Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

ESQUEMAS DE REPARTO DE SECRETOS Y TEORÍA DE LA INFORMACIÓN

Autor: Alejandro Martín Bastardo
Tutor: Umberto Martínez Peñas
Año: 2023/2024

II

Índice general

Resumen

Los esquemas de reparto de secretos son cruciales hoy en día para almacenar de forma segura información sensible (considerada como un secreto), de tal forma que los nodos individuales de almacenamiento no puedan conocer dicha información, mientras que si se reúnen suficientes nodos, consiguen obtener dicha información. Estos esquemas fueron introducidos por Shamir, se basan principalmente en códigos algebraicos (como los de Reed-Solomon) y proporcionan seguridad incondicional. En este trabajo, definiremos formalmente dichos esquemas, los estudiaremos basados en diferentes familias de códigos algebraicos, y analizaremos su seguridad utilizando resultados de teoría de la información.

Abstract

Secret sharing schemes are crucial nowadays for securely storing sensitive information (considered as a secret) in such a way that individual storage nodes cannot access this information, while a sufficient number of nodes together can retrieve it. These schemes were introduced by Shamir, are primarily based on algebraic codes (such as Reed-Solomon codes), and provide unconditional security. In this work, we will formally define these schemes, study them based on different families of algebraic codes, and analyze their security using information theory results.

Introducción

Los esquemas de reparto de secretos son fundamentales en la criptografía moderna, pues fueron diseñados para proteger información sensible dividiéndola en múltiples partes, asegurando que un secreto completo solo puede ser reconstruido cuando se reúnen un número suficiente de ellas. La idea fue introducida por primera vez por Adi Shamir [17] en 1979.

El propósito principal de estos esquemas es aumentar la seguridad de la información confidencial. Por ejemplo, en una organización, un esquema de reparto de secretos puede utilizarse para asegurar que ningún individuo tenga acceso completo a una información crítica sin la colaboración de otros. Esto es particularmente útil en escenarios donde la seguridad y la integridad de los datos son cruciales, como en la gestión de claves criptográficas, control de acceso en sistemas distribuidos, y procesos de autenticación robusta.

A grandes rasgos, un esquema de reparto de secretos típico funciona de la siguiente manera: un secreto S se divide en n partes diferentes. Cuando r de esas partes se reúnen, el secreto podrá ser recuperado. Por el contrario, si contamos con t o menos partes del secreto, este quedará completamente indeterminado. Los valores r y t se denominan umbrales, y su valor será objeto de estudio en esta memoria. Este tipo de esquemas permite diseñar sistemas flexibles y seguros donde la redundancia juega un papel crucial en la recuperación del secreto. Uno de los esquemas más conocidos es el esquema de Shamir, que utiliza la interpolación de polinomios para dividir el secreto y garantizar su reconstrucción solo cuando se poseen suficientes partes.

La aplicación de los esquemas de reparto de secretos va más allá de la mera protección de datos. Estos métodos se emplean en diversas áreas como el almacenamiento distribuido, sistemas de voto electrónico, y en la protección de propiedad intelectual. Además, son una herramienta clave en la construcción de protocolos criptográficos más complejos, tales como los protocolos de firma digital distribuida y la computación segura multipartita.

En el primer capítulo se presentarán los resultados y conceptos necesarios para el desarrollo de la memoria. Partiremos dando unas definiciones de álgebra básica para introducir, a continuación, los cuerpos finitos, que supo-

nen la base sobre la cual construiremos los esquemas de reparto de secretos. Posteriormente introduciremos las bases de la teoría de la información, definiendo e interpretando el concepto de entropía y mostrando algunas de sus propiedades fundamentales. El concepto de entropía será de utilidad posteriormente, pues a partir de ella expresaremos la información obtenida por un conjunto de participantes acerca del secreto. Ha sido por tanto necesario incluir tras cada resultado una breve interpretación en términos de la incertidumbre. Para terminar con este primer capítulo, repasaremos la teoría de los códigos correctores de errores y de los códigos Reed-Solomon, de importancia capital en esta memoria.

En el segundo capítulo se define formalmente el esquema de reparto de secretos que desarrollaremos en esta memoria, basado en dos códigos lineales encajados con umbrales r y t. En el teorema 2.1 calcularemos en términos de la información mutua y la entropía condicionada la información filtrada a un conjunto de partes; esto es, la cantidad de información a la que accede un grupo de participantes. Seremos capaces también, al final de este capítulo, de establecer unos valores para r y t en función de los pesos relativos de Hamming generalizados y de la distancia mínima.

El siguiente capítulo tiene por objetivo particularizar los resultados anteriores a los códigos MDS. Además, seremos capaces de demostrar la seguridad del esquema de reparto de secretos de Shamir, pues veremos que es equivalente a un esquema de reparto basado en códigos Reed-Solomon encajados. En el teorema 3.2 estudiaremos cómo se ven modificadas las cotas del capítulo segundo cuando se trata con códigos MDS.

Por último, y con el objetivo de estudiar nuestro esquema de reparto de secretos en otras familias de códigos, introduciremos los códigos Reed-Muller. Calcularemos sus parámetros fundamentales, como la dimensión y la distancia mínima, y veremos que un código Reed-Muller dual vuelve a ser un código Reed-Muller. Finalmente, particularizaremos las cotas del capítulo segundo para los códigos Reed-Muller.

Capítulo 1

Preliminares

A lo largo de esta sección, se introducirán los conceptos clave que serán de utilidad a lo largo de esta memoria. Empezaremos definiendo las estructuras algebraicas con las que trabajaremos, enunciando sus propiedades y los principales resultados, pues suponen la base sobre la cual construiremos el esquema de reparto de secretos.

Por el contrario, la Teoría de la Información no se imparte en ninguna de las asignaturas obligatorias del grado, por lo que se presentarán las nociones clave también en este capítulo. Aspectos tales como la entropía y la información mutua proporcionan un conocimiento valioso del mensaje a estudiar, por lo que su definición y los principales resultados estarán muy presentes a lo largo de la memoria.

En la última sección se hará un breve resumen de los aspectos fundamentales de la teoría de códigos correctores y en especial se hablará del código de Reed-Solomon, que será en el que nos centraremos en un capítulo posterior. Se definirá lo que es un código y su dual, así como sus matrices generatriz y de control, entre otros conceptos.

1.1. Conceptos algebraicos

En esta breve sección se presentará el marco algebraico sobre el que se desarrollará la memoria. Fundamentalmente, nos centraremos en los cuerpos finitos. No obstante, en esta sección se muestran conceptos y resultados previos que serán de utilidad más adelante. Las definiciones de las principales estructuras algebraicas, que damos por conocidas, así como los principales resultados se pueden encontrar en [4], [10] y [13].

Definición 1.1. Sea A un anillo conmutativo y $a \in A$ un elemento no nulo. Diremos que a es un *divisor de cero* si existe un elemento no nulo $b \in A$ tal

que $ab = 0$.

Definición 1.2. Sea A un anillo conmutativo y sean $a, b \in A$. Entonces A es un *dominio de integridad* si $ab = 0$ implica que $a = 0$ o $b = 0$ para cada $a, b \in A$. En otras palabras, A es un dominio de integridad si no tiene elementos divisores de cero.

El siguiente resultado será de utilidad más adelante, y se deduce de la definición de dominio de integridad.

Teorema 1.1. *Todo dominio de integridad finito es un cuerpo.*

Demostración. Sea $A = \{a_1, a_2, \ldots, a_n\}$ un anillo de integridad finito. Sea $a \in A$ distinto de cero. Multipliquemos cada elemento de A por a, de forma que tendremos aa_i para $1 \leq i \leq n$. Todos estos elementos son distintos. En efecto, supongamos que $aa_i = aa_j$, entonces $a(a_i - a_j) = 0$. Como estamos en un dominio de integridad y $a \neq 0$, entonces $a_i - a_j = 0$, lo que implica que $a_i = a_j$. Por tanto, todo elemento de A, y en particular 1_A, es de la forma aa_i, para algún i con $1 \leq 1 \leq n$. Como también $a_i a = aa_i = 1$, entonces a_i es el inverso multiplicativo de a. Por lo tanto, los elementos no nulos de A forman un grupo multiplicativo, lo que quiere decir que A es un cuerpo. □

Definición 1.3. Sea A un anillo conmutativo. Un *ideal* de A es un subconjunto $I \subset A$ no vacío y cerrado para combinaciones lineales con coeficientes en A. Esto es, dados los elementos $a_1, a_2, \ldots, a_n \in I$, entonces $r_1 \cdot a_1 + r_2 \cdot a_2 + \ldots + r_n \cdot a_n$ también pertenece a I si los coeficientes $r_1, r_2, \ldots, r_n$ están en A. Si existe un elemento $b \in I$ tal que $I = (b) \equiv \{a \cdot b : a \in A\}$, entonces decimos que el ideal es *principal*. Si A es un dominio de integridad en el que todo ideal es principal, entonces A es un *dominio de ideales principales*.

Dado un ideal I del anillo conmutativo A, podremos definir porciones de A llamadas *clases de equivalencia* módulo I. Dos elementos $c, d \in A$ serán congruentes módulo I si $c - d \in I$. La clase de un elemento $a \in A$ será representada como $[a] = a + I$, ya que está formada por elementos de A de la forma $a + b$, para algún $b \in I$. Se puede probar, siguiendo la definición anterior, que el conjunto de clases de A módulo I forman un anillo conmutativo, llamado *anillo cociente*, para las operaciones:

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I)(b + I) = ab + I.$$

Por ejemplo, considerando el anillo de los números enteros $\mathbb{Z}$ y $n \in \mathbb{Z}$, los elementos del anillo $\mathbb{Z}/(n)$ son: $[0], [1], \ldots, [n-1]$ o equivalentemente $0 + (n), 1 + (n), \ldots, n - 1 + (n)$.

Definición 1.4. Sea A un anillo. Un elemento $p \neq 0$ es *primo* si p no es una unidad y cumple la siguiente condición: si p divide al producto ab, con $a, b \in A$, entonces p divide a a o p divide a b.

Teorema 1.2. *El anillo $\mathbb{Z}/(p)$, siendo p un número primo, es un cuerpo.*

Demostración. Basta probar, por el teorema 1.1 que $\mathbb{Z}/(p)$ es un dominio de integridad. Sean $[a], [b] \in \mathbb{Z}/(p)$. Entonces $[a][b] = [ab] = 0$ si y solo si $ab = kp$ para un entero k. Como p es primo, p divide a ab si y solo si p divide a a o p divide a b. Por lo tanto, o bien $[a] = 0$ o bien $[b] = 0$. Por lo tanto, $\mathbb{Z}/(p)$ no contiene divisores de cero y es un dominio de integridad. □

Definición 1.5. Sean A y B dos anillos y $f : A \longrightarrow B$ una aplicación. Diremos que f es un *homomorfismo* si conserva las operaciones ($f(a + b) = f(a) + f(b)$ y $f(ab) = f(a)f(b)$) y si conserva el elemento unidad ($f(1_A) = 1_B$). Si la aplicación fuese biyectiva, f sería un *isomorfismo* de anillos.

Definición 1.6. Sea A un anillo. Sea $\phi : \mathbb{Z} \longrightarrow A$ el único homomorfismo de anillos que lleva 1 en 1_A. Puesto que $\mathbb{Z}$ es dominio de ideales principales, existe n no negativo tal que $\ker(\phi) = (n)$. A dicho n se le conoce como la *característica de A*.

Teorema 1.3. *Todo cuerpo finito F tiene característica p prima.*

Demostración. Sea n la característica de F. Si $n = rq$, con $1 < r < q$, entonces para todo $a \in A$ se tiene que $0 = na = rqa$. De este modo, r y q serían divisores de cero en el cuerpo F, que por definición, es dominio de integridad. Por lo tanto, la característica de F debe ser o 0 o un número primo. Sin embargo, al tratarse F de un cuerpo finito, su característica no puede ser 0. En efecto, atendiéndonos a la definición 1.6, si $n = 0$, ϕ sería inyectiva, y como $\phi(\mathbb{Z}) \subset F$, F contendría un subconjunto de cardinal infinito, lo cual es absurdo. Por tanto, todo cuerpo finito tiene característica p prima. □

Lema 1.1. *Sea A un anillo conmutativo de característica prima p. Entonces*

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n},$$

con $a, b \in A$ y $n \in \mathbb{N}$.

Demostración. Teniendo en cuenta que, para cada $i \in \mathbb{Z}$ con $0 < i < p$,

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i} \equiv 0 \mod p,$$

se sigue del binomio de Newton que

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p.$$

Aplicando inducción sobre n se obtiene el resultado pedido. Además, sabiendo que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, se sigue que

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

de donde $(a-b)^{p^n} = a^{p^n} - b^{p^n}$ □

Si bien a lo largo de la memoria se trabajará con polinomios sobre cuerpos finitos, no se expondrán en detalle las definiciones más básicas. Para ello, se recomienda recurrir a [4] y [10].

Con las operaciones suma y producto, el conjunto de polinomios sobre un anillo A presenta, a su vez, estructura de anillo, y se denota como $A[x]$. Los polinomios de grado 0, conocidos como constantes, también forman parte de $A[x]$, de modo que $A \subset A[x]$.

Definición 1.7. Sea F un cuerpo y $F[x]$ su anillo de polinomios asociado. Un polinomio $p \in F[x]$ es *irreducible* sobre F (o *irreducible* en $F[x]$) si p tiene grado positivo y $p = bc$, con $b, c \in F[x]$ implica que o b o c es un polinomio constante.

En el estudio del álgebra abstracta, las extensiones de cuerpos juegan un papel fundamental en la comprensión de las estructuras algebraicas. Comenzaremos por definir qué es una extensión de cuerpos algebraicos y nos sumergiremos en el estudio de sus propiedades básicas.

Definición 1.8. Sea F un cuerpo. Un subconjunto K de F que tiene estructura de cuerpo con las operaciones de F es un *subcuerpo* de F. Diremos también que F es una *extensión* de K y lo representaremos como $F|K$. Además, si $K \neq F$, diremos que K es un *subcuerpo propio* de F.

Definición 1.9. Sea $F|K$ una extensión de cuerpos. El *grado de la extensión* es la dimensión de F como espacio vectorial sobre K. Se representa como $[F : K]$. Diremos que la extensión es finita si lo es su grado.

Definición 1.10. Un cuerpo F que no contiene subcuerpos propios se llama *cuerpo primo*. Todo cuerpo finito de orden primo es primo. La intersección de todos los subcuerpos de F es el *subcuerpo primo* de F.

El cuerpo de los números racionales, $\mathbb{Q}$, por ejemplo, es un cuerpo primo. Veremos ahora un resultado que será de utilidad en la caracterización de los cuerpos finitos.

Teorema 1.4. *El subcuerpo primo de un cuerpo F es o bien isomorfo a $\frac{\mathbb{Z}}{(p)}$, si F tiene característica prima p, o bien a $\mathbb{Q}$, si la característica de F es 0.*

Definición 1.11. Sea K un cuerpo, $f \in K[x]$ un polinomio de grado positivo y F una extensión de K. Entonces se dice que f se *descompone completamente* en F si existen elementos $\alpha_1, \alpha_2, ..., \alpha_r \in F$ tales que

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r),$$

siendo a el coeficiente principal de f. Diremos que F es el *cuerpo de descomposición* de f si es el cuerpo más pequeño que contiene a K y a las raíces de f, es decir

$$F = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Además, el cuerpo de descomposición de un polinomio será único salvo isomorfismos.

1.2. Cuerpos finitos

Se presentarán en esta sección las principales propiedades acerca de los cuerpos finitos. Para escribir los resultados y sus demostraciones, se ha tomado como referencia [10].

Lema 1.2. *Sea F un cuerpo finito, y sea K un subcuerpo de F con q elementos. Entonces F tiene q^m elementos, donde $m = [F : K]$.*

Demostración. Como F es finito y es un espacio vectorial sobre K, será un espacio vectorial de dimensión finita sobre K. Si $[F : K] = m$, existe una base de F como espacio vectorial sobre K formada por m elementos, $b_1, b_2, \ldots, b_m$. Todo elemento de F puede ser escrito en términos de la base como $a_1b_1 + a_2b_2 + \cdots + a_mb_m$, con $a_1, a_2, \ldots, a_m \in K$. Como los a_i pueden tomar q valores diferentes, entonces F tiene exactamente q^m elementos. □

Teorema 1.5. *Sea F un cuerpo finito. Entonces F tiene p^n elementos, donde p es la característica prima de F y n es el grado de F sobre su subcuerpo primo.*

Demostración. De acuerdo con el teorema 1.3, por ser F finito tiene característica prima p. Por lo tanto, en virtud del teorema 1.4, el subcuerpo primo de F es isomorfo a $\frac{\mathbb{Z}}{(p)}$, que contiene p elementos. El resto se deduce aplicando el lema 1.2. □

El siguiente teorema, útil en la prueba de los resultados posteriores, no será demostrado en este trabajo. Puede encontrarse en el Teorema 1.46 de [10].

Teorema 1.6. *El grupo multiplicativo F^* de un cuerpo finito con q elementos es cíclico. Un generador de F^* es un elemento primitivo de F.*

Lema 1.3. *Si F es un cuerpo finito con q elementos, entonces todo $a \in F$ cumple que $a^q = a$.*

Demostración. Si $a = 0$, el resultado es evidente. Supongamos $a \in F \setminus \{0\} = F^*$. Del teorema 1.6, se conoce que los elementos de F^* forman un grupo multiplicativo cíclico de orden $q - 1$. Por tanto, $a^{q-1} = 1$, y multiplicando a ambos lados de la igualdad por a, se deduce que $a^q = a$. □

El siguiente lema será útil para demostrar posteriormente el teorema de existencia y unicidad de cuerpos finitos.

Lema 1.4. *Si F es un cuerpo finito con q elementos y K es un subcuerpo de F, entonces el polinomio $x^q - x \in K[x]$ factoriza en $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a),$$

y F es un cuerpo de descomposición de $x^q - x$ sobre K.

Demostración. El polinomio $x^q - x$ de grado q tiene como mucho q raíces en F. Por el lema 1.3, conocemos estas q raíces, que son los elementos de F. Por lo tanto, este polinomio se descompone en F siguiendo la fórmula del enunciado, y no puede descomponerse completamente en ningún otro cuerpo más pequeño. □

Teorema 1.7. *(Existencia y unicidad de cuerpos finitos). Para cada primo p y para cada entero positivo n existe un cuerpo finito con p^n elementos. Además, cualquier cuerpo finito con $q = p^n$ elementos es isomorfo al cuerpo de descomposición del polinomio $x^q - x$ sobre $\mathbb{F}_p$.*

Demostración. (Existencia). Para $q = p^n$ se considera el polinomio en $\mathbb{F}_p[x]$ $f(x) = x^q - x$, y sea F su cuerpo de descomposición sobre $\mathbb{F}_p$. Como su derivada, $f'(x) = qx^{q-1} - 1 = -1$ en $\mathbb{F}_p[x]$, $f(x)$ tiene q raíces distintas (si $f(x)$ tuviese raíces múltiples, también serían raíces de $f'(x) = -1$, y es obvio que $f'(x)$ no tiene raíces). Sea $S = \{a \in F : a^q - a = 0\}$. Entonces S es un subcuerpo de F, ya que: (i) S contiene al 0 y al 1; (ii) si $a, b \in S$, es claro que, por el lema 1.1 $(a - b)^q = a^q - b^q = a - b$. Luego $a - b \in S$; (iii) para $a, b \in S$ con $b \neq 0$, se sigue que $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, por tanto $ab^{-1} \in S$. Además, $f(x)$ debe descomponerse totalmente en S puesto que S contiene todas sus raíces. En consecuencia, $F = S$, y como S tiene q elementos (las q raíces de $f(x)$) F es un cuerpo finito de $q = p^n$ elementos.

(Unicidad). Sea F un cuerpo finito con $q = p^n$ elementos. Por el teorema 1.5, F tiene característica prima p, de modo que contiene a $\mathbb{F}_p$ como subcuerpo. Se sigue del lema anterior que F es un cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$, y como el cuerpo de descomposición de un polinomio es único salvo isomorfismos (se puede comprobar en [4] o [10]), F es único. □

Definición 1.12. Sea $p \in \mathbb{Z}$ un número primo. Entonces $\mathbb{F}_p \equiv \mathbb{Z}/(p)$ es el *cuerpo finito de orden p.*

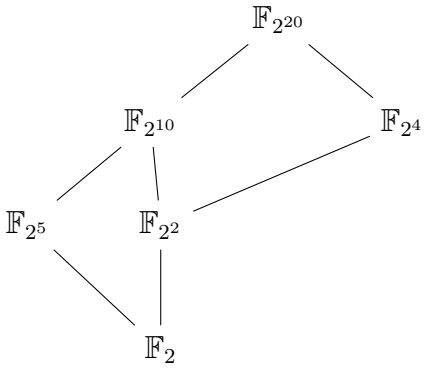
El teorema 1.7 justifica que se trate con *el* cuerpo finito de $q = p^n$ elementos o *el* cuerpo finito de orden q. Denotaremos, de ahora en adelante, este cuerpo como $\mathbb{F}_q$.

Teorema 1.8. *Sea $\mathbb{F}_q$ el cuerpo finito con $q = p^n$ elementos. Entonces todo subcuerpo de $\mathbb{F}_q$ tiene orden p^m, donde m es un divisor positivo de n. Recíprocamente, si m es un entero positivo que divide a n, entonces existe un único subcuerpo de $\mathbb{F}_q$ con p^m elementos.*

Demostración. Claramente, si K es un subcuerpo de $\mathbb{F}_q$ debe tener orden p^m para $m \leq n$. El lema 1.2 prueba que $q = p^n$ debe ser una potencia de p^m, esto es, existe $r \in \mathbb{N}$ tal que $(p^m)^r = p^{mr} = p^n$, luego m divide a n.

Recíprocamente, si m es un divisor positivo de n, entonces $p^m - 1$ divide a $p^n - 1$, de modo que $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$ en $\mathbb{F}_p[x]$. De este modo, todas las raíces de $x^{p^m} - x$ son raíces de $x^{p^n} - x$ y pertenecen a $\mathbb{F}_q$. Por lo tanto, $\mathbb{F}_q$ contiene al cuerpo de descomposición de $x^{p^m-1} - 1$ sobre $\mathbb{F}$ que será de orden p^m por lo visto en el teorema 1.7. Dicho subcuerpo es único. En efecto, si hubiese dos subcuerpos de orden p^m en $\mathbb{F}_q$, entonces el polinomio $x^{p^m} - x$ tendría más de p^m raíces distintas en $\mathbb{F}_{p^m}$, lo cual es absurdo. □

Ejemplo 1.1. Los subcuerpos de $F_{2^{20}}$ vendrán dados por los divisores positivos de 20, esto es: $1, 2, 4, 5$ y 10. Las relaciones entre los subcuerpos vienen dadas por el siguiente diagrama:



1.3. Teoría de la información

En este capítulo se introducirán los conceptos más básicos de la Teoría de la Información, así como sus resultados más destacados, que serán de ayuda en el desarrollo teórico de esta memoria. En particular, se expondrán las nociones de *entropía* e *información mutua*, así como sus relaciones e interpretaciones.

El concepto de *entropía* da cuenta de la incertidumbre sobre una variable aleatoria, y se puede encontrar en diversos ámbitos científicos, como por ejemplo, en la Termodinámica. Sea X una variable aleatoria discreta sobre un conjunto finito $\mathscr{X}$, que llamaremos *alfabeto*, que sigue una función de probabilidad definida por $p(x) = Pr\{X = x\}, x \in \mathscr{X}$. Por simplificar, $p(x) \equiv p_X(x)$, de modo que $p(x)$ y $p(y)$ se referirán a dos variables aleatorias diferentes, X e Y, cada una con función de probabilidad diferente. Las principales referencias de esta sección se pueden encontrar en [3] y [12].

