Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas

Un código óptimo aplicado a procesos de identificación

ELLERY GREGORIO CHACUTO LÓPEZ

Trabajo presentado como requisito parcial para optar al título de Magíster en Matemáticas

Director: Prof. Dr. Ismael Gutiérrez García

Barranquilla, Agosto de 2014

Dedicatoria

A Dios por su gran bendición a mi vida, a mi familia por brindarme su apoyo en cada meta que me propongo y a todas y cada una de las personas que han sido parte fundamental en mi proceso de formación profesional.

Agradecimientos

A Dios por darme la oportunidad de cumplir una meta más, de igual manera agradezco a todos los docentes del postgrado en Matemáticas de la Universidad Del Norte por todos sus aportes durante todos estos años. En especial al Dr. Ismael Gutierrez García por su dedicación y ayuda durante todo este proyecto.

Introducción

En general el proceso de identificación de personas en las redes de investigaciones médicas en procesos administrativos y en otras áreas es fundamental para el buen funcionamiento y optimización del servicio brindado ya que una mala identificación puede generar serios problemas. Por ejemplo en la prestación del servicio de salud una mala identificación puede ocasionar errores de medicación, errores de prueba, procedimientos a personas incorrectas, entrega de bebes a familias equivocadas entre otras.

Una de las metas de este trabajo es proponer un modelo de codificación para generar identificadores de personas (PID), los cuales tengan propiedades óptimas para la correción y detección de errores, en particular nuestro código tiene la capacidad de corregir dos errores y de detectar cuatro errores, estó en el caso que sucede alguna falla en el proceso de transmisión de la información, además en el caso que se detecte más de un error en la transmisión podrá determinar que tan confiable fue la transmisión recibida.

El presente trabajo de tesis es en su gran mayoría de caracter monográfico. En ella se presentan varios detalles omitidos en el articulo base de este trabajo [2], los cuales facilitarán a futuros estudiantes una lectura más simple de este tema. Cabe destacar como aporte original al trabajo todo lo presentado en el capítulo tres. En el se establece la construcción de un código con parámetros $[11, 7, 5]$ sobre el cuerpo finito $\mathbb{F}_{2^{10}}$, el cual podría ser usado para la generación de PID, con la ventaja de tener una mejor opción de aplicaciones criptográficas, las cuales no son aplicables en el trabajo citado que inspiro esta tesis.

Índice general

1 Preliminares **2**
- 1.1 Cuerpos finitos . . . 2
  - 1.1.1 Existencia y unicidad de los cuerpos finitos . . . 11
  - 1.1.2 La estructura de un cuerpo finito . . . 13
- 1.2 Códigos lineales . . . 15
  - 1.2.1 Matriz generadora . . . 21
  - 1.2.2 Matriz de control . . . 23
  - 1.2.3 MDS-códigos . . . 26

2 Un código óptimo para generar identificadores **29**
- 2.1 Introducción . . . 29
- 2.2 El servicio de generación de IDs . . . 31
- 2.3 Un código para la generación de IDs . . . 34
  - 2.3.1 La aritmetica del cuerpo finito . . . 34
  - 2.3.2 El código usado y algunas de sus propiedades . . . 35
  - 2.3.3 Control de errores . . . 37
- 2.4 Confiabilidad del código . . . 44
- 2.5 Un ejemplo de un PID válido . . . 51

3 Una extensión del código **56**
- 3.1 Preliminares . . . 56
- 3.2 Una nueva forma de generar IDs . . . 59
- 3.3 La construcción del código . . . 60

Bibliografa **62**

Capítulo 1

Preliminares

1.1 Cuerpos finitos

1.1.1 Definición. Un conjunto no vacío K sobre el cual están definidas dos operaciones binarias $+$ y $\cdot$ (suma y multiplicación respectivamente) se denomina un `cuerpo`, si se verifican

(1) $(K, +)$ es un grupo abeliano.

(2) $(K^\times, \cdot)$ es un grupo abeliano. $(K^\times = K - \{0\})$

(3) **Propiedad distributiva.** $a(b + c) = ab + ac$, para todo $a, b, c \in K$.

Un cuerpo se llama `finito`, si el conjunto subyacente K lo es.

1.1.2 Ejemplos. (a) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos.

(b) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es un cuerpo.

(c) Si p es un número primo, entonces $\mathbb{Z}_p$ es un cuerpo finito.

En lo que sigue L y K denotan siempre dos cuerpos.

1.1.3 Definición. Decimos que L es una `extensión` de K, si existe un monomorfismo $i : K \longrightarrow L$. Usaremos la notación L/K. Es claro que

$$K \cong i(K) \leq L,$$

por lo tanto es usual identificar K con $i(K)$ y escribir $K \subseteq L$.

1.1.4 Ejemplos. Son extensiones de cuerpos: $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

1.1.5 Nota. Si L/K es una extensión de cuerpos, entonces podemos dotar a L de una estructura de espacio vectorial sobre K. En efecto, $(L, +)$ es un grupo abeliano y podemos definir una multiplicación por escalar

$$\cdot : K \times L \longrightarrow L$$

de la siguiente manera:

$$(k, l) \longmapsto kl,$$

para todo $k \in K$ y $l \in L$.

1.1.6 Definición. Sea L/K una extensión de cuerpos. La dimensión de L sobre K se nota con $|L : K|$ y se denomina `el grado` de la extensión. Si $|L : K| \in \mathbb{N}$, entonces decimos que la extensión L/K es `finita`. En caso contrario decimos que la extensión es `infinita`. Las extensiones de grado 2 se denominan `cuadráticas` y las de grado 3 se denominan `cúbicas`.

1.1.7 Ejemplos. (a) $|\mathbb{C} : \mathbb{R}| = 2$, ya que $B = (1, \mathrm{i})$ es una base para $\mathbb{C}$ sobre $\mathbb{R}$.

(b) $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, ya que $B = (1, \sqrt{2})$ es una base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

1.1.8 Teorema. (Fórmula del grado) Sea M un cuerpo con $K \leq M \leq L$. Entonces

$$|L : K| = |L : M|\ |M : K|.$$

Demostración. Sean $B_1 = (v_i \mid i \in I)$ una base para L sobre M y $B_2 = (w_j \mid j \in J)$ una base para M sobre K. Demostramos que

$$B := (w_j v_i \mid j \in J,\ i \in I)$$

es una base para L sobre K. Recordemos que todas las sumas que aparezcan tienen solo un número finito de términos no nulos.
Sea $a \in L$. Entonces

$$a = \sum_{i \in I} a_i v_i, \quad \text{con } a_i \in M,$$

además cada $a_i \in M$ tiene la forma

$$a_i = \sum_{j \in J} k_{ij} w_j, \quad \text{con } k_{ij} \in K.$$

Por lo tanto

$$a = \sum_{i \in I} \sum_{j \in J} k_{ij} w_j v_i.$$

Esto demuestra que B es un sistema de generadores de L sobre K.
Supongamos ahora que

$$\sum_{i \in I} \Big(\sum_{j \in J} k_{ij} w_j \Big) v_i = 0.$$

Entonces, dado que B_1 es una base, para todo $i \in I$ se verifica que

$$\sum_{j \in J} k_{ij} w_j = 0.$$

Dado que B_2 es una base, se tiene entonces que $k_{ij} = 0$, para todo $i \in I$ y para todo $j \in J$. Esto demuestra la independencia lineal de B. □

1.1.9 Definición. Sean L/K una extensión de cuerpos y $a \in L$.

(a) Notamos con $K(a)$ al subcuerpo mas pequeño de L que contiene a $K \cup \{a\}$. $K(a)$ se llama el subcuerpo de L formado a partir de K `por adjunción de` a.

(b) Si $L = K(a)$, entonces decimos que L/K es una extensión `simple`.

1.1.10 Ejemplo. La no existencia de cuerpos intermedios entre $\mathbb{C}$ y $\mathbb{R}$ garantiza que $\mathbb{R}(i) = \mathbb{C}$. En efecto, $\mathbb{R}(i)$ es un subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{R}$. Por lo tanto $\mathbb{C}/\mathbb{R}$ es simple. En general se cumple que $\mathbb{C} = \mathbb{R}(z)$, para todo $z \in \mathbb{C} \setminus \mathbb{R}$. Por lo tanto todo número complejo, no real, es un elemento primitivo.

1.1.11 Definición. Sea L/K una extensión de cuerpos y $a \in L$.

(a) Decimos que a es `algebraico` sobre K, si existe $0 \neq f \in K[x]$ tal que $f(a) = 0$. En caso contrario, es decir, si para todo $0 \neq f \in K[x]$ se verifica que $f(a) \neq 0$, entonces decimos que a es `trascendente` sobre K.

(b) L/K se denomina `algebraica`, si todo elemento de L es algebraico sobre K. En caso, contrario ésta se llama trascendente.

1.1.12 Ejemplos. (a) Todo $a \in K$ es algebraico sobre K, ya que éste es raíz de $f = x - a \in K[x]$.

(*b*) La extensión $\mathbb{C}/\mathbb{R}$ es algebraica, ya que para todo $z = a+b\mathrm{i} \in \mathbb{C}$ se verifica que z es raíz del polinomio

$$f = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x].$$

(*c*) $\sqrt[3]{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, ya que para $f = x^3 - 2 \in \mathbb{Q}[x]$ se cumple que $f(\sqrt[3]{2}) = 0$.

1.1.13 Teorema. Sean L/K una extensión de cuerpos y $a \in L$ algebraico sobre K. Entonces

(*a*) Existe un único polinomio mónico $m_{a,K} \in K[x]$ irreducible sobre K que satisface $m_{a,K}(a) = 0$.

(*b*) Si $f \in K[x]$ satisface $f(a) = 0$, entonces $m_{a,K} \mid f$.

(*c*) Si $f \in K[x]$ es mónico, irreducible y satisface $f(a) = 0$, entonces $f = m_{a,K}$.

Demostración.

(*a*) **Existencia.** Sea $\varphi : K[x] \longrightarrow L$ la función sustitución en a. Entonces

$$\ker(\varphi) = \{f \in K[x] \mid f(a) = 0\}.$$

Dado que a es algebraico sobre K, se tiene que $\ker(\varphi) \neq \emptyset$. Dado que $\ker(\varphi)$ es un ideal de $K[x]$, del primer teorema de isomorfía se sigue que

$$K[x]/\ker(\varphi) \cong \mathrm{Im}(\varphi) \subseteq L.$$

Es claro que $\mathrm{Im}(\varphi)$ no tiene divisores de cero. Por lo tanto $\ker(\varphi)$ es un ideal primo.

Por otro lado, dado que $K[x]$ es una anillo de ideales principales, se verifica que $\ker(\varphi)$ es un ideal principal generado por un elemento primo y por lo tanto irreducible. Esto es, $\ker(\varphi) = (g)$. Si b_n es el coeficiente principal de g, entonces definimos

$$m_{a,K} = \tfrac{1}{b_n} g.$$

Se verifica inmediatamente que $m_{a,K}$ es mónico, irreducible sobre K, que

$$\ker(\varphi) = (g) = (m_{a,K})$$

y además $m_{a,K}(a) = 0$.

Unicidad. Se sigue del hecho que $m_{a,K}$ es mónico.

(*b*) Si $f(a) = 0$, entonces $f \in (m_{a,K})$. En consecuencia $m_{a,K} \mid f$.

(*c*) De (*b*) se sigue que $m_{a,K} \mid f$. Por lo tanto existe $g \in K[x]$ tal que $f = m_{a,K} \cdot g$. De la irreducibilidad de f se sigue que $g \in K$. Finalmente, dado que f es mónico, se sigue que $g = 1$. □

1.1.14 Definición. Sean L/K una extensión de cuerpos y $a \in L$ algebraico sobre K. El polinomio $m_{a,K} \in K[x]$ garantizado por el teorema anterior se denomina el `polinomio minimal` de a sobre K. Si en el contexto no hay lugar a confusión, escribimos m_a en lugar de $m_{a,K}$.

1.1.15 Ejemplos. (*a*) Para todo $a \in K$ se verifica que $m_{a,K} = x - a$.

(*b*) Sea $a = \mathrm{i} \in \mathbb{C}$. Entonces $m_{a,\mathbb{Q}} \in \mathbb{Q}[x]$ está dado por $m_{a,\mathbb{Q}} = x^2 + 1$.

(*c*) Sea $a = \sqrt{2} \in \mathbb{R}$. Entonces $m_{a,\mathbb{Q}} \in \mathbb{Q}[x]$ está dado por $m_{a,\mathbb{Q}} = x^2 - 2$.

(*d*) Sea $a = \sqrt[3]{2} \in \mathbb{R}$. Entonces $m_{a,\mathbb{Q}} = x^3 - 2 \in \mathbb{Q}[x]$.

(*e*) Sea $a = \sqrt{2} + \sqrt{3} \in \mathbb{R}$. Entonces $m_{a,\mathbb{Q}} = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$.

En el siguiente teorema examinamos la estructura de la extensión simple $K(a)/K$, con a un elemento de una extensión L de K.

1.1.16 Teorema. Sean L/K una extensión de cuerpos y $a \in L$.

(*a*) Si a es algebraico sobre K, entonces $K(a) \cong K[x]/(m_a)$.

(*b*) Si a es algebraico sobre K y $n = \mathrm{grad}(m_a)$, entonces

$$B = (1, a, \ldots, a^{n-1})$$

es una base para $K(a)$ sobre K. En particular

$$|K(a) : K| = \mathrm{grad}(m_a).$$

Demostración.

(*a*) Sea $\varphi : K[x] \longrightarrow L$ el homomorfismo de sustitución. Note que

$$\ker(\varphi) = \{f \mid f \in K[x],\ f(a) = 0\} = (m_a).$$

Usando el primer teorema de isomorfía se tiene que

$$K[x]/(m_a) = K[x]/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

Dado que m_a es irreducible y $K[x]$ es una anillo de ideales principales, se verifica que (m_a) es un ideal maximal de $K[x]$ y por lo tanto $K[x]/(m_a)$ es un cuerpo. En consecuencia $\mathrm{Im}(\varphi)$ es un cuerpo.

Es claro que $K \cup \{a\} \subseteq \mathrm{Im}(\varphi)$. Por lo tanto $K(a) \subseteq \mathrm{Im}(\varphi)$. Dado que la otra contenencia es inmediata, se sigue la igualdad.

(b) Sea φ nuevamente el homomorfismos de sustitución. Entonces de la sobreyectividad se sigue que dado $b \in K(a)$ existe $g \in K[x]$ tal que $b = g(a)$. Aplicando el algoritmo de Euclides tenemos que

$$g = m_a q + r, \quad \text{con } \mathrm{grad}(r) < \mathrm{grad}(m_a).$$

Entonces

$$r(a) = g(a) - m_a(a)q(a) = g(a) = b.$$

Esto demuestra que dado $b \in K(a)$ siempre es posible encontrar $g \in K[x]$ con $\mathrm{grad}(g) < \mathrm{grad}(m_a)$ y $g(a) = b$.

Entonces si $g = \sum_{j=0}^{n-1} k_j x^j$, se verifica que

$$b = g(a) = \sum_{j=0}^{n-1} k_j a^j.$$

Por lo tanto $B = (1, a, \ldots, a^{n-1})$ es un sistema de generadores para $K(a)$ sobre K.

Para demostrar la independencia lineal de B, supongamos que $\sum_{j=0}^{n-1} k_j a^j = 0$, con $k_j \in K$ y no todos estos son cero. Si definimos

$$h := \sum_{j=0}^{n-1} k_j x^j,$$

entonces $h(a) = 0$ y se tendría que $m_a \mid h$, lo cual es una contradicción, ya que

$$\mathrm{grad}(m_a) = n > n - 1 \geq \mathrm{grad}(h).$$

□

1.1.17 Nota. Como consecuencia del teorema anterior, si $\mathrm{grad}(m_a) = n$, entonces

$$K(a) = \Big\{ \sum_{j=0}^{n-1} k_j a^j \mid k_j \in K \Big\}. \tag{1.1}$$

1.1.18 Ejemplos. (a) Dado que $m_{i,\mathbb{R}} = x^2 + 1$, se tiene que $|\mathbb{C} : \mathbb{R}| = 2$. Por lo tanto del teorema anterior se verifica que

$$\mathbb{R}(i) = \{g(i) \mid g \in \mathbb{R}[x],\ \text{grad}(g) < 2\} = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}.$$

(b) Sea la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Sabemos que $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$. Por lo tanto $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$ y así

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

(c) Sea la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Sabemos que $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$. Por consiguiente $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ y así

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

El siguiente teorema, conocido en la literatura como teorema de Kronecker resulta de gran importancia para la construcción de cuerpos finitos.

1.1.19 Teorema. Sea $f \in K[x]$ irreducible. Entonces

(a) El anillo $L := K[x]/(f)$ es un cuerpo.

(b) La función $\pi : K \longrightarrow L$ definida por $\pi(a) = a + (f)$ es inyectiva. Es decir, podemos identificar K con $\pi(K)$ y ver a L como una extensión de K.

