Decodificar RS.

Decodifican RS.

Sea w=c+e

la palabra recibida, con wt(e) s t= [n-k].

Decodifican RS.

Sea w = c + ela pelabra recibida, con  $wt(e) \le t = \frac{[n-\kappa]}{2}$ .

Sabemos  $d = n - \kappa + 1$   $\kappa = -d + n + 1$ es decir: c = e - connector e = d - 1

```
Decodifican R-S.

Sea w = c + e

la palabra recibida, con wt(e) \le t = \begin{bmatrix} n-\kappa \\ -z \end{bmatrix}.

Sabemos d = n-\kappa+1

k = -\kappa+1+1

k = -\kappa+1+1

es decin: C es e-connector

e = \begin{bmatrix} d-1 \\ -z \end{bmatrix}

Buscamus un polinomio

Q(x,y) = Q_0(x) + y Q_1(x) \in F_q[x,y] \setminus \{o\},
```

```
Decodifican RS.

Sea w = c + e

la palabra necibida, con wt(e) \le t = \frac{[n-\kappa]}{2}.

Sabemos d = n - \kappa + 1

\kappa = n + n + 1

es decir: C es e-connector

e = \left[\frac{d-1}{2}\right]

Buscamos un polinomio

Q(x,y) = Q_0(x) + y Q_1(x) \in \mathbb{F}_q[x,y] \setminus \{e\},

t.q.:

1) Q(x_i, w_i) = 0, i = 1, ..., n (w_i = x_i f(x_i) + e_i)

2) deg Q_0 \le n - 1 - t,

3) deg Q_1 \le n - 1 - t - (\kappa - 1).
```

Decodificar RS. Sea w=c+ela palabra recibida, con  $wt(e) \le t = \begin{bmatrix} n-\kappa \\ 2 \end{bmatrix}$ .

la palabra recibida, con  $wt(e) \le t = \begin{bmatrix} n-\kappa \\ 2 \end{bmatrix}$ . es decir: C es e-connector e = d-1 Buscamos un polinomio  $Q(x,y) = Q_0(x) + y Q_1(x) \in \mathbb{F}_q[x,y] \setminus \{0\},$ t.q.: 1) Q(xi, wi)=0, i=1,..., n (wi= xif(xi)+ei) 2) deg Qo & n-1-t, 3) deg Q, & n-1-t-(K-1). Esto es posible por que 1) son n ecuaciones lineales homogeneas. Siendo  $n-1-t+1+n-1-t-(\kappa-1)+1 > n+1$ existe una solución.

Dem: Sea c=f(x) y w=c+e, wt(e) st.

Teoriema: Si la palabra código envíada es generada por f(x)y hay menos de  $\frac{d}{z}$  errores,  $f(x) = -\frac{Q_0(x)}{Q_1(x)}$ .

Dem: Sea c = f(x) y w = c + e,  $wt(e) \le t$ . Q(x,y) cálculado en (xif(xi) + ei) es o.

Q(xi, f(xi)+ei)=0.

Dem: Sea c=f(x) y w=c+e,  $wt(e) \le t$ . Q(x,y) cálculado en (xif(xi)+ei) es o.

Q(xi, f(xi)+ei)=0.

Siendo que  $e_i=0$  para por lo menos n-t i's, tenemos que Q(x, f(x)) tiene n-t reros o más (cuando  $e_i=w_i$ ).

Teoriema: Si la palabra código envíada es generada por f(x)y hay menos de  $\frac{d}{2}$  errores,  $f(x) = -\frac{Q_0(x)}{Q_1(x)}$ .

Dem: Sea c=l(x) y xy=c+a x,t(e) t

Dem: Sea c=f(x) y w=c+e,  $wt(e) \le t$ . Q(x,y) cálculado en (xif(xi)+ei) es o.

Q(xi, f(xi)+ei)=0.

Siendo que e:=0 para por la menos n-t i's, tenemos que Q(x, f(x)) tiene n-t zeros o más (cuando ci=wi). Ahora deg  $Q(x, f(x)) \le n-t-1 \Longrightarrow Q(x, f(x)) = 0$ . Teoriema: Si la palabra código envíada es generada por f(x) y hay menos de  $\frac{1}{2}$  errores,  $f(x) = -\frac{Q_0(x)}{Q_1(x)}$ .

Dem: Sea c = f(x) y w = c + e,  $wt(e) \le t$ . Q(x,y) códiculado en (xif(xi) + ei) es o. Q(xi,f(xi) + ei) = 0.

Siendo que  $e_i = 0$  para por lo menos n-t i's, tenemos que Q(x,f(x)) tiene n-t terros o más (cuando ci = wi).

Ahora deg  $Q(x,f(x)) \le n-t-1 \Longrightarrow Q(x,f(x)) = 0$ .

