UNIVERSIDAD AUTÓNOMA METROPOLITANA
Iztapalapa

Departamento de Matemáticas

Funciones perfectamente no-lineales, casi-bent, esquemas de compartición de secretos y autenticación

Presenta
Juan Carlos Ku Cauich

Asesor

Dr. Horacio Tapia Recillas

México
mayo de 2008

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE EXAMEN DE GRADO

No. 00023

FUNCIONES PERFECTAMENTE NO-LINEALES, CASI-BENT, ESQUEMAS DE COMPARTICION DE SECRETOS Y AUTENTICACION

UNIVERSIDAD AUTÓNOMA METROPOLITANA
DIRECCIÓN DE SISTEMAS ESCOLARES
Casa abierta al tiempo

JUAN CARLOS KU CAUICH
ALUMNO

REVISÓ

LIC. JULIO CESAR DE LARA ISASSI
DIRECTOR DE SISTEMAS ESCOLARES

En México, D.F., se presentaron a las 16:00 horas del día 25 del mes de agosto del año 2008 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. JOSE NOE GUTIERREZ HERRERA
DR. GUILLERMO MORALES LUNA
DR. HORACIO TAPIA RECILLAS

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRO EN CIENCIAS (MATEMÁTICAS)

DE: JUAN CARLOS KU CAUICH

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

DIRECTORA DE LA DIVISIÓN DE CBI

DRA. VERONICA MEDINA BAÑUELOS

PRESIDENTE

DR. JOSE NOE GUTIERREZ HERRERA

VOCAL

DR. GUILLERMO MORALES LUNA

SECRETARIO

DR. HORACIO TAPIA RECILLAS

Índice general

Agradecimientos

Agradezco a mis padres y hermanos, en general a toda mi familia y amigos, a mi asesor el Dr. Horacio Tapia Recillas, sin los cuales no hubiese sido posible realizar este trabajo. Al CONACYT por la ayuda económica. A los profesores que de forma directa o indirecta apoyaron en este trabajo.

Introducción

Las funciones Booleanas son aquellas cuyo dominio y contradominio son $\mathbb{F}_2^n$ y $\mathbb{F}_2$ respectivamente, es decir, $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Éstas son muy importantes en Teoría de Códigos y Criptografía ya que entre otras cosas generan vectores binarios, por ejemplo el código de Reed-Muller $R(r, n)$, el cual es el conjunto de los vectores binarios de longitud 2^n formado por las imágenes de las distintas funciones Booleanas de $\mathcal{B}_n$ de grado a lo más r (grado en su forma polinomial), donde $\mathcal{B}_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$. Estos códigos lineales son utilizados en varias aplicaciones, por ejemplo el código $R(1, 5)$, fue utilizado en 1972 para transmitir imágenes de marte por la nave Mariner 9. En general un $[n, k, d]_q$ código lineal $\mathcal{C}$ sobre un campo finito $\mathbb{F}_q$, q la potencia de un primo, es un subespacio lineal de $\mathbb{F}_q^n$ de dimensión k y peso mínimo d, donde

$$d := \text{ mín } \{w(x)|x \in \mathcal{C}, x \neq 0\},$$

y $w(x)$ es el peso de Hamming de un elemento x, el cual es el número de entradas distintas de cero de x. Se define también la distancia de Hamming entre dos funciones Booleanas f y g por

$$d(f, g) := |\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}|,$$

y la distancia de Hamming entre dos elementos

$$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n,$$

por

$$d(x, y) := |\{i|\ x_i \neq y_i, i = 1, \ldots, n\}|.$$

Las funciones "bent", que son un caso particular de funciones Booleanas, fueron introducidas y estudiadas por Rothaus en el año de 1976 ([**32**]). Estas son funciones cuya no-linealidad es máxima, es decir, se encuentran lo más alejadas posible de las funciones lineales Booleanas, o lo que es lo mismo, se encuentran lo más alejadas del código de Reed-Muller $R(1, n)$, alejadas en términos de la distancia de Hamming. Posteriormente las funciones bent han sido generalizadas para funciones $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, p un primo. Entre estas funciones también se encuentran las funciones "casi-bent", de las cuales se tiene su existencia cuando $p = 2$, estas funciones también tienen no-linealidad máxima. Las funciones bent y las casi-bent son muy importantes en Teoría de Códigos y Criptografía, algunas de estas aplicaciones como en criptoanálisis pueden ser encontradas por ejemplo en [**1**] y [**21**].

Los esquemas de compartición de secretos fueron introducidos por G. R. Blakley ([**2**]) y A. Shamir ([**33**]) en el año de 1979. Blakey en su esquema utiliza geometría proyectiva, mientras que Shamir basó su modelo en la interpolación de polinomios. Muchas construcciones se han propuesto desde entonces, una de estas es basada en la Teoría de Códigos, la cual se introduce en l981, después varios autores consideran los códigos lineales correctores de errores (consultar por ejemplo [**26**], [**28**]). Los esquemas de compartición de secretos consisten en distribuir la información de un secreto entre varias entidades, de modo que con la información de cierto número de estas entidades el secreto pueda ser recuperado. Por ejemplo, en un banco la clave para abrir una caja fuerte puede ser distribuida entre varias entidades. En un principio todo código lineal puede ser utilizado para la construcción de esquemas de compartición de secretos, pero determinar cuales conjuntos de entidades pueden ser utilizados para determinar el secreto, es muy difícil y esto depende de las palabras mínimas del código dual del código considerado ([**26**]). El presente trabajo está principalmente enfocado a describir esquemas de compartición de secretos basados en códigos lineales sobre un campo finito $\mathbb{F}_q$, $q = p^r$, los cuales a su vez se obtienen a partir de funciones perfectamente no-lineales (equivalentemente funciones bent) cuando $p \neq 2$ y funciones casi-bent cuando $p = 2$.

En el caso de $p \neq 2$ se ha seguido muy de cerca el trabajo [**6**] donde a partir de una función perfectamente no-lineal $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ se construye un código lineal sobre un campo de la forma $\mathbb{F}_{p^h}$, h un divisor de n, y este código, siguiendo la construcción de Massey ([**26**]) es usado para dar un esquema de compartición de secretos (Capítulo 4).

Para el caso $p = 2$, usando funciones casi-bent con ideas similares al caso $p \neq 2$ se define un código lineal sobre un campo de la forma $\mathbb{F}_{2^h}$ y se determinan algunas de sus propiedades las cuales son usadas para describir un esquema de compartición de secretos. Usando estos esquemas se determinan, de dos maneras, extensiones de esquemas de compartición de secretos cuando el campo base son los números binarios. Consideramos que con este caso, el cual no aparece en la literatura, queda cubierto el problema de describir esquemas de compartición de secretos basados en códigos lineales sobre un campo finito $\mathbb{F}_q$, $q = p^r$ de cualquier característica $p > 0$, determinados por funciones perfectamente no-lineales $(p \neq 2)$ y casi-bent $(p = 2)$.

Otra de las aplicaciones de las funciones perfectamente no-lineales y las casi-bent es en la descripción de esquemas de autenticación ([**36**]). Siguiendo [**18**] y [**8**] se presentan algunos de estos esquemas. Los esquemas de autenticación son diseñados para autentificar los mensajes transmitidos. Si una transmisor desea enviar un mensaje a un receptor, como el canal de comunicación es público, hay el riesgo de que un enemigo pueda deliberadamente observar y mas aún causar un disturbio en la comunicación. Un transmisor y un receptor comparten una llave secreta, al enviar una pieza de información al receptor, éste utiliza su llave para autenticar el mensaje en cuyo caso acepta el mensaje como auténtico o en caso

contrario es rechazado.

En los últimos años los esquemas de autenticación han sido objeto de estudios de diversos grupos de investigación ([**20**], [**12**], [**34**], [**35**]). Existen varias formas para describir estos esquemas entre los que se incluyen métodos combinatorios ([**37**]), algebraicos ([**39**]), por medio de anillos de Galois ([**29**]). Recientemente usando funciones perfectamente no-lineales y casi perfectamente no-lineales ([**18**], [**8**]) se han descrito esquemas de esta naturaleza.

Este trabajo consta de 6 capítulos. En el Capítulo 1 se dan definiciones y resultados básicos tales como la traza de un elemento de un campo, caracteres, sumas de Gauss y propiedades que se derivan de éstas, ya que varias de las propiedades de las funciones perfectamente no-lineales, casi-bent, se obtienen gracias a estas definiciones y resultados. En el Capítulo 2 introducimos la definición de una función Booleana, algunos conceptos de suma importancia como el espectro de Fourier, que es en términos de éste como se define una función perfectamente no-lineal. Posteriormente trabajamos con las funciones $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, p un número primo, de las cuales se definen las funciones bent vectoriales, casi-bent, perfectamente no-lineales y las casi perfectamente no-lineales. También analizamos la relación entre estas funciones. En el Capítulo 3 definimos las funciones bent $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$, q la potencia de un primo impar, los cuales resultan ser también funciones perfectamente no-lineales. El Capítulo 4 es dedicado a la construcción de códigos lineales utilizando funciones perfectamente no-lineales $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$, q la potencia de un primo impar, y posteriormente se da la construcción de esquemas de compartición de secretos en base a estos códigos, utilizando el método de Massey. En el Capítulo 5 se da la construcción de códigos lineales construidos en base a funciones casi-bent, es decir, para funciones $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, n impar, los cuales también son utilizados para la construcción de esquemas de compartición de secretos por el método de Massey, obteniendo de este modo la construcción de esquemas de compartición de secretos para funciones $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$, q cualquier primo. Existen casos en que el espacio secreto es pequeño, o sea $\mathbb{F}_2$, en estos casos se dan dos extensiones de estos esquemas los cuales nos generan esquemas con un espacio de secretos mayor a comparación del original. Finalmente en el Capítulo 6 se da la construcción de esquemas de autenticación por medio de las funciones perfectamente no-lineales y las casi-bent.

Capítulo 1

Antecedentes

Definiciones básicas como la traza, los caracteres y resultados en este capítulo son de suma importancia para la comprensión y solución de teoremas útiles para los propósitos de este trabajo. Se da por hecho el conocimiento y algunas propiedades de un campo finito e inmediatamente procedemos a definir la función traza sobre un campo finito, la cual es dada en términos del automorfismo de Frobenius. A partir de la traza es posible dar la definición de una función caracter, del cual se dan varias propiedades. Sumas de Gauss definidas a partir de estos caracteres son también mencionadas con algunas de sus propiedades. Se puede consultar [**24**] y [**38**] para la teoría con respecto a los campos finitos y la traza. La teoría respecto a los caracteres y sumas de Gauss puede verse en [**24**].

1. Traza

Sea $\mathbb{F}_q$ un campo finito con q elementos, q la potencia de un primo (en este trabajo q denotará la potencia de un primo a menos que se especifique lo contrario) y $\mathbb{F}_{q^n}$ una extensión de $\mathbb{F}_q$. Un automorfismo de $\mathbb{F}_{q^n}$ el cual deja fijo todo elemento de $\mathbb{F}_q$ es llamado un automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Se define un automorfismo $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ por

$$\sigma : \alpha \to \alpha^q,\ \alpha \in \mathbb{F}_{q^n}.$$

σ es un automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y es llamado el automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

DEFINICIÓN 1.1. *Sea $\alpha \in \mathbb{F}_{q^n}$, la traza de α sobre $\mathbb{F}_q$, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) : \mathbb{F}_q^n \to \mathbb{F}_q$, está definida por*

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) := \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha),$$

donde σ es el automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

En consecuencia,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

Es decir, la traza de α sobre $\mathbb{F}_q$ es la suma de los conjugados de α con respecto a $\mathbb{F}_q$. En particular si $\mathbb{F}_p$ es el subcampo primo de $\mathbb{F}_{q^n}$, entonces $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha)$ es llamada la traza absoluta de α.

Se tienen las siguientes propiedades de la función traza:

TEOREMA 1.2. *(*[**24**],[**38**]*) La función traza $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ satisface las siguientes propiedades:*

1. *$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ es una transformación lineal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, donde ambos, $\mathbb{F}_{q^n}$ y $\mathbb{F}_q$ son considerados como espacios vectoriales sobre $\mathbb{F}_q$,*
2. *$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = na$ para toda $a \in \mathbb{F}_q$,*
3. *$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ para toda $\alpha \in \mathbb{F}_{q^n}$,*
4. *Para $\alpha \in \mathbb{F}_{q^n}$, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0 \iff \alpha = \beta - \beta^q$, para algún $\beta \in \mathbb{F}_{q^n}$.*

DEMOSTRACIÓN. Demostremos el útimo punto.

La condición suficiente es resuelta inmediatamente.

Si $\alpha \in \mathbb{F}_{q^n}$, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$, sea β raíz del polinomio $x^q - x - \alpha$ en alguna extensión de $\mathbb{F}_{q^n}$. Entonces $\beta^q - \beta = \alpha$ y

$$\begin{aligned} 0 &= Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \\ &= (\beta^q - \beta) - (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{n-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^n} - \beta^{q^{n-1}}) \\ &= \beta^{q^n} - \beta, \end{aligned}$$

por lo que $\beta \in \mathbb{F}_{q^n}$, y de aquí se tiene el resultado. □

TEOREMA 1.3. *(*[**24**],[**38**]*) Sea K un campo finito, F una extensión finita de K y E una extensión finita de F. Entonces,*

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha)) \qquad \text{para toda } \alpha \in E.$$

DEMOSTRACIÓN. La demostración es directa de la definición de la traza y la característica de un campo. □

2. Caracteres

Sea G un grupo abeliano finito con elemento identidad 1_G. Un caracter χ de G es un homomorfismo de G al grupo multiplicativo $\mathbb{C}_1$ de los números complejos de magnitud 1,

$$\chi : G \to \mathbb{C}_1.$$

Ya que $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$, entonces $\chi(1_G) = 1$. Más aún,

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1, \text{ para toda } g \in G,$$

es decir, las imágenes de χ son $|G|$-ésimas raíces de la unidad.

Como $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = 1$, luego $\chi(g^{-1}) = \overline{\chi(g)}$ para toda $g \in G$, donde $\overline{\chi(g)}$ denota la conjugación compleja de $\chi(g)$. Se define el caracter trivial χ_0 por $\chi_0(g) = 1$ para toda $g \in G$, todos los demás caracteres serán llamados no-triviales. Dado un número finito de caracteres $\chi_1, \ldots, \chi_n$ de G, se define el caracter producto $\chi_1 \cdots \chi_n$ por

$$(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g) \qquad \text{para toda } g \in G.$$

Si

$$\chi_1 = \cdots = \chi_n = \chi,$$

entonces escribimos χ^n en vez de $\chi_1 \cdots \chi_n$. Sea $G^\wedge$ el conjunto de caracteres de G, es decir,

$$G^\wedge := \{\chi : G \to \mathbb{C} |\ \chi \text{ caracter de } G\}.$$

Entonces $G^\wedge$ forma un grupo abeliano bajo la multiplicación de caracteres, además $G^\wedge$ es finito pues los valores de los caracteres de G son $|G|$-ésimas raíces de la unidad.

EJEMPLO 2.1. *Sea G un grupo finito cíclico de orden n con generador g. Para un entero fijo j, $0 \leq j \leq n-1$, la función*

$$\chi_j(g^k) = e^{2\pi ijk/n}, \qquad k = 0, 1, \ldots, n-1$$

define un caracter de G.

Obsérvese que $\{\chi_j : j = 0, \ldots, n-1\} = G^\wedge$, pues si χ es cualquier caracter de G, entonces $\chi(g)$ debe ser una raíz n-ésima de la unidad, es decir, $\chi(g) = e^{2\pi ij/n}$ para algún j, $0 \leq j \leq n-1$, por lo tanto $\chi = \chi_j$.

TEOREMA 2.2. *(*[**24**]*) Sea H un subgrupo del grupo abeliano finito G y ψ un caracter de H. Entonces ψ se puede extender a un caracter de G, o sea existe un caracter χ de G con $\chi(h) = \psi(h)$ para toda $h \in H$.*

DEMOSTRACIÓN. Sea $a \in G$, $a \notin H$, H_1 el subgrupo de G generado por H y a, y considérese el menor entero positivo m tal que $a^m \in H$. Si $g \in H_1$, entonces $g = a^j h, 0 \leq j < m, h \in H$. Se define una función ψ_1 en H_1 tal que

$$\psi_1(g) = w^j \psi(h),$$

donde w es un número fijo complejo tal que $w^m = \psi(a^m)$, entonces ψ es un caracter de H_1 : sea $g' = a^k h'$, $0 \leq k < m$, $h' \in H$, $g' \in H_1$,
si $i + j < m$, $\psi_1(gg') = w^{j+k}\psi(hh') = \psi_1(g)\psi_1(g')$,
si $j + k \geq m$, $gg' = a^{j+k-m}(a^m hh')$, luego $\psi_1(gg') = \psi_1(g)\psi_1(g')$.

Nótese que $\psi_1(h) = \psi(h)$ si $h \in H$. Si $H_1 = G$, terminamos, de lo contrario se procede del mismo modo. □

COROLARIO 2.3. *(*[**24**]*) Para elementos g_1, $g_2 \in G$ distintos, existe un caracter χ de G tal que $\chi(g_1) \neq \chi(g_2)$.*

DEMOSTRACIÓN. Sean $h = g_1 g_2^{-1} \neq 1_G$ y $H = \langle h \rangle$. Se sabe que existe un caracter ψ de H tal que $\psi(h) \neq 1$, pues todos los caracteres de H son de la forma $\psi_j(h^k) = e^{2\pi ikj/|H|}$. Por el Teorema 2.2 existe un caracter χ de G tal que $\chi(a) = \psi(a)$ para toda $a \in H$, en particular $\chi(h) = \psi(h) \neq 1$, luego $\chi(g_1) \neq \chi(g_2)$. □

TEOREMA 2.4. *(*[**24**]*) Sea χ_0 el caracter trivial y χ un caracter no trivial del grupo abeliano finito G. Entonces,*

$$\sum_{g \in G} \chi_0(g) = |G| \ \ y \ \ \sum_{g \in G} \chi(g) = 0.$$

Si $g \in G$ con $g \neq 1_G$, entonces,

$$\sum_{\chi \in G^\wedge} \chi(g) = 0.$$

DEMOSTRACIÓN. La primera igualdad es directa. Si χ es un caracter no trivial, existe $h \in G$ tal que $\chi(h) \neq 1$, por lo que,

$$\chi(h) \left(\sum_{g \in G} \chi(g) \right) = \sum_{g \in G} \chi(g),$$

entonces,

$$\left(\sum_{g \in G} \chi(g) \right) (\chi(h) - 1) = 0,$$

por consiguiente,

$$\sum_{g \in G} \chi(g) = 0.$$

Considérese $\widehat{g}$ definido por $\widehat{g}(\chi) = \chi(g)$, $\chi \in G^\wedge$, luego $\widehat{g}$ es un caracter del grupo abeliano finito $G^\wedge$. Además $\widehat{g}$ es no trivial, pues por el Corolario 2.3 existe $\chi \in G^\wedge$ tal que $\chi(g) \neq \chi(1_G)$, es decir, $\widehat{g}(\chi) \neq \widehat{1}_G(\chi) = 1$, por lo tanto por la primera parte de la prueba,

$$\sum_{\chi \in G^\wedge} \chi(g) = \sum_{\chi \in G^\wedge} \widehat{g}(\chi) = 0.$$

□

TEOREMA 2.5. *(*[**24**]*) El número de caracteres de un grupo abeliano finito G es igual a $|G|$, es decir $|G^\wedge| = |G|$.*

DEMOSTRACIÓN.

$$|G^\wedge| = \sum_{g \in G} \sum_{\chi \in G^\wedge} \chi(g) = \sum_{\chi \in G^\wedge} \sum_{g \in G} \chi(g) = |G|.$$

□

Como un caso particular del Ejemplo 2.1, se tiene lo siguiente:

EJEMPLO 2.6. *Sea g un elemento primitivo de $\mathbb{F}_q$ ($q = p^n, p$ primo), los caracteres del grupo multiplicativo de $\mathbb{F}_q$ están dados de la forma,*

$$\psi_j(g^k) = e^{2\pi i j k/(q-1)}, k \in \{0, 1, \ldots, q-2\},$$

$j = 0, 1, \ldots, q-2$.

Los caracteres del grupo multiplicativo de $\mathbb{F}_q$ son llamados caracteres multiplicativos de $\mathbb{F}_q$. Estos son todos los caracteres multiplicativos de $\mathbb{F}_q$, ya que cualquier caracter multiplicativo de $\mathbb{F}_q$ satisface $\psi(g) = e^{2\pi i j k/(q-1)}$ para algún $j \in \{0, 1, \ldots, q-2\}$, pues éstos son raíces $(q-1)$-ésimas de la unidad, luego $\psi(g^k) = \psi_j(g^k)$ $\forall k \in \{0, 1, \ldots, q-2\}$.

TEOREMA 2.7. *([**22**]) Sea ψ un caracter multiplicativo de $\mathbb{F}_q$. ψ^n es trivial sí y sólo si el orden de ψ divide a $d = (n, q-1)$.*

DEMOSTRACIÓN.

$\Leftarrow$) Sea r el orden de ψ, luego $r|d$, por lo que $r|n$, y de aquí $n = sr$, así $\psi^n = (\psi^r)^s = 1$.

$\Rightarrow$) Sea r el orden de ψ, como $\psi^n = \psi_0$, entonces $r|n$. Por otro lado como $\{\psi^0, \ldots, \psi^{r-1}\}$ es un subgrupo de $G^\wedge$, $r|q-1$, lo cual implica que $r|d$. □

DEFINICIÓN 2.8. *Sea $\eta(c) = 1$ si c es el cuadrado de un elemento de $\mathbb{F}_q$ y sea $\eta(c) = -1$ en otro caso.*

TEOREMA 2.9. *([**40**]) η es un caracter multiplicativo de $\mathbb{F}_q$. Además $\eta = \psi_{\frac{q-1}{2}}$. Donde $\psi_{\frac{q-1}{2}}$ es la notación de los caracteres multiplicativos de $\mathbb{F}_q$ del Ejemplo 2.6.*

DEMOSTRACIÓN. En general se sabe que la ecuación $x^n = a$ en el grupo multiplicativo de un campo $\mathbb{F}_q$ tiene solución sí y sólo si $a^{q-1/(n,q-1)} = 1$, luego, si g es un elemento primitivo de $\mathbb{F}_q$,

$$x^2 = g^k \text{ tiene solución sí y sólo si } g^{(q-1)k/2} = 1.$$

También $g^{(q-1)k/2} = 1$ tiene solución sí y sólo si k es par o cero. De este modo se han identificado los $\frac{q-1}{2}$ elementos de $\mathbb{F}_q^*$ que se pueden expresar como un cuadrado. Por otro lado,

$$\psi_{\frac{q-1}{2}}(g^k) = e^{\pi i k},$$

donde si k es par es igual a 1, de lo contrario es igual a -1. □

TEOREMA 2.10. *([**40**]) Sean η y η' los caracteres cuadráticos (de orden 2) en $\mathbb{F}_q$ y $\mathbb{F}_p$ respectivamente, $q = p^n$. Entonces $\eta(c) = \eta'(c)$ para cualquier $c \in \mathbb{F}_p^*$. Si n es par, $\eta(c) = 1$ para cualquier $c \in \mathbb{F}_p^*$, si n es impar, $\sum_{c\in\mathbb{F}_p^*} \eta(c) = 0$.*

DEMOSTRACIÓN. Sea g un elemento primitivo de $\mathbb{F}_q$. Entonces $g^{\frac{p^n-1}{p-1}}$ es un elemento primitivo de $\mathbb{F}_p$ y

$$\eta(g^c) = \psi_{\frac{q-1}{2}}(g^c) = e^{2\pi i \frac{q-1}{2} c/q-1} = e^{\pi i c} = e^{2\pi i \frac{p-1}{2} c/p-1} = \psi_{\frac{p-1}{2}}(g^c) = \eta'(g^c),$$

de aquí $\eta_{|\mathbb{F}_p^*} = \eta'$. Por otro lado,

$$\frac{p^n - 1}{p-1} = p^{n-1} + p^{n-2} + \cdots + p + 1,$$

por lo que $c = \frac{p^n-1}{p-1}$ es impar si n es impar y es par si n es par, luego,

$$\eta((g^c)^r) = e^{\pi i c r}, r = 1, \ldots, p-1,$$

de donde se tiene el resultado. □

Sea $\mathbb{F}_q$ un campo finito y $\mathbb{F}_p$ su campo primo. La función χ_1 definida por

$$\chi_1(c) = e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(c)/p} \qquad \text{para toda } c \in \mathbb{F}_q,$$

es un caracter del grupo aditivo de $\mathbb{F}_q$, pues $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$, ya que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(c_1 + c_2) = Tr_{\mathbb{F}_q/\mathbb{F}_p}(c_1) + Tr_{\mathbb{F}_q/\mathbb{F}_p}(c_2)$.

En lugar de la expresión, caracter del grupo aditivo de $\mathbb{F}_q$, se usará la expresión, caracter aditivo de $\mathbb{F}_q$. El caracter χ_1 es llamado el caracter aditivo canónico de $\mathbb{F}_q$.

Se conocen todos los caracteres aditivos de $\mathbb{F}_q$:

TEOREMA 2.11. *([**24**]) Para $b \in \mathbb{F}_q$, la función χ_b con $\chi_b(c) = \chi_1(bc)$ para toda $c \in \mathbb{F}_q$, $q = p^n$, p primo, es un caracter aditivo de $\mathbb{F}_q$, y todo caracter aditivo de $\mathbb{F}_q$ es obtenido de esta forma.*

DEMOSTRACIÓN. Es claro que χ_b es un caracter aditivo de $\mathbb{F}_q$ y además χ_1 es distinto del caracter trivial pues $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$ sí y sólo si α es raíz del polinomio,

$$x + x^p + \cdots + x^{p^{n-1}} \in \mathbb{F}_p[x],$$

pero este polinomio tiene a lo más p^{n-1} raíces en $\mathbb{F}_q$, y $\mathbb{F}_q$ tiene p^n elementos, por lo tanto existe $\alpha \in \mathbb{F}_q$ tal que $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \neq 0$, luego si $a, b \in \mathbb{F}_q, a \neq b$, entonces,

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1(ac)\left(\chi_1(bc)\right)^{-1} = \chi_1(ac)\chi_1(-bc) = \chi_1((a-b)c) \neq 1,$$

para $c \in \mathbb{F}_q$ elegido convenientemente, por lo que χ_a y χ_b son caracteres distintos, entonces si b corre a través de todos los valores de $\mathbb{F}_q$, se obtienen q caracteres distintos, los cuales son todos por el Teorema 2.5. □

2.1. Sumas de Gauss.

DEFINICIÓN 2.12. *Sea $\mathbb{F}_q$ un campo con q elementos y sean ψ, χ los caracteres multiplicativo y aditivo respectivamente de $\mathbb{F}_q$. La suma de Gauss $G(\psi, \chi)$ está definida por*

$$G(\psi, \chi) := \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c).$$

Véase [**24**] para la prueba del siguiente resultado.

TEOREMA 2.13. *Sea $\mathbb{F}_q$ un campo con q elementos, $q = p^n$, p un primo impar, η el caracter cuadrático de $\mathbb{F}_q$ y χ_1 el caracter aditivo canónico de $\mathbb{F}_q$. Entonces,*

$$G(\eta, \chi_1) = \begin{cases} (-1)^{n-1}q^{1/2} & si \quad p \equiv 1 \textit{ mód } 4 \\ (-1)^{n-1}i^n q^{1/2} & si \quad p \equiv 3 \textit{ mód } 4 \end{cases}.$$

□

Sea χ_1 el caracter aditivo canónico de $\mathbb{F}_q$, se define,

$$S_r(\mu, \nu) := \sum_{x \in \mathbb{F}_q} \chi_1(\mu x^{p^r+1} + \nu x) \quad \mu, \nu \in \mathbb{F}_q.$$

TEOREMA 2.14. *([**15**]) Sea $n/(n,r)$ impar, $a \neq 0$. Entonces,*

$$S_r(a,0) = \begin{cases} (-1)^{n-1}q^{1/2}\eta(a) & si \quad p \equiv 1 \textit{ mód } 4 \\ (-1)^{n-1}i^n q^{1/2}\eta(a) & si \quad p \equiv 3 \textit{ mód } 4 \end{cases}.$$

DEMOSTRACIÓN. Como $n/(n,r)$ es impar, $(p^r+1, p^n-1) = 2$, si $x \neq 0$,

$$\begin{aligned} \chi_1(ax^{p^r+1}) &= \frac{1}{q-1}\sum_{y\in\mathbb{F}_q^*}\chi_1(y)\sum_{\psi}\psi(ax^{p^r+1})\overline{\psi(y)} \\ &= \frac{1}{q-1}\sum_{\psi}\psi(ax^{p^r+1})\sum_{y\in\mathbb{F}_q^*}\chi_1(y)\overline{\psi(y)} \\ &= \frac{1}{q-1}\sum_{\psi}\psi(ax^{p^r+1})G(\overline{\psi},\chi_1), \end{aligned}$$

entonces,

$$\begin{aligned} &\sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}) \\ &= \frac{1}{q-1}\left(\sum_{x\in\mathbb{F}_q^*}\sum_{\psi}\psi(ax^{p^r+1})G(\overline{\psi},\chi_1)\right)+1 \\ &= \frac{1}{q-1}\left(\sum_{\psi}\psi(a)G(\overline{\psi},\chi_1)\sum_{x\in\mathbb{F}_q^*}\psi^{p^r+1}(x)\right)+1 \\ &= \frac{1}{q-1}\left(-1(q-1)+\eta(a)G(\eta,\chi_1)(q-1)\right)+1 = \eta(a)G(\eta,\chi_1) \\ &= S_r(a,0) = \begin{cases} (-1)^{n-1}q^{1/2}\eta(a) & si \quad p \equiv 1 \text{ mód } 4 \\ (-1)^{n-1}i^n q^{1/2}\eta(a) & si \quad p \equiv 3 \text{ mód } 4 \end{cases}. \end{aligned}$$

□

La prueba del siguiente resultado se puede consultar en [**15**], página 245.