(c) El polinomio $f \in K[x] \subseteq L[x]$ tiene una raíz en L. Esta raíz está dada por $a := x + (f)$.

(d) $|L : K| = \text{grad}(f)$.

Demostración.

(a) Es conocido que de la irreducibilidad de f se sigue que (f) es un ideal maximal de $K[x]$. Por lo tanto L es un cuerpo.

(b) Es claro que π es un homomorfismo. Para demostrar la inyectividad, sean $a, b \in K$. Entonces

$$\pi(a) = \pi(b) \Leftrightarrow a + (f) = b + (f) \Leftrightarrow a - b \in (f).$$

Dado que $\text{grad}(f) \geq 1$ y $a - b \in K$, solo queda libre la opción $a - b = 0$. Es decir, $a = b$.

(c) Sea $f = \sum_{j=0}^{n} a_j x^j$. Entonces

$$f(a) = \sum_{j=0}^{n} a_j (x^j + (f)) = \sum_{j=0}^{n} a_j x^j + (f) = f + (f) = 0.$$

(d) Sea $g + (f) \in L$ cualquiera, con $g = \sum_{j=0}^{m} a_j x^j$. Dado que

$$g + (f) = \sum_{j=0}^{m} a_j x^j + (f) = \sum_{j=0}^{m} a_j (x + (f))^j = \sum_{j=0}^{m} a_j a^j \in K(a),$$

se sigue que $L = K(a)$. Usando el teorema 1.1.16(b) se tiene que

$$|L : K| = |K(a) : K| = \text{grad}(m_{a,K}) = \text{grad}(f),$$

con lo cual se tiene la afirmación. □

El teorema anterior establece la existencia de un cuerpo K con p^m elementos, sobre la base de la existencia de un polinomio $f \in \mathbb{Z}_p[x]$ irreducible con grado m.

1.1.20 Ejemplo. Existe un único polinomio irreducible de grado 2 sobre $\mathbb{Z}_2$ y está dado por

$$f = x^2 + x + 1.$$

Del teorema anterior se sigue quee $K := \mathbb{Z}_2[x]/(f)$ es un cuerpo con 4 elementos. Esto es,

$$K = \{0 + (f), 1 + (f), x + (f), x + 1 + (f)\}.$$

Si definimos $w := x + (f)$, entonces

$$\begin{aligned} w^1 &= w \\ w^2 &= 1 + w \\ w^3 &= 1. \end{aligned}$$

Note que

$$\begin{aligned} w^1 &= 0 \cdot 1 + 1 \cdot w \\ w^2 &= 1 \cdot 1 + 1 \cdot w \\ w^3 &= 1 \cdot 1 + 0 \cdot w. \end{aligned}$$

En consecuencia

$$K = \{0, 1, w, w^2\}.$$

Las tablas se las operaciones están dadas por

$+$	0	1	w	w^2
0	0	1	w	w^2
1	1	0	w^2	w
w	w	w^2	0	1
w^2	w^2	w	1	0

$\cdot$	0	1	w	w^2
0	0	0	0	0
1	0	1	w	w^2
w	0	w	w^2	1
w^2	0	b	1	w

Además se verifica que

$$f(w) = w^2 + w + 1 = w + 1 + w + 1 = 0.$$

Es decir, w es una raíz de f en K. Note que $B = (1, w)$ es una base para K sobre $\mathbb{Z}_2$. Por lo tanto K es una extensión de $\mathbb{Z}_2$ de grado 2.

1.1.21 Ejemplo. Existen dos polinomios irreducibles de grado 3 sobre $\mathbb{Z}_2$. Estos son $f = x^3 + x + 1$ y $g = x^3 + x^2 + 1$. Del teorema anterior se sigue que $K := \mathbb{Z}_2[x]/(f)$ es un cuerpo con 8 elementos. Si definimos nuevamente $w := x + (f)$, entonces se tiene que

$$\begin{aligned}
w^1 &= w \\
w^2 &= w^2 \\
w^3 &= 1 + w \\
w^4 &= w + w^2 \\
w^5 &= 1 + w + w^2 \\
w^6 &= 1 + w^2 \\
w^7 &= 1.
\end{aligned}$$

Note que

$$\begin{aligned}
w^1 &= 0 \cdot 1 + 1 \cdot w + 0 \cdot w^2 \\
w^2 &= 0 \cdot 1 + 0 \cdot w + 1 \cdot w^2 \\
w^3 &= 1 \cdot 1 + 1 \cdot w + 0 \cdot w^2 \\
w^4 &= 0 \cdot 1 + 1 \cdot w + 1 \cdot w^2 \\
w^5 &= 1 \cdot 1 + 1 \cdot w + 1 \cdot w^2 \\
w^6 &= 1 \cdot 1 + 0 \cdot w + 1 \cdot w^2 \\
w^7 &= 1 \cdot 1 + 0 \cdot w + 0 \cdot w^2.
\end{aligned}$$

En consecuencia

$$K = \{0, 1, w, w^2, w^3, w^4, w^5, w^6\}.$$

Además se verifica que

$$f(w) = w^3 + w + 1 = w + 1 + w + 1 = 0.$$

Es decir, w es una raíz de f en K. Como en el ejemplo anterior, note que $B = (1, w, w^2)$ es una base para K sobre $\mathbb{Z}_2$. Por lo tanto K es una extensión de $\mathbb{Z}_2$ de grado 3.

1.1.1 Existencia y unicidad de los cuerpos finitos

1.1.22 Definición. Sean K un cuerpo y $f \in K[x]$ no constante. Una extensión L de K se denomina `cuerpo de descomposición` de f sobre K, si se verifican:

(a) f se descompone totalmente en $L[x]$. Es decir, existen $a, a_1, \ldots, a_n \in L$ tales que

$$f = a(x - a_1) \cdots (x - a_n).$$

(b) Si M es un cuerpo intermedio no trivial de L/K, entonces f no se descompone totalmente en $M[x]$.

Note que (b) es equivalente a:

(b)′ $L = K(a_1, \ldots, a_n)$, donde $a_1, \ldots, a_n \in L$ y son raíces de f.

De la definición se sigue que el cuerpo de descomposición de un polinomio f es el cuerpo más pequeño sobre el cual f se descompone totalmente. Además, dado que L/K es finitamente generada por elementos algebraicos, por lo tanto L/K es una extensión algebraica.

1.1.23 Teorema. (Existencia de cuerpos de descomposición) Todo polinomio no constante $f \in K[x]$ tiene un cuerpo de descomposición L sobre K.

Demostración. Procedemos por inducción sobre el grado de f. Esto significa que el procedimiento consiste en construir el cuerpo L extendiendo a K mediante adjunción de raíces de f una tras otra.

Paso 1. Si $\text{grad}(f) = 1$, entonces $L = K$ y se tiene el resultado.

Paso 2. Si $\text{grad}(f) > 1$ y $f = (x - a_1)g$ en K, entonces se puede aplicar la hipótesis de inducción a g y encontramos un cuerpo L en el cual g se descompone en factores lineales. Este cuerpo L resulta ser el cuerpo buscado.

Paso 3. Supongamos que $\text{grad}(f) > 1$ y f no tiene factores lineales. Sea g un factor de f, irreducible sobre K. Aplicando la construcción del teorema 1.1.19 se obtiene una extensión de K dada por el cuerpo $L' = K[x]/(g)$, el el cual g tiene la raíz $x + (g)$. Note que ahora f tiene un factor lineal sobre L' y podemos regresar y aplicar el paso 2 a L'.

Continuando de esta manera se agregan raíces de f y se reduce el grado del polinomio hasta descomponerlo completamente. □

1.1.24 Teorema. Para toda potencia de un número primo $q = p^n$ existe salvo isomorfía un único cuerpo $\mathbb{F}_q$ con q elementos.

Demostración.

`Existencia.` Sean $f = x^q - x \in \mathbb{Z}_p[x]$ y K el cuerpo de descomposición de f. Sea además $A \subseteq K$ el conjunto de las raíces de f. Es decir,

$$A = \{a \in K \mid a^q = a\}.$$

Demostramos que $A = K$ y que $|K| = q$. Para todo $a \in \mathbb{Z}_p$ se verifica que $a^p = a$. Por lo tanto

$$a^q = a^{p^n} = a^p = a.$$

Esto es, $\mathbb{Z}_p \subseteq A$.

Sean ahora $a, b \in A$ cualesquiera. Entonces

$$(a-b)^q = (a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b.$$

y si $b \neq 0$

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}.$$

Esto demuestra que A es un subcuerpo de K que contiene a $\mathbb{Z}_p$.Dado que el cuerpo de descomposición de f es el cuerpo mas pequeño que contiene a $\mathbb{Z}_p$ y a todas las raices de f, se sigue que

$$\mathbb{Z}_p(A) = A = K.$$

Demostramos ahora que todo polinomio no constante que aparezca en la descomposición de f tiene multiplicidad 1. En efecto, note que

$$f' = p^n x^{p^n - 1} - 1 = -1.$$

Por lo tanto f no tiene raices múltiples. En consecuencia se tiene que $|A| = |K| = q$.

`Unicidad, salvo isomorfía.` Es conocido que todo cuerpo L con q elementos es cuerpo de descomposición del polinomio $f = x^q - x$ sobre su subcuerpo primo. Dado que los cuerpos primos de K y L son isomorfos, se sigue que L y K también lo son. □

Notación. Para denotar un cuerpo finito K con q elementos, escribimos $\mathbb{F}_q$. Es usual también la notación $\texttt{GF}(q)$.

1.1.25 Ejemplo. $\mathbb{F}_4$ es el cuerpo de descomposición de $f = x^4 - x$. Note que

$$f = x(x^3 - 1) = x(x-1)(x^2 + x + 1) \in \mathbb{Z}_2[x].$$

Los primeros dos factores nos dan las raíces 0 y 1. El polinomio $g = x^2 + x + 1$ es irreducible sobre $\mathbb{Z}_2$ y en consecuencia es el polinomio minimal de sus raíces. Sea $\omega \in \mathbb{F}_4$ una raíz de g. Entonces, dado que $|\mathbb{F}_4 : \mathbb{F}_2| = \text{grad}(g) = 2$ se tiene que

$$\mathbb{F}_4 = \mathbb{Z}_2(\omega) = \{x + y\omega \mid x, y \in \mathbb{Z}_2\} = \{0, 1, \omega, 1 + \omega\}.$$

Note que al ser ω una raíz de g se verifica que $\omega^2 = 1 + a$. Por lo tanto, si definimos $\beta := 1 + \omega$ las tablas de las operaciones en $\mathbb{F}_4$ son

$+$	0	1	ω	β
0	0	1	ω	β
1	1	0	β	ω
ω	ω	β	0	1
β	β	ω	1	0

$\cdot$	0	1	ω	β
0	0	0	0	0
1	0	1	ω	β
ω	0	ω	β	1
β	0	b	1	ω

1.1.2 La estructura de un cuerpo finito

1.1.26 Lema. Sean $m, n \in \mathbb{N}$ y K un cuerpo. Entonces

(*a*) $(x^m - 1) \mid (x^n - 1)$ en $K[x]$ si y solo si $m \mid n$ en $\mathbb{Z}$.

(*b*) $(p^m - 1) \mid (p^n - 1)$ en $\mathbb{Z}$ si y solo si $m \mid n$ en $\mathbb{Z}$.

Demostración.

(*a*) Usando la división con resto se tiene que $n = sm + t$ con $s, t \in \mathbb{N}_0$ y $0 \leq t < m$ y además

$$\begin{aligned} x^n - 1 &= x^{sm+t} - 1 \\ &= x^t(x^{sm} - 1) + (x^t - 1) \\ &= x^t((x^m)^s - 1) + (x^t - 1) \\ &= x^t(x^m - 1)\sum_{j=0}^{s-1} x^{jm} + (x^t - 1). \end{aligned}$$

En consecuencia

$$\begin{aligned} m \mid n &\Leftrightarrow t = 0 \\ &\Leftrightarrow x^t = 1 \\ &\Leftrightarrow (x^m - 1) \mid (x^n - 1). \end{aligned}$$

(b) Similar como (a). □

En el siguiente lema se demuestra que existe una correspondencia entre el retículo de los subcuerpos de $\mathbb{F}_{p^n}$ y el retículo de los divisores del número natural n.

1.1.27 Lema. Sean $m, n \in \mathbb{N}$ y $L \cong \mathbb{F}_{p^n}$. Entonces L admite un subcuerpo $K \cong \mathbb{F}_{p^m}$ si y solo si $m \mid n$ en $\mathbb{Z}$.

Demostración. Supongamos que L admite un subcuerpo $K \cong \mathbb{F}_{p^m}$ y sea $d := |L : K|$. Entonces

$$p^n = |L| = |K|^d = p^{md}.$$

En consecuencia $m \mid n$.

Reciprocamente, supongamos que $m \mid n$ y denotemos con P el cuerpo primo de L. Del lema anterior se sigue que $(p^m - 1) \mid (p^n - 1)$ en $\mathbb{Z}$ y

$$(x^{p^m-1} - 1) \mid (x^{p^n-1} - 1).$$

Note que L es un cuerpo de descomposición de $f := x^{p^n-1} - 1$ sobre P. Por lo tanto L contiene un cuerpo de descomposición K de $f := x^{p^m-1} - 1$ sobre P. Claramente se verifica que $K \cong \mathbb{F}_{p^m}$. □

1.1.28 Ejemplos. (a) Los únicos subcuerpos de $\mathbb{F}_4$ son $\mathbb{F}_2$ que es su subcuerpo primo y $\mathbb{F}_4$.

(b) Los únicos subcuerpos de $\mathbb{F}_8$ son $\mathbb{F}_2$ que es su subcuerpo primo y $\mathbb{F}_8$.

(c) Los únicos subcuerpos de $\mathbb{F}_{16}$ son $\mathbb{F}_2$, $\mathbb{F}_4$ y $\mathbb{F}_{16}$.

(d) Los únicos subcuerpos de $\mathbb{F}_{2^{18}}$ son $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^9}$ y $\mathbb{F}_{2^{18}}$.

1.2 Códigos lineales

1.2.1 Definición. Sea K un alfabeto de q elementos y $n \in \mathbb{N}$. Un subconjunto no vacío C de K^n se denomina un *código de bloque* ó simplemente un código de longitud n sobre el alfabeto K.

En adelante el *alfabeto* considerado es el único, salvo isomorfía, cuerpo finito con q elementos, $\mathbb{F}_q$. Recordemos que para $n \in \mathbb{N}$ notamos con $\mathbb{F}_q^n$ el producto cartesiano de n copias de $\mathbb{F}_q$. Es decir,

$$\mathbb{F}_q^n = \{(a_1, \ldots, a_n) \mid a_j \in \mathbb{F}_q\}.$$

Con las operaciones suma y multiplicacción por escalar por componentes se verifica que $\mathbb{F}_q^n$ es un espacio vectorial sobre $\mathbb{F}_q$.

1.2.2 Definición. Decimos que C es un *código lineal* de longitud n sobre $\mathbb{F}_q$, si C es un subespacio vectorial de $\mathbb{F}_q^n$. Escribiremos para ello $C \leq \mathbb{F}_q^n$. Los elementos de C se denominan *codewords*. Un código definido sobre el cuerpo $\mathbb{F}_2$ es denominado *binario* y un código *ternario* corresponde entonces a uno definido sobre el cuerpo $\mathbb{F}_3$.

Si el canal no trabaja libre de errores, entonces un codeword enviado $(c_1, \ldots, c_n) \in C$ es recibido como el vector $(v_1, \ldots, v_n) \in \mathbb{F}_q^n$. El número de errores ocurridos durante la transmisión está dado por el número de elementos del conjunto

$$\{j \mid c_j \neq v_j,\ j = 1, \ldots, n\}.$$

En la siguiente definición precisamos la noción de distancia entre vectores de $\mathbb{F}_q^n$, para ello definimos una función sobre $\mathbb{F}_q^n$ denominada *distancia de Hamming*.

1.2.3 Definición. Para $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ definimos la *distancia de Hamming* d entre u y v de la siguiente manera

$$\mathrm{d}(u, v) := |\{j \mid u_j \neq v_j,\ j = 1, \ldots, n\}|.$$

1.2.4 Ejemplo. Para $u = (1, 1, 0, 0, 1, 0, 1)$, $v = (0, 1, 1, 1, 0, 0, 1) \in \mathbb{F}_2^7$ se verifica que $\mathrm{d}(u, v) = 4$.

1.2.5 Teorema. La distancia de Hamming d es una métrica sobre $\mathbb{F}_q^n$. Es decir, para todo $u, v, w \in \mathbb{F}_q^n$ se verifican

(*a*) $\mathrm{d}(u, v) \geq 0$ y $\mathrm{d}(u, v) = 0$ si y solo si $u = v$.

(b) $\mathrm{d}(u,v) = \mathrm{d}(v,u)$ (Simetría).

(c) $\mathrm{d}(u,v) \leq \mathrm{d}(u,w) + \mathrm{d}(w,v)$. (Desigualdad triangular).