Thora deg  $Q(x, f(x)) \le n-t-1 \Longrightarrow Q(x, f(x)) = 0$ . Es decire  $Q(x) + f(x)Q_1(x) = 0$ , cómo queriomos

Ceoriema: Si la palabra código envíada es generada por fíx) y hay menos de  $\frac{d}{2}$  errores,  $f(x) = -\frac{Q_0(x)}{Q_1(x)}$ Dem: Sea c=f(x) y w=c+e, wt(e) &t. Q(x,y) cálculado en (xif(xi)+ei) es o. Q(xi, s(xi)+ei)=0. Siendo que ei=o para por lo menos n-t i's, tenemos que Q(x, f(x)) tiene n-t reros o más (cuando ci=wi). Ahora deg Q(x, f(x)) & n-t-1 => Q(x, f(x)) = 0. Es decire  $Q(x) + f(x)Q_1(x) = 0$ , como querciamos 

Por semplicidad, llamamos

lo=n-1-t, l1=n-1-(K-1)-t.

Dem: Sea c=f(x) y w=c+e,  $wt(e) \le t$ . Q(x,y) cálculado en (xif(xi)+ei) es o.

Q(xi, f(xi)+ei)=0.

Siendo que ei=o para por lo menos n-t i's, tenemos que Q(x, f(x)) tiene n-t reros o más (cuando ci=wi).

Ahora deg  $Q(x, f(x)) \le n-t-1 \Longrightarrow Q(x, f(x)) = 0$ . Es decire  $Q(x) + f(x)Q_1(x) = 0$ , cómo querciomos

Por semplicidad, llamamos

 $l_0 = n - 1 - t, l_1 = n - 1 - (\kappa - 1) - t.$ Siendo  $Q(x, y) = Q_0(x) + yQ_1(x) = Q_1(x) \left( y + \frac{Q_0(x)}{Q_1(x)} \right)$   $= Q_1(x) \left( y - g(x) \right)$ 

los xis donde hay ennones son cerros de Q1(x), que por eso se llama polinomo localizador de ennones.

Dem: Sea c=f(x) y w=c+e,  $wt(e) \le t$ . Q(x,y) cálculado en (xif(xi)+ei) es o.

Q(xi, f(xi)+ei)=0.

Siendo que ei=o para por lo menos n-t i's, tenemos que Q(x, f(x)) tiene n-t reros o más (cuando ci=wi).

Ahora deg  $Q(x, f(x)) \le n-t-1 \Longrightarrow Q(x, f(x)) = 0$ . Es decire  $Q(x) + f(x)Q_1(x) = 0$ , cómo querciamos

Por semplicidad, llamamos

 $l_0 = n - 1 - t, l_1 = n - 1 - (\kappa - 1) - t.$ Siends  $Q(x, y) = Q_0(x) + y Q_1(x) = Q_1(x) \left( y + \frac{Q_0(x)}{Q_1(x)} \right)$   $= Q_1(x) \left( y - g(x) \right)$ 

los xis donde hay ennones son cerros de Q1(x), que por eso se llama polinomro localizador de ennones.

Algoritmo

INPUT: w= w1 ... wn.

Teoriema: Si la palabra código envíada es generada por flx)
y hay menos de  $\frac{1}{4}$  errores,  $f(x) = -\frac{Q_0(x)}{Q_1(x)}$ .

Dem: Sea c = f(x) y w = c + e,  $wt(e) \le t$ . Q(x,y) códiculado en (xif(xi) + ei) es o. Q(xi, f(xi) + ei) = 0.Siendo que e := 0 para por lo menos n - t i's, tenemos que  $Q(x, f(x)) \text{ tiene } n - t \text{ teros } \sigma \text{ más } (\text{cuando } ci = wi).$ Ahora  $\deg Q(x, f(x)) \le n - t - 1 \Longrightarrow Q(x, f(x)) = 0.$ Es decire  $Q(x) + f(x)Q_1(x) = 0$ , cómo queriomos  $\int_0 = n - 1 - t$ Siendo  $Q(x,y) = Q_0(x) + yQ_1(x) = Q_1(x)$   $f(y) + \frac{Q_0(x)}{Q_1(x)}$   $= Q_1(x) (y - f(x))$ 

los xis donde hay ennones son cerros de Q1(x), que por eso se llama polinomo localizador de ennones.

Algoritmo

INPUT: w= w1 ... wn.

② Sean 
$$Q_o(x) = \sum_{j=0}^{l_o} Q_{o,j} \times i$$
,  $Q_1(x) = \sum_{j=0}^{l_o} Q_{1,j} \times i$ ,  $q(x) = -\frac{Q_o(x)}{Q_1(x)}$ 

$$Q_{o}(x) = \sum_{j=0}^{l_{o}} Q_{o,j} \times i, \quad Q_{1}(x) = \sum_{j=0}^{l_{1}} Q_{1,j} \times i, \quad \mathbf{g}(x) = -\frac{Q_{o}(x)}{Q_{1}(x)}$$

3 Si 
$$f(x) \in \mathbb{F}_q[x]$$
 OUTPUT  $c = f(x_1) \cdots f(x_n)$ 

$$Q_{o}(x) = \sum_{j=0}^{l_{o}} Q_{o,j} x^{j}, \quad Q_{1}(x) = \sum_{j=0}^{l_{1}} Q_{1,j} x^{j}, \quad \mathbf{g}(x) = -\frac{Q_{o}(x)}{Q_{1}(x)}$$

3 Si 
$$f(x) \in \mathbb{F}_q[x]$$
 OUTPUT  $c = f(x_1) \cdots f(x_n)$ 

si no

OUTPUT ennor.