Locally recoverable J-affine variety codes

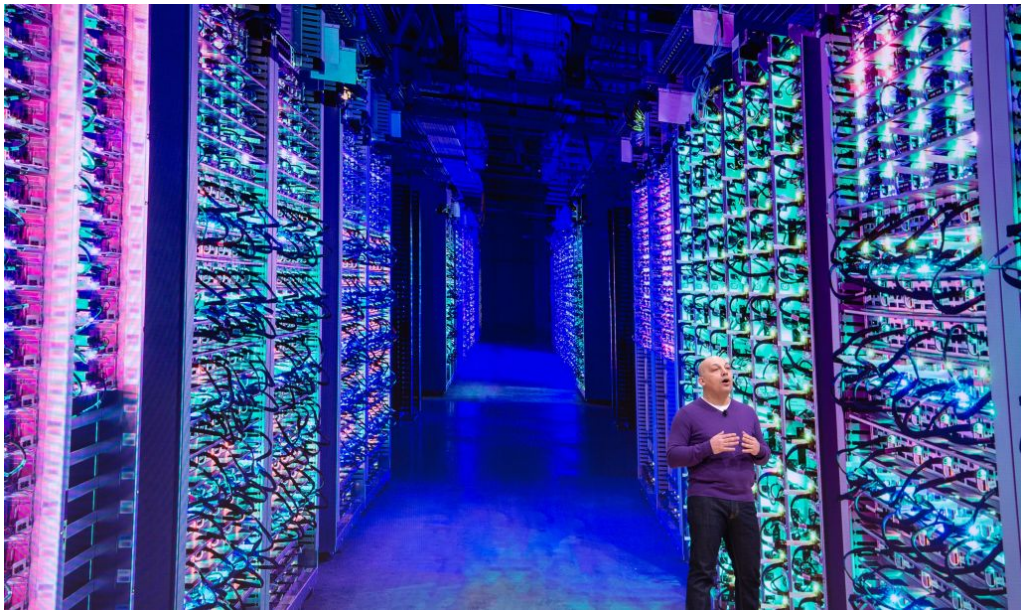
Seminario de Álgebra, Geometría algebraica y Singularidades

Fernando Hernando

IMAC/UJI

8 de febrero de 2022

Motivación



Los sistemas distribuidos y de almacenamiento en la nube han llegado a una escala tan masiva que la recuperación de errores ahora es una tarea habitual y no algo esporádico. Además, los sistemas de almacenamiento deben proporcionar alta disponibilidad de datos para garantizar un alto rendimiento. Para satisfacer estas necesidades, la redundancia y la codificación de datos es indispensable en el sistema.

¿Qué significa localmente recuperable?

Los sistemas de almacenamiento actuales, para poder ser fiables, deben de ser resistentes a varios errores de nodos concurrentes. Por lo tanto, un sistema de almacenamiento debe diseñarse para reparar eficientemente dichos errores. La eficiencia en la reparación de un error en un solo nodo se puede cuantificar bajo los siguientes parámetros (cada uno relevante para diferentes sistemas de almacenamiento y aplicaciones).

¿Qué significa localmente recuperable?

Los sistemas de almacenamiento actuales, para poder ser fiables, deben de ser resistentes a varios errores de nodos concurrentes. Por lo tanto, un sistema de almacenamiento debe diseñarse para reparar eficientemente dichos errores. La eficiencia en la reparación de un error en un solo nodo se puede cuantificar bajo los siguientes parámetros (cada uno relevante para diferentes sistemas de almacenamiento y aplicaciones).

i) el número de bits transferidos en la red, es decir, el ancho de banda de reparación,

ii) el número de bits leídos,

iii) **localidad de reparación, es decir, el número de nodos que participan en el proceso de reparación**.

Borrón vs Error

En un borrón se conoce la posición del nodo que falló mientras que en un error no.

Una manera sencilla es repetir cada bit varias veces:

$$1 \to 11$$

$$0 \to 00$$

Borrón vs Error

En un borrón se conoce la posición del nodo que falló mientras que en un error no.

Una manera sencilla es repetir cada bit varias veces:

$$1 \to 11$$

$$0 \to 00$$

Si recibimos 10 sabremos que hay un error pero no podremos decidir si enviaron 1 o 0.

Borrón vs Error

En un borrón se conoce la posición del nodo que falló mientras que en un error no.

Una manera sencilla es repetir cada bit varias veces:

$$1 \to 11$$

$$0 \to 00$$

Si recibimos 10 sabremos que hay un error pero no podremos decidir si enviaron 1 o 0.

$$1 \to 111$$

$$0 \to 000$$

Si recibimos 110 lo mas probables es que el el bit enviado fuera 1.

Por cada bit the informacion mandamos 3, ratio 1/3 y podemos corregir un error, ¿podemos hacerlo mejor ?

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos siendo $q = p^r$.

Definición

Un **código lineal** C es un subespacio vectorial de $\mathbb{F}_q^n$

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos siendo $q = p^r$.

Definición

Un **código lineal** C es un subespacio vectorial de $\mathbb{F}_q^n$

Denotemos por k la **dimensión** de C. Una base de C puesta en forma matricial es una matriz $k \times n$ que denotamos por G **matriz generatriz**.

Codificar es: $(a_1, \ldots, a_k)G = (c_1, \ldots, c_n)$.

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos siendo $q = p^r$.

Definición

Un **código lineal** C es un subespacio vectorial de $\mathbb{F}_q^n$

Denotemos por k la **dimensión** de C. Una base de C puesta en forma matricial es una matriz $k \times n$ que denotamos por G **matriz generatriz**.

Codificar es: $(a_1, \ldots, a_k)G = (c_1, \ldots, c_n)$.

Definición

$a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$.

$$d(a,b)\#\{i \mid a_i \neq b_i\}, \quad wt(a)\#\{i \mid a_i \neq 0\}$$

$$d = d(C) = min\{d(a,b) \min a, b \in C\} = min\{wt(a) \mid a \in C\}.$$

Códigos lineales

Decimos que un código C es $[n, k, d]_q$ si tiene:
Longitud n.
Dimension k
Distancia mínima d.

Códigos lineales

Decimos que un código C es $[n, k, d]_q$ si tiene:
Longitud n.
Dimension k
Distancia mínima d.

Definition

El **dual** de C lo denotamos por $C^{\perp}$ y se define como

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid < x, c >= 0, \forall c \in C\}.$$

Códigos lineales

Decimos que un código C es $[n, k, d]_q$ si tiene:
Longitud n.
Dimension k
Distancia mínima d.

Definition

El **dual** de C lo denotamos por $C^{\perp}$ y se define como

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid < x, c >= 0, \forall c \in C\}.$$

$C^{\perp}$ es un código $[n, n-k, d^{\perp}]$ cuya matriz generatiz denotamos por H y se llama **matriz de control de C**.