Además d es invariante bajo traslaciones. Es decir, para todo $u, v, w \in \mathbb{F}_q^n$ se verifica que $\mathrm{d}(u+w, v+w) = \mathrm{d}(u,v)$.

Demostración. La no negatividad y la simetría son inmediatas. Sean $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$. Para la desigualdad triangular note que si $u_j \neq v_j$, entonces $u_j \neq w_j$ o $v_j \neq w_j$. Con lo cual se sigue la afirmación. Por otro lado,

$$\begin{aligned} \mathrm{d}(u,v) &= |\{j \mid u_j \neq v_j,\ j = 1, \ldots, n\}| \\ &= |\{j \mid u_j + w_j \neq v_j + w_j,\ j = 1, \ldots, n\}| \\ &= \mathrm{d}(u+w, v+w), \end{aligned}$$

con lo cua se tiene la afirmación. □
La distancia mínima de un código es un parámetro importante, el cual definimos a continuación.

1.2.6 Definición. Sea $\{0\} \neq C \leq \mathbb{F}_q^n$. Se define la *distancia mínima* de C, notada con $\mathrm{d}(C)$, de la siguiente manera:

$$\mathrm{d}(C) := \min\{\mathrm{d}(c, c') \mid c, c' \in C, c \neq c'\}$$

Si $C = \{0\}$, entonces $\mathrm{d}(C) := 0$.

1.2.7 Definición. Sea $C \leq \mathbb{F}_q^n$.

(a) Si $\dim_{\mathbb{F}_q}(C) = k$ y $\mathrm{d}(C) = d$, entonces decimos que C es un $[n,k,d]$-*código* sobre $\mathbb{F}_q$. Si la distancia mínima no es importante en el contexto, entonces decimos simplemente que C es un $[n,k]$-*código* sobre $\mathbb{F}_q$.

(b) Llamamos a $[n,k,d]$ los *parámetros* de C. También es usual decir que C es un $[n,k,d]_q$-código.

1.2.8 Ejemplos. Códigos binarios y sus parámetros.

(a) Un $[6,1,6]$-código binario

$$C = \{(0,0,0,0,0,0), (1,1,1,1,1,1)\}.$$

(b) Un $[3,3,1]$-código binario

$$\begin{aligned} C =&\{(0,0,0),(0,0,1),(0,1,0),(1,0,0),\\ &(0,1,1),(1,1,0),(1,0,1),(1,1,1)\}. \end{aligned}$$

(c) Un $[4,3,2]$-código binario

$$\begin{aligned} C =&\{(0,0,0,0),(0,0,1,1),(1,0,1,0),(0,1,0,1),\\ &(1,0,0,1),(0,1,1,0),(1,1,0,0),(1,1,1,1)\}. \end{aligned}$$

Similar como en los espacios vectoriales euclidianos se puede definir la noción de esferas o bolas con respecto a la distancia de Hamming.

1.2.9 Definición. Sea $r \in \mathbb{N}_0$. Para $u \in \mathbb{F}_q^n$ definimos

$$B_r(u) := \{v \mid v \in \mathbb{F}_q^n,\ \mathrm{d}(u,v) \leq r\}$$

y se denomina *esfera* o *bola* con centro en u y radio r.

1.2.10 Lema. Si $u \in \mathbb{F}_q^n$ y $r \in \mathbb{N}_0$, entonces

$$|B_r(u)| = \sum_{j=0}^{r} \tbinom{n}{j}(q-1)^j.$$

Es decir, para todo $u \in \mathbb{F}_q^n$ la esfera $B_r(u)$ tiene el mismo número de elementos.

Demostración. Note que para todo $j = 0, 1 \ldots, r$ se verifica que

$$\left|\{v \in \mathbb{F}_q^n \mid \mathrm{d}(u,v) = j\}\right| = \tbinom{n}{j}(q-1)^j.$$

Por lo tanto

$$|B_r(u)| = \sum_{j=0}^{r} \tbinom{n}{j}(q-1)^j.$$

Es decir, el número de elementos de $B_r(u)$ no depende del centro de ésta. □

1.2.11 Ejemplo. Para todo $c \in \mathbb{F}_2^3$ se verifica que

$$|B_1(c)| = \sum_{j=0}^{1} \tbinom{3}{j}(2-1)^j = 1 + \tbinom{3}{1} = 4.$$

Como ilustración tenemos

$$\begin{aligned} B_1(1,1,1) &= \{(1,1,1),(0,1,1),(1,1,0),(1,0,1)\}\\ B_1(1,0,1) &= \{(1,0,1),(0,0,1),(1,1,1),(1,0,0)\}. \end{aligned}$$

1.2.12 Definición. Sea C un código sobre $\mathbb{F}_q$, con distancia mínima d y sea $t \in \mathbb{N}_0$.

(a) C se denomina un código *detector de hasta t errores* o simplemente un código *t-detector*, si y solo si $t \leq d-1$.

(b) C se llama un código *corrector de hasta t errores* o simplemente un código *t-corrector*, si y solo si $t \leq \frac{d-1}{2}$.

1.2.13 Teorema. Sean C un código sobre $\mathbb{F}_q$, con distancia mínima d y $t \in \mathbb{N}_0$.

(a) Si C es un código t-detector, entonces para todo $c \in C$ se verifica que c es el único codeword en $B_t(c)$.

(b) Si C es un código t-corrector, entonces para todo $c, c' \in C$ con $c' \neq c$ se verifica que $B_t(c) \cap B_t(c') = \emptyset$.

Demostración.

(a) Si existiese $c' \in C$ con $c' \in B_t(c)$, entonces

$$d \leq \mathrm{d}(c, c') \leq t \leq d-1,$$

lo cual es una contradicción.

(b) Supongamos que existe $x \in B_t(c) \cap B_t(c')$. Entonces

$$\mathrm{d}(x, c) \leq t \quad \wedge \quad \mathrm{d}(x, c') \leq t.$$

De la desigualdad triangular se sigue que

$$d \leq \mathrm{d}(c, c') \leq \mathrm{d}(c, x) + \mathrm{d}(x, c') \leq 2t \leq d-1,$$

lo cual es una contradiccón. □

1.2.14 Corolario Sean C un código sobre $\mathbb{F}_q$, con distancia mínima d. Entonces

(a) C puede ser usado para detectar hasta $d-1$ errores.

(b) C puede ser usado para corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.

Demostración. Es consecuencia inmediata del teorema anterior. □
En general tenemos entonces la siguiente tabla:

d(C)	errores detectados	errores corregidos
1	0	0
2	1	0
3	2	1
4	3	1
5	4	2
6	5	2
7	6	3
⋮	⋮	⋮

Con ayuda de la función peso, la cual describimos a continuación, se puede determinar la distancia mínima de un código lineal con una simplificación considerable en los cálculos.

1.2.15 Definición. Sea $C \leq \mathbb{F}_q^n$.

(a) Definimos la *función peso* $\mathrm{wt} : \mathbb{F}_q^n \longrightarrow \mathbb{N}_0$ de la siguiente manera: Para $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$

$$\mathrm{wt}(x) := \mathrm{d}(x, 0) = |\{j \mid x_j \neq 0\}|.$$

El número $\mathrm{wt}(x)$ se denomina el *peso* de x.

(b) Si $C \neq \{0\}$, entonces se define el *peso mínimo* de C, notado con $\mathrm{wt}(C)$, de la siguiente manera

$$\mathrm{wt}(C) := \min\{\mathrm{wt}(x) \mid 0 \neq x \in C\}.$$

Para $C = \{0\}$ se define $\mathrm{wt}(C) = 0$.

(c) El *soporte* de $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ se nota y define mediante

$$\mathrm{sop}(x) := \{j \mid x_j \neq 0\}.$$

Para $U \subseteq \mathbb{F}_q^n$ definimos aemás $\mathrm{sop}(U) := \bigcup_{u \in U} \mathrm{sop}(u)$. En particular $\mathrm{wt}(u) = |\mathrm{sop}(u)|$ y $\mathrm{sop}(U) = \{j \mid \exists u = (u_1, \ldots, u_n) \in U, \text{ con } u_j \neq 0\}$.

1.2.16 Teorema. Sea C un código lineal de longitud n sobre $\mathbb{F}_q$. Entonces $\mathrm{d}(C) = \mathrm{wt}(C)$.

Demostración. Supongamos que $C \neq \{0\}$. De la invariancia bajo traslaciones de d se sigue

$$\begin{aligned} \mathrm{d}(C) &= \min\{\mathrm{d}(c,c') \mid c,c' \in C,\ c \neq c'\} \\ &= \min\{\mathrm{d}(c-c',0) \mid c,c' \in C,\ c \neq c'\} \\ &= \min\{\mathrm{d}(x,0) \mid x \in C,\ x \neq 0\} \\ &= \mathrm{wt}(C). \end{aligned}$$

Si $C = \{0\}$, entonces la afirmación es inmediata. □

1.2.17 Ejemplo. Sea $C \leq \mathbb{F}_2^7$ el conjunto solución del sistema homogeneo de ecuaciones lineales $Ax^t = 0$, donde

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \text{y} \quad x = (x_1, \ldots, x_7).$$

Se verifica que

$$\begin{aligned} C &= \{(x_4 + x_6 + x_7, x_4 + x_5 + x_6, x_5 + x_6 + x_7, x_4, x_5, x_6, x_7) \mid x_j \in \mathbb{F}_2\} \\ &= \{av_1 + bv_2 + cv_3 + dv_4 \mid a,b,c,d \in \mathbb{F}_2\}, \end{aligned}$$

donde

$$\begin{aligned} v_1 &= (1,1,0,1,0,0,0) \\ v_2 &= (0,1,1,0,1,0,0) \\ v_3 &= (1,1,1,0,0,1,0) \\ v_4 &= (1,0,1,0,0,0,1). \end{aligned}$$

Se verifica que $B = (v_1, v_2, v_3, v_4)$ es una base para C. Por lo tanto $\dim_{\mathbb{F}_2} C = 4$

y así $|C| = 2^4$. Listamos a continuacíon el resto de los elementos de C.

$$\begin{aligned}
0 &= (0,0,0,0,0,0,0)\\
v_1 + v_2 &= (1,0,1,1,1,0,0)\\
v_1 + v_3 &= (0,0,1,1,0,1,0)\\
v_1 + v_4 &= (0,1,1,1,0,0,1)\\
v_2 + v_3 &= (1,0,0,0,1,1,0)\\
v_2 + v_4 &= (1,1,0,0,1,0,1)\\
v_3 + v_4 &= (0,1,0,0,0,1,1)\\
v_1 + v_2 + v_3 &= (0,1,0,1,1,1,0)\\
v_1 + v_2 + v_4 &= (0,0,0,1,1,0,1)\\
v_1 + v_3 + v_4 &= (1,0,0,1,0,1,1)\\
v_2 + v_3 + v_4 &= (0,0,0,1,1,0,1)\\
v_1 + v_2 + v_3 + v_4 &= (1,1,1,1,1,1,1).
\end{aligned}$$

Examinando los pesos de los vectores se sigue que $\mathrm{d}(C) = \mathrm{wt}(C) = 3$. Entonces C es un $[7,4,3]$-código binario.

1.2.1 Matriz generadora

Notemos con $\mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ al conjunto de todas las matrices con entradas en el cuerpo $\mathbb{F}_q$, que poseen k filas y n columnas. Si $A \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$, entonces notamos con A^t la matriz *transpuesta* de A y con $\mathrm{Rang}(A)$ el *rango* de A. Si f es un vector fila, entonces f^t denotará un vector columna.

1.2.18 Definición. Sea C un $[n,k]$-código sobre $\mathbb{F}_q$ y sean $g_1 = (g_{11}, \ldots, g_{1n})$, $\ldots$, $g_k = (g_{k1}, \ldots, g_{kn}) \in \mathbb{F}_q^n$. Si $B = (g_1, \ldots, g_n)$ es una base para C, entonces diremos que

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$$

es una *matriz generadora* de C.
Si C admite una matriz generadora G en la forma

$$G = (I_k \mid B),$$

entonces esta se denomina matriz generadora en *forma estándar*.

No todo código lineal tiene una matriz generadora en forma estándar. Por ejemplo, considere el código C con matriz generadora

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Demostraremos mas adelante que siempre existe un *código equivalente*, que admite una matriz generadora en forma estándar.

1.2.19 Observación. Si $G \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ es una matriz generadora de un $[n,k]$-código sobre $\mathbb{F}_q$, entonces $\mathrm{Rang}(G) = k$.

1.2.20 Ejemplos. (a) Todo código de repetición de longitud n sobre $\mathbb{F}_q$ tiene matriz generadora

$$G = (1, 1, \ldots, 1).$$

(b) Si C es el código binario de control de paridad de longitud 3, entonces

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

es una matriz generadora para C.

(c) El $[7,4,3]$-código binario presentado en el ejemplo 1.2.17 tiene matriz generadora

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

1.2.21 Lema. Sea C un $[n,k]$-código sobre $\mathbb{F}_q$. Entonces $G \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ es una matriz generadora de C, si y sólo si

$$C = \{uG \mid u \in \mathbb{F}_q^k\}.$$

Demostración. Note inicialmente que, si $u = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ y

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q),$$

entonces

$$uG = \sum_{j=1}^{k} u_j g_j \in \mathbb{F}_q^n. \tag{1.2}$$

Supongamos inicialmente que G es una matriz generadora para C. Dado que cada $g_j \in C$, de (1.2) se sigue que $uG \in C$, para todo $u \in \mathbb{F}_q^k$. Esto demuestra que $\{uG \mid u \in \mathbb{F}_q^k\} \subseteq C$.
Por otro lado, si $c \in C$, entonces existen $c_1, \ldots, c_n \in \mathbb{F}_q$ tales que

$$c = \sum_{j=1}^{k} c_j g_j.$$

En consecuencia de (1.2) se sigue que $c = uG$, con $u = (c_1, \ldots, c_k) \in \mathbb{F}_q^k$. Esto demuestra que $C \subseteq \{uG \mid u \in \mathbb{F}_q^k\}$ y se tiene la afirmación.
Recíprocamente, supongamos que $C = \{uG \mid u \in \mathbb{F}_q^k\}$, con

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q).$$

Sea $B = (e_j \mid j = 1, \ldots, k)$ la base canónica de $\mathbb{F}_q^k$. Entonces para todo $j = 1, \ldots, k$ se verifica que

$$e_j G = g_j$$

y en consecuencia las filas de G pertenecen a C.
Nuevamente de (1.2) y de la hipótesis se sigue que, si $c \in C$, entonces existen $c_1, \ldots, c_n \in \mathbb{F}_q$ tales que $c = \sum_{j=1}^{k} c_j g_j$. Es decir, $C = \langle g_1, \ldots, g_k \rangle$. Dado que $\dim_{\mathbb{F}_q} C = k$, se sigue que $(g_1, \ldots, g_k)$ es una base para C y consecuentemente G es una matriz generadora para C. □

1.2.2 Matriz de control

1.2.22 Definición. Sea C un $[n, k]$-código sobre $\mathbb{F}_q$, con $k < n$. Decimos que $H \in \mathrm{Mat}_{n-k\times n}(\mathbb{F}_q)$ es una *matriz de control* para C, si

$$C = \{u \in \mathbb{F}_q^n \mid Hu^t = 0\}.$$

En el siguiente teorema demostramos que dado un $[n, k]$-código C sobre $\mathbb{F}_q$, siempre existe una matriz de control para C. Además la demostración del teorema suministra un algoritmo para determinar una matriz de control de C, a partir de una matriz generadora de este.

1.2.23 Teorema. Sea C un $[n, k]$-código sobre $\mathbb{F}_q$, con $k < n$. Entonces existe una matriz de control H para C. Además $\mathrm{Rang}(H) = n - k$.

Demostración. Sea

$$G := \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in M_{k\times n}(\mathbb{F}_q)$$

una matriz generadora para C y consideremos el sistema homogeneo de ecuaciones lineales

$$Gx^t = 0. \tag{1.3}$$

Del teorema de la nulidad sabemos que

$$n = \text{Rang}(G) + \eta(G),$$

donde $\eta(G)$ denota la dimensión sobre $\mathbb{F}_q$ del conjunto solución del sistema (1.3). Dado que $\text{Rang}(G) = k$, se tiene que $\eta(G) = n - k$.
Sea $B = (h_1, \ldots, h_{n-k})$, una base para el espacio solución del sistema (1.3). Definamos la matriz $H \in \text{Mat}(n-k \times n, K)$ mediante

$$H := \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}.$$

Entonces para todo $i = 1, \ldots, k$, se verifica que $Hg_i^t = 0$. Por lo tanto, para todo $x \in C$ se tiene que $Hx^t = 0$.
Usando nuevamente el teorema de la nulidad se tiene que

$$n = \text{Rang}(H) + \eta(H).$$

Dado que $\text{Rang}(H) = n - k$, se sigue que $\eta(H) = k$ y en consecuencia, $C = \{x \in \mathbb{F}_q^n \mid Hx^t = 0\}$. □

1.2.24 Ejemplo. Sea C un $[4, 2]$-código binario con matriz generadora

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

El conjunto solución de $Gx^t = 0$ está dado por

$$S = \{(0, x_2, x_3, x_2) \mid x_2, x_3 \in \mathbb{F}_2\}.$$

Por lo tanto una matriz de control para C es

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

1.2.25 Teorema. Si $G = (I_k|A) \in M_{k\times n}(\mathbb{F}_q)$ es una matriz generadora para un $[n, k]$-código C, entonces $H = (-A^t \mid I_{n-k})$ es una matriz de control para C.