TEOREMA 2.15. *Si $n/(n,r)$ es impar, entonces $a^{p^r}x^{p^{2r}} + ax$ es una permutación en $\mathbb{F}_q$, $q = p^n$, p primo impar.*

DEMOSTRACIÓN. Se puede ver que $a^{p^r}x^{p^{2r}} + ax$ es una transformación lineal en $\mathbb{F}_q$ debido a la característica de $\mathbb{F}_q$. Sea $(n,r) = d$, supóngase que $x_1 \neq 0$ es una solución de la ecuación $a^{p^r}x^{p^{2r}} + ax = 0$, entonces,

$$x_1^{p^{2r}-1} = -a^{1-p^r},$$

lo cual implica que,

$$\left(x_1^{p^{2r}-1}\right)^{\frac{p^n-1}{p^d-1}} = \left(-(a^{-1})^{p^r-1}\right)^{\frac{p^n-1}{p^d-1}},$$

por lo que,

$$\left(x_1^{p^n-1}\right)^{\frac{p^{2r}-1}{p^d-1}} (-1)^{\frac{p^n-1}{p^d-1}} \left(a^{p^n-1}\right)^{\frac{p^r-1}{p^d-1}} = 1,$$

luego,

$$(-1)^{\frac{p^n-1}{p^d-1}} = 1,$$

por lo tanto,

$$(-1)^{1+p^d+p^{2d}+\cdots+p^{(\frac{n}{d}-1)d}} = 1,$$

lo cual es una contradicción, pues $1 + p^d + p^{2d} + \cdots + p^{(\frac{n}{d}-1)d}$ es impar, ya que $n/(n, r)$ es impar. Entonces el núcleo de la función lineal $a^{p^r} x^{p^{2r}} + ax$ es cero, y de aquí $a^{p^r} x^{p^{2r}} + ax$ es una permutación. □

TEOREMA 2.16. *([**23**]) Si $a \notin \{x^d | x \in \mathbb{F}_{2^n}\}$, $d = 2^r + 1$, entonces $a^{2^r} x^{2^{2r}} + ax$ es una permutación en $\mathbb{F}_{2^n}$.*

DEMOSTRACIÓN. No es difícil ver que $a^{2^r} x^{2^{2r}} + ax$ es una transformación lineal en $\mathbb{F}_{2^n}$ debido a la característica de $\mathbb{F}_{2^n}$. Supóngase que $x_1 \neq 0$ es una solución de la ecuación $a^{2^r} x^{2^{2r}} + ax = 0$, entonces $x_1^{2^{2r}-1} = a^{1-2^r}$ implica que $x_1^{2^{2r}-1} = (a^{-1})^{2^r-1}$, como $(2^r - 1, 2^r + 1) = 1$, luego el lado izquierdo es una d-ésima potencia, mientras que el lado derecho no lo es, pues a no es una d-ésima potencia, por lo que se tiene una contradicción Por lo tanto el núcleo de la función $a^{2^r} x^{2^{2r}} + ax$ es cero, lo cual implica que $a^{2^r} x^{2^{2r}} + ax$ es una permutación. □

TEOREMA 2.17. *([**16**]) Sean $q = p^n$, p primo impar y r un entero tal que $n/(n, r)$ es impar. Supóngase que $a, b \neq 0$ y $x_{a,b}$ la única solución de la ecuación $a^{p^r} x^{p^{2r}} + ax + b^{p^r} = 0$. Entonces,*

$$S_r(a, b) = \begin{cases} (-1)^{n-1} q^{1/2} \eta(-a) \overline{\chi_1(a x_{a,b}{}^{p^r+1})} & si \quad p \equiv 1 \text{ mód } 4 \\ (-1)^{n-1} i^{3n} q^{1/2} \eta(-a) \overline{\chi_1(a x_{a,b}{}^{p^r+1})} & si \quad p \equiv 3 \text{ mód } 4 \end{cases}.$$

DEMOSTRACIÓN.

$$\begin{aligned} S_r(a, b) S_r(-a, 0) &= \sum_{y \in \mathbb{F}_q} \chi_1(-a y^{p^r+1}) \sum_{w \in \mathbb{F}_q} \chi_1(a w^{p^r+1} + bw) \\ &= \sum_{y \in \mathbb{F}_q} \chi_1(-a y^{p^r+1}) \sum_{x \in \mathbb{F}_q} \chi_1(a(x + y)^{p^r+1} + b(x + y)) \\ &= \sum_{x,y \in \mathbb{F}_q} \chi_1\left(a(x + y)^{p^r+1} + b(x + y)\right) \chi_1(-a y^{p^r+1}) \\ &= \sum_{x,y \in \mathbb{F}_q} \chi_1\left(a(x + y)^{p^r+1} + b(x + y) - a y^{p^r+1}\right) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{x,y\in\mathbb{F}_q} \chi_1\left(a(x^{p^r+1}+x^{p^r}y+y^{p^r}x+y^{p^r+1})+bx+by-ay^{p^r+1}\right)\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1(ax^{p^r}y+axy^{p^r}+by)\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1\left(a^{p^r}x^{p^{2r}}y^{p^r}+axy^{p^r}+b^{p^r}y^{p^r}\right)\\
&= \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1\left(y^{p^r}(a^{p^r}x^{p^{2r}}+ax+b^{p^r})\right).
\end{aligned}
$$

Nótese que en las operaciones anteriores la suma interior es cero para toda x, a excepción cuando $x = x_{a,b}$, en cuyo caso la suma interior es q. Aplicando el Teorema 2.14 se tiene que,

$$
\begin{aligned}
& S_r(a,b)S_r(-a,0) = q\chi_1(ax_{a,b}^{p^r+1}+bx_{a,b})\\
=\ & q\chi_1(x_{a,b}(ax_{a,b}^{p^r}+b))\\
=\ & q\chi_1(x_{a,b}^{p^r}(ax_{a,b}^{p^r}+b)^{p^r}) = q\chi_1(x_{a,b}^{p^r}(a^{p^r}x_{a,b}^{p^{2r}}+b^{p^r}))\\
=\ & q\chi_1(x_{a,b}^{p^r}(-ax_{a,b})) = q\chi_1(-ax_{a,b}^{p^r+1}) = q\overline{\chi_1(ax_{a,b}^{p^r+1})},
\end{aligned}
$$

luego,

$$
\begin{aligned}
& S_r(a,b) = (S_r(-a,0))^{-1}\, q\overline{\chi_1(ax_{a,b}^{p^r+1})}\\
=\ & \begin{cases} (-1)^{n-1}q^{1/2}\eta(-a)\overline{\chi_1(ax_{a,b^{p^r+1}})} & si \quad p\equiv 1 \text{ mód } 4\\ (-1)^{n-1}i^{3n}q^{1/2}\eta(a)\overline{\chi_1(ax_{a,b^{p^r+1}})} & si \quad p\equiv 3 \text{ mód } 4 \end{cases}.
\end{aligned}
$$

□

TEOREMA 2.18. *([**40**]) Sea $q = p^n$, p primo impar. Entonces para toda $a \in \mathbb{F}_q$,*

$$
\begin{aligned}
& |\{x\in\mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)=0\}|\\
=\ & \begin{cases} p^{n-1} & \textit{si n es impar}\\ \frac{1}{p}\left(q-\eta(a)(p-1)q^{1/2}\right) & \textit{si n es par y } p\equiv 1 \textit{ mód } 4\\ \frac{1}{p}\left(q-i^n\eta(a)(p-1)q^{1/2}\right) & \textit{si n es par y } p\equiv 3 \textit{ mód } 4 \end{cases}.
\end{aligned}
$$

DEMOSTRACIÓN.

$$
\begin{aligned}
& |\{x\in\mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)=0\}| = \frac{1}{p}\sum_{x\in\mathbb{F}_q}\sum_{c\in\mathbb{F}_p} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(acx^2)/p}\\
=\ & \frac{1}{p}\left(q+\sum_{c\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(acx^2)/p}\right) = \frac{1}{p}\left(q+\sum_{c\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q}\chi_1(acx^2)\right),
\end{aligned}
$$

si $x \neq 0$,

$$\chi_1(acx^2) = \frac{1}{q-1}\sum_{y\in\mathbb{F}_q^*}\chi_1(y)\sum_{\psi}\psi(acx^2)\overline{\psi(y)}$$

$$= \frac{1}{q-1}\sum_{\psi}\psi(acx^2)\sum_{y\in\mathbb{F}_q^*}\chi_1(y)\overline{\psi(y)} = \frac{1}{q-1}\sum_{\psi}\psi(acx^2)G(\overline{\psi},\chi_1),$$

entonces,

$$\sum_{x\in\mathbb{F}_q}\chi_1(acx^2) = \frac{1}{q-1}\left(\sum_{x\in\mathbb{F}_q^*}\sum_{\psi}\psi(acx^2)G(\overline{\psi},\chi_1)\right)+1$$

$$= \frac{1}{q-1}\left(\sum_{\psi}\psi(ac)G(\overline{\psi},\chi_1)\sum_{x\in\mathbb{F}_q^*}\psi^2(x)\right)+1$$

$$= \frac{1}{q-1}\left(-1(q-1)+\eta(ac)G(\eta,\chi_1)(q-1)\right)+1 = \eta(ac)G(\eta,\chi_1),$$

por lo que,

$$|\{x\in\mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)=0\}| = \frac{1}{p}\left(q+\sum_{c\in\mathbb{F}_p^*}\eta(ac)G(\eta,\chi_1)\right)$$

$$= \frac{1}{p}\left(q+\eta(ac)G(\eta,\chi_1)\sum_{c\in\mathbb{F}_p^*}\eta(c)\right).$$

De donde se tiene el resultado dependiendo del caso. □

Capítulo 2

Funciones bent, casi-bent, perfectamente no-lineales y casi perfectamente no-lineales

Las funciones bent, casi-bent, perfectamente no-lineales y casi perfectamente no-lineales tienen aplicaciones muy importantes en Teoría de Códigos y Criptografía. Por ejemplo en los sistemas de cifrado de llave privada para la resistencia a los ataques lineales y a los ataques diferenciales. Para los lectores interesados en estas definiciones y aplicaciones se puede consultar [**1**] y [**21**]. En el presente trabajo se estudian las funciones mencionadas y varias de sus propiedades. En particular estas funciones serán de utilidad para la construcción de códigos lineales en base a estas funciones y posteriormente para la construcción de esquemas de compartición de secretos y esquemas de autenticación. En este capítulo se inicia trabajando con las funciones $f : \mathbb{F}_2^n \to \mathbb{F}_2$, llamadas las funciones Booleanas, de las cuales en particular se tienen las funciones bent. Se da una caracterización de no-linealidad máxima para las funciones bent y las casi bent, la cual se interpreta como las funciones más alejadas de las funciones lineales, alejada en términos de una distancia llamada la distancia de Hamming. Para esto se tienen definiciones como el espectro de Fourier de una función $f : \mathbb{F}_2^n \to \mathbb{R}$, el peso de Hamming de una función Booleana, la definición de un código lineal y en particular la de un código lineal llamado el código de Reed-Muller con el cual se puede medir la no-linealidad de una función Booleana. Una descripción más detallada respecto a los códigos lineales, funciones Booleanas y peso Hamming pueden consultarse en [**25**] y [**31**]. Con respecto a las funciones Bent y espectro de Fourier se puede consultar [**25**]. Posteriormente se trabaja con funciones $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, donde se definen las funciones perfectamente no-lineales, las casi perfectamente no-lineales, las funciones casi-bent, y es generalizada la definición de una función bent. Con respecto a estas funciones se puede consultar [**3**], [**10**] y [**13**].

1. Funciones Booleanas

Sea $\mathbb{F}_2$ el campo con 2 elementos y $\mathbb{F}_2^n$ definido por

$$\mathbb{F}_2^n := \{(v_1, \ldots, v_n) |\ v_1, \ldots, v_n \in \mathbb{F}_2\}.$$

No es difícil ver que $\mathbb{F}_2^n$ es un espacio vectorial de dimensión n sobre el campo $\mathbb{F}_2$ con las operaciones de suma y producto usuales (la adición en este espacio vectorial es módulo 2).

DEFINICIÓN 1.1. *Se llama función Booleana a toda función*

$$f : \mathbb{F}_2^n \to \mathbb{F}_2.$$

DEFINICIÓN 1.2. *Se denota como $\mathcal{B}_n$ al conjunto de funciones Booleanas de n entradas, es decir,*

$$\mathcal{B}_n := \{f | f : \mathbb{F}_2^n \to \mathbb{F}_2\}.$$

Nótese que el conjunto de imágenes de una función $f \in \mathcal{B}_n$ determina un vector de longitud 2^n, es decir, $\left(f(v)_{v\in\mathbb{F}_2^n}\right)$.

$\mathcal{B}_n$ tiene estructura de espacio vectorial sobre $\mathbb{F}_2$ con las operaciones comunes de suma de funciones y multiplicación de un escalar por una función, es decir,

$$(f+g)(x) = f(x) + g(x) \text{ y } (cf)(x) = cf(x),$$

$f, g \in \mathcal{B}_n$, $c \in \mathbb{F}_2$. Una base de $\mathcal{B}_n$ está dada por el conjunto de funciones Booleanas cuyas imágenes corresponden al conjunto

$$\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$$

(no es difícil verificar este hecho). Por lo que $\mathcal{B}_n$ tiene dimensión 2^n como estructura de espacio vectorial y su número de elementos es 2^{2^n}.

EJEMPLO 1.3. *La función $f(x) \in \mathcal{B}_3$ definida por*

$$f(x_1,x_2,x_3) = 1 + x_1x_2 + x_1x_2x_3,$$

es un ejemplo de función Booleana.

La suma en el ejemplo anterior es considerada módulo 2, y el conjunto de imágenes de f determina el vector

$$(1,1,1,1,1,1,0,1),$$

o sea, $(1,1,1,1,1,1,0,1) = (f(p_1), f(p_2), \ldots, f(p_8))$, donde $p_1,\ldots,p_8$, son los distintos elementos de $\mathbb{F}_2^3$ dados en el orden usual (en correspondencia con los números $0,1,\ldots,7$).

DEFINICIÓN 1.4. *Se define la transformada de Fourier de la función $f : \mathbb{F}_2^n \to \mathbb{R}$ por la función*

$$\widehat{f}(a) := \sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{a\cdot x},$$

donde $a \cdot x$ es el producto punto usual en $\mathbb{F}_2^n$. Más aún, los valores $\widehat{f}(a)$ son llamados los coeficientes de Fourier de f y el conjunto de coeficientes de Fourier de f es llamado el espectro de Fourier de f.

En particular de la definición anterior se puede considerar a f como una función Booleana.

La transformada de Fourier de la función $\zeta_f := (-1)^f$, f una función Booleana, al aplicar la definición anterior, está dada por

$$\widehat{\zeta_f}(a) = \sum_{x\in F_2^n} (-1)^{f(x)+a\cdot x}.$$

En adelante $\widehat{\zeta_f}$ representará la suma anterior. Nótese que $\widehat{\zeta_f}(a)$ determina el número de ceros menos el número de unos de la función $f(x) + a \cdot x$.

DEFINICIÓN 1.5. *Sea $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. El soporte de x denotado por $sop(x)$, está definido por*

$$sop(x) := \{i | x_i \neq 0, 1 \leq i \leq n\}.$$

El peso de Hamming de x denotado por $w(x)$, está definido por la cardinalidad del soporte de x, o sea,

$$w(x) := |\{i | x_i \neq 0, 1 \leq i \leq n\}|.$$

DEFINICIÓN 1.6. *Sea $f \in \mathcal{B}_n$. El soporte de f denotado como $sop(f)$, está definido por*

$$sop(f) := \{x \in \mathbb{F}_2^n | f(x) \neq 0\}.$$

El peso de Hamming de $f \in \mathcal{B}_n$ denotado por $w(f)$, está definido por la cardinalidad del soporte de f, o sea,

$$w(f) := |\{x \in \mathbb{F}_2^n | f(x) \neq 0\}|.$$

DEFINICIÓN 1.7. *La distancia de Hamming entre dos elementos x, y de $\mathbb{F}_2^n$ está definida por*

$$d(x, y) := w(x + y).$$

La distancia de Hamming entre dos funciones Booleanas f, g está definida por

$$d(f, g) := w(f + g).$$

Una forma de representar a las funciones Booleanas es la Forma Algebraica Normal (F.A.N.).

DEFINICIÓN 1.8. *Se dice que una función Booleana f se encuentra en su F.A.N. si está escrita de la forma*

$$f(x_1, \ldots, x_n) := \sum_{u \in \mathbb{F}_2^n} a_u (\prod_{i=1}^{n} x_i^{u_i}); \quad u = (u_1, \ldots, u_n), \quad a_u \in \mathbb{F}_2.$$

Nótese que en el Ejemplo 1.3 la función f está expresada en su F.A.N.

Sea $\mathcal{R} := \mathbb{F}_2[x_1, x_2, \ldots, x_n]/(x_i^2 - x_i)$. $\mathcal{R}$ tiene estructura de espacio vectorial sobre $\mathbb{F}_2$ y una base está dada por el conjunto

$$\{x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k} : 0 \leq i_k \leq 1, 1 \leq k \leq n\},$$

por lo que la dimensión de $\mathcal{R}$ es

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$

y su número de elementos es 2^{2^n}.

Se puede dar una relación entre $\mathcal{R}$ y $\mathcal{B}_n$ de la siguiente manera:

TEOREMA 1.9. *([**4**]) Sea $f : \mathbb{F}_2^n \to \mathbb{F}_2$ una función Booleana. Entonces,*

$$a_u = \sum_{x \leq u} f(x) \text{ sí y sólo si } f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \left(\prod_{i=1}^{n} x_i^{u_i} \right),$$

$x = (x_1, \ldots, x_n) \leq u = (u_1, \ldots, u_n)$ *sí y sólo si* $\forall\ i \in \{1, \ldots, n\},\ x_i \leq u_i$. *Donde las sumas son consideradas módulo* 2.

DEMOSTRACIÓN. La prueba es por inducción con respecto a n. □

En base a la relación obtenida del Teorema 1.9 es posible obtener una transformación lineal no singular entre $\mathcal{R}$ y $\mathcal{B}_n$, por lo que $\mathcal{R} \cong \mathcal{B}_n$.

En particular se tienen las siguientes funciones:

DEFINICIÓN 1.10. *Las funciones Booleanas básicas son las funciones afines definidas por el conjunto*

$$\mathcal{A} = \{f | f(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n + a_0 = a \cdot x + a_0\},$$

donde $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ *y* $a_0 \in \mathbb{F}_2$.

1.1. Código lineal binario. Un código es una combinación de signos que representan algo dentro de un sistema establecido y muchos de ellos son utilizados en la vida diaria, por ejemplo los códigos de barras que simplemente es una forma de identificar un artículo de modo que una máquina pueda leer la información respecto a éste. También se estudian los códigos detectores-correctores de errores ([**25**]), lo cuales detectan errores y también los corrigen, por ejemplo los utilizados en los reproductores de discos compactos.

Introducimos la definición de un código lineal binario:

DEFINICIÓN 1.11. *Un código* $[n, k, d]_2$ *lineal binario, es un subespacio lineal* $\mathcal{C}$ *de* $\mathbb{F}_2^n$, *de dimensión* k *y peso mínimo* d, *donde*

$$d := \textit{mín}\{w(x) | x \in \mathcal{C}, x \neq 0\},$$

o sea el peso mínimo de $\mathcal{C}$ *es el menor peso de los elementos no cero del código.*

El peso mínimo determina en cierto sentido cuando es lo mejor posible un código lineal, pues indica el número de errores que puede detectar y corregir en un código lineal. En particular se tiene la definición de un código de Reed-Muller.

DEFINICIÓN 1.12. *Sea* $0 \leq r \leq n$. *El código de Reed-Muller de orden* r *y longitud* 2^n *que se denota como* $\mathcal{R}(r, n)$, *es el conjunto de los vectores de longitud* 2^n *formado por las imágenes de las distintas funciones Booleanas en* $\mathcal{B}_n$ *de grado a lo más* r *(grado de la F.A.N.) obtenidas al aplicar la función evaluación,*

$$ev : \mathcal{R}_r^n \to \mathbb{F}_2^{2^n},$$

definida como,

$$ev(f) := (f(p_1), f(p_2), \ldots, f(p_{2^n})),$$

donde,

$$\mathcal{R}_r^n := \{f \in \mathcal{B}_n : gr(f) \leq r\},$$

y $p_1, p_2, \ldots, p_{2^n}$ *son los distintos elementos de* $\mathbb{F}_2^n$.

TEOREMA 1.13. *(*[**25**],[**31**]*) $\mathcal{R}(r,n)$ tiene dimensión*

$$k = \left(\begin{array}{c} n \\ 0 \end{array} \right) + \left(\begin{array}{c} n \\ 1 \end{array} \right) + \cdots + \left(\begin{array}{c} n \\ r \end{array} \right).$$

DEMOSTRACIÓN. Una base para las funciones Booleanas en su F.A.N. correspondientes a los respectivos elementos de $\mathcal{R}(r,n)$ está dada por

$$\{x_1^{i_1} \cdots x_k^{i_k} : 0 \leq i_k \leq 1, \sum i_k \leq r, 1 \leq k \leq n\},$$

de este modo los vectores correspondientes a esta base son una base para $\mathcal{R}(r,n)$, ya que la función evaluación anterior es una transformación lineal inyectiva. □

TEOREMA 1.14. *(*[**25**],[**31**]*) El código de Reed-Muller $\mathcal{R}(r,n)$ tiene peso mínimo 2^{n-r}.*

□

Obsérvese que $ev(\mathcal{A}) = \mathcal{R}(1,n)$, donde $\mathcal{A}$ es el conjunto de las funciones Booleanas afines.

1.2. La no-linealidad.

DEFINICIÓN 1.15. *La no-linealidad, denotada N_f, de la función Booleana f, es la distancia de Hamming entre f y el conjunto de las funciones afines, es decir,*

$$N_f := \textit{mín}_{g \in \mathcal{A}} d(f,g).$$

En forma equivalente, la no-linealidad de f es la distancia de Hamming entre $ev(f)$ y el código de Reed-Muller $\mathcal{R}(1,n)$.

La definición de no-linealidad puede consultarse en [**4**] y la prueba del siguiente resultado en [**25**], donde se expresa la no-linealidad en términos de la trasformada de Fourier .

TEOREMA 1.16. *La no-linealidad de la función Booleana f está dada por*

$$N_f = 2^{n-1} - \frac{1}{2} \textit{máx}_{a \in \mathbb{F}_2^n} |\widehat{\zeta_f}(a)|.$$

DEMOSTRACIÓN. Con respecto a las imágenes de la función $f(x) + a \cdot x$,

núm. ceros $-$ núm. unos $=$ núm ceros $+$ núm. unos $-$ 2 veces núm. unos,

o sea,

$$\widehat{\zeta_f}(a) = 2^n - 2d(f, a \cdot x),$$

de aquí,

$$d(f, a \cdot x) = \frac{1}{2}(2^n - \widehat{\zeta_f}(a)).$$

Por otro lado,

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a \cdot x+1} = -\widehat{\zeta_f}(a),$$

entonces con respecto a las imágenes de la función $f(x) + a \cdot x + 1$,

núm. ceros $-$ núm. unos $=$ núm. ceros $+$ núm. unos $-$ 2 veces núm. unos,

o sea,

$$-\widehat{\zeta_f}(a) = 2^n - 2d(f, a \cdot x + 1),$$

por lo tanto,

$$d(f, a \cdot x + 1) = \frac{1}{2}(2^n - \widehat{\zeta_f}(a)).$$

Entonces,

$$N_f = \text{mín}_{a \in \mathbb{F}_2^n} \left\{ 2^{n-1} \pm \frac{1}{2}\widehat{\zeta_f}(a) \right\},$$

luego,

$$N_f = 2^{n-1} - \frac{1}{2}\text{máx}_{a \in \mathbb{F}_2^n} |\widehat{\zeta_f}(a)|.$$

□

La igualdad de Parseval es de importancia para la prueba de la no-linealidad máxima de una función bent.

TEOREMA 1.17. *(Igualdad de Parseval) (*[**25**]*)*

$$\sum_{a \in \mathbb{F}_2^n} \widehat{\zeta_f}(a)^2 = 2^{2n}.$$

DEMOSTRACIÓN. El resultado se obtiene resolviendo el producto directamente y efectuando la suma. □

2. Funciones bent

En esta sección se definen las funciones bent $f : \mathbb{F}_2^n \to \mathbb{F}_2$. La definición de función bent así como varias de sus propiedades podemos encontrarlas en varias referencias, por ejemplo [**4**], [**5**], [**23**] y [**25**].

DEFINICIÓN 2.1. *Una función Booleana en $\mathbb{F}_2^n$ con n par es llamada bent, si $\widehat{\zeta_f}(a) = \pm 2^{\frac{n}{2}}$ para toda $a \in \mathbb{F}_2^n$.*

De la definición de la transformada de Fourier se tiene que una función bent más una función afín, es bent.

COROLARIO 2.2. *(*[**25**]*) Las funciones bent tienen la no-linealidad máxima.*

DEMOSTRACIÓN. Aplicando la igualdad de Parseval, no puede existir una función tal que $\text{máx}_{a \in \mathbb{F}_2^n} |\widehat{\zeta_f}(a)| < \pm 2^{\frac{n}{2}}$. □

La no-linealidad de una función bent f es

$$N_f = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

TEOREMA 2.3. *(*[**25**]*) Las funciones Booleanas*

$$f(x_1, \ldots, x_m) \text{ y } g(y_1, \ldots, y_n)$$

son bent sí y sólo si la función Booleana

$$h(x_1, \ldots, x_m, y_1, \ldots, y_n) = f(x_1, \ldots, x_m) + g(y_1, \ldots, y_n),$$

es bent.

DEMOSTRACIÓN. De la definición de la transformada de Fourier,

$$\widehat{\zeta_h}(a) = \widehat{\zeta_f}(c)\widehat{\zeta_g}(d),\ a = (c, d).$$

$\Leftarrow$) Si f y g son bent, es claro que h es bent.

$\Rightarrow$) Si h es bent, entonces f y g también lo son pues de lo contrario h no satisfaría la igualdad de Parseval. □

EJEMPLO 2.4. *La función* $f(x_1, x_2) = x_1x_2 \in \mathcal{B}_2$ *es bent ya que,*

$$\widehat{\zeta_f}(0,0) = 2, \widehat{\zeta_f}(0,1) = 2, \widehat{\zeta_f}(1,0) = 2, \widehat{\zeta_f}(1,1) = -2,$$

y su no-linealidad es

$$N_f = 1.$$

EJEMPLO 2.5. *La función*

$$f(x_1, x_2, x_3, x_4) = x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2 \in \mathcal{B}_4$$

es bent ya que,

$$\textit{máx}_{a \in \mathbb{F}_2^n} |\widehat{\zeta_f}(a)| = 2^{4/2} = 4,$$

y su no-linealidad es

$$N_f = 6.$$

No está demás mencionar que para $n = 2$ y $n = 4$ en $\mathcal{B}_n$ existen 8 y 896 funciones bent respectivamente. Es un problema abierto contar estas funciones para valores grandes de n ([**5**]).

Las funciones bent del ejemplo siguiente son llamadas la clase Maiorana-McFarland ([**23**]).

EJEMPLO 2.6. *Sea* $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ *una permutación y* $h : \mathbb{F}_2^k \to \mathbb{F}_2$ *una función arbitraria. Entonces* $f : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2$ *definida por*

$$f(x, y) = x \cdot \pi(y) + h(y),\ x, y \in \mathbb{F}_2^k,$$

es una función bent.

DEMOSTRACIÓN. Sea $c = (a, b) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$ fijo y $z = (x, y) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$. Entonces,

$$\widehat{\zeta_f}(c) = \sum_{z \in \mathbb{F}_2^k \times \mathbb{F}_2^k} (-1)^{f(x)+c\cdot z} = \sum_{x,y \in \mathbb{F}_2^k} (-1)^{x\cdot\pi(y)+h(y)+(a,b)\cdot(x,y)}$$

$$= \sum_{y \in \mathbb{F}_2^k} (-1)^{h(y)+b\cdot y} \sum_{x \in \mathbb{F}_2^k} (-1)^{x\cdot(\pi(y)+a)}.$$

Nótese que la suma interior se hace cero, a menos que $\pi(y) = a$, o sea, $y = \pi^{-1}(a)$, en cuyo caso la suma interior es 2^k, luego,

$$\widehat{\zeta_f}(c) = 2^k(-1)^{h(\pi^{-1}(a))+b\cdot\pi^{-1}(a)},$$

por lo tanto,

$$|\widehat{\zeta_f}(c)| = 2^k.$$

□

Para un ejemplo más de funciones bent se tienen las siguientes relaciones.

Se puede identificar el espacio vectorial $\mathbb{F}_2^n$ con el campo de Galois $\mathbb{F}_{2^n}$. Es conveniente elegir un isomorfismo de modo que el producto escalar canónico (producto punto) en $\mathbb{F}_2^n$ coincida con el producto escalar canónico en $\mathbb{F}_{2^n}$, el cual es la traza del producto:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(xy),\ x, y \in \mathbb{F}_{2^n}.$$

Por lo tanto si se considera una función Booleana de la forma

$$f(x) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d),\ \alpha \in \mathbb{F}_{2^n},$$

entonces la transformada de Fourier de la función $\zeta_f = (-1)^f$ está dada por

$$\widehat{\zeta_f}(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d + ax)} = \sum_{x\in\mathbb{F}_{2^n}} \chi_1(\alpha x^d + ax),$$

donde $\chi_1(\cdot) = (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\cdot)}$ es el caracter aditivo canónico de $\mathbb{F}_{2^n}$.

Nótese que si

$$f(x) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d),\ \alpha \in \mathbb{F}_{2^n}$$

es tal que $(d, 2^n - 1) = 1$, se tiene que

$$\widehat{\zeta_f}(0) = \sum_{x\in\mathbb{F}_{2^n}} \chi_1(\alpha x^d) = 0,$$

pues x^d es una permutación en $\mathbb{F}_{2^n}$, por lo que f no es bent en estos casos.

El siguiente resultado genera ejemplos de funciones bent.

TEOREMA 2.7. *([**23**]) Sea $\alpha \in \mathbb{F}_{2^n}$, $r \in \mathbb{N}$, $d = 2^r + 1$ y n par. Entonces la función*

$$f(x) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d),\ x \in \mathbb{F}_{2^n},$$

es bent sí y sólo si $\alpha \notin \{x^d | x \in \mathbb{F}_{2^n}\}$.

DEMOSTRACIÓN.

⇐)Supóngase que α no es una d-ésima potencia en $\mathbb{F}_{2^n}$. Entonces por el Teorema 2.16 del Capítulo 1, para cualquier $a \in \mathbb{F}_{2^n}$ existe una única $\gamma \in \mathbb{F}_{2^n}$ tal que

$\alpha^{2^r}x^{2^{2r}}+\alpha\gamma=a^{2^r}$, es decir, $\alpha^{2^r}x^{2^{2r}}+\alpha\gamma+a^{2^r}=0$. Entonces,

$$\begin{aligned}
\widehat{\zeta_f}(a) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d+ax)}=\sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha x^d+ax)\\
&= \sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha x^d+\alpha\gamma^{2^r}x+\alpha x^{2^r}\gamma+\alpha\gamma^d+\alpha\gamma^d+\alpha\gamma^{2^r}x+\alpha\gamma x^{2^r}+ax)\\
&= \sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha(x+\gamma)^d+\alpha\gamma^d+\alpha\gamma^{2^r}x+\alpha\gamma x^{2^r}+ax)\\
&= \sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha(x+\gamma)^d+\alpha\gamma^d+(x\alpha\gamma^{2^r})^{2^r}+\alpha\gamma x^{2^r}+(ax)^{2^r})\\
&= \sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha(x+\gamma)^d+\alpha\gamma^d+x^{2^r}(\alpha^{2^r}\gamma^{2^{2r}}+\alpha\gamma+a^{2^r}))\\
&= \sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha(x+\gamma)^d+\alpha\gamma^d)=(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha\gamma^d)}\sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha(x+\gamma)^d)\\
&= (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha\gamma^d)}\sum_{x\in\mathbb{F}_{2^n}}\chi_1(\alpha(x)^d)=(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha\gamma^d)}\widehat{\zeta_f}(0).
\end{aligned}$$

Ya que el resultado anterior es para toda $a\in\mathbb{F}_{2^n}$, de la igualdad de Parseval se tiene que $\widehat{\zeta_f}(a)=\pm 2^{n/2}$ para toda $a\in\mathbb{F}_{2^n}$.

$\Rightarrow$)Sea f bent. Procediendo por contradicción, entonces $\alpha\neq 0$ es una d-ésima potencia. Por otro lado, si α no es una d-ésima potencia, entonces por la primera parte de la prueba f es bent. Por lo tanto $f(x)$ es una función bent para toda $\alpha\in\mathbb{F}_{2^n}^*$, lo cual no es posible pues de lo contrario se podría construir una función bent vectorial lo cual no es posible. En la siguiente sección se abordará el tema de función bent vectorial en donde se concluye la prueba. □

3. Funciones bent vectoriales y perfectamente no-lineales

En esta sección se definen las funciones bent y perfectamente no-lineales, $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$, y se resuelve la equivalencia que existe entre ellas, así como la existencia de estas funciones para los distintos valores de n y m.

Las siguientes definiciones son de importancia para definir las funciones bent y las perfectamente no-lineales.

DEFINICIÓN 3.1. *Se definen*

$$L_F(a,b):=\{x\in\mathbb{F}_2^n|\ b\cdot F(x)+a\cdot x=0\}$$

y

$$\lambda_F(a,b):=2\left(|L_F(a,b)|-2^{n-1}\right),$$

$b\in\mathbb{F}_2^m\backslash\{0\}$, $a\in\mathbb{F}_2^n$.

Obsérvese que

$$\begin{aligned}
&\lambda_F(a,b)\\
=\ &|\{x\in\mathbb{F}_2^n|\ b\cdot F(x)+a\cdot x=0\}|-|\{x\in\mathbb{F}_2^n|\ b\cdot F(x)+a\cdot x=1\}|.
\end{aligned}$$

Si $|L_F(a,b)| = \frac{|\mathbb{F}_2^n|}{2}$, entonces el número de ceros y el número de unos de la función $b \cdot F(x) + a \cdot x$, $b \in \mathbb{F}_2^m \backslash \{0\}$, $a \in \mathbb{F}_2^n$ coinciden.

DEFINICIÓN 3.2. *Se define,*

$$D_a F(x) := F(x+a) - F(x).$$

De la definición se tiene que,

$$D_a F^{-1}(b) = \{x \in \mathbb{F}_2^n | F(x+a) - F(x) = b\}.$$

DEFINICIÓN 3.3. *Se define,*

$$\delta_a F^{-1}(b) := |D_a F^{-1}(b)|.$$

DEFINICIÓN 3.4. *Se definen,*

$$\Lambda_F := sup_{a,b \neq 0} |\lambda_F(a,b)| \ \ y \ \ \Delta_F := sup_{a \neq 0, b} \delta_a F^{-1}(b).$$

Nótese que $\lambda_F(a,b) = \widehat{\zeta_{b \cdot F}}(a)$. O sea $\lambda_F(a,b)$ es la transformada de Fourier de la función Booleana $b \cdot F$ evaluada en a. En el caso de n par, Λ_F alcanza el menor valor $2^{n/2}$, pues es el menor valor que pueden alcanzar las funciones Booleanas $b \cdot F$ en caso de que alguna de ellas sea bent.