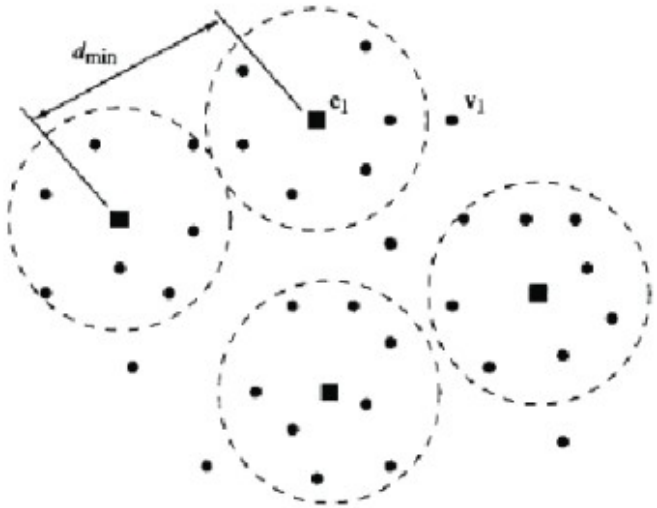
$$c \in C \Leftrightarrow Hc^t = 0.$$

Un código lineal C de distancia minima d puede:

- detectar $d-1$ errores.
  $H(c+e)^t = Hc^t + He^t = He^t \neq 0$.

Un código lineal C de distancia minima d puede:

- detectar $d-1$ errores.
  $H(c+e)^t = Hc^t + He^t = He^t \neq 0$.
- corregir $\lfloor \frac{d-1}{2} \rfloor$ errores.



Conjetura MDS

Cota Singleton

$$d \leq n - k + 1$$

Maximum Distance Separable

Si $d = n - k + 1$ se dice que el codigo es MDS.

Conjetura MDS

Cota Singleton

$$d \leq n - k + 1$$

Maximum Distance Separable

Si $d = n - k + 1$ se dice que el codigo es MDS.

Conjetura

La longitud n de un código de máxima distancia separable de dimensión k es como máximo $q + 1$, salvo que q sea par y $k = 3$ o $k = q - 1$. En tal caso es como máximo $q + 2$.

Paréntesis: Geometría Finita

Se C un código MDS $[n, k, n-k+1]_q$ con matriz generatriz $G_{k\times n}$. Cada columna de G puede entenderse como un punto $(p_0, \ldots, p_{k-1}) \in \mathbb{P}G(k-1, q)$. Tenemos un conjunto $\Delta = \{P_1, \ldots, P_n\}$ de n puntos en $\mathbb{P}G(k-1, q)$.

Paréntesis: Geometría Finita

Se C un código MDS $[n, k, n-k+1]_q$ con matriz generatriz $G_{k\times n}$. Cada columna de G puede entenderse como un punto $(p_0, \ldots, p_{k-1}) \in \mathbb{P}G(k-1, q)$. Tenemos un conjunto $\Delta = \{P_1, \ldots, P_n\}$ de n puntos en $\mathbb{P}G(k-1, q)$.

C es MDS $\Leftrightarrow$ cualquier subconjunto de k columnas es linealmente independiente pero $k+1$ no lo son $\Leftrightarrow$ $k+1$ puntos cualesquiera de Δ no están en un hiperplano$\overset{def}{\Leftrightarrow}$ Δ es un n-arco en $\mathbb{P}G(k-1, q)$ (Segre).

Paréntesis: Geometría Finita

Se C un código MDS $[n, k, n-k+1]_q$ con matriz generatriz $G_{k\times n}$. Cada columna de G puede entenderse como un punto $(p_0, \ldots, p_{k-1}) \in \mathbb{P}G(k-1, q)$. Tenemos un conjunto $\Delta = \{P_1, \ldots, P_n\}$ de n puntos en $\mathbb{P}G(k-1, q)$.

C es MDS $\Leftrightarrow$ cualquier subconjunto de k columnas es linealmente independiente pero $k+1$ no lo son $\Leftrightarrow$ $k+1$ puntos cualesquiera de Δ no están en un hiperplano$\overset{def}{\Leftrightarrow}$ Δ es un n-arco en $\mathbb{P}G(k-1, q)$ (Segre).

Problemas de Segre

- Dados k y q, cuál es el máximo valor de n tal que un n-arco existe en $\mathbb{P}G(k-1, q)$?
- Para que valores de k y q, con $q > k+1$, se tiene que todo $(q+1)$-arco de $\mathbb{P}G(k-1, q)$ es una curva normal racional.
- Dados k y q con $q > n+1$, para que valores de n se tiene que un n-arco de $\mathbb{P}G(k-1, q)$ esta contenido en un $(q+1)$-arco de $\mathbb{P}G(k-1, q)$?

n-Arcos en $\mathbb{P}G(2,q)$

Theorem

Sea Δ un n arco en $\mathbb{P}G(2,q)$.

- $n \leq q+2$.
- *Si q impar , $n \leq q+1$.*
- *Toda cónica no singular de $\mathbb{P}G(2,q)$ es un $q+1$-arco*
- *Si q es par, todo $q+1$-arco en $\mathbb{P}G(2,q)$ extiende a un $q+2$-arco.*

n-Arcos en $\mathbb{P}G(2,q)$

Theorem

Sea Δ un n arco en $\mathbb{P}G(2,q)$.

- $n \leq q+2$.
- *Si q impar , $n \leq q+1$.*
- *Toda cónica no singular de $\mathbb{P}G(2,q)$ es un $q+1$-arco*
- *Si q es par, todo $q+1$-arco en $\mathbb{P}G(2,q)$ extiende a un $q+2$-arco.*

Los $q+1$-arcos se llaman ovalos y los $q+2$-arcos se llaman ovalos completos o hyperovalos

n-Arcos en $\mathbb{P}G(2,q)$

Theorem

Sea Δ un n arco en $\mathbb{P}G(2,q)$.