Demostración. Note que $H \in M_{(n-k)\times n}(\mathbb{F}_q)$. Por lo tanto solo es necesario demostrar que

$$C = \{c \in \mathbb{F}_q^k \mid Hc^t = 0\}.$$

Del lema 1.2.21 se tiene que

$$C = \{xG \mid x \in \mathbb{F}_q^k\}.$$

Sea $c \in C$. Entonces $c = xG$, para algún $x \in \mathbb{F}_q^k$ y se tiene que

$$\begin{aligned} Hc^t &= H(xG)^t \\ &= HG^t x^t \\ &= (-A^t \mid I_{n-k})(I_k \mid A)^t x^t \\ &= (-A^t \mid I_{n-k})\begin{pmatrix} I_k \\ A^t \end{pmatrix} x^t \\ &= (-A^t I_k + I_{n-k}A^t)x^t \\ &= (-A^t + A^t)x^t \\ &= 0. \end{aligned}$$

Esto demuestra que

$$C \subseteq \{c \in \mathbb{F}_q^n \mid Hc^t = 0\}.$$

Usando el teorema de la nulidad se sigue que

$$n = \text{Rang}(H) + \dim_{\mathbb{F}_q}\{c \in \mathbb{F}_q^n \mid Hc^t = 0\}.$$

Dado que $\text{Rang}(H) = n - k$, se sigue que

$$\dim_{\mathbb{F}_q}\{c \in \mathbb{F}_q^n \mid Hc^t = 0\} = k,$$

y dado que $\dim_{\mathbb{F}_q} C = k$, se tiene la conclusión. □

1.2.26 Ejemplo. Sea C un $[7, 3]$-código binario con matriz generadora

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

La matriz de control de C está dada por

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

En el siguiente teorema demostramos que la matriz de control de un código C puede utilizarse para determinar la distancia mínima de este.

1.2.27 Teorema. Sean C un $[n,k]$-código sobre $\mathbb{F}_q$, con $k > 1$ y $H \in \mathrm{Mat}(n-k \times n, \mathbb{F}_q)$ una matriz de control para C. Las siguientes afirmaciones son equivalentes:

(a) La distancia mínima de C es d.

(b) H tiene un conjunto de d columnas linealmente dependientes y no admite un conjunto de $d-1$ columnas linealmente dependientes.

Demostración. (a) $\Rightarrow$ (b) Supongamos que $\mathrm{d}(C) = d$ y sea $c \in C$ con $\mathrm{wt}(c) = d$. Entonces $Hc^t = 0$ y dado que c tiene d posiciones no nulas, se verifica que existen d columnas de H que son linealmente dependientes. No obstante, note que cualquier $d-1$ columnas de H son linealmente independientes, ya que de lo contrario existiría $0 \neq x \in C$ con $\mathrm{wt}(x) = d-1$, lo cual es una contradicción.
(b) $\Rightarrow$ (a) Sean $s_1, \ldots, s_n$ las columnas de H y $s_{i_1}, \ldots, s_{i_d}$, con $i_j \in \{1, \ldots, n\}$ linealmente dependientes. Entonces existen $c_j \in K$ tales que

$$\sum_{j=1}^{n} c_j s_j = 0,$$

y $c_j \neq 0$ exactamente para $j \in \{i_1, \ldots, i_d\}$. Si definimos $c = (c_1, \ldots, c_n)$, entonces se verifica que $Hc^t = 0$ y $\mathrm{wt}(c) = d$. En consecuencia $c \in C$ y $\mathrm{wt}(C) \leq d$.
Supongamos que existiese $0 \neq x \in C$ con $\mathrm{wt}(x) = m < d$. Entonces se tendría que $Hx^t = 0$, lo cual implicaría la existencia de m columnas de H linealmente dependiente, lo cual es una contradicción. Por lo tanto $\mathrm{wt}(C) = d$ y se tiene la conclusión. □

1.2.3 MDS-códigos

1.2.28 Teorema. (Cota de Singleton) Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$. Entonces

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

O equivalentemente

$$|C| \leq q^{n-d+1}.$$

Demostración. Consideremos la función

$$f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-d+1}$$

definida por

$$f(x_1, \ldots, x_n) := (x_1, \ldots, x_{n-d+1}).$$

Dado que dos codewords distintos tienen distancia por lo menos d, se tiene que la restricción de f a C es inyectiva. En efecto, sean $x, y \in \mathbb{F}_q^n$, digamos $x = (x_1, \ldots, x_n)$ y $y = (y_1, \ldots, y_n)$.
Si $x \neq y$, entonces forzosamente $(x_1, \ldots, x_{n-d+1}) \neq (x'_1, \ldots, x'_{n-d+1})$, ya que de lo contrario se tendría que $\mathrm{d}(x, x') \leq d - 1$, lo cual es contradictorio. Por lo tanto

$$q^k = |C| = |f(C)| \leq |\mathbb{F}_q^{n-d+1}| = q^{n-d+1}.$$

En consecuencia

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

y se tiene que $d \leq n - k + 1$. □

1.2.29 Definición. Decimos que un código C es un *MDS-código*, si C alcanza la cota de Singleton. Es decir, si $|C| = q^{n-d+1}$. O equivalentemente $d = n - k + 1$.

Este nombre se deriva de su sigla en ingles *Maximum Distance Separable*.

1.2.30 Ejemplo. Consideremos el código binario de control de paridad

$$C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\} \subseteq \mathbb{F}_2^4.$$

Entonces $n = 4$, $d = 2$ y $|C| = 8$. Es claro que C alcanza la igualdad en la cota de Singleton. Es decir, existe un MDS-código con parámetros $(4, 8, 2)$.

En la teoría de códigos lineales es de gran importancia conocer la distribución de pesos de los elementos de un código dado. Esta idea se formaliza en la siguiente definición.

1.2.31 Definición. Sean C un código de longitud n sobre $\mathbb{F}_q$. Para $0 \leq j \leq n$, denotamos con A_j el número de codewords con peso j. Esto es,

$$A_j := |\{c \in C \mid \mathrm{wt}(c) = j\}|.$$

Entonces, el polinomio definido por $\sum_{j=0}^{n} A_j x^j \in \mathbb{Z}[x]$ se denomina *enumerador de pesos* de C y el vector $(A_0, A_1, ..., A_n)$ se denomina la *distribución de pesos* de C.

El valor distinto de cero más pequeño de i tal que $A_i > 0$ es la distancia mínima del código. Es decir, $A_i = 0$, para todo $i \in \{1, \ldots, d-1\}$.
La distribución de pesos de un MDS-código es un resultado conocido y que será de gran utilidad en el próximo capítulo. Lo enunciamos a continuación.

1.2.32 Teorema. Sea C un $[n, k, d]$-MDS-código sobre $\mathbb{F}_q$. Entonces la distribución de pesos de C esta dada por $A_0 = 1$, $A_i = 0$, para todo $i \in \{1, \ldots, d-1\}$ y

$$\begin{aligned} A_i &= \tbinom{n}{i} \sum_{j=0}^{i-d} (-1)^j \tbinom{i}{j} (q^{i+1-d-j} - 1) \\ &= \tbinom{n}{i}(q-1) \sum_{j=0}^{i-d} (-1)^j \tbinom{i-1}{j} q^{i-d-j}, \end{aligned}$$

para $d \leq i \leq n$, donde $d = n - k + 1$.

Demostración. Ver teorema 7.4.1 en [25].

1.2.33 Ejemplo. Sea C un $[8, 6, 3]$-código sobre el cuerpo $\mathbb{F}_{2^5}$. Note que C es un MDS-código. Entonces del teorema anterior se sigue que la distribución de pesos de C está dada por

$$\begin{aligned} A_0 &= 1 \\ A_3 &= 1736 \\ A_4 &= 62930 \\ A_5 &= 1565872 \\ A_6 &= 24267544 \\ A_7 &= 214942344 \\ A_8 &= 832901397. \end{aligned}$$

Note efectivamente que

$$\sum_{i=0}^{8} A_i = 1073741824 = |C| = q^{n-d+1}.$$

Capítulo 2

Un código óptimo para generar identificadores

2.1 Introducción

La generación de identificadores (ID) de una persona o de un objeto es una necesidad básica en el tratamiento de datos de identidad, en procesos administrativos, en ecología, en redes de investigación médica, en la atención de salud, en ecología y en muchas otras áreas de investigación, [2], [16], [17].

En la prestación del servicio de salud, por ejemplo, la falta de una correcta identificación de los pacientes sigue dando lugar a errores tales como medicación, errores de transfusión, errores de pruebas, procedimientos a personas equivocadas y la asignación de niños a familias equivocadas.

Según datos de la Comisión conjunta de los Estados unidos de América (JC[1]), la Comisión conjunta Internacional (JCI[2]) y de la Organización Mundial

[1]En ingles **The Joint Commission** es la entidad de salud acreditada más grande de los Estados Unidos que trabaja en la promoción de la calidad y la seguridad. Fundada en 1951, la JC evalúa y acredita a más de 20,000 organizaciones y programas de salud en los Estados Unidos. Es una organización independiente, sin fines de lucro. La JC es el establecimiento de normas más antigua y más grande del país y el organismo de acreditación en la asistencia sanitaria.

[2]En ingles **The internacional Joint Commission** es la división internacional de la JC. Su misión es mejorar la calidad de la atención de la salud a nivel mundial. Durante más de 75 años, la JC se ha dedicado a mejorar la calidad y la seguridad de los servicios de atención en salud en los Estados unidos. Actualmente, la JC es la principal agencia acreditadora de organizaciones de salud en los Estados Unidos. La JCI es la institución más confiable en materia de acreditación internacional.

de la Salud (OMS[3]), en la prestación del servicio de salud, la falta de una correcta identificación de los pacientes sigue dando lugar a errores tales como medicación, errores de transfusión, errores de pruebas, procedimientos a personas equivocadas y la asignación de niños a familias equivocadas.

Entre noviembre 2003 y julio de 2005, la Agencia Nacional para la Seguridad del Paciente del Reino Unido denunció 236 incidentes y algunas pérdidas relacionadas con la falta de pulseras de identificación o pulseras con información incorrecta, [12].

El Centro Nacional para la Seguridad del Paciente del Departamento de Asuntos de Veteranos de los Estados Unidos (VA), citó en más de 100 oportunidades la identificación incorrecta del paciente al hacer análisis de causas fundamentales individuales, entre enero de 2000 y marzo 2003, [6].

Las principales áreas en las que puede producirse una identificación incorrecta del paciente incluyen la administración de medicamentos, flebotomía, transfusiones de sangre e intervenciones quirúrgicas. La tendencia a reducir las horas de trabajo de los miembros de los equipos clínicos conduce a un aumento del número de personas que atienden a cada paciente, en consecuencia se aumenta la probabilidad de problemas de traspaso y de comunicación, [9].

Debido a que la identificación incorrecta de pacientes ha sido determinada como causa fundamental de muchos errores, en el año 2003 la JC ubicó la mejora de la precisión de identificación del paciente en el primer lugar de sus objetivos nacionales para la Seguridad del Paciente, el cual sigue siendo un requisito para la acreditación [8].

Mientras que en algunos países se usan tradicionalmente las pulseras para identificar a los pacientes hospitalizados, las pulseras perdidas y o la información incorrecta limitan la eficacia de este sistema. La codificación por colores facilita el reconocimiento visual rápido de cuestiones específicas, pero la falta de un sistema de codificación estandarizado ha dado lugar a errores por parte del personal que presta atención a los pacientes en varios establecimientos, [13].

Existen nuevas tecnologías que pueden mejorar la identificación del paciente, por ejemplo, los códigos de barras. Algunos de ellos han demostrado ser económicos, [14], [15], [16], [17], [18] y [19]. Independientemente de la tec-

[3]**La Organización Mundial de la Salud** es la autoridad directiva y coordinadora de la acción sanitaria en el sistema de las Naciones Unidas. Es la responsable de desempeñar una función de liderazgo en los asuntos sanitarios mundiales, configurar la agenda de las investigaciones en salud, establecer normas, articular opciones de política basadas en la evidencia, prestar apoyo técnico a los países y vigilar las tendencias sanitarias mundiales. En agosto de 2005, la OMS designó a la JCI como el primer y único centro colaborativo en el mundo dedicado exclusivamente a la seguridad del paciente.

nología o el enfoque utilizado para la identificación de los pacientes con exactitud, la planificación cuidadosa de los procesos de atención asegurará la debida identificación de los pacientes antes de cualquier intervención médica y proporcionará una atención más segura, con considerablemente menos errores.

No obstante la unicidad de la identificación permanece sin una solución definitiva. En esta dirección deseamos orientar nuestro trabajo. Es decir, proponer un modelo de codificación para generar identificadores, de tal forma que estos tengan propiedades óptimas de seguridad además de la detección y corrección de errores, en el sentido de la teoría de la información, y más preciso en el de la codificación matemática, [20], [22], [21], [25].

2.2 El servicio de generación de IDs

Un modelo estándar para el servicio de generación de identificadores personales (PID) o de la utilización de estos reside en un servidor web con una subyacente base de datos, en el cual un cliente llama al servicio a través de una interfaz en la web. En general este servicio consta de dos algoritmos

- Un algoritmo de coincidencia y
- Un algoritmo generador de ID, el cual es uno de los objetivos centrales de esta investigación.

Presentamos en la siguiente figura una ilustración de este procedimiento.

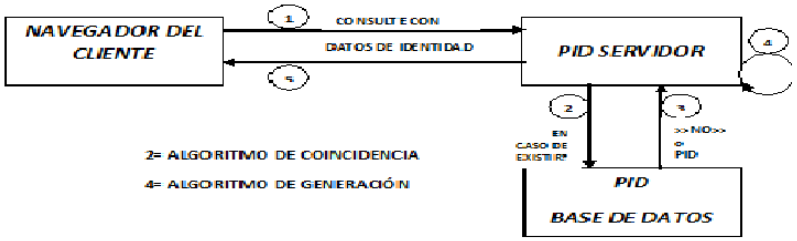

Figura 2.1: Generación o validación de un PID.

Un aspecto importante es que en las redes de atención de pacientes a menudo se hace necesario la asignación de pseudónimos para el manejo de los datos, a fin de mantener su confidencialidad. Técnicamente hablando, los seudónimos

son funciones de una vía [1], [11] y su fortaleza depende de quién posee la clave del cifrado. La creación de pseudónimos sólo tiene sentido, si se posee un procedimiento de identificación confiable antes de cortar la conexión con los datos de identidad y naturalmente la calidad de los los datos debe estar asegurada antes.

Para que un ID pueda ser utilizado de manera razonable y conveniente se desea que éste cumpla con los siguientes requerimientos:

- Constar solamente de letras y números. Es decir, debe ser de tipo alfanumérico.
- Contener uno o más caracteres adicionales para la detección y eventual corrección de errores
- Tener una longitud fija y un número adecuado de caracteres.
- Evitar las inferencias con los correspondientes datos de identidad, ni de tiempo ni de orden de su generación.

La primera parte de este último requisito es realizada mediante un contador simple, para cumplir con la segunda parte el contador es encriptado. Este paso de cifrado puede parecer exagerado, pero se hace prácticamente sin ningún costo extra y por otro lado es útil en ciertas configuraciones o ajustes. además no afecta el procedimiento de codificación dado a continuación, solo el preprocesamiento de la información.

Para cumplir con los requerimientos en la generación de ID se usa un alfabeto alfa-numérico, por ejemplo podría constar de los números $0, \ldots, 9$ y algunas letras del alfabeto castellano. Por ejemplo, del conjunto $\{A, B, C, \ldots, Z\}$ podemos excluir la letras B, I, O, S, las cuales pueden ser confundidas con los caracteres 8, 1, 0 y 5 respectivamente. Usando seis de estos 32 caracteres podríamos representar

$$32^6 = (2^5)^6 = 2^{30} \approx 10^9,$$

aproximadamente mil millones de codewords distintos de longitud seis, eventualmente suficiente para una red de investigación médica.

Para facilitar la realización de cálculos matemáticos se establece una correspondencia entre los 32 caracteres de nuestro alfabeto y el cuerpo finito $\mathbb{F}_{32}$. Para tal procedimiento consideramos el orden lexicográfico. Es decir, hacemos corresponder al 0 la cadena de bits $00000, \ldots$, al 9 le corresponde 01001 , a la A le corresponde 01010 y así hasta la Z, a la cual le corresponde la cadena 11111. En la siguiente tabla se presenta la correspondencia completa.