De manera natural la no-linealidad N_F de una función vectorial $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ está definida por

$$N_F := \text{mín}_{0 \neq b \in \mathbb{F}_2^m} \text{mín}_{g \in \mathcal{A}} d(b \cdot F, g),$$

$\mathcal{A}$ el conjunto de las funciones afines. O sea, la no-linealidad de F está definida como la mínima distancia de Hamming entre las combinaciones lineales no cero de las funciones coordenada de F y el conjunto de todas las funciones afines. Por lo tanto la no-linealidad de una función vectorial está dada por la relación

$$N_F = 2^{n-1} - \frac{1}{2} \text{máx}_{\substack{a \in \mathbb{F}_2^n \\ 0 \neq b \in \mathbb{F}_2^m}} |\widehat{\zeta_{b \cdot F}}(a)| = 2^{n-1} - \frac{1}{2} \text{máx}_{\substack{a \in \mathbb{F}_2^n \\ 0 \neq b \in \mathbb{F}_2^m}} |\widehat{\lambda_F}(a,b)|,$$

y este resultado es directo al utilizar la relación de no-linealidad para funciones Booleanas, el cual está dada por

$$N_f = 2^{n-1} - \frac{1}{2} \text{máx}_{a \in \mathbb{F}_2^n} |\widehat{\zeta_f}(a)|,$$

f una función Booleana. Luego, los menores valores de $\text{sup}_{a,b \neq 0} |\lambda_F(a,b)|$ corresponden a una mayor no-linealidad de F.

Extendamos la definición de función bent $f : \mathbb{F}_2^n \to \mathbb{F}_2$, a funciones bent vectoriales $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. De aquí en adelante simplemente se les llamará funciones bent a las funciones bent vectoriales.

DEFINICIÓN 3.5. *Si n es par, una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es bent sí y sólo si para toda $0 \neq b \in \mathbb{F}_2^m$, la función Booleana*

$$x \to b \cdot F(x),$$

es bent,

o sea,

$$\forall b \neq 0, \forall a \quad \lambda_F(a,b) = \pm 2^{\frac{n}{2}}.$$

Como $\lambda_F(a,b) = \widehat{\zeta_{b\cdot F}}(a)$, entonces si F es bent, $0 \neq b \cdot F$ es bent, por lo que el menor valor que puede alcanzar Λ_F es $2^{n/2}$ en caso de que F sea bent, luego, su no-linealidad está dada por $N_F = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Los valores de Δ_F, están acotados dependiendo de n y m.

TEOREMA 3.6. *(*[**13**]*) Para cualquier función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se tiene que $\Delta_F \geq 2^{n-m}$.*

DEMOSTRACIÓN. Si $a \in \mathbb{F}_2^n$, entonces $\sum_{b\in\mathbb{F}_2^m} \delta_a F^{-1}(b) = 2^n$. De aquí se obtiene el resultado pues $2^m 2^{n-m} = 2^n$, y si $\delta_a F^{-1}(b) < 2^{n-m}$, luego un valor de $\delta_a F^{-1}(b)$ será mayor que 2^{n-m} para así compensar la suma. □

La desigualdad anterior no puede ser una igualdad si $n < m$, pues 2^{n-m} no sería un entero.

DEFINICIÓN 3.7. *Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es llamada perfectamente no-lineal (PN) sí y sólo si $\Delta_F = 2^{n-m}$.*

Observación: Si $\Delta_F = 2^{n-m}$, entonces $\delta_a F^{-1}(b) = 2^{n-m}$ para toda $a \in \mathbb{F}_2^n$, $a \neq 0$ y toda $b \in \mathbb{F}_2^m$. Esto es ya que $\delta_a F^{-1}(b) \leq \Delta_F = 2^{n-m}$ y $2^m 2^{n-m} = 2^n$. Si para algún par (a,b) se tiene que $\delta_a F^{-1}(b) < 2^{n-m}$, entonces al hacer variar el elemento b no se obtendrían las 2^n soluciones.

Para poder dar la relación entre las funciones bent y las funciones perfectamente no-lineales se tienen las siguientes definiciones y resultados.

DEFINICIÓN 3.8. *Se llama función característica de $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, denotada por θ_F, a la función Booleana*

$$\theta_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2,$$

tal que

$$\theta_F(x,y) := \begin{cases} 1 & si \quad y = F(x) \\ 0 & si \quad y \neq F(x) \end{cases}.$$

DEFINICIÓN 3.9. *Sean f y g funciones sobre $\mathbb{F}_2^n$ a $\mathbb{C}$. Se denota por $f \otimes g$ el producto convolucional*

$$(f \otimes g)(a) := \sum_{x\in\mathbb{F}_2^n} f(x) g(a+x).$$

TEOREMA 3.10. *(*[**13**]*) Sea $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$. Entonces,*

$$\delta_a F^{-1}(b) = (\theta_F \otimes \theta_F)(a,b).$$

DEMOSTRACIÓN. Utilizando la Definición 3.9 obtenemos que,

$$\begin{aligned}(\theta_F \otimes \theta_F)(a,b) &= \sum_{x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} \theta_F(x,y)\theta_F(a+x,b+y)\\ &= \sum_{x\in\mathbb{F}_2^n} \theta_F(a+x,b+F(x))\\ &= |\{x\in\mathbb{F}_2^n | b+F(x)=F(a+x)\}|\\ &= \delta_a F^{-1}(b).\end{aligned}$$

□

Recordando que $\widehat{\theta_F}$ es la transformada de Fourier de la función θ_F, se tiene el siguiente resultado:

TEOREMA 3.11. *([**13**]) Sea $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$. Entonces,*

$$\lambda_F(a,b) = \widehat{\theta_F}(a,b).$$

DEMOSTRACIÓN. De la definición de la transformada de Fourier y la Definición 3.1,

$$\begin{aligned}\widehat{\theta_F}(a,b) &= \sum_{x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} \theta_F(x,y)(-1)^{a\cdot x+b\cdot y} = \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x+b\cdot F(x)}\\ &= 2|L_F(a,b)| - 2^n = 2(|L_F(a,b)| - 2^{n-1}) = \lambda_F(a,b).\end{aligned}$$

□

En general, para toda función f Booleana se tienen las siguientes propiedades clásicas de la transformada de Fourier:

$$\left(\widehat{f}\right)^2 = \widehat{f\otimes f}, \qquad \widehat{\widehat{f}} = 2^n f, \qquad \sum_{a\in\mathbb{F}_2^n} f(a) = \widehat{f}(0).$$

Ahora ya se puede dar la equivalencia entre funciones bent y perfectamente no-lineales.

TEOREMA 3.12. *([**13**]) Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es perfectamente no-lineal sí y sólo si es bent.*

DEMOSTRACIÓN.

$\Rightarrow$) Sea $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ una función PN. Entonces $\Delta_F = 2^{n-m}$, por lo tanto $\delta_a F^{-1}(b) = 2^{n-m}$ para toda $a \in \mathbb{F}_2^n$, $a \neq 0$, $b \in \mathbb{F}_2^m$. También $\delta_0 F^{-1}(0) = 2^n$ y $\delta_0 F^{-1}(b) = 0$ para $b \neq 0$, pues $D_0 F^{-1}(b) = \phi$ para $b \neq 0$. Ahora por el Teorema 3.10 se tiene que,

$$(\theta_F \otimes \theta_F)(a,b) = \delta_a F^{-1}(b).$$

Luego si $b \neq 0$,

$$\begin{aligned}(\widehat{\theta_F}(a,b))^2 &= (\widehat{\theta_F \otimes \theta_F})(a,b) = \sum_{x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (\theta_F \otimes \theta_F)(x,y)(-1)^{a\cdot x+b\cdot y} \\ &= \sum_{y\in\mathbb{F}_2^m} (\theta_F \otimes \theta_F)(0,y)(-1)^{a\cdot 0+b\cdot y} \\ &+ \sum_{0\neq x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (\theta_F \otimes \theta_F)(x,y)(-1)^{a\cdot x+b\cdot y} \\ &= 2^n + 2^{n-m} \sum_{0\neq x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (-1)^{a\cdot x+b\cdot y}.\end{aligned}$$

Como,

$$\sum_{0\neq x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (-1)^{a\cdot x+b\cdot y} = \begin{cases} 0 & si \quad a=0, b\neq 0 \\ 0 & si \quad a\neq 0, b\neq 0 \end{cases},$$

entonces,

$$(\widehat{\theta_F}(a,b))^2$$

$$= 2^n + 2^{n-m} \sum_{x\neq 0, x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (-1)^{a\cdot x+b\cdot y} = \begin{cases} 2^n & si \quad a=0, b\neq 0 \\ 2^n & si \quad a\neq 0, b\neq 0 \end{cases}.$$

Por lo tanto,

$$(\widehat{\theta_F}(a,b))^2 = 2^n \quad \text{si} \quad b\neq 0,$$

o sea,

$$\lambda_F(a,b) = \widehat{\theta_F}(a,b) = \pm 2^{\frac{n}{2}}$$

para toda (a,b), $b\neq 0$.

$\Leftarrow$) Si F es bent, entonces,

$$\begin{aligned}(\theta_F \otimes \theta_F)(a,b) &= \frac{1}{2^{n+m}}(\widehat{\widehat{\theta_F \otimes \theta_F}})(a,b) = \frac{1}{2^{n+m}}(\widehat{\widehat{\theta_F}(a,b)})^2 \\ &= \frac{1}{2^{n+m}} \sum_{x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (\widehat{\theta_F}(x,y))^2(-1)^{a\cdot x+b\cdot y}.\end{aligned}$$

Ya que, $\widehat{\theta_F}(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x+b\cdot F(x)}$, luego,

$$\widehat{\theta_F}(0,0) = 2^n \quad \text{y} \quad \widehat{\theta_F}(x,0) = 0, \quad x\neq 0.$$

Entonces,

$$\begin{aligned}
& (\theta_F \otimes \theta_F)(a,b) \\
= \; & \frac{1}{2^{n+m}}(2^{2n} + \sum_{0\neq y\in\mathbb{F}_2^m} (\widehat{\theta_F}(0,y))^2(-1)^{b\cdot y} \\
+ \; & \sum_{0\neq x\in\mathbb{F}_2^n} (-1)^{a\cdot x} \sum_{y\in\mathbb{F}_2^m} (\widehat{\theta_F}(x,y))^2(-1)^{b\cdot y}) \\
= \; & \frac{1}{2^{n+m}}(2^{2n} + 2^n(\sum_{0\neq y\in\mathbb{F}_2^m} (-1)^{b\cdot y}) + \sum_{0\neq x\in\mathbb{F}_2^n} (-1)^{a\cdot x}(2^n \sum_{0\neq y\in\mathbb{F}_2^m} (-1)^{b\cdot y})) \\
= \; & \frac{1}{2^{n+m}}(2^{2n} - 2^n + \sum_{0\neq x\in\mathbb{F}_2^n} (-1)^{a\cdot x}(-2^n)) \\
= \; & \frac{1}{2^{n+m}}(2^{2n} - 2^n + 2^n) = 2^{n-m}.
\end{aligned}$$

De aquí,

$$\delta_a F^{-1}(b) = (\theta_F \otimes \theta_F)(a,b) = 2^{n-m} \quad \forall\, 0 \neq a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m.$$

Por lo tanto F es una función perfectamente no-lineal. □

La existencia de una función bent $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ no es posible para todos los valores de m y n.

TEOREMA 3.13. *([**13**]) Las funciones bent, $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, existen únicamente para $n \geq 2m$ y n par.*

DEMOSTRACIÓN. Si F es bent, entonces para toda $b \neq 0$, $b \in \mathbb{F}_2^m$, se tiene que $\widehat{\theta_F}(a,b) = \pm 2^{\frac{n}{2}}$, por lo que n es par. Se definen

$$S = 2^{-\frac{n}{2}} \sum_{0\neq b\in\mathbb{F}_2^m} \widehat{\theta_F}(0,b)$$

y

$$r_0 = |\{b \neq 0, b \in \mathbb{F}_2^m |\ \widehat{\theta_F}(0,b) = 2^{n/2}\}|.$$

Si $\widehat{\theta_F}(0,b) = 2^{\frac{n}{2}}$, entonces en S se tiene un término igual a 1, y cuando $\widehat{\theta_F}(0,b) = -2^{\frac{n}{2}}$, luego en S se tiene un término igual a -1, lo cual implica que

$$S = r_0 - (2^m - 1 - r_0) = 2r_0 - 2^m + 1,$$

de donde S es un entero impar. Por otro lado se tiene que,

$$\begin{aligned}
&\sum_{0\neq b\in\mathbb{F}_2^m} \widehat{\theta_F}(0,b)\\
= &\sum_{b\in\mathbb{F}_2^m} \widehat{\theta_F}(0,b) - \widehat{\theta_F}(0,0) = \sum_{b\in\mathbb{F}_2^m}\sum_{x\in\mathbb{F}_2^n} (-1)^{b\cdot F(x)} - 2^n\\
= &\sum_{x\in\mathbb{F}_2^n}\sum_{b\in\mathbb{F}_2^m} (-1)^{b\cdot F(x)} - 2^n\\
= &\ 2^m a_0 - 2^n,
\end{aligned}$$

donde a_0 es la cardinalidad del conjunto $\{x \in \mathbb{F}_2^n | F(x) = 0\}$, luego,

$$S = 2^{-\frac{n}{2}}(2^m a_0 - 2^n).$$

Por lo tanto,

$$a_0 = 2^{\frac{n}{2}-m}(S + 2^{\frac{n}{2}}).$$

Como a_0 es un entero y S es un entero impar, entonces $2^{\frac{n}{2}-m}$ debe ser un entero. Por consiguiente $n \geq 2m$. □

Recordando la prueba del Teorema 2.7, $f(x) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d)$, n par, no puede ser una función bent para toda $\alpha \in \mathbb{F}_{2^n}^*$, ya que de lo contrario es posible construir una función bent $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ de la siguiente manera:

$$F = \left(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x^d), Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d), \ldots, Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^{n-1}x^d)\right),$$

donde α es un elemento primitivo de $\mathbb{F}_{2^n}$. Si $\mathbf{w} = (w_0, \ldots, w_{n-1}) \in \mathbb{F}_2^n \backslash \{\mathbf{0}\}$, entonces,

$$\begin{aligned}
\mathbf{w}\cdot F &= w_0 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x^d) + \cdots + w_{n-1} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha^{n-1}x^d)\\
&= Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w_0 x^d + \cdots + w_{n-1}\alpha^{n-1}x^d)\\
&= Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}((w_0 + \cdots + w_{n-1}\alpha^{n-1})x^d),
\end{aligned}$$

por lo que F es bent, pero esto no es cierto, por lo que se concluye que $f(x) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha x^d)$ no puede ser una función bent para toda $\alpha \in \mathbb{F}_{2^n}^*$.

4. Funciones casi-bent y casi perfectamente no-lineales

En esta sección se definen las funciones casi-bent y casi perfectamente no-lineales $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, algunas propiedades como su no-linealidad, y se resuelve la relación que existe entre ellas, así como la existencia de estas funciones para los distintos valores de n y m.

En general para funciones $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se tiene que $\Delta_F \geq 2$.

DEFINICIÓN 4.1. *Las funciones $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ tal que $\Delta_F = 2$, son llamadas casi perfectamente no-lineales (CPN).*

Como $\Delta_F \geq 2^{n-m}$, las funciones CPN existen únicamente cuando $m \geq n$ o cuando $(n, m) = (2, 1)$.

TEOREMA 4.2. *([**13**]) Para toda función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se tiene que*

$$\sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} \left(\widehat{\theta_F}(a,b)\right)^4 \geq 2^{2n}(3\times 2^{n+m} - 2^{m+1} - 2^{2n}),$$

con la igualdad sí y sólo si F es CPN.

DEMOSTRACIÓN. Resolviendo:

$$\begin{aligned}
\sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} \left(\widehat{\theta_F}(a,b)\right)^4 &= \sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} \left(\widehat{\theta_F\otimes\theta}_F(a,b)\right)^2 \\
&= \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} \left(\widehat{\theta_F\otimes\theta}_F(a,b)\right)^2 - \sum_{a\in\mathbb{F}_2^n} \left(\widehat{\theta_F\otimes\theta}_F(a,0)\right)^2 \\
&= \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} \left(\widehat{\delta_a F^{-1}}(b)\right)^2 - \sum_{a\in\mathbb{F}_2^n} \left(\widehat{\delta_a F^{-1}}(0)\right)^2 \\
&= \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} \left(\widehat{\delta_a F^{-1}}(b)\right)^2 (-1)^{(0,0)\cdot(a,b)} - \sum_{a\in\mathbb{F}_2^n} \left(\widehat{\delta_a F^{-1}}(0)\right)^2 \\
&= \left(\widehat{\delta_0 F^{-1}}(0)\right)^2 - \sum_{a\in\mathbb{F}_2^n} \left(\widehat{\delta_a F^{-1}}(0)\right)^2.
\end{aligned}$$

Ahora como $\delta_a F^{-1}(b) = (\theta_F\otimes\theta_F)(a,b)$ y $\widehat{\theta_F\otimes\theta}_F(a,b) = \left(\widehat{\theta_F}(a,b)\right)^2$, entonces $\widehat{\delta_a F^{-1}}(b) = \left(\widehat{\theta_F}(a,b)\right)^2$, luego $\left(\widehat{\delta_a F^{-1}}(b)\right)^2 = \left(\widehat{\theta_F}(a,b)\right)^4$, y por el Teorema 3.11, $\widehat{\theta_F}(a,b) = \lambda_F(a,b)$, por lo tanto,

$$\left(\widehat{\theta_F}(a,b)\right)^4 = (\lambda_F(a,b))^4,$$

de aquí se tiene,

$$\left(\widehat{\delta_a F^{-1}}(b)\right)^2 = (\lambda_F(a,b))^4,$$

por consiguiente,

$$\begin{aligned}
\sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} \left(\widehat{\theta_F}(a,b)\right)^4 &= \left(\widehat{\delta_0 F^{-1}}(0)\right)^2 - \sum_{a\in\mathbb{F}_2^n} (\lambda_F(a,0))^4 \\
&= (\widehat{\delta_F\otimes\delta}_F(0,0))^2 - 2^{4n} = 2^{n+m}(\delta_F\otimes\delta_F)(0,0) - 2^{4n} \\
&= 2^{n+m}(\delta_F\otimes\delta_F)(0,0) - 2^{4n}.
\end{aligned}$$

Ya que,

$$\begin{aligned}
(\delta_F\otimes\delta_F)(0,0) &= \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} \delta_a F^{-1}(b)\delta_a F^{-1}(b) \\
&= \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} (\delta_a F^{-1}(b))^2 = 2^{2n} + \sum_{0\neq a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} (\delta_a F^{-1}(b))^2,
\end{aligned}$$

luego,

$$\begin{aligned}
&\sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n}\left(\widehat{\theta}_F(a,b)\right)^4 = 2^{n+m}(\delta_F\otimes\delta_F)(0,0) - 2^{4n}\\
= \;& 2^{n+m}\left(2^{2n} + \sum_{0\neq a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m}(\delta_a F^{-1}(b))^2\right) - 2^{4n}\\
= \;& 2^{n+m}\sum_{0\neq a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m}(\delta_a F^{-1}(b))^2 + 2^{3n+m} - 2^{4n}.
\end{aligned}$$

Para todo entero $n \geq 0$, se tiene que $n^2 = 2n$ sí y sólo si $n = 2$ o $n = 0$. De aquí, para toda $a \neq 0$ y toda b se tiene que $(\delta_a F^{-1}(b))^2 \geq 2\delta_a F^{-1}(b)$, y la igualdad se da sí y sólo si F es CPN. Dado que,

$$\sum_{0\neq a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m}\delta_a F^{-1}(b) = \sum_{0\neq a\in\mathbb{F}_2^n}\sum_{b\in\mathbb{F}_2^m}\delta_a F^{-1}(b) = \sum_{0\neq a\in\mathbb{F}_2^n} 2^n = 2^n(2^n-1),$$

entonces,

$$\begin{aligned}
&\sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n}\left(\widehat{\theta}_F(a,b)\right)^4\\
= \;& 2^{n+m}\sum_{0\neq a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m}(\delta_a F^{-1}(b))^2 + 2^{3n+m} - 2^{4n}\\
\geq \;& 2^{n+m}\sum_{0\neq a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} 2\delta_a F^{-1}(b) + 2^{3n+m} - 2^{4n}\\
= \;& 2^{n+m}2\times 2^n(2^n-1) + 2^{3n+m} - 2^{4n} = 2^{2n}(3\times 2^{n+m} - 2^{m+1} - 2^{2n}),
\end{aligned}$$

o sea,

$$\sum_{b\neq 0, b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n}(\widehat{\theta}_F(a,b))^4 \geq 2^{2n}(3\times 2^{n+m} - 2^{m+1} - 2^{2n}),$$

con la igualdad sí y sólo si F es casi perfectamente no-lineal. □

TEOREMA 4.3. *(*[**13**]*) Para toda función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se tiene que,*

$$\Lambda_F \geq \left(3\times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}\right)^{1/2},$$

con la igualdad sí y sólo si F es casi perfectamente no-lineal y $\lambda_F(\cdot,\cdot)$ tiene los tres distintos valores, $\lambda_F(a,b) = 0,\ \lambda_F(a,b) = -\Lambda_F$ o $\lambda_F(a,b) = \Lambda_F$.

DEMOSTRACIÓN. Observación: para toda función $N(a,b)$ sobre $\mathbb{Z}$, con a en $\mathbb{F}_2^n$ y $b \in \mathbb{F}_2^m$, se cumple que,

$$M = \sup_{a,b\neq 0} N^2(a,b) \geq \frac{\sum_{a\in\mathbb{F}_2^n, 0\neq b\in\mathbb{F}_2^m} N^4(a,b)}{\sum_{a\in\mathbb{F}_2^n, 0\neq b\in\mathbb{F}_2^m} N^2(a,b)},$$

y la igualdad se da sí y sólo si,

$$\forall \quad a \in \mathbb{F}_2^n, 0 \neq b \in \mathbb{F}_2^m \begin{cases} N(a,b) = 0 \\ \text{o } N(a,b) = -\sqrt{M} \\ \text{o } N(a,b) = +\sqrt{M} \end{cases}.$$

Por otro lado,

$$\begin{aligned} & \sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} (\widehat{\theta_F}(a,b))^2 = \sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} (\widehat{\theta_F \otimes \theta_F})(a,b) \\ = & \sum_{0\neq b\in\mathbb{F}_2^m, a\in\mathbb{F}_2^n} \widehat{\delta_a F^{-1}}(b) = \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} \widehat{\delta_a F^{-1}}(b) - \sum_{a\in\mathbb{F}_2^n} \widehat{\delta_a F^{-1}}(0) \\ = & \widehat{(\delta_0 F^{-1}}(0)) - \sum_{a\in\mathbb{F}_2^n} (\lambda_F(a,0))^2 = 2^{n+m}\delta_0 F^{-1}(0) - (\lambda_F(0,0))^2 \\ = & 2^{2n}(2^m - 1). \end{aligned}$$

Por la observación y el Teorema 4.2,

$$\begin{aligned} \Lambda_F^2 = & \sup_{a\in\mathbb{F}_2^n, 0\neq b\in\mathbb{F}_2^m} (\widehat{\theta_F}(a,b))^2 \geq \frac{\sum_{a\in\mathbb{F}_2^n, 0\neq b\in\mathbb{F}_2^m} (\widehat{\theta}_F)^4(a,b)}{\sum_{a\in\mathbb{F}_2^n, 0\neq b\in\mathbb{F}_2^m} (\widehat{\theta}_F)^2(a,b)} \\ \geq & \frac{2^{2n}(3^{n+m} - 2^{m+1} - 2^{2n})}{2^{2n}(2^m - 1)} = \frac{3^{n+m} - 2^{m+1} - 2^{2n}}{2^m - 1} \\ = & 3 \times 2^n - 2 - 2\frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}, \end{aligned}$$

donde la desigualdad es una igualdad sí y sólo si F es casi perfectamente no-lineal y

$$\forall \quad a, b \neq 0 \begin{cases} \widehat{\theta}_F(a,b) = 0 \\ \text{o } \widehat{\theta}_F(a,b) = -\Lambda_F \\ \text{o } \widehat{\theta}_F(a,b) = +\Lambda_F \end{cases},$$

o sea,

$$\forall \quad a, b \neq 0 \begin{cases} \lambda_F(a,b) = 0 \\ \text{o } \lambda_F(a,b) = -\Lambda_F \\ \text{o } \lambda_F(a,b) = +\Lambda_F \end{cases}.$$

□

DEFINICIÓN 4.4. *Se dice que la función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es casi-bent, si*

$$\Lambda_F = \left(3 \times 2^n - 2 - 2\frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}\right)^{1/2}.$$

Veamos para que valores de n y m la definición de función casi-bent tiene sentido:

TEOREMA 4.5. *([**13**]) Si la función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es casi-bent, entonces $n \leq m$, o $n = 2$ y $m = 1$.*

DEMOSTRACIÓN. Si F es casi-bent, entonces F es casi perfectamente no-lineal, luego $n \leq m$, o $n = 2$ y $m = 1$. □

Se puede ver que las funciones bent y las casi-bent coinciden cuando $n = 2$ y $m = 1$. Luego si F es casi-bent y no bent, entonces $n \leq m$.

El siguiente resultado restringe aún más los valores de n y m para los cuales se tiene la existencia de funciones casi-bent.

TEOREMA 4.6. *([**13**]) Si $m > n$, $n \neq 1$, entonces $2^m - 1$ no divide a $(2^n - 1)(2^{n-1} - 1)$.*

DEMOSTRACIÓN.

$$\begin{aligned} & (2^n - 1)(2^{n-1} - 1) = 2^{2n-1} - 2^{n-1} - 2^n + 1 \\ = \;& 2^{2n-1} - 2^{n-1} - 22^{n-1} + 1 = 2^{2n-1} - 3 \times 2^{n-1} + 1 \\ = \;& (2^m - 1)2^{2n-1-m} - (3 \times 2^{n-1} - 2^{2n-1-m} - 1) = A(2^m - 1) - B, \end{aligned}$$

donde,

$A = 2^{2n-1-m}$, $B = 3 \times 2^{n-1} - 2^{2n-1-m} - 1$. $n - m < 0$,
luego, $2^{2n-1-m} = 2^{n-1+n-m} < 2^{n-1}$, por lo que $2^{n-1} - 2^{2n-1-m} > 0$, lo cual implica que,

$$\begin{aligned} & 3 \times 2^{n-1} - 2^{2n-1-m} = 22^{n-1} + 2^{n-1} - 2^{2n-1-m} \\ = \;& 2^n + 2^{n-1} - 2^{2n-1-m} > 2^n > 1. \end{aligned}$$

Por lo tanto,

$$B = 3 \times 2^{n-1} - 2^{2n-1-m} - 1 > 0.$$

Por otro lado $m \geq n + 1$. Entonces $n - m \leq -1$, por lo que $0 < 2^{n-m} \leq \frac{1}{2}$, luego, $2 < 3 - 2^{n-m} < 3$, lo cual implica que,

$$\begin{aligned} & 2^{n-1}(3 - 2^{n-m}) \leq 3 \times 2^{n-1} = 2\frac{3}{2}2^{n-1} \\ = \;& 2^n 2^{log_2(\frac{3}{2})} < 2^{n+log_2(\frac{3}{2})} < 2^{n+1} \leq 2^m. \end{aligned}$$

Ahora $2^{n-1}(3 - 2^{n-m}) < 2^m$ sí y sólo si $3 \times 2^{n-1} - 2^{2n-1-m} - 1 < 2^m - 1$ sí y sólo si $B < 2^m - 1$, por lo tanto,

$$0 < B < 2^m - 1,$$

de aquí,

$$\frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1} = \frac{A(2^m - 1) - B}{2^m - 1}$$

no puede ser un entero. □

Por el resultado anterior se tiene que

$$\left(3 \times 2^n - 2 - 2\frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}\right)^{1/2}$$

no es un entero si $m > n$.

COROLARIO 4.7. *([**13**]) Si $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es una función casi-bent y no bent, entonces $m = n$, n impar. Además $\Lambda_F = 2^{\frac{n+1}{2}}$ si $m = n$.*

DEMOSTRACIÓN. Por el Teorema 4.6 y la observación anterior. Además

$$\left(3 \times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}\right)^{1/2} = 2^{\frac{n+1}{2}}$$

si $n = m$, por lo que n es impar. □

Nótese que las funciones casi-bent $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, n impar, tienen no-linealidad máxima, la cual está dada por (consultar la referencia [**8**]):

$$N_F = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

A continuación se tiene un ejemplo de funciones casi-bent, antes se tiene el siguiente resultado:

TEOREMA 4.8. *([**27**]) Si G es un subcampo con 2^s elementos de $\mathbb{F}_{2^n}$, $s = (k, n)$, entonces*

$$x \in \alpha(G \setminus \{0\}) \text{ sí y sólo si } x \text{ satisface } x^{2^k-1} = \alpha^{2^k-1},\ \alpha \in \mathbb{F}_{2^n}.$$

DEMOSTRACIÓN. $x_1 \in \alpha(G \setminus \{0\})$ implica que $x_1 = \alpha e, e \in (G \setminus \{0\})$, luego, $x_1^{2^k-1} = \alpha^{2^k-1}e^{2^k-1} = \alpha^{2^k-1}e^{2^{sq}}e^{-1} = \alpha^{2^k-1}$, de aquí se tiene que $x_1^{2^k-1} = \alpha^{2^k-1}$. Nótese que las condiciones necesarias anteriores, también son suficientes. □

TEOREMA 4.9. *([**27**]) Sea $F(x) = x^{2^k+1}$, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, donde k es un entero tal que $s = (k, n)$. Entonces $\Delta_F = 2^s$. Si $\frac{n}{s}$ es impar, la distancia de Hamming de la función Booleana $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wF(x))$ al conjunto de las funciones afines es igual a $2^{n-1} - 2^{\frac{n+s}{2}-1}$ para toda $w \in \mathbb{F}_{2^n}^*$.*

DEMOSTRACIÓN. Si $0 \neq a, b \in \mathbb{F}_{2^n}$, luego $\delta_a F^{-1}(b) \geq 2$ o 0, ya que si x_1 es solución de $F(x + a) - F(x) = b$, entonces $x_1 + a$ también es solución.