- $n \leq q+2$.
- *Si q impar , $n \leq q+1$.*
- *Toda cónica no singular de $\mathbb{P}G(2,q)$ es un $q+1$-arco*
- *Si q es par, todo $q+1$-arco en $\mathbb{P}G(2,q)$ extiende a un $q+2$-arco.*

Los $q+1$-arcos se llaman ovalos y los $q+2$-arcos se llaman ovalos completos o hyperovalos

F.Hernando and Gary McGuire: Proof of a Conjecture of Segre and Bartocci on Monomial Hyperovals in Projective Planes. Design Codes and Cryptography, December 2012, Volume 65, Issue 3, pp 275-289

Des. Codes Cryptogr. (2012) 65:275–289
DOI 10.1007/s10623-012-9624-3

Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes

Fernando Hernando · Gary McGuire

Received: 14 October 2010 / Revised: 13 October 2011 / Accepted: 25 January 2012 /
Published online: 16 February 2012

Abstract The existence of certain monomial hyperovals $D(x^k)$ in the finite Desarguesian projective plane $PG(2, q)$, q even, is related to the existence of points on certain projective plane curves $g_k(x, y, z)$. Segre showed that some values of k ($k = 6$ and 2^i) give rise to hyperovals in $PG(2, q)$ for infinitely many q. Segre and Bartocci conjectured that these are the only values of k with this property. We prove this conjecture through the absolute irreducibility of the curves g_k.

Códigos Reed-Solomon

$\mathbb{F}_q[x]_{k-1} =< 1, x, x^2, \ldots, x^{k-1} >.$
$P := \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q.$

Códigos Reed-Solomon

$\mathbb{F}_q[x]_{k-1} =< 1, x, x^2, \ldots, x^{k-1} >$.
$P := \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$.

$$ev : \mathbb{F}_q[x]_{k-1} \to \mathbb{F}_q^n$$

$$f \to (f(P_1), \ldots, f(P_n))$$

$$C = Im(ev) =< ev(1), ev(x), \ldots, ev(x^{k-1}) >$$

C es un código $[n, k, n-k+1]_q$ (MDS).

Códigos Reed-Solomon

$\mathbb{F}_q[x]_{k-1} =< 1, x, x^2, \ldots, x^{k-1} >$.
$P := \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$.

$$ev : \mathbb{F}_q[x]_{k-1} \to \mathbb{F}_q^n$$

$$f \to (f(P_1), \ldots, f(P_n))$$

$$C = Im(ev) =< ev(1), ev(x), \ldots, ev(x^{k-1}) >$$

C es un código $[n, k, n-k+1]_q$ (MDS).

Los códigos Reed-Solomon son una subfamilia de los códigos AG.

Paréntesis: Códigos AG

Sea X una variedad proyectiva lisa sobre un cuerpo finito $\mathbb{F}_q$.
$D = \{P_1, \ldots, P_n\}$ un conjunto de puntos racionales de X.
H un divisor de X con soporte disjunto de D.

Paréntesis: Códigos AG

Sea X una variedad proyectiva lisa sobre un cuerpo finito $\mathbb{F}_q$.
$D = \{P_1, \ldots, P_n\}$ un conjunto de puntos racionales de X.
H un divisor de X con soporte disjunto de D.

$$L(H) := \{f \in \mathbb{F}_q(X) \mid (f) + H \geq 0\} \cup \{0\}$$

$$ev_D : L(H) \to \mathbb{F}_q^n$$

$$ev_D(f) = (f(P_1), \ldots, f(P_n)).$$

$C = C(X, D, H) := Im(ev_D)$.

Paréntesis: Códigos AG

Sea X una variedad proyectiva lisa sobre un cuerpo finito $\mathbb{F}_q$.
$D = \{P_1, \ldots, P_n\}$ un conjunto de puntos racionales de X.
H un divisor de X con soporte disjunto de D.

$$L(H) := \{f \in \mathbb{F}_q(X) \mid (f) + H \geq 0\} \cup \{0\}$$
$$ev_D : L(H) \to \mathbb{F}_q^n$$
$$ev_D(f) = (f(P_1), \ldots, f(P_n)).$$

$C = C(X, D, H) := Im(ev_D)$.

Riemann–Roch theorem

Si X es un curva de género g tal que $2g - 2 < deg(H) < n$ entonces:

$$k = deg(H) - g + 1$$

$$d \geq n - deg(H).$$

$X = \mathbb{P}$ y $H = (k-1)\infty$ tenemos el código Reed-Solomon.

Cota de Hasse-Weil

Número de puntos racionales

$$q + 1 - 2g\sqrt{(q)} \leq X(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{(q)}$$

Cota de Hasse-Weil

Número de puntos racionales

$$q+1-2g\sqrt{(q)} \leq X(\mathbb{F}_q) \leq q+1+2g\sqrt{(q)}$$

Curva Maximal

Si $X(\mathbb{F}_q) = q+1+2g\sqrt{(q)}$ se dice que la curva es maximal.

Cota de Hasse-Weil

Número de puntos racionales

$$q+1-2g\sqrt{(q)} \leq X(\mathbb{F}_q) \leq q+1+2g\sqrt{(q)}$$

Curva Maximal

Si $X(\mathbb{F}_q) = q+1+2g\sqrt{(q)}$ se dice que la curva es maximal.

Problema

Encontrar curvas con muchos puntos racionales.

Códigos localmente recuperables

Son aquellos códigos en los cuales podemos corregir borrones a partir de un subconjunto de coordenadas.

Notación

Dado un subconjunto de índices $R \subseteq \{1, \ldots, n\}$ denotamos por π_R la proyección en las coordenadas de R.

Código perforado es

$$C[R] := \{\pi_R(\mathbf{c}) \mid \mathbf{c} \in C\}.$$

localidad (r, δ)

Un código LRC C tiene **localidad** (r, δ) si $\forall i \in \{1, \ldots, n\}$ $\exists R = R(i) \subseteq \{1, \ldots, n\}$ tal que:

1. $i \in R$ y $\#R \leq r + \delta - 1$,
2. $d(C[R]) \geq \delta$.

R es un (r, δ)-**conjunto de recuperación**.

localidad (r, δ)

Un código LRC C tiene **localidad** (r, δ) si $\forall i \in \{1, \ldots, n\}$ $\exists R = R(i) \subseteq \{1, \ldots, n\}$ tal que:

1. $i \in R$ y $\#R \leq r + \delta - 1$,
2. $d(C[R]) \geq \delta$.

R es un (r, δ)-**conjunto de recuperación**.

Desigualdad tipo Singleton códigos LRC

$$k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1) \leq n + 1.$$

Si se da la igualdad, diremos que C es **óptimo**.

Códigos J-afines I

- $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ y tomamos m enteros $N_j > 1$ tal que $N_j - 1$ divide a $q - 1$ para $1 \leq j \leq m$.

Códigos J-afines I

- $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ y tomamos m enteros $N_j > 1$ tal que $N_j - 1$ divide a $q - 1$ para $1 \leq j \leq m$.
- $J \subseteq \{1, 2, \ldots, m\}$, sea I_J el ideal generado por $X_j^{N_j} - X_j$ cuando $j \notin J$ y por $X_j^{N_j - 1} - 1$ en otro caso.
- $R_J := \mathbb{F}_q[X_1, X_2, \ldots, X_m]/I_J$.