Definición 1.13. Sea X una variable aleatoria discreta tal que $X \sim p(x)$. La *entropía* $H(X)$ de X se define como

$$H(X) = -\sum_{x \in \mathscr{X}} p(x) \log p(x).$$

Generalmente, el logaritmo que aparece en la fórmula es en base 2, y la entropía se expresa en *bits*. Puesto que $x \log x \longrightarrow 0$ cuando $x \longrightarrow 0$ por continuidad, definimos que $0 \log p(0) = 0$, lo cual es lógico: los sucesos imposibles no modifican la entropía.

Si la base del logaritmo es b, denotaremos a la entropía de la variable aleatoria X como $H_b(X)$. Si la base del logaritmo es e las unidades de la entropía son *nats*. Nótese que la entropía no depende de los valores que toma la variable aleatoria X, sino de las probabilidades.

Es apropiado, de cara al tratamiento con esquemas de reparto de secretos, dar una interpretación de la entropía. Como se ha mencionado anteriormente, dará cuenta de la incertidumbre sobre una variable aleatoria antes de realizarse una medida de ésta. Otra forma de entender el concepto de entropía es el aprendizaje recibido de la variable aleatoria después de obtenerse un resultado. A continuación se muestran dos ejemplos que tratan sobre situaciones opuestas y que ponen de manifiesto estas interpretaciones.

Ejemplo 1.2. Supongamos que tenemos una variable aleatoria X sobre el conjunto $\{a, b, c, d\}$ tal que $p(a) = 1$ y $p(b) = p(c) = p(d) = 0$. En este ejemplo sabemos de antemano que el único suceso posible es a, mientras que b, c y d no ocurrirán jamás. Por tanto

$$H(X) = -\log(1) - 0 \cdot \log(0) - 0 \cdot \log(0) - 0 \cdot \log(0) = -0 - 0 - 0 - 0 = 0.$$

Lógicamente, la incertidumbre sobre la variable X es nula, pues conocemos, antes de realizarse la medida, el resultado que se obtendrá.

Ejemplo 1.3. Por el contrario, supongamos que X sigue una distribución de probabilidad uniforme sobre el conjunto $\{a, b, c, d\}$ de modo que $p(a) = p(b) = p(c) = p(d) = 1/4$. La entropía asociada será

$$H(X) = -\frac{1}{4}\log(\frac{1}{4}) - \frac{1}{4}\log(\frac{1}{4}) - \frac{1}{4}\log(\frac{1}{4}) - \frac{1}{4}\log(\frac{1}{4}) = 2 \text{ bits.}$$

Se puede observar el contraste con el ejemplo anterior. Ahora, a priori, no hay ningún resultado favorecido: todos pueden ocurrir con la misma probabilidad. Por tanto, la incertidumbre antes de realizarse la medida es total.

Estos dos ejemplos pueden resumirse, de un modo más general, de la siguiente manera. Sea X una variable aleatoria que puede dar como resultado 1 con probabilidad p y 0 con probabilidad $1 - p$. Por definición,

$$H(X) = -p\log(p) - (1-p)\log(1-p) \equiv H(p).$$

En la siguiente figura, donde se representa $H(p)$ frente a p, se puede comprobar lo explicado en los ejemplos. Si $p = 1$ o $p = 0$, la entropía será 0, es decir, no hay incertidumbre en la medida, pues se conoce el resultado antes de realizarse la experiencia. Por el contrario, la entropía será máxima cuando $p = 1/2$, esto es, cuando X sigue una distribución de probabilidad uniforme.

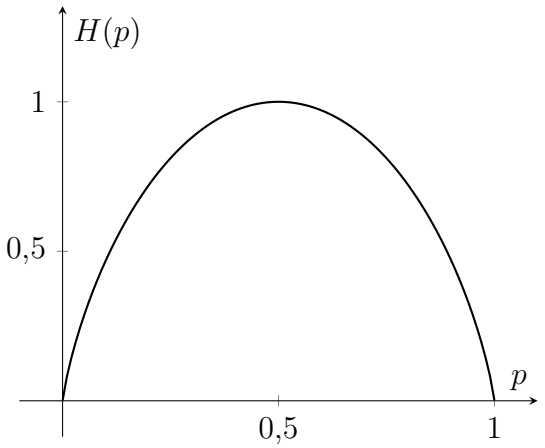


Figura 1.1: Valor de la entropía en función de p.

Otro modo de entender la entropía es como el número de bits necesarios para representar un número determinado de objetos. Esto es, el número promedio de bits en el que se puede almacenar información. El siguiente ejemplo, que se encuentra en [1], da una idea bastante clara de este concepto.

Ejemplo 1.4. Supongamos una variable aleatoria X que puede tomar 8 posibles valores, cada uno con probabilidad 1/8. La entropía de esta variable es

$$H(X) = -8 \cdot \frac{1}{8} \log(\frac{1}{8}) = 3 \text{ bits.}$$

En este caso, si quisiéramos transmitir la información de la variable X, podríamos hacerlo utilizando un número de 3 bits. Por el contrario, si cada uno de los valores que puede tomar la variable aleatoria se alcanzase con probabilidades $A = \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{64}, \frac{1}{64}, \frac{1}{64}, \frac{1}{64}\}$, la entropía sería

$$H(X) = \sum_{x \in A} -x \log x = 2 \text{ bits.}$$

Se puede comprobar cómo la distribución uniforme alcanza un valor mayor de la entropía que la no uniforme. En este caso, podemos sacar partido de que la distribución de probabilidades es no uniforme para transmitir la información a un receptor asignando a los eventos más probables palabras más cortas, a expensas de códigos más largos para los eventos menos probables, con la esperanza de obtener una longitud de código promedio más corta.

Si miramos la entropía como el grado de desorden de un sistema, como se hace en la Física Estadística, aquel con mayor entropía (todos los posibles resultados son igual de probables), es el más desordenado.

Definición 1.14. Sea X una variable aleatoria discreta tal que $X \sim p(x)$. Se define la *esperanza* o *valor esperado* de la variable aleatoria $g(X)$ como

$$E_p[g(X)] \equiv E[g(X)] = \sum_{x \in \mathscr{X}} g(x)p(x).$$

Obsérvese que si $g(X) = \log \frac{1}{p(X)}$, la entropía de X puede reescribirse como

$$H(X) = E\left[\log \frac{1}{p(X)}\right].$$

Directamente de la definición se obtienen una serie de resultados que dan cuenta de las principales propiedades de la entropía.

Lema 1.5. *Sea X una variable aleatoria discreta tal que $X \sim p(x)$. Entonces $H(X) \geq 0$.*

Demostración. Para todo $x \in \mathscr{X}$ se sigue que $0 \leq p(x) \leq 1$, de modo que $\log p(x) \leq 0$. Por lo tanto, $-\log p(x) \geq 0$. □

Lema 1.6. $H_b(X) = (\log_b a) H_a(X)$.

Demostración. Siguiendo las propiedades del cambio de base de los logaritmos, claramente $\log_b p = \log_b a \log_a p$. □

Ejemplo 1.5. Sea X una variable aleatoria sobre el conjunto discreto $\{a, b, c\}$ que toma los siguientes valores:

x	$P(X = x)$
a	$3/10$
b	$5/10$
c	$2/10$

La entropía de X será:

$$H(X) = -\left(\frac{3}{10}\log_2\frac{3}{10} + \frac{5}{10}\log_2\frac{5}{10} + \frac{2}{10}\log_2\frac{2}{10}\right) = 1,49\ldots$$

Se definen ahora diferentes conceptos para el par de variables aleatorias discretas X e Y.

Definición 1.15. La *entropía conjunta* $H(X, Y)$ de dos variables aleatorias discretas (X, Y) con función de distribución de probabilidad conjunta $p(x, y)$ se define como

$$H(X, Y) = -\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x, y)\log p(x, y) = -E[\log p(X, Y)].$$

Como se hizo en el caso de la entropía de una sola variable aleatoria, podemos generalizar su interpretación al caso de una distribución conjunta de variables aleatorias como la cantidad de incertidumbre que existe en dos variables aleatorias conjuntamente.

Definición 1.16. Si $(X, Y) \sim p(x, y)$, la *entropía condicional* $H(Y|X)$ se define como

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathscr{X}} p(x)H(Y|X = x) \\ &= -\sum_{x\in\mathscr{X}} p(x)\sum_{y\in\mathscr{Y}} p(y|x)\log p(y|x) \\ &= -\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x, y)\log p(y|x) \\ &= -E\left[\log p(Y|X)\right]. \end{aligned}$$

En otras palabras, la entropía condicional $H(Y|X)$ cuantifica la cantidad de información necesaria para describir el resultado de una variable aleatoria Y conocido el valor de X.

Nota 1.1. *Obsérvese que* $H(Y|X) \neq H(X|Y)$.

El siguiente resultado es de importancia capital en la Teoría de la Información. Si bien será enunciado en un primer momento para dos variables aleatorias, es posible generalizarlo para un conjunto mayor, como veremos después.

Teorema 1.9. *(Regla de la cadena). Sean* X *e* Y *dos variables aleatorias discretas que siguen una función de probabilidad conjunta* $p(x, y)$*. Entonces*

$$H(X, Y) = H(X) + H(Y|X).$$

Demostración. Haciendo uso de las definiciones y sabiendo que

$$p(x, y) = p(x)p(y|x),$$

y que $\sum_{y \in \mathscr{Y}} p(x, y) = p(x)$, se sigue que:

$$\begin{aligned} H(X, Y) &= -\sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x, y) \log p(x, y) \\ &= -\sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x, y) \log p(x)p(y|x) \\ &= -\sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x, y) \log p(x) - \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x, y) \log p(y|x) \\ &= -\sum_{x \in \mathscr{X}} p(x) \log p(x) - \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x, y) \log p(y|x) \\ &= H(X) + H(Y|X). \end{aligned}$$

De manera equivalente, y utilizando el formalismo de la esperanza, tomando el valor esperado a ambos lados de la siguiente ecuación

$$\log p(X, Y) = \log p(X) + \log p(Y|X),$$

se obtendría análogamente el resultado pedido. □

En efecto, si primero obtenemos el resultado de X, habremos ganado $H(X)$ bits de información. De modo que si queremos describir el estado total del sistema dado por las variables (X, Y) conjuntamente, será necesario obtener el valor de Y conocido X, que después de ser medido proporcionará $H(Y|X)$ bits de información. Este resultado se puede generalizar a más variables aleatorias, así como su interpretación.

Corolario 1.1. $H(X,Y|Z) = H(X|Z) + H(Y|X,Z)$.

Demostración. Se sigue la misma cadena de igualdades que en el teorema anterior para llegar al resultado. □

Nota 1.2. *Es claro que* $H(X) + H(Y|X) = H(Y) + H(X|Y)$*, lo cual da cuenta de la simetría de la entropía conjunta. De lo anterior deducimos que* $H(X)-H(X|Y) = H(Y)-H(Y|X)$*, esto es, lo que se reduce la incertidumbre de* X *una vez conocido* Y *es igual a lo que se reduce la incertidumbre de* Y *una vez conocido* X*.*

Definición 1.17. Supongamos dos variables aleatorias discretas X e Y cuya ley de probabilidad conjunta viene dada por $p(x,y)$ y con funciones de probabilidad marginal $p(x)$ y $p(y)$. La *información mutua* $I(X;Y)$ se define como

$$I(X;Y) = \sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}.$$

El siguiente lema dará cuenta del significado intuitivo de la información mutua. De la definición observamos que $I(X;Y)$ mide la información que X e Y comparten. El siguiente lema afirma que la información mutua mide en cuánto el conocimiento de una variable reduce nuestra incertidumbre sobre la otra.

Lema 1.7. *En las condiciones anteriores,* $I(X;Y) = H(X) - H(X|Y)$*.*

Demostración. Sin más que aplicar las definiciones, se sigue que:

$$\begin{aligned}
I(X;Y) &= \sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \\
&= \sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x,y)\log\frac{p(x|y)}{p(x)} \\
&= -\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x,y)\log p(x) + \sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x,y)\log p(x|y) \\
&= -\sum_{x\in\mathscr{X}} p(x)\log p(x) - \left(-\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} p(x,y)\log p(x|y)\right) \\
&= H(X) - H(X|Y).
\end{aligned}$$

□

De este lema se deduce, por simetría, que $I(X;Y) = H(Y) - H(Y|X)$. Esto quiere decir que X proporciona tanta información de Y como Y de X. También, aplicando la regla de la cadena, se puede observar que $I(X;Y) = H(X)+H(Y)-H(X,Y)$. Por último, si $Y = X$, entonces $I(X;X) = H(X)-H(X|X) = H(X)$. Debido a esto, en muchas ocasiones a la entropía se le conoce como *autoinformación.*

El siguiente diagrama mostrará la relación entre $H(X), H(Y), H(X,Y)$, $H(Y|X), H(X|Y)$ e $I(X;Y)$. Obsérvese que $I(X;Y)$ corresponde a la intersección de la información contenida en X con la información contenida en Y.

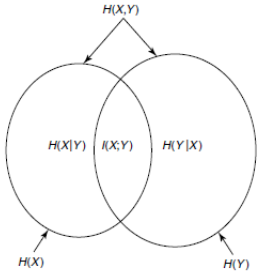


Figura 1.2: Relaciones entre las entropías y la información mutua de dos variables.

Se estudiarán ahora las propiedades de la información mutua y de la entropía para un conjunto de variables aleatorias. En particular, se probará la regla de la cadena generalizada de la entropía y se enunciará un resultado similar para la información mutua.

Teorema 1.10. *(Regla de la cadena para la entropía). Sean $X_1, X_2, ..., X_n$ variables aleatorias que siguen la función de probabilidad $p(x_1, x_2, ..., x_n)$. Entonces*

$$H(X_1, X_2, ..., X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1}, ..., H_1).$$

Demostración. Por inducción, es claro que

1. Si $n = 2$, $H(X_1, X_2) = H(X_1) + H(X_2|X_1)$ por la regla de la cadena.

2. Si $n = 3$, $H(X_1, X_2, X_3) = H(X_1)+H(X_2, X_3|X_1) = H(X_1)+H(X_2|X_1)+H(X_3|X_2, X_1)$.

3. Asumiendo el resultado cierto para $n-1$ y razonando como en el caso $n=3$, se sigue que:

$$\begin{aligned} H(X_1, X_2, \ldots, X_n) &= H(X_1) + H(X_2, X_3, \ldots, X_n|X_1) \\ &= H(X_1) + H(X_2|X_1) + \cdots + H(X_n|X_{n-1}, \ldots, X_1). \end{aligned}$$

□

Definición 1.18. La *información mutua condicional* de dos variables X e Y con respecto a una variable Z dada se define como

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z).$$

Del mismo modo que para la entropía, existe una regla de la cadena para la información mutua.

Teorema 1.11. *(Regla de la cadena para la información mutua).*

$$I(X_1, X_2, ..., X_n; Y) = \sum_{i=1}^{n} I(X_i; Y|X_{i-1}, X_{i-2}, ..., X_1).$$

Demostración. El resultado pedido se obtiene aplicando el lema 1.7 y el teorema 1.10.

$$\begin{aligned} I(X_1, X_2, ..., X_n; Y) &= H(X_1, X_2, ..., X_n) - H(X_1, X_2, ..., X_n|Y) \\ &= \sum_{i=1}^{n} H(X_i|X_{i-1}, ..., X_1) - \sum_{i=1}^{n} H(X_i|X_{i-1}, ..., X_1, Y) \\ &= \sum_{i=1}^{n} (H(X_i|X_{i-1}, ..., X_1) - H(X_i|X_{i-1}, ..., X_1, Y)) \\ &= \sum_{i=1}^{n} I(X_i; Y|X_1, X_2, ..., X_{i-1}). \end{aligned}$$

□

El siguiente lema, que no probaremos, será muy útil en la demostración de los dos siguientes resultados.

Lema 1.8. *La función* $\log_2$ *verifica:*

$$\log_2 z < (z-1)\log_2 e \text{ si } z > 0,\ z \neq 1.$$

$$\log_2 z = (z-1)\log_2 e \text{ si } z = 1.$$

Teorema 1.12. *Sea X una variable aleatoria discreta tal que $X \sim p(x)$ para todo $x \in \mathscr{X}$. Entonces $H(X) \leq \log_2 |\mathscr{X}|$, donde $|\mathscr{X}|$ representa el número de elementos del alfabeto $\mathscr{X}$. La igualdad se alcanza si y solo si X sigue una ley de probabilidad uniforme.*

Demostración. Probaremos que $H(X) - \log_2 |\mathscr{X}| \leq 0$. Atendiendo a las definiciones, se observa que:

$$\begin{aligned} H(X) - \log_2 |\mathscr{X}| &= \sum_{x \in \mathscr{X}} p(x) \log_2 \frac{1}{p(x)} - \log_2 |\mathscr{X}| \sum_{x \in \mathscr{X}} p(x) \\ &= \sum_{x \in \mathscr{X}} p(x) \log_2 \frac{1}{p(x)|\mathscr{X}|}. \end{aligned}$$

Aplicando el lema 1.8 a $z = \frac{1}{p(x)|\mathscr{X}|}$, se sigue que:

$$\begin{aligned} H(X) - \log_2 |\mathscr{X}| &\leq \log_2 e \sum_{x \in \mathscr{X}} p(x) \left(\frac{1}{p(x)|\mathscr{X}|} - 1 \right) \\ &\leq \log_2 e \left(\sum_{x \in \mathscr{X}} \frac{1}{|\mathscr{X}|} - \sum_{x \in \mathscr{X}} p(x) \right) \\ &= \log_2 e (1 - 1) = 0. \end{aligned}$$

La igualdad se dará únicamente si $\frac{1}{p(x)|\mathscr{X}|} = 1$, esto es, si $p(x) = \frac{1}{|\mathscr{X}|}$. En otras palabras, la igualdad se alcanza únicamente si X sigue una ley de probabilidad uniforme. □

De la definición de información mutua $I(X;Y)$, es claro que siempre aprenderemos algo de una variable aleatoria conocida la otra, salvo en el caso en que estas sean independientes. En ese caso, conocer Y no aporta ningún tipo de aprendizaje sobre X. El siguiente resultado afirma que $I(X;Y)$ será siempre un valor positivo salvo que X e Y sean independientes, en cuyo caso $I(X;Y) = 0$.

Teorema 1.13. *La información mutua de dos variables aleatorias discretas X e Y verifica que $I(X;Y) \geq 0$, dándose la igualdad exclusivamente en el caso en que X e Y sean independientes.*

Demostración. Mostraremos que $-I(X;Y) \leq 0$. Utilizando el lema 1.8, se

sigue que:

$$\begin{aligned}
-I(X;Y) &= \sum_{x,y} p(x,y) \log_2 \frac{p(x)p(y)}{p(x,y)} \\
&\leq \log_2 e \sum_{x,y} p(x,y) \left(\frac{p(x)p(y)}{p(x,y)} - 1 \right) \\
&\leq \log_2 e \left(\sum_{x,y} p(x)p(y) - \sum_{x,y} p(x,y) \right) \\
&\leq \log_2 e \left(\sum_{x} p(x) \sum_{y} p(y) - 1 \right) = 0.
\end{aligned}$$

La igualdad se dará si y solo si $\frac{p(x)p(y)}{p(x,y)} = 1$, o equivalentemente, si $p(x,y) = p(x)p(y)$, esto es, si y solo si las variables X e Y son independientes. □

Corolario 1.2. *Sean X e Y dos variables aleatorias discretas. Entonces*

$$H(X|Y) \leq H(X),$$

donde la igualdad se alcanza únicamente si X e Y son independientes.

Demostración. En virtud del teorema anterior, se sigue que

$$0 \leq I(X;Y) = H(X) - H(X|Y).$$

□

El corolario anterior evidencia lo expuesto en el teorema 1.13. Conocer de antemano el resultado de una variable aleatoria Y reduce la incertidumbre sobre X. Sin embargo, si ambas variables son independientes, conocer Y no dice nada sobre X, es decir, la incertidumbre sobre X se mantendría igual.

Corolario 1.3. *Sean $X_1, X_2, ..., X_n$ variables aleatorias discretas que siguen la función de probabilidad conjunta $p(x_1, x_2, ..., x_n)$. Entonces*

$$H(X_1, X_2, ..., X_n) \leq \sum_{i=1}^{n} H(X_i),$$

donde la igualdad se alcanza si y solo si las variables X_i son independientes entre sí.

Demostración. Siguiendo la regla de la cadena para las entropías,

$$H(X_1, X_2, ..., X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1}, ..., X_1) \leq \sum_{i=1}^{n} H(X_i).$$

La desigualdad es debida al corolario 1.2 De ahí se deduce también que la igualdad vendría dada en el caso de que las variables aleatorias fuesen independientes entre sí. □

1.4. Códigos correctores de errores

En esta sección se introducirán los principales conceptos acerca de los códigos correctores, así como los resultados más fundamentales. Generalmente, se trabajará con códigos que transforman datos de longitud k en otros de longitud n, $n > k$, añadiendo términos a la palabra saliente para darle redundancia. Es importante decir que la redundancia, por lo general, no se considera positiva. Sin embargo, en este contexto, se introducen términos redundantes para obtener un beneficio específico: la corrección de errores. En la presente memoria la redundancia estará enfocada a mejorar la seguridad, protegiendo el secreto. Para más información se puede consultar [7] y [14].

Definición 1.19. Sea Q un conjunto de q símbolos llamado *alfabeto*. Sea Q^n el conjunto de n-vectores $\mathbf{x}= (x_1, x_2, ..., x_n)$, con $x_i \in Q$ para todo $i \in \{1, 2, ..., n\}$. Un *código en bloque* $\mathscr{C}$ de *longitud* n sobre Q es un subconjunto no vacío de Q^n. Los elementos de $\mathscr{C}$ son las *palabras*. Si $\mathscr{C}$ contiene M palabras, entonces M es el *tamaño* del código. Se denotará un código de longitud n y tamaño M como (n, M). Si $M = q^k$, entonces se pondrá que $\mathscr{C}$ es un código $[n, k]$. Para todo código (n, M) sobre Q, se llama *redundancia* al valor $n - \log_q(M)$. Finalmente, la *tasa de información* del código se define como $R = \frac{\log_q(M)}{n}$ y representa cuántos símbolos de información transmitimos por cada n símbolos reales enviados por el canal.

La eventualidad de errores puede requerir que se protejan los datos en ciertos entornos. Para lograr esta protección, es esencial incorporar información adicional a los datos, permitiendo detectar, enmascarar e incluso corregir posibles errores en ellos. Es por eso por lo que a las palabras del código se le añaden términos, lo que hemos llamado redundancia.

Ejemplo 1.6. Sea $Q = \{0, 1\}$. El *código de repetición* de longitud 3 sobre Q es aquel cuyas palabras son los elementos del tipo (a, a, a). De este modo, las dos únicas palabras posibles en este caso son $(0, 0, 0)$ y $(1, 1, 1)$. Así, el valor

de la redundancia será $3 - \log_2(2) = 2$ y presenta una tasa de información $R = 1/3$. Evidentemente, este ratio tiene sentido, ya que para enviar un uno o un cero necesitamos enviar tres unos o tres ceros, por tanto enviamos un símbolo de información por cada tres símbolos reales que leemos.

Ejemplo 1.7. Se presentará ahora un ejemplo en el que el tamaño del código no es potencia del cardinal del alfabeto. Sea $\mathscr{C}$ el código binario de longitud n formado por todas aquellas palabras que tienen exactamente dos unos. ¿Cuántas palabras pueden formarse? El primer 1 puede ir en n posiciones diferentes, mientras que el segundo puede ocupar únicamente $(n-1)$. Sin embargo, todos estos elementos están duplicados. Por lo tanto, $M = \frac{n(n-1)}{2}$.