Sean $x_1 \neq x_2$ dos soluciones, entonces,

$$b = (x_1 + a)^{2^k+1} + x_1^{2^k+1} = (x_2 + a)^{2^k+1} + x_2^{2^k+1},$$

por lo que,

$$(x_1 + a)^{2^k}(x_1 + a) + (x_2 + a)^{2^k}(x_2 + a) = x_1^{2^k+1} + x_2^{2^k+1},$$

luego,

$$(x_1 + x_2)^{2^k} a + (x_1 + x_2)a^{2^k} = 0.$$

Entonces,

$$(x_1 + x_2)^{2^k-1} = a^{2^k-1}.$$

Nótese que las implicaciones anteriores también son suficientes. Ya que $(2^k - 1, 2^n - 1) = 2^s - 1$, si $x^{2^k-1} = c$, $c \in \mathbb{F}_{2^n}^*$ tiene solución, entonces tiene exactamente $2^s - 1$ soluciones en $\mathbb{F}_{2^n}^*$. Sean x_0, x_i soluciones distintas de $(x + a)^{2^k-1} +$

$x^{2^k-1} = b$, luego por el procedimiento anterior y el Teorema 4.8, $x_0 + x_i \in \alpha(G \setminus \{0\})$, por lo que $x_i \in x_0 + \alpha(G \setminus \{0\})$ por lo que $\delta_a F^{-1}(b) = 2^s$ o 0. Nótese que al menos existe una b tal que $\delta_a F^{-1}(b) = 2^s$, lo cual implica que $\Delta_F = 2^s$. Como $n/(n,k)$ es impar, entonces $(2^k+1, 2^n-1) = 1$, por lo cual $F(x) = x^{2^k+1}$ es una permutación. Considerando un isomorfismo entre $\mathbb{F}_2^n$ y $\mathbb{F}_{2^n}$ de modo que el producto punto coincida con la traza se tiene que

$$\lambda_F(a,w) = \sum_{x\in\mathbb{F}_2^n} (-1)^{w\cdot F(x)+a\cdot x} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wF(x))+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ax)},$$

y de aquí,

$$\begin{aligned}
(\lambda_F(a,w))^2 &= \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wx^{2^k+1})+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ax)}\right) \\
&\quad \left(\sum_{y\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(x+y)^{2^k+1})+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a(x+y))}\right) \\
&= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(x+y)^{2^k+1})+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wx^{2^k+1})} \\
&= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(x^{2^k}y+y^{2^k}x))}.
\end{aligned}$$

Sea $y \in \mathbb{F}_{2^n}^*$, denótese por E_y la imagen de la función lineal

$$H_y : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ H_y(x) = F(x+y) + F(x) + F(y) = x^{2^k}y + y^{2^k}x,$$

luego el núcleo de H_y está dado por $\{x \in \mathbb{F}_{2^n}^* |\ x^{2^k-1} = y^{2^k-1}\} \cup \{0\}$, entonces por el Teorema 4.8, el núcleo de H_y es el conjunto yG, donde G es un subcampo de $\mathbb{F}_{2^n}$ de 2^s elementos. Por lo tanto E_y tiene dimensión $n-s$. Por otro lado para cada $y \neq 0$ se tiene que,

$$\begin{cases} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta) = 0\ \ \forall \beta \in E_y \\ \text{o} \\ \sum_{\beta\in E_y} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta)} = 0 \end{cases},$$

ya que si $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta)$ no es la función cero, dado que $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta)}$ es un caracter distinto del trivial sobre E_y, la suma anterior es cero. Por otro lado el conjunto de elementos y tal que $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta) = 0$ para toda $\beta \in E_y$, o lo que es lo mismo el conjunto de elementos y tal que $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(x^{2^k}y + xy^{2^k})) = 0$ para toda $x \in \mathbb{F}_{2^n}$, forma un subespacio lineal Y de $\mathbb{F}_{2^n}$. También para toda $\beta \in E_y$ se tiene la equivalencia $F(x+y) + F(x) + F(y) = \beta \Leftrightarrow (x+y)^{2^k+1} + x^{2^k+1} = \beta - y^{2^k+1}$, y por la primera parte de la prueba se sabe que esta ecuación tiene 2^s

soluciones, luego,

$$\begin{aligned}
&(\lambda_F(a,w))^2 \\
= \;& 2^n + \sum_{y\in\mathbb{F}_{2^n}^*} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})} 2^s \sum_{\beta\in E_y} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta)} \\
= \;& 2^n + \sum_{y\in Y\setminus\{0\}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})} 2^s 2^{n-s} \\
= \;& 2^n + 2^n \sum_{y\in Y\setminus\{0\}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}.
\end{aligned}$$

Para resolverse la última igualdad, veamos cuantos elementos tiene $Y : y \in Y$ sí y sólo si,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wyx^{2^k}) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k}x) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w^{2^k}y^{2^{2k}}x^{2^k}) \; \forall x \in \mathbb{F}_{2^n},$$

luego,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}((wy - w^{2^k}y^{2^{2k}})x^{2^k}) = 0 \; \forall x \in \mathbb{F}_{2^n},$$

por lo que,

$$wy - w^{2^k}y^{2^{2k}} = 0, \text{ pues } (2^k, 2^n - 1) = 1,$$

y de aquí,

$$wy = w^{2^k}y^{2^{2k}},$$

sí y sólo si,

$$w^{2^k-1}y^{2^{2k}-1} = 1.$$

Entonces,

$$\left(wy^{2^k+1}\right)^{2^k-1} = 1.$$

Nótese que las implicaciones anteriores también son suficientes. Ya que $(2^k + 1, 2^n - 1) = 1$ y $(2^k - 1, 2^n - 1) = 2^s - 1$, entonces para la última ecuación existen exactamente 2^s soluciones en $\mathbb{F}_{2^n}^*$, por lo tanto Y tiene 2^s elementos. Nótese que la función $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wx^{2^k+1})$ es lineal en Y, pues

$$\begin{aligned}
& Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(y_1+y_2)^{2^k+1}) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(y_1+y_2)^{2^k}(y_1+y_2)) \\
= \;& Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w(y_1^{2^k+1} + y_1^{2^k}y_2 + y_2^{2^k}y_1 + y_2^{2^k+1})) \\
= \;& Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy_1^{2^k+1} + wy_2^{2^k+1}).
\end{aligned}$$

Ya que $F(x)$ es una permutación entonces $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}$ es un caracter. Como el número de caracteres es finito entonces existirá $a \in \mathbb{F}_{2^n}$ tal que los caracteres $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)}$ y $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}$ coincidan. Eligiendo $a \in \mathbb{F}_{2^n}$ convenientemente se tiene que

$$(\lambda_F(a,w))^2 = 2^n + 2^n(2^s - 1) = 2^{n+s}.$$

Utilizando la relación de no-linealidad se obtiene el resultado deseado. □

Directamente del Teorema 4.9, considerando $s = 1$, se tiene el siguiente ejemplo:

EJEMPLO 4.10. *Sea* $F(x) = x^{2^k+1}$, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, *donde* k *es un entero tal que* $(k, n) = 1$. *Entonces* $\Delta_F = 2$.
Si n *es impar, entonces* F *es casi-bent.*

Con respecto a $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, se resume como sigue:

Si F es bent y casi-bent, entonces $n = 2$ y $m = 1$.

Si F es bent, entonces $n \geq 2m$, n par.

Si F es casi-bent y no bent, entonces $n = m$ con n impar.

Capítulo 3

Funciones bent y perfectamente no-lineales $F : \mathbb{F}_q^n \to \mathbb{F}_q$

En este capítulo se trabaja con funciones $F : \mathbb{F}_q^n \to \mathbb{F}_q$ y de manera natural se extiende la definición de una función bent para este tipo de funciones. En particular si $n = 1$ se tienen funciones $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, $q = p^m$, o en forma equivalente, $F : \mathbb{F}_p^m \to \mathbb{F}_p^m$. Estamos interesados en las funciones bent $F : \mathbb{F}_p^m \to \mathbb{F}_p^m$, ya que en capítulos posteriores serán de utilidad para la construcción de esquemas de compartición de secretos y esquemas de autenticación ([**36**]).

1. Funciones bent y perfectamente no-lineales $F : \mathbb{F}_q^n \to \mathbb{F}_q$

DEFINICIÓN 1.1. *([**14**]) Sea $f : \mathbb{F}_q^n \to \mathbb{F}_q$ una función. La transformada de Fourier de f, es la función con valores complejos $c_{f,\chi}(\cdot) : \mathbb{F}_q^n \to \mathbb{C}$, definida por*

$$c_{f,\chi}(\lambda) := \sum_{x \in \mathbb{F}_q^n} \chi(f(x) - \lambda \cdot x),$$

donde $\chi : \mathbb{F}_q \to \mathbb{C}$ es cualquier caracter aditivo no-trivial de $\mathbb{F}_q$.

Nótese que,

$$c_{f,\chi}(\lambda) = c_{f,\chi_a}(\lambda) = \sum_{x \in \mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(f(x)-\lambda\cdot x))/p},$$

para alguna $a \in \mathbb{F}_q^*$.

Se generaliza la definición de una función bent de la siguiente manera:

DEFINICIÓN 1.2. *([**14**]) La función $f : \mathbb{F}_q^n \to \mathbb{F}_q$ es bent, si todo coeficiente de Fourier tiene magnitud $q^{n/2}$ para cualquier caracter aditivo no-trivial, es decir,*

$$|\sum_{x \in \mathbb{F}_q^n} \chi(f(x) - \lambda \cdot x)| = q^{n/2},$$

para toda $\lambda \in \mathbb{F}_q^n$ y todo $\chi \neq \chi_0$.

En particular se pueden considerar funciones $F : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^n$, p primo impar, o en forma equivalente $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, entonces,

$$c_{F,\chi_a}(\lambda) = \sum_{x \in \mathbb{F}_q} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(F(x)-\lambda x))/p},$$

para algún $a \in \mathbb{F}_q^*$, con $\lambda \in \mathbb{F}_q$. Luego si F es bent,

$$|c_{aF,\chi_1}(\lambda)| = |\sum_{x\in\mathbb{F}_q} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(aF(x)-\lambda x))/p}| = p^{n/2},$$

para toda $a \in \mathbb{F}_q^*$ y toda $\lambda \in \mathbb{F}_q$.

También se generaliza la definición de una función perfectamente no-lineal.

DEFINICIÓN 1.3. *([**14**]) La función $f : \mathbb{F}_q^n \to \mathbb{F}_q$ es perfectamente no-lineal si para toda $a \in \mathbb{F}_q^n$, $a \neq 0$, la función diferencia,*

$$D_a f(x) = f(x + a) - f(x)$$

es balanceada.

El siguiente resultado da una equivalencia entre las funciones perfectamente no-lineales y las funciones bent.

TEOREMA 1.4. *([**14**]) Una función $f : \mathbb{F}_q^n \to \mathbb{F}_q$ es perfectamente no-lineal sí y sólo si f es bent.*

DEMOSTRACIÓN. Considérese el caracter χ_a sobre $\mathbb{F}_q$, distinto del trivial.

$\Rightarrow$) Sea f perfectamente no-lineal. Entonces,

$$\begin{aligned}
&|c_{f,\chi_a}(\lambda)|^2 = c_{f,\chi_a}(\lambda)\overline{c_{f,\chi_a}(\lambda)}\\
=\ &\left(\sum_{x_1\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(f(x_1)-\lambda\cdot x_1))/p}\right)\left(\sum_{x_2\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(-f(x_2)+\lambda\cdot x_2))/p}\right)\\
=\ &\sum_{x_1,x_2\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(f(x_1)-f(x_2)+\lambda\cdot(x_2-x_1)))/p}\\
=\ &\sum_{x_1,x_2\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(-(f(x_2)-f(x_1))+\lambda\cdot(x_2-x_1)))/p}\\
=\ &\sum_{z\in\mathbb{F}_q^n}\sum_{x\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(-(f(x+z)-f(x))+\lambda\cdot z))/p}\\
=\ &\sum_{z\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(\lambda\cdot z))/p}\sum_{x\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(-a(f(x+z)-f(x)))/p} = q^n,
\end{aligned}$$

$z = x_2 - x_1$, es decir, f es bent.

$\Leftarrow$) Si f es bent, sea,

$$S_{\chi_a}(f, z) = \sum_{x\in\mathbb{F}_q^n} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(f(x+z)-f(x)))/p},$$

luego,

$$\sum_{z\in\mathbb{F}_q^n} \chi_a(\lambda\cdot z)\overline{S_{\chi_a}(f, z)} = q^n.$$

Ordenando los elementos de $\mathbb{F}_q^n$:

$$\alpha_0 = 0, \alpha_1, \ldots, \alpha_{q^n-1},$$

la ecuación se expresa:

$$\begin{pmatrix} \chi_a(\alpha_0 \cdot \alpha_0) & \chi_a(\alpha_0 \cdot \alpha_1) & \cdots & \chi_a(\alpha_0 \cdot \alpha_{q^n-1}) \\ \chi_a(\alpha_1 \cdot \alpha_0) & \chi_a(\alpha_1 \cdot \alpha_1) & \cdots & \chi_a(\alpha_1 \cdot \alpha_{q^n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_a(\alpha_{q^n-1} \cdot \alpha_0) & \chi_a(\alpha_{q^n-1} \cdot \alpha_1) & \cdots & \chi_a(\alpha_{q^n-1} \cdot \alpha_{q^n-1}) \end{pmatrix}$$

$$\begin{pmatrix} \overline{S_{\chi_a}(f, \alpha_0)} \\ \overline{S_{\chi_a}(f, \alpha_1)} \\ \vdots \\ \overline{S_{\chi_a}(f, \alpha_{q^n-1})} \end{pmatrix} = \begin{pmatrix} q^n \\ q^n \\ \vdots \\ q^n \end{pmatrix},$$

multiplicando,

$$\begin{pmatrix} \chi_a(-\alpha_0 \cdot \alpha_0) & \chi_a(-\alpha_1 \cdot \alpha_0) & \cdots & \chi_a(-\alpha_{q^n-1} \cdot \alpha_0) \\ \chi_a(-\alpha_0 \cdot \alpha_1) & \chi_a(-\alpha_1 \cdot \alpha_1) & \cdots & \chi_a(-\alpha_{q^n-1} \cdot \alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_a(-\alpha_0 \cdot \alpha_{q^n-1}) & \chi_a(-\alpha_1 \cdot \alpha_{q^n-1}) & \cdots & \chi_a(-\alpha_{q^n-1} \cdot \alpha_{q^n-1}) \end{pmatrix}$$

en ambos lados de la igualdad, se obtiene,

$$\begin{pmatrix} q^n & 0 & \cdots & n \\ 0 & q^n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & q^n \end{pmatrix} \begin{pmatrix} \overline{S_{\chi_a}(f, \alpha_0)} \\ \overline{S_{\chi_a}(f, \alpha_1)} \\ \vdots \\ \overline{S_{\chi_a}(f, \alpha_{q^n-1})} \end{pmatrix}$$

$$= \begin{pmatrix} q^n \left[\chi_a(-\alpha_0 \cdot \alpha_0) + \chi_a(-\alpha_1 \cdot \alpha_0) + \cdots + \chi_a(-\alpha_{q^n-1} \cdot \alpha_0)\right] \\ q^n \left[\chi_a(-\alpha_0 \cdot \alpha_1) + \chi_a(-\alpha_1 \cdot \alpha_1) + \cdots + \chi_a(-\alpha_{q^n-1} \cdot \alpha_1)\right] \\ \vdots \\ q^n \left[\chi_a(-\alpha_0 \cdot \alpha_{q^n-1}) + \chi_a(-\alpha_1 \cdot \alpha_{q^n-1}) + \cdots + \chi_a(-\alpha_{q^n-1} \cdot \alpha_{q^n-1})\right] \end{pmatrix}.$$

Luego,

$$\overline{S_{\chi_a}(f, \alpha_j)} = \sum_{i=0}^{q^n-1} \chi_a(-\alpha_i \cdot \alpha_j) = 0,$$

para $j = 1, \ldots, q^n - 1$. Por lo tanto f es perfectamente no-lineal. □

Obsérvese que si $|c_{f,\chi}(\lambda)| = q^{n/2}$ para algún caracter χ, entonces,

$$|c_{f,\chi}(\lambda)| = q^{n/2}$$

para cualquier caracter distinto del trivial, pues si $|c_{f,\chi_1}(\lambda)| = q^{n/2}$, sin pérdida de generalidad, entonces considerando el caracter χ_1 en forma similar a la prueba del Teorema 1.4, f es perfectamente no-lineal, de aquí nuevamente por el Teorema 1.4, f es bent. Por lo tanto $|c_{f,\chi_a}(\lambda)| = q^{n/2}$, $a \in \mathbb{F}_q^*$.

Algunos ejemplos de funciones bent.

EJEMPLO 1.5. *(*[**14**],[**40**]*) Sea p impar, se tienen los siguientes ejemplos de funciones bent:*

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^{p^k+1}$, $k > 0$, $n/(n,k)$ *impar,*
$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^{3^k+1}$, k *impar,* $(n,k) = 1$,
$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^2$,
$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^{10} + x^6 - x^2$, n *impar.*

Capítulo 4

Construcción de códigos lineales y esquemas de compartición de secretos basados en funciones perfectamente no-lineales

En este capítulo se describe la construcción de códigos lineales y esquemas de compartición de secretos basados en funciones perfectamente no-lineales $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ tomando como referencia los resultados de [**40**] y [**6**]. Se inicia el capítulo con la construcción de códigos lineales basados en funciones perfectamente no-lineales, posteriormente estos códigos proporcionan características deseables para la construcción de esquemas de compartición de secretos siguiendo el método descrito por Massey ([**26**], se puede ver también [**6**]). En el siguiente capítulo se abordan estos temas considerando el caso $p = 2$, es decir, al utilizar las funciones casi-bent.

1. Construcción de códigos lineales basados en funciones perfectamente no-lineales

Al hablar de funciones perfectamente no-lineales, se entiende que también son funciones bent, dada la equivalencia que existe entre ellas (Teorema 1.4 sobre $\mathbb{F}_q$). En esta sección se estudian códigos lineales basados en funciones bent $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$, $p \neq 2$ primo ([**6**]).

DEFINICIÓN 1.1. *Considérese $p \neq 2$ primo, h número natural divisor de n, y $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ una función bent tal que $F(0) = 0$. Sean $a, b \in \mathbb{F}_{p^n}$,*

$$F_{a,b}(x) := aF(x) + bx$$

y

$$C_{a,b} := (Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(\gamma))_{\gamma \in \mathbb{F}^*_{p^n}}).$$

Se define

$$\mathcal{C} := \{C_{a,b} : a, b \in \mathbb{F}_{p^n}\} \subseteq \mathbb{F}_{p^h}^{p^n-1}.$$

Es fácil ver que $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_{p^h}$. Nótese que las funciones $F_{a,b}$ y las funciones $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(x))$, son funciones bent. Veamos cuales son los parámetros de este código.

Para el peso de las palabras del código, únicamente se tiene una cota, el siguiente resultado ([**18**]) es muy importante para la solución de esta cota.

TEOREMA 1.2. *Sea $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $q = p^m$, $p \neq 2$ primo, una función bent. Considérese $(a, b) \neq (0, 0)$ y $u \in \mathbb{F}_q$, si*

$$N(a, b, u) = |\{x \in \mathbb{F}_{q^n} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(x) + bx) = u\}|,$$

entonces,

$$\frac{q^n - (q-1)q^{n/2}}{q} \leq N(a, b, u) \leq \frac{q^n + (q-1)q^{n/2}}{q}.$$

DEMOSTRACIÓN. Si $a = 0$ y $b \neq 0$, entonces, $N(a, b, u) = q^{n-1}$, por lo tanto las desigualdades se dan. Sea $\chi_1(\cdot) := e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(\cdot)/p}$ el caracter aditivo canónico de $\mathbb{F}_q$, y $\psi_1(\cdot) := e^{2\pi i Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\cdot)/p}$ el caracter aditivo canónico de $\mathbb{F}_{q^n}$. Si $a \neq 0$ para cualquier $x \in \mathbb{F}_{q^n}$ y $u \in \mathbb{F}_q$,

$$\begin{aligned}
& qN(a, b, u) \\
= & \sum_{x \in \mathbb{F}_{q^n}} \left[\sum_{y \in \mathbb{F}_q} \chi_1(y(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(x) + bx) - u)) \right] \\
= & q^n + \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^n}} \chi_1 \left(y \left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(x) + bx) - u \right) \right) \\
= & q^n + \sum_{y \in \mathbb{F}_q^*} \chi_1(-yu) \sum_{x \in \mathbb{F}_{q^n}} \psi_1(yaF(x) + ybx).
\end{aligned}$$

De esta relación se sigue que:

$$\begin{aligned}
& |qN(a, b, u) - q^n| \\
= & \left| \sum_{y \in \mathbb{F}_q^*} \chi_1(-yu) \sum_{x \in \mathbb{F}_{q^n}} \psi_1(yaF(x) + ybx) \right| \\
\leq & (q-1)q^{n/2},
\end{aligned}$$

y de aquí se tiene el resultado. □

COROLARIO 1.3. *([**6**]) En el código lineal $\mathcal{C}$ de la Definición 1.1, todo peso no cero w en $\mathcal{C}$ satisface*

$$\frac{p^h - 1}{p^h} \left(p^n - p^{n/2} \right) \leq w \leq \frac{p^h - 1}{p^h} \left(p^n + p^{n/2} \right).$$

DEMOSTRACIÓN. Por el Teorema 1.2 y ya que $F(0) = 0$, se tiene que,

$$\begin{aligned}
& \frac{p^n - (p^h - 1)p^{n/2}}{p^h} - 1 \leq |\{x \in \mathbb{F}_{q^n}^* : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(x) + bx) = 0\}| \\
\leq & \frac{p^n + (p^h - 1)p^{n/2}}{p^h} - 1.
\end{aligned}$$

Por lo tanto,

$$\begin{aligned} & p^n - 1 - \left(\frac{p^n + (p^h - 1)p^{n/2}}{p^h} - 1 \right) \leq w \\ \leq \quad & p^n - 1 - \left(\frac{p^n - (p^h - 1)p^{n/2}}{p^h} - 1 \right), \end{aligned}$$

de lo cual se sigue que:

$$p^n - \left(\frac{p^n + (p^h - 1)p^{n/2}}{p^h} \right) \leq w \leq p^n - \left(\frac{p^n - (p^h - 1)p^{n/2}}{p^h} \right),$$

y por consiguiente se tiene el resultado. □

TEOREMA 1.4. *(*[**6**]*) El código lineal $\mathcal{C}$ de la Definición 1.1, es un $[p^n - 1, 2n/h, d]_{p^h}$ código lineal.*

DEMOSTRACIÓN. La longitud es clara. Analicemos la dimensión del código. Para esto veamos que el conjunto,

$$D = \{C_{1,0}, C_{\alpha,0}, \ldots, C_{\alpha^{r-1},0}, C_{0,1}, C_{0,\alpha}, \ldots, C_{0,\alpha^{r-1}}\},$$

es una base para este código, donde α es un elemento primitivo de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_{p^h}$ y $r = n/h$. Probar que D genera $\mathcal{C}$ es equivalente a ver que el conjunto,

$$E = \{Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{1,0}(x)), Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{\alpha,0}(x)), \ldots, Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{\alpha^{r-1},0}(x)),$$
$$Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,1}(x)), Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,\alpha}(x)), \ldots, Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,\alpha^{r-1}}(x))\},$$

genera,

$$\{Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(x)) : a, b \in \mathbb{F}_{p^n}\}.$$

Sean,

$$Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(x)) \in \{Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(x)) : a, b \in \mathbb{F}_{p^n}\},$$
$$a = d_0 1 + d_1\alpha + \cdots + d_{r-1}\alpha^{r-1}, \quad b = e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1}$$

y

$$d_0, d_1, \ldots, d_{r-1}, e_0, e_1, \ldots, e_{r-1} \in \mathbb{F}_{p^h}.$$

Entonces,

$$\begin{aligned} & Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(x)) = Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(aF(x) + bx) \\ & = Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}((d_0 1 + d_1\alpha + \cdots + d_{r-1}\alpha^{r-1})F(x) \\ & +(e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1})x) = d_0 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F(x)) \\ & +d_1 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(\alpha F(x)) + \cdots + d_{r-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(\alpha^{r-1}F(x)) \\ & +e_0 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(x) + e_1 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(\alpha x) + \cdots + e_{r-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(\alpha^{r-1}x) \\ & = d_0 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{1,0}(x)) + d_1 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{\alpha,0}(x)) + \cdots \\ & +d_{r-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{\alpha^{r-1},0}(x)) + e_0 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,1}(x)) \\ & +e_1 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,\alpha}(x)) + \cdots + e_{r-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,\alpha^{r-1}}(x)). \end{aligned}$$

Probar que el conjunto D es linealmente independiente es equivalente a ver que el conjunto E es linealmente independiente.

Sean,

$$d_0, d_1, \ldots, d_{r-1}, e_0, e_1, \ldots, e_{r-1} \in \mathbb{F}_{p^h}.$$

Si

$$\begin{aligned}
&d_0 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{1,0}(x)) + d_1 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{\alpha,0}(x)) + \cdots \\
&+d_{r-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{\alpha^{r-1},0}(x)) + e_0 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,1}(x)) \\
&+e_1 Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,\alpha}(x)) + \cdots + e_{r-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{0,\alpha^{r-1}}(x)) = 0 \\
&\forall x \in \mathbb{F}_{p^n}^*,
\end{aligned}$$

se tiene que,

$$\begin{aligned}
&Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}((d_0 1 + d_1\alpha + \cdots + d_{r-1}\alpha^{r-1})F(x) \\
&+(e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1})x) = 0 \ \forall x \in \mathbb{F}_{p^n}^*.
\end{aligned}$$

Considérense,

$$\theta_1 = d_0 1 + d_1\alpha + \cdots + d_{r-1}\alpha^{r-1} \quad \text{y} \quad \theta_2 = e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1}.$$

Si

$$Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(\theta_1 F(x) + \theta_2 x) = 0 \quad \forall x \in \mathbb{F}_{p^n}^*,$$

entonces $\theta_1 = \theta_2 = 0$, ya que,

$$Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(\theta_1 F(x) + \theta_2 x)$$

es una función bent si al menos $\theta_1 \neq 0$, y es una función lineal si $\theta_1 = 0$ y $\theta_2 \neq 0$. De aquí se tiene el resultado. □

Con respecto al código lineal anterior se puede conocer una cota para el peso mínimo de su código dual. Antes se enuncia el siguiente resultado.

TEOREMA 1.5. *(Sphere-packing bound) Sea $\mathcal{D}$ un $[n, k, d]_q$ código lineal con distancia mínima $2t + 1$ ó $2t + 2$. Entonces,*

$$q^k \left[1 + \begin{pmatrix} n \\ 1 \end{pmatrix}(q-1) + \cdots + \begin{pmatrix} n \\ t \end{pmatrix}(q-1)^t\right] \leq q^n.$$

□

TEOREMA 1.6. *En el código lineal $\mathcal{C}$ de la definición anterior si $p \geq 3$ y $n > 1$, entonces,*

$$2 \leq d^{\perp} \leq 4.$$

DEMOSTRACIÓN. Aplicando el Teorema 1.5 al código dual del código de la definición anterior se tiene que,

$$(p^h)^{p^n-1-2n/h}\left[1 + \begin{pmatrix} p^n-1 \\ 1 \end{pmatrix}(p^h-1) + \cdots + \begin{pmatrix} p^n-1 \\ t \end{pmatrix}(p^h-1)^t\right]$$

$\leq (p^h)^{p^n-1}$,

lo cual implica que,

$$1 + \left(\begin{array}{c} p^n - 1 \\ 1 \end{array} \right) (p^h - 1) + \cdots + \left(\begin{array}{c} p^n - 1 \\ t \end{array} \right) (p^h - 1)^t \leq p^{2n}.$$

Si se supone que $d^\perp \geq 5$, entonces,

$$\begin{aligned} & 1 + \left(\begin{array}{c} p^n - 1 \\ 1 \end{array} \right) (p^h - 1) + \cdots + \left(\begin{array}{c} p^n - 1 \\ t \end{array} \right) (p^h - 1)^t \\ = & \frac{2 + 2(p^n - 1)(p^h - 1) + (p^{2n} - 3p^n + 2)(p^h - 1)^2}{2} \\ \geq & \frac{2 + 4(p^n - 1) + 4(p^{2n} - 3p^n + 2)}{2} \\ = & \frac{2p^{2n} + 2 \times 3^2(3^2 - 4) + 6}{2} \\ > & p^{2n}, \end{aligned}$$

lo cual es una contradicción, por lo que $d^\perp \leq 4$. No es difícil ver que $d^\perp \neq 1$ (véase el Teorema 1.3 del siguiente capítulo). Luego $2 \leq d^\perp \leq 4$. □

De este modo se han obtenido parámetros del código lineal de la definición anterior, sin embargo, no ha sido posible hallar la distribución de pesos. La siguiente definición es la de un código lineal ([**6**]) en donde esto si es posible.

DEFINICIÓN 1.7. *Considérese $p \neq 2$ primo y $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ una función definida por $F(x) = x^{p^r+1}$, $n/(n, r)$ impar, la cual es una función bent. Sean $a, b \in \mathbb{F}_{p^n}$,*

$$F_{a,b}(x) := aF(x) + bx$$

y

$$C_{a,b} := (Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(F_{a,b}(\gamma))_{\gamma \in \mathbb{F}_{p^n}^*}).$$

Se define

$$\mathcal{C} := \{C_{a,b} : a, b \in \mathbb{F}_{p^n}\} \subseteq \mathbb{F}_p^{p^n-1}.$$

Es fácil ver que $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_p$.

El siguiente resultado da la longitud, dimensión y peso mínimo del código anterior para el caso n impar, así como una relación con el código dual.

TEOREMA 1.8. *([**40**]) Sea $\mathcal{C}$ de la Definición 1.7, entonces $\mathcal{C}^\perp$ tiene peso mínimo $d^\perp = 3$ ó 4. Si n es impar, $\mathcal{C}$ es un $[p^n - 1, 2n, (p-1)p^{n-1} - p^{\frac{n-1}{2}}]_p$ código lineal, más aún, los distintos pesos de las palabras no cero del código $\mathcal{C}$ son:*

$$(p-1)p^{n-1} - p^{\frac{n-1}{2}}, \quad (p-1)p^{n-1}, \quad (p-1)p^{n-1} + p^{\frac{n-1}{2}}.$$

DEMOSTRACIÓN. La prueba de la longitud y dimensión del código lineal se sigue del caso $h = 1$ de la Definición 1.1.

Veamos la prueba del peso mínimo del código dual: si $d^{\perp} = 2$, entonces existe $\mathbf{c} = (c_1, c_2, \ldots, 0) \in \mathcal{C}^{\perp}$ tal que sin pérdida de generalidad consideramos $c_1 \neq 0 \neq c_2$ y todas las demás coordenadas igual a cero. Luego,

$$(c_1, c_2, \ldots, 0) \cdot (Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(aF(x_1) + bx_1), \ldots, Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(aF(x_{p^n-1}) + bx_{p^n-1}))$$

$= 0 \; \forall (a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, lo cual implica que,

$$Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(aF(x_1) + bx_1) = c(Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(aF(x_2) + bx_2)),$$

$\forall\ (a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, tal que $x_1 \neq x_2$ y $c \in \mathbb{F}_p^*$, o equivalentemente,

$$aF(x_1) + bx_1 = c(aF(x_2) + bx_2)\ \forall (a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$$

sí y sólo si, $x_1 = cx_2$, $F(x_1) = cF(x_2)$, es decir, $F(cx_2) = cF(x_2)$. Nótese que todas las relaciones anteriores son equivalencias. También se tiene que $F(cx_2) = c^{p^r+1}x_2^{p^r+1} \neq cx_2^{p^r+1}$, ya que de lo contrario $c^{p^r+1} = c$ por lo que $(p^n - 1)|p^r$, lo cual es una contradicción. Por lo tanto $d^{\perp} \neq 2$, y de aquí $3 \leq d^{\perp} \leq 4$.

Veamos los distintos pesos de las palabras del código: sea $C_{a,b} \in \mathcal{C}$, si $a = b = 0$, $C_{a,b}$ es la palabra cero.
Si $a = 0$, $b \neq 0$, como bx es lineal, $w(C_{a,b}) = (p-1)p^{n-1}$.
Si $a \neq 0$, $b = 0$, sea $q = p^n$, por el Teorema 2.18 del Capítulo 1,

$$\begin{aligned} q - w(C_{a,b}) &= |\{x \in \mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^{p^r+1}) = 0\}| \\ &= |\{x \in \mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2) = 0\}| = p^{n-1}, \end{aligned}$$

y por lo tanto,

$$w(C_{a,b}) = p^n - p^{n-1} = (p-1)p^{n-1}.$$

Si $a \neq 0$, $b \neq 0$,

$$\begin{aligned} & q - w(C_{a,b}) = |\{x \in \mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^{p^r+1} + bx) = 0\}| \\ = \; & \frac{1}{p} \sum_{x \in \mathbb{F}_q} \sum_{c \in \mathbb{F}_p} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(acx^{p^r+1} + bcx)/p} \\ = \; & \frac{1}{p} \left(q + \sum_{c \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(acx^{p^r+1} + bcx)/p} \right) \\ = \; & \frac{1}{p} \left(q + \sum_{c \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(acx^{p^r+1} + bcx) \right) = \frac{1}{p} \left(q + \sum_{c \in \mathbb{F}_p^*} S_r(ac, bc) \right). \end{aligned}$$

Por otro lado para cualquier $c \in \mathbb{F}_p^*$, la ecuación,

$$(ac)^{p^r} x^{p^{2r}} + acx + (bc)^{p^r} = 0,$$

es equivalente a,

$$a^{p^r} x^{p^{2r}} + ax + b^{p^r} = 0,$$

pues $c^{p^r} = c$. Por el Teorema 2.15 del Capítulo 1, esta ecuación tiene una única solución $x_{a,b}$, y por el Teorema 2.17 del Capítulo 1,

$$S_r(ac, bc) = \begin{cases} (-1)^{n-1} q^{1/2} \eta(-ac) \overline{\chi_1(acx_{a,b}{}^{p^r+1})} & si \quad p \equiv 1 \text{ mód } 4 \\ (-1)^{n-1} i^{3n} q^{1/2} \eta(-ac) \overline{\chi_1(acx_{a,b}{}^{p^r+1})} & si \quad p \equiv 3 \text{ mód } 4 \end{cases},$$

luego si $Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^{p^r+1}) = 0$, entonces,

$$\sum_{c \in \mathbb{F}_p^*} S_r(ac, bc) = q^{1/2} \eta(-a) \sum_{c \in \mathbb{F}_p^*} \eta(c) = 0,$$

lo cual implica que,

$$w(C_{a,b}) = p^n - p^{n-1} = (p-1)p^{n-1}.$$

Si $Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^{p^r+1}) \neq 0$, sea $r = -Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax_{a,b}^{p^r+1})$ y χ'_1, η' los caracteres aditivo canónico y cuadrático sobre $\mathbb{F}_p$ respectivamente, entonces

$$\begin{aligned} & \sum_{c \in \mathbb{F}_p^*} S_r(ac, bc) = q^{1/2} \eta(-a) \sum_{c \in \mathbb{F}_p^*} \eta(c) \overline{\chi_1(acx_{a,b}^{p^r+1})} \\ = \quad & q^{1/2} \eta(-a) \sum_{c \in \mathbb{F}_p^*} \eta(c) e^{2\pi i(-Tr_{\mathbb{F}_q/\mathbb{F}_p}(acx_{a,b}^{p^r+1}))} = q^{1/2} \eta(-a) \sum_{c \in \mathbb{F}_p^*} \eta(c) e^{2\pi irc} \\ = \quad & q^{1/2} \eta(-a) \sum_{c' \in \mathbb{F}_p^*} \eta(c'/r) e^{2\pi ic'} = q^{1/2} \eta(-a/r) \sum_{c' \in \mathbb{F}_p^*} \eta'(c') \chi'_1(c') \\ = \quad & q^{1/2} \eta(-a/r) G(\eta', \chi'_1) = \pm p^{n/2} p^{1/2} = \pm p^{\frac{n+1}{2}}, \end{aligned}$$

donde $rc = c'$. Luego $w(C_{a,b}) = p^n - p^{n-1} \pm p^{\frac{n+1}{2}} = (p-1)p^{n-1} \pm p^{\frac{n+1}{2}}$, y el resultado queda probado □

Más aún, en el caso del código lineal de la Definición 1.7, se tiene la distribución de pesos para el caso n impar y n par.