Códigos J-afines I

- $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ y tomamos m enteros $N_j > 1$ tal que $N_j - 1$ divide a $q - 1$ para $1 \leq j \leq m$.
- $J \subseteq \{1, 2, \ldots, m\}$, sea I_J el ideal generado por $X_j^{N_j} - X_j$ cuando $j \notin J$ y por $X_j^{N_j - 1} - 1$ en otro caso.
- $R_J := \mathbb{F}_q[X_1, X_2, \ldots, X_m]/I_J$.
- $Z_J = Z(I_J) = \{P_1, P_2, \ldots, P_{n_J}\}$: el conjunto de ceros sobre $\mathbb{F}_q$ del ideal de definicion de R_J.

Códigos J-afines I

- $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ y tomamos m enteros $N_j > 1$ tal que $N_j - 1$ divide a $q - 1$ para $1 \leq j \leq m$.
- $J \subseteq \{1, 2, \ldots, m\}$, sea I_J el ideal generado por $X_j^{N_j} - X_j$ cuando $j \notin J$ y por $X_j^{N_j - 1} - 1$ en otro caso.
- $R_J := \mathbb{F}_q[X_1, X_2, \ldots, X_m]/I_J$.
- $Z_J = Z(I_J) = \{P_1, P_2, \ldots, P_{n_J}\}$: el conjunto de ceros sobre $\mathbb{F}_q$ del ideal de definicion de R_J.
- $\mathrm{ev}_J : R_J \to \mathbb{F}_q^{n_J}$, $\mathrm{ev}_J(f) = (f(P_1), f(P_2), \ldots, f(P_{n_J}))$, donde $n_J = \prod_{j \notin J} N_j \prod_{j \in J}(N_j - 1)$.

Códigos J-afines II

Sea $T_j = N_j - 1$ excepto cuando $j \in J$, en cuyo caso, $T_j = N_j - 2$. Consideramos el conjuntto

$$\mathcal{H}_J := \{0, 1, \ldots, T_1\} \times \{0, 1, \ldots, T_2\} \times \cdots \times \{0, 1, \ldots, T_m\}$$

y un subconjunto no vacio $\Delta \subseteq \mathcal{H}_J$.

Definition

Se define código de variedad J-affine dado por Δ, y lo denotamos por E_Δ^J, como esl subespacio vectorial (sobre $\mathbb{F}_q$) de $\mathbb{F}_q^{n_J}$ generado por la evaluación ev_J de las clases en R_J correspondientes a los monomios $X^{\boldsymbol{a}} := X_1^{a_1} X_1^{a_2} \cdots X_m^{a_m}$ tal que $\boldsymbol{a} = (a_1, a_2, \ldots, a_m) \in \Delta$.

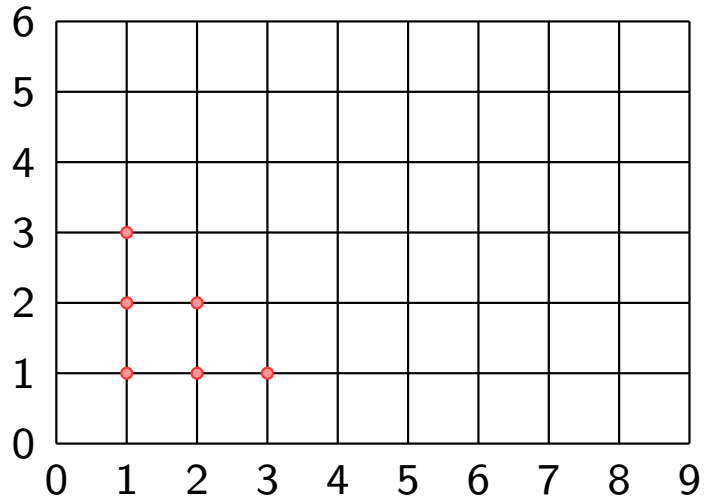
Ejemplo

Sean $p = 2$, $r = 6$ y $m = 2$ (dos variables), con $q = 2^6 = 64$. Tomamos $N_1 - 1 = 9$ y $N_2 - 1 = 7$.

- Si $J = \{\}$, $T_1 = 9$ y $T_2 = 7$, $n_J = 80$.
- Si $J = \{1\}$, $T_1 = 8$ y $T_2 = 7$, $n_J = 72$.
- Si $J = \{2\}$, $T_1 = 9$ y $T_2 = 6$, $n_J = 70$.
- Si $J = \{1, 2\}$, $T_1 = 8$ y $T_2 = 6$, $n_J = 63$.

En el caso $J = \{2\}$, $T_1 = 9$ y $T_2 = 6$, $n_J = 70$, el anillo es $\mathbb{F}_{64}[X, Y]/ < X^{10} - X, Y^7 - 1 >$

$$\Delta = \{(1,1),(1,2),(1,3),(1,2),(2,2),(1,3)\} \subset \{0,1,\ldots,9\} \times \{0,1,\ldots,6\}$$



E_Δ^J es un código lineal de parámetros $[70, 6, d]_{64}$

Aplicación Traza

- $q = p^r$, sea s un entero positivo tal que s divide a r.
- $\mathrm{tr}_r^s : \mathbb{F}_{p^r} \to \mathbb{F}_{p^s}$ definida como $\mathrm{tr}_r^s(x) = x + x^{p^s} + \cdots + x^{p^{s(\frac{r}{s}-1)}}$.
- $\mathbb{F}_{p^r}^{n_J} \to \mathbb{F}_{p^s}^{n_J}$, determinada por tr_r^s componentwise.
- $\mathcal{T} : R_J \to$, $\mathcal{T}(f) = f + f^{p^s} + \cdots + f^{p^{s(\frac{r}{s}-1)}}$.

Aplicación Traza

- $q = p^r$, sea s un entero positivo tal que s divide a r.
- $\mathrm{tr}_r^s : \mathbb{F}_{p^r} \to \mathbb{F}_{p^s}$ definida como $\mathrm{tr}_r^s(x) = x + x^{p^s} + \cdots + x^{p^{s(\frac{r}{s}-1)}}$.
- $\mathbb{F}_{p^r}^{n_J} \to \mathbb{F}_{p^s}^{n_J}$, determinada por tr_r^s componentwise.
- $\mathcal{T} : R_J \to$, $\mathcal{T}(f) = f + f^{p^s} + \cdots + f^{p^{s(\frac{r}{s}-1)}}$.

Sea $g \in R_J$. Son equivalente:

1. $g = \mathcal{T}(h)$, con $h \in R_J$.
2. $g^{p^s} = g$.
3. g evalua en $\mathbb{F}_{p^s}$.