Enumeración	Caracter	Elemento en $\mathbb{F}_{32}$
0	0	(00000)
1	1	(00001)
2	2	(00010)
3	3	(00011)
4	4	(00100)
5	5	(00101)
6	6	(00110)
7	7	(00111)
8	8	(01000)
9	9	(01001)
10	A	(01010)
11	C	(01011)
12	D	(01100)
13	E	(01101)
14	F	(01110)
15	G	(01111)
16	H	(10000)
17	J	(10001)
18	K	(10010)
19	L	(10011)
20	M	(10100)
21	N	(10101)
22	P	(10110)
23	Q	(10111)
24	R	(11000)
25	T	(11001)
26	U	(11010)
27	V	(11011)
28	W	(11100)
29	X	(11101)
30	Y	(11110)
31	Z	(11111)

Tabla 2.1: Correspondencia Alfabeto - $\mathbb{F}_{32}$.

2.3 Un código para la generación de IDs

El enfoque planteado en la sección anterior deja espacio para 2 caracteres adicionales y propone un código que detecte dos errores y corrija un error, el cual será construido mas adelante y lo llamaremos un $[8, 6, 3]$-MDS-código sobre el cuerpo finito $\mathbb{F}_{32}$.

La idea inicial es que el algoritmo procese una cadena de bits de longitud 30, los cuales escribiremos como vectores con seis componentes sobre el cuerpo $\mathbb{F}_{32}$, y el resultado de todo el procedimiento matemático es una cadena de bits de longitud 40 que se traduce finalmente en una cadena de ocho caracteres.

2.3.1 La aritmetica del cuerpo finito

El polinomio $f = T^5+T^2+1 \in \mathbb{F}_2[T]$ en la indeterminada T sobre el cuerpo binario $\mathbb{F}_2$ es irreducible. Por lo tanto, por el teorema Kronecker 1.1.19, el anillo cociente $\mathbb{F}_2[T]/(f)$ es un cuerpo finito con $2^5 = 32$ elementos. En consecuencia este, salvo isomorfía es el cuerpo $\mathbb{F}_{32}$. Si representamos sus elementos por vectores en $\mathbb{F}_2^5$, esto es, cadenas de bits de longitud cinco, entonces la adición en $\mathbb{F}_{32}$ es la adición de vectores sobre $\mathbb{F}_2$ la cual es la disyunción exclusiva de cadena de bits (XOR).

Si $t \in \mathbb{F}_{32}$ denota la clase residual de T. Es decir, $t = T + (f)$, entonces $\mathbb{F}_{32}$ tiene como base sobre $\mathbb{F}_2$ el sistema

$$(1, t, t^2, t^3, t^4),$$

correspondiente a la base canonica de $\mathbb{F}_2^5$

$$\begin{aligned} e_1 &= (00001) \\ e_2 &= (00010) \\ e_3 &= (00100) \\ e_4 &= (01000) \\ e_5 &= (10000), \end{aligned}$$

en ese orden. La tabla de multiplicación completa se deriva de la siguiente formula:

$$t^5 = t^2 + 1.$$

Para $x = (x_1, x_2, x_3, x_4, x_5)$, se tiene que $x = x_1t^4 + x_2t^3 + x_3t^2 + x_4t + x_5$, en particular los productos con potencias pequeñas de t se ven de la siguiente manera:

$$\begin{aligned} t \cdot x &= t(x_1t^4 + x_2t^3 + x_3t^2 + x_4t + x_5) \\ &= x_1(t^2+1) + x_2t^4 + x_3t^3 + x_4t^2 + x_5t \\ &= x_1t^2 + x_1 + x_2t^4 + x_3t^3 + x_4t^2 + x_5t \\ &= (x_2t^4, x_3t^3, x_1t^2 + x_4t^2, x_5, x_1) \\ &= (x_2, x_3, x_4 + x_1, x_5, x_1). \end{aligned}$$

$$\begin{aligned} t^2 \cdot x &= t^2(x_1t^4 + x_2t^3 + x_3t^2 + x_4t + x_5) \\ &= x_1((t^2+1)t) + x_2t^2 + x_2 + x_3t^4 + x_4t^3 + x_5t^2 \\ &= x_1(t^3 + t) + x_2t^2 + x_2 + x_3t^4 + x_4t^3 + x_5t^2 \\ &= x_1t^3 + x_1t + x_2t^2 + x_2 + x_3t^4 + x_4t^3 + x_5t^2 \\ &= (x_3t^4, x_1t^3 + x_4t^3, x_2t^2 + x_5t^2, x_1t, x_2) \\ &= (x_3, x_1 + x_4, x_2 + x_5, x_1, x_2). \end{aligned}$$

$$\begin{aligned} t^3 \cdot x &= t^3(x_1t^4 + x_2t^3 + x_3t^2 + x_4t + x_5) \\ &= x_1(t^2+1)t^2 + x_2(t^2+1)t + x_3(t^2+1) + x_4t^4 + x_5t^3 \\ &= x_1(t^4 + t^2) + x_2(t^3 + t) + x_3(t^2+1) + x_4t^4 + x_5t^3 \\ &= x_1t^4 + x_1t^2 + x^2t^3 + x_2t + x_3t^2 + x_3 + x_4t^4 + x_5t^3 \\ &= (x_1 + x_4)t^4 + (x_2 + x_5)t^3 + (x_1 + x_3)t^2 + x_2t + x_3 \\ &= (x_1 + x_4, x_2 + x_5, x_1 + x_3, x_2, x_3). \end{aligned}$$

$$\begin{aligned} t^4 \cdot x &= t^4(x_1t^4 + x_2t^3 + x_3t^2 + x_4t + x_5) \\ &= x_1t^5t^3 + x_2t^5t^2 + x_3t^5t + x_4t^5 + x_5t^4 \\ &= x_1(t^2+1)t^3 + x_2(t^2+1)t^2 + x_3(t^2+1)t + x_4(t^2+1) + x_5t^4 \\ &= x_1(t^5 + t^3) + x_2(t^4 + t^2) + x_3(t^3 + t) + x_4(t^2+1) + x_5t^4 \\ &= (x_2 + x_5, x_1 + x_3, x_1 + x_2 + x_4, x_3, x_1 + x_4). \end{aligned}$$

2.3.2 El código usado y algunas de sus propiedades

El proceso de codificación consiste en una transformación lineal

$$\varphi : \mathbb{F}_{32}^6 \longrightarrow \mathbb{F}_{32}^8,$$

definido por la matriz

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & t & t^2 \\ 0 & 1 & 0 & 0 & 0 & 0 & t^2 & t^4 \\ 0 & 0 & 1 & 0 & 0 & 0 & t^3 & t^6 \\ 0 & 0 & 0 & 1 & 0 & 0 & t^4 & t^8 \\ 0 & 0 & 0 & 0 & 1 & 0 & t^5 & t^{10} \\ 0 & 0 & 0 & 0 & 0 & 1 & t^6 & t^{12} \end{pmatrix}.$$

Es decir, esta función φ envía $u = (u_1, u_2, u_3, u_4, u_5, u_6) \in \mathbb{F}_{32}^6$ en

$$\varphi(u) = uG = c = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \in \mathbb{F}_{32}^8.$$

Entonces $u_i = c_i$, para todo $i = 1, \ldots, 6$. Esto es, las primeras seis coordenadas permanecen invariantes en la codificación y los dos últimos símbolos, c_7 y c_8, corresponden a las ecuaciones de control del código, las cuales están dadas por

$$c_7 = tu_1 + t^2u_2 + t^3u_3 + t^4u_4 + t^5u_5 + t^6u_6 \tag{2.1}$$

$$c_8 = t^2u_1 + t^4u_2 + t^6u_3 + t^8u_4 + t^{10}u_5 + t^{12}u_6. \tag{2.2}$$

(a) **La distancia mínina.** Por definición esta corresponde al número mínimo de posiciones en las cuales dos codewords difieren. Demostramos que $d(C) = 3$.

Demostración. Sean c y $c' \in C$ con $c \neq c'$. Dado que C es un espacio vectorial, $c - c' \in C$, y $c - c' \neq 0$. Por lo tanto $c - c'$ es una combinación lineal de las filas de G.

Cada una de las filas de G tienen exactamente tres coordenadas no nulas. Una combinación de dos filas distintas i y j de G tienen exactamente dos posiciones distintas de cero dentro de las seis primeras posiciones. Las dos últimas posiciones de dicha combinación no pueden anularse simultáneamente, ya que de lo contrario

$$at^i + bt^j = 0 = at^{2i} + bt^{2j},$$

con $a, b \neq 0$ implicaría que $t^j = t^i$, lo cual no es posible ya que $i \neq j$. Una combinación de tres o mas filas de G resulta en tres o mas coordenadas diferentes de cero en las seis primeras posiciones. En cualquier caso el número de coordenadas diferentes de cero es mayor que dos y por lo tanto, c y c' difieren en al menos tres posiciones. □

(b) **La capacidad para la detección.** Si en un codeword enviado se adulteran dos bits, es decir se presentan dos errores, entonces estos se pueden detectar.

Demostración. Es consecuencia inmediata del corolario 1.2.14 (a). □

(c) **La capacidad para la corrección.** Si en un codeword enviado se adultera un bit, es decir se presenta un error, entonces este se puede corregir de forma automática.

Demostración. Es consecuencia inmediata del corolario 1.2.14 (b). □

(d) **La calidad del código.** C es un MDS-código. En consecuencia un código óptimo para la corrección y detección de errores.

Demostración. Esta afirmación se sigue del teorema de la cota de Singleton, la cual restringe la distancia mínima d por la redundancia de un código $d \leq n - k + 1$. La distancia mínima d no puede ser mayor que tres. □

(e) **La matriz de control de paridad.** Sea $c \in \mathbb{F}_{32}^8$. Entonces $c \in C$ si y solo si $Hc^t = 0$, donde H es la matriz de control de paridad del código C y está dada por

$$H = \begin{pmatrix} t & t^2 & t^3 & t^4 & t^5 & t^6 & 1 & 0 \\ t^2 & t^4 & t^6 & t^8 & t^{10} & t^{12} & 0 & 1 \end{pmatrix}. \tag{2.3}$$

Demostración. Se sigue del teorema 1.2.25. □

2.3.3 Control de errores

Supongamos que un codeword $c = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \in C$ es enviado y que en el proceso de transmisión pudieron haber ocurrido errores en los datos de entrada, por lo que el vector recibido $y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{F}_{32}^8$ podría no ser el codeword original c. Entonces una pregunta válida es: ¿Cual es el valor mas probable para c?

Resolvemos este interrogante en el siguiente teorema.

2.3.1 Teorema. (Algoritmo de decodificación-correción)
Consideremos el producto matricial

$$\begin{aligned} Hy^t &= \begin{pmatrix} t & t^2 & t^3 & t^4 & t^5 & t^6 & 1 & 0 \\ t^2 & t^4 & t^6 & t^8 & t^{10} & t^{12} & 0 & 1 \end{pmatrix} (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)^t \\ &= \begin{pmatrix} y_1 t + y_2 t^2 + y_3 t^3 + y_4 t^4 + y_5 t^5 + y_6 t^6 + y_7 \\ y_1 t^2 + y_2 t^4 + y_3 t^6 + y_4 t^8 + y_5 t^{10} + y_6 t^{12} + y_8 \end{pmatrix} \\ &=: \begin{pmatrix} a \\ b \end{pmatrix}. \end{aligned}$$

Entonces el siguiente algoritmo de decodificación produce un codeword válido $\widehat{y}$ en los siguientes siete casos:

(1) Si $a = 0 = b$, entonces $y \in C$ es un codeword válido. Entonces $\widehat{y} := y$.

(2) Si $a \neq 0 = b$, entonces se reemplaza y_7 por $y_7 + a$, por lo tanto

$$\widehat{y} = (y_1, y_2, y_3, y_4, y_5, y_6, y_7 + a, y_8).$$

(3) Si $b \neq 0 = a$, entonces reemplazaremos c_8 por $c_8 + b$, por lo tanto

$$\widehat{y} = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8 + b).$$

(4) Si $a \neq 0$ y $\dfrac{b}{a} = t^i$ con algún $i = 1, \ldots, 6$, entonces reemplazaremos y_i por $y_i + \dfrac{a}{t^i}$, por lo tanto

$$\widehat{y} = \big(y_1, \ldots, y_i + \frac{a}{t^i}, \ldots, y_8\big).$$

(5) Si $0 \neq a = (y_i + y_{i+1})t^{18+i}$ y $\dfrac{b}{a} = t^{18+i}$ con algún $i = 1, \ldots, 5$, entonces transponemos las coordenadas de las posiciones i e $i + 1$, por lo tanto

$$\widehat{y} = (y_1, \ldots, y_{i+1}, y_i, \ldots, y_8).$$

(6) Si $0 \neq a = (y_6 + y_7)(t^6 + 1)$ y $\dfrac{b}{a} = t^{16}$, entonces transponemos las coordenadas de las posiciones 6 y 7, por lo tanto

$$\widehat{y} = (y_1, \ldots, y_5, y_7, y_6, y_8).$$

(7) Si $0 \neq a = b = y_7 + y_8$, entonces transponemos las coordenadas de las posiciones 7 y 8, por lo tanto

$$\widehat{y} = (y_1, \ldots, y_6, y_8, y_7).$$

Demostración. Para demostrar que $\widehat{y} \in C$, usamos la matriz de control de paridad. del código. Recordemos que si $c \in \mathbb{F}_{32}^8$, entonces $c \in C$ si y solo si $H\widehat{y}^t = 0$, donde H que denota la matriz de control de paridad del código C. Es importante no perder de vista que la característica del cuerpo $\mathbb{F}_{32}^8$ es 2. En consecuencia $2a = 0$, por lo tanto

$$(a + b)^2 = a^2 + b^2,$$

para todos $a, b \in \mathbb{F}_{32}$.

(1) Sea $a = 0 = b$. Entonces y es un codeword válido y no debe ser cambiado. Por lo tanto $\widehat{y} := y$.

(2) Si $a \neq 0 = b$ en este caso reemplazaremos y_7 por $y_7 + a$, veamos en detalle.

$$\begin{aligned} H\widehat{y}^t &= \begin{pmatrix} y_1t + y_2t^2 + y_3t^3 + y_4t^4 + y_5t^5 + y_6t^6 + y_7 + a \\ y_1t^2 + y_2t^4 + y_3t^6 + y_4t^8 + y_5t^{10} + y_6t^{12} + y_8 \end{pmatrix} \\ &= \begin{pmatrix} y_1t + y_2t^2 + y_3t^3 + y_4t^4 + y_5t^5 + y_6t^6 + y_7 \\ y_1t^2 + y_2t^4 + y_3t^6 + y_4t^8 + y_5t^{10} + y_6t^{12} + y_8 \end{pmatrix} + \begin{pmatrix} a \\ 0 \end{pmatrix} \\ &= Hy^t + H(0, \ldots, 0, a, 0)^t \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 2a \\ b \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \end{aligned}$$

Por lo tanto es un codeword válido.

(3) Si $b \neq 0 = a$, en este caso reemplazaremos y_8 por $y_8 + b$, veamos en detalle.

$$\begin{aligned} H\widehat{y}^t &= \begin{pmatrix} y_1t + y_2t^2 + y_3t^3 + y_4t^4 + y_5t^5 + y_6t^6 + y_7 \\ y_1t^2 + y_2t^4 + y_3t^6 + y_4t^8 + y_5t^{10} + y_6t^{12} + y_8 + b \end{pmatrix} \\ &= \begin{pmatrix} y_1t + y_2t^2 + y_3t^3 + y_4t^4 + y_5t^5 + y_6t^6 + y_7 \\ y_1t^2 + y_2t^4 + y_3t^6 + y_4t^8 + y_5t^{10} + y_6t^{12} + y_8 \end{pmatrix} + \begin{pmatrix} 0 \\ b \end{pmatrix} \\ &= Hy^t + H(0, \ldots, 0, 0, b)^t \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 0 \\ b \end{pmatrix} \\ &= \begin{pmatrix} a \\ 2b \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \end{aligned}$$

Por lo tanto es un codeword válido.