Una herramienta para conocer la distribución de pesos en el caso n impar es el siguiente resultado de relaciones de Pless ([**30**]). Sea,

$$\binom{n}{r} := \begin{cases} \frac{n!}{r!(n-r)!} & si \quad n \geq r \geq 0 \\ 0 & si \quad r > n \end{cases}.$$

TEOREMA 1.9. *(Relaciones de Pless,* [**30**]*) Sea C un $[n, k]$ código lineal sobre $\mathbb{F}_2$. Si A_i es el número de palabras de peso i de C y B_i el número de palabras de peso i en $C^\perp$. Entonces,*

$$\sum_{j=0}^{n} j^r A_j = \sum_{j=0}^{n} (-1)^j B_j \Big(\sum_{v=0}^{r} v! S(r, v) 2^{k-v} \binom{n-j}{n-v} \Big),$$

donde,

$$S(r, v) = \frac{1}{v!} \sum_{i=0}^{v} (-1)^{v-i} \binom{v}{i} i^r.$$

La ecuación es para cualquier r, por lo que hay una infinidad de tales relaciones.

□

TEOREMA 1.10. *([**40**]) Sea $\mathcal{C}$ el código de la Definición 1.7 con n impar. Entonces la distribución de pesos de este código está dada por:*

$$\begin{aligned}
&A_0 = 1,\\
&A_{(p-1)p^{n-1}-p^{\frac{n-1}{2}}} = (p-1)(p^n-1)\tfrac{p^{n-1}+p^{(n-1)/2}}{2},\\
&A_{(p-1)p^{n-1}} = (p^{n-1}+1)(p^n-1),\\
&A_{(p-1)p^{n-1}+p^{\frac{n-1}{2}}} = (p-1)(p^n-1)\tfrac{p^{n-1}-p^{(n-1)/2}}{2}.
\end{aligned}$$

DEMOSTRACIÓN. Por el Teorema 1.8 se tiene que los distintos pesos del código $\mathcal{C}$ son,

$$(p-1)p^{n-1}-p^{\frac{n-1}{2}}, \quad (p-1)p^{n-1}, \quad (p-1)p^{n-1}+p^{\frac{n-1}{2}}.$$

Por otro lado se sabe que $\mathcal{C}^{\perp}$ tiene peso mínimo mayor que 2, por lo que $B_1 = B_2 = 0$, donde B_1 y B_2 son el número de palabras de peso 1 y 2 respectivamente del código dual, luego de las relaciones de Pless se obtienen las siguientes tres ecuaciones:

1. $\sum_{j=0}^{n} A_j = p^{2n}$
2. $\sum_{j=0}^{n} jA_j = p^{2n-1}(p-1)(p^n-1)$
3. $\sum_{j=0}^{n} j^2A_j = p^{2n-2}(p-1)(p^n-1)(p+(p-1)(p^n-2))$.

Al resolver el sistema se tiene la afirmación. □

TEOREMA 1.11. *Sea $\mathcal{C}$ el código lineal de la Definición 1.7. Si n es par, la distribución de pesos de este código es:*

$$\begin{aligned}
&A_{(p-1)p^{n-1}-(p-1)p^{n/2-1}} = \frac{p^n-1}{2p}\left(q+(p-1)q^{1/2}\right),\\
&A_{(p-1)p^{n-1}+(p-1)p^{n/2-1}} = \frac{p^n-1}{2p}\left(q-(p-1)q^{1/2}\right),\\
&A_{(p-1)p^{n-1}-p^{n/2-1}} = \frac{p^n-1}{2p}(p-1)\left(q+q^{1/2}\right),\\
&A_{(p-1)p^{n-1}+p^{n/2-1}} = \frac{p^n-1}{2p}(p-1)\left(q-q^{1/2}\right),\\
&A_{(p-1)p^{n-1}} = p^n-1.
\end{aligned}$$

DEMOSTRACIÓN. Si $a = 0, b \neq 0$, ya que $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(F_{a,b})$ es lineal, entonces $w(C_{0,b}) = (p-1)p^{n-1}$. De estas palabras existen p^n-1 elementos en el código. Si $a \neq 0, b = 0$, sea $q = p^n$, por el Teorema 2.18 del Capítulo 1,

$$\begin{aligned}
& q - w(C_{a,0}) = |\{x \in \mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^{p^r+1}) = 0\}|\\
= \;& |\{x \in \mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2) = 0\}|\\
= \;& \begin{cases} \frac{1}{p}\left(q-\eta(a)(p-1)q^{1/2}\right) & \text{si } p \equiv 1 \text{ mód } 4\\ \frac{1}{p}\left(q-i^n\eta(a)(p-1)q^{1/2}\right) & \text{si } p \equiv 3 \text{ mód } 4 \end{cases},
\end{aligned}$$

lo cual implica que,

$$w(C_{a,0}) = (p-1)p^{n-1} \pm (p-1)p^{n/2} - 1,$$

dependiendo del valor de $\eta(a)$, luego para cada uno de esos casos existen $\frac{p^n-1}{2}$ palabras con ese peso.
Si $a \neq 0, b \neq 0$, de manera similar a la prueba del Teorema 1.8 se tiene que

$$w(C_{a,b}) = (p-1)p^{n-1} - \frac{1}{p}\sum_{c\in\mathbb{F}_p^*} S_r(ac, bc),$$

y por el Teorema 2.17 del Capítulo 1,

$$S_r(ac,bc) = \begin{cases} (-1)^{n-1}q^{1/2}\eta(-ac)\overline{\chi_1(acx_{a,b}{}^{p^r+1})} & si \quad p \equiv 1 \text{ mód } 4 \\ (-1)^{n-1}i^{3n}q^{1/2}\eta(-ac)\overline{\chi_1(acx_{a,b}{}^{p^r+1})} & si \quad p \equiv 3 \text{ mód } 4 \end{cases},$$

donde $x_{a,b}$ es la única solución para la ecuación $a^{p^r}x^{p^{2r}} + ax + b^{p^r}$. Para cualquier $c \in \mathbb{F}_p^*$ se tiene $\eta(c) = 1$, $\eta(-c) = 1$ y

$$\sum_{c\in\mathbb{F}_p^*} \overline{\chi_1(acx_{a,b}{}^{p^r+1})} = \begin{cases} p-1 & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) = 0 \\ -1 & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) \neq 0 \end{cases}.$$

Sea $R_{a,b} = \sum_{c\in\mathbb{F}_p^*} S_r(ac, bc)$, luego,

$$R_{a,b} = \begin{cases} -q^{1/2}\eta(a)(p-1) & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) = 0,\ p \equiv 1 \text{ mód } 4 \\ q^{1/2}\eta(a) & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) \neq 0,\ p \equiv 1 \text{ mód } 4 \\ -i^n q^{1/2}\eta(a)(p-1) & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) = 0,\ p \equiv 3 \text{ mód } 4 \\ i^n q^{1/2}\eta(a) & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) \neq 0,\ p \equiv 3 \text{ mód } 4 \end{cases}.$$

Nótese que el número de veces en que ocurre cada peso depende de $R_{a,b}$, y éste a su vez depende del valor de $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1})$. También para $a \in \mathbb{F}_q^*$ fija, existe un único $x_{a,b}$ que satisface $a^{p^r}x^{p^{2r}} + ax = -b^{p^r}$ para cada $b \in \mathbb{F}_q^*$. Estas $x_{a,b}$ recorren todos los elementos de $\mathbb{F}_q^*$. Así, para un elemento $a \in \mathbb{F}_q^*$, los valores y las frecuencias de $ax_{a,b}^{p^r+1}$ cuando b corre sobre $\mathbb{F}_q^*$ son los mismos valores y frecuencias de ay^{p^r+1} cuando y corre sobre $\mathbb{F}_q^*$, y éstos a su vez son los mismos valores y frecuencias de az^2 cuando z corre sobre $\mathbb{F}_q^*$.
Si $\eta(a) = 1$, entonces,

$$R_{a,b} = \begin{cases} -q^{1/2}(p-1) & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) = 0,\ p \equiv 1 \text{ mód } 4 \\ q^{1/2} & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) \neq 0,\ p \equiv 1 \text{ mód } 4 \end{cases}.$$

Luego, si $\eta(a) = 1$, $p \equiv 1$ mód 4,

$$w(C_{a,b}) = \begin{cases} (p-1)p^{n-1} + (p-1)p^{n/2-1} & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) = 0 \\ (p-1)p^{n-1} - p^{n/2-1} & \text{si } Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax_{a,b}{}^{p^r+1}) \neq 0 \end{cases}.$$

Entonces por el Teorema 2.18 del Capítulo 1 y el caso $C_{a,0}$, $a \neq 0$,

$$w(C_{a,b}) = (p-1)p^{n-1} + (p-1)p^{n/2-1},$$

ocurre,

$$\frac{p^n-1}{2}\left(\frac{1}{p}(q-(p-1)q^{1/2})-1\right)+\frac{p^n-1}{2}=\frac{p^n-1}{2p}\left(q-(p-1)q^{1/2}\right)$$

veces.

$$w(C_{a,b})=(p-1)p^{n-1}-p^{n/2-1},$$

ocurre,

$$q-\left(\frac{1}{p}(q-(p-1)q^{1/2})\right)=\frac{p-1}{p}\left(q+q^{1/2}\right)$$

veces.
Si $\eta(a)=-1$, $p\equiv 1$ mód 4, notando que solo ocurre un cambio de signo en las valores de $R_{a,b}$ y aplicando nuevamente el Teorema 2.18 del Capítulo 1, para $\eta(a)=-1$, y procediendo de manera similar se tiene que,

$$w(C_{a,b})=(p-1)p^{n-1}-(p-1)p^{n/2-1},$$

ocurre,

$$\frac{p^n-1}{2}\left(\frac{1}{p}(q+(p-1)q^{1/2})-1\right)+\frac{p^n-1}{2}=\frac{p^n-1}{2p}\left(q+(p-1)q^{1/2}\right)$$

veces. Similarmente,

$$w(C_{a,b})=(p-1)p^{n-1}+p^{n/2-1},$$

ocurre,

$$q-\left(\frac{1}{p}(q+(p-1)q^{1/2})\right)=\frac{p-1}{p}\left(q-q^{1/2}\right)$$

veces.
El caso $p\equiv 3$ mód 4 es similar al caso anterior al considerar $\eta(a)=1$, $\eta(a)=-1$ y $m\equiv 0$ mód 4, pues no se ven afectados los valores de $R_{a,b}$ y $|\{x\in\mathbb{F}_q : Tr_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)=0\}|$.
Si $m\equiv 2$ mód 4, únicamente ocurren cambios de signo, pero éstos no afectan el resultado al considerar los casos $\eta(a)=1$ y $\eta(a)=-1$. Por consiguiente la afirmación del teorema queda probada. □

2. Esquemas de compartición de secretos basados en funciones perfectamente no-lineales

Los esquemas de compartición de secretos fueron introducidos por G. R. Blakey ([**2**]) y A. Shamir ([**33**]) en el año de 1979. En los esquemas de compartición de secretos, se considera un secreto en la responsabilidad de varias entidades, tal que con cierto número de estas el secreto puede ser recuperado, pero este secreto no se puede obtener con un número menor de participantes. Un encargado o repartidor asigna una parte del secreto a cada una de las entidades. En un banco por ejemplo, existe una bóveda que debe ser abierta todo los días, para esto el banco emplea tres personas de modo que al faltar al menos una de estas personas, la bóveda no puede ser abierta. En criptografía visual, al sobreponer un número finito de láminas se

puede reconocer una imagen de tal modo que con un menor número de estas láminas esto no es posible. Existen varios esquemas de compartición de secretos, por ejemplo el esquema Threshold de Shamir, el cual puede consultarse en [**36**].

3. Esquemas de compartición de secretos, método de Massey

Hay varias formas de usar los códigos lineales para construir un esquema de compartición de secretos. Uno es el descrito por James L. Massey ([**26**], ver también [**6**]).

El método desarrollado por Massey se puede describir de la siguiente forma:

- Sea $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$ una matriz generadora de un $[n, k, d]_q$ código lineal $\mathcal{C}$. Se considerarán todos los vectores columna de la matriz generadora, distintos de cero.
- En el esquema de compartición de secretos basado en $\mathcal{C}$, el secreto es un elemento de $\mathbb{F}_q$ elegido aleatoriamente. $\mathbb{F}_q$ es llamado el espacio de secretos.
- Se tienen $n-1$ participantes $P_1, P_2, \ldots, P_{n-1}$ y un encargado P_0.
- Para calcular las acciones (parte del secreto) con respecto al secreto s, el encargado elige aleatoriamente un vector
$$u = (u_0, \ldots, u_{k-1}) \in \mathbb{F}_q^k$$
tal que $s = u\mathbf{g}_0$. Hay en total q^{k-1} de tales vectores $u \in \mathbb{F}_q^k$ pues $u\mathbf{g}_0$ es una función lineal.
- El elemento u se toma como un vector de información y se determina el vector codificado
$$\begin{aligned} uG &= u(\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}) = (u\mathbf{g}_0, u\mathbf{g}_1, \ldots, u\mathbf{g}_{n-1}) \\ &= (t_0, t_1, \ldots, t_{n-1}) = t. \end{aligned}$$
- El encargado asigna t_i al participante P_i como su acción para cada $i \geq 1$, en donde la acción es una parte de la información del secreto.

Nótese que $t_0 = u\mathbf{g}_0 = s$.

El siguiente resultado, el cual proporciona una relación entre las acciones y las columnas de la matriz generadora del código lineal que se está considerando, se refiere para toda $u \in \mathbb{F}_q^k$ tal que $u\mathbf{g}_0 = s$, donde el secreto s es fijo, por lo tanto en el siguiente resultado y para los que se deriven de este, se sobreentenderá este hecho. Más adelante se dará un ejemplo de esta situación. Nótese que los conjuntos de acciones
$$\{t_{i_1}, \ldots, t_{i_m}\},$$
no necesariamente son los mismos al considerar distintos valores de u, pero el conjunto de participantes si lo es.

TEOREMA 3.1. *([**26**],[**6**]) Las acciones*
$$(t_{i_1}, t_{i_2}, \ldots, t_{i_m}) = u(\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}),$$

donde $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$ *es la matriz generadora de un código lineal, determinan el secreto sí y sólo si* $\mathbf{g}_0$ *es una combinación lineal de* $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$.

DEMOSTRACIÓN.
$\Leftarrow$) Si $\mathbf{g}_0$ es una combinación lineal de $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}$, entonces,

$$\mathbf{g}_0 = c_{i_1}\mathbf{g}_{i_1} + \cdots + c_{i_m}\mathbf{g}_{i_m},$$

de lo cual se sigue que,

$$u\mathbf{g}_0 = uc_{i_1}\mathbf{g}_{i_1} + \cdots + uc_{i_m}\mathbf{g}_{i_m},$$

lo cual implica que,

$$s = c_{i_1}t_{i_1} + \cdots + c_{i_m}t_{i_m}.$$

$\Rightarrow$) Si $s = c_{i_1}t_{i_1} + \cdots + c_{i_m}t_{i_m}$, entonces,

$$u\mathbf{g}_0 = c_{i_1}u\mathbf{g}_{i_1} + \cdots + c_{i_m}u\mathbf{g}_{i_m},$$

luego,

$$s = u\mathbf{g}_0 = u(c_{i_1}\mathbf{g}_{i_1} + \cdots + c_{i_m}\mathbf{g}_{i_m}).$$

Por lo tanto,

$$\mathbf{g}_0 = c_{i_1}\mathbf{g}_{i_1} + \cdots + c_{i_m}\mathbf{g}_{i_m}$$

pues tenemos dos funciones lineales iguales, ya que esta igualdad se da para toda $u \in \mathbb{F}_q^k$ tal que $s = u\mathbf{g}_0$. □

Utilizando el teorema anterior se tiene el siguiente resultado, el cual nos da una relación con el código dual del código que se está considerando.

COROLARIO 3.2. *(*[**26**],[**6**]*) Sea* G *una matriz generadora de un* $[n, k]_q$ *código lineal* $\mathcal{C}$. *En el esquema de compartición de secretos basado en* $\mathcal{C}$, *un conjunto de acciones* $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ *determinan el secreto sí y sólo si existe una palabra*

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0) \qquad (*)$$

en el código dual $\mathcal{C}^\perp$, *donde se tiene que* $c_{i_j} \neq 0$ *para al menos una* j, $1 \leq i_1 < \cdots < i_m \leq n-1$ *y* $1 \leq m \leq n-1$.

DEMOSTRACIÓN. Nótese que G es una matriz verificadora de paridad del código dual $\mathcal{C}^\perp$. Para una palabra de la forma $(*)$ en $\mathcal{C}^\perp$ se tiene que,

$$\begin{aligned} &G(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)^\perp \\ &= (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)^\perp = 0 \end{aligned}$$

sí y sólo si,

$$\mathbf{g}_0 + c_{i_1}\mathbf{g}_{i_1} + \cdots + c_{i_m}\mathbf{g}_{i_m} = 0,$$

o equivalentemente,

$$\mathbf{g}_0 = -c_{i_1}\mathbf{g}_{i_1} - \cdots - c_{i_m}\mathbf{g}_{i_m},$$

y de aquí, utilizando el Teorema 3.1 se tiene el resultado. □

Si un grupo de participantes puede recuperar el secreto combinando sus acciones, entonces cualquier grupo de participantes conteniendo este grupo puede

también recuperar el secreto.

Se puede dar una relación más estrecha con el código dual, para esta relación se requieren los siguientes conceptos ([**6**]):

- Un grupo de participantes es llamado "conjunto de acceso mínimo" si ellos pueden recuperar el secreto con sus acciones, pero cualquier subgrupo propio de este no lo puede hacer.
- El soporte de un vector $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ es definido por

$$sop(\mathbf{c}) = \{1 \leq i \leq n : c_i \neq 0\}.$$

- Una palabra $\mathbf{c}_2$ se dice que cubre a una palabra $\mathbf{c}_1$, si el soporte de $\mathbf{c}_2$ contiene al de $\mathbf{c}_1$.
- Una palabra $\mathbf{c}$ es llamada mínima si sólo cubre a múltiplos no cero de ella.

COROLARIO 3.3. *([**26**],[**6**]) Sea $\mathcal{C}$ un $[n,k]_q$ código lineal. En el esquema de compartición de secretos basado en C, existe una correspondencia uno a uno entre la familia de conjuntos de acceso mínimo y el conjunto de palabras mínimas del código dual $\mathcal{C}^{\perp}$ cuya primera entrada es* 1.

DEMOSTRACIÓN. Sea A un conjunto de acceso mínimo y

$$t = \{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$$

su respectivo conjunto de acciones, luego t determina el secreto. Entonces por el Corolario 3.2 hay una palabra

$$\mathbf{c} = (1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$$

en el código $\mathcal{C}^{\perp}$ tal que $s = -c_{i_1}t_{i_1} - \cdots - c_{i_m}t_{i_m}$. Además $c_{i_j} \neq 0\ \forall j$ tal que $1 \leq j \leq m$. Más aún $\mathbf{c}$ es una palabra mínima del código dual $\mathcal{C}^{\perp}$, pues los coeficientes de las acciones correspondientes a conjuntos de acceso mínimo siempre son distintos de cero, ya que si un coeficiente c_{i_j} fuese cero, se podría suprimir el participante correspondiente a ese coeficiente.

Si $\mathbf{c}$ es una palabra mínima de $\mathcal{C}^{\perp}$ con 1 en la primera entrada, digamos $\mathbf{c} = (1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$, $c_{i_j} \neq 0, \forall j \in \{1, \ldots, m\}$, por el Corolario 3.2 existe un conjunto de acciones $t = \{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ que determinan el secreto s considerado. A este conjunto le corresponde un conjunto de acceso mínimo, ya que si se prescinde de uno de estos participantes, nuevamente por el Corolario 3.2, se tendría una palabra contenida propiamente en $\mathbf{c}$. □

Los conceptos anteriores se pueden ilustrar con el siguiente ejemplo. Considérese el código lineal binario $[7, 4, 3]$ de Hamming $\mathcal{H}$, cuya matriz verificadora de paridad es

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

y matriz generadora,

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

Considérese un esquema sobre $\mathcal{H}^{\perp}$ y elegimos $u = (1, 0, 1)$. Ya que H es una matriz generadora para $\mathcal{H}^{\perp}$, entonces $s = (1, 0, 1) \cdot (1, 1, 0)$. Si se desea conocer los conjuntos de acceso mínimo, una forma, es determinando las palabras mínimas con uno en la primera entrada del código lineal $\mathcal{H}$:

$$\mathcal{H} = \left\{ \begin{array}{lll} (1,0,0,1,0,0,1), & (1,0,0,0,1,1,0), & (0,1,0,0,1,0,1), \\ (0,0,1,0,0,1,1), & (0,1,0,1,0,1,0), & (0,0,1,1,1,0,0), \\ (1,1,1,0,0,0,0), & (1,0,1,0,1,0,1), & (0,1,1,0,1,1,0), \\ (1,0,1,1,0,1,0), & (0,1,1,1,0,0,1), & (0,0,0,1,1,1,1), \\ (1,1,0,1,1,0,0), & (1,1,0,0,0,1,1), & (0,0,0,0,0,0,0), \\ (1,1,1,1,1,1,1). & & \end{array} \right\}.$$

Es fácil ver que todas las palabras con uno en la primera entrada son palabras mínimas, a excepción de la palabra $(1, 1, 1, 1, 1, 1, 1)$.

Sean $\{t_1, t_2, t_3, t_4, t_5, t_6\}$ las acciones de los respectivos participantes

$$\{P_1, P_2, P_3, P_4, P_5, P_6\}.$$

Entonces,

$$\begin{aligned} s = 1 &= t_3 + t_6 \\ &= t_4 + t_5 \\ &= t_2 + t_3 \\ &= t_2 + t_4 + t_6 \\ &= t_2 + t_3 + t_5 \\ &= t_1 + t_3 + t_4 \\ &= t_1 + t_5 + t_6, \end{aligned}$$

son las combinaciones de todos los conjuntos de acceso mínimo. Para el elemento $u = (1, 0, 1)$ se tiene $t_1 = 0, t_2 = 1, t_3 = 0, t_4 = 1, t_5 = 0, t_6 = 1$. Podríamos pensar que podemos suprimir t_3 en la primera combinación, pues $t_3 = 0$. Pero si consideramos $u = (1, 0, 0)$, entonces $s = 1, t_3 = 1$ y $t_6 = 0$. Obsérvese que $(1, 0, 0)$ es una elemento tal que $(1, 0, 0) \cdot (1, 1, 0) = 1$. Sin embargo este no es un buen ejemplo de esquema, pues cualquier atacante tiene probabilidad $1/2$ de descubrir el secreto.

La estructura de acceso de un esquema de compartición de secretos, son los conjuntos de acceso mínimo que determinan el secreto. Gracias a los resultados anteriores, para determinar la estructura de acceso del esquema de compartición de secretos basado en un código lineal, solo se necesita determinar el conjunto de palabras mínimas cuya primera coordenada es 1 del código dual. Sin embargo, no en todos los casos es posible determinar el conjunto de las palabras mínimas. Es

un problema abierto el determinar el conjunto de todas las palabras mínimas de un código lineal ([**6**]).

3.1. La estructura de acceso mínimo del esquema de compartición de secretos. Se ha descrito la construcción general de un esquema de compartición de secretos basado en un código lineal $\mathcal{C}$. Procediendo del mismo modo se puede ver que también tenemos un esquema de compartición de secretos basado en el código dual $\mathcal{C}^{\perp}$.

TEOREMA 3.4. *([**6**]) Sea $\mathcal{C}$ un $[n, k, d]_q$ código lineal y*

$$G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$$

una matriz generadora. Si cada palabra no cero de $\mathcal{C}$ es mínima, entonces en el esquema de compartición de secretos basado en $\mathcal{C}^{\perp}$ se tiene que:

1. *Hay en total q^{k-1} conjuntos de acceso mínimo.*
2. *Cuando $d^{\perp} = 2$, la estructura de acceso es la siguiente:*
   a) Si $\mathbf{g}_i$ es un múltiplo de $\mathbf{g}_0$, $1 \leq i \leq n-1$, entonces el participante P_i, está incluido en todo conjunto de acceso mínimo.
   b) Si $\mathbf{g}_i$, no es un múltiplo de $\mathbf{g}_0$, $1 \leq i \leq n-1$, entonces el participante P_i está incluido en $(q-1)q^{k-2}$ conjuntos de acceso mínimo.
3. *Si $d^{\perp} \geq 3$, para cualquier t fija tal que*

$$1 \leq t \leq \text{mín}\{k-1, d^{\perp}-2\},$$

se tiene que todo grupo de t participantes está incluido en

$$(q-1)^t q^{k-(t+1)}$$

conjuntos de acceso mínimo.

DEMOSTRACIÓN. Veamos primero que el número total de conjuntos de acceso mínimo es q^{k-1}. Se está trabajando con un esquema de compartición de secretos basado en $\mathcal{C}^{\perp}$, luego para calcular el número total de conjuntos de acceso mínimo, sólo se necesita calcular el número de palabras mínimas de $\mathcal{C}$, cuya primera coordenada es 1. Recordar que se está suponiendo que toda columna de cualquier matriz generadora no es la columna cero, luego $\mathbf{g}_0 \neq \mathbf{0}$. Por lo tanto el producto interior $u\mathbf{g}_0$ toma cada elemento de $\mathbb{F}_q^*$ exactamente q^{k-1} veces cuando u corre sobre todos los elementos distintos de cero de $\mathbb{F}_q^k$, pues es una función lineal.

Supóngase ahora que $d^{\perp} = 2$. Determinemos la estructura de acceso mínimo basado en $\mathcal{C}^{\perp}$. Para cualquier $1 \leq i \leq n-1$, si $\mathbf{g}_i = a\mathbf{g}_0$ para algún $a \in \mathbb{F}_q^*$, entonces $u\mathbf{g}_0 = 1$ implica que $u\mathbf{g}_i = a \neq 0$. Por lo tanto el participante P_i está en todo conjunto de acceso mínimo, ya que en cualquier palabra $(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0)$ (cuya primera entrada es 1) de $\mathcal{C}$, siempre será distinto de cero la i-ésima entrada, luego por el Corolario 3.3, todo conjunto que determine el secreto siempre incluirá a la acción t_i. En particular al conjunto de acciones que provienen de un conjunto de participantes de acceso mínimo.

Si $\mathbf{g}_i$ no es un múltiplo de $\mathbf{g}_0$, para cualquier $1 \leq i \leq n-1$ se tiene que $(u\mathbf{g}_0, u\mathbf{g}_i)$ toma cada elemento de $\mathbb{F}_q^2$, q^{k-2} veces cuando el vector corre sobre $\mathbb{F}_q^k$ (pues la operación $u \cdot (\mathbf{g}_0, \mathbf{g}_1)$ es una función lineal con contradominio $\mathbb{F}_q^2$). Luego,

$$|\{u : (u\mathbf{g}_0 \neq 0, u\mathbf{g}_i \neq 0)\}| = (q-1)^2 q^{k-2}$$

y

$$|\{u : (u\mathbf{g}_0 = 1, u\mathbf{g}_i \neq 0)\}| = (q-1)q^{k-2}.$$

Recordando que los elementos distintos de cero de $\mathcal{C}$ son palabras mínimas, entonces como $u\mathbf{g}_0 = 1$ y $u\mathbf{g}_i \neq 0$ son coordenadas de las palabras de $\mathcal{C}$, luego por el corolario anterior existen precisamente $(q-1)q^{k-2}$ conjuntos de acceso mínimo en el cual P_i está implicado.

Supóngase que $d^\perp \geq 3$ y $1 \leq t \leq \text{mín}\{k-1, d^\perp - 2\}$. Consideremos $1 \leq i_1 < i_2 < \cdots \leq n-1$ un conjunto de enteros positivos. Entonces,

$$\mathbf{g}_0, \mathbf{g}_{i_1}, \mathbf{g}_{i_2}, \ldots, \mathbf{g}_{i_t},$$

son linealmente independientes y

$$(u\mathbf{g}_0, u\mathbf{g}_{i_1}, u\mathbf{g}_{i_2}, \ldots, u\mathbf{g}_{i_t}),$$

toma cada elemento de $\mathbb{F}_q^{t+1}$, $q^{k-(t+1)}$ veces, cuando u corre sobre $\mathbb{F}_q^k$. Luego

$$|\{u : (u\mathbf{g}_0 \neq 0, u\mathbf{g}_{i_1} \neq 0, \ldots, u\mathbf{g}_{i_t} \neq 0)\}| = (q-1)^{t+1} q^{k-(t+1)}$$

y

$$|\{u : (u\mathbf{g}_0 = 1, u\mathbf{g}_{i_1} \neq 0, \ldots, u\mathbf{g}_{i_t} \neq 0)\}| = (q-1)^t q^{k-(t+1)}.$$

Donde similar a las observaciones anteriores, se puede decir que el número de conjuntos de acceso mínimo donde P_i es incluido es

$$(q-1)^t q^{k-(t+1)}.$$

□

En vista del resultado anterior, hay un interesante problema de construir códigos donde cada palabra no cero sea una palabra mínima.

TEOREMA 3.5. *([6]) Sea $\mathcal{C}$ un $[n,k]_q$ código lineal, $w_{mín}$ y $w_{máx}$ los pesos mínimo y máximo no cero respectivamente de las palabras del código. Si*

$$\frac{w_{mín}}{w_{máx}} > \frac{q-1}{q},$$

entonces cada palabra no cero de $\mathcal{C}$ es una palabra mínima.

DEMOSTRACIÓN. Supóngase que

$$\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \text{ cubre } \mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$$

y que $\mathbf{u}$ no es un múltiplo de $\mathbf{v}$. Entonces,

$$w_{\text{mín}} \leq w(\mathbf{v}) \leq w(\mathbf{u}) \leq w_{\text{máx}}.$$

Por otro lado, sea $t \in \mathbb{F}_q^*$ y $m_t = |\{i : v_i \neq 0, u_i = tv_i\}|$, luego,

$$\sum_{t \in \mathbb{F}_q^*} m_t = w(\mathbf{v}),$$

por lo que existe $t \in \mathbb{F}_q^*$ tal que $m_t \geq \frac{w(\mathbf{v})}{q-1}$, pues se está dividiendo $w(\mathbf{v})$ en $q-1$ partes y hay $q-1$ términos de la forma m_t sumándose. Si todos los términos son menores a cada una de las partes iguales en que se dividió $w(\mathbf{v})$, entonces no se tendría la igualdad anterior, pues $\mathbf{u}$ cubriría a $\mathbf{v}$, y de aquí,

$$w(\mathbf{u} - t\mathbf{v}) = w(\mathbf{u}) - m_t \leq w(\mathbf{u}) - \frac{w(\mathbf{v})}{q-1} \leq w_{\text{máx}} - \frac{w_{\text{mín}}}{q-1}$$
$$< \frac{q}{q-1} w_{\text{mín}} - \frac{w_{\text{mín}}}{q-1} = w_{\text{mín}},$$

lo cual es una contradicción. Por lo tanto si $\mathbf{u}$ cubre a $\mathbf{v}$, entonces $\mathbf{u}$ es múltiplo de $\mathbf{v}$, para $\mathbf{u}$ y $\mathbf{v}$ arbitrarios con esta propiedad. Por lo tanto cada palabra no cero de $\mathcal{C}$ es una palabra mínima. □

3.2. Esquemas de compartición de secretos. Al utilizar las propiedades de los códigos lineales construidos en base a funciones bent, se puede obtener la estructura de acceso de los esquemas de compartición de secretos basados en estos códigos.