Aplicación Traza

- $q = p^r$, sea s un entero positivo tal que s divide a r.
- $\mathrm{tr}_r^s : \mathbb{F}_{p^r} \to \mathbb{F}_{p^s}$ definida como $\mathrm{tr}_r^s(x) = x + x^{p^s} + \cdots + x^{p^{s(\frac{r}{s}-1)}}$.
- $\mathbb{F}_{p^r}^{n_J} \to \mathbb{F}_{p^s}^{n_J}$, determinada por tr_r^s componentwise.
- $\mathcal{T} : R_J \to$, $\mathcal{T}(f) = f + f^{p^s} + \cdots + f^{p^{s(\frac{r}{s}-1)}}$.

Sea $g \in R_J$. Son equivalente:

1. $g = \mathcal{T}(h)$, con $h \in R_J$.
2. $g^{p^s} = g$.
3. g evalua en $\mathbb{F}_{p^s}$.

Sean $p = 2, r = 4$

$$tr_4^2(x) = x + x^4; \quad tr_4^1(x) = x + x^2 + x^4 + x^8;$$

Conjuntos Ciclotomicos

- *Conjuntos ciclotomicos*: subconjuntos $\mathfrak{I}$ de $\mathbb{Z}_{T_1} \times \mathbb{Z}_{T_2} \times \cdots \times \mathbb{Z}_{T_m}$ tal que $\mathfrak{I} = \{p^s \cdot \boldsymbol{a} \mid \boldsymbol{a} \in \mathfrak{I}\}$, donde $p^s \cdot \boldsymbol{a} = (p^s a_1, p^s a_2, \ldots, p^s a_m)$.

Conjuntos Ciclotomicos

- *Conjuntos ciclotomicos*: subconjuntos $\mathfrak{I}$ de $\mathbb{Z}_{T_1} \times \mathbb{Z}_{T_2} \times \cdots \times \mathbb{Z}_{T_m}$ tal que $\mathfrak{I} = \{p^s \cdot \boldsymbol{a} \mid \boldsymbol{a} \in \mathfrak{I}\}$, donde $p^s \cdot \boldsymbol{a} = (p^s a_1, p^s a_2, \ldots, p^s a_m)$.
- $\mathfrak{I}$ es *minimal* si todo elemento de $\mathfrak{I}$ se puede expresar como $p^{si} \cdot \boldsymbol{a}$ para algún elemento $\boldsymbol{a} \in \mathfrak{I}$ y algún i.

Conjuntos Ciclotomicos

- *Conjuntos ciclotomicos*: subconjuntos $\mathfrak{I}$ de $\mathbb{Z}_{T_1} \times \mathbb{Z}_{T_2} \times \cdots \times \mathbb{Z}_{T_m}$ tal que $\mathfrak{I} = \{p^s \cdot \boldsymbol{a} \mid \boldsymbol{a} \in \mathfrak{I}\}$, donde $p^s \cdot \boldsymbol{a} = (p^s a_1, p^s a_2, \ldots, p^s a_m)$.
- $\mathfrak{I}$ es *minimal* si todo elemento de $\mathfrak{I}$ se puede expresar como $p^{si} \cdot \boldsymbol{a}$ para algún elemento $\boldsymbol{a} \in \mathfrak{I}$ y algún i.
- El conjunto de conjuntos ciclotomicos minimales: $\{\mathfrak{I}_{\mathbf{a}}\}_{\mathbf{a} \in \mathcal{A}}$. Siendo $\mathcal{A}$ el conjunto de representates más pequeños de $\mathfrak{I}_{\mathbf{a}}$.

Conjuntos Ciclotomicos

- *Conjuntos ciclotomicos*: subconjuntos $\mathfrak{I}$ de $\mathbb{Z}_{T_1} \times \mathbb{Z}_{T_2} \times \cdots \times \mathbb{Z}_{T_m}$ tal que $\mathfrak{I} = \{p^s \cdot \boldsymbol{a} \mid \boldsymbol{a} \in \mathfrak{I}\}$, donde $p^s \cdot \boldsymbol{a} = (p^s a_1, p^s a_2, \ldots, p^s a_m)$.
- $\mathfrak{I}$ es *minimal* si todo elemento de $\mathfrak{I}$ se puede expresar como $p^{si} \cdot \boldsymbol{a}$ para algún elemento $\boldsymbol{a} \in \mathfrak{I}$ y algún i.
- El conjunto de conjuntos ciclotomicos minimales: $\{\mathfrak{I}_{\mathbf{a}}\}_{\mathbf{a} \in \mathcal{A}}$. Siendo $\mathcal{A}$ el conjunto de representates más pequeños de $\mathfrak{I}_{\mathbf{a}}$.
- $i_{\mathbf{a}} := \operatorname{card}(\mathfrak{I}_{\mathbf{a}})$.

Conjuntos Ciclotomicos

- *Conjuntos ciclotomicos*: subconjuntos $\mathfrak{I}$ de $\mathbb{Z}_{T_1} \times \mathbb{Z}_{T_2} \times \cdots \times \mathbb{Z}_{T_m}$ tal que $\mathfrak{I} = \{p^s \cdot \boldsymbol{a} \mid \boldsymbol{a} \in \mathfrak{I}\}$, donde $p^s \cdot \boldsymbol{a} = (p^s a_1, p^s a_2, \ldots, p^s a_m)$.
- $\mathfrak{I}$ es *minimal* si todo elemento de $\mathfrak{I}$ se puede expresar como $p^{si} \cdot \boldsymbol{a}$ para algún elemento $\boldsymbol{a} \in \mathfrak{I}$ y algún i.
- El conjunto de conjuntos ciclotomicos minimales: $\{\mathfrak{I}_{\mathbf{a}}\}_{\mathbf{a} \in \mathcal{A}}$. Siendo $\mathcal{A}$ el conjunto de representates más pequeños de $\mathfrak{I}_{\mathbf{a}}$.
- $i_{\mathbf{a}} := \operatorname{card}(\mathfrak{I}_{\mathbf{a}})$.

Sean $p = 2, r = 4, s = 1$.

$$I_0 = \{0\}, I_1\{1, 2, 4, 8\}, I_3 = \{3, 6, 9, 12\}, I_5 = \{5, 10\}, I_7 = \{7, 11, 13, 14\}.$$

$$\mathcal{A} = \{0, 1, 3, 5, 7\}.$$

Subfield-Subcode

Sea Δ un subconjunto de $\mathcal{H}_J$

$$C_\Delta^J = E_\Delta^J \cap \mathbb{F}_{p^s}^{n_J} =< ev_J(\mathcal{T}(f)) \mid Sop(\mathcal{T}(f)) \subseteq \Delta > .$$

- La longitud es n_J.
- La dimension es $\sum_{\mathbf{a}\in\mathcal{A}|\mathfrak{I}_\mathbf{a}\subset\Delta} i_\mathbf{a}$.