Definición 1.20. Sea $\mathscr{C}$ un código $[n, k]$ sobre Q. Un *codificador* de $\mathscr{C}$ es una biyección

$$\epsilon : Q^k \longrightarrow Q^n$$

tal que $\mathscr{C} = \epsilon(Q^k)$. Sea $\mathbf{c} \in \mathscr{C}$. Entonces existe un único $\mathbf{m} \in Q^k$ con $\mathbf{c} = \epsilon(\mathbf{m})$. De ahora en adelante, $\mathbf{m}$ se llamará *mensaje* o *fuente* de $\mathbf{c}$.

En la definición anterior, ϵ transforma palabras de $\mathscr{C}$, es decir, palabras de tamaño k, en palabras de tamaño n, entonces $n - k = n - \log_q(M)$ es la redundancia del código. Para medir la diferencia entre dos palabras del código, se introducirá una métrica en Q^n, llamada la *distancia de Hamming.*

Definición 1.21. Sean $\mathbf{x} = (x_1, x_2, ..., x_n)$, $\mathbf{y} = (y_1, y_2, ..., y_n) \in Q^n$. La *distancia de Hamming* entre $\mathbf{x}$ e $\mathbf{y}$, $d(\mathbf{x}, \mathbf{y})$, es el número de elementos en los que difieren. Esto es:

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|.$$

La distancia de Hamming será importante en la teoría de códigos correctores, pues será de utilidad medir los errores, en el sentido de componentes modificadas de la palabra original, del código. Es decir, si enviamos la palabra x y recibimos y, entonces $d(x, y)$ mide cuántos errores hay en y con respecto a x. Veamos que, en efecto, la distancia de Hamming así definida es una métrica.

Proposición 1.1. *La distancia de Hamming es una métrica bien definida sobre Q^n. Es decir, para todo $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in Q^n$ se cumple que:*

1. *$d(\boldsymbol{x}, \boldsymbol{y}) \geq 0$, donde la igualdad se cumple si y solo si $\boldsymbol{x} = \boldsymbol{y}$.*
2. *$d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$.*
3. *(Desigualdad triangular). $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$.*

Demostración. (1) y (2) son evidentes, deduciéndose sencillamente aplicando la definición. Para demostrar la desigualdad triangular, es claro que si $x_i \neq z_i$, entonces o bien $x_i \neq y_i$ o bien $y_i \neq z_i$. □

Corolario 1.4. *La distancia de Hamming es invariante bajo traslaciones, esto es, si* $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in Q^n$*, entonces:*

$$d(\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{z}) = d(\boldsymbol{x}, \boldsymbol{y}).$$

Definición 1.22. La *distancia mínima* de un código $\mathscr{C} \subset Q^n$ se define como:

$$d = d(\mathscr{C}) = \text{mín}\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathscr{C}, \mathbf{x} \neq \mathbf{y}\},$$

si $\mathscr{C}$ contiene más de una palabra, y será $d = n + 1$ si $\mathscr{C}$ contiene sólo una palabra. Se denotará por (n, M, d) a un código $\mathscr{C}$ con longitud n, tamaño M y distancia mínima d.

Ejemplo 1.8. Sea $\mathbf{u} = (1, 1, 0, 0, 1)$ y sea $\mathbf{v} = (1, 0, 1, 0, 1)$. La distancia de Hamming entre $\mathbf{u}$ y $\mathbf{v}$, $d(\mathbf{u}, \mathbf{v}) = 2$.

Un caso interesante de esta distancia se encuentra en el código de repetición.

Ejemplo 1.9. El código de repetición de longitud n, que se ha definido previamente, tiene una distancia mínima n, para todo $n \in \mathbb{N}$.

La teoría de códigos tratará de buscar, para ciertos n y M, un código con la mayor distancia mínima posible junto con sus algoritmos de codificación y decodificación adecuados, lo cual resulta útil, pues la distancia mínima del código nos dice cuántos errores y pérdidas podemos corregir en una palabra. La introducción de una métrica permite, como en el espacio euclídeo con el producto escalar, definir esferas y bolas. Si bien en esta memoria no se ahondará en estos conceptos, es posible encontrar más información en [14].

Supongamos el caso en el que el alfabeto Q es un cuerpo finito. Entonces Q^n es un espacio vectorial, de modo que será natural centrarse en códigos que tengan estructura de subespacio vectorial y sean, por tanto, lineales.

Definición 1.23. Un *código lineal* $\mathscr{C}$ es un subespacio vectorial de $\mathbb{F}_q^n$. La *dimensión* de un código lineal $\mathscr{C}$ se corresponde con su dimensión como subespacio vectorial sobre $\mathbb{F}_q$. Un código lineal $\mathscr{C}$ de longitud n y de dimensión k se denotará como $[n, k]_q$, o simplemente como $[n, k]$. Si además se conoce la distancia mínima d de $\mathscr{C}$, entonces $[n, k, d]_q$ o $[n, k, d]$ serán los *parámetros* del código.

Claramente, para un código lineal $\mathscr{C}$ de parámetros $[n, k]$ sobre $\mathbb{F}_q$, su tamaño $M = q^k$.

Definición 1.24. Sea $\mathbf{x} \in \mathbb{F}_q^n$. Se define el *soporte* de una palabra $\mathbf{x}$, que se denotará como $supp(\mathbf{x})$, como el conjunto de las posiciones en las que la palabra no se anula, esto es:

$$supp(\mathbf{x}) = \{i \in \{1, 2, ..., n\} : x_i \neq 0\}.$$

Se define el *peso* de $\mathbf{x}$, denotado por $w(\mathbf{x})$, como el número de elementos en el soporte de $\mathbf{x}$. El *peso mínimo* de un código $\mathscr{C}$, mwt(C), es el menor de los pesos de las palabras no nulas.

Proposición 1.2. *La distancia mínima de un código lineal $\mathscr{C}$ es igual a su peso mínimo.*

Demostración. Puesto que $\mathscr{C}$ es un código lineal, por definición se sigue que $\mathbf{0} \in \mathscr{C}$ y para todo $\mathbf{c}_1, \mathbf{c}_2 \in C$, $\mathbf{c}_1 - \mathbf{c}_2 \in \mathscr{C}$. De este modo, $w(\mathbf{c}) = d(\mathbf{0}, \mathbf{c})$ y $d(\mathbf{c}_1, \mathbf{c}_2) = w(\mathbf{c}_1 - \mathbf{c}_2)$. De aquí se deduce el resultado. □

Definición 1.25. Sean $\mathscr{C}$ y $\mathscr{D}$ dos códigos lineales sobre $\mathbb{F}_q$ de longitud n. Si $\mathscr{D} \subset \mathscr{C}$, entonces $\mathscr{D}$ es un subcódigo de $\mathscr{C}$.

Nota 1.3. *Sea $\mathscr{C}$ un código de parámetros $[n, k, d]$. Entonces para todo r, con $1 \leq r \leq k$, existen subcódigos de dimensión r. Además, la distancia mínima de un subcódigo $\mathscr{D}$ es siempre mayor o igual a d (puesto que $\mathscr{D} \subset \mathscr{C}$). Entonces, tomando un subcódigo se puede garantizar la construcción de un código de menor dimensión y con una distancia mínima mayor o igual que la de $\mathscr{C}$ (obsérvese que no podemos garantizar en todos los casos que la distancia mínima de $\mathscr{D}$ sea mayor que la de $\mathscr{C}$, pues existen códigos de peso constante).*

Ejemplo 1.10. Sea $\mathscr{C}$ un código sobre $\mathbb{F}_2^4$ formado por las posibles combinaciones lineales del conjunto de elementos

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

Se puede observar que es lineal. Su longitud n es 4, su distancia mínima es 2 (como el código es lineal, basta con observar el peso mínimo) y su dimensión es 3 (es fácil comprobar que el conjunto B está formado por elementos linealmente independientes, que forman una base, y estos generan el resto de elementos de $\mathscr{C}$).

Como se ha mencionado anteriormente, todo código lineal $\mathscr{C}$ de parámetros $[n, k]$ forma un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k. Por tanto,

existirá una base formada por k palabras del código linealmente independientes, $\mathbf{g}_1, \mathbf{g}_2, ..., \mathbf{g}_k$. Sea $\mathbf{g}_i = (g_{i,1}, g_{i,2}, ..., g_{i,n})$. Entonces

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}.$$

Además, todo $\mathbf{c} \in \mathscr{C}$ se puede poner como combinación lineal de los elementos de la base, esto es, $\mathbf{c} = m_1\mathbf{g}_1 + m_2\mathbf{g}_2 + ... + m_k\mathbf{g}_k$, con $m_1, m_2, ..., m_k \in \mathbb{F}_q$. Sea $\mathbf{m} = (m_1, m_2, ..., m_k) \in \mathbb{F}_q^k$. Entonces $\mathbf{c} = \mathbf{m}G$.

Definición 1.26. Una matriz G de tamaño $k \times n$ con elementos en $\mathbb{F}_q$ es una *matriz generatriz* de un código lineal $\mathscr{C}$ sobre $\mathbb{F}_q$ si las filas de G son una base de $\mathscr{C}$.

Un código lineal $\mathscr{C}$ de parámetros $[n, k]$ puede tener más de una matriz generatriz, pero todas las matrices generatrices deben tener en común ser de tamaño $k \times n$, de rango k y generar el código $\mathscr{C}$. Recíprocamente, toda matriz de tamaño $k \times n$ y de rango k es la matriz generatriz de un código lineal sobre $\mathbb{F}_q$ de parámetros $[n, k]$.

Definición 1.27. Sea $\mathscr{C} \subset \mathbb{F}_q^n$ un código lineal con parámetros $[n, k]$ de matriz generatriz G. Una *matriz de control* H de $\mathscr{C}$ es una matriz $(n-k) \times n$ de rango $n - k$ tal que $HG^t = 0$, donde G^t representa la matriz transpuesta de G. En particular, dado $\mathbf{x} \in \mathbb{F}_q^n$, entonces $\mathbf{x} \in \mathscr{C}$ si y solo si $H\mathbf{x}^t = \mathbf{0}$.

Definición 1.28. Sean $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. Se define el producto interno sobre $\mathbb{F}_q^n$ como:

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

Definición 1.29. Para un código $\mathscr{C}$ de parámetros $[n, k]$ se define el *código dual* $\mathscr{C}^\perp$ como:

$$\mathscr{C}^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{x} = 0 \ \forall \mathbf{c} \in \mathscr{C}\}.$$

Proposición 1.3. *Sea $\mathscr{C}$ un código de parámetros $[n, k]$ con matriz generatriz G. Entonces $\mathscr{C}^\perp$ es un código de parámetros $[n, n-k]$ con matriz de control G.*

Demostración. Las siguientes afirmaciones son equivalentes:

$$\mathbf{x} \in \mathscr{C}^\perp,$$

$$\mathbf{c} \cdot \mathbf{x} = 0 \ \forall \mathbf{c} \in \mathscr{C},$$

$$\mathbf{m}G\mathbf{x}^t = 0 \ \forall \mathbf{m} \in \mathbb{F}_q^k,$$
$$G\mathbf{x}^t = \mathbf{0}.$$

Esto implica que $\mathscr{C}^\perp$ es el subespacio anulador de G. Como G es una matriz de tamaño $k \times n$ de rango k, $\mathscr{C}^\perp$ tiene dimensión $n-k$ y G es la matriz de control de $\mathscr{C}^\perp$. □

Definición 1.30. Sean los códigos $\mathscr{C}$, $\mathscr{C}_1$ y $\mathscr{C}_2$ contenidos en $\mathbb{F}_q^n$. Se dice que $\mathscr{C}_1$ y $\mathscr{C}_2$ son *ortogonales* si $\mathbf{x} \cdot \mathbf{y} = 0$ para todos $\mathbf{x} \in \mathscr{C}_1$ y $\mathbf{y} \in \mathscr{C}_2$. Se dice que estos códigos son *duales* si $\mathscr{C}_2 = \mathscr{C}_1^\perp$. Si $\mathscr{C} = \mathscr{C}^\perp$, diremos que el código $\mathscr{C}$ es *autodual*.

El siguiente resultado dará cuenta de una propiedad de los códigos duales, que será utilizada asiduamente a lo largo de esta memoria.

Proposición 1.4. *Sea $\mathscr{C}$ un código de parámetros $[n,k]$. Entonces:*

$$(\mathscr{C}^\perp)^\perp = \mathscr{C}.$$

Demostración. Sea $\mathbf{c} \in \mathscr{C}$. Entonces $\mathbf{c} \cdot \mathbf{x} = 0$ para todo $\mathbf{x} \in \mathscr{C}^\perp$. De este modo, $\mathscr{C} \subset (\mathscr{C}^\perp)^\perp$. Además, aplicando la Proposición 2.4.21, se sigue que, como $\mathscr{C}^\perp$ tiene dimensión $n-k$, el código $(\mathscr{C}^\perp)^\perp$ tendrá dimensión $n-(n-k)=k$. Así, puesto que $\mathscr{C} \subset (\mathscr{C}^\perp)^\perp$ y $\dim(\mathscr{C}) = \dim((\mathscr{C}^\perp)^\perp)$, necesariamente $\mathscr{C} = (\mathscr{C}^\perp)^\perp$.

□

Corolario 1.5. *Sea $\mathscr{C}$ un código lineal. Entonces:*

1. *G será una matriz generatriz de $\mathscr{C}$ si y solo si G es una matriz de control de $\mathscr{C}^\perp$.*
2. *H es una matriz de control de $\mathscr{C}$ si y solo si H es una matriz generatriz de $\mathscr{C}^\perp$.*

Demostración. El aserto (1) se deduce de la Proposición 2.4.21, mientras que el segundo es una consecuencia de aplicar (1) al código $\mathscr{C} = (\mathscr{C}^\perp)^\perp$ usando que $\mathscr{C} = (\mathscr{C}^\perp)^\perp$. □

La siguiente cota, conocida como *cota de Singleton*, relaciona todos los parámetros característicos de los códigos lineales, y permitirá definir un tipo de códigos particular, llamados *códigos MDS*.

Teorema 1.14. *(Cota de Singleton). Sea $\mathscr{C}$ un código sobre $\mathbb{F}_q$ de tipo $[n,k,d]$ con q^k elementos, entonces*

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

Demostración. Sabemos que habrá un total de q^k palabras en el código, cada una de longitud n. Como $d \leq n$ por la definición de distancia mínima, suprimiremos los últimos $d-1$ términos de cada palabra del código. Se obtienen así q^k elementos de $\mathbb{F}_q^{n-d+1}$.
Supongamos que dos de estos elementos, llamados $\mathbf{x}$ e $\mathbf{y}$, fuesen iguales. Entonces, recuperando los $d-1$ términos que se habían suprimido, habremos encontrado dos palabras cuya distancia es $d(\mathbf{x}, \mathbf{y}) = d - 1 < d$, lo cual es absurdo. De este modo, estamos en condiciones de afirmar que los q^k elementos de $\mathbb{F}_q^{n-d+1}$ que hemos formado son distintos dos a dos. Dicho de otra manera, de los q^{n+d-1} elementos de $\mathbb{F}_q^{n-d+1}$, q^k son distintos. De este modo, $k \leq n - d + 1$, y así, $d \leq n - k + 1$. □

Si bien previamente hemos dicho que nos conviene tener un código con la mayor distancia mínima posible, también nos interesa un código que tenga una dimensión grande. Por tanto, la cota de Singleton nos dice cómo puede ser de grande uno de estos parámetros con respecto al otro.

Definición 1.31. Los códigos que alcanzan la cota de Singleton, esto es, aquellos códigos $\mathscr{C}$ de tipo $[n, k, d]$ tales que $d = n - k + 1$, se llaman *códigos MDS* (del inglés, *Maximum Distance Separable*).

Los códigos MDS son por tanto códigos óptimos para la distancia con respecto a la dimensión o viceversa. El siguiente lema será de utilidad, posteriormente, para mostrar ciertas propiedades sobre la matriz generatriz y la matriz de control de un código MDS.

Lema 1.9. *Sea H la matriz de paridad de un código $\mathscr{C}$. Entonces la distancia mínima d de $\mathscr{C}$ es el menor entero positivo tal que existen d columnas de H linealmente dependientes.*

Demostración. Sean $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$ las columnas de H, y sea $\mathbf{c}$ una palabra no nula de peso w. Sea $supp(\mathbf{c}) = \{j_1, j_2, \ldots, j_w\}$. Entonces, como $H\mathbf{c}^\perp = \mathbf{0}$ por definición, se sigue que $c_{j_1}\mathbf{h}_{j_1} + c_{j_2}\mathbf{h}_{j_2} + \cdots + c_{j_w}\mathbf{h}_{j_w} = \mathbf{0}$. Por lo tanto, las columnas $\mathbf{h}_{j_1}, \mathbf{h}_{j_2}, \ldots, \mathbf{h}_{j_w}$ son linealmente dependientes.

Recíprocamente, si $\mathbf{h}_{j_1}, \mathbf{h}_{j_2}, \ldots, \mathbf{h}_{j_w}$ son linealmente dependientes, entonces existen constantes $a_1, a_2, \ldots, a_w$, no todas nulas, tales que se cumple la relación $a_1\mathbf{h}_{j_1} + a_2\mathbf{h}_{j_2} + \cdots + a_w\mathbf{h}_{j_w} = \mathbf{0}$. Por tanto, es posible construir una palabra $\mathbf{c}$ del código tal que $H\mathbf{c}^\top$ donde $c_j = 0$ si $j \neq j_i$ para todo i, y $c_j = a_i$ si $j = j_i$ para algún i. □

Proposición 1.5. *Sea $\mathscr{C}$ un código $[n, k, d]$ sobre $\mathbb{F}_q$. Sea G una matriz generatriz y H una matriz de control de $\mathscr{C}$. Entonces son equivalentes:*

1. *$\mathscr{C}$ es MDS.*

2. *Todo conjunto de $n-k$ columnas de H es linealmente independiente.*

3. *Todo conjunto de k columnas de G es linealmente independiente.*

Demostración. Como la distancia mínima de $\mathscr{C}$ es d, cualquier conjunto de $d-1$ columnas de H son linealmente independientes por el lema 1.9. Por la cota de Singleton, $d \leq n-k+1$. Entonces $d = n-k+1$ si y solo si $n-k$ columnas de H son linealmente independientes. Por tanto, hemos probado que 1 es equivalente a 2.

Supongamos que se cumple 3. Sea $\mathbf{c} \in \mathscr{C}$ una palabra que es cero en k coordenadas. Supongamos también que $\mathbf{c} = \mathbf{x}G$ para algún $\mathbf{x} \in \mathbb{F}_q^k$. Sea G' la matriz cuadrada obtenida a partir de G considerando únicamente las k columnas en las posiciones nulas de $\mathbf{c}$. Entonces $\mathbf{x}G' = \mathbf{0}$, lo que implica que $\mathbf{x} = \mathbf{0}$. Así, $\mathbf{c} = \mathbf{0}$. Por lo tanto, la distancia mínima de $\mathscr{C}$ será, al menos, $n-(k-1) = n-k+1$, con lo cual, combinando esto con la cota de Singleton, se sigue que $d = n-k+1$ y $\mathscr{C}$ es MDS. Recíprocamente, supongamos que $\mathscr{C}$ es MDS. Sea G una matriz generatriz de $\mathscr{C}$. Sea G' una matriz cuadrada consistente en k columnas elegidas de G. Sea $\mathbf{x} \in \mathbb{F}_q^k$ tal que $\mathbf{x}G' = \mathbf{0}$. Entonces $\mathbf{c} = \mathbf{x}G$ es una palabra del código con peso, al menos, $n-k$. Pero como el peso mínimo debe ser $n-k+1$ al ser $\mathscr{C}$ un código MDS, necesariamente $\mathbf{c} = \mathbf{0}$. Así, $\mathbf{x} = \mathbf{0}$, pues el rango de G es k. Por tanto, las k columnas son independientes. □

Corolario 1.6. *El dual de un código MDS es también MDS.*

Demostración. Sea H una matriz de control de un código MDS $\mathscr{C}$ de parámetros $[n, k, n-k+1]$. Entonces por la proposición 1.5, $n-k$ columnas de H son linealmente independientes. También sabemos, por el corolario 1.5, que H es una matriz generatriz de $\mathscr{C}^\perp$. Entonces aplicando el aserto tercero de la proposición 1.5, se sigue que $\mathscr{C}^\perp$ es un código MDS de parámetros $[n.n-k, k+1]$. □

De ahora en adelante, nos centraremos en los *códigos de Reed-Solomon*. Veremos que son códigos MDS y que pueden ser obtenidos evaluando ciertos polinomios. Estos códigos fueron introducidos en 1959 [15] y son ampliamente utilizados por su eficacia y sencillez. A modo de curiosidad, un ejemplo de aplicación de este código se encuentra en la sonda *Galileo*, lanzada a Júpiter en 1989, para proteger la información contra errores en los datos transmitidos sobre un canal de comunicaciones. Más aplicaciones de este tipo de códigos se hallan en la corrección de errores en CDs, DVDs, códigos QR, comunicaciones en fibra óptica y servidores a gran escala de almacenamiento de datos, entre otros. Los códigos Reed-Solomon sobre cuerpos de característica 2 y sus subcódigos sobre $\mathbb{F}_2$ son los códigos bloque más utilizados en la práctica.

Definición 1.32. Sea un entero $k \leq n$. Denotaremos por $\mathbb{P}_k[x]$ al conjunto de todos los polinomios con coeficientes en $\mathbb{F}_q$ con grado menor que k.

$$\mathbb{P}_k[x] = \{f \in \mathbb{F}_q[x] : \deg(f) < k\}.$$

Por definición, $\mathbb{P}_k[x]$ es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión k, donde $\{1, x, x^2, ..., x^{k-1}\}$ forma una base.

Definición 1.33. Sean $x_1, x_2, ..., x_n$ elementos de $\mathbb{F}_q$ distintos (con $n \leq q$). Un *código de Reed-Solomon* de longitud n y dimensión k viene dado por:

$$RS_{k,n} = \{(f(x_1), f(x_2), ..., f(x_n)) \in \mathbb{F}_q^n : f \in \mathbb{P}_k\}.$$

Lema 1.10. *$RS_{k,n}$ es un código lineal de longitud n.*

Demostración. Sean $\mathbf{c} = (f(x_1), f(x_2), ..., f(x_n))$ y $\mathbf{c'} = (f'(x_1), f'(x_2), ..., f'(x_n))$ dos elementos diferentes de $RS_{k,n}$. Entonces, si $\alpha, \beta \in \mathbb{F}_q$:

$$\alpha\mathbf{c} + \beta\mathbf{c'} = ((\alpha f + \beta f')(x_1), (\alpha f + \beta f')(x_2), ..., (\alpha f + \beta f')(x_n)).$$

Y como $\alpha f + \beta f' \in \mathbb{P}_k$, claramente $\alpha\mathbf{c} + \beta\mathbf{c'} \in RS_{k,n}$. □

Lema 1.11. *La dimensión de $RS_{k,n}$ es k.*

Demostración. Sea la aplicación de evaluación definida por

$$\begin{aligned} ev : \mathbb{P}_k &\to \mathbb{F}_q^n \\ f &\mapsto (f(x_1), f(x_2), ..., f(x_n)) \end{aligned}$$

Evidentemente, la aplicación ev es lineal. Además, $\mathrm{Im}(ev) = RS_{k,n}$. Probemos ahora que $\ker(ev) = \{0\}$. En efecto, supongamos $f \in \ker(ev)$. Por definición, $f(x_1) = f(x_2) = ... = f(x_n) = 0$. Por lo tanto, x_1, x_2, ..., x_n son n raíces distintas del polinomio f. Sin embargo, f tiene grado menor que k, y $k \leq n$. De este modo, la única posibilidad es que $f = 0$, y por tanto $\ker(ev) = \{0\}$. Así, como ev es inyectiva, es claro que $\mathbb{P}_k$ e $\mathrm{Im}(ev) = RS_{k,n}$ son espacios isomorfos, y puesto que $\mathbb{P}_k$ es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión k, $RS_{k,n}$ tendrá también dimensión k. □

Teorema 1.15. *El código de Reed-Solomon $RS_{k,n}$ es MDS.*

Demostración. Sea $\mathbf{c} = (f(x_1), f(x_2), ..., f(x_n)) \in RS_{k,n}$ una palabra no nula. Entonces $f \in \mathbb{P}_k$, de modo que f tiene grado menor que k. Por tanto, $\mathbf{c}$ puede tener, a lo sumo, $k-1$ entradas nulas. Esto implica que, para todo $\mathbf{c} \in RS_{k,n}$ no nulo, al menos $n - (k-1)$ entradas serán no nulas, por lo que su peso será $w(\mathbf{c}) \geq n - k + 1$.