TEOREMA 3.6. *([**6**]) Consideremos $\mathcal{C}$ el código lineal de la definición 1.1. Si $p^h < (p^{n/2}+1)/2$, entonces las palabras del código $\mathcal{C}$ son mínimas.*

DEMOSTRACIÓN.

$$\frac{w_{\text{mín}}}{w_{\text{máx}}} \geq \frac{p^n - p^{n/2}}{p^n + p^{n/2}} = \frac{p^{n/2}-1}{p^{n/2}+1} > \frac{p^h - 1}{p^h}.$$

Por otro lado,

$$p^h < (p^{n/2}+1)/2,$$

entonces,

$$p^h - 1 < (p^{n/2}-1)/2,$$

lo cual implica que,

$$\frac{p^{n/2}-1}{2} + (p^h - 1)(\frac{p^{n/2}-1}{2}) > p^h - 1 + (p^h - 1)(\frac{p^{n/2}-1}{2}),$$

de esta expresión tenemos que,

$$(\frac{p^{n/2}-1}{2})(p^h - 1 + 1) > (p^h - 1)(\frac{p^{n/2}-1}{2} + 1),$$

luego,

$$\frac{\frac{p^{n/2}-1}{2}}{\frac{p^{n/2}-1}{2} + 1} > \frac{p^h - 1}{p^h - 1 + 1}.$$

Por lo tanto,

$$\frac{p^{n/2}-1}{p^{n/2}+1} > \frac{p^h - 1}{p^h}.$$

Entonces por el Teorema 3.5, todas las palabras son mínimas. □

TEOREMA 3.7. *([**6**]) Sea $\mathcal{C}$ el código lineal de la definición 1.1 y una matriz generadora $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, g_{p^n-2})$. Si $p^h < (p^{n/2}+1)/2$, entonces en el esquema de compartición de secretos basado en $\mathcal{C}^\perp$, el número total de participantes es $p^n - 2$ y hay en total p^{2n-h} conjuntos de acceso mínimo.*

1. *Cuando $d^\perp = 2$, si $\mathbf{g}_i$ es un múltiplo de $\mathbf{g}_0$, $1 \leq i \leq p^n - 2$, entonces el participante P_i está incluido en todo conjunto de acceso mínimo.*
   Si $\mathbf{g}_i$ no es un múltiplo de $\mathbf{g}_0$, $1 \leq i \leq p^n - 2$, entonces el participante P_i está incluido en

$$(p^h - 1)p^{2n-2h}$$

   conjuntos de acceso mínimo.
2. *Si $d^\perp \geq 3$, para t fija tal que $1 \leq t \leq$ mín$\{(2n/h) - 1, d^\perp - 2\}$, todo grupo de t participantes está incluido en*

$$(p^h - 1)^t p^{2n-(t+1)h}$$

   conjuntos de acceso mínimo.

DEMOSTRACIÓN. La afirmación se sigue del Teorema 3.6 y el Teorema 3.4. □

Se tiene el siguiente ejemplo:

Sea $\mathcal{C}$ el código lineal de la definición 1.1, con los campos $\mathbb{F}_{3^3}$ y $\mathbb{F}_3$, en donde $F(x) = x^2$ es la función bent. La matriz generadora del código $\mathcal{C}$ está dada por $G =$

$$\left(\begin{array}{c|cccccccccccccccccc} & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 1 & 1 & 2 \\ & 1 & 0 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 0 & 1 & 2 & 0 \\ I_6 & 0 & 1 & 0 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 0 & 1 & 2 \\ & 1 & 2 & 2 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 0 & 1 & 2 & 0 & 0 & 1 & 0 \\ & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 0 & 1 & 2 & 0 & 0 & 1 \\ & 2 & 1 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 1 & 1 & 2 & 1 \end{array}\right),$$

y la matriz generadora del código $\mathcal{C}^{\perp}$, está dada por $H =$

$$\left(\begin{array}{c|cccccc} & 2 & 2 & 0 & 2 & 0 & 1 \\ & 1 & 0 & 2 & 1 & 2 & 2 \\ & 2 & 0 & 0 & 1 & 1 & 0 \\ & 0 & 2 & 0 & 0 & 1 & 1 \\ & 1 & 1 & 2 & 1 & 0 & 0 \\ & 0 & 1 & 1 & 2 & 1 & 0 \\ & 0 & 0 & 1 & 1 & 2 & 1 \\ & 1 & 1 & 0 & 2 & 1 & 1 \\ I_{20} & 1 & 2 & 1 & 1 & 2 & 0 \\ & 0 & 1 & 2 & 1 & 1 & 2 \\ & 2 & 2 & 1 & 1 & 1 & 2 \\ & 2 & 1 & 2 & 0 & 1 & 2 \\ & 2 & 1 & 1 & 1 & 0 & 2 \\ & 2 & 1 & 1 & 0 & 1 & 1 \\ & 1 & 0 & 1 & 2 & 0 & 0 \\ & 0 & 1 & 0 & 1 & 2 & 0 \\ & 0 & 0 & 1 & 0 & 1 & 2 \\ & 2 & 2 & 0 & 0 & 0 & 2 \\ & 2 & 1 & 2 & 2 & 0 & 1 \\ & 1 & 0 & 1 & 0 & 2 & 2 \end{array}\right).$$

Considérese el esquema sobre $\mathcal{C}^{\perp}$. Si se desea conocer los conjuntos de acceso mínimo, una forma, es determinando las palabras mínimas con uno en la primera entrada del código lineal $\mathcal{C}$. El código lineal $\mathcal{C}$ tiene 243 palabras mínimas con uno en la primera entrada, por lo que es el número de conjuntos de acceso mínimo que se tiene en el esquema. Aquí escribimos algunas palabras mínimas:

$(1,1,1,2,0,0,1,1,2,1,0,0,0,0,0,1,2,1,0,2,0,0,2,2,0,1)$
$(1,1,0,0,1,0,2,0,0,0,1,1,1,0,1,1,1,2,0,2,2,0,2,2,0,0)$,
$(1,1,1,0,1,0,2,1,0,0,2,0,0,0,0,2,0,0,2,1,1,0,1,2,1,2)$,
$(1,0,2,0,2,0,1,0,2,1,1,2,0,0,2,0,0,1,2,0,0,2,2,1,0,2)$,
$(1,1,2,0,2,0,2,0,2,2,0,1,0,2,0,2,1,0,1,2,0,1,2,2,2,2)$,
$(1,1,0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1,1,2,0,1)$,
$(1,2,0,0,2,0,0,1,2,0,0,2,2,1,0,2,1,0,2,0,2,0,1,0,2,1)$,
$(1,0,0,0,2,0,1,1,2,1,2,1,2,0,1,1,2,2,1,2,2,2,1,1,1,1)$,
$(1,0,0,0,2,1,0,2,2,0,2,1,1,2,1,2,0,0,2,1,2,2,2,2,0,2)$,
$(1,1,0,0,2,1,1,2,2,1,1,0,1,1,2,1,1,2,1,0,2,1,2,0,2,2)$,
$(1,2,0,0,2,1,2,2,2,2,0,2,1,0,0,0,2,1,0,2,2,0,2,1,1,2)$,
$(1,2,1,0,2,1,2,0,2,2,1,1,0,0,2,1,1,2,2,1,1,0,1,1,2,1)$,
$(1,0,1,0,2,1,0,0,2,0,0,0,0,2,0,0,2,1,1,0,1,2,1,2,1,1)$,
$(1,1,1,0,2,1,1,0,2,1,2,2,0,1,1,2,0,0,0,2,1,1,1,0,0,1)$,
$(1,1,2,0,2,1,1,1,2,1,0,1,2,1,0,0,2,1,2,1,0,1,0,0,1,0)$,
$(1,2,2,0,2,1,2,1,2,2,2,0,2,0,1,2,0,0,1,0,0,0,0,1,0,0)$,
$(1,0,2,0,2,1,0,1,2,0,1,2,2,2,2,1,1,2,0,2,0,2,0,2,2,0)$,

$(1,0,2,1,2,1,1,0,1,0,0,0,1,0,1,0,0,2,2,2,1,1,0,2,0,0)$,
$(1,1,2,1,2,1,2,0,1,1,2,2,1,2,2,2,1,1,1,1,1,0,0,0,2,0)$,
$(1,2,2,1,2,1,0,0,1,2,1,1,1,1,0,1,2,0,0,0,1,2,0,1,1,0)$.

Por el Corolario 3.3 para cada palabra mínima con uno en la primera entrada se tiene un conjunto de acceso mínimo, el cual está formado por las acciones correspondientes a las entradas distintas de cero. Al expresar el secreto s como combinación lineal de las acciones, como coeficientes se consideran los negativos de las entradas distintas de cero de cada palabra mínima correspondiente con uno en la primera entrada. Por ejemplo la primera palabra de la lista anterior corresponde al siguiente conjunto de acceso mínimo:

$\{t_1, t_2, t_3, t_6, t_7, t_8, t_9, t_{15}, t_{16}, t_{17}, t_{19}, t_{22}, t_{23}, t_{25}\}$.

Si s es un secreto (elegido de $\mathbb{F}_3$), entonces las combinaciones lineales de las acciones de los conjuntos de acceso mínimo correspondientes a las primeras tres palabras de la lista anterior están dadas por

$s = 2t_1 + 2t_2 + t_3 + 2t_6 + 2t_7 + t_8 + 2t_9 + 2t_{15} + t_{16} + 2t_{17} + t_{19} + t_{22} + t_{23} + 2t_{25}$,
$s = 2t_1 + 2t_4 + t_6 + 2t_{10} + 2t_{11} + 2t_{12} + 2t_{14} + 2t_{15} + 2t_{16} + t_{17} + t_{19} + t_{20} + t_{22} + t_{23}$,
$s = 2t_1 + 2t_2 + 2t_4 + t_6 + 2t_7 + t_{10} + t_{15} + t_{18} + 2t_{19} + 2t_{20} + 2t_{22} + t_{23} + 2t_{24} + t_{25}$.

Si por ejemplo $s = 1$, cada una de estas combinaciones lineales deben ser satisfechas para toda $u \in \mathbb{F}_3^{20}$, tal que

$$u \cdot (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0,2,0,1) = 1,$$

es decir, el producto de u y la primera columna de la matriz generadora de $\mathcal{C}^{\perp}$. Nótese que para cada elemento u, los valores de las acciones no son las mismas, pues esa misma u al muliplicarse por cada una de las columnas de la matriz generadora de $\mathcal{C}^{\perp}$ se obtiene una correspondiente acción. Por ejemplo, si $u = (1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$, entonces todas las acciones son igual a cero, a excepción de $t_{20} = 2$, $t_{21} = 2$, $t_{23} = 2$, $t_{25} = 1$. Si $u = (1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$, entonces todas las acciones son igual a cero, a excepción de $t_1 = 1, t_{21} = 2, t_{22} = 2, t_{24} = 2$. Si $u = (1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$ entonces todas las acciones son igual a cero, a excepción de $t_1 = 1$, $t_2 = 1$, $t_{20} = 2$, $t_{21} = 2, t_{22} = 2, t_{23} = 1$. Puede observarse que cualquiera de los tres conjuntos de acciones anteriores satisface las combinaciones antes escritas si $s = 1$.

Capítulo 5

Construcción de códigos lineales y esquemas de compartición de secretos basados en funciones casi-bent

En este capítulo se presentan resultados análogos a los obtenidos en el Capítulo 4 ($p \neq 2$), ya que se presenta el caso $p = 2$, es decir, utilizando funciones $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, por lo que es necesario considerar las llamadas funciones casi-bent ([**13**]) (para la construcción de códigos lineales y esquemas de compartición de secretos en base a estas funciones). Se inicia dando la construcción de códigos lineales en base a las funciones casi-bent obteniendo sus parámetros y posteriormente se da la construcción de esquemas de compartición de secretos utilizando estos códigos lineales siguiendo el método de Massey. Más aún se presentan dos extensiones de estos esquemas cuando el espacio secreto es $\mathbb{F}_2$.

1. Construcción de códigos lineales en base a funciones casi-bent

En esta sección se da la construcción de códigos lineales basados en funciones casi-bent.
Construcción $n = hr$, $h > 1$.

DEFINICIÓN 1.1. *Si $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $n = hr$ impar, es una función casi-bent, sean $a, b \in \mathbb{F}_{2^n}$,*

$$F_{a,b}(x) := aF(x) + bx$$

y

$$C_{a,b} := (Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{a,b}(\gamma))_{\gamma \in \mathbb{F}_{2^n}^*}).$$

Se define

$$\mathcal{C} := \{C_{a,b} : a, b \in \mathbb{F}_{2^n}\} \subseteq \mathbb{F}_{2^h}^{2^n-1}.$$

Es fácil ver que $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_{2^h}$. Nótese que las funciones $F_{a,b}(x) := aF(x) + bx$ son también funciones casi-bent.

TEOREMA 1.2. *La dimensión del código lineal $\mathcal{C}$ de la Definición 1.1 es $2n/h$, y una base está dada por el conjunto*

$$D = \{C_{1,0}, C_{\alpha,0}, \ldots, C_{\alpha^{r-1},0}, C_{0,1}, C_{0,\alpha}, \ldots, C_{0,\alpha^{r-1}}\},$$

donde $r = n/h$ y α es un elemento primitivo de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_{2^h}$.

DEMOSTRACIÓN. Analicemos la dimensión del código. Para esto, veamos que el conjunto

$$D = \{C_{1,0}, C_{\alpha,0}, \ldots, C_{\alpha^{r-1},0}, C_{0,1}, C_{0,\alpha}, \ldots, C_{0,\alpha^{r-1}}\},$$

es una base para este código. Probar que D genera $\mathcal{C}$ es equivalente a ver que el conjunto

$$E = \{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{1,0}(x)), Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{\alpha,0}(x)), \ldots, Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{\alpha^{r-1},0}(x)),$$
$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{0,1}(x)), Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{0,\alpha}(x)), \ldots, Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{0,\alpha^{r-1}}(x))\},$$

genera al subespacio

$$\{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{a,b}(x)) : a, b \in \mathbb{F}_{2^n}\},$$

y la prueba es similar a la del Teorema 1.4 del capítulo anterior.

Probar que el conjunto D es linealmente independiente es equivalente a demostrar que el conjunto E es linealmente independiente sobre $\mathbb{F}_{2^h}$.

Sean,

$$d_0, d_1, \ldots, d_{r-1}, e_0, e_1, \ldots, e_{r-1} \in \mathbb{F}_{2^h}.$$

Si

$$\begin{aligned}
&d_0 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{1,0}(x)) + d_1 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{\alpha,0}(x)) + \cdots \\
&+d_{r-1} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{\alpha^{r-1},0}(x)) + e_0 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{0,1}(x)) \\
&+e_1 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{0,\alpha}(x)) + \cdots + e_{r-1} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F_{0,\alpha^{r-1}}(x)) = 0 \\
&\forall x \in \mathbb{F}_{2^n}^*,
\end{aligned}$$

se tiene que,

$$\begin{aligned}
&Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}((d_0 1 + d_1\alpha + \cdots + d_{r-1}\alpha^{r-1})F(x) \\
&+(e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1})x) = 0 \ \forall x \in \mathbb{F}_{2^n}^*.
\end{aligned}$$

Considérense,

$$\theta_1 = d_0 1 + d_1\alpha + \cdots + d_{r-1}\alpha^{r-1} \quad \text{y} \quad \theta_2 = e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1}.$$

Si $\theta_1 = 0$ y $\theta_2 \neq 0$,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\theta_2 x) = 0 \ \forall x \in \mathbb{F}_{2^n}^*,$$

lo cual no es posible pues la función traza es balanceada. Si $\theta_1 \neq 0$ y $\theta_2 \neq 0$,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\theta_1 F(x) + \theta_2 x) = 0 \quad \forall x \in \mathbb{F}_{2^n}^*,$$

luego,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\theta_1 F(x) + \theta_2 x) = Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\theta_1 F(x) + \theta_2 x)) = 0$$

$\forall x \in \mathbb{F}_{2^n}^*$ lo cual no es posible, pues como F es casi-bent,

$$|\{x | Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\theta_1 F(x) + \theta_2 x) = 1\}| \in \{2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}}\},$$

ya que si $\lambda_F(b, a) = \widehat{\zeta_{aF}}(b) = 2^{\frac{n+1}{2}}$ y se define,

$$A = |\{x : Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(aF(x) + bx) = 1\}|$$

y

$$B = |\{x : Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(aF(x) + bx = 0)\}|,$$

se tiene,

$$B - A = \lambda_F(b, a) = 2^{\frac{n+1}{2}},$$

y por lo tanto,

$$A = B - 2^{\frac{n+1}{2}} = 2^n - A - 2^{\frac{n+1}{2}},$$

lo cual implica,

$$A = \frac{2^n - 2^{\frac{n+1}{2}}}{2} = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Si $\lambda_F(b, a) = -2^{\frac{n+1}{2}}$, entonces,

$$B - A = \widehat{\zeta_{aF}}(b) = -2^{\frac{n+1}{2}}$$

implica,

$$A = B + 2^{\frac{n+1}{2}} = 2^n - A + 2^{\frac{n+1}{2}},$$

y por consiguiente,

$$A = \frac{2^n + 2^{\frac{n+1}{2}}}{2} = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

Si $\lambda_F(a, b) = 0$, entonces, $B - A = 0$, lo cual implica, $B = A$ y por lo tanto,

$$A = 2^{n-1}.$$

Si $\theta_1 \neq 0$ y $\theta_2 = 0$, entonces,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\theta_1 F(x)) = 0 \qquad \forall x \in \mathbb{F}_{2^n}^*,$$

y

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\theta_1 F(x)) = Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\theta_1 F(x))) = 0 \; \forall x \in \mathbb{F}_{2^n}^*,$$

lo cual no es posible pues como F es casi-bent, entonces,

$$|\{x | Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\theta_1 F(x)) = 1\}| \in \{2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}}\}.$$

Por lo tanto $\theta_1 = 0$ y $\theta_2 = 0$, y ya que $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ es una base de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_{2^h}$, se tiene que,

$$d_0 = d_1 = \cdots = d_{r-1} = e_0 = e_1 = \cdots = e_{r-1} = 0.$$

Por lo que el código lineal $\mathcal{C}$ es de dimensión $2n/h$. □

En el siguiente resultado se da una cota del peso mínimo del código dual del código lineal de la Definición 1.1. En particular este resultado permitirá conocer ciertas características del esquema de compartición de secretos que se construirá usando el método de Massey a partir de este código.

TEOREMA 1.3. *([7]) Sea $\mathcal{C}$ el código lineal de la Definición 1.1. Entonces $\mathcal{C}^\perp$ tiene peso mínimo mayor o igual que* 5.

DEMOSTRACIÓN. Sabemos que

$$\{C_{1,0}, C_{\alpha,0}, \ldots, C_{\alpha^{r-1},0}, C_{0,1}, C_{0,\alpha}, \ldots, C_{0,\alpha^{r-1}}\}$$

es una base para $\mathcal{C}$, luego,

$$G = \begin{pmatrix} C_{1,0} \\ C_{\alpha,0} \\ \vdots \\ C_{\alpha^{r-1},0} \\ C_{0,1} \\ C_{0,\alpha} \\ \vdots \\ C_{0,\alpha^{r-1}} \end{pmatrix} =$$

$$\begin{pmatrix} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F(1)) & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F(\alpha)) & \cdots & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(F(\alpha^{2^n-2})) \\ Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha F(1)) & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha\, F(\alpha)) & \ldots & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha F(\alpha^{2^n-2})) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{r-1}F(1)) & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{r-1}F(\alpha)) & \cdots & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{r-1}F(\alpha^{2^n-2})) \\ Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(1) & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha) & \cdots & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{2^n-2}) \\ Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha 1) & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha\alpha) & \ldots & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha\alpha^{2^n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{r-1}1) & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{r-1}\alpha) & \cdots & Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{r-1}\alpha^{2^n-2}) \end{pmatrix},$$

es una matriz generadora para $\mathcal{C}$. Obsérvese que ninguna columna de la matriz G es cero, pues si suponemos que la columna $j+1$, $j = 0, \ldots, 2^n - 2$, es la columna cero, entonces,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^j) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+1}) = \cdots = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+r-1}) = 0,$$

y de aquí, si x es un elemento arbitrario de $\mathbb{F}_{2^n}^*$,

$$x = e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1},$$

$$\begin{aligned} &Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^j x) = e_0 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^j) + e_1 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+1}) + \cdots \\ &+e_{r-1}Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+r-1}) = 0,\ \forall x \Rightarrow \alpha^j = 0, \end{aligned}$$

lo cual es una contradicción.

Si dos columnas de G son iguales, digamos las columnas $i+1$ y $j+1$, y sin pérdida de generalidad se supone que $i < j$, entonces,

$$\begin{aligned} &Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^j - \alpha^i) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+1} - \alpha^{i+1}) = \cdots \\ &= Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+r-1} - \alpha^{i+r-1}) = 0, \end{aligned}$$

de aquí, si x es un elemento arbitrario de $\mathbb{F}_{2^n}^*$,

$$x = e_0 1 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1},$$

y por lo tanto,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}((\alpha^j-\alpha^i)x) = e_0 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^j-\alpha^i)$$
$$+e_1 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+1}-\alpha^{i+1}) + \cdots + e_{r-1} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+r-1}-\alpha^{i+r-1})$$
$$= 0,\ \forall x,$$

y de aquí $\alpha^j - \alpha^i = 0$, luego $\alpha^j = \alpha^i$, lo cual es también una contradicción. Como G es una matriz generadora para $\mathcal{C}$, entonces es una matriz verificadora de paridad para $\mathcal{C}^\perp$, por lo tanto,

$$x \in \mathcal{C}^\perp \text{ sí y sólo si } Gx^t = 0,$$

luego, si una palabra de $x \in \mathcal{C}^\perp$ tiene peso 1, implica que una columna de G es cero, lo cual no es posible. Si una palabra $x \in \mathcal{C}^\perp$ tiene peso 2, implica que 2 columnas de G son iguales, lo cual también es una contradicción. Por lo tanto el código lineal $\mathcal{C}$ tiene peso mínimo mayor que 2.

Si $\mathcal{C}^\perp$ tiene peso mínimo 4, sea $\mathbf{c} = (c_1, c_2, c_3, c_4, \ldots, 0) \in \mathcal{C}^\perp$ tal que sin pérdida de generalidad las primeras cuatro coordenadas son distintas de cero y las demás igual a cero. Entonces,

$$c_1 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_1)+bx_1) + c_2 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_2)+bx_2)$$
$$+c_3 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_3)+bx_3) + c_4 Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_4)+bx_4) = 0$$

para toda $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, donde x_1, x_2, x_3 y x_4 son elementos distintos de $\mathbb{F}_{2^n}^*$. Entonces,

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(bx_1) + Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(bx_2) + Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(bx_3) + Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(bx_4) = 0$$

para toda $b \in \mathbb{F}_{2^n}$ y

$$Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_1)) + Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_2)) + Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_3))$$
$$+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x_4)) = 0$$

para toda $a \in \mathbb{F}_{2^n}$, por lo que,

$$bx_1 + bx_2 + bx_3 + bx_4 = 0$$

y

$$aF(x_1) + aF(x_2) + aF(x_3) + aF(x_4) = 0$$

para toda $(a,b) \in \mathbb{F}_{2^n}$. Nótese que las implicaciones anteriores son de hecho equivalencias. Eligiendo a y b distintos de cero, tenemos que

$$x_1 + x_2 + x_3 + x_4 = 0 \ \text{ y } \ F(x_1) + F(x_2) + F(x_3) + F(x_4) = 0 \qquad (*)$$

Por otro lado la ecuación $F(x+a) + F(x) = b$, puede verse como

$$x + y = a \ \text{ y } \ F(x) + F(y) = b,$$

si existiesen dos soluciones distintas de x, dos soluciones distintas de y y éstos a su vez distintas entre sí satisfaciendo esta relación, entonces la existencia de estas cuatro soluciones para algún $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ es equivalente a la existencia de cuatro soluciones satisfaciendo $(*)$. En el caso de funciones casi-bent sólo es posible dar dos soluciones a la ecuación $F(x) + F(x+a) = b$. De manera similar se procede si $d^\perp = 3$. Por lo tanto F es casi-bent sí y sólo si $d^\perp \geq 5$.

□

El siguiente resultado ([**8**]) es útil para la obtención de una cota para los pesos del código lineal de la Definición 1.1.

TEOREMA 1.4. *Sea* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *una función y* $\mathbb{F}_{2^h}$ *un subcampo de* $\mathbb{F}_{2^n}$. *Considérese*

$$(a_1, b_1), \ldots, (a_l, b_l) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$$

l pares ordenados linealmente independientes sobre $\mathbb{F}_{2^h}$. *Para los elementos* $u_1, \ldots, u_l \in \mathbb{F}_{2^h}$, *se define,*

$$\begin{aligned} & N(F; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) \\ := \quad & |\{x \in \mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) = u_i, i = 1, \ldots, l\}|. \end{aligned}$$

Si $l = 1$, *entonces:*

$$|N(F; a_1, b_1; u_1) - 2^{n-h}| \leq \left(1 - \frac{1}{2^h}\right)(2^n - 2N_F),$$

donde N_F *denota la no-linealidad de* F. *Si* $a_1, a_2, \ldots, a_l$ *son linealmente dependientes sobre* $\mathbb{F}_{2^h}$, *entonces para toda l,*

$$|N(F; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) - 2^{n-lh}| \leq \left(1 - \frac{1}{2^h}\right)(2^n - 2N_F).$$

DEMOSTRACIÓN. Sean $\chi(\cdot) := (-1)^{Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(\cdot)}$ el caracter aditivo canónico de $\mathbb{F}_{2^h}$ y $\psi(\cdot) := (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\cdot)}$ el caracter aditivo canónico de $\mathbb{F}_2^n$. Entonces,

$$
\begin{aligned}
& 2^{lh} N(F; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) \\
= & \sum_{x \in \mathbb{F}_{2^n}} \left[\sum_{y_1 \in \mathbb{F}_{2^h}} \chi(y_1(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_1 F(x) + b_1 x) - u_1)) \right] \cdots \\
\cdots & \left[\sum_{y_l \in \mathbb{F}_{2^h}} \chi(y_l(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_l F(x) + b_l x) - u_l)) \right] \\
= & \sum_{x \in \mathbb{F}_{2^n}} \sum_{y_1 \in \mathbb{F}_{2^h}} \cdots \sum_{y_l \in \mathbb{F}_{2^h}} \prod_{i=1}^{l} \chi\left(y_i(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) - u_i) \right) \\
= & \sum_{x \in \mathbb{F}_{2^n}} \sum_{y_1 \in \mathbb{F}_{2^h}} \cdots \sum_{y_l \in \mathbb{F}_{2^h}} \chi\left(\sum_{i=1}^{l} y_i(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) - u_i) \right) \\
= & 2^n + \sum_{\substack{y_1, \ldots, y_l \in \mathbb{F}_{2^h} \\ (y_1, \ldots, y_l) \neq (0, \ldots, 0)}} \\
& \sum_{x \in \mathbb{F}_{2^n}} \chi\left(\sum_{i=1}^{l} y_i(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) - u_i) \right) \\
= & 2^n + \sum_{\substack{y_1, \ldots, y_l \in \mathbb{F}_{2^h} \\ (y_1, \ldots, y_l) \neq (0, \ldots, 0)}} \\
& \sum_{x \in \mathbb{F}_{2^n}} \chi\left(\sum_{i=1}^{l} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(y_i a_i F(x) + b_i x) - y_i u_i \right) \\
= & 2^n + \sum_{\substack{y_1, \ldots, y_l \in \mathbb{F}_{2^h} \\ (y_1, \ldots, y_l) \neq (0, \ldots, 0)}} \\
& \sum_{x \in \mathbb{F}_{2^n}} \chi\left(\sum_{i=1}^{l} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(y_i a_i F(x) + b_i x) \right) \chi\left(\sum_{i=1}^{l} y_i u_i \right) \\
= & 2^n + \sum_{\substack{y_1, \ldots, y_l \in \mathbb{F}_{2^h} \\ (y_1, \ldots, y_l) \neq (0, \ldots, 0)}} \\
& \chi\left(\sum_{i=1}^{l} y_i u_i \right) \sum_{x \in \mathbb{F}_{2^n}} \chi\left(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}} \left(\sum_{i=1}^{l} (y_i a_i F(x) + b_i x) \right) \right)
\end{aligned}
$$

$$
\begin{aligned}
&= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \chi\left(\sum_{i=1}^{l} y_i u_i\right) \sum_{x\in\mathbb{F}_{2^n}} \psi\left(\sum_{i=1}^{l}(y_i a_i F(x) + b_i x)\right) \\
&= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \chi\left(\sum_{i=1}^{l} y_i u_i\right) \mu_{y_1a_1+\cdots+y_la_l, y_1b_1+\cdots+y_lb_l}(F), \\
&\quad \text{donde } \mu_{c,d} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(cF(x)+dx)}.
\end{aligned}
$$

Ahora fijemos $(y_1,\ldots,y_l) \neq (0,\ldots,0)$, si $y_1a_1 + \cdots + y_la_l = 0$. Entonces $y_1b_1 + \cdots + y_lb_l \neq 0$ pues $(a_1,b_1),\ldots,(a_l,b_l)$ son linealmente independientes sobre $\mathbb{F}_{2^h}$, luego,

$$\mu_{y_1a_1+\cdots+y_la_l, y_1b_1+\cdots+y_lb_l}(F) = 0.$$

Supóngase ahora que $y_1a_1 + \cdots + y_la_l \neq 0$. Como se sabe que la no-linealidad de una función vectorial está dada de la forma

$$N_F = 2^{n-1} - \frac{1}{2}\text{máx}_{\substack{a\in\mathbb{F}_{2^n}^* \\ b\in\mathbb{F}_{2^n}}} |\mu_F(a,b)|,$$

entonces,

$$\text{máx}_{\substack{a\in\mathbb{F}_{2^n}^* \\ b\in\mathbb{F}_{2^n}}} |\mu_F(a,b)| = 2^n - 2N_F,$$

luego, $|\mu_{y_1a_1+\cdots+y_la_l, y_1b_1+\cdots+y_lb_l}(F)| \leq 2^n - 2N_F$ por lo que,

$$
\begin{aligned}
&2^{lh}N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l) - 2^n \\
&= \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \chi\left(\sum_{i=1}^{l} y_i u_i\right) \mu_{y_1a_1+\cdots+y_la_l, y_1b_1+\cdots+y_lb_l}(F),
\end{aligned}
$$

lo cual implica que,

$$\begin{aligned}
& |2^{lh}N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l)-2^n| \\
\leq\ & \Big| \sum_{\substack{y_1,\ldots,y_l\in\mathbb{F}_{2^h}\\(y_1,\ldots,y_l)\neq(0,\ldots,0)}} \mu_{y_1a_1+\cdots+y_la_l,y_1b_1+\cdots+y_lb_l}(F)\Big| \\
\leq\ & \sum_{\substack{y_1,\ldots,y_l\in\mathbb{F}_{2^h}\\(y_1,\ldots,y_l)\neq(0,\ldots,0)}} 2^n-2N_F \\
=\ & (2^n-2N_F)|\{(y_1,\ldots,y_l)\in\mathbb{F}_{2^h}^l : y_1a_1+\cdots+y_la_l\neq 0\}| \\
\leq\ & (2^n-2N_F)(2^{lh}-2^{(l-1)h}),
\end{aligned}$$

por lo tanto,

$$|2^{lh}N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l)-2^n|\leq(2^n-2N_F)(2^{lh}-2^{(l-1)h}),$$

concluyendo que,

$$|N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l)-2^{n-lh}|\leq(1-\frac{1}{2^h})(2^n-2N_F),$$

y el resultado queda probado. □

En general, para cualquier función $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ se tiene la siguiente cota:

COROLARIO 1.5. *Sea $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ y $u_1,\ldots,u_{2^h-1}$, todos los elementos de $\mathbb{F}_{2^h}^*$. Entonces*

$$\begin{aligned}
& (2^h-1)\left(2^{n-h}-(1-\frac{1}{2^h})(2^n-2N_F)\right) \\
\leq\ & |\{x\in\mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx)\in\mathbb{F}_{2^h}^*\}| \\
\leq\ & (2^h-1)\left(2^{n-h}+(1-\frac{1}{2^h})(2^n-2N_F)\right).
\end{aligned}$$

DEMOSTRACIÓN. Sean

$$N_{u_i}=|\{x\in\mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx)=u_i\}|, i=1,\ldots,2^h-1.$$

Entonces
$\Big||\{x\in\mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx)\in\mathbb{F}_{2^h}^*\}|-(2^h-1)(2^{n-h})\Big|$
$=\Big|N_{u_1}-2^{n-h}+N_{u_2}-2^{n-h}+\cdots+N_{u_{2^h-1}}-2^{n-h}\Big|$
$\leq|N_{u_1}-2^{n-h}|+\cdots+|N_{u_{2^h-1}}-2^{n-h}|\leq(2^h-1)(1-\frac{1}{2^h})(2^n-2N_F)$, lo cual

implica que,

$$\begin{aligned} & (2^h-1)\left(2^{n-h}-(1-\frac{1}{2^h})(2^n-2N_F)\right) \\ \leq\ & |\{x\in\mathbb{F}_{2^n}: Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx)\in\mathbb{F}_{2^h}^*\}| \\ \leq\ & (2^h-1)\left(2^{n-h}+(1-\frac{1}{2^h})(2^n-2N_F)\right). \end{aligned}$$

□

En particular si $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ es una función casi-bent se tiene el siguiente resultado:

COROLARIO 1.6. *Si $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ es una función casi-bent y $u_1,\ldots,u_{2^h-1}$ todos los elementos de $\mathbb{F}_{2^h}^*$, entonces,*

$$\begin{aligned} & (2^h-1)\left(2^{n-h}-(1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right) \\ \leq\ & |\{x\in\mathbb{F}_{2^n}: Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx)\in\mathbb{F}_{2^h}^*\}| \\ \leq\ & (2^h-1)\left(2^{n-h}+(1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right). \end{aligned}$$

DEMOSTRACIÓN. Como F es casi-bent, $N_F=2^{n-1}-2^{\frac{n-1}{2}}$, sustituyendo en la desigualdad del Corolario 1.5 se prueba la afirmación. □

El siguiente resultado proporciona una cota para los pesos del código lineal de la Definición 1.1.

