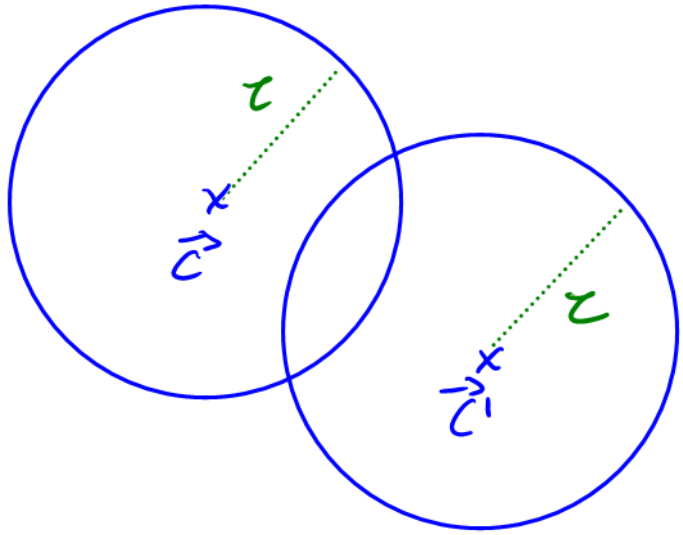
DECODIFICACIÓN EN LISTA

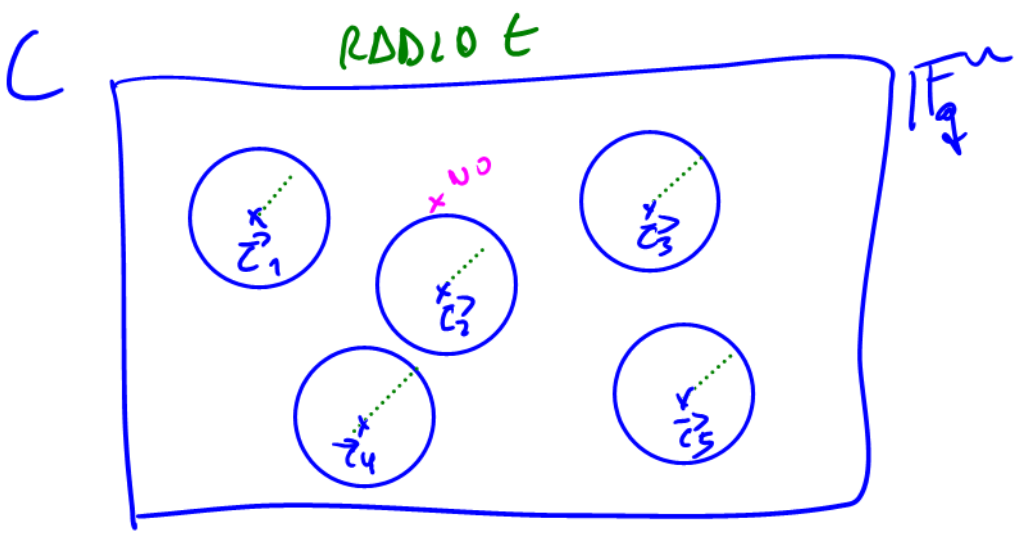
UN CÓDIGO LINEAL TIENE UNA CAPACIDAD CORRECTORA $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

POR LO QUE SI SUPONEMOS QUE RECIBIMOS $\vec{r} = \vec{c} + \vec{e}$ CON $w(\vec{e}) \leq t$, VAMOS A OBTENER LA PALABRA ENVIADA $\vec{c}$