Pero por la cota de Singleton, la distancia mínima $d = \mathrm{mín}(w(\mathbf{c})) \leq n - k + 1$, para todo $\mathbf{c} \in RS_{k,n}$ no nulo. Así, $d = n - k + 1$. □

Ejemplo 1.11. Mostremos ahora un ejemplo de aplicación del código Reed-Solomon, en particular, uno de parámetros $[10, 5]$ sobre $\mathbb{F}_{11}$. Obsérvese que en este cuerpo finito, el 2 es un elemento primitivo, de este modo, como $q = 11$, su orden será 10. Ya que 2 es un elemento primitivo, es un elemento generador del grupo multiplicativo $\mathbb{F}_q^*$. De este modo, $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, y nombremos $2^i = x_i$. Cada elemento $(a_0, a_1, a_2, a_3, a_4) \in \mathbb{F}_{11}^5$ será codificado como

$$(f(x_0), f(x_1), f(x_2), \ldots, f(x_9)),$$

donde f es el polinomio $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$. Tomando la base canónica de $\mathbb{F}_{11}^5$ y codificándola, tendremos una base del código de Reed-Solomon y nos permitirá construir la matriz generatriz. De esta manera, una matriz generatriz de $\mathscr{C}$ está formada por los elementos

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 3 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 1 & 3 & 9 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 6 & 1 & 3 & 9 & 6 \end{bmatrix},$$

que en términos de potencias de dos se escribiría como

$$G = \begin{bmatrix} (2^0)^0 & (2^1)^0 & (2^2)^0 & (2^3)^0 & (2^4)^0 & (2^5)^0 & (2^6)^0 & (2^7)^0 & (2^8)^0 & (2^9)^0 \\ (2^0)^1 & (2^1)^1 & (2^2)^1 & (2^3)^1 & (2^4)^1 & (2^5)^1 & (2^6)^1 & (2^7)^1 & (2^8)^1 & (2^9)^1 \\ (2^0)^2 & (2^1)^2 & (2^2)^2 & (2^3)^2 & (2^4)^2 & (2^5)^2 & (2^6)^2 & (2^7)^2 & (2^8)^2 & (2^9)^2 \\ (2^0)^3 & (2^1)^3 & (2^2)^3 & (2^3)^3 & (2^4)^3 & (2^5)^3 & (2^6)^3 & (2^7)^3 & (2^8)^3 & (2^9)^3 \\ (2^0)^4 & (2^1)^4 & (2^2)^4 & (2^3)^4 & (2^4)^4 & (2^5)^4 & (2^6)^4 & (2^7)^4 & (2^8)^4 & (2^9)^4 \end{bmatrix}.$$

Para un caso más general, la matriz generatriz de un código Reed-Solomon $[n, k]$ se escribiría como

$$G = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_0 & x_1 & \ldots & x_{n-1} \\ \vdots & \vdots & \ldots & \vdots \\ x_0^{k-1} & x_1^{k-1} & \ldots & x_{n-1}^{k-1} \end{bmatrix},$$

y si α fuese un elemento primitivo de $\mathbb{F}_q$, entonces las matrices generatriz y de control serían:

$$G = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & \alpha & \ldots & \alpha^{n-1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha^{k-1} & \ldots & \alpha^{(k-1)(n-1)} \end{bmatrix} \text{ y } H = \begin{bmatrix} 1 & \alpha & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \ldots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha^{n-k} & \ldots & \alpha^{(n-k)(n-1)} \end{bmatrix}.$$

Capítulo 2

Esquemas de reparto de secretos

Supongamos que debemos proteger cierta información confidencial. Lo natural es, en un primer momento, encriptar la información. Sin embargo, si no se ha sido especialmente cuidadoso, el método de encriptación podría filtrarse a un adversario, recuperando la información en contra de nuestra voluntad. Por lo tanto, se necesitará un método diferente para proteger el sistema de cifrado. Podría considerarse, en primer lugar, guardarlo en un lugar concreto y protegido (como puede ser un ordenador o la mente humana). Sin embargo, pese a ser el método más seguro, es el menos fiable, pues tanto el ordenador como el humano pueden perder la memoria, haciendo el secreto inaccesible. Una solución sería guardar una copia en diferentes lugares, pero esto incrementaría el riesgo en la seguridad, pues si varias personas obtienen una copia de la clave, por ejemplo, uno de ellos podría traicionar al grupo.

Una solución a este problema es la siguiente. Sea D el conjunto de datos que se quiere proteger, llamado *secreto*. El objetivo será dividir D en n partes, $D_1, D_2, \ldots, D_n$ de modo que, dados r y t enteros no negativos tales que $r > t$:

1. Conociendo r o más partes de D se puede recuperar el secreto.

2. Conociendo t o menos partes de D, el secreto quedará completamente indeterminado (o sea, D puede tomar cualquier valor con igual probabilidad).

Esto se conoce como un *esquema de reparto de un secreto* de umbral (r, t), aspectos que definiremos y trataremos con mayor rigor posteriormente. Es importante destacar que este tipo de sistemas de seguridad están muy presentes en, por ejemplo, los sistemas de votación de países o en la protección de cuentas bancarias.

Ejemplo 2.1. Supongamos un esquema de reparto de secretos entre n participantes. Sea k un número entero positivo tal que $k < n$, de forma que $n = 2k - 1$, $r = k$ y $t = k - 1$. Se podrá recuperar el secreto incluso si $k - 1$ partes del secreto son destruidas, ya que sobrevivirían $2k - 1 - (k - 1) = k$ partes del secreto. Por el contrario, los adversarios no serán capaces de recuperar el secreto con $k - 1$ partes de las k restantes. Este es un tipo de esquemas de reparto de secretos de umbrales $(k, k - 1)$ para n participantes, que se llaman esquemas *perfectos*, donde $r = t + 1$. Más adelante, se dará una definición formal de estos esquemas.

Esta clase de esquemas resultará útil, por ejemplo, cuando un grupo de individuos con intereses en conflicto debe cooperar. No obstante, este método permite que los integrantes puedan vetarse entre ellos. Sin embargo, al elegir correctamente los parámetros r y t, podemos otorgar a cualquier mayoría lo suficientemente grande la autoridad para tomar alguna acción, mientras damos a cualquier minoría lo suficientemente grande el poder para bloquearla. No obstante, no es obligatorio que $r > \frac{n}{2}$, de modo que si $r < \frac{n}{2}$, no haría falta una mayoría para recuperar el secreto. Del mismo modo, no siempre ocurre que $t < \frac{n}{2}$. Podría ocurrir que $t \geq \frac{n}{2}$, de modo que una mayoría no tendría acceso al secreto. No obstante, lo habitual es que $r > \frac{n}{2}$ y $t < \frac{n}{2}$ de forma que hace falta una mayoría para recuperar el secreto, pero ninguna minoría de participantes de tamaño menor que t puede conocer algo del secreto. Las principales referencias para este capítulo serán [9] y [17].

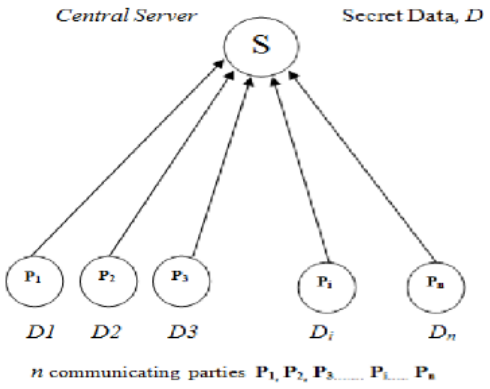


Figura 2.1: Esquema de reparto de un secreto.

Definición 2.1. La colección de partes que dan acceso al secreto se conoce como *estructura de acceso* del esquema de compartición de secretos. Un elemento de la estructura de acceso se conoce como *conjunto calificado*. Por

el contrario, un conjunto de participantes que no pertenece a la estructura de acceso se conoce como *conjunto no calificado*. En el caso de los esquemas del tipo umbral, que son los que trataremos en esta memoria, esta definición resulta trivial: aquellos conjuntos de r o más participantes formarán parte de la estructura de acceso.

Se definirá a continuación un esquema de reparto de secretos a partir de un par de códigos lineales encajados, introduciendo en un primer lugar la notación que se empleará de ahora en adelante, tomando como referencia [9]. Este no es el único tipo de esquema de reparto de secretos, pero es el que seguiremos en esta memoria. Para más información acerca de otros tipos de esquemas (como los esquemas ideales o los construidos con matroides) es interesante leer [18].

Definición 2.2. *(Esquema de reparto de secretos).* Sea $\mathscr{C}_1 \subset \mathbb{F}_q^n$ un código lineal sobre $\mathbb{F}_q$, y sea $\mathscr{C}_2 \subset \mathscr{C}_1$ un subcódigo de $\mathscr{C}_1$. Asumiremos que $\mathscr{C}_1$ y $\mathscr{C}_2$ se han elegido de tal forma que $\mathscr{C}_1 \neq \mathscr{C}_2$. Sea $\mathscr{L} \subset \mathbb{F}_q^n$ un código lineal sobre $\mathbb{F}_q$ elegido de forma que:

$$\mathscr{C}_1 = \mathscr{L} + \mathscr{C}_2 \ \ y \ \ \mathscr{L} \cap \mathscr{C}_2 = \{0\}. \tag{2.1}$$

De este modo, todo elemento $\mathbf{c}_1 \in \mathscr{C}_1$ se puede poner de forma única como $\mathbf{c}_1 = \mathbf{p} + \mathbf{c}_2$, con $\mathbf{p} \in \mathscr{L}$ y $\mathbf{c}_2 \in \mathscr{C}_2$. De esta manera, si se considera sobre $\mathscr{C}_1$ la clase de equivalencia módulo $\mathscr{C}_2$, se sigue que:

$$\dim(\mathscr{C}_1/\mathscr{C}_2) = \dim(\mathscr{L}) \equiv \ell.$$

Nótese que $\mathscr{L}$ podría elegirse completando una base de $\mathscr{C}_2$ hasta conseguir una base de $\mathscr{C}_1$.

Sea $\mathbf{s} \in \mathbb{F}_q^\ell$ un secreto que consideramos una variable aleatoria uniformemente distribuida sobre $\mathbb{F}_q^\ell$. El proceso de construcción de n partes se realiza de la siguiente manera. En primer lugar, se elige, de forma aleatoria y uniforme sobre $\mathscr{C}_2$, una palabra $\mathbf{c}_2 \in \mathscr{C}_2$ independiente de $\mathbf{s}$. Sea $\psi : \mathbb{F}_q^\ell \to \mathscr{L}$ un isomorfismo cualquiera. Entonces, las partes del secreto $\mathbf{s}$ se definirán como las componentes c_i de la palabra $\mathbf{c}_1 = \psi(s) + \mathbf{c}_2$. Por tanto, $\mathbf{c}_1$ es un *vector de partes* del secreto.

2.1. Información filtrada a un conjunto de partes

A lo largo de esta sección, se dará cuenta de la información obtenida del secreto a partir de un número $m < n$ de partes. La estructura del esquema de

reparto de secretos será la que hemos definido anteriormente en la definición 2.2, esto es, para códigos lineales encajados. Las principales referencias para esta sección se encuentran en [2], [5] y [9].

Llegados a este punto, queremos conocer si el subconjunto $\mathscr{J}$ proporcionará la suficiente información como para reconstruir el secreto o por el contrario hará que el secreto permanezca inaccesible. Por tanto, introduciremos dos definiciones que darán cuenta del significado de la *privacidad total* de un secreto y de la *reconstrucción única*.

Definición 2.3. (Privacidad total del secreto). Sea $\mathscr{J} \subset \{1, 2, \ldots, n\}$. Diremos que $\mathscr{J}$ ofrece *privacidad total* del secreto si $I(S; C_{\mathscr{J}}) = 0$, esto es, que las partes en los índices $\mathscr{J}$ no ofrecen ningún tipo de información sobre el secreto.

Definición 2.4. (Reconstrucción única del secreto). Sea $\mathscr{J} \subset \{1, 2, \ldots, n\}$. Diremos que $\mathscr{J}$ ofrece *reconstrucción única* del secreto si $I(S; C_{\mathscr{J}}) = H(S)$, esto es, que la información que proporciona $C_{\mathscr{J}}$ sobre S es toda la incertidumbre que existía sobre S, lo que quiere decir que se obtiene toda la información del secreto.

Buscamos ahora relacionar cuánta incertidumbre permanece en el secreto conocidas algunas de sus partes.

Definición 2.5. Sea S una variable aleatoria cuyo valor observado es el vector secreto $\mathbf{s}$. Sea $\mathscr{A} = \{1, 2, \ldots, n\}$. Sea $C_{\mathscr{J}} = (C_i : i \in \mathscr{J})$ un vector formado por variables aleatorias, con $\mathscr{J} \subset \mathscr{A}$, donde el valor observado de cada C_i es c_i, una partición del secreto. Entonces la *incertidumbre mínima* de S teniendo m partes, con $m < n$, es

$$\Delta_m = \min_{\mathscr{J} \subset \mathscr{A}, |\mathscr{J}|=m} H(S|C_{\mathscr{J}}).$$

También se conoce como la *equivocación* del secreto.

Es conveniente, como se ha hecho en las secciones anteriores, dar una breve interpretación de este resultado en términos de la incertidumbre o la cantidad de información adquirida. Por definición, $H(S|C_{\mathscr{J}})$ representa aquello que queda por conocerse de S (su incertidumbre) habiendo hallado $C_{\mathscr{J}}$. Como se toma el valor mínimo, Δ_m representa la mínima incertidumbre que podemos tener de S habiendo conocido m partes del secreto.

Nota 2.1. *Si bien se omite por comodidad en la escritura, en esta sección siempre que se trate con la entropía (definición 1.13), se considerará el logaritmo en base q.*

Sea $\mathscr{A} = \{1, 2, \ldots, n\}$ un conjunto de índices que representa los participantes en la repartición del secreto. Sea $\mathscr{J} \subset \mathscr{A}$ y $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$. Entonces $P_{\mathscr{J}}(\mathbf{c})$ es un vector de tamaño $|\mathscr{J}|$ tal que $P_{\mathscr{J}}(\mathbf{c}) = (c_j)_{j \in \mathscr{J}}$. Por ejemplo, si $\mathbf{c} = (1, 1, 0, 1)$ y $\mathscr{J} = \{2, 3\}$, entonces $P_{\mathscr{J}}(\mathbf{c}) = (1, 0)$.

Definición 2.6. Sea $\mathscr{C} \subset \mathbb{F}_q^n$ un código lineal. El *código proyección* $P_{\mathscr{J}}(\mathscr{C})$ se define como:

$$P_{\mathscr{J}}(\mathscr{C}) = \{P_{\mathscr{J}}(\mathbf{c}) : \mathbf{c} \in \mathscr{C}\}.$$

A partir del código proyección se define también el código acortado.

Definición 2.7. Sea $\mathscr{J} \subset \mathscr{A} = \{1, 2, \ldots, n\}$. El *código acortado* $\mathscr{C}_{\mathscr{J}}$ de un código $\mathscr{C} \subset \mathbb{F}_q^n$ se define como

$$\mathscr{C}_{\mathscr{J}} = \{P_{\mathscr{J}}(\mathbf{c}) : \mathbf{c} \in \mathscr{C}, c_i = 0, \forall i \notin \mathscr{J}\}.$$

Las definiciones 2.6 y 2.7 se pueden extender para los códigos duales. Dado un código lineal $\mathscr{C} \subset \mathbb{F}_q^n$ y un conjunto de índices $\mathscr{J}$, entonces es claro que:

$$(P_{\mathscr{J}}(\mathscr{C}))^{\perp} = \{\mathbf{x} \in P_{\mathscr{J}}(\mathbb{F}_q^n) : \mathbf{x} \cdot \mathbf{y} = 0, \forall \mathbf{y} \in P_{\mathscr{J}}(\mathscr{C})\},$$
$$(\mathscr{C}_{\mathscr{J}})^{\perp} = \{\mathbf{x} \in P_{\mathscr{J}}(\mathbb{F}_q^n) : \mathbf{x} \cdot \mathbf{y} = 0, \forall \mathbf{y} \in \mathscr{C}_{\mathscr{J}}\}.$$

De aquí, se sigue la siguiente proposición.

Proposición 2.1. *Sean $\mathscr{J}$ y $\mathscr{C}$ como en la definición anterior. Se puede comprobar que $\left(P_{\mathscr{J}}(\mathscr{C})\right)^{\perp} = (\mathscr{C}^{\perp})_{\mathscr{J}}$ y que $P_{\mathscr{J}}(\mathscr{C}^{\perp}) = (\mathscr{C}_{\mathscr{J}})^{\perp}$.*

Demostración. Claramente, $(\mathscr{C}^{\perp})_{\mathscr{J}} \subset \left(P_{\mathscr{J}}(\mathscr{C})\right)^{\perp}$. Recíprocamente, sea $\mathbf{c} \in \left(P_{\mathscr{J}}(\mathscr{C})\right)^{\perp}$. Así, $\mathbf{c} \cdot \mathbf{a} = 0$ para cada $\mathbf{a} \in P_{\mathscr{J}}(\mathscr{C})$, de modo que $\sum_{i \in \mathscr{J}} c_i a_i = 0$. Por tanto, el vector $\hat{\mathbf{c}}$ formado por las $|\mathscr{J}|$ componentes de $\mathbf{c}$ y $n - |\mathscr{J}|$ ceros, estará en $\mathscr{C}^{\perp}$, pues se tendría que

$$\sum_{i=1}^{n} \hat{c}_i \hat{a}_i = \sum_{i \in \mathscr{J}} c_i a_i = 0,$$

para cada $\hat{\mathbf{a}} \in \mathscr{C}$.

Sea ahora $\mathbf{c} \in P_{\mathscr{J}}(\mathscr{C}^{\perp})$ tal que $\mathbf{c} = P_{\mathscr{J}}(\hat{\mathbf{c}})$. Es evidente que $\mathbf{c} \cdot \mathbf{b} = 0$ para todo $\mathbf{b} \in \mathscr{C}_{\mathscr{J}}$, pues si $\hat{\mathbf{b}} \in \mathscr{C}$, se sigue que $\hat{\mathbf{c}} \cdot \hat{\mathbf{b}} = 0$, y como $\hat{\mathbf{b}}$ está formado por $\mathbf{b}$ junto con ceros en las posiciones fuera de $\mathscr{J}$, se tiene el resultado. Así, $P_{\mathscr{J}}(\mathscr{C}^{\perp}) \subset (\mathscr{C}_{\mathscr{J}})^{\perp}$. El recíproco vuelve a ser evidente, sin más que tomar las definiciones. □

Esta definición proporciona un tratamiento importante para los esquemas de reparto de secretos. Si, como antes, tenemos dividido el secreto en m partes diferentes, el código acortado eliminará los elementos fuera de los índices que nos interesan (aquellos que vienen marcados por el conjunto $\mathscr{J}$). En los siguientes ejemplos se muestra con claridad el significado de esta definición. En estos casos se trabajará con códigos lineales sobre el cuerpo $\mathbb{F}_2$.

Ejemplo 2.2. Sea el conjunto de índices $\mathscr{J} = \{1\}$. Si

$$\mathscr{C} = \{[1,1],[1,0],[0,1],[0,0]\} \subset \mathbb{F}_2^2,$$

entonces $\mathscr{C}_{\mathscr{J}} = \{[1],[0]\} = \mathbb{F}_2$.

Ejemplo 2.3. Sea el conjunto de índices $\mathscr{J} = \{1,2\}$. Si

$$\mathscr{C} = \{[0,0,0],[0,1,1],[1,0,1],[1,1,0]\} \subset \mathbb{F}_2^3,$$

entonces $\mathscr{C}_{\mathscr{J}} = \{[0,0],[1,1]\}$.

A continuación, dados dos códigos lineales $\mathscr{C}_1$ y $\mathscr{C}_2$, con $\mathscr{C}_2 \subset \mathscr{C}_1$, se estudiará la diferencia entre las dimensiones de sus respectivos códigos acortados.

Definición 2.8. (Máxima dimensión relativa). Sea $\mathscr{C}_1 \subset \mathbb{F}_q^n$ un código lineal y sea $\mathscr{C}_2$ un subcódigo de $\mathscr{C}_1$. La *máxima dimensión relativa de tamaño i* entre $\mathscr{C}_1$ y $\mathscr{C}_2$ se define como

$$K_i(\mathscr{C}_1, \mathscr{C}_2) = \max_{|\mathscr{J}|=i} \{\dim(\mathscr{C}_1)_{\mathscr{J}} - \dim(\mathscr{C}_2)_{\mathscr{J}}\},$$

con $1 \leq i \leq n$.

Los siguientes lemas, introducidos por Forney en [5], permiten establecer relaciones entre los códigos proyectados y los códigos acortados, en especial, en términos de sus dimensiones. Serán de utilidad para demostrar teoremas posteriores. Supongamos que $\mathscr{A} = \{1,2,\ldots,n\}$ es un conjunto de índices.

Lema 2.1. *(Primer lema de Forney). Sea $\mathscr{C}$ un código lineal de parámetros $[n,k]$ y $\mathscr{J} \subset \mathscr{A}$ un conjunto de índices, entonces*

$$k = \dim\left(P_{\mathscr{J}}(\mathscr{C})\right) + \dim\left(\mathscr{C}_{\mathscr{A}\setminus\mathscr{J}}\right).$$

Demostración. Se considera la aplicación $P_{\mathscr{J}} : \mathscr{C} \to P_{\mathscr{J}}(\mathscr{C})$. Claramente, se puede observar que es un homomorfismo cuya imagen es $P_{\mathscr{J}}(\mathscr{C})$ y su núcleo es $\mathscr{C}_{\mathscr{A}\setminus\mathscr{J}}$, por tanto, en virtud del primer teorema de isomorfía se sigue que $P_{\mathscr{J}}(\mathscr{C}) \cong \mathscr{C}/\mathscr{C}_{\mathscr{A}\setminus\mathscr{J}}$. □

Lema 2.2. *(Segundo lema de Forney). Sea $\mathscr{C}$ un código lineal de parámetros $[n,k]$ y $\mathscr{J}$ un conjunto de índices. Entonces, $\mathscr{C}_{\mathscr{J}}$ y $P_{\mathscr{J}}(\mathscr{C}^{\perp})$, entendidos como subespacios de $P_{\mathscr{J}}(\mathbb{F}_q^{|\mathscr{J}|})$, son duales el uno del otro. En particular,*

$$|\mathscr{J}| = \dim(\mathscr{C}_{\mathscr{J}}) + \dim(P_{\mathscr{J}}(\mathscr{C}^{\perp})).$$

Demostración. Por la proposición 2.1, $P_{\mathscr{J}}(\mathscr{C}^{\perp}) = (\mathscr{C}_{\mathscr{J}})^{\perp}$, de donde se sigue el resultado.