Subfield-Subcode

Sea Δ un subconjunto de $\mathcal{H}_J$

$$C_\Delta^J = E_\Delta^J \cap \mathbb{F}_{p^s}^{n_J} =< ev_J(\mathcal{T}(f)) \mid Sop(\mathcal{T}(f)) \subseteq \Delta > .$$

- La longitud es n_J.
- La dimension es $\sum_{\mathbf{a}\in\mathcal{A}|\mathfrak{I}_\mathbf{a}\subset\Delta} i_\mathbf{a}$.

Sean $p = 2, r = 4, s = 1$. $\Delta = I_0 \cup I_1 = \{0, 1, 2, 4, 8\} \subset \{0 \dots 14\}$.
C_Δ^J está generado por la evaluación de las siguientes trazas:

$$\mathcal{T}(x^0), \mathcal{T}(x^1), \mathcal{T}(\alpha^1 x^1), \mathcal{T}(\alpha^2 x^1), \mathcal{T}(\alpha^3 x^1)$$

Siendo $\alpha \in \mathbb{F}_{16}$ un elemento primitivo.
C_Δ^J tiene paramaetros $[15, 5]_2$.

Para poder hacer códigos LRC suponemos que exitse un subconjunto no vacio de indices $L \subseteq J$ tal que $p^s - 1 \mid N_j - 1$ para todo $j \in L$.

Para poder hacer códigos LRC suponemos que exitse un subconjunto no vacio de indices $L \subseteq J$ tal que $p^s - 1 \mid N_j - 1$ para todo $j \in L$.

Sea $\lambda \in \mathbb{F}_q^*$ y P un punto de $\mathbb{F}_q^{n_J}$. Denotamos por $\lambda \cdot P$ al punto que se obtiene multiplicando por λ las coordenadas de P que se encuentran en las posiciones indicadas por L.

Para poder hacer códigos LRC suponemos que exitse un subconjunto no vacio de indices $L \subseteq J$ tal que $p^s - 1 \mid N_j - 1$ para todo $j \in L$.

Sea $\lambda \in \mathbb{F}_q^*$ y P un punto de $\mathbb{F}_q^{n_J}$. Denotamos por $\lambda \cdot P$ al punto que se obtiene multiplicando por λ las coordenadas de P que se encuentran en las posiciones indicadas por L.

Sean α y η elementos primitivos de $\mathbb{F}_q$ y $\mathbb{F}_{p^s}$ respectivamente. Para $1 \leq j \leq m$ definimos $\gamma_j = \alpha^{\frac{q-1}{N_j-1}} \in \mathbb{F}_q$.

Para poder hacer códigos LRC suponemos que exitse un subconjunto no vacio de indices $L \subseteq J$ tal que $p^s - 1 \mid N_j - 1$ para todo $j \in L$.

Sea $\lambda \in \mathbb{F}_q^*$ y P un punto de $\mathbb{F}_q^{n_J}$. Denotamos por $\lambda \cdot P$ al punto que se obtiene multiplicando por λ las coordenadas de P que se encuentran en las posiciones indicadas por L.

Sean α y η elementos primitivos de $\mathbb{F}_q$ y $\mathbb{F}_{p^s}$ respectivamente. Para $1 \leq j \leq m$ definimos $\gamma_j = \alpha^{\frac{q-1}{N_j-1}} \in \mathbb{F}_q$.

Sean l y n dos enteros no negativos. Si $j \in L$, se tiene que :

$$(\gamma_j^l \eta^n)^{N_j-1} = 1$$

Prueba

$$\left(\gamma_j^l \eta^n\right)^{N_j-1} = \left(\alpha^{\frac{q-1}{N_j-1}}\right)^{l(N_j-1)} \left(\eta^{N_j-1}\right)^n = \left(\alpha^{q-1}\right)^l \left(\eta^{q-1}\right)^{n\frac{N_j-1}{q-1}} = 1.$$

Conjuntos de recuperación

$$R_{t_0} := \{P^L_{n,t_0} = \eta^n \cdot_L P_{t_0} \ : \ 0 \leq n \leq q-2\}.$$

Para todo $\boldsymbol{a} \in \mathcal{A}$ definimos $\sigma_L(\boldsymbol{a}) = \sum_{j \in L} a_j \in \mathbb{Z}$.

Conjuntos de recuperación

$$R_{t_0} := \{P^L_{n,t_0} = \eta^n \cdot_L P_{t_0} \ : \ 0 \leq n \leq q-2\}.$$

Para todo $\boldsymbol{a} \in \mathcal{A}$ definimos $\sigma_L(\boldsymbol{a}) = \sum_{j \in L} a_j \in \mathbb{Z}$.

Teorema

Sea $\boldsymbol{a} \in \mathcal{A}$ y sean k y n dos enteros tal que $0 \leq k \leq i_{\boldsymbol{a}} - 1$ y $0 \leq n \leq q-1$. Entonces,

$$\mathcal{T}_{\boldsymbol{a}}(\xi^k_{\boldsymbol{a}} X^{\boldsymbol{a}}) \left(P^L_{n,t_0}\right) = \eta^{n\sigma_L(\boldsymbol{a})} \mathcal{T}_{\boldsymbol{a}}(\xi^k_{\boldsymbol{a}} X^{\boldsymbol{a}}) \left(P_{t_0}\right).$$

Conjuntos de recuperación

$$R_{t_0} := \{P^L_{n,t_0} = \eta^n \cdot_L P_{t_0} \ : \ 0 \leq n \leq q-2\}.$$

Para todo $\boldsymbol{a} \in \mathcal{A}$ definimos $\sigma_L(\boldsymbol{a}) = \sum_{j \in L} a_j \in \mathbb{Z}$.