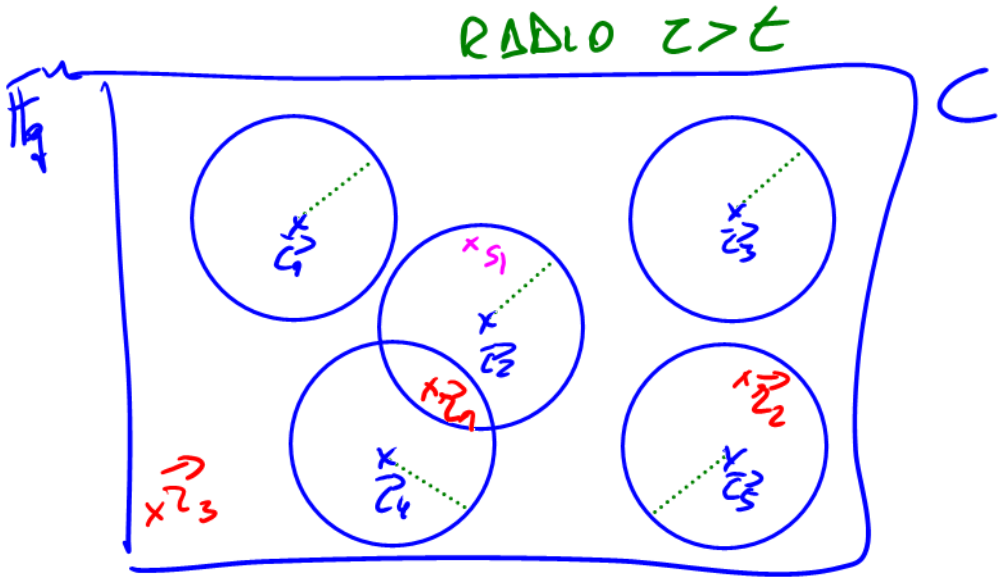
LA IDEA AHORA ES SUPONER QUE SE HAN COMETIDO τ ERRORES CON $\tau \geq t$. AHORA NO PODEMOS GARANTIZAR QUE VAMOS A PODER DECODIFICAR DE LA MISMA FORMA



LAS BOLAS DE CENTRO LAS PALABRAS DEL CÓDIGO Y RADIO τ NO SON DISJUNTAS



DECODIFICACION UNICA



DECODIFICACIÓN EN LISTA

PARA $\vec{r}_1$ OUTPUT $L = \{\vec{c}_2, \vec{c}_4\}$, PARA $\vec{r}_3$ OUTPUT $L = \{\}$

$\vec{r}_2$ OUTPUT $L = \{\vec{c}_5\}$ $\quad w(\vec{e}) > \tau$ $\quad L = \emptyset$

CUANDO $w(\vec{e}) \leq \tau$

OUTPUT: SON TODAS LAS PALABRAS DEL CÓDIGO QUE ESTÉN A DISTANCIA MENOR O IGUAL QUE τ DE LA PALABRA RECIBIDA

VAMOS A MODIFICAR EL ALGORITMO DE DECODIFICACIÓN DE CÓDIGOS REED-SOLOMON PARA QUE HAGA DECODIFICACIÓN EN LISTA.

- C CÓDIGO REED-SOLOMON: $RS_{k,n}$ $[n, k, d]$ $d = n+1-k$
- $\vec{r} \in \mathbb{F}_q^n$ PALABRA RECIBIDA
- $\vec{r} = \vec{c} + \vec{e}$, CON $w(\vec{e}) \leq \tau$ $(\tau \geq t)$

QUEREMOS DETERMINAR EL POLINOMIO

$$Q(X, Y) = \underbrace{Q_0(x)}_{n-\tau-1} + \underbrace{Q_1(x)Y}_{n-\tau-1-(k-1)} + \underbrace{Q_2(x)Y^2}_{n-\tau-1-2(k-1)} + \cdots + \underbrace{Q_\ell(x)Y^\ell}_{n-\tau-1-\ell(k-1)}$$

TAL QUE

$\ell \geq 1$ $\ell > 1$ DL

$$\begin{cases} 1)\ Q(x_i, r_i) = 0 \quad , \ i = 1, \dots, n \\ 2)\ \deg(Q_j(x)) \leq n - \tau - 1 - j(k-1) \quad j = 0, \dots, \ell \\ 3)\ Q(x, y) \neq 0 \ \text{(COMO POLINOMIO)} \end{cases}$$

LEMA: SI $Q(x,y)$ CUMPLE 1), 2) Y 3) Y SI

$\vec{r} = \vec{c} + \vec{e}$ CON $w(\vec{e}) \leq \tau$ Y $c = (f(x_1), \dots, f(x_n))$

CON $\deg(f(x)) < k$ $\Rightarrow$

$$(y - f(x)) \mid Q(x, y)$$

DEM:

