UNIVERSIDAD AUTÓNOMA METROPOLITANA

Compartición de secretos sobre campos finitos y esquemas de autenticación sobre anillos de Galois basados en funciones casi bent y bent

Presenta
Juan Carlos Ku Cauich

Para el grado de
Doctor en Ciencias (Matemáticas)

Asesor de tesis:
Dr. Horacio Tapia Recillas

Unidad Iztapalapa
Departamento de Matemáticas

México
Diciembre de 2012

Índice general

Resumen

En este trabajo se estudian las funciones perfectamente no-lineales, casi perfectamente no-lineales, bent y casi-bent sobre campos finitos, y las funciones bent sobre los anillos de Galois a fin de dar la construcción de esquemas de compartición de secretos y esquemas de autenticación utilizando estas funciones.

Introducción

Los esquemas de compartición de secretos fueron introducidos por G. R. Blakley ([**2**]) y A. Shamir ([**46**]) 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 éstas basada en la Teoría de Códigos, la cual se introduce en l981 ([**36**]), después varios autores consideran los códigos lineales correctores de errores (consultar por ejemplo [**39**], [**41**]).

Un esquema de compartición de secretos consiste en distribuir entre un número finito n de entidades, información asociada a un secreto de tal manera que reuniendo la información de k entidades $(1 \leq k \leq n)$ el secreto se pueda recuperar. De este modo una sola identidad no puede conocer el secreto o más aún reuniendo su información menos de k entidades éstos no puede conocer el secreto, por lo que el secreto está resguardado de las entidades internas o entidades externas. Por ejemplo en la apertura de cajas de seguridad, la clave para abrir una caja puede ser distribuida entre varias entidades.

Utilizando los códigos lineales es posible la construcción de esquemas de compartición de secretos. Ya que para determinar cuales conjuntos de entidades pueden ser utilizados para determinar el secreto depende de las palabras mínimas del código dual, del código considerado ([**39**]), es entonces conveniente considerar códigos lineales en donde estas palabras sean posibles de determinar. En este trabajo construimos códigos lineales cuyas palabras del código dual son palabras mínimas.

Esquemas de compartición de secretos basados en códigos lineales sobre $\mathbb{F}_q$, $q = p^r$, p primo, se han discutido (presentado en [**7**]) cuando $p \neq 2$. En este trabajo se presenta un esquema de esta naturaleza cuando $p = 2$ ([**31**]), es decir, considerando funciones casi-bent.

Los esquemas de autenticación ([**50**]) son diseñados para autenticar los mensajes enviados por un transmisor a un receptor a través de un canal de comunicación público. Si un transmisor desea enviar un mensaje a un receptor existe el riesgo de que un intruso pueda deliberadamente observar y mas aún causar un disturbio en la comunicación. El transmisor y el receptor comparten una llave secreta, y al enviar una pieza de información al receptor, el receptor utiliza la 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 ([**14**], [**24**], [**47**], [**48**]). Existen varias técnicas para describir estos esquemas entre los que se incluyen métodos combinatorios ([**51**]), algebraicos ([**54**]), por medio de anillos

de Galois ([**42**]) y entre otros usando funciones perfectamente no-lineales y casi perfectamente no-lineales sobre campos finitos describiendo esquemas de esta naturaleza en [**9**] y [**21**]. En este trabajo se introducen las funciones bent sobre anillos de Galois, esta clase de funciones se puede ver en el Capítulo 3. Usando funciones bent sobre anillos de Galois de característica p^2, p primo (con la propiedad de aún obtener funciones bent al multiplicar estas funciones por cualquier unidad del anillo de Galois), y utilizando la función de Gray sobre estos anillos se presenta la construcción de esquemas de autenticación sobre anillos de Galois ([**10**]) y sobre campos finitos [**30**]). En particular estos esquemas se tienen utilizando la familia de funciones bent construida en el Capítulo 3, los cuales tienen mejores cotas (probabilidades de aceptar como auténticos mensajes insertados por intrusos) respecto a trabajos en donde se utilizan funciones bent y casi-bent sobre campos finitos, y funciones racionales y polinomios no-degenerados sobre anillos de Galois ([**21**], [**9**], [**42**]).

Considerando los ataques por imitación y por substitución por parte de un intruso, al enviarse información a través de un canal de comunicación público, este trabajo se enfoca a encontrar cotas respecto a las probabilidades de que éstos se concluyan, es decir, que el receptor acepte como auténtico el mensaje insertado por el intruso.

Este trabajo está organizado de la siguiente manera: en el Capítulo 1 se recuerdan definiciones y resultados básicos que serán útiles a lo largo del trabajo, entre los cuales se encuentran: caracteres, funciones booleanas y propiedades de éstas. Se define también la transformada de Fourier, que es en términos de éste como se define una función perfectamente no-lineal, y los códigos lineales.