□

Una vez se han definido el código proyectado y el código acortado y se han demostrado sus propiedades principales, estamos en condiciones de estudiar la reconstrucción del secreto tal y como se ha definido en 2.4. Vemos también que las definiciones 2.3 y 2.4 tienen sentido con lo que se expuso en el lema 1.7, que afirma que

$$I(S; C_{\mathscr{J}}) = H(S) - H(S|C_{\mathscr{J}}),$$

y como el significado de reconstrucción única quiere decir que conocidas los m índices de $\mathscr{J}$ el secreto S sería descubierto, esto implica que $H(S|C_{\mathscr{J}}) = 0$ (no hay incertidumbre conocido $C_{\mathscr{J}}$). Por tanto, nuestra definición es consistente con la teoría. El siguiente teorema servirá para caracterizar estas definiciones en términos de las dimensiones de los códigos proyectados. La siguiente proposición relacionará el valor de la entropía de la variable aleatoria S construida en la definición 2.2 con el número de componentes del secreto sobre el alfabeto $\mathbb{F}_q$.

Proposición 2.2. *En las condiciones de la definición 2.2, $\ell = H(S)$.*

Demostración. Puesto que según la definición 2.2 el secreto se escoge como una variable aleatoria uniforme sobre $\mathbb{F}_q^{\ell}$, de acuerdo con el teorema 1.12, se sigue que $H(S) = \log_q |\mathbb{F}_q^{\ell}| = \log_q q^{\ell} = \ell$. □

Teorema 2.1. *El conjunto de índices $\mathscr{J}$ ofrece privacidad total del secreto si y solo si* $\dim\left(P_{\mathscr{J}}(\mathscr{C}_1)\right) - \dim\left(P_{\mathscr{J}}(\mathscr{C}_2)\right) = 0$. *Por otro lado, $\mathscr{J}$ permite reconstrucción única del secreto si y solo si* $\dim\left(P_{\mathscr{J}}(\mathscr{C}_1)\right) - \dim\left(P_{\mathscr{J}}(\mathscr{C}_2)\right) = \ell$. *Más generalmente, se tiene que*

$$\ell - H(S|C_{\mathscr{J}}) = \dim\left(P_{\mathscr{J}}(\mathscr{C}_1)\right) - \dim\left(P_{\mathscr{J}}(\mathscr{C}_2)\right).$$

Demostración. De acuerdo con la proposición 1.7, puesto que $H(S) = \ell$, y usando la propiedad de simetría de la información mutua, entonces

$$\begin{aligned} I(S; C_{\mathscr{J}}) &= \ell - H(S|C_{\mathscr{J}}) \\ &= H(C_{\mathscr{J}}) - H(C_{\mathscr{J}}|S). \end{aligned}$$

Por lo tanto, únicamente habrá que probar que $H(C_{\mathscr{J}}) = \dim(P_{\mathscr{J}}(\mathscr{C}_1))$ y que $H(C_{\mathscr{J}}|S) = \dim(P_{\mathscr{J}}(\mathscr{C}_2))$. Para ello, emplearemos el teorema 1.12. Puesto que, por definición, $C_{\mathscr{J}}$ es una variable uniforme sobre $P_{\mathscr{J}}(\mathscr{C}_1)$, se sigue que

$$H(C_{\mathscr{J}}) = \log_q |P_{\mathscr{J}}(\mathscr{C}_1)| = \dim_{\mathbb{F}_q}\left(P_{\mathscr{J}}(\mathscr{C}_1)\right).$$

Por otra parte,

$$H(C_{\mathscr{J}}|S) = H((C_2)_{\mathscr{J}}) = \log_q |P_{\mathscr{J}}(\mathscr{C}_2)| = \dim_{\mathbb{F}_q}\left(P_{\mathscr{J}}(\mathscr{C}_2)\right),$$

ya que $\mathbf{c} = \mathbf{c}_2 + \psi(\mathbf{s})$, y como ahora estamos calculando la entropía conociendo $\mathbf{s}$, podemos considerar $\mathbf{s}$ como un valor fijo, de modo que $\mathbf{c}$ no es más que una traslación de $\mathbf{c}_2$, que es una distribución uniforme en $\mathscr{C}_2$, de modo que $\mathbf{c}$ también lo es. □

El siguiente teorema dará cuenta de la equivocación el secreto a partir de $m < n$ de sus partes, mostrando su relación con la dimensión relativa.

Teorema 2.2. *En las condiciones de la definición 2.2, la equivocación del secreto para m partes viene dada por*

$$\Delta_m = \ell - K_m\left((\mathscr{C}_2)^\perp, (\mathscr{C}_1)^\perp\right).$$

Demostración. Sea $\mathscr{J}$ un conjunto de índices con $|\mathscr{J}| = m < n$. De acuerdo con el teorema 2.1

$$H(S|C_{\mathscr{J}}) = \ell - \dim\left(P_{\mathscr{J}}(\mathscr{C}_1)\right) + \dim\left(P_{\mathscr{J}}(\mathscr{C}_2)\right). \tag{2.2}$$

Por el lema 2.2, tenemos que para todo código lineal $\mathscr{C} \subset \mathbb{F}_q^n$ se cumple que $P_{\mathscr{J}}(\mathscr{C}^\perp) = (\mathscr{C}_{\mathscr{J}})^\perp$. Por lo tanto, aplicando la proposición 1.4

$$P_{\mathscr{J}}(\mathscr{C}) = P_{\mathscr{J}}((\mathscr{C}^\perp)^\perp) = \left((\mathscr{C}^\perp)_{\mathscr{J}}\right)^\perp.$$

De este modo, la ecuación 2.2 puede escribirse como

$$\begin{aligned} H(S|C_{\mathscr{J}}) &= \ell - \dim\left((\mathscr{C}_1^\perp)^\perp_{\mathscr{J}}\right) + \dim\left((\mathscr{C}_2^\perp)^\perp_{\mathscr{J}}\right) \\ &= \ell - m + \dim\left((\mathscr{C}_1^\perp)_{\mathscr{J}}\right) + m - \dim\left((\mathscr{C}_2^\perp)_{\mathscr{J}}\right) \\ &= \ell - \dim\left((\mathscr{C}_2^\perp)_{\mathscr{J}}\right) + \dim\left((\mathscr{C}_1^\perp)_{\mathscr{J}}\right). \end{aligned}$$

Por lo tanto, la equivocación del secreto Δ_m viene dada por

$$\begin{aligned} \Delta_m &= \min_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} H(S|C_{\mathscr{J}}) \\ &= \min_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} \left\{\ell - \dim\left((\mathscr{C}_2^\perp)_{\mathscr{J}}\right) + \dim\left((\mathscr{C}_1^\perp)_{\mathscr{J}}\right)\right\} \\ &= \ell - \max_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} \left\{\dim\left((\mathscr{C}_2^\perp)_{\mathscr{J}}\right) - \dim\left((\mathscr{C}_1^\perp)_{\mathscr{J}}\right)\right\} \\ &= \ell - K_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp). \end{aligned}$$

□

2.2. Umbrales límite

Como se ha expuesto al inicio de este capítulo, generalmente los esquemas de compartición de secretos presentan dos umbrales, t y r, con $t < r$, que cumplen lo siguiente:

1. Disponer de t o menos partes del secreto proporciona información mutua $I(S; \mathscr{C}_{\mathscr{J}}) = 0$, con $|\mathscr{J}| = t$.

2. Disponer de r o más partes del secreto proporciona información mutua $I(S; \mathscr{C}_{\mathscr{J}}) = H(S)$, con $|\mathscr{J}| = r$.

En esta sección especificaremos los valores máximo y mínimo que pueden tomar t y r respectivamente. Para ello, emplearemos el peso relativo de Hamming generalizado. Se tomarán como principales referencias [5], [9] y [11].

Nota 2.2. *Para lo que sigue, se empleará una definición del código acortado donde no se reduce la longitud. Para no confundirlo, lo denotaremos como $\mathscr{C}(\mathscr{J})$, que vendrá definido como*

$$\mathscr{C}(\mathscr{J}) = \{\boldsymbol{c} : \boldsymbol{c} \in \mathscr{C}, c_i = 0, \forall i \notin \mathscr{J}\}.$$

Será más cómoda de utilizar en lo sucesivo, y es equivalente a la definición 2.7.

Definición 2.9. Sea $\mathscr{A} = \{1, 2, \ldots, n\}$. Dado $\mathscr{C}_1 \subset \mathbb{F}_q^n$ un código lineal y $\mathscr{C}_2 \subset \mathscr{C}_1$ el *peso i-ésimo relativo generalizado* (RGHW) $M_i(\mathscr{C}_1, \mathscr{C}_2)$ viene dado por

$$M_i(\mathscr{C}_1, \mathscr{C}_2) = \min_{\mathscr{J} \subset \mathscr{A}} \{|\mathscr{J}| : \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) \geq i\},$$

para $1 \leq i \leq \dim(\mathscr{C}_1/\mathscr{C}_2)$.

Si bien esta definición será la más empleada en esta sección, es posible definir los pesos relativos generalizados a partir de los pesos de Hamming generalizados.

Definición 2.10. Sea $\mathscr{C}$ un código lineal y sea $\mathscr{D} \subset \mathscr{C}$. Se define el *soporte* de $\mathscr{D}$ como el conjunto de posiciones donde al menos una palabra de $\mathscr{D}$ es distinta de cero, esto es,

$$supp(\mathscr{D}) = \{i : \text{ existe } \mathbf{x} \in \mathscr{D}, \text{ tal que } x_i \neq 0\}.$$

El *peso* de $\mathscr{D}$, $wt(\mathscr{D})$, se define como el cardinal del soporte $supp(\mathscr{D})$.

Se definen ahora los pesos de Hamming generalizados, a partir de los cuales podremos hallar su relación con los pesos relativos de Hamming generalizados.

Definición 2.11. (Peso de Hamming generalizado). Supongamos que $\mathscr{C}$ es un código lineal $[n, k]$. Entonces para cada $m \leq k$, el peso m-ésimo generalizado de Hamming de $\mathscr{C}$ se define como

$$d_m(\mathscr{C}) = \text{mín}\{wt(\mathscr{D}) : \mathscr{D} \text{ es un subcódigo m-dimensional de } \mathscr{C}\}.$$

Nota 2.3. *Obsérvese que cualquier código lineal $\mathscr{C}$ de dimensión 1 tiene una palabra distinta de cero como base, de modo que $d_1(\mathscr{C}) = wt(\mathscr{C}) = d$, siendo d la distancia mínima del código. Si $d_n(\mathscr{C}) \neq n$, entonces $\mathscr{C}$ es degenerado.*

Una vez introducido el soporte de un subcódigo, es posible dar una nueva definición de los pesos de Hamming relativos generalizados, en términos del soporte.

Definición 2.12. Sea $\mathscr{C}_2 \subset \mathscr{C}_1$ dos códigos lineales sobre $\mathbb{F}_q$. Para $m = 1, 2, \ldots, \dim(\mathscr{C}_1) - \dim(\mathscr{C}_2)$, el *peso relativo m-ésimo generalizado de Hamming* se define como

$$M_m(\mathscr{C}_1, \mathscr{C}_2) = \text{mín}\{wt(\mathscr{D}) : \mathscr{D} \subset \mathscr{C}_1, \dim(\mathscr{D}) = m, \mathscr{D} \cap \mathscr{C}_2 = \{\mathbf{0}\}\}.$$

Proposición 2.3. *Las definiciones 2.9 y 2.12 son equivalentes.*

Demostración. Sea

$$r_m = \text{mín}\{wt(\mathscr{D}) : \mathscr{D} \subset \mathscr{C}_1, \dim(\mathscr{D}) = m, \mathscr{D} \cap \mathscr{C}_2 = \{\mathbf{0}\}\}.$$

Sabemos que $\mathscr{C}_2(\mathscr{J}) \subset \mathscr{C}_1(\mathscr{J})$. Supongamos que $\dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) = m$ y que $M_m(\mathscr{C}_1, \mathscr{C}_2) = |\mathscr{J}|$. Sea G_1 la matriz generatriz de $\mathscr{C}_2(\mathscr{J})$. Añadiendo los términos correspondientes, es posible extender esta matriz a una generatriz de $\mathscr{C}_1(\mathscr{J})$, de modo que, volviendo a llamar G_1 a la matriz generatriz de $\mathscr{C}_2(\mathscr{J})$, se tiene que

$$G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}.$$

De esta manera, eliminando la acción de $\mathscr{J}$ sobre el código $\mathscr{D}$ generado por G_2 cumple que $\dim(\mathscr{D}) = m$, $\mathscr{D} \cap \mathscr{C}_2 = \{\mathbf{0}\}$ y que $wt(\mathscr{D}) \leq wt(\mathscr{C}_1(\mathscr{J})) = |\mathscr{J}|$, de modo que $r_m \leq M_m(\mathscr{C}_1, \mathscr{C}_2)$.
Recíprocamente, supongamos que $r_m = wt(\mathscr{D})$, donde $\dim(\mathscr{D}) = m$ y $\mathscr{D} \cap$

$\mathscr{C}_2 = \{\mathbf{0}\}$, de donde se sigue que, si $\mathscr{K} = supp(\mathscr{D})$, $\mathscr{C}_2(\mathscr{K}) \cap \mathscr{D} = \{\mathbf{0}\}$. Así, $\mathscr{C}_2(\mathscr{K}) \oplus \mathscr{D} \subset \mathscr{C}_1(\mathscr{K})$, y así

$$\dim(\mathscr{C}_1(\mathscr{K})) - \dim(\mathscr{C}_2(\mathscr{K})) \geq \mathscr{D} = m.$$

De esta manera, y de acuerdo con la definición 2.9, se observa que

$$r_m = wt(\mathscr{D}) = |supp(\mathscr{D})| \geq M_m(\mathscr{C}_1, \mathscr{C}_2).$$

Así, $r_m = M_m(\mathscr{C}_1, \mathscr{C}_2)$ y las definiciones son equivalentes. □

Nota 2.4. *Se puede observar que $M_m(\mathscr{C}_1, \{\boldsymbol{0}\}) = d_m(\mathscr{C}_1)$. En efecto, todo súbcodigo $\mathscr{D} \subset \mathscr{C}_1$ tiene intersección $\{\boldsymbol{0}\}$ con $\mathscr{C}_2 = \{\boldsymbol{0}\}$, y sin más que observar las dos definiciones se puede concluir. En particular, $M_1(\mathscr{C}_1, \{\boldsymbol{0}\}) = d(\mathscr{C}_1)$, donde $d(\mathscr{C}_1)$ es la distancia mínima de $\mathscr{C}_1$. Por último, se observa de la definición 2.12 que $M_1(\mathscr{C}_1, \mathscr{C}_2)$ se corresponde con el peso mínimo de las palabras de $\mathscr{C}_1$ que no están en $\mathscr{C}_2$. Esto se conoce como la distancia relativa entre los códigos $\mathscr{C}_1$ y $\mathscr{C}_2$.*

Proposición 2.4. *Sea $\mathscr{C}_1 \subset \mathbb{F}_q^n$ un código lineal y sea $\mathscr{C}_2 \subset \mathscr{C}_1$ un subcódigo lineal. Para $0 \leq i \leq n-1$ se tiene que*

$$0 \leq K_{i+1}(\mathscr{C}_1, \mathscr{C}_2) - K_i(\mathscr{C}_1, \mathscr{C}_2) \leq 1.$$

Demostración. Sea $\mathscr{J} \subset \mathscr{A} = \{1, 2, \ldots, n\}$ un conjunto de índices, y sea $t \notin \mathscr{J}$. Sean

$$\begin{aligned} f &= \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})), \\ g &= \dim(\mathscr{C}_1(\mathscr{J} \cup \{t\})) - \dim(\mathscr{C}_2(\mathscr{J} \cup \{t\})). \end{aligned}$$

Observemos que se pueden dar dos situaciones:

1. $\dim(\mathscr{C}_2(\mathscr{J} \cup \{t\})) = \dim(\mathscr{C}_2(\mathscr{J}))$. Entonces $f + 1 \geq g \geq f$.

2. $\dim(\mathscr{C}_2(\mathscr{J} \cup \{t\})) = \dim(\mathscr{C}_2(\mathscr{J})) + 1$. Si se considera como una matriz el código $(\mathscr{C}_2)_{\mathscr{J} \cup \{t\}}$, donde cada fila representaría una palabra del código, se tiene que la columna t-ésima es linealmente independiente de las columnas de $\mathscr{C}_2(\mathscr{J})$. Entonces también la t-ésima columna de $\mathscr{C}_1(\mathscr{J} \cup \{t\})$ es independiente de las columnas de $\mathscr{C}_1(\mathscr{J})$. Así

   $$\dim(\mathscr{C}_1(\mathscr{J} \cup \{t\})) = \dim(\mathscr{C}_1(\mathscr{J})) + 1,$$

   de modo que $f = g$.

De lo anterior, se sigue que $f+1 \geq g \geq f$. Por tanto, es fácil comprobar que

$$K_i(\mathscr{C}_1, \mathscr{C}_2) + 1 \geq K_{i+1}(\mathscr{C}_1, \mathscr{C}_2) \geq K_i(\mathscr{C}_1, \mathscr{C}_2),$$

de donde se deduce el resultado pedido. □

De esta manera, se ha podido comprobar que K_i es no decreciente con i, y el incremento de K_i hasta K_{i+1} puede ser de, como mucho, una unidad. El siguiente teorema resulta de gran importancia, pues proporciona una conexión entre los pesos relativos generalizados de Hamming y la dimensión relativa.

Teorema 2.3. *Sea $\mathscr{C}_1$ un código de parámetros $[n, k_1]$ y $\mathscr{C}_2 \subset \mathscr{C}_1$ un subcódigo $[n, k_2]$. Entonces*

$$M_j(\mathscr{C}_1, \mathscr{C}_2) = \text{mín}\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) \geq j\},$$

y también

$$K_i(\mathscr{C}_1, \mathscr{C}_2) = \text{máx}\{j : M_j(\mathscr{C}_1, \mathscr{C}_2) \leq i\},$$

donde $0 \leq i \leq n$ y $0 \leq j \leq k_1 - k_2$.

Demostración. Para la primera,

$$\begin{aligned}
&\text{mín}\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) \geq j\} = \\
&= \text{mín}\{i : \exists |\mathscr{J}| = i \text{ tal que } \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) \geq j\} \\
&= \text{mín}\{|\mathscr{J}| : \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) \geq j\} = M_j(\mathscr{C}_1, \mathscr{C}_2),
\end{aligned}$$

mientras que para la segunda igualdad,

$$\begin{aligned}
&\text{máx}\{j : M_j(\mathscr{C}_1, \mathscr{C}_2) \leq i\} = \\
&= \text{máx}\{j : \exists |\mathscr{J}| \leq i \text{ tal que } \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) \geq j\} \\
&= \text{máx}\{\dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) : |\mathscr{J}| \leq i\} = K_i(\mathscr{C}_1, \mathscr{C}_2).
\end{aligned}$$

□

Pronto veremos la importancia que tiene este teorema, pues en la sección anterior se ha relacionado la equivocación del secreto Δ_m con el parámetro K_i, y aquí se ha mostrado una relación existente entre los pesos generalizados y K_i. De este modo, seremos capaces de dar una relación entre la equivocación del secreto y los pesos generalizados.

Proposición 2.5. *Sea $\mathscr{A} = \{1, 2, \ldots, n\}$. Para un código lineal $\mathscr{C}_1 \subset \mathbb{F}_q^n$ de parámetros $[n, k_1]$ y un subcódigo $\mathscr{C}_2 \subset \mathscr{C}_1$ de tipo $[n, k_2]$, $M_j(\mathscr{C}_1, \mathscr{C}_2)$ es creciente con j. Además, se tiene que $M_0(\mathscr{C}_1, \mathscr{C}_2) = 0$ y*

$$\begin{aligned} M_j(\mathscr{C}_1, \mathscr{C}_2) &= \min_{\mathscr{J} \subset \mathscr{A}} \{|\mathscr{J}| : \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) = j\} \\ &= \min\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) = j\}. \end{aligned}$$

Demostración. En virtud de la proposición 2.4 sabemos que $K_i(\mathscr{C}_1, \mathscr{C}_2)$ es no decreciente con i, que toma todos los valores desde $K_0(\mathscr{C}_1, \mathscr{C}_2) = 0$ hasta $K_n(\mathscr{C}_1, \mathscr{C}_2) = k_1 - k_2 = \ell$. El incremento de $K_i(\mathscr{C}_1, \mathscr{C}_2)$ a $K_{i+1}(\mathscr{C}_1, \mathscr{C}_2)$ será como mucho de 1. Además, como K_i es no decreciente con i, es claro que

$$\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) = j\} \cap \{i : K_i(\mathscr{C}_1, \mathscr{C}_2) \geq j + 1\} = \emptyset. \tag{2.3}$$

Por lo que, de acuerdo con el teorema 2.3, se sigue que

$$\begin{aligned} M_j(\mathscr{C}_1, \mathscr{C}_2) &= \min\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) \geq j\} \\ &= \min\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) = j\}, \end{aligned}$$

donde $0 \leq j \leq k_1 - k_2 = \ell$. Por lo tanto, de esta cadena de igualdades y de acuerdo con la ecuación 2.3, $M_j(\mathscr{C}_1, \mathscr{C}_2)$ es creciente con j, pues $K_i(\mathscr{C}_1, \mathscr{C}_2)$ es no decreciente con i. Por último, de lo anterior, se tiene que

$$M_j(\mathscr{C}_1, \mathscr{C}_2) = \min_{\mathscr{J} \subset \mathscr{A}} \{|\mathscr{J}| : \dim(\mathscr{C}_1(\mathscr{J})) - \dim(\mathscr{C}_2(\mathscr{J})) = j\}.$$

□

Esta proposición de monotonía tiene también una interpretación en términos de la equivocación. Aumentando el número de partes, aumentará también el valor de $M_j(\mathscr{C}_1, \mathscr{C}_2)$. Teniendo en cuenta los teoremas 2.2 y 2.3, estamos en condiciones de afirmar que a mayor número de partes, menor será la equivocación del secreto. Podremos obtener, al igual que para los pesos de Hamming relativos generalizados, unas propiedades de monotonía, y finalmente, un equivalente de la cota de Singleton para pesos de Hamming generalizados.