Teorema

Sea $\boldsymbol{a} \in \mathcal{A}$ y sean k y n dos enteros tal que $0 \leq k \leq i_{\boldsymbol{a}} - 1$ y $0 \leq n \leq q-1$. Entonces,

$$\mathcal{T}_{\boldsymbol{a}}(\xi^k_{\boldsymbol{a}} X^{\boldsymbol{a}}) \left(P^L_{n,t_0}\right) = \eta^{n\sigma_L(\boldsymbol{a})} \mathcal{T}_{\boldsymbol{a}}(\xi^k_{\boldsymbol{a}} X^{\boldsymbol{a}}) \left(P_{t_0}\right).$$

$\mathbb{F}_4 \subset \mathbb{F}_{16}$, luego $\eta = \alpha^5$ siendo $\alpha^{15} = 1$.
$2^2 - 1 \mid N - 1 = 15 \Rightarrow L = J = \{1\}$.
$\boldsymbol{a} = 1 \in \mathcal{A} = \{0, 1, 2, 3, 5, 6, 7, 10, 11\}$.

$$\mathcal{T}_{\boldsymbol{a}}(X^{\boldsymbol{a}})(\alpha^{7+5}) = \alpha^{12} + \alpha^{48} = \alpha^{12} + \alpha^3 = \alpha^5(\alpha^7 + \alpha^{13}) = \alpha^5 \mathcal{T}_{\boldsymbol{a}}(X^{\boldsymbol{a}})(\alpha^7)$$

Prueba

$$\mathcal{T}_{\boldsymbol{a}}(\xi_{\boldsymbol{a}}^k X^{\boldsymbol{a}})\left(P_{n,t_0}^L\right) = \sum_{t=0}^{i_{\boldsymbol{a}}-1}\left(\xi_{\boldsymbol{a}}^k \prod_{l\in L}(\eta^n \gamma_l^{k_l})^{a_l} \prod_{l\notin L}(\gamma_l^{k_l})^{a_l}\right)^{tp^s}$$

$$= \eta^{n\sigma_L(\boldsymbol{a})} \sum_{t=0}^{i_{\boldsymbol{a}}-1}\left(\xi_{\boldsymbol{a}}^k \prod_{l=1}^{m}(\gamma_l^{k_l})^{a_l}\right)^{tp^s} = \eta^{n\sigma_L(\boldsymbol{a})}\mathcal{T}_{\boldsymbol{a}}(\xi_{\boldsymbol{a}}^k X^{\boldsymbol{a}})\left(P_{t_0}\right)$$

Teorema

Sea $\Delta = \cup_{l=1}^{r} \mathfrak{I}_{\boldsymbol{a}_l}$, donde $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_r\} \subset \mathcal{A}$ with $r \leq p^s - 2$. Si los enteros $\sigma_L(\boldsymbol{a}_1), \sigma_L(\boldsymbol{a}_2), \ldots, \sigma_L(\boldsymbol{a}_r)$ son dos a dos diferentes modulo $q-1$, entonces el subfield-subcode $\mathcal{C}_{\Delta}^{J}$ es un código LRC con localidad $\leq r$.

Teorema

Sea $\Delta = \cup_{l=1}^{r} \mathfrak{I}_{\boldsymbol{a}_l}$, donde $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_r\} \subset \mathcal{A}$ with $r \leq p^s - 2$. Si los enteros $\sigma_L(\boldsymbol{a}_1), \sigma_L(\boldsymbol{a}_2), \ldots, \sigma_L(\boldsymbol{a}_r)$ son dos a dos diferentes modulo $q-1$, entonces el subfield-subcode $\mathcal{C}_\Delta^J$ es un código LRC con localidad $\leq r$.

Proof.

Sea $\boldsymbol{c} = \mathrm{ev}_J(h) \in \mathcal{C}_\Delta^J$. Descomponemos h como

$$h = h_{\boldsymbol{a}_1} + h_{\boldsymbol{a}_2} + \cdots + h_{\boldsymbol{a}_r},$$

donde $h_{\boldsymbol{a}_l}$ es una combinación lineal de polinomios de la forma $\mathcal{T}_{\boldsymbol{a}_l}(\xi_{\boldsymbol{a}_l}^k X^{\boldsymbol{a}_l})$, $0 \leq k \leq i_{\boldsymbol{a}_l} - 1$, y coeficientes en $\mathbb{F}_{p^s}$. Fijado un índice $t_0 \in \{1, 2, \ldots, n\}$. vamos a ver que el conjunto de puntos $R = \{P_{n_i, t_0}^L : i = 1, 2, \ldots, r\}$ correspondiente a r n_i's consecutivos y no nulos, es un conjunto de recuperación de t_0. □

$h\left(P_{t_0}\right)$ es deconocido, consideramos el siguiente sistema de ecuaciones lineales

$$
\begin{aligned}
h\left(\eta^{n_1} \cdot_L P_{t_0}\right) &= \eta^{n_1 \sigma_L(\boldsymbol{a}_1)} h_{\boldsymbol{a}_1}\left(P_{t_0}\right) + \eta^{n_1 \sigma_L(\boldsymbol{a}_2)} h_{\boldsymbol{a}_2}\left(P_{t_0}\right) + \cdots + \eta^{n_1 \sigma_L(\boldsymbol{a}_r)} h_{\boldsymbol{a}_r}\left(P_{t_0}\right), \\
h\left(\eta^{n_2} \cdot_L P_{t_0}\right) &= \eta^{n_2 \sigma_L(\boldsymbol{a}_1)} h_{\boldsymbol{a}_1}\left(P_{t_0}\right) + \eta^{n_2 \sigma_L(\boldsymbol{a}_2)} h_{\boldsymbol{a}_2}\left(P_{t_0}\right) + \cdots + \eta^{n_2 \sigma_L(\boldsymbol{a}_r)} h_{\boldsymbol{a}_r}\left(P_{t_0}\right), \\
&\vdots \\
h\left(\eta^{n_r} \cdot_L P_{t_0}\right) &= \eta^{n_r \sigma_L(\boldsymbol{a}_1)} h_{\boldsymbol{a}_1}\left(P_{t_0}\right) + \eta^{n_r \sigma_L(\boldsymbol{a}_2)} h_{\boldsymbol{a}_2}\left(P_{t_0}\right) + \cdots + \eta^{n_r \sigma_L(\boldsymbol{a}_r)} h_{\boldsymbol{a}_r}\left(P_{t_0}\right).
\end{aligned}
$$

$h(P_{t_0})$ es deconocido, consideramos el siguiente sistema de ecuaciones lineales

$$
\begin{aligned}
h\left(\eta^{n_1} \cdot_L P_{t_0}\right) &= \eta^{n_1 \sigma_L(\boldsymbol{a}_1)} h_{\boldsymbol{a}_1}\left(P_{t_0}\right) + \eta^{n_1 \sigma_L(\boldsymbol{a}_2)} h_{\boldsymbol{a}_2}\left(P_{t_0}\right) + \cdots + \eta^{n_1 \sigma_L(\boldsymbol{a}_r)} h_{\boldsymbol{a}_r}\left(P_{t_0}\right), \\
h\left(\eta^{n_2} \cdot_L P_{t_0}\right) &= \eta^{n_2 \sigma_L(\boldsymbol{a}_1)} h_{\boldsymbol{a}_1}\left(P_{t_0}\right) + \eta^{n_2 \sigma_L(\boldsymbol{a}_2)} h_{\boldsymbol{a}_2}\left(P_{t_0}\right) + \cdots + \eta^{n_2 \sigma_L(\boldsymbol{a}_r)} h_{\boldsymbol{a}_r}\left(P_{t_0}\right), \\
&\vdots \\
h\left(\eta^{n_r} \cdot_L P_{t_0}\right) &= \eta^{n_r \sigma_L(\boldsymbol{a}_1)} h_{\boldsymbol{a}_1}\left(P_{t_0}\right) + \eta^{n_r \sigma_L(\boldsymbol{a}_2)} h_{\boldsymbol{a}_2}\left(P_{t_0}\right) + \cdots + \eta^{n_r \sigma_L(\boldsymbol{a}_r)} h_{\boldsymbol{a}_r}\left(P_{t_0}\right).
\end{aligned}
$$