COROLARIO 1.7. *Sea $\mathcal{C}$ el código de la Definición 1.1 y w el peso de una palabra no cero de $\mathcal{C}$. Entonces,*

$$(2^h-1)\left(2^{n-h}-(1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right)\leq w\leq(2^h-1)\left(2^{n-h}+(1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right).$$

DEMOSTRACIÓN. La prueba se sigue del Corolario 1.6. □

Si se añade la condición $F(0)=0$ a la función $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, se obtiene una cota distinta de los pesos de las palabras no cero del código de la Definición 1.1.

COROLARIO 1.8. *Sea $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ una función tal que $F(0)=0$ y $u_1,\ldots,u_{2^h-1}$ todos los elementos de $\mathbb{F}_{2^h}^*$. Entonces,*

$$\begin{aligned} & \frac{2^h-1}{2^h}(2^n-(2^n-2N_F)) \\ \leq\ & |\{x\in\mathbb{F}_{2^n}^*: Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx)\in\mathbb{F}_{2^h}^*\}| \\ \leq\ & \frac{2^h-1}{2^h}(2^n+(2^n-2N_F)). \end{aligned}$$

DEMOSTRACIÓN. Si $(a,b) \neq (0,0)$, como $F(0)=0$, se del Teorema 1.4 se sigue que,

$$\begin{aligned} & 2^{n-h} - \frac{2^h-1}{2^h}(2^n - 2N_F) - 1 \\ \leq\ & |\{x \in \mathbb{F}_{2^n}^* : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) = 0\}| \\ \leq\ & 2^{n-h} + \frac{2^h-1}{2^h}(2^n - 2N_F) - 1, \end{aligned}$$

lo cual implica que,

$$\begin{aligned} & 2^n - 1 - \left(2^{n-h} - \frac{2^h-1}{2^h}(2^n - 2N_F) - 1\right) \\ \leq\ & |\{x \in \mathbb{F}_{2^n}^* : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) \in \mathbb{F}_{2^h}^*\}| \\ \leq\ & 2^n - 1 - \left(2^{n-h} + \frac{2^h-1}{2^h}(2^n - 2N_F) - 1\right), \end{aligned}$$

y por consiguiente,

$$\begin{aligned} & \frac{2^h-1}{2^h}(2^n - (2^n - 2N_F)) \\ \leq\ & |\{x \in \mathbb{F}_{2^n}^* : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) \in \mathbb{F}_{2^h}^*\}| \\ \leq\ & \frac{2^h-1}{2^h}(2^n + (2^n - 2N_F)), \end{aligned}$$

probando así la afirmación. □

COROLARIO 1.9. *Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent tal que $F(0)=0$ y $u_1, \ldots, u_{2^h-1}$ todos los elementos de $\mathbb{F}_{2^h}^*$. Entonces,*

$$\begin{aligned} & \frac{2^h-1}{2^h}(2^n - 2^{\frac{n+1}{2}}) \\ \leq\ & |\{x \in \mathbb{F}_{2^n}^* : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) \in \mathbb{F}_{2^h}^*\}| \\ \leq\ & \frac{2^h-1}{2^h}(2^n + 2^{\frac{n+1}{2}}). \end{aligned}$$

DEMOSTRACIÓN. La afirmación se sigue del Corolario 1.8. □

En la Definición 1.1 se considera a $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent. Con respecto a este código lineal determinado por esta función se tiene el siguiente resultado:

COROLARIO 1.10. *Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent tal que $F(0) = 0$ y $\mathcal{C}$ el código lineal determinado por esta función (ver Definición 1.1). Entonces el peso w de cualquier palabra no-cero de $\mathcal{C}$ es tal que:*

$$\frac{2^h-1}{2^h}(2^n - 2^{\frac{n+1}{2}}) \leq w \leq \frac{2^h-1}{2^h}(2^n + 2^{\frac{n+1}{2}}).$$

DEMOSTRACIÓN. La prueba se sigue del Corolario 1.9. □

De este modo, con respecto al código lineal de la Definición 1.1 se han determinado la longitud, dimensión, una cota para los pesos de las palabras no cero, y una cota para el peso mínimo del código dual.

Construcción $n = hr$, $h = 1$.

A continuación se dará la definición de un código lineal cuando el divisor h de n es igual a 1, es decir, cuando el contradominio de la función traza es $\mathbb{F}_2$, en este caso, es posible conocer un poco más de la estructura de este código a comparación del código definido anteriormente pues es posible hallar la distribución de pesos de este código lineal.

DEFINICIÓN 1.11. *Sea n impar y $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ una función casi-bent. Para $a, b \in \mathbb{F}_{2^n}$ sea*

$$F_{a,b}(x) := aF(x) + bx,$$
$$C_{a,b} := (Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(F_{a,b}(\gamma))_{\gamma \in \mathbb{F}_{2^n}^*})$$

y

$$\mathcal{C} := \{C_{a,b} : a, b \in \mathbb{F}_{2^n}\} \subseteq \mathbb{F}_2^{2^n-1}.$$

Es fácil ver que $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_2$. A continuación se determina la dimensión de este código:

TEOREMA 1.12. *La dimensión del código lineal $\mathcal{C}$ de la Definición 1.11 es 2n y una base está dada por el conjunto,*

$$A = \{C_{1,0}, C_{\alpha,0}, \ldots, C_{\alpha^{n-1},0}, C_{0,1}, C_{0,\alpha}, \ldots C_{0,\alpha^{n-1}}\},$$

donde α es un elemento primitivo de $\mathbb{F}_{2^n}$.

DEMOSTRACIÓN. La prueba es similar a la del Teorema 1.2, pues es un caso particular de ese resultado. □

Estamos interesados en saber la distribución de pesos de este código lineal, la cual proporciona entre otras cosas el peso mínimo del código. Entre las herramientas para conocer la distribución de pesos se tiene el siguiente resultado con respecto al código dual y las relaciones de Pless ([**30**]).

TEOREMA 1.13. *([**7**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Entonces $\mathcal{C}^\perp$ tiene peso mínimo mayor o igual que 5.*

DEMOSTRACIÓN. Se sigue del Teorema 1.3 cuando $h = 1$. □

TEOREMA 1.14. *Los distintos pesos del código lineal $\mathcal{C}$ de la Definición 1.11 están dados por*

$$2^{n-1} - 2^{\frac{n-1}{2}},\ 2^{n-1} + 2^{\frac{n-1}{2}} \text{ o, } 2^{n-1}.$$

DEMOSTRACIÓN. Si $\lambda_F(b,a) = \widehat{\zeta_{a\cdot F}}(b) = 2^{\frac{n+1}{2}}$, definimos

$$A = |\{x : Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(aF(x) + bx) = 1\}|,$$
$$B = |\{x : Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(aF(x) + bx = 0)\}|.$$

Entonces,

$$B - A = \lambda_F(b,a) = 2^{\frac{n+1}{2}},$$

lo cual implica que,

$$A = B - 2^{\frac{n+1}{2}} = 2^n - A - 2^{\frac{n+1}{2}},$$

y por consiguiente,

$$A = \frac{2^n - 2^{\frac{n+1}{2}}}{2} = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Si $\lambda_F(b,a) = -2^{\frac{n+1}{2}}$,

$$B - A = \widehat{\chi}_{bF}(a) = -2^{\frac{n+1}{2}}$$

lo cual implica que,

$$A = B + 2^{\frac{n+1}{2}} = 2^n - A + 2^{\frac{n+1}{2}},$$

y en consecuencia,

$$A = \frac{2^n + 2^{\frac{n+1}{2}}}{2} = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

Si $\lambda_F(a,b) = 0$, entonces $B - A = 0$ por lo que $B = A$. Entonces $A = 2^{n-1}$ y de aquí se tiene el resultado. □

En base a los resultados anteriores es posible obtener la distribución de pesos del código lineal de la Definición 1.11.

TEOREMA 1.15. *El código $\mathcal{C}$ de la Definición 1.11, tiene las características de un $[2^n - 1, 2n, 2^{n-1} - 2^{\frac{n-1}{2}}]$ código lineal binario, donde todo $A_i = 0$ (A_i es el número de palabras de peso i del código $\mathcal{C}$), excepto,*

$A_0 = 1$,
$A_{2^{n-1}-2^{\frac{n-1}{2}}} = (2^n - 1)(2^{n-2} + 2^{\frac{n-3}{2}})$,
$A_{2^{n-1}} = (2^n - 1)(2^{n-1} + 1)$,
$A_{2^{n-1}+2^{\frac{n-1}{2}}} = (2^n - 1)(2^{n-2} - 2^{\frac{n-3}{2}})$.

DEMOSTRACIÓN. En particular del Teorema 1.9 se tiene que,

1. $\sum_{j=0}^{n} A_j = 2^k$
2. $\sum_{j=0}^{n} jA_j = 2^{k-1}(n - B_1)$
3. $\sum_{j=0}^{n} j^2 A_j = 2^{k-2}n(n+1) - 2^{k-1}nB_1 + 2^{k-1}B_2$,

donde B_1 y B_2 son el número de palabras de peso 1 y 2 respectivamente del código dual $\mathcal{C}^{\perp}$. Si $a = 2^{n-1}$, $b = 2^{n-1} - 2^{\frac{n-1}{2}}$ y $c = 2^{n-1} + 2^{\frac{n-1}{2}}$, por el Teorema 1.14 y el Teorema 1.13 se tiene que,

$A_a + A_b + A_c = 2^{2n} - 1$,

$$2^{n-1}A_a + (2^{n-1} - 2^{\frac{n-1}{2}})A_b + (2^{n-1} + 2^{\frac{n-1}{2}})A_c = 2^{2n-1}(2^n - 1)$$
$$(2^{n-1})^2 A_a + (2^{n-1} - 2^{\frac{n-1}{2}})^2 A_b + (2^{n-1} + 2^{\frac{n-1}{2}})^2 A_c = 2^{3n-2}(2^n - 1).$$

Resolviendo el sistema se sigue el resultado deseado. □

En general se tiene el siguiente resultado, el cual puede ser encontrado en la referencia [**11**]:

TEOREMA 1.16. *Sea $\mathcal{D}$ un $[2^n - 1, 2n, d]$ un código lineal binario tal que $\mathbf{1} = (1, \ldots, 1) \notin \mathcal{D}$. Sea $d^\perp \geq 3$ y w_0 el mas pequeño w tal que $0 < w < 2^{n-1}$ y*

$$A_w + A_{2^n - w} \neq 0.$$

Entonces,

$$w_0 \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

y la igualdad se da sí y sólo si el peso de toda palabra de $\mathcal{D}$ pertenece a

$$\{0, 2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}}\}.$$

□

Nótese que en particular para el código que nos interesa $\mathcal{C}$ se tiene que $w_0 = 2^{n-1} - 2^{\frac{n-1}{2}}$, ya que $A_w + A_{2^n-w} = 0$ cuando $w < 2^{n-1} - 2^{\frac{n-1}{2}}$ y que $2^{n-1} - 2^{\frac{n-1}{2}}$ es el menor entero con esta propiedad en este código lineal.

2. Esquemas de compartición de secretos basados en funciones casi-bent

Utilizando el método descrito por Massey se ha dado la construcción de esquemas de compartición de secretos utilizando funciones bent. En esta sección se presentan resultados similares en el caso de característica 2 utilizando las funciones casi-bent. Una vez construidos los códigos lineales en base a funciones casi-bent en la sección anterior, ya se pueden utilizar para la construcción de esquemas de compartición de secretos.

Veamos que en el código lineal de la Definición 1.1 todas las palabras son mínimas:

TEOREMA 2.1. *Sea $\mathcal{C}$ el código lineal de la Definición 1.1. Si $n \geq 5h$, $h \geq 3$, entonces toda palabra de $\mathcal{C}$ es mínima.*

DEMOSTRACIÓN. Del Corolario 1.7 se sigue que,

$$\frac{w_{\text{mín}}}{w_{\text{máx}}} \geq \frac{(2^h - 1)\left(2^{n-h} - (1 - \frac{1}{2^h})2^{\frac{n+1}{2}}\right)}{(2^h - 1)\left(2^{n-h} + (1 - \frac{1}{2^h})2^{\frac{n+1}{2}}\right)} = \frac{2^{n-h} - \frac{2^h - 1}{2^h}(2^{\frac{n+1}{2}})}{2^{n-h} + \frac{2^h - 1}{2^h}(2^{\frac{n+1}{2}})}$$

$$= \frac{2^n - (2^h - 1)(2^{\frac{n+1}{2}})}{2^n + (2^h - 1)(2^{\frac{n+1}{2}})} = \frac{2^{\frac{n-1}{2}} - (2^h - 1)}{2^{\frac{n-1}{2}} + (2^h - 1)}.$$

Si $n \geq 5h$, $h \geq 3$,

$$2^{2h+1} = 2^{2h}2 = (2^{4h}2^2)^{1/2} = (\frac{2^{4h}2^3}{2})^{1/2} \leq (\frac{2^{4h}2^h}{2})^{1/2} = (\frac{2^{5h}}{2})^{1/2}$$
$$= (2^{5h-1})^{1/2} = 2^{\frac{5h-1}{2}},$$

lo cual implica que,

$$2^{2h+1} - 32^h + 1 < 2^{\frac{5h-1}{2}} = 2^{\frac{n-1}{2}},$$

es decir,

$$2^{2h+1} - 32^h + 1 < 2^{\frac{n-1}{2}},$$

por lo que,

$$-22^{2h} + 22^h + 2^h + 2^{\frac{n-1}{2}} - 1 > 0,$$

y de aquí,

$$-2^h2^h - 2^h2^h + 2^h + 2^h + 2^h + 2^{\frac{n-1}{2}} - 1 > 0.$$

Por consiguiente,

$$2^h2^{\frac{n-1}{2}} - 2^h2^h + 2^h > 2^h2^{\frac{n-1}{2}} + 2^h2^h - 2^h - 2^{\frac{n-1}{2}} - 2^h + 1,$$

luego,

$$2^h\left(2^{\frac{n-1}{2}} - 2^h + 1\right) > (2^h - 1)\left(2^{\frac{n-1}{2}} + 2^h - 1\right),$$

entonces,

$$\frac{2^{\frac{n-1}{2}} - (2^h - 1)}{2^{\frac{n-1}{2}} + (2^h - 1)} > \frac{2^h - 1}{2^h}.$$

Por lo tanto,

$$\frac{w_{\text{mín}}}{w_{\text{máx}}} > \frac{2^h - 1}{2^h},$$

y el resultado se sigue del Teorema 3.5 del Capítulo 4.

Nótese que si $n = 3h$, entonces

$$2^{2h+1} - 32^h + 1 = 2^{h+1}2^h - 32^h + 1 = 2^h(2^{h+1} - 3) + 1$$
$$= 2^h(2^h + 2^h - 3) > 2^h2^h > 2^{\frac{h-1}{2}}2^h = 2^{\frac{3h-1}{2}} = 2^{\frac{n-1}{2}},$$

lo cual implicaría que,

$$\frac{2^{\frac{n-1}{2}} - (2^h - 1)}{2^{\frac{n-1}{2}} + (2^h - 1)} < \frac{2^h - 1}{2^h}.$$

Por lo que no se podría deducir la desigualdad entre $\frac{w_{\text{mín}}}{w_{\text{máx}}}$ y $\frac{2^h-1}{2^h}$. □

Con respecto a la función casi-bent $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ del código lineal de la Definición 1.1 se tiene el siguiente resultado:

TEOREMA 2.2. *Sea $\mathcal{C}$ el código lineal de la Definición 1.1 tal que $F(0) = 0$. Si $n \geq 3h$, $h \geq 3$, entonces toda palabra no cero del código es mínima.*

DEMOSTRACIÓN. Utilizando el Corolario 1.10,

$$\frac{w_{\text{mín}}}{w_{\text{máx}}} \geq \frac{\frac{2^h-1}{2^h}(2^n - 2^{\frac{n+1}{2}})}{\frac{2^h-1}{2^h}(2^n + 2^{\frac{n+1}{2}})} = \frac{2^{\frac{n+1}{2}}(2^{\frac{n-1}{2}} - 1)}{2^{\frac{n+1}{2}}(2^{\frac{n-1}{2}} + 1)} = \frac{2^{\frac{n-1}{2}} - 1}{2^{\frac{n-1}{2}} + 1}.$$

Si $n \geq 3h$, $h \geq 3$,

$$2^{h+1} = 2^h 2 = (2^{2h}2^2)^{1/2} = (\frac{2^{2h}2^3}{2})^{1/2} \leq (\frac{2^{2h}2^h}{2})^{1/2} = (\frac{2^{3h}}{2})^{1/2}$$
$$= 2^{\frac{3h-1}{2}} \leq 2^{\frac{n-1}{2}},$$

luego,

$$2^{h+1} - 1 < 2^{\frac{n-1}{2}},$$

por lo que,

$$2^h 2^{\frac{n-1}{2}} - 2^h > 2^h 2^{\frac{n-1}{2}} + 2^h - 2^{\frac{n-1}{2}} - 1,$$

lo cual implica que,

$$2^h \left(2^{\frac{n-1}{2}} - 1\right) > (2^h - 1)\left(2^{\frac{n-1}{2}} + 1\right),$$

y por consiguiente,

$$\frac{2^{\frac{n-1}{2}} - 1}{2^{\frac{n-1}{2}} + 1} > \frac{2^h - 1}{2^h}.$$

Por lo tanto,

$$\frac{w_{\text{mín}}}{w_{\text{máx}}} > \frac{2^h - 1}{2^h}.$$

El resultado se sigue del Teorema 3.5 del Capítulo 4. □

TEOREMA 2.3. *Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Si $n > 3$, entonces toda palabra no cero de $\mathcal{C}$ es una palabra mínima.*

DEMOSTRACIÓN. Por el Teorema 1.14,

$$w_{\text{mín}} = 2^{n-1} - 2^{\frac{n-1}{2}} \text{ y } w_{\text{máx}} = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

Si $n > 3$, entonces,

$$2^{\frac{n+1}{2}} - 3 > 0,$$

lo cual implica que,

$$2 \times 2^{\frac{n+1}{2}} - 2 > 2^{\frac{n-1}{2}} + 1.$$

Por lo tanto,

$$\frac{2^{n-1} - 2^{\frac{n-1}{2}}}{2^{n-1} + 2^{\frac{n-1}{2}}} > \frac{1}{2}.$$

El resultado se sigue del Teorema 3.5 del Capítulo 4. □

Obsérvese que si $n = 1$, entonces la desigualdad del resultado anterior no es cierta.

Ahora se puede dar un esquema de compartición de secretos análogo al descrito en [**6**] ($p \neq 2$) con la función casi-bent $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ utilizada en la Definición 1.1:

TEOREMA 2.4. *Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Si $n \geq 5h$, $h \geq 3$, o $F(0) = 0$ con la condición $n \geq 3h$, $h \geq 3$, entonces en el esquema de compartición de secretos basado en $\mathcal{C}^{\perp}$ se tiene que:*

- *Hay en total 2^{2n-h} conjuntos de acceso mínimo.*
- *Para cualquier t fija tal que $1 \leq t \leq$ mín$\{2n/h - 1, d^{\perp} - 2\}$, todo grupo de t participantes está incluido en*

$$(2^h - 1)^t \left(2^h\right)^{2n/h-(t+1)}$$

conjuntos de acceso mínimo.

DEMOSTRACIÓN. La prueba se sigue del Teorema 2.1, Teorema 2.2, Teorema 3.4 del Capítulo 4, y utilizando el hecho de que $d^{\perp} > 2$. □

TEOREMA 2.5. *Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Si $n > 3$, entonces en el esquema de compartición de secretos basado en $\mathcal{C}^{\perp}$ se tiene que:*

- *Existen un total de 2^{2n-1} conjuntos de acceso mínimo.*
- *Para cualquier t fija tal que $1 \leq t \leq$ mín$\{2n - 1, d^{\perp} - 2\}$, todo grupo de t participantes está incluido en $2^{2n-(t+1)}$ conjuntos de acceso mínimo.*

DEMOSTRACIÓN. La afirmación se sigue del Teorema 2.3 y el Teorema 3.4 del Capítulo 4. □

3. Extensiones de esquemas de compartición de secretos

En esta sección utilizando el esquema de compartición basado en $\mathcal{C}^{\perp}$ donde $\mathcal{C}$ es el código lineal de la Definición 1.11 se dan dos diferentes extensiones cuyo nuevo espacio de secretos es $\mathbb{F}_2^l$, para l suficientemente grande.

3.1. Extensión 1. Ya que en el esquema de compartición de secretos basado en el código lineal $\mathcal{C}^{\perp}$, donde $\mathcal{C}$ es el código lineal de la Definición 1.11, el espacio de secretos tiene cardinalidad pequeña, ya que el secreto solo puede ser el 0 o el 1, consideramos entonces una extensión de este esquema de compartición de secretos, cuyo nuevo espacio de secretos es $\mathbb{F}_2^l$, donde l es suficientemente grande.

La extensión se describe de la siguiente manera:

- Un secreto en el esquema extendido es un elemento de la forma

$$s = (s_1, s_2, \ldots, s_l),$$

donde $s_j \in \mathbb{F}_2$.

- El secreto $(s_1, s_2, \ldots, s_l)$ en el esquema extendido será recuperado obteniendo cada s_j uno por uno, utilizando el esquema de compartición de secretos descrito anteriormente.

- En el esquema de compartición de secretos descrito anteriormente, para cada s_j, se le asigna la acción $t_{i,j}$ al participante P_i, donde $i = 1, \ldots, n-1$.

- En el esquema de compartición de secretos extendido, para el secreto $(s_1, s_2, \ldots, s_l)$ al participante P_i se le asigna la acción $(t_{i,1}, t_{i,2}, \ldots, t_{i,l})$.

3.2. Extensión 2. También se puede construir un esquema de compartición de secretos extendido, considerando distintos esquemas de compartición de secretos basados en los duales de códigos lineales construidos a partir de funciones casi-bent.

- Si $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ es una función definida por $F(x) = x^{2^r+1}$ tal que $(r, n) = 1$, $1 \leq r \leq t$, donde $n = 2t + 1$, entonces F es casi-bent.
- Sean
$$F_{a,b}^{r_j}(x) = ax^{2^{r_j}+1} + bx, \quad a, b \in \mathbb{F}_{2^n},$$
$j = 1, 2, \ldots, l$, con las r_j distintas y
$$C_{a,b}^{r_j} = (Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(F_{a,b}^{r_j}(\gamma))_{\gamma \in \mathbb{F}_{2^n}^*}).$$
Entonces se construyen los códigos
$$\mathcal{C}^{r_j} = \{C_{a,b}^{r_j} : a, b \in \mathbb{F}_{2^n}\} \subseteq \mathbb{F}_2^{2^n-1}.$$
- En el esquema extendido, para cada secreto $(s_1, s_2, \ldots, s_l)$ al participante $P_i, i = 1, \ldots, n-1$ se le asigna la acción $(t_{i,1}, t_{i,2}, \ldots, t_{i,l})$, donde $t_{i,j}$ es obtenido considerando el esquema de compartición de secretos basado en $\mathcal{C}^{r_j \perp}$.

Para los esquemas de compartición de secretos, los campos más pequeños que se deben considerar son $\mathbb{F}_{2^3}$ y $\mathbb{F}_{2^{15}}$. Esto es por la condición $h \geq 3$ y $n \geq 5h$ al consinderar $\mathbb{F}_{2^h}$ y $\mathbb{F}_{2^n}$, el cual no asegura que todas las palabras del código son palabras mínimas. Un programa computacional es muy tardado para ejemplificar lo anterior, y los vectores que se obtienen son demasiado grandes para escribirse en este trabajo.

Capítulo 6

Esquemas de autenticación

Un esquema de autenticación provee un método de asegurar la integridad de la información al ser enviada a través de un canal público. Un transmisor y un receptor comparten una llave secreta, la cual permite al receptor, corroborar que el mensaje recibido es auténtico. Un esquema de autenticación (sin secreto) es una cuadrupla:

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E} = \{E_k : k \in \mathcal{K}\}),$$

donde $\mathcal{S}$ es el espacio fuente, $\mathcal{T}$ el espacio de etiquetado, $\mathcal{K}$ el espacio de llaves y $E_k : \mathcal{S} \to \mathcal{T}$ es una regla de codificación. Los conjuntos $\mathcal{S}$, $\mathcal{T}$ y $\mathcal{K}$ se suponen finitos y no vacíos.

Tanto transmisor como receptor comparten una llave secreta $k \in \mathcal{K}$. El transmisor desea enviar una pieza de información (llamada fuente) $s \in \mathcal{S}$ al receptor, el transmisor calcula $t = E_k(s) \in \mathcal{T}$ e inserta al canal público el mensaje m que consiste del par ordenado (s, t). El receptor al recibir $m' = (s', t')$, calcula $E_k(s')$ y verifica si $E_k(s') = t'$, si es así, el receptor acepta el mensaje como auténtico, en otro caso el mensaje es rechazado. Como el canal de comunicación es público hay riesgo de que un enemigo pueda deliberadamente observar, y más aún causar un disturbio en la comunicación. Se asume que el enemigo puede insertar un mensaje en el canal o substituir el mensaje observado m con otro mensaje m'. Por consiguiente, se consideran dos tipos de ataque: el ataque por imitación y el ataque por substitución. En el ataque por imitación el enemigo deliberadamente elige un mensaje y lo inserta en el canal esperando que el receptor lo acepte como auténtico. Utilizamos P_I para denotar la máxima probabilidad de que este ataque ocurra. En el ataque por substitución el enemigo observa un mensaje $m = (s, t)$ y lo reemplaza con un mensaje $m' = (s', t')$ donde $s \neq s'$, esperando que el receptor acepte el nuevo mensaje como auténtico. El símbolo P_S es utilizado para denotar la máxima probabilidad de que este ataque ocurra. En este trabajo se asume que todos los elementos del espacio fuente y del espacio llave son igualmente probables a ser elegidos. Para mayor información con respecto a los esquemas de autenticación puede consultarse en [**36**].

Sea H una función que asocia cada llave a la regla de codificación que se genera a partir de esta llave. Si $H : k \to E_k$, $k \in \mathcal{K}$ es uno a uno, entonces las reglas de codificación serán igualmente probables.

Ya que las llaves y los elementos del espacio fuente son equiprobables, entonces ([**18**]):

$$P_I = \max_{s \in \mathcal{S}, t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : E_k(s) = t\}|}{|\mathcal{K}|}.$$

Como en el ataque por substitución el oponente observa el mensaje dado por $m = (s,t)$, y lo reemplaza con otro mensaje $m' = (s',t')$, en donde $s \neq s'$, y ya que las llaves y los elementos del espacio fuente son igualmente probables, entonces ([**18**]):

$$P_S = \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|}.$$

El enemigo intentará elegir mensajes que aumenten la probabilidad de tener éxito en el fraude. Por lo tanto el esquema de autenticación debe ser diseñado de tal forma que las probabilidades de fraude sean lo más pequeño posible.

Se tienen las siguientes cotas generales para P_I y P_S ([**18**]):

$$P_I \geq \frac{1}{|\mathcal{T}|} \text{ y } P_S \geq \frac{1}{|\mathcal{T}|},$$

ya que $|\mathcal{T}|P_I \geq \sum_{t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : E_k(s) = t\}|}{|\mathcal{K}|} = 1$. En forma análoga para P_S. Por lo tanto el objetivo es tener P_I y P_S lo más cercano posible a

$$\frac{1}{|\mathcal{T}|}.$$

A continuación un ejemplo de un esquema de autenticación el cual puede consultarse en [**36**]:

$$\begin{aligned} \mathcal{S} &= \mathbb{Z}_3 \\ \mathcal{T} &= \mathbb{Z}_3, \\ \mathcal{K} &= \mathbb{Z}_3 \times \mathbb{Z}_3, \\ \mathcal{E} &= \{e_k : k \in \mathcal{K}\}, \end{aligned}$$

y $e_{ij}(s) = is + j$ mód 3.

Supóngase que la llave es elegida aleatoriamente. Se tiene la siguiente tabla, la cual proporciona todos los valores $e_{ij}(s)$. Las llaves determinan los renglones y los elementos del espacio fuente las columnas.

llave	0	1	2
$(0,0)$	0	0	0
$(0,1)$	1	1	1
$(0,2)$	2	2	2
$(1,0)$	0	1	2
$(1,1)$	1	2	0
$(1,2)$	2	0	1
$(2,0)$	0	2	1
$(2,1)$	1	0	2
$(2,2)$	2	1	0

.

Considérese un ataque por imitación:

Sea K_0 la llave elegida por el transmisor y el receptor. Para cualquier pareja (s,t) que el enemigo inserte en el canal, se tiene que $P_I = \frac{3}{9} = \frac{1}{3}$, como nos muestra la tabla, pues siempre existen tres elementos de $\mathcal{K}$ tal que $e_{ij}(s) = t$.

Analicemos el ataque por substitución:
Supóngase que el enemigo observa el mensaje $(0,0)$ en el canal. Esto le proporciona información acerca de la llave. Él sabe que

$$k_0 \in \{(0,0),(1,0),(2,0)\}.$$

Supóngase que el enemigo reemplaza el mensaje $(0,0)$ con el mensaje $(1,1)$. El enemigo llevará a cabo el fraude si elige la llave $k_0 = (1,0)$. Luego $P_S = \frac{1}{3}$. En general la observación del mensaje (s,t) restringe la llave a una de tres posibilidades. O sea, para cada elección (s',t') del enemigo, siempre hay una única llave de las tres posibles que autentifica el mensaje.

En el resto del capítulo se da la construcción de esquemas de autenticación, una utilizando funciones bent y otra utilizando funciones casi-bent. En estos esquemas las reglas de codificación están dadas en términos de funciones bent y casi-bent respectivamente.

1. Construcciones basadas en funciones bent

A continuación se presentan dos construcciones de esquemas de autenticación basadas en funciones bent([**18**]).

1.1. Construcción 1.

Como una primera construcción tenemos:

DEFINICIÓN 1.1. *Sea $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ una función bent, donde q es la potencia de un primo impar. Se define un esquema de autenticación $(\mathcal{S},\mathcal{T},\mathcal{K},\mathcal{E} = \{E_k :$*

$k \in \mathcal{K}\}$), *donde,*

$$\begin{aligned}\mathcal{S} &= \mathbb{F}_{q^n} \times \mathbb{F}_{q^n},\\ \mathcal{T} &= \mathbb{F}_q,\\ \mathcal{K} &= \mathbb{F}_{q^n} \times \mathbb{F}_q,\\ \mathcal{E} &= \{E_k : k \in \mathcal{K}\},\end{aligned}$$

y

$$E_k(s) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2,$$

$k = (k_1, k_2) \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

En el siguiente resultado se obtiene $|\mathcal{K}| = |\mathcal{E}|$.

TEOREMA 1.2. *(*[**18**]*) La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección.*

DEMOSTRACIÓN. Veamos la inyectividad. Supóngase que $E_k = E_{k'}$, donde $k = (k_1, k_2), k' = (k_1', k_2') \in \mathbb{F}_{q^n} \times \mathbb{F}_q$.