Proposición 2.6. *Para cualquier código lineal $\mathscr{C}$ de parámetros $[n, k]$ se cumple que*

$$1 \leq d_1(\mathscr{C}) < \ldots < d_k(\mathscr{C}) \leq n.$$

Demostración. Si bien esta proposición puede deducirse de lo expuesto en la nota 2.4 y de la proposición 2.5, se ofrecerá aquí una demostración alternativa. Para todo $1 \leq r \leq k - 1$ se comprueba trivialmente de la definición que

$1 \leq d_r(\mathscr{C}) \leq d_{r+1}(\mathscr{C}) \leq n$. Sea $\mathscr{D}$ un subcódigo de $\mathscr{C}$ de dimensión $r+1$ tal que $wt(\mathscr{D}) = d_{r+1}(\mathscr{C})$. Elijamos cualquier índice $i \in supp(\mathscr{D})$. Sea

$$\mathscr{E} = \{\mathbf{x} : \mathbf{x} \in \mathscr{D} \text{ y } x_i = 0\}.$$

Es claro que $\mathscr{E}$ es un código acortado de $\mathscr{D}$, y que $r \leq \dim(\mathscr{E}) \leq r+1$ (pues es posible que al hacer cero una componente de cada palabra del código, se reduzca en una unidad la dimensión). Sin embargo, por la elección de i y por la definición de soporte, existe una palabra $\mathbf{c} \in \mathscr{D}$ tal que $c_i \neq 0$. Entonces, $\mathbf{c} \notin \mathscr{E}$. Por lo tanto, $\mathscr{E}$ está contenido estrictamente en $\mathscr{D}$, por lo tanto, $\dim(\mathscr{E}) = r$. Ahora, por definición de los pesos de Hamming generalizados, se sigue que

$$d_r(\mathscr{C}) \leq wt(\mathscr{E}) \leq wt(\mathscr{D}) - 1 = d_{r+1}(\mathscr{C}) - 1.$$

De esta manera, $d_r(\mathscr{C}) \leq d_{r+1}(\mathscr{C}) - 1 < d_{r+1}(\mathscr{C})$, que es lo que queríamos probar. □

Teorema 2.4. *Sea $\mathscr{C}_1$ un código lineal de parámetros $[n, k_1]$ y $\mathscr{C}_2 \subset \mathscr{C}_1$ un subcódigo de $\mathscr{C}_1$ de parámetros $[n, k_2]$. Entonces*

$$M_m(\mathscr{C}_1, \mathscr{C}_2) \leq n - k_1 + m, \text{ con } m = 1, 2, \ldots, k_1 - k_2.$$

Demostración. De la definición 2.8 se sigue que $K_{n-k_2}(\mathscr{C}_1, \mathscr{C}_2) \geq k_1 - k_2$. Empleando la relación que existe entre K y M dada por el teorema 2.3 se sigue que

$$M_{k_1-k_2}(\mathscr{C}_1, \mathscr{C}_2) = \text{mín}\{i : K_i(\mathscr{C}_1, \mathscr{C}_2) \geq k_1 - k_2\} \leq n - k_2.$$

Además, puesto que por la proposición 2.5, se cumple que $M_{k_1-k_2}(\mathscr{C}_1, \mathscr{C}_2) \leq n - k_2$, y $M_0(\mathscr{C}_1, \mathscr{C}_2) = 0$. De esta manera, para todo $1 \leq m \leq k_1 - k_2$, aprovechando el carácter creciente de M con m, se sigue que

$$M_m(\mathscr{C}_1, \mathscr{C}_2) \leq n - k_1 + m.$$

□

Teorema 2.5. *(Cota de Singleton generalizada). Para un código lineal $\mathscr{C}$ de parámetros $[n, k]$ se tiene, para cada $1 \leq m \leq k$, que*

$$d_m(\mathscr{C}) \leq n - k + m.$$

Aquellos que alcanzan la cota de Singleton son los códigos MDS.

Demostración. No es más que un corolario del teorema 2.4 aplicando lo señalado en la nota 2.4, sin embargo, se ofrece como complemento una prueba diferente. La demostración se realizará por inducción sobre $k - m$. Supongamos que $k - m = 0$. Entonces, por la proposición 2.6 se sigue que $d_m = d_k \leq n = n - 0 = n - (k - m) = n - k + m$.

Asumamos ahora que se cumple que $d_m \leq n - k + m$ para algún $m \leq k$. De la proposición 2.6 se tiene que

$$d_{m-1} \leq d_m - 1 \leq n - k + (m - 1),$$

de donde se sigue el resultado. □

Análogamente, se probaría el siguiente resultado.

Corolario 2.1. *En las mismas condiciones que en el teorema anterior, se sigue que*

$$M_m(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) \leq k + m, \text{ con } m = 1, 2, \ldots, k_1 - k_2.$$

Estamos en condiciones ahora de enunciar un teorema que relacione los pesos relativos de Hamming generalizados con el umbral (r, t) del esquema de reparto de secretos.

Teorema 2.6. *Sea el esquema de reparto de secretos de la definición 2.2. Sea un conjunto de índices $\mathscr{J} \subset \{1, 2, \ldots, n\}$. Entonces el máximo valor de t para el cual se tiene que $I(S; C_{\mathscr{J}}) = 0$ para todo $|\mathscr{J}| \leq t$ es*

$$t = M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) - 1,$$

y el mínimo valor de r para el cual se da que $I(S; C_{\mathscr{J}}) = H(S)$ para todo $|\mathscr{J}| \geq r$ es

$$r = n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1.$$

Demostración. Sea $\mathscr{J} \subset \mathscr{A}$ un conjunto de índices con $|\mathscr{J}| = m$. De acuerdo con el lema 1.7

$$I(S; C_{\mathscr{J}}) = H(S) - H(S|C_{\mathscr{J}}).$$

Por definición, se sigue que

$$\begin{aligned} \Delta_m &= \min_{\mathscr{J} \subset \mathscr{A}, |\mathscr{J}| = m} H(S|C_{\mathscr{J}}) \\ &= \min_{\mathscr{J} \subset \mathscr{A}, |\mathscr{J}| = m} \big(H(S) - I(S; C_{\mathscr{J}})\big) \\ &= H(S) - \max_{\mathscr{J} \subset \mathscr{A}, |\mathscr{J}| = m} I(S; C_{\mathscr{J}}). \end{aligned}$$

Por tanto, aplicando el teorema 2.2

$$\begin{aligned}\max_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} I(S;C_{\mathscr{J}}) &= H(S) - \min_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} H(S|C_{\mathscr{J}}) \\ &= \ell - \ell + K_m(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}) \\ &= K_m(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}).\end{aligned}$$

De acuerdo con las proposiciones 2.5 y 2.3, el tamaño más pequeño de $\mathscr{J}$ para el cual se tiene que $I(S;C_{\mathscr{J}}) = 1$ es

$$\min\{m : K_m(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}) = 1\} = M_1(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}).$$

De modo que si $|\mathscr{J}| \leq M_1(\mathscr{C}_2^{\perp},\mathscr{C}_1^{\perp}) - 1$, entonces $I(S;C_{\mathscr{J}}) = 0$.

Por otro lado, de acuerdo con el lema 2.1, para $i = 1, 2$ se tiene que

$$\dim\left(\mathscr{C}_i(\mathscr{A}\setminus\mathscr{J})\right) + \dim\left(P_{\mathscr{J}}(\mathscr{C}_i)\right) = \dim(\mathscr{C}_i).$$

Como además $\dim(\mathscr{C}_1) = \ell + \dim(\mathscr{C}_2)$ y

$$H(S|C_{\mathscr{J}}) = \ell - \dim\left(P_{\mathscr{J}}(\mathscr{C}_1)\right) + \dim\left(P_{\mathscr{J}}(\mathscr{C}_2)\right),$$

es claro que

$$\begin{aligned}H(S|C_{\mathscr{J}}) &= \ell - \dim\mathscr{C}_1 + \dim\left(\mathscr{C}_1(\mathscr{A}\setminus\mathscr{J})\right) + \dim\mathscr{C}_2 - \dim\left(\mathscr{C}_2(\mathscr{A}\setminus\mathscr{J})\right) \\ &= \dim\left(\mathscr{C}_1(\mathscr{A}\setminus\mathscr{J})\right) - \dim\left(\mathscr{C}_2(\mathscr{A}\setminus\mathscr{J})\right).\end{aligned}$$

Llamemos $\overline{\mathscr{J}} = \mathscr{A}\setminus\mathscr{J}$. Tomando en cuenta lo anterior, la información mutua mínima entre S y el vector de variables aleatorias $C_{\mathscr{J}}$ será

$$\begin{aligned}\min_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} I(S;C_{\mathscr{J}}) &= H(S) - \max_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} H(S|C_{\mathscr{J}}) \\ &= \ell - \max_{\mathscr{J}\subset\mathscr{A},|\mathscr{J}|=m} \left\{\dim\left(\mathscr{C}_1(\overline{\mathscr{J}})\right) - \dim\left(\mathscr{C}_2(\overline{\mathscr{J}})\right)\right\} \\ &= \ell - \max_{\overline{\mathscr{J}}\subset\mathscr{A},|\overline{\mathscr{J}}|=n-m} \left\{\dim\left(\mathscr{C}_1(\overline{\mathscr{J}})\right) - \dim\left(\mathscr{C}_2(\overline{\mathscr{J}})\right)\right\} \\ &= \ell - K_{n-m}(\mathscr{C}_1,\mathscr{C}_2).\end{aligned}$$

De acuerdo con la proposición 2.5, el tamaño más grande de $\mathscr{J}$ tal que $I(S;C_{\mathscr{J}}) = H(S) - 1$ viene dado por

$$\begin{aligned}\max\{m : K_{n-m}(\mathscr{C}_1,\mathscr{C}_2) = 1\} &= \max\{n-m : K_m(\mathscr{C}_1,\mathscr{C}_2) = 1\} \\ &= n - \max\{m : K_m(\mathscr{C}_1,\mathscr{C}_2) = 1\} \\ &= n - M_1(\mathscr{C}_1,\mathscr{C}_2).\end{aligned}$$

Por lo tanto, si

$$|\mathscr{J}| \geq n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1,$$

entonces $I(S; C_{\mathscr{J}}) = H(S)$.

Obsérvese que la demostración de este teorema muestra que los umbrales del esquema de reparto de secretos son siempre estrictos, pues se ha comprobado que existen conjuntos de índices $\mathscr{J} \subset \mathscr{A}$ con $|\mathscr{J}| = M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp})$ que cumplen que $I(S; C_{\mathscr{J}}) = 1$ y otros $\mathscr{J} \subset \mathscr{A}$ con $|\mathscr{J}| = n - M_1(\mathscr{C}_1, \mathscr{C}_2)$ tales que $I(S; C_{\mathscr{J}}) = H(S) - 1$. □

Corolario 2.2. *De acuerdo con el teorema anterior, se sigue que los umbrales del esquema de reparto de secretos con el que estamos trabajando son*

$$t = M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) - 1,$$
$$r = n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1.$$

Nota 2.5. *Supongamos que en la definición 2.2 el secreto* $\boldsymbol{s}$ *se elige de acuerdo a una distribución arbitraria sobre* $\mathbb{F}_q^n$ *e independiente de* $\boldsymbol{c}_2$*. También en este caso se cumple el teorema 2.6, aunque las cotas podrían no ser ajustadas.*

Para terminar, de acuerdo con el teorema 2.6, siempre será posible recuperar el secreto $\mathbf{s}$ a partir de un subconjunto de las partes. En efecto, el tamaño más pequeño del conjunto de índices $\mathscr{J}$ para el cual se tiene que $I(S; C_{\mathscr{J}}) = \ell = H(S)$ es, de manera análoga a como se vio en la demostración del teorema anterior,

$$\text{mín}\{m : K_m(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) = \ell\} = M_\ell(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}),$$

y como por la definición 2.9, $M_\ell(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) \leq n$, dicho subconjunto existe.

Finalmente trataremos de relacionar las cotas establecidas en el teorema 2.6

$$|\mathscr{J}| \leq M_1(\mathscr{C}_2^{\perp}\mathscr{C}_1^{\perp}) - 1, \tag{2.4}$$

$$|\mathscr{J}| \geq n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1. \tag{2.5}$$

con los pesos generalizados d_i. En nuestro caso, $i = 1$, y por tanto coinciden con la distancia mínima de cada uno de los códigos con los que estamos trabajando y sus duales (definición 1.22). De esta manera, no será necesario trabajar con las dimensiones relativas, sino con la distancia mínima de cada código, más fácil de calcular. Sin embargo, se perderá el carácter de cota afinada.

Proposición 2.7. *Partiendo de las igualdades obtenidas en el teorema 2.6, entonces* $M_1(\mathscr{C}_2^{\perp}\mathscr{C}_1^{\perp}) - 1 \geq d(\mathscr{C}_2^{\perp}) - 1$ *y* $n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1 \leq n - d(\mathscr{C}_1) + 1$.

Demostración. De la definición 2.9 se sigue que $M_1(\mathscr{C}_1, \mathscr{C}_2) \geq M_1(\mathscr{C}_1, \{\mathbf{0}\})$. De la nota 2.4 se sigue que $d(\mathscr{C}_1) = M_1(\mathscr{C}_1, \{\mathbf{0}\})$. Así, $M_1(\mathscr{C}_1, \mathscr{C}_2) \geq d(\mathscr{C}_1)$. Por lo tanto,

$$n - d(\mathscr{C}_1) + 1 \geq n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1.$$

De manera análoga, $M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) \geq M_1(\mathscr{C}_2^{\perp}, \{\mathbf{0}\}) = d(\mathscr{C}_2^{\perp})$. Entonces,

$$M_1(\mathscr{C}_2^{\perp}\mathscr{C}_1^{\perp}) - 1 \geq d(\mathscr{C}_2^{\perp}) - 1,$$

que es lo que queríamos probar. □

Con estas acotaciones, es posible estimar las cotas obtenidas en el teorema 2.6 pero tomando como parámetro la distancia mínima del código.

Corolario 2.3. *El conjunto $\mathscr{J}$ ofrece privacidad total del secreto si se tiene que $|\mathscr{J}| \leq d(\mathscr{C}_2^{\perp}) - 1$. El conjunto $\mathscr{J}$ ofrece reconstrucción única del secreto si se cumple que $|\mathscr{J}| \geq n - d(\mathscr{C}_1) + 1$.*

Demostración. No hay más que combinar las demostraciones del teorema 2.6 y de la proposición 2.7. □

Se muestra un ejemplo ahora en el que $M_1(\mathscr{C}_1, \mathscr{C}_2) > d(\mathscr{C}_1)$.

Ejemplo 2.4. Sea el código lineal binario $\mathscr{C}_1$ con matriz generatriz G_1 y el subcódigo $\mathscr{C}_2 \subset \mathscr{C}_1$ con matriz generatriz G_2

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \text{ y } G_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Claramente, $d(\mathscr{C}_1) = d(\mathscr{C}_2) = 2$. Si se comprueban, para todos los conjuntos de índices $\mathscr{J}$ de cardinal 2, los códigos $\mathscr{C}_1(\mathscr{J})$ y $\mathscr{C}_2(\mathscr{J})$, se observa que $K_2(\mathscr{C}_1, \mathscr{C}_2) = 0$. Puesto que la dimensión relativa es estrictamente creciente, $M_1(\mathscr{C}_1, \mathscr{C}_2) > 2$. Por lo tanto, $M_1(\mathscr{C}_1, \mathscr{C}_2) > d(\mathscr{C}_1)$.

Capítulo 3

Reparto de secretos sobre códigos MDS

Una vez hemos expuesto el esquema general del reparto de secretos para códigos encajados, pasaremos a particularizarlo para un tipo de códigos muy particular: los códigos MDS, esto es, aquellos que alcanzan la cota de Singleton, como se expuso en la definición 1.31. Para ello, se introducirá el esquema de Shamir, el primer formalismo dedicado a la explicación del reparto de secretos, y que apareció en 1979 en [17]. Se mostrará también, para dejar clara su implementación informática, el algoritmo empleado por este método de compartición de secretos. Posteriormente, una vez se han establecido las bases del esquema de Shamir, se extenderá el esquema de reparto de secretos de la definición 2.2 a los códigos Reed-Solomon tomando como referencia [14] y [6], recuperándose así el esquema de Shamir. Esto permitirá demostrar formalmente, mediante la aplicación de los resultados probados en el capítulo anterior, la seguridad del esquema de Shamir. En primer lugar, se expondrá un razonamiento intuitivo de la seguridad del esquema de Shamir. Posteriormente, se particularizará la definición 2.2 a los códigos Reed-Solomon, hallando a partir de estos el esquema de Shamir.

3.1. Esquema de Shamir

Como se mencionó en la introducción, el esquema de Shamir fue el primer esquema de reparto de secretos en presentar un riguroso formalismo, descrito en [17]. De este se derivan los demás, siendo la vía que une los esquemas de reparto de secretos con los códigos MDS, en particular, los Reed-Solomon. Describiremos un esquema de Shamir con umbral (r, t), del mismo modo que se hizo en el capítulo anterior.

Este esquema se basa en la interpolación de polinomios. Esto es, dados r puntos de la forma $(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)$, donde los x_i son distintos dos a dos, existe un único polinomio $q(x)$ de grado a lo sumo $r-1$ tal que $q(x_i) = y_i$ para $i = 1, 2, \ldots, r$. En base a la fórmula de la interpolación polinómica de Lagrange,

$$q(X) = \sum_{i=1}^{r} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}, \tag{3.1}$$

de donde se sigue que, efectivamente, $q(x_i) = y_i$ para $i = 1, 2, \ldots, r$ y que $\deg(q(X)) \leq r - 1$. El siguiente teorema dará cuenta de la existencia y unicidad del polinomio de interpolación de Lagrange (para más información se puede consultar [16]).

Teorema 3.1. *Dados r puntos de la forma $(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r) \in \mathbb{R}^2$ distintos dos a dos, existe un único polinomio $q(X)$ de grado menor o igual que $r-1$ que verifica que $q(x_i) = y_i$ para todo $i = 1, 2, \ldots r$.*

Demostración. La existencia del polinomio se ha mostrado en la ecuación 3.1, de modo que solo resta probar la unicidad. Esta se deduce del teorema fundamental del álgebra de la siguiente manera: si $p(X)$ fuese otro polinomio interpolador de grado menor o igual que $r-1$ entonces la diferencia $r(X) = q(X) - p(X)$ sería un polinomio con r ceros distintos $x_1, x_2, \ldots, x_r$, siendo un polinomio de grado a lo sumo $r-1$ pero con r raíces, por tanto, debe ser idénticamente nulo. Así, $r(X) = 0$ y $q(X) = p(X)$, obteniéndose la unicidad pedida. □

Definición 3.1. (Esquema de Shamir). Sean $1 \leq k \leq n$ y $1 \leq t \leq n - k$ dos números enteros, y tomemos $r = t + k$. Nótese que $1 \leq t < r \leq n$. Sea además $q = p^m$ una potencia de un primo p tal que $q \geq n$. El conjunto de posibles secretos será $S = \mathbb{F}_q^k$, de donde se extraerá aleatoriamente un secreto $\mathbf{s} = (s_0, s_1, \ldots, s_{k-1}) \in \mathbb{F}_q^k$.

Se elige ahora, de manera aleatoria sobre $\mathbb{F}_q^t$ un vector $\mathbf{c} = (c_0, c_1, \ldots, c_{t-1}) \in \mathbb{F}_q^t$ y se construye el polinomio

$$f = c_0 + c_1 X + c_2 X^2 + \ldots + c_{t-1} X^{t-1} + s_0 X^t + s_1 x^{t+1} + \ldots + s_{k-1} X^{t+k-1},$$

entregando al participante i-ésimo el valor $f(a_i) = b_i \in \mathbb{F}_q$, donde los valores $a_1, a_2, \ldots, a_n \in \mathbb{F}_q$ son elementos distintos dos a dos. Sin embargo, y a diferencia de los vectores $\mathbf{s}$ y $\mathbf{c}$, que únicamente los conoce quien reparte el secreto, los parámetros a_i, n, k, q, r, t y el proceso de cifrado de la información se suponen públicos. Este es el esquema de Shamir de umbral (r, t).

Recuperación del secreto. En efecto, estudiaremos ahora cómo sería posible recuperar el secreto a partir de r participantes. Sean $1 \leq i_1, i_2, \ldots, i_r \leq n$ un conjunto de índices. Puesto que estos índices representan un conjunto de participantes, cada uno de ellos tiene asignado un valor $b_{i_j} = f(a_{i_j})$, con $j = 1, 2, \ldots, r$. Como $r = t + k$ y f es un polinomio de grado estrictamente menor que r, este conjunto de participantes será capaz de recuperar f por medio del polinomio interpolador de Lagrange. De esta manera, obtendrán

$$f(X) = f_0 + f_1 X + f_2 X^2 + \ldots + f_{t+k-1} X^{t+k-1},$$

con $f_i \in \mathbb{F}_q$ para $1 \leq i \leq t + k - 1$, y como $s_0 = f_t$, $s_1 = f_{t+1}, \ldots, s_{k-1} = f_{t+k-1}$, el secreto habría sido recuperado (los elementos aleatorios del vector $\mathbf{c}$ que constituían los t primeros coeficientes de f se descartan).

Privacidad total del secreto. Si bien no daremos ahora una demostración formal (se dará cuando se introduzcan los esquemas basados en los códigos Reed-Solomon), es posible hacer un razonamiento intuitivo que proporcione información sobre el umbral t. Supongamos ahora un conjunto de índices $1 \leq i_1, i_2, \ldots, i_t \leq n$ que representan un grupo de t participantes reunidos para hallar el secreto $\mathbf{s}$. Como antes, conocen $b_{i_j} = f(a_{i_j})$, con $j = 1, 2, \ldots, t$. El objetivo es mostrar que cualquier secreto $\mathbf{s}' = (s'_1, s'_2, \ldots, s'_{k-1}) \in \mathbb{F}_q^k$ diferente a $\mathbf{s}$ puede dar lugar a los valores $b_{i_j} \in \mathbb{F}_q$ para $j = 1, 2, \ldots, t$. De esta manera, la incertidumbre sobre el secreto sería total, como hemos visto en el capítulo anterior, e incluso disponiendo de una capacidad computacional ilimitada el secreto no podría recuperarse.

Por el teorema de interpolación de Lagrange, existe un único polinomio de grado menor que t tal que

$$h(X) = c'_0 + c'_1 X + c'_2 X^2 + \ldots + c'_{t-1} X^{t-1},$$

con $c'_i \in \mathbb{F}_q$ para cada $1 \leq i \leq t - 1$ y que cumpla

$$h(a_{i_j}) = b_{i_j} - \sum_{i=0}^{k-1} s'_i a_{i_j}^{t+i}, \text{ con } j = 1, 2, \ldots, t.$$

De esta manera, es posible construir un polinomio $g(X)$ de tal forma que

$$\begin{aligned} g(X) &= h(X) + \sum_{i=0}^{k-1} s'_i X^{t+i} \\ &= c'_0 + c'_1 X + \ldots + c'_{t-1} X^{t-1} + s'_0 X^t + s'_1 x^{t+1} + \ldots + s'_{k-1} X^{t+k-1}. \end{aligned}$$

Así, es posible obtener $b_{i_j} = g(a_{i_j}) = f(a_{i_j})$ para cada $j = 1, 2, \ldots, t$. Por tanto, los b_{i_j} podrían haberse obtenido también si se hubiera considerado el secreto $\mathbf{s}'$.

Quedaría demostrar que el vector $\mathbf{c}' = (c'_0, c'_1, \ldots, c'_{t-1}) \in \mathbb{F}_q^t$ es una variable aleatoria sobre $\mathbb{F}_q^t$, pues $\mathbf{c}$ también lo era. Busquemos una relación entre $\mathbf{c}$ y $\mathbf{c}'$ por medio de la siguiente matriz de Vandermonde de tamaño $t \times t$ sobre $\mathbb{F}_q$

$$V = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ a_{i_1} & a_{i_2} & \ldots & a_{i_t} \\ a_{i_1}^2 & a_{i_2}^2 & \ldots & a_{i_t}^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_1}^{t-1} & a_{i_2}^{t-1} & \ldots & a_{i_t}^{t-1} \end{bmatrix}.$$

Por el teorema de interpolación de Lagrange, esta matriz es invertible (obsérvese [16]). Sea $\mathbf{d} = (d_{i_1}, d_{i_2}, \ldots, d_{i_t}) \in \mathbb{F}_q^t$ tal que

$$d_{i_j} = \sum_{i=0}^{k-1} (s_i - s'_i) a_{i_j}^{t+1} \text{ para cada} j = 1, 2, \ldots, t.$$

Es posible ver entonces que

$$\mathbf{c'}V = \mathbf{c}V + \mathbf{d}, \text{ siendo } \mathbf{c'} \text{ y } \mathbf{c} \text{ vectores fila.}$$

Como V es invertible, se sigue que $\mathbf{c'} = \mathbf{c} + \mathbf{d}V^{-1}$, y puesto que $\mathbf{d}V^{-1} \in \mathbb{F}_q^t$ únicamente depende de $a_{i_1}, a_{i_2}, \ldots, a_{i_t}$ y de las componentes de $\mathbf{s}$ y $\mathbf{s'}$, que son elementos fijos de $\mathbb{F}_q$ no aleatorios, $\mathbf{c'}$ es la traslación de una variable aleatoria uniforme sobre $\mathbb{F}_q^t$, de modo que $\mathbf{c'}$ también lo es.