(4) Si $a \neq 0$ y $\dfrac{b}{a} = t^i$ con algún $i = 1, \ldots, 6$, entonces reemplazaremos y_i por $y_i + \dfrac{a}{t^i}$. En efecto,

$$\begin{aligned} H\widehat{y}^t &= Hy^t + H(0,\ldots,\frac{a}{t^i},\ldots,0)^t \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a \\ at^i \end{pmatrix} \\ &= \begin{pmatrix} 2a \\ 2b \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \end{aligned}$$

(5) Si $0 \neq a = (y_i + y_{i+1})t^{18+i}$ y $\dfrac{b}{a} = t^{18+i}$ con algún $i = 1,\ldots,5$, entonces transponemos las coordenadas de las posiciones i e $i+1$. Note que

$$\begin{aligned} H\widehat{y}^t &= Hy^t + H(0,\ldots,y_i + y_{i+1}, y_i + y_{i+1},\ldots,0)^t \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} (y_i + y_{i+1})t^i + (y_i + y_{i+1})t^{i+1} \\ (y_i + y_{i+1})t^{2i} + (y_i + y_{i+1})t^{2i+2} \end{pmatrix} \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} (y_i + y_{i+1})(t^i + t^{i+1}) \\ (y_i + y_{i+1})(t^{2i} + t^{2i+2}) \end{pmatrix} \qquad (2.4) \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} (y_i + y_{i+1})t^{18+i} \\ (y_i + y_{i+1})(t^{18+i})^2 \end{pmatrix} \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} (y_i + y_{i+1})t^{18+i} \\ (y_i + y_{i+1})(t^{18+i})^2 \end{pmatrix} \\ &= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \begin{pmatrix} 2a \\ 2b \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \end{aligned}$$

En (2.4) afirmamos que $t^i + t^{i+1} = t^{18+i}$ y $t^{2i} + t^{2i+2} = (t^{18+i})^2$. Procedemos a justificarlas. Tenga en cuenta que $t^5 = t^2 + 1$.

$$\begin{aligned}
t^{18+i} &= (t^5)^3 \cdot t^3 \cdot t^i \\
&= (t^2+1)^3 \cdot t^3 \cdot t^i \\
&= (t^6 + 3t^4 + 3t^2 + 1) \cdot t^3 \cdot t^i \\
&= ((t^2+1) \cdot t + 3t^4 + 3t^2 + 1) \cdot t^3 \cdot t^i \\
&= (t^6 + t^4 + 3t^7 + 3t^5 + t^3) \cdot t^i \\
&= ((t^2+1)t + t^4 + 3t^2(t^2+1) + 3(t^2+1) + t^3) \cdot t^i \\
&= (2t^3 + 4t^4 + 6t^2 + t + 3) \cdot t^i \\
&= (t+1) \cdot t^i \\
&= t^{i+1} + t^i.
\end{aligned}$$

Además

$$t^{2i} + t^{2i+2} = t^{2i} + \underbrace{2t^i t^{i+1}}_{0} + t^{2i+2} = (t^i + t^{i+1})^2 = (t^{18+i})^2.$$

(6) Si $0 \neq a = (y_6 + y_7)(t^6+1)$ y $\dfrac{b}{a} = t^{16}$, entonces transponemos las coordenadas de las posiciones 6 y 7. Note que

$$\begin{aligned}
H\widehat{y}^t &= Hy^t + H(0, \ldots, y_6 + y_7, y_6 + y_7, 0)^t \\
&= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} (y_6+y_7)t^6 + y_6 + y_7 \\ (y_6+y_7)t^{12} \end{pmatrix} \\
&= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} \underbrace{(y_6+y_7)(t^6+1)}_{a} \\ (y_6+y_7)t^{12} \end{pmatrix} \qquad (2.5) \\
&= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a \\ \underbrace{(y_6+y_7)(t^6+1)}_{a}\, t^{16} \end{pmatrix} \\
&= \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix} \\
&= \begin{pmatrix} 2a \\ 2b \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 0 \end{pmatrix}.
\end{aligned}$$

En (2.5) afirmamos que $(y_6+y_7)t^{12} = (y_6+y_7)(t^6+1)\cdot t^{16}$. Es suficiente entonces demostrar que $(t^6+1)t^4 = 1$. En efecto,

$$\begin{aligned}(t^6+1)t^4 &= t^{10}+t^4\\ &= (t^2+1)^2+t^4\\ &= t^4+2t^2+1+t^4\\ &= 2t^4+2t^2+1\\ &= 1.\end{aligned}$$

(7) Si $0 \neq a = b = y_7 + y_8$, entonces transponemos las coordenadas de las posiciones 7 y 8. Note que

$$\begin{aligned}H\widehat{y}^t &= Hy^t + H(0,\ldots,0,y_7+y_8,y_7+y_8)^t\\ &= \begin{pmatrix}a\\b\end{pmatrix} + \begin{pmatrix}y_7+y_8\\y_7+y_8\end{pmatrix}\\ &= \begin{pmatrix}a\\b\end{pmatrix} + \begin{pmatrix}a\\b\end{pmatrix}\\ &= \begin{pmatrix}2a\\2b\end{pmatrix}\\ &= \begin{pmatrix}0\\0\end{pmatrix}.\end{aligned}$$

En todos los otros casos, y no será un codeword válido y no será corregido (el error es detectado pero no hay manera alguna de corregirlo).

2.3.2 Teorema. Usando el algoritmo de decodificación indicado anteriormente un error es corregido, dos errores son detectados y una transposición de dos caracteres adyacentes es revertida.

Demostración.
Sean $c = (c_1,\ldots,c_8) \in C$ el codeword transmitido, $y = (y_1,\ldots,y_8)$ es el vector recibido y supongamos que $\widehat{y} = (\widehat{y}_1,\ldots,\widehat{y}_8)$ es el codeword decodificado en los casos del 1 al 7 dados anteriormente. Entonces la diferencia

$$e := (e_1,\ldots,e_8) = y - c$$

es el vector de error de transmisión y los valores de prueba son:

$$\begin{aligned}\begin{pmatrix} a \\ b \end{pmatrix} &= Hy^t \\ &= H(c+e)^t \\ &= Hc^t + He^t \\ &= He^t \\ &= \begin{pmatrix} e_1t + e_2t^2 + e_3t^3 + e_4t^4 + e_5t^5 + e_6t^6 + e_7 \\ e_1t^2 + e_2t^4 + e_3t^6 + e_4t^8 + e_5t^{10} + e_6t^{12} + e_8 \end{pmatrix}\end{aligned}$$

Distinguiremos tres casos.

Caso 1. Asumamos que ocurrió un solo error en la posición i. Entonces $e = (0, \ldots, 0, e_i, 0, \ldots, 0)$ y

$$(a,b) = \begin{cases} (e_it^i, e_it^{2i}), & \text{si} \quad i = 1, \ldots, 6 \\ (e_7, 0) & \text{si} \quad i = 7 \\ (0, e_8) & \text{si} \quad i = 8. \end{cases} \tag{2.6}$$

Aplicando el algoritmo de decodificación

$$\widehat{y} = \begin{cases} y + (0 \ldots, \frac{a}{t^i}, \ldots, 0) & \text{si } \ i = 1, \ldots, 6 \ \text{ de acuerdo con la regla (4)} \\ y + (0 \ldots, a, 0) & \text{si } \ i = 7 \quad \text{de acuerdo con la regla (2)} \\ y + (0 \ldots, 0, a) & \text{si } \ i = 8 \quad \text{de acuerdo con la regla (3).} \end{cases}$$

En cualquier caso, $\widehat{y} = y + e = y - e = c$ y el error de transmisión es corregido.

Caso 2. Asumamos que se produjeron dos errores. Dado que la distancia mínima de C es 3, se verifica que dos codewords diferentes difieren en al menos tres coordenadas. En consecuencia, dos errores no pueden cambiar un codeword en otro. Por lo tanto $Hy^t \neq (0,0)^t$ y el codeword es detectado.

Caso 3. Supongamos que dos caracteres distintos en las posiciones i y $i+1$ han sido transpuestos. Entonces

$$e = (0, \ldots, 0, e_i, e_{i+1}, 0, \ldots, 0) = (0 \ldots, c_i + c_{i+1}, c_i + c_{i+1}, \ldots, 0)$$

y

$$\binom{a}{b} = \begin{cases} \begin{pmatrix} (c_i + c_{i+1})(t^i + t^{i+1}) \\ (c_i + c_{i+1})(t^{2i} + t^{2i+2}) \end{pmatrix} & \text{si } \ i \leq 5, \\ \begin{pmatrix} (c_6 + c_7)(t^6 + 1) \\ (c_6 + c_7)t^{12} \end{pmatrix} & \text{si } \ i = 6, \\ \begin{pmatrix} (c_7 + c_8) \\ (c_7 + c_8) \end{pmatrix} & \text{si } \ i = 7. \end{cases}$$

Dado que

$$\frac{(t^{2i} + t^{2i+2})}{t^i + t^{i+1}} = \frac{(t^i + t^{i+1})^2}{t^i + t^{i+1}} = t^i + t^{i+1} = t^{18+i},$$

para $i = 1, \ldots, 5$ y

$$\frac{t^{12}}{t^6 + 1} = t^{16}$$

y

$$c_i + c_{i+1} = y_i + y_{i+1}$$

podemos aplicar las reglas (5) (6), y (7) del algoritmo de decodificación, con lo cual tenemos que $\widehat{y} = c$ y la transposición de dos caracteres adyacentes es corregida. □

2.4 Confiabilidad del código

Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$ y supongamos que un codeword $c \in C$ fue enviado a través de un canal ruidoso y que es recibido un vector $y \in \mathbb{F}_q^n$. Una técnica simple de decodificación es buscar el codeword *mas cercano*, con respecto a la distancia de Hamming. Usualmente esta técnica es denominada decodificación mediante el *vecino próximo*. Este método es razonable, siempre que el canal cumpla con las siguientes condiciones, las cuales en la práctica se satisfacen a menudo. Supondremos que detrás está siempre el alfabeto $\mathbb{F}_q$, el cuerpo con q elementos.

(1) Todo símbolo $a \in \mathbb{F}_q$ tiene la misma probabilidad $p < \frac{q-1}{q}$ de ser recibido con error.

(2) Si un símbolo es recibido con error entonces cada uno de los $q-1$ errores posibles es igualmente probable.

La condición (1) establece que $1 - p > \frac{1}{q}$ es la probabilidad de transmitir un símbolo sin error. En el caso $q = 2$, esto significa que un bit pasa a través del canal sin perturbación con una probabilidad mayor que $\frac{1}{2}$. De la condición (2) se sigue que la probabilidad de adulteración en otro símbolo dado es $\frac{p}{q-1} < \frac{1}{q}$.

Los canales que satisfacen las propiedades (1) y (2) se denominan *simétricos q-arios*. En el caso $q = 2$ los canales con tales propiedades se denominarán *simétricos binarios*. Las probabilidades de transmisión en un canal simétrico binario se pueden esquematizar de la siguiente manera:

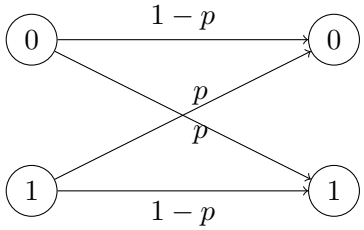

Figura 2.2: Canal simétrico binario.

Si se mantienen las hipótesis dadas anteriormente, entonces la probabilidad de que un codeword incorrecto no sea detectado o equivalentemente de una decodificación incorrecta se puede calcular de manera explícita, si se conoce la distribución de pesos del código C. Antes de que iniciemos con la cuantificación de la confiabilidad de un código, especificamos la estrategia para la decodificación y la probabilidad de una decodificación errónea como la base de nuestras consideraciones.

Cuando se trata el tema de errores en la decodificación, lo usual es elegir el punto de vista del transmisor para obtener definiciones exactas de dichas probabilidades. Al enviar un mensaje uno puede preocuparse por el hecho que un decodificador no puede detectar la existencia de un error en la transmisión. La probabilidad de un error no sea detectado bajo el supuesto que un codeword c haya sido enviado se puede expresar en términos de la distribución de pesos del código C de la siguiente manera:

Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$. Para $c \in C$ y $v \in \mathbb{F}_q^n$ denotamos con $P(v|c)$ la probabilidad condicional de que sea recibido el vector v, dado que fue enviado el codeword c. Una decodificación de máxima verosimilitud decodifica el vector $v \in \mathbb{F}_q^n$ mediante un codeword $c \in C$, para el cual se verifica que

$$P(v|c) = \max_{c' \in C} P(v|c'). \tag{2.7}$$

Es decir, mediante el codeword con mayor probabilidad de haber sido enviado. Si existe más de un codeword que alcanza dicho máximo, entonces se elige uno aleatoriamente. Se puede demostrar que para canales simétricos q-arios se verifica que

$$P(v|c') = (\tfrac{p}{q-1})^j (1-p)^{n-j}, \quad \text{con} \quad d(v,c') = j.$$

Para una demostración puede verse [24].

2.4.1 Definición. Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$. Si $t \leq \frac{d-1}{2}$ y $p < \frac{q-1}{q}$ es la probabilidad de error del canal. Se define $P_{ue}(C,t,p)$ como la probabilidad de que un codeword w con $d(w,c') \leq t$ para algún codeword $c' \in C \backslash \{c\}$ se reciba si $c \in C$ es transmitido. Es decir,

$$P_{ue}(C,t,p) = P(Y \in \bigcup_{c \neq c' \in C} B_t(c') \mid X = c)$$

donde X e Y denotan, respectivamente, las variables aleatorias para "enviar un codeword $c \in C$ y recibir un vector $w \in \mathbb{F}_q^n$".

La idea de decodificación es aceptar mensajes decodificados sólo si el codeword recibido no contiene un número grande de errores . Intuitivamente, parece claro que en la medida que una codeword recibido debe ser sometida a muchas correcciones, el resultado de la decodificación es sin duda una disminución de la confiabilidad. Para aclarar este hecho, es necesario analizar un algoritmo de decodificación que distingue entre pocos y muchos errores detectables. En consecuencia, fijamos un número máximo de errores aceptables para la decodificación, el cual denotamos con t. Si se detectan más errores en un codeword transmitido, el codeword decodificado no se acepta como confiable y el mensaje debe ser ignorado o retransmitido, si esto es posible. Esta estrategia para la decodificación es denominada t-acotada.

2.4.2 Definición. Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$ y sean $t \leq \frac{d-1}{2}$ la cota de confiabilidad de la decodificación, $p < \frac{q-1}{q}$ es la probabilidad de error del canal y $v \in \mathbb{F}_q^n$ un vector recibido. Si existe un codeword $c' \in C$ con $d(v,c') \leq t$, entonces el vector v es decodificado mediante c'. Si tal codeword no existe, entonces el vector v es rechazado. Esta estrategia para la decodificación se llamará t-acotada.

En este enfoque se debe calcular la probabilidad de decodificación errónea para un vector recibido fijo v, en su lugar y al promediar el resultado en el conjunto

de los codewords que pueden ser decodificados mediante una estrategia t-acotada. Una vector recibido fijo v que es decodificable con estrategia t-acotada está a lo mas a una distancia t de un codeword c'. Por lo tanto, la probabilidad de decodificación errónea, suponiendo que se recibió un vector v está dada por

$$\sum_{c \in C \setminus \{c'\}} P(c \text{ transmitido} \mid v \text{ recibido}). \tag{2.8}$$

Para promediar dentro del conjunto de palabras decodificables mediante una estrategia t-acotada uno tiene que ponderar estas probabilidades individuales de decodificación falsa mediante

$$P\big(v \text{ recibido} \mid v \in \bigcup_{c' \in C} \{w \in \mathbb{F}_q^n \mid d(c', w) \leq t\}\big). \tag{2.9}$$

En conjunto, esta promediada probabilidad de falsas decodificaciones resulta en la siguiente definición.

2.4.3 Definición. Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$ y sean $t \leq \frac{d-1}{2}$ es la cota de confiabilidad de la decodificación y $p < \frac{q-1}{q}$ es la probabilidad de error del canal. Se define $P_{fd}(C, t, p)$ como la probabilidad de falsa decodificación condicionada a una estrategia de decodificación t-acotada mediante

$$P_{fd}(C, t, p) = P(X \in C \setminus \{c\} \mid Y \in B_t(c)),$$

para $c \in C$ y $v \in \mathbb{F}_q^n$.

Como consecuencia de las condiciones de equiprobabilidad impuestas al canal se tiene que

$$P_{fd}(C, t, p) = P(X \in C \setminus \{0\} \mid Y \in B_t(0)).$$

La confiabilidad de un código C bajo una estrategia de decodificación t-acotada se define por

$$T(C, t, p) = 1 - P_{fd}(C, t, p).$$

En el siguiente teorema se presenta una relación entre las funciones P_{ue} y P_{fd}.

2.4.4 Teorema. Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$. Si $t \leq \frac{d-1}{2}$ y $p < \frac{q-1}{q}$, entonces

$$P(Y \in B_t(0)) \cdot P_{fd}(C, t, p) = \frac{1}{|C|} P_{ue}(C, t, p).$$

Demostración.

$$\begin{aligned} P(Y \in B_t(0))\cdot P_{fd}(C,t,p) &= P(X \in C \setminus \{0\} \mid Y \in B_t(0)) \\ &= \sum_{0\neq c\in C} \sum_{w\in B_t(0)} P(X=c \mid Y=w) \\ &= \sum_{0\neq c\in C} \sum_{w\in B_t(0)} P(Y=w \mid X=c)\cdot P(X=c) \\ &= \frac{1}{|C|} P_{ue}(C,t,p). \end{aligned}$$

Esta última igualdad se debe a las condiciones impuestas al canal. Es decir,

$$P(X=c) = \frac{1}{|C|}.$$

Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$. En el siguiente resultado podemos ver que las funciones $P_{fd}(C,t,p)$ y $P_{ue}(C,t,p)$ solo difieren en términos que no tienen que ver con el código en si, sino con los parámetro t y p.