Como $E_k(s) = E_{k'}(s)\ \forall s = (a, b) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, si $s = (0, 0)$ entonces,

$$\begin{aligned}k_2 &= Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(0F(k_1) + 0k_1) + k_2 = E_k(0, 0) = E_{k'}(0, 0)\\ &= Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(0F(k_1') + 0k_1') + k_2' = k_2',\end{aligned}$$

lo cual implica que,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2 = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1') + bk_1') + k_2,$$

por lo tanto,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a(F(k_1) - F(k_1')) + b(k_1 - k_1')) = 0,\ \forall s = (a, b) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}.$$

Si $a = 0$,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b(k_1 - k_1')) = 0, \forall b \in \mathbb{F}_{q^n},$$

así,

$$k_1 = k_1',$$

por lo que,

$$k = (k_1, k_2) = (k_1', k_2') = k'.$$

□

En el siguiente resultado se dan aproximaciones de P_I y P_S :

TEOREMA 1.3. *(*[**18**]*) Para el esquema de autenticación definido anteriormente,*

$$P_I = \frac{1}{q},\ P_S \leq \frac{1}{q} + \frac{q-1}{q^{(n+2)/2}}.$$

Más aún, $|\mathcal{S}| = q^{2n}, |\mathcal{T}| = q, |\mathcal{K}| = |\mathcal{E}| = q^{n+1}$.

DEMOSTRACIÓN. Sean $k = (k_1, k_2)$, $s = (a, b)$, $s' = (a', b')$.

$$P_I = \text{máx}_{s\in\mathcal{S},t\in\mathcal{T}} \frac{|\{k = (k_1, k_2) \in \mathcal{K} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2 = t\}|}{|\mathcal{K}|}.$$

Si $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) = r \in \mathbb{F}_q$, entonces,

$$\exists\,!\, r' \;\; Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + r' - r = t,$$

por lo que,

$$\exists\,!\, k_2 \;\; Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2 = t,$$

y de aquí,

$$|\{k \in \mathcal{K} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_{q^h}}(aF(k_1) + bk_1) + k_2 = t\}| = q^n.$$

No es difícil ver que $|\mathcal{K}| = q^{n+1}$, luego,

$$P_I = \frac{q^n}{q^{n+1}} = \frac{1}{q}.$$

Por otro lado,

$$P_S = \begin{array}{c} \text{máx} \\ s \in \mathcal{S} \\ t \in \mathcal{T} \end{array} \begin{array}{c} \text{máx} \\ s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T} \end{array} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|}.$$

Analizando el numerador:

$$\begin{aligned} & M = \{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\} \\ = & \left\{k \in \mathcal{K} : \begin{array}{c} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2 = t \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a'F(k_1) + b'k_1) + k_2 = t' \end{array}\right\} \\ = & \left\{k \in \mathcal{K} : \begin{array}{c} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2 = t \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left[(a - a')F(k_1) + (b - b')k_1\right] = t - t' \end{array}\right\}, \end{aligned}$$

por consiguiente,

$$\begin{aligned} & \left|\left\{k \in \mathcal{K} : \begin{array}{c} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2 = t \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left[(a - a')F(k_1) + (b - b')k_1\right] = t - t' \end{array}\right\}\right| \\ = & \left|\left\{k_1 \in \mathbb{F}_{q^n} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left[(a - a')F(k_1) + (b - b')k_1\right] = t - t'\right\}\right|, \end{aligned}$$

ya que si se tiene que

$$k_1 \in \left\{k_1 \in \mathbb{F}_{q^n} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left[(a - a')F(k_1) + (b - b')k_1\right] = t - t'\right\}$$

entonces,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left[(a - a')F(k_1) + (b - b')k_1\right] = t - t',$$

lo cual implica que,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) - Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a'F(k_1) + b'k_1) + t' = t.$$

Para k_1, existe una única k_2 tal que

$$-Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a'F(k_1) + b'k_1) + t' = k_2,$$

o sea, dada k_1 existe una única k_2 tal que

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1)+bk_1)+k_2=t.$$

Luego,

$$|M|=\left|\left\{k_1\in\mathbb{F}_{q^n}: Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left[(a-a')F(k_1)+(b-b')k_1\right]=t-t'\right\}\right|.$$

Y por el Teorema 1.2 del Capítulo 4 se sigue que,

$$M\leq q^{n-1}+(q-1)\,q^{n/2-1}.$$

Por lo tanto,

$$P_S\leq\frac{q^{n-1}+(q-1)\,q^{n/2-1}}{q^n}=\frac{1}{q}+\frac{q-1}{q^{(n+2)/2}}.$$

□

En el esquema anterior, P_I y su cota coinciden. Para obtener P_I pequeños, basta considerar valores grandes de q, de este modo se tendrá un buen esquema de autenticación con respecto a P_I. Para obtener un valor pequeño de P_S necesitamos números grandes de q^n y de q (notación anterior) y mejor aún si la diferencia entre q^n y q es grande.

Se tiene el siguiente ejemplo: Considérese $\mathbb{F}_{3^2}$, $\mathbb{F}_3$ y la función bent $F(x)=x^2$. Utilizando el esquema anterior se tiene entonces que $P_I=1/3$ y $P_S\leq 5/9$ (con la fórmula de las cotas). Por medio de un programa computacional se tiene que efectivamente $P_I=9/27=1/3$. Este resultado se puede obtener considerando cualquier pareja $(a,b)\in\mathbb{F}_{3^2}\times\mathbb{F}_{3^2}$, y cualquier elemento de $\mathbb{F}_3$, pues cualquier elemento del campo $\mathbb{F}_3$ se obtiene 9 veces, por ejemplo,

$$\begin{aligned}&|\{(k_1,k_2)\in\mathbb{F}_{3^2}: E_k(\alpha,\alpha+2)=1\}|\\ =\;&|\{(k_1,k_2): Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha F(k_1)+(\alpha+2)k_1)+k_2=1\}|=9,\end{aligned}$$

en donde α es un elemento primitivo de $\mathbb{F}_{3^2}$. También se obtiene que

$$|\{(k_1,k_2)\in\mathbb{F}_{3^2}: E_{(k_1,k_2)}(2,2\alpha+2)=0,\ E_{(k_1,k_2)}(\alpha+1,2\alpha+2)=0\}|=5.$$

Por lo que $P_S=5/9$. En este caso las cotas resultaron ser igual a P_I y P_S respectivamente. Que en este ejemplo P_S alcanze su cota, no es bueno, ya que en el esquema se desea encontrar valores pequeños de P_S.

1.2. Construcción 2**.** Se define un esquema de autenticación basado en funciones bent ([**18**]), como sigue:

DEFINICIÓN 1.4. *Sea $F:\mathbb{F}_{q^n}\to\mathbb{F}_{q^n}$ una función bent, donde q es la potencia de un primo impar. Se define un esquema de autenticación $(\mathcal{S},\mathcal{T},\mathcal{K},\mathcal{E}=\{E_k: k\in\mathcal{K}\})$, donde,*

$$\begin{aligned}&\mathcal{S}=\{\{1\}\times\mathbb{F}_{q^n}\}\cup\{(0,1)\}\subseteq\mathbb{F}_{q^n}\times\mathbb{F}_{q^n},\\ &\mathcal{T}=\mathbb{F}_q,\\ &\mathcal{K}=\mathbb{F}_{q^n},\\ &\mathcal{E}=\{E_k: k\in\mathcal{K}\},\end{aligned}$$

y

$$E_k(s) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k) + bk),$$

$k \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

El siguiente resultado ([**18**]) se obtiene $|\mathcal{K}| = |\mathcal{E}|$.

TEOREMA 1.5. *La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección.*

DEMOSTRACIÓN. Supóngase que $E_k = E_{k'}$, $k, k' \in \mathbb{F}_{q^n}$. Veamos que $k = k'$:

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k) + bk) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k') + bk'), \ \ \forall\ (a, b) \in \mathcal{S}.$$

Si $a = 0$ y $b = 1$, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(k - k') = 0$.
Si $a = 1$ y $b \in \mathbb{F}_q$,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(F(k) - F(k')) = -Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b(k - k')) = -bTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(k - k') = 0.$$

Si $a = 1$ y $b \in \mathbb{F}_{q^n}$,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b(k - k')) = -Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(F(k) - F(k')) = 0\ \forall\ b \in \mathbb{F}_{q^n},$$

por lo tanto $k = k'$. □

El siguiente resultado ([**18**]) es de importancia para la obtención de aproximaciones de P_I y P_S.

TEOREMA 1.6. *Sea $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ una función bent, donde q es la potencia de un primo impar. Sean $(a_1, b_1) \neq (a_2, b_2)$ elementos de $\mathcal{S}$, $u_1, u_2 \in \mathbb{F}_q$ y*

$$\begin{aligned} & N(a_1, b_1, a_2, b_2; u_1, u_2) \\ = \ & |\{x \in \mathbb{F}_{q^n} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_iF(x) + b_ix) = u_i, i = 1, 2\}|. \end{aligned}$$

Entonces,

$$\frac{q^n - (q^2 - q)q^{n/2}}{q^2} \leq N(a_1, b_1, a_2, b_2; u_1, u_2) \leq \frac{q^n + (q^2 - q)q^{n/2}}{q^2}.$$

DEMOSTRACIÓN. Como (a_1, b_1) y (a_2, b_2) son elementos distintos de $\mathcal{S}$, entonces son linealmente independientes sobre $\mathbb{F}_q$. Consideremos ahora a $\chi(\cdot) := e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(\cdot)/p}$ como el caracter aditivo canónico de $\mathbb{F}_q$ y consideremos a $\psi(\cdot) := e^{2\pi i Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\cdot)/p}$

el caracter aditivo canónico de $\mathbb{F}_{q^n}$, luego se tiene que,

$$
\begin{aligned}
& q^2 N(F; a_1, b_1, a_2, b_2; u_1, u_2) \\
= & \sum_{x \in \mathbb{F}_{q^n}} \left[\sum_{y_1 \in \mathbb{F}_q} \chi(y_1(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_1 F(x) + b_1 x) - u_1)) \right] \\
& \left[\sum_{y_2 \in \mathbb{F}_q} \chi(y_2(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_2 F(x) + b_2 x) - u_2)) \right] \\
= & \sum_{x \in \mathbb{F}_{q^n}} \sum_{y_1 \in \mathbb{F}_q} \sum_{y_2 \in \mathbb{F}_q} \prod_{i=1}^{2} \chi\left(y_i(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_i F(x) + b_i x) - u_i) \right) \\
= & \sum_{x \in \mathbb{F}_{q^n}} \sum_{y_1 \in \mathbb{F}_q} \sum_{y_2 \in \mathbb{F}_q} \chi\left(\sum_{i=1}^{2} y_i(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_i F(x) + b_i x) - u_i) \right) \\
= & \; q^n + \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}} \\
& \sum_{x \in \mathbb{F}_{q^n}} \chi\left(\sum_{i=1}^{2} y_i(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_i F(x) + b_i x) - u_i) \right) \\
= & \; q^n + \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}} \\
& \sum_{x \in \mathbb{F}_{q^n}} \chi\left(\sum_{i=1}^{2} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y_i a_i F(x) + b_i x) - y_i u_i \right) \\
= & \; q^n + \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}}
\end{aligned}
$$

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{q^n}} \chi\left(\sum_{i=1}^{2} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y_i a_i F(x)+b_i x)\right)\chi\left(-\sum_{i=1}^{2} y_i u_i\right)\\
=\ & q^n + \sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}} \chi\left(-\sum_{i=1}^{2} y_i u_i\right)\sum_{x\in\mathbb{F}_{q^n}}\chi\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\sum_{i=1}^{2}(y_i a_i F(x)+b_i x)\right)\right)\\
=\ & q^n + \sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}} \chi\left(-\sum_{i=1}^{2} y_i u_i\right)\sum_{x\in\mathbb{F}_{q^n}}\psi\left(\sum_{i=1}^{2}(y_i a_i F(x)+b_i x)\right)\\
=\ & q^n + \sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}} \chi\left(-\sum_{i=1}^{2} y_i u_i\right)\mu_{y_1a_1+y_2a_2,y_1b_1+y_2b_2}(F),
\end{aligned}$$

$$\text{donde } \mu_{c,d}=\sum_{x\in\mathbb{F}_{q^n}} e^{2\pi i Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(cF(x)+dx)/p}.$$

Sea $(y_1,y_2)\neq(0,0)$ fijo. Si $y_1a_1+y_2a_2=0$ entonces $y_1b_1+y_2b_2\neq 0$, ya que $(a_1,b_1),(a_2,b_2)$ son linealmente independientes sobre $\mathbb{F}_q$, por lo tanto:

$$\mu_{y_1a_1+y_2a_2,y_1b_1+y_2b_2}(F)=0.$$

Si $y_1a_1+y_2a_2\neq 0$,

$$\begin{aligned}
&q^2N(F;a_1,b_1,a_2,b_2;u_1,u_2)-q^n\\
=\ & \sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}} \chi\left(\sum_{i=1}^{l} y_i u_i\right)\mu_{y_1a_1+y_2a_2,y_1b_1+y_2b_2}(F),
\end{aligned}$$

lo cual implica que,

$$|q^2N(F;a_1,b_1,a_2,b_2;u_1,u_2)-q^n|$$

$$\leq \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}} |\mu_{y_1 a_1 + y_2 a_2, y_1 b_1 + y_2 b_2}(F)|$$

$$\leq \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}} q^{n/2} = (q^2 - q) q^{n/2}.$$

De aquí se tiene el resultado. □

A continuación se dan aproximaciones de P_I y P_S.

TEOREMA 1.7. *([**18**]) Para el esquema de autenticación definido anteriormente se tiene que,*

$$P_I \leq \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{n/2}},\ P_S \leq \frac{1}{q} + \frac{q^2 - 1}{q(q^{n/2} - q + 1)}.$$

Más aún, $|\mathcal{S}| = q^n + 1, |\mathcal{T}| = q, |\mathcal{K}| = |\mathcal{E}| = q^n$.

DEMOSTRACIÓN. Para cualquier $(a, b) \in \mathcal{S}$, al menos una entrada es distinta de cero. Utilizando el Teorema 1.2 del Capítulo 4,

$$|\{k \in \mathcal{K} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(af(k) + bk) = t\}| \leq \frac{q^n - (q-1)q^{n/2}}{q},$$

luego,

$$P_I = \text{máx}_{s \in \mathcal{S}, t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(af(k) + bk) = t\}}{|\mathcal{K}|}$$

$$\leq \frac{q^n + (q-1)q^{n/2}}{q^{n+1}} = \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{n/2}}.$$

Hallemos P_S. Nuevamente por el Teorema 1.2 del Capítulo 4,

$$|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}| \geq \frac{q^n - (q-1)q^{n/2}}{q},$$

y por el Teorema 1.6,

$$|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}| \leq \frac{q^n + (q^2 - q)q^{n/2}}{q^2}.$$

Por lo tanto,

$$P_S = \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|}$$

$$\leq \frac{q^n + (q^2 - q)q^{n/2}}{(q^n - (q-1)q^{n/2})q} = \frac{1}{q} + \frac{q^2 - 1}{q(q^{n/2} - q + 1)}.$$

□

En estos esquemas es importante obtener cotas muy pequeñas respecto a P_I y P_S, pues de este modo se obtienen buenos equemas de autenticación ya que P_I y P_S serán números muy pequeños. Nótese que es mejor si P_I y P_S no alcanzan las respectivas cotas. Al considerar q^n y q como antes, si nos fijamos en la expresión de las cotas, se obtienen muy pequeñas si q^n y q son números grandes y mejor aún si la diferencia entre q^n y q también es grande.

Se tienen los siguientes ejemplos: Considérese $\mathbb{F}_{3^2}$ y $\mathbb{F}_3$ y la función bent $F(x) = x^2$. Utilizando el esquema anterior se tiene que $P_I \leq 0.5555$ y $P_S \leq 3$ (con la fórmula de las cotas). Por medio de un programa computacional se tiene que $P_I = 5/9 = 0.5555$, este resultado se obtiene por ejemplo considerando

$$\begin{aligned} & |\{k \in \mathbb{F}_{3^2} : E_k(1, \alpha + 1) = 1\}| \\ = \; & |\{k \in \mathbb{F}_{3^2} : Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(F(k) + (\alpha + 1)k) = 1\}| = 5, \end{aligned}$$

en donde α es un elemento primitivo de $\mathbb{F}_{3^2}$. En este ejemplo la cota de P_S no es buena. Más aún, al utilizar el programa, se tiene que $P_S = 2/2 = 1$, pues

$$|\{k \in \mathbb{F}_{3^2} : E_k(1, \alpha^5) = 1,\ E_k(1, \alpha^2) = 2\}| = 2.$$

y

$$|\{k \in \mathbb{F}_{3^4} : E_k(1, \alpha^5) = 1\}| = 2.$$

En este caso la cota de P_I es grande, y P_I alcanza esta cantidad, lo cual no es recomendable, pues nuestro deseo es encontrar la menor cantidad posible para P_I. Veamos que sucede para un campo mayor sobre $\mathbb{F}_3$.

Considérese $\mathbb{F}_{3^4}$, $\mathbb{F}_3$ y la función bent $F(x) = x^2$. Utilizando el esquema anterior se tiene que $P_I \leq 0.4074$ y $P_S \leq 0.7142$ (con la fórmula de las cotas). Por medio de un programa computacional se tiene que $P_I = 30/81 = 0.3703$, este resultado se obtiene por ejemplo considerando

$$\begin{aligned} & |\{k \in \mathbb{F}_{3^4} : E_k(1, 2\alpha + 1) = 1\}| \\ = \; & |\{k \in \mathbb{F}_{3^4} : Tr_{\mathbb{F}_{3^4}/\mathbb{F}_3}(F(k) + (2\alpha + 1)k) = 1\}| = 30, \end{aligned}$$

en donde α es un elemento primitivo de $\mathbb{F}_{3^4}$. También se obtiene que

$$|\{k \in \mathbb{F}_{3^4} : E_k(0, 1) = 1,\ E_k(1, \alpha^{16}) = 2\}| = 12.$$

Ya que $|\{k \in \mathbb{F}_{3^4} : E_k(0, 1) = 1\}| = 27$, entonces $P_S = 12/27 = 0.4444$, pues es la mayor razón que se puede hallar. En este caso la cota de P_I va disminuyendo respecto al ejemplo anterior y mejor aún, la cantidad P_I no alcanza la respectiva cota. Por otro lado, la cota de P_S ya es significativa, aunque no es buena. Pero en este caso P_S no alcanza su respectiva cota.

Por último considérese $\mathbb{F}_{3^6}$ y $\mathbb{F}_3$ y la función bent $F(x) = x^2$. Utilizando el esquema anterior se tiene que $P_I \leq 0.3580$ y $P_S \leq 0.4399$ (con la fórmula de las

cotas). Por medio de un programa computacional se tiene que $P_I = 261/729 = 0.3580$, este resultado se obtiene por ejemplo considerando

$$\begin{aligned} & |\{k \in \mathbb{F}_{3^6} : E_k(1, \alpha^{84}) = 1\}| \\ = \quad & |\{k \in \mathbb{F}_{3^6} : Tr_{\mathbb{F}_{3^6}/\mathbb{F}_3}(F(k) + (\alpha^{84})k) = 1\}| = 261, \end{aligned}$$

en donde α es un elemento primitivo de $\mathbb{F}_{3^6}$. Con respecto a P_S, debido a lo tardado del programa computacional por el tamaño de los vectores y la cantidad que se generan, se hallaron solamente algunas razones, por ejemplo una razón que se encontro fue entre

$$A = |\{k \in \mathbb{F}_{3^6} : E_k(1, \alpha^{50}) = 1,\ E_k(1, \alpha^{104}) = 0\}| = 90$$

y

$$B = |\{k \in \mathbb{F}_{3^6} : E_k(1, \alpha^{104}) = 0\}| = 234,$$

por lo que $A/B = 0.3846$. En este caso P_I alcanza la cantidad de su cota, pero se puede ver que P_I es menor con respecto al ejemplo anterior. Por otro lado la cota de P_S va disminuyendo respecto al ejemplo anterior, aunque en este caso no se halló P_S. En estos ejemplos se encuentran muchas razones los cuales no alcanzan P_I y P_S respectivamente. Esto es importante pues no necesariamente se elijen siempre los elementos del espacio fuente y el espacio de etiquetado que corrresponden a razones que alcanzan P_I y P_S. Cabe mencionar que esto ejemplos son ilustrativos, pues se consideran números pequeños.

2. Construcciones basadas en funciones casi-bent

También es posible la construcción de esquemas de autenticación con una pequeña probabilidad de engaño al utilizar funciones casi-bent ([**8**]), en el cual un relevante parámetro es la no-linealidad de la función f. A continuación se presentan 2 construcciones basadas en funciones casi-bent. Para mayores detalles se puede consultar [**8**].

2.1. Construcción 1. Se define un esquema de autenticación basado en funciones $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ de la siguiente manera:

DEFINICIÓN 2.1. *Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función. Se define un esquema de autenticación $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E} = \{E_k : k \in \mathcal{K}\})$, donde,*

$$\begin{aligned} \mathcal{S} &= \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \\ \mathcal{T} &= \mathbb{F}_{2^h}, \\ \mathcal{K} &= \mathbb{F}_{2^n} \times \mathbb{F}_{2^h}, \\ \mathcal{E} &= \{E_k : k \in \mathcal{K}\}, \end{aligned}$$

y

$$E_k(s) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(af(k_1) + bk_1) + k_2,$$

$k = (k_1, k_2) \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

En el siguiente resultado ([**8**]) se obtiene $|\mathcal{K}| = |\mathcal{E}|$.

TEOREMA 2.2. *La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección.*

DEMOSTRACIÓN. La solución es similar a la del Teorema 1.2. □

En el siguiente resultado ([**8**]) se obtienen aproximaciones para P_I y P_S :

TEOREMA 2.3. *Para el esquema de autenticación definido anteriormente se tiene que,*

$$P_I = \frac{1}{2^h} \text{ y } P_S \leq \frac{1}{2^h} + \left(1 - \frac{1}{2^h}\right)\left(1 - \frac{N_F}{2^{n-1}}\right).$$

Más aún,

$$|\mathcal{S}| = 2^{2n}, |\mathcal{T}\ | = 2^h, |\mathcal{K}| = |\mathcal{E}| = 2^{n+h}.$$

DEMOSTRACIÓN. La prueba es similar a la del Teorema 1.3. □

TEOREMA 2.4. *([**8**]) En particular para el esquema de autenticación definido anteriormente, si $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ es una función casi-bent, entonces,*

$$P_I = \frac{1}{2^h} \text{ y } P_S \leq \frac{1}{2^h} + \frac{1 - 2^{-h}}{2^{\frac{n-1}{2}}}.$$

□

Se omitieron ejemplos en este caso, debido a lo tardado del programa computacional por el tamaño de los vectores y la cantidad que se generan, ya que los campos más pequeños a considerar son $\mathbb{F}_{2^9}$ y $\mathbb{F}_{2^3}$. Los vectores que se obtienen en este caso son de longitud 4096 y el número de estos vectores es 262144.

2.2. Construcción 2. Se define un esquema de autenticación basado en funciones $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ de la siguiente manera ([**8**]):

DEFINICIÓN 2.5. *Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función. Se define un esquema de autenticación $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E} = \{E_k : k \in \mathcal{K}\})$, donde,*

$$\begin{aligned}
&\mathcal{S} = \{1\} \times \mathbb{F}_{2^n} \cup \{(0,1)\} \subseteq \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \\
&\mathcal{T} = \mathbb{F}_{2^h}, \\
&\mathcal{K} = \mathbb{F}_{2^n}, \\
&\mathcal{E} = \{E_k : k \in \mathcal{K}\},
\end{aligned}$$

y

$$E_k(s) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(k) + bk),$$

$k \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

En el siguiente resultado se obtiene $|\mathcal{K}| = |\mathcal{E}|$.

TEOREMA 2.6. *([**8**]) La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección*

DEMOSTRACIÓN. La prueba es similar a la del Teorema 1.5. □

TEOREMA 2.7. *([**8**]) Para el esquema de autenticación definido anteriormente se tiene que,*

$$P_I \leq \frac{1}{2^h} + \left(1 - \frac{1}{2^h}\right)\left(1 - \frac{N_F}{2^{n-1}}\right),\ P_S \leq \frac{1}{2^h} + \frac{(2^h - 2^{-h})(2^n - 2N_F)}{2^n - (2^h - 1)(2^n - 2N_F)}.$$

Más aún $|\mathcal{S}| = 2^n + 1, |\mathcal{T}| = 2^h, |\mathcal{K}| = |\mathcal{E}| = 2^n$.

DEMOSTRACIÓN. La prueba es similar a la del Teorema 1.7. □

TEOREMA 2.8. *([**8**]) Para el esquema de autenticación definido anteriormente, si* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *es una función casi bent, entonces,*

$$P_I \leq \frac{1}{2^h} + \left(\frac{2^h - 1}{2^h}\right)\frac{1}{2^{\frac{n-1}{2}}} \text{ y } P_S \leq \frac{1}{2^h} + \frac{2^{2h} - 1}{2^h\left(2^{\frac{n-1}{2}} - 2^h + 1\right)}.$$

□

Considérese $\mathbb{F}_{2^9}, \mathbb{F}_{2^3}$ y la función casi-bent $F(x) = x^3$. Al utilizar el esquema anterior se tiene que $P_I \leq 0.1796$ y $P_S \leq 1$ (con la fórmula de las cotas). Por medio de un programa computacional se obtienen varias razónes aproximadas a la cota de P_I. Por ejemplo, se obtiene $80/512 = 0.1562$. Este resultado se obtiene considerando

$$\begin{aligned} & |\{k \in \mathbb{F}_{2^9} : E_k(1, \alpha^{23}) = 0\}| \\ = \ & |\{k \in \mathbb{F}_{2^9} : Tr_{\mathbb{F}_{2^9}/\mathbb{F}_{2^3}}(F(k) + (\alpha^{23})k) = 0\}| = 80. \end{aligned}$$

En donde α es un elemento primitivo de $\mathbb{F}_{2^9}$. El programa computacional es muy tardado para ejecutarse completamente en una simple computadora, razón por el cual se obtiene una aproximación de P_I y se deja P_S pendiente. Al igual que para funciones bent, al considerarse valores grandes de 2^h y 2^n (notación en los esquemas anteriores) se obtiene un mejor esquema, ya que las cotas se hacen muy pequeñas. Mejor aún si la diferencia entre 2^h y 2^n es grande, las cotas son mejores.

Bibliografía

[1] Biham, E. and Shamir, A. "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, vol. 4, 1991, pp. 3-72, .

[2] Blakey, G.R. "Safeguarding cryptographic keys", in Proc. Nat. Computer Conf., vol. 48, New York, Jun. 1979, pp. 313-317.

[3] Budaghyan, L.; Carlet, C. and Pott, A. "New classes of Almost Bent and Almost Perfect Nonlinear Polynomials", IEEE Transactions on Information Theory, vol. 52, no. 3, March 2006, pp. 1141-1152.

[4] Carlet, C. and Guillot, Ph. "A new representation of Boolean Functions", Springer-Verlag Berlin Heidelberg, 1999, pp. 94-103.

[5] Carlet, C. and Guillot, Ph. "Bent, resilient functions and the Numerical Normal Form", DIMACS SDMTCS, 56, 2001, pp. 87-96

[6] Carlet, C.; Ding, C. and Yuan, J. "Linear Codes From Perfect Nonlinear Mappings and Their Secret Sharing Schemes", IEEE Transactions on Information Theory, vol. 51, no. 6, June 2005, pp. 2089-2102.

[7] Carlet, C.; Ding, C. and Zinoviev, V. "Codes, bent functions and permutations suitable for Des-like cryptosystems", Designs, Codes and Cryptography, vol. 15, 1998, pp. 125-156.

[8] Carlet, C.; Ding, C. and Niederreiter, H. "Authentication schemes from highly nonlinear functions", Designs, Codes and Cryptography, 2006, pp. 71-79.

[9] Carlet, C. and Prouff, E. "Vectorial Functions and Covering Sequences", Finite Fields and Applications, Lecture Notes in Computer Science, 2003, Toulouse, Fq7, G. L. Mullen, A. Poli and H. Stichtenoth eds, 2004, pp. 215-248, .

[10] Canteaut, A.; Charpin P. and Dobbertin H. "A new Characterization of Almost Bent Functions", IEEE Transactions on Information Theory, vol. 51, no. 6, June 2005, pp. 186-200.

[11] Canteaut, A; Charpin, P. and Dobbertin, H. "Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences", SIAM J. Discrete Math., vol. 13, no. 1, 2000, pp. 105-138 .

[12] Carter, J. L. and Wegman, M. N."Universal classes of hash functions", J. Comput. Syst. Sci., vol 18, 1979, pp. 143-154.

[13] Chabaud, F. and Vaudenay, S. "Links Between Differential and Linear Cryptanalysis", in Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, A. D. Santis, Ed. New York: Springer-Verlag, 1995, pp. 356-365.

[14] Coulter, R. S. and Matthews, R. W. "Bent Polynomials Over Finite Fields", Bull. Austral. Math. Soc. 56, 1997, pp. 429-437.

[15] Coulter, Robert S. "Explicit evaluations of some Weil sums", Acta Arith. 83, 1998, pp. 241-251.

[16] Coulter, Robert S. "Further evaluations of Weil sums", Acta Arith. 86, 1998, pp. 217-226.

[17] Coulter, Robert S. "The Number of Rational Points of a Class of Artin-Schreier Curves", Finite Fields Their Appl., vol. 8, 2002, pp. 397-413.

[18] Ding, C. "Systematic Authentication Codes From Highly Nonlinear Functions", IEEE Transactions on Information Theory, vol. 50, no. 10, October 2004, pp. 2421-2428.

[19] Ding, C. and Yuan, J. "Covering and Secret Sharing with Linear Codes", in Discrete Mathematics and Theoretical Computer Science, Lecture Notes in Computer Science, C. S. Calude, M. J. Dinneen, and V. Vajnovszki, Eds. Heidelberg, Germany, Springer-Verlag, 2003, pp. 11-25.

[20] Gilbert, E. N.; MacWilliams, F. J. and Sloane, N. J. "Codes which detect deception", The Bell System Technical Journal, 1974, pp. 405-424.

[21] Heys, H."A Tutorial on Linear and Differential Cryptanalysis", Electrical and Computer Engineering Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John´s, NF. Canada.

[22] Ireland, K. and Rosen, M. *"A Classical Introduction to Modern Number Theory"*, Springer-Verlag New York, Inc, second edition, 1990.

[23] Leander, N. "Monomial Bent Functions", IEEE Transactions on Information Theory, vol. 52, Feb. 2006, pp. 738-743.

[24] Lidl, R. and Niederreiter, H. *"Finite Fields"*, Cambridge, U.K, Cambridge Univ. Press, vol. 20 of Encyclopedia of Mathematics and Its Applications. Reading, MA; Addison-Wesley, 1997.

[25] MacWilliams, F.J. and Sloane, N. J. *"The Theory of Error Correcting Codes"*, Elsevier Science Publisher B.V., North-Holland Mathematical Library, vol. 16, 1977

[26] Massey, James L. "Minimal Codewords and Secret Sharing", in Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden, August 1993, pp. 276-279.

[27] Nyberg, K. "Differentially uniform mappings for cryptography", in Advances in Cryptography. Eurocrypt'93, Lecture Notes in Computer Science, T. Helleseth, Ed. New York: Springer-Verlag, 1993, pp. 55-64.

[28] Okada, K. and Kurosawa, K. "MDS secret sharing scheme secure against cheaters", IEEE Transactions on Information Theory, vol. 46, no. 3, May. 2000, pp. 1078-1081.

[29] Özbudak, F. and Saygi, Z. "Some constructions of systematic authentication codes using Galois rings". Designs, Codes and Cryptography, vol. 41, no. 3, 2006, pp. 343-357.

[30] Pless, V. "Power moments identities on weight distributions in error correcting codes", Info. and Control, vol. 6, 1963, pp. 147-152.

[31] Roman, Steven *"Coding and Information Theory"*, Graduate Texts in Mathematics, Springer-Verlag, 1992.

[32] Rothaus, O. S. "On bent functions", J. Comb. Theory, 20A, 1976, pp. 300-305.

[33] Shamir, A. "How to share a secret", Commun. ACM, vol. 22, Dec. 1979, pp. 612-613.

[34] Simmons, G. J. "Authentication theory/coding theory", In advances in Cryptology-Crypto 84, 1984, pp. 411-431.

[35] Simmons, G. J. "A survey of information authentication", in Contemporary Cryptology, The Science of Information Integrity, Ed. Piscataway, IEEE Press, 1992, pp. 379-419.

[36] Stinson, D. R. *"Cryptography Theory and Practice"*, CRC Press, LCC, 1995.

[37] Stinson, D. R. "Some constructions and bounds for authentication codes", Journal of Cryptology, Ed. Springer New York, vol 1, no. 1, 1988, pp. 37-51

[38] Wan, Zhe-Xian *"Lectures on Finite Fields and Galois Rings"*, World Scientific Publishing Co. Pte. Ltd., 2003.

[39] Xing, C.; Wang, H. and Lam, K. Y. "Constructions of authentication codes from algebraic curves over finite fields", IEEE Transactions on Information Theory, 2000, pp. 886-892.

[40] Yuan, J.; Carlet, C. and Ding, C. "The Weight Distribution of a Class of Linear Codes From Perfect Nonlinear Functions", IEEE Transactions on Information Theory, vol. 52, no. 2, February 2006, pp. 712-717.