Una vez mostrado el proceso de reconstrucción y la privacidad del secreto, se darán unas breves definiciones sobre ciertos tipos de esquemas de Shamir. Estos no son más que una particularización del caso general, y se clasificarán en función de la relación existente entre t y r.

Definición 3.2. (Esquema perfecto de Shamir). Un esquema umbral tal que $r = t + 1$ también se llama *perfecto*, ya que un conjunto $\mathscr{J} \subset \{1, 2, \ldots, n\}$ puede o bien tener el secreto si $|\mathscr{J}| \geq t + 1$ o bien ninguna información acerca del secreto, si $|\mathscr{J}| \leq t$. Un esquema de Shamir puede hacerse perfecto tomando $k = 1$. Este caso es interesante pues el secreto s es un escalar, esto es, $s \in \mathbb{F}_q$, y es igual al tamaño de los datos de cada participante, $\log_2(q)$ bits. Esta propiedad es necesaria para todo esquema perfecto.

Definición 3.3. (Esquemas rampa). Aquellos en los que $k > 1$ son los *esquemas rampa*. Así, tendremos que $r > t+1$ y existen conjuntos de participantes

$\mathscr{J}$ tales que $t < |\mathscr{J}| < r$, para los cuales los participantes de $\mathscr{J}$ puedan adquirir cierta información sobre el secreto. Este caso fue estudiado en la sección anterior, en particular en el teorema 2.1.

Ejemplo 3.1. Vamos a construir un esquema de Shamir de umbral $(3, 6)$. Sea $q = 2^3 = 8$, y el cuerpo $\mathbb{F}_8$. Sea α un elemento generador de $\mathbb{F}_8^*$. Para cada $i = 1, 2, \ldots, 6$ asignemos a cada participante el valor $x_i = \alpha^i$. Supongamos que el secreto S da como resultado el valor $s = \alpha^5$, que queremos repartir. De manera aleatoria y uniforme sobre $\mathbb{F}_8$, se toma $a_1 = \alpha^3$ y $a_2 = \alpha^6$, tal que

$$q(X) = \alpha^5 + \alpha^3 X + \alpha^6 X^2.$$

Recordemos que dado un elemento generador del grupo multiplicativo, el cuerpo $\mathbb{F}_8$ puede ser descrito como $\mathbb{F}_8 \equiv \frac{\mathbb{F}_8[\alpha]}{(\alpha^3+\alpha+1)}$, por ejemplo. Evaluando, se sigue que, $y_1 = q(\alpha) = \alpha^3, y_2 = q(\alpha^2) = \alpha^3, y_3 = q(\alpha^3) = \alpha^6, y_4 = q(\alpha_4) = \alpha^5, y_6 = q(\alpha_6) = \alpha^6$. Imaginemos que los participantes 2, 3 y 5 se unen para obtener el secreto. Entonces es claro que

$$\begin{aligned} c_2 &= \frac{x_3}{x_3 - x_2}\frac{x_5}{x_5 - x_2} = 1 \\ c_3 &= \frac{x_2}{x_2 - x_3}\frac{x_5}{x_5 - x_3} = 1 \\ c_5 &= \frac{x_2}{x_2 - x_5}\frac{x_2}{x_2 - x_5} = 1 \end{aligned}$$

Puesto que $c_2 y_2 + c_3 y_3 + c_5 y_5 = \alpha^5 = s$, el secreto ha sido reconstruido.

Resulta interesante mostrar el algoritmo empleado por Shamir para un esquema perfecto de reparto de secretos.

Algorithm 1 Esquema de Shamir

Require: Secreto s, umbral k, número total de partes n.

Ensure: Partes distribuidas entre los participantes y reconstrucción del secreto

1: Elija una potencia de un número primo q
2: Elija un polinomio aleatorio $q(X)$ de grado $k-1$ sobre $\mathbb{F}_q$ tal que $f(0) = s$
3: **for** $i = 1$ to n **do**
4: Calcule $f(i)$
5: Distribuya la acción $(i, f(i))$ entre los participantes
6: **end for**
7: **Reconstrucción del Secreto:**
8: Reúna un conjunto de acciones de tamaño al menos t
9: Utilice el algoritmo de interpolación de Lagrange para encontrar $f(x)$ que pasa por los puntos dados
10: El secreto original s es $f(0)$

3.2. Particularización al caso de códigos Reed-Solomon.

En este capítulo particularizaremos el esquema de reparto de secretos al caso de códigos correctores de errores de tipo MDS, y en particular, para los códigos Reed-Solomon descritos en el primer capítulo, recuperando a partir de ellos el esquema de Shamir. Se mostrará, además, cómo quedan las cotas de 2.6 aplicadas a los códigos MDS, empleando para ello los resultados del segundo capítulo. Describir el esquema de Shamir en función de los códigos Reed-Solomon encuentra entre sus ventajas el demostrar formalmente su seguridad del método.

Supongamos n participantes, y sea $\mathscr{L}$ un código Reed-Solomon de dimensión ℓ sobre $\mathbb{F}_q$, esto es, $RS_{\ell,n}$. Sea $\mathscr{C}_1$ el código Reed-Solomon $RS_{k_1,n}$ obtenido de expandir $\mathscr{L}$. Sea $\mathscr{C}_2$ el código Reed-Solomon empleado para completar $\mathscr{L}$ hasta $\mathscr{C}_1$, esto es, $RS_{k_2,n}$, con $k_1 = k_2 + \ell$, de modo que $\mathscr{C}_1 = \mathscr{C}_2 \oplus \mathscr{L}$. Así, encontramos una formulación del esquema de reparto de secretos similar a la que se describió en la definición 2.2. Consideremos ahora un secreto $\mathbf{s} = (s_0, s_1, \ldots, s_{\ell-1}) \in \mathbb{F}_q^\ell$, elegido de manera uniforme y aleatoria sobre $\mathbb{F}_q^\ell$. A partir de $\mathbf{s}$ se construye el polinomio $f(X)$ de la siguiente manera

$$f(X) = s_0 + s_1 X + \ldots + s_{\ell-1} X^{\ell-1}.$$

Sean $a_1, a_2, \ldots, a_n$ elementos distintos de $\mathbb{F}_q$, de modo que

$$(f(a_1), f(a_2), \ldots, f(a_n)) \in RS_{\ell,n}.$$

Sea $\mathbf{c}_2 = (c'_0, c'_1, \ldots, c'_{k_2-1}) \in \mathscr{C}_2$ una palabra elegida de manera aleatoria sobre $\mathscr{C}_2$ e independiente de $\mathbf{s}$. Como antes, será posible construir el polinomio

$$g(X) = c'_0 + c'_1 X + \ldots c'_{k_2-1} X^{k_2-1},$$

de forma que $(g(a_1), g(a_2), \ldots, g(a_n)) \in RS_{k_2,n}$. Sea ahora $\mathbf{c}_1 \in \mathscr{C}_1$ tal que

$$\mathbf{c}_1 = \big(g(a_1) + a_1^{k_2} f(a_1), g(a_2) + a_2^{k_2} f(a_2), \ldots, g(a_n) + a_n^{k_2} f(a_n)\big) \in RS_{k_1,n},$$

pues existe un polinomio $h(X) = g(X) + X^{k_2} f(X)$ con grado $\deg h(X) < k_1$ tal que $h(a_i) = g(a_i) + a_i^{k_2} f(a_i)$. En efecto,

$$h(X) = c_0 + c_1 X + \ldots c'_{k_2-1} X^{k_2-1} + s_0 X^{k_2} + \ldots s_{\ell-1} X^{k_2+\ell-1}.$$

De esta manera, y de acuerdo con lo expuesto en el teorema 2.1, un conjunto de índices cualesquiera ofrecerá privacidad total del secreto si y solo si $\dim(\mathscr{C}_1) = \dim(\mathscr{C}_2)$, esto es, si y solo si $k_1 = k_2$ y $\ell = 0$. Por el contrario, el secreto podrá reconstruirse si y solo si $\dim(\mathscr{C}_1) - \dim(\mathscr{C}_2) = \ell$, o sea, si y solo si $k_1 - k_2 = \ell$, con $\ell > 0$. Nótese que hemos reconstruido el esquema de secretos de Shamir a partir de códigos Reed-Solomon, y aplicando el teorema 2.1 del capítulo dos, hemos podido obtener una demostración algebraica del esquema de Shamir, donde $r = k_1$ y $t = k_2$, con $r = t + \ell$, con $1 \leq \ell \leq n$.

$(RS_k(n, b))^\perp = RS_{n-k}(n, n - b + 1)$.

Por último, observemos cómo varían las cotas dadas en 2.6 para los códigos MDS. Sea $\mathscr{C}$ un código MDS sobre $\mathbb{F}_q$ de dimensión k y de longitud n. Entonces $\mathscr{C}^\perp$ es también un código MDS por el corolario 1.6 de parámetros $[n, n-k, k+1]$. Del teorema 2.5, se sigue que

$$\begin{aligned} &d_m(\mathscr{C}) = n - k + m, \text{ con } m = 1, 2, \ldots, k. \\ &d_m(\mathscr{C}^\perp) = k + m, \text{ con } m = 1, 2, \ldots, k. \end{aligned} \tag{3.2}$$

Sea $\mathscr{C}_2 \subset \mathscr{C}_1$ dos códigos MDS tales que $\dim(\mathscr{C}_1) = k_1$ y $\dim(\mathscr{C}_2) = k_2$ y $l = k_1 - k_2$. De las definiciones 2.11 y 2.12 se sigue que $M_m(\mathscr{C}_1, \mathscr{C}_2) \geq d_m(\mathscr{C}_1)$, para $m = 1, 2, \ldots, l$ (pues la definición de los pesos relativos es más restrictiva que la de los pesos generalizados). De manera análoga, se tendría que $M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) \geq d_m(\mathscr{C}_2^\perp)$.

Como hemos visto, la cota de Singleton para pesos generalizados es idéntica para los pesos de Hamming relativos generalizados. Como estamos tratando con códigos MDS, se cumple por una parte que $d_m(\mathscr{C}_1) = n-k+m$, con $d_m \leq M_m(\mathscr{C}_1, \mathscr{C}_2)$. Sin embargo, por el teorema 2.4 se tiene que $M_m(\mathscr{C}_1, \mathscr{C}_2) \leq n - k + m = d_m(\mathscr{C}_1)$. Por lo tanto, $M_m(\mathscr{C}_1, \mathscr{C}_2) = d_m(\mathscr{C}_1)$, y razanando de manera equivalente, $M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) = d_m(\mathscr{C}_2^\perp)$.

Finalmente, será posible enunciar un esquema de reparto de secretos con umbrales que dependan de los pesos relativos de Hamming generalizados para $m > 1$.

Definición 3.4. Diremos que un esquema de reparto de secretos tiene umbral de privacidad $(t_1, \ldots, t_\ell)$ y de reconstrucción $(r_1, \ldots, r_\ell)$ si $t_1, \ldots, t_\ell$ son los mayores valores posibles y $r_1, \ldots, r_\ell$ son los menores valores posibles para los cuales:

1. Un adversario no puede obtener m q-bits de información sobre el secreto $\mathbf{s}$ con t_m particiones.

2. Un adversario puede reconstruir m q-bits de información sobre el secreto $\mathbf{s}$ con r_m particiones.

Observemos que para $\ell = 1$ recuperamos el esquema de la definición 2.2, obteniendo r y t a partir del teorema 2.6. En base a lo discutido en el capítulo segundo, $t_m = M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) - 1$, pues $M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp)$ es el tamaño más pequeño del conjunto de índices que puede recuperar m q-bits de información sobre $\mathbf{s}$ (teorema 2.2). Del mismo modo, será posible (léase [6]) poner r_m como $r_m = n - M_{\ell-m+1}(\mathscr{C}_1, \mathscr{C}_2) + 1$.

Proposición 3.1. *Con la notación empleada anteriormente,*

$$M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) = n - M_{\ell-m+1}(\mathscr{C}_1, \mathscr{C}_2) + 1.$$

Demostración. Partiendo de las ecuaciones 3.2, es claro que

$$\begin{aligned} &d_m(\mathscr{C}_2) = n - k_2 + m, \text{ con } m = 1, 2, \ldots, \ell. \\ &d_m(\mathscr{C}^\perp) = M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) = k_2 + m, \text{ con } m = 1, 2, \ldots, \ell. \end{aligned}$$

Por otro lado,

$$\begin{aligned} M_{\ell-m+1}(\mathscr{C}_1, \mathscr{C}_2) = d_{\ell-m+1} &= n - k_1 + \ell - m + 1 \\ &= n - k_1 + k_1 - k_2 - m + 1 \\ &= n - k_2 - m + 1. \end{aligned}$$

De donde se obtiene que

$$n - M_{\ell-m+1}(\mathscr{C}_1, \mathscr{C}_2) + 1 = k_2 + m = M_m(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp).$$

□

Por lo tanto, si nos referimos a las acotaciones halladas por el teorema 2.6 y ponemos $t = M_1(\mathscr{C}_2^\perp, \mathscr{C}_1^\perp) - 1$ y $r = n - M_1(\mathscr{C}_1, \mathscr{C}_2)$, podremos probar el siguiente resultado.

Teorema 3.2. *Empleando la notación anterior, para un esquema de reparto de secretos formado por dos códigos lineales encajados MDS y partiendo de las cotas del teorema 2.6, se cumple que,*

$$t = r - 1.$$

Demostración. Por la proposición 3.1, si particularizamos para el caso en que $\ell = 1$ y $m = 1$, se sigue que

$$M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) = n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1.$$

De esta manera,

$$\begin{aligned} t &= M_1(\mathscr{C}_2^{\perp}, \mathscr{C}_1^{\perp}) - 1 \\ &= n - M_1(\mathscr{C}_1, \mathscr{C}_2) + 1 - 1 \\ &= n - M_1(\mathscr{C}_1, \mathscr{C}_2) \\ &= r - 1. \end{aligned}$$

□

Como consecuencia, para un caso más general, si se razona de manera similar, se tendría que

$$t_m = r_m - 1.$$

Capítulo 4

Reparto de secretos sobre códigos Reed-Muller

Si bien en el capítulo anterior se ha particularizado el esquema de reparto de secretos de la definición 2.2 para los códigos Reed-Solomon encajados, es posible dar un paso más. Recordemos que los códigos Reed-Solomon están basados en la evaluación de polinomios en una sola variable real sobre cuerpos finitos. Sin embargo, pese a que la seguridad de los esquemas de reparto de secretos basados en códigos MDS es óptima por lo demostrado en el capítulo anterior, el número de participantes n está limitado por el tamaño del cuerpo, de modo que $n \leq q$. El empleo de códigos Reed-Muller en el espacio afín de dimensión m permitirá aumentar el número de participantes, pues ahora $n \leq q^m$, por lo que n puede ser mayor que q. Existen otras familias de códigos que admiten un n mucho más grande que q, como los códigos álgebro-geométricos. A pesar de que estas otras familias de códigos no sean MDS, pueden escogerse pares de códigos encajados, por lo que podremos construir esquemas de reparto de secretos como los mostrados en el capítulo segundo. La principal referencia en este capítulo será [13].

4.1. Introducción a los códigos Reed-Muller

En esta sección se definirán propiamente los códigos Reed-Muller, y se dará cuenta de sus principales propiedades: dimensión, distancia mínima y código dual. Será importante asentar bien los conceptos de este tipo de códigos correctores, pues de ellos emanará otro esquema de reparto de secretos.

Se empezará definiendo una clase más general de códigos, los códigos de evaluación.

Definición 4.1. (Códigos de evaluación). Sea $\mathscr{P} = \{P_1, P_2, \ldots, P_n\}$ un conjunto de puntos pertenecientes a un conjunto $\mathbb{X}$ con cierta estructura geométrica. Sea V un espacio vectorial cuyos elementos son funciones del tipo

$$f : \mathbb{X} \longrightarrow \mathbb{F}_q.$$

Se considera ahora la aplicación de *evaluación en* $\mathscr{P}$ definida como

$$\begin{aligned} ev_{\mathscr{P}} : V &\longrightarrow \mathbb{F}_q^n, \\ f &\mapsto (f(P_1), f(P_2), \ldots, f(P_n)). \end{aligned}$$

Si la aplicación $ev_{\mathscr{P}}$ es lineal, su imagen será un subespacio vectorial de $\mathbb{F}_q^n$, esto es, un código lineal sobre $\mathbb{F}_q$ de longitud n, cuyas palabras serán los $ev_{\mathscr{P}}(f)$, con $f \in V$. Diremos que este es un *código obtenido por evaluación en* $\mathscr{P}$ *de las funciones de* V. Los parámetros de este código podrán deducirse a partir de las características de V como subespacio vectorial.

Los códigos Reed-Muller son un tipo especial de códigos de evaluación, donde $\mathbb{X} = \mathbb{F}_q^m$ y $V = \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ es el anillo de polinomios sobre $\mathbb{F}_q$ en las variables $X_1, X_2, \ldots, X_m$. La definición 4.1 también incluye a los códigos álgebro-geométricos, donde $\mathbb{X}$ es una curva algebraica sobre un cuerpo finito y V es un espacio de Riemann-Roch. Comenzaremos exponiendo ciertas propiedades del anillo de polinomios V que serán de gran interés para el desarrollo de este capítulo. En primer lugar, un polinomio de $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ es de la forma

$$f(X_1, X_2, \ldots, X_m) = \sum_{i_1, i_2, \ldots, i_m} a_{i_1, i_2, \ldots, i_m} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m},$$

donde los i_j son enteros no negativos y los $a_{i_1, i_2, \ldots, i_m} \in \mathbb{F}_q$.

Definición 4.2. Al evaluar todos los puntos de $\mathbb{F}_q^m$, f induce una función

$$\hat{f} : \mathbb{F}_q^m \longrightarrow F_q,$$

llamada *función polinómica asociada a* f. De ahora en adelante, ambas funciones se representarán con la letra f indistintamente.

Nótese que en $\mathbb{R}$ y en $\mathbb{C}$ distintos polinomios inducen funciones polinómicas distintas. Sin embargo, en un cuerpo finito no se mantiene esta propiedad, pues para todo $a \in \mathbb{F}_q$ se cumple que $a^q = a$, de modo que los polinomios X_i y X_i^q son distintos pero inducen la misma función polinómica. Es por ello que se debe considerar el anillo cociente

$$A = \mathbb{F}_q[X_1, X_2, \ldots, X_m] / \langle X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m \rangle.$$

De esta manera, la clase del polinomio $f = \sum a_{i_1,i_2,\ldots,i_m} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m}$, tiene un único representante $f^* = \sum b_{j_1,j_2,\ldots,j_m} X_1^{j_1} X_2^{j_2} \cdots X_m^{j_m}$, donde se cumple que $0 \leq j_1, j_2 \ldots, j_m \leq q-1$. Al polinomio f^* se le conoce como *polinomio reducido de* f e induce la misma función polinómica que f. El polinomio f^* se obtiene a partir de f, tomando como exponentes j_l los reducidos de los i_l módulo $q-1$ y sumando los monomios así obtenidos.

La siguiente proposición afirma que el cociente A nos da exactamente un representante para cada función polinómica en m variables.

Proposición 4.1. *Sea* $f \in \mathbb{F}_q[X_1, X_2, \ldots, X_m]$. *Si* $f(\boldsymbol{v}) = 0$ *para todo* $\boldsymbol{v} \in \mathbb{F}_q^m$, *entonces* $f^* = 0$.

Demostración. Por inducción sobre m. Para $m = 1$ el resultado es claramente cierto, pues el polinomio f^* tendría $\mathbb{F}_q$ raíces, pero $\deg f^* < |\mathbb{F}_q|$. Puesto que el número de raíces distintas de un polinomio es a lo sumo su grado, necesariamente $f^* = 0$. Supongamos que la proposición se cumple para $m-1$. Sea $f^* \in \mathbb{F}_q[X_1, X_2, \ldots, X_m]$. Si agrupamos los monomios de f^* que tengan el mismo exponente en X_m, se tiene que

$$f^* = g_0(X_1, \ldots, X_{m-1}) + g_1(X_1, \ldots, X_{m-1})X_m + \ldots + g_m(X_1, \ldots, X_{m-1})X_m^r,$$

donde $r < q$ y los $g_i(X_1, \ldots, X_{m-1}) \in \mathbb{F}_q[X_1, \ldots, X_{m-1}]$ son reducidos. Para $(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}) \in \mathbb{F}_q^{m-1}$ se considera el polinomio

$$\begin{aligned} &f^*(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}, X_m) \\ &= g_0(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}) + g_1(\alpha_1, \ldots, \alpha_{m-1})X_m + \ldots + g_r(\alpha_1, \ldots, \alpha_{m-1})X_m^r. \end{aligned}$$

Vemos que este polinomio está en $\mathbb{F}_q[X_m]$, es reducido y que tiene por raíces todos los elementos de $\mathbb{F}_q$, así, $f^*(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}, X_m) = 0$, es decir, que $g_i(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}) = 0$ para $i = 0, 1, \ldots, r$. Es necesario decir que f y f^* tienen la misma evaluación en todo punto de $\mathbb{F}_q^m$ porque su diferencia está en el ideal generado por los $x_i^q - x_i$, y cualquier combinación lineal de estos polinomios se anula en todo punto de $\mathbb{F}_q^m$, por lo que $f - f^*$ tiene como evaluación 0 en todo punto, es decir, f y f^* tienen la misma evaluación. Puesto que este razonamiento sirve para todos los puntos de $\mathbb{F}_q^{m-1}$, es posible aplicar la hipótesis de inducción, de modo que $g_i(X_1, X_2, \ldots, X_{m-1}) = 0$ para todo $i = 1, 2, \ldots, r$. Por lo tanto, $f^* = 0$. □

Es posible observar que dos polinomios pertenecientes a la misma clase en A (esto es, que sus polinomios reducidos coinciden) inducen la misma función polinómica, pues si f y g están en la misma clase, entonces $f - ges$ combinación de los $x_i^q - x_i$, y estos se anulan en todo punto. Recíprocamente,

por la proposición anterior, si dos polinomios inducen la misma función polinómica, ambos pertenecen a la misma clase de A. Pasemos ahora a definir propiamente los códigos Reed-Muller.

Proposición 4.2. *Sea $m \in \mathbb{N}$. Sea el cuerpo finito $\mathbb{F}_q$ y sea $n = q^m$. Impongamos una relación de orden sobre el conjunto $\mathbb{F}_q^m$, de modo que $\mathbb{F}_q^m = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$. Sea $\mathscr{P} = \mathbb{F}_q^m$. Entonces la aplicación de evaluación*

$$\begin{aligned} ev : \mathbb{F}_q[X_1, \ldots, X_m] &\to \mathbb{F}_q^n, \\ f &\mapsto (f(\boldsymbol{v}_1), f(\boldsymbol{v}_2), \ldots, f(\boldsymbol{v}_n)). \end{aligned}$$

es lineal y sobreyectiva.

Demostración. Puesto que la linealidad resulta obvia, mostraremos únicamente la sobreyectividad. Se considera para cada $\mathbf{v} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_q^m$ el polinomio

$$F_{\mathbf{v}}(X_1, \ldots, X_m) = \prod_{i=1}^{m} [1 - (X_i - \alpha_i)^{q-1}],$$

que verifica que

$$F_{\mathbf{v}}(\mathbf{w}) = \begin{cases} 1 & \text{si } \mathbf{w} = \mathbf{v}; \\ 0 & \text{si } \mathbf{w} \neq \mathbf{v}. \end{cases}$$

(pues $(\beta_i - \alpha_i)^{q-1} = 1$ si $\beta_i \neq \alpha_i$ en $\mathbb{F}_q$). Así, el conjunto $\{ev(F_{\mathbf{v}}) : \mathbf{v} \in \mathbb{F}_q^m\}$ es una base de $\mathbb{F}_q^n$. De la linealidad de ev se tiene la sobreyectividad. En efecto, sea $\mathbf{b} \in \mathbb{F}_q^n = (b_1, b_2, \ldots, b_n)$. Haciendo

$$b_j = \sum_{i=1}^{n} \lambda_i F_{\mathbf{v}_i}(\mathbf{w}_j) = \lambda_j \text{ para cada } j = 1, 2, \ldots, n,$$

queda mostrada la sobreyectividad. □

Definición 4.3. Sean $r \in \mathbb{N}$. Entonces el conjunto $\mathbb{F}_q[X_1, X_2, \ldots, X_m]^{(r)}$ denotará el conjunto de polinomios en $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ con grado $\leq r$. Este conjunto es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión finita.