2.4.5 Teorema. Sean C un $[n,k,d]$-código sobre $\mathbb{F}_q$ y $t \leq \frac{d-1}{2}$ entonces:

$$\begin{aligned} P_{fd}(C,t,p) &= \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}} \\ &= 1 - \frac{\sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}. \end{aligned}$$

Demostración. De acuerdo con lo visto en el teorema 2.4.4 tenemos

$$\begin{aligned}
\frac{P_{ue}(C,t,p)}{P_{fd}(C,t,p)} &= |C| \cdot P(Y \in B_t(0)) \\
&= |C| \cdot \sum_{c \in C} P(Y \in B_t(0) \mid X = c) \\
&= |C| \cdot \sum_{c \in C} P(Y \in B_t(0) \mid X = c) P(X = c) \\
&= |C| \cdot P(X = c) \sum_{c \in C} P(Y \in B_t(0) \mid X = c) \\
&= |C| \cdot \frac{1}{|C|} \sum_{c \in C} P(Y \in B_t(0) \mid X = c) \\
&= P(Y \in B_t(0) \mid X = 0) + \sum_{0 \neq c \in C} P(Y \in B_t(0) \mid X = c) \\
&= \sum_{i=0}^{t} \tbinom{n}{i} p^i (1-p)^{n-i} + P_{ue}(C,t,p).
\end{aligned}$$

Dado que

$$P(Y \in B_t(0) \mid X = 0) = \sum_{i=0}^{t} \tbinom{n}{i} p^i (1-p)^{n-i},$$

se sigue que

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \tbinom{n}{i} p^i (1-p)^{n-i}}.$$

Al buscar códigos adecuados para la detección o corrección de errores, la confiabilidad del código es un criterio importante. La mejor opción es entonces escoger un código con máxima $T(C,t,p)$.

2.4.6 Lema. Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$ con $d \geq 2$ y sean $0 \leq t \leq \frac{d-1}{2}$ la cota de confiabilidad de la decodificación, $p < \frac{q-1}{q}$ es la probabilidad de error del canal. Entonces

$$\lim_{p \to 0} \frac{P_{fd}(C,t,p)}{(\frac{p}{1-p})^{d-t}} = A_d \, \tbinom{d}{t} (q-1)^{t-d}.$$

Demostración. Ver lema 4.3 en [4].

En particular la probabilidad de una falsa decodificación está dada aproximadamente por

$$P_{fd}(C,t,p) \approx A_d \ \tbinom{d}{t} \left(\tfrac{p}{(1-p)(q-1)}\right)^{d-t},$$

siempre que p sea lo suficientemente pequeño.

En nuestra situación C es un código lineal sobre $\mathbb{F}_{32}$ con distancia minima 3. Ademas C es un MDS código , el número de codewords con tres coordenadas distintas de cero es $A_3 = 1736$. Ahora sea p la probabilidad de error de un simple caracter. Entonces, la probabilidad de no detectar un PID equivocado $t = 0$ en el teorema anterior está dado por:

$$\begin{aligned} P &= A_d \ \tbinom{d}{t} \left(\tfrac{p}{(1-p)(q-1)}\right)^{d-t} \\ &= A_3 \ \tbinom{3}{0} \left(\tfrac{p}{(1-p)(32-1)}\right)^{3-0} \\ &= 1736.(1)\frac{(p)^3}{(1-p)^3.31^3} \\ &= 0.058\frac{p^3}{(1-p)^3} \\ &\approx 0.6p^3 \end{aligned}$$

Siempre que p sea lo suficientemente pequeño.

La probabilidad de una correccíon automática errónea $t = 1$ está dada por:

$$\begin{aligned} P &= A_d \ \tbinom{d}{t} \left(\tfrac{p}{(1-p)(q-1)}\right)^{d-t} \\ &= A_3 \ \tbinom{3}{1} \left(\tfrac{p}{(1-p)(32-1)}\right)^{3-1} \\ &= 1736.(3)\frac{(p)^2}{(1-p)^2.31^2} \\ &= 5.4193\frac{p^2}{(1-p)^2} \\ &\approx 5.42p^2 \end{aligned}$$

Siempre que p no sea tan grande.

2.4.7 Ejemplo. Si asumimos que tenemos una tasa de error $p = 0.003$ entonces una correccíon automática tendría una tasa de error de:

$$\begin{aligned} P &= A_d \ \tbinom{d}{t} \left(\tfrac{p}{(1-p)(q-1)}\right)^{d-t} \\ &= A_3 \ \tbinom{3}{1} \left(\tfrac{0.003}{(1-0.003)(32-1)}\right)^{3-1} \\ &= 4.9 \times 10^{-5}, \end{aligned}$$

lo cual es razonablemente bajo para los analisis estadisticos, pero inaceptable cuando el PID es usado en un contexto de tratamiento del paciente.

La probabilidad de que un PID incorrecto no sea detectado esta dada por:

$$\begin{aligned} P &= A_d \binom{d}{t} \left(\frac{p}{(1-p)(q-1)}\right)^{d-t} \\ &= A_3 \binom{3}{0} \left(\frac{0.003}{(1-0.003)(32-1)}\right)^{3-0} \\ &= 1736.(1)\frac{(0.003)^3}{(1-0.003)^3.31^3} \\ &\approx 1.6 \times 10^{-9}, \end{aligned}$$

lo cual es suficientemente pequeño para todas las aplicaciones.

2.5 Un ejemplo de un PID válido

En la siguiente figura se muestra una visión general de los dos pasos del algoritmo de generación de un PID. El primer paso es un procedimiento de cifrado, es decir, donde entra la seguridad de la información y el segundo paso agrega dos caracteres.

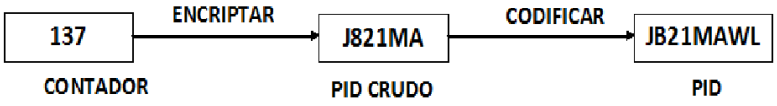

Figura 2.3: Proceso de codificación

La palabra `J821MAWL` es un PID válido, el cual esta representado por el vector $(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$ en donde:

$$\begin{aligned} c_1 &= J = (10001) \\ c_2 &= 8 = (01000) \\ c_3 &= 2 = (00010) \\ c_4 &= 1 = (00001) \\ c_5 &= M = (10100) \\ c_6 &= A = (01010). \end{aligned}$$

De acuerdo con la función de traslación mostrado en el proceso de codificación. Verifiquemos la primera suma de control.

$$\begin{aligned} t \cdot c_1 &= t(10001) \\ &= t(t^4 + 1) \\ &= t^5 + t \\ &= t^2 + 1 + t \\ &= (00111). \end{aligned}$$

$$\begin{aligned} t^2 \cdot c_2 &= t^2(01000) \\ &= t^2(t^3) \\ &= t^5 \\ &= t^2 + 1 \\ &= (00101). \end{aligned}$$

$$\begin{aligned} t^3 \cdot c_3 &= t^3(00010) \\ &= t^3.t \\ &= t^4 \\ &= (10000). \end{aligned}$$

$$\begin{aligned} t^4 \cdot c_4 &= t^4(00001) \\ &= t^4 \\ &= (10000). \end{aligned}$$

$$\begin{aligned} t^5 \cdot c_5 &= t^5(10100) \\ &= t^5(t^4 + t^2) \\ &= t^9 + t^6 \\ &= (t^2 + 1)t^4 + (t^2 + 1)t \\ &= (t^2 + 1)t + t^4 + t^3 + t \\ &= t^3 + t + t^4 + t^3 + t \\ &= t^4 \\ &= (10000). \end{aligned}$$

$$\begin{aligned} t^6 \cdot c_6 &= t^6(01010) \\ &= t^6(t^3 + t) \\ &= t^9 + t^7 \\ &= (t^2+1)t^4 + (t^2+1)t^2 \\ &= t^6 + t^4 + t^4 + t^2 \\ &= (t^2+1)t + t^4 + t^4 + t^2 \\ &= t^3 + t + t^2 \\ &= (01110). \end{aligned}$$

Entonces

$$\begin{aligned} c_7 &= tc_1 + t^2c_2 + t^3c_3 + t^4c_4 + t^5c_5 + t^6c_6 \\ &= (00111) + (00101) + (10000) + (10000) + (10000) + (01110) \\ &= (11100) \\ &= W. \end{aligned}$$

La segunda suma de control está dada por:

$$\begin{aligned} t^2 \cdot c_1 &= t^2.(10001) \\ &= t^2(t^4 + 1) \\ &= t^6 + t^2 \\ &= (t^2+1)t + t^2 \\ &= t^3 + t + t^2 \\ &= (01110). \end{aligned}$$

$$\begin{aligned} t^4 \cdot c_2 &= t^4(01000) \\ &= t^4t^3 \\ &= t^7 \\ &= (t^2+1)t^2 \\ &= t^4 + t^2 \\ &= (10100). \end{aligned}$$

$$\begin{aligned} t^6 \cdot c_3 &= t^6(00010) \\ &= t^6 t \\ &= t^7 \\ &= (t^2+1)t^2 \\ &= t^4 + t^2 \\ &= (10100). \end{aligned}$$

$$\begin{aligned} t^8 \cdot c_4 &= t^8(00001) \\ &= t^8 \\ &= (t^2+1)t^3 \\ &= t^5 + t^3 \\ &= t^2 + 1 + t^3 \\ &= (01101). \end{aligned}$$

$$\begin{aligned} t^{10} \cdot c_5 &= t^{10}(10100) \\ &= t^{10}(t^4 + t^2) \\ &= (t^2+1)^2(t^4 + t^2) \\ &= (t^4+1)(t^4 + t^2) \\ &= t^8 + t^6 + t^4 + t^2 \\ &= (t^2+1)t^3 + (t^2+1)t + t^4 + t^2 \\ &= t^5 + t^3 + t^3 + t + t^4 + t^2 \\ &= t^2 + 1 + t + t^4 + t^2 \\ &= t^4 + t + 1 \\ &= (10011). \end{aligned}$$

$$\begin{aligned} t^{12} \cdot c_6 &= t^{12}(01010) \\ &= t^{12}(t^3 + t) \\ &= t^{15} + t^{13} \\ &= (t^2+1)^3 + (t^2+1)^2 t^3 \\ &= (t^6 + t^4 + t^2 + 1) + (t^4 + 1)t^3 \\ &= ((t^2+1)t + t^4 + t^2 + 1) + t^7 + t^3 \\ &= t^3 + t + t^4 + t^2 + 1 + t^7 + t^3 \\ &= t + t^4 + t^2 + 1 + t^7 \\ &= t + t^4 + t^2 + 1 + (t^2+1)t^2 \\ &= t + t^4 + t^2 + 1 + t^4 + t^2 \\ &= t + 1 \\ &= (00011). \end{aligned}$$

Entonces

$$\begin{aligned} c_8 &= t^2 c_1 + t^4 c_2 + t^6 c_3 + t^8 c_4 + t^{10} c_5 + t^{12} c_6 \\ &= (01110) + (10100) + (10100) + (01101) + (10011) + (00011) \\ &= (10011) \\ &= L. \end{aligned}$$

En donde las primeras seis posiciones del codeword $(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$ son el mensaje y las dos últimas posiciones son las ecuaciones de control. Para nuestro PID válido tendríamos

$$(\underbrace{\texttt{J,8,2,1,M,A}}_{\text{mensaje}}, \underbrace{\texttt{W,L}}_{\text{control}}).$$

Capítulo 3

Una extensión del código

El tema central de este capítulo es construir un código óptimo aplicable a la generación de identificadores, soportado por un cuerpo finito mas grande. Esto a fin de poder implementar a futuro algunas herramientas criptográficas.

3.1 Preliminares

El polinomio con coeficientes binarios $f = T^{10} + T^3 + 1 \in \mathbb{F}_2[T]$ es irreducible. Entonces por el teorema de Kronecker, el anillo cociente $\mathbb{F}_2[T]/(f)$ es un cuerpo con $2^{10} = 1024$ elementos, como se demostró en el teorema 1.1.19. El único cuerpo, salvo isomorfía, con $\mathbb{F}_{2^{10}}$ elementos puede verse como un espacio vectorial 10-dimensional sobre el cuerpo binario $\mathbb{F}_2$. Esto es, todo elemento de $\mathbb{F}_{2^{10}}$ puede ser representado por una cadena de longitud 10.

Sea t la clase residual de T. Entonces $\mathbb{F}_{2^{10}}$ tienen como espacio vectorial sobre $\mathbb{F}_2$, la base

$$B = (t^9, t^8, \ldots, t, 1), \tag{3.1}$$

la cual corresponde a la base canónica

$$\begin{aligned} e_1 &= 1000000000 \\ e_2 &= 0100000000 \\ e_3 &= 0010000000 \\ &\vdots \\ e_{10} &= 0000000001. \end{aligned}$$

Las operaciones en $\mathbb{F}_{2^{10}}$ como espacio vectorial son las usuales, esto es, la adición y la multiplicación por escalar por componentes. Como un cuerpo se tiene además la multiplicación en $\mathbb{F}_{2^{10}}$. La tabla de multiplicación completa es obtenida por la simple regla

$$t^{10} = t^3 + 1, \tag{3.2}$$

similar como se realizó en el capitulo anterior con el cuerpo $\mathbb{F}_{32}$.

Sea $z \in \mathbb{F}_{2^{10}}$, digamos

$$z = (z_1, z_2, \ldots, z_9, z_{10}) = z_1 t^9 + z_2 t^8 + \cdots + z_9 t + z_{10}.$$

Entonces el producto con potencias bajar de t puede verse de la siguiente manera:

$$\begin{aligned}
t \cdot z &= z_1 t^{10} + z_2 t^9 + z_3 t^8 + z_4 t^7 + z_5 t^6 + z_6 t^5 + z_7 t^4 + z_8 t^3 + z_9 t^2 + z_{10} t, \\
t^2 \cdot z &= z_1 t^{11} + z_2 t^{10} + z_3 t^9 + z_4 t^8 + z_5 t^7 + z_6 t^6 + z_7 t^5 + z_8 t^4 + z_9 t^3 + z_{10} t^2, \\
t^3 \cdot z &= z_1 t^{12} + z_2 t^{11} + z_3 t^{10} + z_4 t^9 + z_5 t^8 + z_6 t^7 + z_7 t^6 + z_8 t^5 + z_9 t^4 + z_{10} t^3, \\
t^4 \cdot z &= z_1 t^{13} + z_2 t^{12} + z_3 t^{11} + z_4 t^{10} + z_5 t^9 + z_6 t^8 + z_7 t^7 + z_8 t^6 + z_9 t^5 + z_{10} t^4, \\
t^5 \cdot z &= z_1 t^{14} + z_2 t^{13} + z_3 t^{12} + z_4 t^{11} + z_5 t^{10} + z_6 t^9 + z_7 t^8 + z_8 t^7 + z_9 t^6 + z_{10} t^5, \\
t^6 \cdot z &= z_1 t^{15} + z_2 t^{14} + z_3 t^{13} + z_4 t^{12} + z_5 t^{11} + z_6 t^{10} + z_7 t^9 + z_8 t^8 + z_9 t^7 + z_{10} t^6, \\
t^7 \cdot z &= z_1 t^{16} + z_2 t^{15} + z_3 t^{14} + z_4 t^{13} + z_5 t^{12} + z_6 t^{11} + z_7 t^{10} + z_8 t^9 + z_9 t^8 + z_{10} t^7, \\
t^8 \cdot z &= z_1 t^{17} + z_2 t^{16} + z_3 t^{15} + z_4 t^{14} + z_5 t^{13} + z_6 t^{12} + z_7 t^{11} + z_8 t^{10} + z_9 t^9 + z_{10} t^8, \\
t^9 \cdot z &= z_1 t^{18} + z_2 t^{17} + z_3 t^{16} + z_4 t^{15} + z_5 t^{14} + z_6 t^{13} + z_7 t^{12} + z_8 t^{11} + z_9 t^{10} + z_{10} t^9.
\end{aligned}$$

