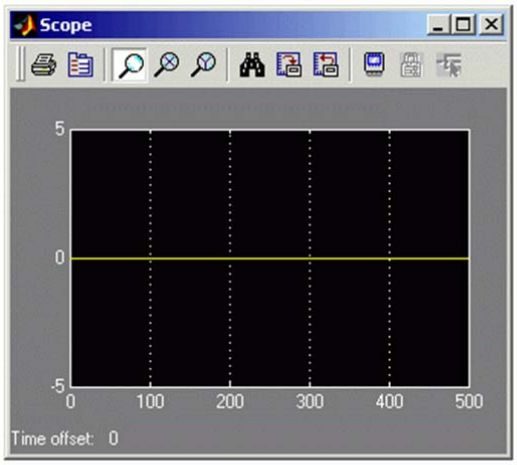


Se vor utiliza următorii parametri:

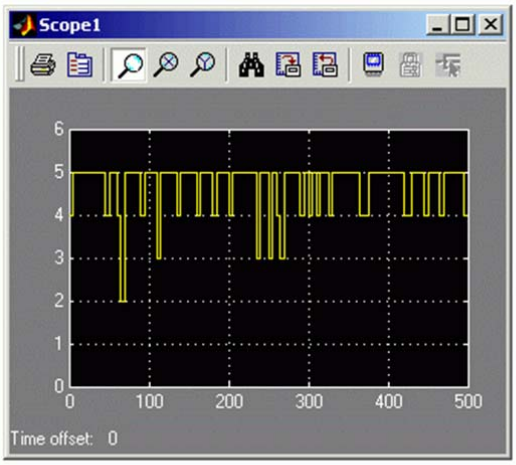
- Random Integer Generator
  - Se stabilește **M-ary number** la `15`.
  - **Initial seed** poate fi orice număr prim mai mare de 30, sau poate fi ieșirea funcției `randseed`.
  - Se bifează **Frame-based outputs**.
  - **Samples per frame** este `5`.
- Integer-Input RS Encoder
  - **Codeword length N** este `15`.
  - Se setează **Message length K** la `5`.
- Gain
  - Parametrul **Gain** este `[0; 0; 0; 0; 0; ones(10,1)]`.
- Integer-Output RS Decoder
  - **Codeword length N** este `15`.
  - Se setează **Message length K** la `5`.
- Sum
  - Lista simbolurilor (**List of signs**) este: `|-+`

Din meniul **Simulation**, se alege **Model Configuration Parameters** și se stabilește **Stop time** la `500`.

La rulare rezultă graficele de mai jos.



Diferența dintre mesajul original și mesajul recuperat



Numărul de erori înainte de corectare

Graficul din partea dreaptă indică numărul erorilor detectate de decodor. De multe ori numărul erorilor este 5 deoarece blocul Gain înlocuiește primele cinci simboluri cu din cod cu zerouri. Valoarea este mai mică de 5 atunci când mesajul transmis conține deja unul sau mai multe zerouri în primele cinci poziții.

Graficul din partea stângă arată diferența dintre mesajul original și mesajul recuperat. Deoarece decodorul a reușit să corecteze toate erorile apărute, diferența este 0.