$a^b \cdot a^c = a^{b+c}$ $\quad (a^b)^c = a^{b \cdot c}$

$Q(X, f(X))$ ES UN POLINOMIO EN X (UNA VARIABLE), TIENE GRADO MENOR O IGUAL QUE $n-\tau-1$

$$Q(X, f(X)) = \underbrace{Q_0(X)}_{\deg \leq 2} + \underbrace{Q_1(X) f(X)}_{n-\tau-1-(k-1)} + \underbrace{Q_2(X) f^2(X)}_{n-\tau-1-2(k-1)} + \cdots + \underbrace{Q_\ell(X) f^\ell(X)}_{n-\tau-1-\ell(k-1)}$$

$\deg \leq 2 \rightarrow n-\tau-1$

$\deg f(X) \leq k-1$

PERO COMO $r_i = f(x_i)$ CUANDO NO HAY ERROR $\Rightarrow$

$Q(x_i, f(x_i)) = Q(x_i, r_i) = 0$ EN AL MENOS $n-\tau$ POSICIONES

x_i ES UNA RAÍZ DE $Q(X, f(X))$

$\Rightarrow$ TIENE MÁS RAICES QUE GRADO $\Rightarrow Q(X, f(X))$ ES EL POLINOMIO 0 (COMO POLINOMIO EN X)

$$Q(X,Y) \in \left(\mathbb{F}_q[x]\right)[Y]$$

POLINOMIO CON VARIABLE Y, COEFICIENTES POLINOMIOS EN X

$$Q(x, f(x)) = 0 \Rightarrow f(x) \text{ ES COMO UNA RAÍZ PARA } Y$$

$$\Rightarrow (Y - f(x)) \mid Q(x, y)$$

ESTO SIGNIFICA QUE TODAS LAS PALABRAS DEL CÓDIGO QUE ESTÉN A DISTANCIA MENOR O IGUAL QUE z DE LA PALABRA RECIBIDA, SE VAN A ENCONTRAR FACTORIZANDO EL POLINOMIO $Q(x,y)$ Y MIRANDO LOS FACTORES DE LA FORMA

$$y - f(x), \text{ CON } \deg f(x) < k$$

¿CUANTAS PALABRAS PUEDE HABER EN LA LISTA?

ℓ COMO MUCHO → GRADO DE $Q(x,y)$ EN y

↳ ADEMÁS NO TODOS LOS FACTORES LINEALES VAN A CORRESPONDER CON PALABRAS DEL CODIGO A DISTANCIA z DE Σ

¿PARA QUE VALORES DE r Y ℓ EL POLINOMIO $Q(x,y)$ VERIFICANDO 1/ 2/ Y 3/ EXISTE?

- TENEMOS UN SISTEMA DE n ECUACIONES LINEALES HOMOGENEO EN LOS COEFICIENTES DE $Q_0^{(x)}, Q_1^{(x)}, \ldots, Q_\ell^{(x)}$ (POR 1/)

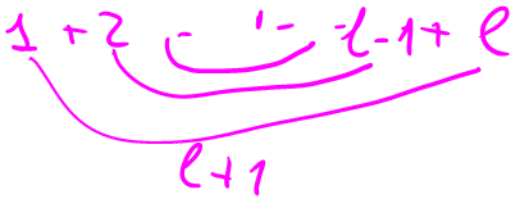
- LUEGO SI TENEMOS UN NÚMERO DE COEFICIENTES MAYOR QUE n, PODEMOS ENCONTRAR $Q(x,y)$ DADO QUE EL SISTEMA TIENE SOLUCIÓN

- NÚMERO DE COEFICIENTES:

$$(n-r) + (n-r-(k-1)) + (n-r-2(k-1)) + \cdots + (n-r-\ell(k-1))$$
$$Q_0 \qquad Q_1 \qquad Q_2 \qquad Q_\ell$$

$$= (\ell+1)(n-\tau) - (k-1)(1+2+\cdots+\ell)$$

$$= (\ell+1)(n-\tau) - (k-1)\frac{\ell+1}{2}\ell$$



QUEREMOS QUE

$$(\ell+1)(n-\tau) - \frac{1}{2}\ell(\ell+1)(k-1) > n$$

DONDE ℓ ES EL MAYOR ENTERO QUE

$\deg Q_\ell$

$$(n-\tau) - \ell(k-1) \geq 0$$

PARA QUE $Q_\ell(x)$ EXISTA

PARA $\ell = 2$

$$(n-\tau) - 2(k-1) \geq 0 \Rightarrow$$

$$k - 1 \leq \frac{n-\tau}{2} \quad (*)$$

ESTO ES MEJOR QUE LA COTA PARA DECODIFICACIÓN ÚNICA: $\epsilon < \frac{d}{2} = \frac{n+1-k}{2}$