Entonces

$$\begin{aligned}
t \cdot z &= z_1(t^3 + 1) + z_2 t^9 + z_3 t^8 + z_4 t^7 + z_5 t^6 + z_6 t^5 + z_7 t^4 + z_8 t^3 + z_9 t^2 + z_{10} t, \\
t^2 \cdot z &= z_1(t^4 + x) + z_2(t^3 + 1) + z_3 t^9 + z_4 t^8 + z_5 t^7 + z_6 t^6 + z_7 t^5 + z_8 t^4 + z_9 t^3 + \\
&\quad z_{10} t^2, \\
t^3 \cdot z &= z_1(t^5 + t^2) + z_2(t^4 + x) + z_3(t^3 + 1) + z_4 t^9 + z_5 t^8 + z_6 t^7 + z_7 t^6 + z_8 t^5 + \\
&\quad z_9 t^4 + z_{10} t^3, \\
t^4 \cdot z &= z_1(t^6 + t^3) + z_2(t^5 + t^2) + z_3(t^4 + x) + z_4(t^3 + 1) + z_5 t^9 + z_6 t^8 + z_7 t^7 + \\
&\quad z_8 t^6 + z_9 t^5 + z_{10} t^4, \\
t^5 \cdot z &= z_1(t^7 + t^4) + z_2(t^6 + t^3) + z_3(t^5 + t^2) + z_4(t^4 + x) + z_5(t^3 + 1) + z_6 t^9 + \\
&\quad z_7 t^8 + z_8 t^7 + z_9 t^6 + z_{10} t^5,
\end{aligned}$$

$$
\begin{aligned}
t^6 \cdot z &= z_1(t^8+t^5)+z_2(t^7+t^4)+z_3(t^6+t^3)+z_4(t^5+t^2)+z_5(t^4+x)+\\
&\quad z_6(t^3+1)+z_7t^9+z_8t^8+z_9t^7+z_{10}t^6,\\
t^7 \cdot z &= z_1(t^9+t^6)+z_2(t^8+t^5)+z_3(t^7+t^4)+z_4(t^6+t^3)+z_5(t^5+t^2)+\\
&\quad z_6(t^4+x)+z_7(t^3+1)+z_8t^9+z_9t^8+z_{10}t^7,\\
t^8 \cdot z &= z_1(t^7+t^3+1)+z_2(t^9+t^6)+z_3(t^8+t^5)+z_4(t^7+t^4)+z_5(t^6+t^3)+\\
&\quad z_6(t^5+t^2)+z_7(t^4+x)+z_8(t^3+1)+z_9t^9+z_{10}t^8,\\
t^9 \cdot z &= z_1(t^8+t^4+x)+z_2(t^7+t^3+1)+z_3(t^9+t^6)+z_4(t^8+t^5)+\\
&\quad z_5(t^7+t^4)+z_6(t^6+t^3)+z_7(t^5+t^2)+z_8(t^4+x)+z_9(t^3+1)+z_{10}t^9.
\end{aligned}
$$

Por lo tanto

$$
\begin{aligned}
t \cdot z &= z_2t^9+z_3t^8+z_4t^7+z_5t^6+z_6t^5+z_7t^4+(z_1+z_8)t^3+z_9t^2+z_{10}t+z_1,\\
t^2 \cdot z &= z_3t^9+z_4t^8+z_5t^7+z_6t^6+z_7t^5+(z_1+z_8)t^4+(z_2+z_9)t^3+z_{10}t^2+\\
&\quad z_1t+z_2,\\
t^3 \cdot z &= z_4t^9+z_5t^8+z_6t^7+z_7t^6+(z_1+z_8)t^5+(z_2+z_9)t^4+(z_3+z_{10})t^3+\\
&\quad z_1t^2+z_2t+z_3,\\
t^4 \cdot z &= z_5t^9+z_6t^8+z_7t^7+(z_1+z_8)t^6+(z_2+z_9)t^5+(z_3+z_{10})t^4+(z_1+z_4)t^3+\\
&\quad z_2t^2+z_3t+z_4,\\
t^5 \cdot z &= z_6t^9+z_7t^8+(z_1+z_8)t^7+(z_2+z_9)t^6+(z_3+z_{10})t^5+(z_1+z_4)t^4+\\
&\quad (z_2+z_5)t^3+z_3t^2+z_4t+z_5,\\
t^6 \cdot z &= z_7t^9+(z_1+z_8)t^8+(z_2+z_9)t^7+(z_3+z_{10})t^6+(z_1+z_4)t^5+(z_2+z_5)t^4+\\
&\quad (z_3+z_6)t^3+z_4t^2+z_5t+z_6,\\
t^7 \cdot z &= (z_1+z_8)t^9+(z_2+z_9)t^8+(z_3+z_{10})t^7+(z_1+z_4)t^6+(z_2+z_5)t^5+\\
&\quad (z_3+z_6)t^4+(z_4+z_7)t^3+z_5t^2+z_6t+z_7,\\
t^8 \cdot z &= (z_2+z_9)t^9+(z_3+z_{10})t^8+(z_1+z_4)t^7+(z_2+z_5)t^6+(z_3+z_6)t^5+\\
&\quad (z_4+z_7)t^4+(z_1+z_5+z_8)t^3+z_6t^2+z_7t+(z_1+z_8),\\
t^9 \cdot z &= (z_3+z_{10})t^9+(z_1+z_4)t^8+(z_2+z_5)t^7+(z_3+z_6)t^6+(z_4+z_7)t^5+\\
&\quad (z_1+z_5+z_8)t^4+(z_2+z_6+z_9)t^3+z_7t^2+(z_1+z_8)t+(z_2+z_9)
\end{aligned}
$$

En consecuencia

$$
\begin{aligned}
t \cdot z &= (z_2, z_3, z_4, z_5, z_6, z_7, z_1 + z_8, z_9, z_{10}, z_1) \\
t^2 \cdot z &= (z_3, z_4, z_5, z_6, z_7, z_1 + z_8, z_2 + z_9, z_{10}, z_1, z_2), \\
t^3 \cdot z &= (z_4, z_5, z_6, z_7, z_1 + z_8, z_2 + z_9, z_3 + z_{10}, z_1, z_2, z_3), \\
t^4 \cdot z &= (z_5, z_6, z_7, z_1 + z_8, z_2 + z_9, z_3 + z_{10}, z_1 + z_4, z_2, z_3, z_4), \\
t^5 \cdot z &= (z_6, z_7, z_1 + z_8, z_2 + z_9, z_3 + z_{10}, z_1 + z_4, z_2 + z_5, z_3, z_4, z_5), \\
t^6 \cdot z &= (z_7, z_1 + z_8, z_2 + z_9, z_3 + z_{10}, z_1 + z_4, z_2 + z_5, z_3 + z_6, z_4, z_5, z_6), \\
t^7 \cdot z &= (z_1 + z_8, z_2 + z_9, z_3 + z_{10}, z_1 + z_4, z_2 + z_5, z_3 + z_6, z_4 + z_7, z_5, z_6, z_7), \\
t^8 \cdot z &= (z_2 + z_9, z_3 + z_{10}, z_1 + z_4, z_2 + z_5, z_3 + z_6, z_4 + z_7, z_1 + z_5 + z_8, z_6, z_7, \\
&\qquad z_1 + z_8), \\
t^9 \cdot z &= (z_3 + z_{10}, z_1 + z_4, z_2 + z_5, z_3 + z_6, z_4 + z_7, z_1 + z_5 + z_8, z_2 + z_6 + z_9, z_7, \\
&\qquad z_1 + z_8, z_2 + z_9).
\end{aligned}
$$

Estas últimas ecuaciones suministran un camino muy eficiente para la implementación de las operacioes definidas sobre el cuerpo.

3.2 Una nueva forma de generar IDs

En esta sección presentamos una alternativa para la generación de IDs con una longitud mayor y mas robustos desde elpunto de vista de la seguridad informática. Similar como en el capítulo anterior, necesitamos que cada ID cumpla con los mismos requerimientos:

- Debe ser de tipo alfa-numérico.
- Contener unos bits de redundancia para la detección y eventual corrección de errores.
- Tener una longitud fija y un número adecuado de caracteres.
- Evitar las inferencias con los correspondientes datos de identidad, ni de tiempo ni de orden de su generación.

Nuevamente nuestro alfabeto base debe constar de los dígitos $0, \ldots, 9$ y las letras del alfabeto castellano consideradas en el capítulo anterior. Es decir, el conjunto $\{A, B, C, \ldots, Z\}$ excluyendo las letras B, I, O, S, por las mismas razones expuestas anteriormente. En total tenemos nuevamente 32 caracteres disponibles.

Para la realización de los cálculos matemáticos se establece una correspondencia entre los anteriores 32 caracteres y los elementos del espacio vectorial cociente $\mathbb{F}_{2^{10}}/\mathbb{F}_{2^5}$ sobre $\mathbb{F}_2$. Del teorema 1.1.27 se sigue que $\mathbb{F}_{2^5}$ es un subcuerpo de $\mathbb{F}_{2^{10}}$ y resulta evidente que el grado de la extensión es 5. En consecuencia el número de elementos de tal espacio cociente es 32.

Nuevamente usamos el orden lexicográfico. Es decir, hacemos corresponder al 0 la clase lateral $00000 + \mathbb{F}_{2^5}, \ldots$, al 9 le corresponde 01001 , a la A le corresponde 01010 y así hasta la Z, a la cual le corresponde la cadena 11111. En la siguiente tabla se presenta la correspondencia completa.

3.3 La construcción del código

Consideremos el $[11, 7]$-código C sobre $\mathbb{F}_{2^{10}}$ con matriz generadora dada por

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & t & t^2 & t^3 & t^4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & t^2 & t^4 & t^6 & t^8 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & t^3 & t^6 & t^9 & t^{12} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & t^4 & t^8 & t^{12} & t^{16} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & t^5 & t^{10} & t^{15} & t^{20} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & t^6 & t^{12} & t^{18} & t^{24} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & t^7 & t^{14} & t^{21} & t^{28} \end{pmatrix}. \tag{3.3}$$

Esto es, si $c = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}) \in C$, entonces $c = xG$, para algún $x = (c_1, c_2, c_3, c_4, c_5, c_6, c_7) \in \mathbb{F}_{2^{10}}^7$ y

$$\begin{aligned} c_8 &= c_1 t + c_2 t^2 + c_3 t^3 + c_4 t^4 + c_5 t^5 + c_6 t^6 + c_7 t^7 \\ c_9 &= c_1 t^2 + c_2 t^4 + c_3 t^6 + c_4 t^8 + c_5 t^{10} + c_6 t^{12} + c_7 t^{14} \\ c_{10} &= c_1 t^3 + c_2 t^6 + c_3 t^9 + c_4 t^{12} + c_5 t^{15} + c_6 t^{18} + c_7 t^{21} \\ c_{11} &= c_1 t^4 + c_2 t^8 + c_3 t^{12} + c_4 t^{16} + c_5 t^{20} + c_6 t^{24} + c_7 t^{28}. \end{aligned}$$

3.3.1 Teorema. El código C con matriz generadora (3.3) tiene distancia mínima 5.

Demostración. Sean $c, c' \in C$ con $c \neq c'$. Dado que las filas de G forman una base para C, se tiene que el codeword $c - c'$ es una combinación lineal de estos vectores. Note que cada fila de G tiene cinco posiciones no nulas. Si consideramos una combinación lineal de la i-ésima y la j-ésima fila, con $i \neq j$, entonces tenemos exactamente dos coordenadas no nulas en las primeras siete

posiciones. Dos posiciones de las últimas cuatro coordenadas no pueden ser cero simultaneamente. Suponga por ejemplo que

$$at^i + bt^j = at^{2i} + bt^{2j} = 0,$$

con $a, b \neq 0$. Entonces se sigue que $t^i = t^j$, lo cual no es posible, ya que $i \neq j$. Tomar una combinación lineal de tres o mas filas de G implica que tres o mas coordenadas son iguales a cero, excluyendo las primeras siete posiciones. En cualquier caso el número de coordenadas diferentes de cero excede tres y por consiguiente c y c' difieren en por lo menso cinco coordenadas. □

3.3.2 Observación. El código construido en el teorema 3.3.1 tiene parametros $[11, 7, 5]$ sobre el cuerpo finito $\mathbb{F}_{2^{10}}$. Usando el corolario 1.2.14 y la cota de Singleton se sigue que

1. El código C puede detectar hasta 4 errores.
2. El código C puede corregir hasta 2 errores.
3. C es un MDS-code.

Como hemos fijado antes, un elemento importante para la descripción de un código lineal C sobre el cuerpo finito $\mathbb{F}_q$ es la matriz de control de paridad. El complemento ortogonal de C es un subespacio vectorial de y por lo tanto un código lineal denominado el código dual de C, el cual denotamos con $C^\perp$. Si C es un $[n, k]$-código, entonces $C^\perp$ es un $[n, n-k]$-código. Recordemos que el código C puede expresarse en términos de la matriz de control de paridad H de la siguiente manera:

$$C = \{x \in \mathbb{F}_q^n \mid Hx^t = 0\}.$$

Del teorema 1.2.25 se sigue el siguiente resulatado.

3.3.3 Corolario El código C con matriz generadora (3.3) tiene la siguiente matriz de control de paridad

$$H = \begin{pmatrix} x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & 1 & 0 & 0 & 0 \\ x^2 & x^4 & x^6 & x^8 & x^{10} & x^{12} & x^{14} & 0 & 1 & 0 & 0 \\ x^3 & x^6 & x^9 & x^{12} & x^{15} & x^{18} & x^{21} & 0 & 0 & 1 & 0 \\ x^4 & x^8 & x^{12} & x^{16} & x^{20} & x^{24} & x^{28} & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.4}$$

Problema. Supongase que un codeword $c \in C$ digamos

$$c = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11})$$

es enviado a través de un canal ruidoso y que el vector $y \in \mathbb{F}_{2^{10}}^{11}$ digamos

$$y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11})$$

es recibido. Se trata de diseñar un algoritmo de decodificación utilizando las cifras de control dadas mediante

$$\begin{aligned}
a &= y_1x + y_2x^2 + y_3x^3 + y_4x^4 + y_5x^5 + y_6x^6 + y_7x^7 + y_8 \\
b &= y_1x^2 + y_2x^4 + y_3x^6 + y_4x^8 + y_5x^{10} + y_6x^{12} + y_7x^{14} + y_9 \\
d &= y_1x^3 + y_2x^6 + y_3x^9 + y_4x^{12} + y_5x^{15} + y_6x^{18} + y_7x^{21} + y_{10} \\
e &= y_1x^4 + y_2x^8 + y_3x^{12} + y_4x^{16} + y_5x^{20} + y_6x^{24} + y_7x^{28} + y_{11}.
\end{aligned}$$

Note que

$$Hy^t = (a, b, d, e)^t.$$

Dado que H es la matriz de control de paridad del código C, se sigue que estas ecuaciones suministran unos apropiados valores de prueba. Por ejemplo, el caso mas simple es cuando $a = b = d = e = 0$, en este caso y es un codeword y en consecuencia se puede decodificar mediante el vector y.

Bibliografía & Referencias

[1] E. R. Berlekamp. Algebraic Coding Theory. Aegean Park Press, 1984.

[2] A. Faldum y K. Pommerening. An optimal code for patient identifiers. Comput Methods Programs Biomed, 2005.

[3] A. Faldum, J. Lafuente, G. Ochoa y W. Willems. Error probabilities for bounded distance decoding.

[4] A. Faldum. On the Trustworthiness of Error-Correcting Codes. IEEE Transactions on information theory, Vol. 53, No. 12, 2007.

[5] R. Hill. *A First Course in Coding Theory.* Clarendon Press, 1986.

[6] D. Mannos. NCPS patient misidentification study: a summary of root cause analyses. VA NCPS Topics in Patient Safety. Washington, DC, United States Department of Veterans Affairs, June-July 2003.

[7] F.J. MacWilliams, N.J.A. Sloane. The Theory of Error-Correcting Codes. North-Holland Mathematical Library, Amsterdam, 1988.

[8] National Patient Safety Goals. Oakbrook Terrace, IL; Joint Commission, 2006.

[9] P. Thomas P y C. Evans. An identity crisis? Aspects of patient misidentification. Clinical Risk, 2004, 10:18-22.

[10] S. A. Vanstone y P. C. Oorschot. An Introduction to Error-Correcting Codes with Applications. Kluwer, 1989.

[11] L. C. Washington. Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications), Chapman & Hall/CRC, 2003.

[12] Wristbands for hospital inpatients improves safety. National Patient Safety Agency, Safer practice notice 11, 22 November 2005.

[13] Use of color-coded patient wristbands creates unnecessary risk. Patient Safety Advisory Supplement, Vol. 2, Sup. 2. Harrisburg, Pennsylvania Patient Safety Authority, 14 December 2005

[14] Edozien L. Correct patient, correct site, correct procedure. Safer Health Care, 27 July 2005.

[15] Right patient - right care. Improving patient safety through better manual and technology-based sys- tems for identification and matching of patients and their care. London, National Patient Safety Agency, 2004.

[16] Dighe A et al. Massachusetts General Hospital - bar coded patient wristband initiative: a CPM initiative. IHI National Forum storyboard presentation, December 2004; Safety Improvement Reports. saferhealth - care, 2005.

[17] Wright AA et al. Bar coding for patient safety. New England Journal of Medicine, 2005,

[18] Emerging technology: hospitals turn to RFID. HealthLeaders, August 2005

[19] Secure identification: the smart card revolution in health care. The Silicon Trust, 4 June 2003.

[20] S. Roman. *Coding and Information Theory.* Springer, 1992.

[21] F.J. Mac Williams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland Mathematical Library, Amsterdam, 1988.

[22] W. Willems, *Codierungstheorie*, Walter de Gruyter Inc., 1999.

[23] J.H. Van Lint, *Introduction to Coding Theory*, Springer-Verlag, New York Heidelberg Berlin 1982.

[24] W. Willems, *Codierungstheorie und Kriptographie*, Birkhäuser Verlag, Basel, 2008.

[25] W.C. Huffman and V. Pless, *Fundamentals of error-correcting Codes*, Cambridge University Press, Cambridge 2003.