Escribimos $\eta_i := \eta^{\sigma_L(\boldsymbol{a}_i)}$, $1 \leq i \leq r$. Escrito en forma matricial,

$$
\begin{pmatrix}
\eta_1^{n_1} & \cdots & \eta_r^{n_1} \\
\eta_1^{n_2} & \cdots & \eta_r^{n_2} \\
\vdots & \ddots & \vdots \\
\eta_1^{n_r} & \cdots & \eta_r^{n_r}
\end{pmatrix}
\begin{pmatrix}
h_{\boldsymbol{a}_1}\left(P_{t_0}\right) \\
h_{\boldsymbol{a}_2}\left(P_{t_0}\right) \\
\vdots \\
h_{\boldsymbol{a}_r}\left(P_{t_0}\right)
\end{pmatrix}
=
\begin{pmatrix}
h\left(\eta^{n_1} \cdot_L P_{t_0}\right) \\
h\left(\eta^{n_2} \cdot_L P_{t_0}\right) \\
\vdots \\
h\left(\eta^{n_r} \cdot_L P_{t_0}\right)
\end{pmatrix}.
$$

Es una matriz de Vandermonde, luego no singular, solución única. De los $h_{\boldsymbol{a}_i}(P_{t_0})$, $1 \leq i \leq r$ obtenemos

$$
h(P_{t_0}) = h_{\boldsymbol{a}_1}(P_{t_0}) + h_{\boldsymbol{a}_2}(P_{t_0}) + \cdots + h_{\boldsymbol{a}_r}(P_{t_0}).
$$

Ejemplo

$\mathbb{F}_{2^3} \subset \mathbb{F}_{2^6}$ tomamos $N-1 = 63 = n_J$.
$\alpha^{63} = 1$ y $\eta^7 = 1 \Rightarrow \eta = \alpha^9$
Como $p^s - 2 = 6$ podemos considerar a lo sumo 6 ciclotomic cosets minimals, luego $\Delta = \{0\} \cup \{1, 8\} \cup \{2, 16\} \cup \{3, 14\} \cup \{4, 32\} \cup \{5, 40\}$.
Siendo $\mathcal{A} = \{0, 1, 2, 3, 4, 5\}$.
$c = ev_J(h) = (h(\alpha), \ldots, h(\alpha^{63}))$ siendo $h = h_0 + h_1 + h_2 + h_3 + h_4 + h_5$.
Supongamos que $h(\alpha)$ es desconocido. Usamos los puntos

$$R_{t_0} = R_1 = \{\alpha^{10}, \alpha^{19}, \alpha^{28}, \alpha^{37}, \alpha^{46}, \alpha^{55}\}$$

$$\begin{aligned}
h\left(\alpha^{10}\right) &= \alpha^{9*0} h_0(\alpha) + \alpha^{9*1} h_1(\alpha) + \cdots + \alpha^{9*5} h_5(\alpha), \\
h\left(\alpha^{19}\right) &= \alpha^{18*0} h_0(\alpha) + \alpha^{18*1} h_1(\alpha) + \cdots + \alpha^{18*5} h_5(\alpha), \\
h\left(\alpha^{28}\right) &= \alpha^{27*0} h_0(\alpha) + \alpha^{27*1} h_1(\alpha) + \cdots + \alpha^{27*5} h_5(\alpha), \\
h\left(\alpha^{37}\right) &= \alpha^{36*0} h_0(\alpha) + \alpha^{37*1} h_1(\alpha) + \cdots + \alpha^{36*5} h_5(\alpha), \\
h\left(\alpha^{46}\right) &= \alpha^{45*0} h_0(\alpha) + \alpha^{45*1} h_1(\alpha) + \cdots + \alpha^{45*5} h_5(\alpha), \\
h\left(\alpha^{55}\right) &= \alpha^{54*0} h_0(\alpha) + \alpha^{54*1} h_1(\alpha) + \cdots + \alpha^{54*5} h_5(\alpha).
\end{aligned}$$

Teorema

Supongamos que $J = \{1, \ldots, m\}$. Sea $\Delta = \cup_{l=1}^{r} \mathfrak{I}_{\boldsymbol{a}_l}$, donde $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_r\} \subset \mathcal{A}$ with $r \leq p^s - 2$. Si los enteros $\sigma_L(\boldsymbol{a}_1), \sigma_L(\boldsymbol{a}_2), \ldots, \sigma_L(\boldsymbol{a}_r)$ contiene exactamente $r \leq q - 1$ valores distintos, entonces para cualquier coordenada t_0, R_{t_0} es un conjunto de recuperación para t_0. Luego, $\mathcal{C}_{\Delta}^{J}$ es un código LRC con localidad $(r, q - r)$.

Sean $q = Q = N_1 = 11$ y $N_2 = 3$. Tomamos $J = \{1, 2\}$, luego $n_J = 20$. Consideramos los conjuntos de definicion
$\Delta = \mathfrak{I}_{(0,0)} \cup \mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,0)} \cup \mathfrak{I}_{(2,0)}$; $\Delta_1 = \Delta \cup \mathfrak{I}_{(3,0)}$; $\Delta_2 = \Delta_1 \cup \mathfrak{I}_{(4,0)}$; $\Delta_3 = \Delta_2 \cup \mathfrak{I}_{(5,0)}$; $\Delta_4 = \Delta_3 \cup \mathfrak{I}_{(1,1)} \cup \mathfrak{I}_{(6,0)}$; y $\Delta_5 = \Delta_4 \cup \mathfrak{I}_{(7,1)}$.
Dan lugar a los siguientes códigos.

q	$[n, k, d]$	$d^\perp$	(r, δ)	$D_{\delta-1}$
11	[20,4,10]	4	(3,8)	0
11	[20,5,10]	4	(4,7)	0
11	[20,6,10]	4	(5,6)	0
11	[20,7,10]	4	(6,5)	0
11	[20,9,8]	6	(7,4)	1
11	[20,10,8]	8	(8,3)	1

Table: Codigos LRC sobre $\mathbb{F}_{11}$.