$$k - 1 = n - 2t \quad (**) \quad \text{SI} \quad (*) > (**)$$

$t = \frac{n+1-k}{2}$ $\quad 2t = n+1-k$ $\quad k-1 = n-2t$

$$\frac{n-\tau}{2} > n - 2\tau \iff n - \tau > 2n - 4\tau \iff 3\tau > n$$

$$\iff \tau > n/3 \quad \text{ES DECIR}$$

VUELVO A (*)

↳ $k - 1 < \frac{n - n/3}{2} \iff k - 1 < \frac{n}{3} \iff k < \frac{n}{3} + 1 \iff$

$$\Leftrightarrow \quad \frac{k}{n} < \frac{1}{3} + \frac{1}{n}$$

$(\ell=2+1)$

QUE PARA ℓ GENERAL NOS DA QUE SI

$$\boxed{\frac{k}{n} < \frac{1}{\ell+1} + \frac{1}{n}}$$

ENTONCES MEJORAMOS EL ALGORITMO DE DECODIFICACIÓN ÚNICA, Y EN ESE CASO

¿CUÁNTO PUEDE SER τ? $\#$ COEFICIENTES $>$ $\#$ ECUACIONES

$$(\ell+1)(n-\tau) - \tfrac{1}{2}\ell(\ell+1)(k-1) > n \Leftrightarrow$$

$$(\ell+1)(n-\tau) > n + \tfrac{1}{2}\ell(\ell+1)(k-1)$$

$$n-\tau > \frac{n}{\ell+1} + \tfrac{1}{2}\ell(k-1)$$

$$\tau < n - \frac{n}{\ell+1} + \frac{1}{2}\ell(k-1) = \frac{n\ell}{\ell+1} + \frac{1}{2}\ell(k-1)$$

$$\boxed{\tau < n\frac{\ell}{\ell+1} - \frac{\ell}{2}(k-1)}$$

(**)

¿QUÉ VALORES PUEDEN TOMAR ℓ Y τ?

CUALQUIERA QUE VERIFIQUEN (*) Y (**)

(*) → MEJORAS DEC. UNICA

(**) → EXISTE POLINOMIO Q

ALGORITMO DE SUDAN PARA DECODIFICAR EN LISTA UNA PALABRA RECIBIDA $\vec{r}$ USANDO UN CÓDIGO REED-SOLOMON DE DIMENSIÓN k Y CON COTA DEL ERROR τ.

1) ENCUENTRA UNA SOLUCIÓN NO NULA DEL SISTEMA DE ECUACIONES LINEALES

$$\sum_{j=0}^{e} \begin{bmatrix} r_1^j & & 0 \\ & r_2^j & \\ 0 & & r_n^j \end{bmatrix} \begin{bmatrix} 1 & x_1 & \cdots & x_1^{\ell_j} \\ 1 & x_2 & \cdots & x_2^{\ell_j} \\ \vdots & \vdots & & \\ 1 & x_n & \cdots & x_n^{\ell_j} \end{bmatrix} \begin{bmatrix} Q_{j0} \\ Q_{j1} \\ \vdots \\ Q_{j\ell_j} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

DONDE $\ell_j = n - c - 1 - j(k-1)$

2) $$Q_j(x) = \sum_{z=0}^{\ell_j} Q_{jz} x^z$$

$$Q(x,y) = \sum_{j=0}^{e} Q_j(x)\, y^j$$

3/ ENCUENTRA LOS FACTORES DE $Q(x,y)$ DE LA FORMA $(y - f(x))$ CON $\deg f(x) < k$

OUTPUT: LA LISTA FORMADA POR TODOS LOS FACTORES ANTERIORES QUE VERIFIQUEN

$$d((f(x_1), \ldots, f(x_m)), (r_1, \ldots, r_m)) \leq t$$

- ¿CÓMO FACTORIZAMOS $Q(x,y)$?

↳ NOSOTROS CON UN COMANDO EN SAGEMATH

EJEMPLO 4.3.1. DEL LIBRO JUSTESEN-HØHOLDT