En el Capítulo 2 se introducen las funciones bent vectoriales, $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q = p^m$, p un número primo, de las cuales se definen las funciones bent vectoriales, casi-bent, perfectamente no-lineales y las casi perfectamente no-lineales, enunciando la relación que se tiene entre éstas ([**15**], [**16**]).

En el Capítulo 3 se introduce una familia de funciones bent sobre un anillo de Galois ([**10**]), los cuales serán usados para los resultados modulares sobre códigos de autenticación.

El Capítulo 4 está enfocado a la construcción de códigos lineales utilizando funciones perfectamente no-lineales sobre $\mathbb{F}_{p^r}$, ($p \neq 2$ primo), y posteriormente se da la construcción de esquemas de compartición de secretos con base en estos códigos lineales utilizando el método de Massey.

En el Capítulo 5 usando funciones casi-bent se resuelve el caso $p = 2$, es decir, se define un código lineal y construye un esquema de compartición de secretos sobre $\mathbb{F}_{2^r}$, ([**31**]). Existen casos en que el espacio secreto es pequeño, por ejemplo $\mathbb{F}_2$, en esta situación se dan dos extensiones de estos esquemas los cuales generan esquemas con un espacio de secretos mayor a comparación del original.

En el Capítulo 6 se da la construcción de esquemas de autenticación por medio de las funciones perfectamente no-lineales y las casi-bent.

Finalmente en el Capítulo 7 se da la construcción de esquemas de autenticación con base en las funciones bent sobre anillos de Galois y para esto también se define la función

de Gray ([**25**]). Se dan comparaciones con esquemas de autenticación de otros trabajos y ejemplos de funciones bent sobre los anillos de Galois de característica 4, los cuales no cumplen con la propiedad específica que se utiliza al construir los esquemas de autenticación presentados en este Capítulo.

Capítulo 1

Antecedentes

En este Capítulo se da por hecho el conocimiento y algunas propiedades de los campos finitos, se recuerdan conceptos básicos como la función traza, caracteres y sumas de Gauss. Respecto a los campos finitos y la traza se puede consultar [**35**] y [**53**], y sobre los caracteres y las sumas de Gauss puede consultarse la referencia [**35**]. Las funciones booleanas y la transformada de Fourier son también introducidas en este Capítulo así como los códigos lineales ([**5**], [**37**], [**45**]), proporcionando algunos ejemplos de éstos.

1. La función traza

Sea $\mathbb{F}_q$ un campo finito con $q = p^n$ (p un número primo, n un entero positivo), 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 grado n de $\mathbb{F}_q$.

Recuérdese que el automorfismo de Frobenius está definido como: $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$,

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

σ es una función de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Nótese que $\sigma(a) = a$, para toda $a \in \mathbb{F}_q$.

DEFINICIÓN 1.1. *La función* $traza$,

$$Tr_{(\mathbb{F}_{q^n}/\mathbb{F}_q)}(\alpha) : \mathbb{F}_{q^n} \to \mathbb{F}_q,$$

de $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$, *está definida como*

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

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

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

La función traza tiene las siguientes propiedades:

TEOREMA 1.2. *(*[**35**],[**53**]*)*

1. $Tr_{(\mathbb{F}_{q^n}/\mathbb{F}_q)}$ *es una transformación lineal de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$.
2. $Tr_{(\mathbb{F}_{q^n}/\mathbb{F}_q)}(a) = na$ *para toda* $a \in \mathbb{F}_q$,
3. $Tr_{(\mathbb{F}_{q^n}/\mathbb{F}_q)}(\sigma(\alpha)) = Tr_{(\mathbb{F}_{q^n}/\mathbb{F}_q)}(\alpha)$ *para toda* $\alpha \in \mathbb{F}_{q^n}$,
4. *(Transitividad de la traza) Sea* K *un campo finito,* F *una extensión finita de* K *y* E *una extensión finita de* F. *Entonces,*

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

5. *Para* $\alpha \in \mathbb{F}_{q^n}$, $Tr_{(\mathbb{F}_{q^n}/\mathbb{F}_q)}(\alpha) = 0 \Longleftrightarrow \alpha = \beta - \beta^q$ *para alguna* $\beta \in \mathbb{F}_{q^n}$.

□

2. Caracteres

En esta Sección se recuerda la definición y propiedades básicas de los caracteres. Para mayores detalles consúltese **[28]**, **[35]** y **[53]**. Sea G un grupo abeliano finito de orden n 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,

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

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

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

es decir, las imágenes de χ son raíces n-ésimas de la unidad.