Con esto, es posible introducir ya una definición de los códigos Reed-Muller.

Definición 4.4. (Código Reed-Muller). Llamamos *código Reed-Muller q-ario de longitud $n = q^m$*, denotado por $RM_q(r, m)$, a la imagen del conjunto $\mathbb{F}_q[X_1, X_2, \ldots, X_m]^{(r)}$ por la aplicación ev de la proposición 4.2.

Nótese que de acuerdo con la proposición 4.2, $RM_q(r,m)$ es un subespacio vectorial de $\mathbb{F}_q^n$.

Corolario 4.1. *Si $r \geq m(q-1)$, entonces $RM_q(r,m) = \mathbb{F}_q^n$.*

Demostración. Es una consecuencia de la proposición 4.2, pues todo polinomio reducido tiene grado menor o igual que $m(q-1)$. □

De acuerdo con este último corolario, únicamente tiene sentido considerar códigos Reed-Muller en el rango $0 \leq r \leq m(q-1)$. Estos $m(q-1)$ códigos están relacionados por la inclusión

$$\langle (1,1,\ldots,1) \rangle = RM_q(0,m) \subset RM_q(1,m) \subset \cdots \subset RM_q(m(q-1),m) = \mathbb{F}_q^n.$$

Pasemos a estudiar ahora la dimensión de los códigos Reed-Muller. Por cómo están construidos, la dimensión de $RM_q(r,m)$ coincide con el número de monomios reducidos en $\mathbb{F}_q[X_1,\ldots,X_m]^{(r)}$. Para ello, será interesante incluir un primer resultado de combinatoria.

Lema 4.1. *El número de formas de colocar t objetos en m celdas, de manera que cada celda no contenga más de s objetos es*

$$\sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{t-i(s+1)+m+1}{t-i(s+1)}.$$

Demostración. El número de formas en que t objetos pueden colocarse en m celdas sin ninguna restricción es

$$\binom{t+m-1}{t}.$$

El número de formas en que se pueden colocar t objetos en m celdas, de manera que i celdas especificadas contengan al menos $s+1$ objetos, es

$$\binom{t-i(s+1)+m+1}{t-i(s+1)}.$$

Por el principio de inclusión-exclusión, obtenemos el resultado pedido. □

Finalmente, podremos dar la dimensión de un código Reed-Muller basándonos en el lema anterior.

Teorema 4.1. *La dimensión de $RM_q(r,m)$ es*

$$k = \sum_{t=0}^{r} \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{t-iq+m+1}{t-iq}.$$

Demostración. El número de monomios reducidos en $\mathbb{F}_q[X_1, \ldots, X_m]$ de grado exactamente t, donde $0 \leq t \leq m(q-1)$, es igual al número de m-uplas $(i_1, \ldots, i_m)$ tales que $0 \leq i_j \leq q-1$ para $j = 1, \ldots, m$ e $i_1 + \cdots + i_m = t$. Es decir, es el número de formas en que se pueden colocar t objetos en m celdas de manera que ninguna celda contenga más de $q-1$ objetos. El lema anterior proporciona, entonces, directamente el resultado. □

Corolario 4.2. *La dimensión del código $RM_2(r, m)$ es*

$$k = \sum_{t=0}^{r} \binom{m}{t}.$$

Demostración. La demostración es análoga a la de la proposición anterior. Únicamente basta con escoger t variables distintas entre las m disponibles, X_1, $X_2, \ldots, X_m$, es decir, $k = \binom{m}{t}$. □

A continuación, pasaremos a dar la distancia mínima de un código Reed-Muller. Si bien no entraremos detalladamente en esto, es conveniente señalar que los códigos Reed-Muller pueden tratarse como códigos cíclicos, mediante una ordenación conveniente de los elementos de $\mathbb{F}_q^m \setminus \{\mathbf{0}\}$. Brevemente, se darán las definiciones de código cíclico y de polinomio generador de un código cíclico.

Definición 4.5. (Código cíclico). Diremos que un código lineal $\mathscr{C}$ de longitud n sobre $\mathbb{F}_q$ es *cíclico* si la propiedad siguiente se verifica: si $(c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$. entonces $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathscr{C}$.

Para el estudio de los códigos cíclicos, es sumamente interesante la identificación que se muestra a continuación. En virtud de los isomorfismos entre espacios vectoriales,

$$\mathbb{F}_q^n \cong \mathbb{F}_q[X]/\langle X^n - 1\rangle \equiv R,$$

de modo que cada vector $(a_0, a_1, \ldots, a_{n-1})$ puede ser identificado con $a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ y con su clase en R, $a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + \langle X^n - 1\rangle$. Sin entrar en más detalle, diremos que todo ideal de A es principal. De esta manera, puede definirse el polinomio generador.

Definición 4.6. (Polinomio generador). Sea $\mathscr{C}$ un código lineal no nulo de longitud n. Existe un único polinomio mónico $g(X) \in \mathbb{F}_q[X]$, divisor de $X^n - 1$, tal que $\mathscr{C} = \langle g(X)\rangle$, llamado *polinomio generador* del código $\mathscr{C}$.

Sea $\alpha \in \mathbb{F}_{q^m}$ un elemento primitivo. Si $\mathbb{F}_q = \mathbb{F}_p[\alpha]$ y si $f(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$ es el polinomio irreducible de α sobre $\mathbb{F}_p$, se define la matriz

compañera C como

$$C = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix}.$$

De acuerdo con el capítulo cinco de [13], el grupo cíclico generado por C, llamado $< C >$, tiene orden $n-1$ (siendo $n = q^m$). Además, puede ser indentificado con $\mathbb{F}_{q^m}^*$. Sea un elemento no nulo $\mathbf{w}_1 \in \mathbb{F}_q^m$. Se definen recursivamente los vectores $\mathbf{w}_2, \mathbf{w}_3, \ldots, \mathbf{w}_{n-1}$ como

$$\mathbf{w}_i = \mathbf{w}_{i-1}C = \mathbf{w}_1 C^{i-1}.$$

Denotaremos por $RM_q^*(r,m)$ el código obtenido a partir de $RM_q(r,m)$ eliminando de todas las palabras la primera coordenada (la correspondiente a la evaluación del vector $\mathbf{0}$) y llamaremos $C(r,m)$ al código

$$C(r,m) = \{f(\mathbf{w}_1), \ldots, f(\mathbf{w}_{n-1}) \mid f \in \mathbb{F}_q[X_1, \ldots, X_m]^{(r)}\}.$$

Este último código es cíclico (puede consultarse el capítulo 12 de [13]) y es equivalente a $RM_q^*(r,m)$, pues únicamente difieren en una permutación de las coordenadas. Si asumimos para los $\mathbf{v}_i$ la misma ordenación que para los $\mathbf{w}_i$, entonces ambos códigos son iguales.

Conviene recordar, además, que todo $h \in \mathbb{Z}$, $h \geq 0$ puede ponerse en base q como

$$h = h_0 + h_1 q + h_2 q^2 + \ldots, \text{ con } 0 \leq h_i \leq q-1.$$

Denotaremos por *peso de h respecto de q*, a $w_q(h) = h_0 + h_1 + \ldots$. El siguiente resultado, que no demostraremos, puede encontrarse en [8], y sobre él descansa la prueba de la distancia mínima de un código Reed-Muller.

Teorema 4.2. *Sea α un elemento primitivo de $\mathbb{F}_{q^m}$. El polinomio $g(X)$, generador de $C(r,m)$, tiene entre sus raíces a los α^h con $0 < w_q(h) < m(q-1) - r$.*

Empleando ahora el teorema 4.2, será sencillo mostrar el siguiente resultado. Puesto que lo emplearemos en la demostración, es necesario mencionar que un código BCH sobre $\mathbb{F}_q$, de longitud n y de distancia mínima δ es un código cíclico generado por el polinomio cuyas raíces son $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$. Todo código BCH de distancia prevista δ tiene una distancia mínima d que verifica que $d \geq \delta$ (obsérvese la proposición 11.1.2 de [13]).

Teorema 4.3. *Si $r = v(q-1)+s$, con $0 \leq s \leq q-1$, entonces la distancia mínima de $RM_q(r,m)$ es $d = (q-s)q^{m-v-1}$.*

Demostración. Notemos que la distancia de un código $RM_q(r,m)$ es mayor que la de $RM_q^*(r,m)$, y por tanto, mayor que la de $C(r,m)$. Sea ahora

$$h_0 = (q-1) + (q-1)q + \ldots + (q-1)q^{m-v-2} + (q-1-s)q^{m-v-1}.$$

Evidentemente, si $0 < h < h_0$, se sigue que $0 < w_q(h) < w_q(h_0)$, donde

$$\begin{aligned} w_q(h_0) &= (m-v-1)(q-1) + (q-1-s) \\ &= (m-v)(q-1) - s = m(q-1) - r. \end{aligned}$$

Entonces, en virtud del teorema 4.2, α^h es una raíz de $g(X)$. Así, $C(r,m)$ es subcódigo de un código BCH (con $b = 1$) determinado por las raíces $\alpha, \alpha^2, \ldots, \alpha^{h_0-1}$, cuya distancia será, al menos, h_0. De esta manera,

$$\begin{aligned} d(C(r,m)) \geq h_0 &= (q-1)(1+q+\ldots+q^{m-v+2}) + (q-1-s)q^{m-v-1} \\ &= (q-s)q^{m-v-1}, \end{aligned}$$

donde la última igualdad viene dada por la fórmula de la suma de una progresión geométrica. De este modo, la distancia mínima de $RM_q(r,m)$, denotada por d, será $d \geq d(C(r,m))$. Para alcanzar la igualdad únicamente habremos de buscar una palabra de $RM_q(r,m)$ cuyo peso sea exactamente $(q-s)q^{m-v-1}$. Para ello, sean $\lambda_1, \ldots, \lambda_s \in \mathbb{F}_q$ elementos distintos con $\lambda_1 = 0$. El polinomio

$$f = \left[\prod_{i=1}^{v}(X_{v+1}^{q-1} - X_i^{q-1})\right]\left[\prod_{j=1}^{s}(X_{v+1} - \lambda_j)\right],$$

tiene grado $v(q-1)+s = r$, luego $ev(f) \in RM_q(r,m)$. Claramente, f se anula en todos los vectores de $\mathbb{F}_q^m$ salvo aquellos de la forma

$$(0, 0, \ldots, 0, a_{v+1}, a_{v+2}, \ldots, a_n),$$

con $a_{v+1} \neq \lambda_i$, con $i = 1, 2, \ldots, s$. Precisamente hay $(q-s)q^{m-v-1}$ de estos vectores, de modo que el peso de la palabra obtenida es $(q-s)q^{m-v-1}$. □

Para terminar con la introducción a los códigos Reed-Muller habremos de calcular su código dual, pues nos servirá para establecer las cotas sobre la seguridad del esquema como las del capítulo segundo. Comenzaremos probando un lema, que será de utilidad para determinar el código dual de un Reed-Muller. Posteriormente, se introducirá un corolario del lema, del cual se deducirá, posteriormente, los parámetros del código dual. Veremos posteriormente que, en efecto, $RM_q(r,m)^{\perp} = RM_q(m(q-1)-r-1, m)$.

Lema 4.2. *Sean $f \in \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ y f^* el reducido de f. Si $\deg(f^*) < m(q-1)$, entonces*

$$\sum_{\boldsymbol{v} \in \mathbb{F}_q^m} f(\boldsymbol{v}) = 0.$$

Demostración. Bastará realizar la prueba para el caso en que f es reducido. Para cada $\mathbf{v} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_q^m$, sea $F_{\mathbf{v}}$ el polinomio introducido en la demostración de la proposición 4.2,

$$F_{\mathbf{v}}(X_1, \ldots, X_m) = \prod_{i=1}^{m} \left[1 - (X_i - \alpha_i)^{q-1}\right],$$

donde recordemos que,

$$F_{\mathbf{v}}(\mathbf{w}) = \begin{cases} 1 & \text{si } \mathbf{w} = \mathbf{v}; \\ 0 & \text{si } \mathbf{w} \neq \mathbf{v}. \end{cases}$$

De acuerdo con esta definición, será posible escribir

$$f(X_1, \ldots, X_m) = \sum_{\mathbf{v} \in \mathbb{F}_q^m} f(\mathbf{v}) F_{\mathbf{v}}(X_1, \ldots, X_m),$$

ya que ambos son polinomios reducidos y sus evaluaciones coinciden en todo punto de $\mathbb{F}_q^m$, por lo que son iguales por la proposición 4.1. Ahora bien, aplicando el binomio de Newton (lema 1.1), es posible escribir

$$(X_i - \alpha_i)^{q-1} = X_i^{q-1} + \alpha_i X_i^{q-2} + \ldots + \alpha_i^{q-1},$$

podremos escribir

$$F_{\mathbf{v}} = (-1)^m X_1^{q-1} \cdots X_m^{q-1} + \text{términos de menor grado},$$

de esta manera,

$$\begin{aligned} f(X_1, \ldots, X_m) &= \sum_{\mathbf{v} \in \mathbb{F}_q^m} f(\mathbf{v})(-1)^m X_1^{q-1} \cdots X_m^{q-1} + \text{términos menor grado} \\ &= \left[(-1)^m \sum_{\mathbf{v} \in \mathbb{F}_q^m} f(\mathbf{v})\right] X_1^{q-1} \cdots X_m^{q-1} + \text{términos menor grado}, \end{aligned}$$

y como $\deg(f) < m(q-1)$, se verifica que $\sum_{\mathbf{v} \in \mathbb{F}_q^m} f(\mathbf{v}) = 0$, ya que el término $X_1^{q-1} \cdots X_m^{q-1}$ (de grado $m(q-1)$) debe desaparecer. □

Estamos en condiciones de enunciar y probar un corolario de este lema.

Corolario 4.3. *Sean $r, s \in \mathbb{N}$. Si $s < m(q-1) - r$, entonces se cumple que $RM_q(s,m) \subset RM_q(r,m)^\perp$.*

Demostración. Sean $\mathbf{c}_1 \in RM_q(r,m)$ y $\mathbf{c}_2 \in RM_q(m(q-1)-r-1,m)$. Supongamos que $\mathbf{c}_1 = ev(f)$, $\mathbf{c}_2 = ev(g)$ para ciertos f, g con $\deg(f) \leq r$, $\deg(g) \leq s$. Sea $*$ el producto componente a componente de dos vectores $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ y $\mathbf{w} = (w_1, w_2, \ldots, w_n)$, esto es,

$$\mathbf{v} * \mathbf{w} = (v_1 w_1, v_2 w_2, \ldots, v_n w_n).$$

Puesto que

$$\mathbf{c}_1 * \mathbf{c}_2 = ev(fg),$$

se tiene que,

$$\mathbf{c}_1 \cdot \mathbf{c}_2 = \sum_{\mathbf{v} \in \mathbb{F}_q^m} (fg)(\mathbf{v}) = 0,$$

en virtud del lema anterior. Esta igualdad implica el resultado. Además, de este lema puede observarse que

$$RM_q(m(q-1)-r-1,m) \subset RM_q(r,m)^\perp.$$

□

Finalmente, daremos un teorema para la dimensión de un código Reed-Muller dual, empleando el corolario y el lema anterior.

Teorema 4.4. $RM_q(r,m)^\perp = RM_q(m(q-1)-r-1,m)$.

Demostración. Por el corolario anterior, $RM_q(m(q-1)-r-1,m) \subset RM_q(r,m)^\perp$. Por tanto, basta con demostrar que

$$\dim\left(RM_q(r,m)\right) + \dim\left(RM_q(m(q-1)-r-1,m)\right) = n.$$

Esta igualdad se demuestra empleando la fórmula del teorema 4.1. Si bien la demostración del caso general es muy tediosa, pues se requiere emplear las propiedades de los números combinatorios, mostraremos únicamente el caso $q = 2$, de modo que la dimensión del dual sería $m - r - 1$. Así,

$$\dim(RM_2(r,m)) = \sum_{i=0}^{r} \binom{m}{i},$$

$$\dim(RM_2(m-r-1,m) = \sum_{i=0}^{m-r-1} \binom{m}{i} = \sum_{i=0}^{m-r-1} \binom{m}{m-i} = \sum_{j=r+1}^{m} \binom{m}{j}.$$

Así,

$$\begin{aligned}\dim\left(RM_q(r,m)\right)+\dim\left(RM_q(m(q-1)-r-1,m)\right) &= \sum_{i=0}^{r}\binom{m}{i}+\sum_{j=r+1}^{m}\binom{m}{j}\\ &= \sum_{i=0}^{m}\binom{m}{i}=(1+1)^m\\ &= 2^m=n,\end{aligned}$$

que es lo que queríamos probar. □

De esta manera, un código Reed-Muller $RM_q(r,m)$ presenta los siguientes parámetros:

1. Tiene **dimensión** $\dim(RM_q(r,m))=\sum_{t=0}^{r}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{t-iq+m+1}{t-iq}$.

2. La **distancia mínima** es $d=(q-s)q^{m-v-1}$, donde $0\leq s\leq q-1$ y $r=v(q-1)+s$.

3. Su **dual** es $RM_q(r,m)^{\perp}=RM_q(m(q-1)-r-1,m)$.

4.2. Reparto de secretos con códigos Reed-Muller

Una vez mostrados todos los parámetros de un código Reed-Muller, seremos capaces de construir un esquema de reparto de secretos sobre códigos Reed-Muller basándonos en la definición 2.2. Podremos, además, en base a las cotas halladas en el teorema 2.6, expresar los umbrales r y t en función de los parámetros correspondientes al código Reed-Muller.

Sea $\mathscr{C}_1$ un código Reed-Muller de parámetros (k_1,m), esto es, $\mathscr{C}_1=RM_q(k_1,m)$. Sea también $\mathscr{C}_2=RM_q(k_2,m)$ un código Reed-Muller de parámetros (k_2,m), con $k_2<k_1$. De acuerdo con la definición de los códigos Reed-Muller, es claro que $\mathscr{C}_2\subset\mathscr{C}_1$. En efecto, ambos son códigos Reed-Muller de longitud $n=q^m$, y además $\mathbb{F}_q[X_1,X_2,\ldots,X_m]^{k_2}\subset\mathbb{F}_q[X_1,X_2,\ldots,X_m]^{k_1}$. Por la proposición 4.2, sus imágenes por ev respetarán la misma relación de inclusión. De esta manera, $\mathscr{C}_2\subset\mathscr{C}_1$.

Sea $\mathscr{L}$ un código tal que $\mathscr{C}_1=\mathscr{L}\oplus\mathscr{C}_2$. Por álgebra lineal básica, es claro que

$$\dim(\mathscr{C}_1)=\dim(\mathscr{L})+\dim(\mathscr{C}_2).$$

En función de las dimensiones de los Reed-Muller halladas en el teorema 4.1, tenemos

$$\sum_{t=0}^{k_1}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{t-iq+m+1}{t-iq} =$$
$$\dim(\mathscr{L})+\sum_{t=0}^{k_2}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{t-iq+m+1}{t-iq}.$$

Entonces, podremos determinar la dimensión del espacio de secretos $\mathscr{L}$ como

$$\begin{aligned}\dim(\mathscr{L}) &= \dim(\mathscr{C}_1)-\dim(\mathscr{C}_2)\\ &= \sum_{t=k_2+1}^{k_1}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{t-iq+m+1}{t-iq}.\end{aligned}$$

Demos ahora los correspondientes valores de las cotas de los umbrales r y t del esquema de reparto de secretos de la definición 2.2. Para ello, usaremos las desigualdades obtenidas en el corolario 2.3. Por tanto, será necesario reescribir, en términos de las distancias mínimas de los códigos Reed-Muller, dichas cotas.

1. Necesitamos obtener, en primera instancia, la distancia mínima del código $\mathscr{C}_2^{\perp}$. El dual de un código Reed-Muller, de acuerdo con la proposición 4.4, es nuevamente un código Reed-Muller. En este caso, $\mathscr{C}_2^{\perp} = RM_q(k_2,m)^{\perp} = RM_q(m(q-1)-k_2-1,m)$. Por lo tanto, su distancia mínima, de acuerdo con el teorema 4.3, será

   $$d(\mathscr{C}_2^{\perp}) = (q-s_2)q^{m-v_2-1},$$

   donde $0\leq s_2\leq q-1$ y v_2 es tal que $k_2 = v_2(q-1)+s_2$.

2. Hallemos ahora la distancia mínima del código $\mathscr{C}_1$. Sin más que aplicar el teorema 4.3,

   $$d(\mathscr{C}_1) = (q-s_1)^{m-v_1-1},$$

   donde $0\leq s_1\leq q-1$ y v_1 es tal que $k_1 = v_1(q-1)+s_1$.

Por lo tanto, una vez recopilados todos los datos de acuerdo con los resultados enunciados en este capítulo sobre códigos Reed-Muller, y habiendo elegido un secreto $\mathbf{s}\in\mathscr{L}$, será posible decir que, de acuerdo con el corolario 2.3 y para un conjunto de índices $\mathscr{J}$:

- Si $|\mathscr{J}| \leq (q - s_2)q^{m-v_2-1} - 1$, el conjunto de índices ofrece privacidad total del secreto.
- Por el contrario, si $|\mathscr{J}| \geq n - (q - s_1)^{m-v_1-1} + 1$, el conjunto de índices ofrece la reconstrucción única del secreto.

Bibliografía

[1] Christopher M Bishop and Nasser M Nasrabadi. *Pattern recognition and machine learning*, volume 4. Springer, 2006.

[2] Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert De Haan, and Vinod Vaikuntanathan. Secure computation from random error correcting codes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 291–310. Springer, 2007.

[3] Thomas M Cover. *Elements of information theory*. John Wiley & Sons, 1999.

[4] FÉLIX DELGADO DE LA MATA, MARÍA CONCEPCIÓN FUERTES FRAILE, and SEBASTIAN XAMBO DESCAMPS. *Introducción al álgebra. 2a*. Ediciones Paraninfo, SA, 2021.

[5] G David Forney. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Transactions on information theory*, 40(6):1741–1752, 1994.

[6] Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Diego Ruano, and Yuan Luo. Relative generalized hamming weights of one-point algebraic geometric codes. *IEEE Transactions on Information Theory*, 60(10):5938–5949, 2014.

[7] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

[8] Tadao Kasami, Shu Lin, and W Peterson. New generalizations of the reed-muller codes–i: Primitive codes. *IEEE Transactions on information theory*, 14(2):189–199, 1968.

[9] Jun Kurihara, Tomohiko Uyematsu, and Ryutaroh Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight. *IEICE Transactions on*

Fundamentals of Electronics, Communications and Computer Sciences, 95(11):2067–2075, 2012.

[10] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[11] Yuan Luo, Chaichana Mitrpant, AJ Han Vinck, and Kefei Chen. Some new characters on the wire-tap channel of type ii. *IEEE Transactions on information theory*, 51(3):1222–1229, 2005.

[12] David JC MacKay. *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[13] Carlos Munuera and Juan Tena. *Codificación de Información*. Universidad de Valladolid, 1997.

[14] Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin, and Relinde Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, 2017.

[15] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[16] Jesús María Sanz-Serna. *Diez lecciones de cálculo numérico*. Universidad de Valladolid, Secretariado de Publicaciones e Intercambio Editorial, 2010.

[17] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[18] Douglas R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2(4):357–390, 1992.