Ya que $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = 1$, entonces $\chi(g^{-1}) = \overline{\chi(g)}$ para toda $g \in G$, es decir, $\chi(g^{-1})$ es el conjugado de $\chi(g)$. Se define el caracter trivial χ_0 como $\chi_0(g) = 1$, para toda $g \in G$, los demás caracteres serán llamados no-triviales. Dado un número finito de caracteres $\chi_1, \ldots, \chi_n$ de G, el caracter producto $\chi_1 \cdots \chi_n$ está definido como

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

En particular cuando

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

se escribe χ^n en lugar de $\chi_1 \cdots \chi_n$. Sea $\widetilde{G}$ el conjunto de caracteres de G, es decir,

$$\widetilde{G} := \{\chi : G \to \mathbb{C}_1 | \ \chi \text{ caracter de } G\}.$$

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* $\chi_j : G \to \mathbb{C}_1$, *definida por*

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

es un caracter de G.

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

Como un caso particular del Ejemplo 2.1 se tiene el siguiente resultado sobre campos finitos:

EJEMPLO 2.2. *Sea* g *un elemento primitivo de* $\mathbb{F}_q$ $(q = p^n, p \text{ primo})$. *Los caracteres del grupo multiplicativo de* $\mathbb{F}_q$ *son de la forma,*

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

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

Los caracteres del grupo multiplicativo de $\mathbb{F}_q$ son llamados caracteres multiplicativos de $\mathbb{F}_q$. Cualquier caracter multiplicativo de $\mathbb{F}_q$ satisface $\psi(g) = e^{2\pi ij/(q-1)}$, para alguna $j \in \{0, 1, \ldots, q-2\}$, ya que estas son raíces $(q-1)$-ésimas de la unidad, por lo que $\psi(g^k) = \psi_j(g^k)$ para toda $k \in \{0, 1, \ldots, q-2\}$. Por lo tanto $\psi(g) = \psi_j$ para alguna $j \in \{0, 1, \ldots, q-2\}$. De aquí se puede concluir que los caracteres dados en el ejemplo anterior son todos los caracteres multiplicativos de $\mathbb{F}_q$.

Propiedades de los caracteres incluyen los siguientes ([**35**]):

TEOREMA 2.3. *Sea χ_0 el caracter trivial y χ un caracter no trivial del grupo abeliano finito G de orden n. Entonces,*

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

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

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

□

Más aún, se tiene un isomorfismo de grupos.

TEOREMA 2.4. *Sea G un grupo abeliano finito de orden n. Entonces $\widetilde{G} \cong G$.*

□

TEOREMA 2.5. *([**28**]) Sea ψ un caracter multiplicativo de $\mathbb{F}_q$. ψ^n es trivial si y sólo si el orden de ψ divide a $d = (n, q-1)$.*

DEMOSTRACIÓN. Resolviendo:

$\Leftarrow$) Sea r el orden de ψ, luego $r|d$, y entonces $r|n$. Por lo tanto $n = sr$, 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, ya que $\{\psi^0, \ldots, \psi^{r-1}\}$ es un subgrupo de $\widetilde{G}$, entonces $r|q-1$, lo cual implica que $r|d$. □

Sea $\eta(c) = 1$ si c es el cuadrado de un elemento de $\mathbb{F}_q$ y $\eta(c) = -1$ en otro caso, y considérese el caracter multiplicativo de $\mathbb{F}_q$, $\psi_{\frac{q-1}{2}}$ (utilizando la notación del Ejemplo 2.2). Entonces,

TEOREMA 2.6. *([**55**]) Sea q la potencia de un número primo impar. La función η es un caracter multiplicativo de $\mathbb{F}_q$ tal que $\eta = \psi_{\frac{q-1}{2}}$.*

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

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

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

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

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

TEOREMA 2.7. *([**55**]) 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 los elementos $c \in \mathbb{F}_p^*$, y 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

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

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

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

luego $w = \frac{p^n-1}{p-1}$ es par si n es par, y es impar si n es impar.

Sea $c \in \mathbb{F}_p^*$. Entonces $c = (g^w)^r$, para alguna $r \in \{1, \cdots, p-1\}$, de aquí si n es par, $\eta(c) = \eta((g^w)^r) = e^{\pi icr} = 1$, y si n es impar, $\sum_{c\in\mathbb{F}_p^*} \eta(c) = \sum_{r\in\{1,\cdots,p-1\}} \eta(g^{wr}) = 0$, concluyendo de este modo el resultado. □

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

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

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 utilizará la expresión, caracter aditivo de $\mathbb{F}_q$. El caracter χ_1 es llamado el caracter aditivo canónico de $\mathbb{F}_q$.

El siguiente resultado proporciona todos los caracteres aditivos de $\mathbb{F}_q$:

TEOREMA 2.8. *([**35**]) 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 manera.*

□

3. Sumas de Gauss

Las sumas de Gauss sobre campos finitos son definidas en términos de los caracteres. Las propiedades mencionadas a continuación serán de importancia al construir códigos lineales con base en funciones bent y casi-bent. Para mayores detalles se puede consultar por ejemplo [**17**], [**18**], [**55**] y [**35**].

DEFINICIÓN 3.1. *Sea $\mathbb{F}_q$ un campo con $q = p^n$ elementos y ψ, χ, caracteres multiplicativo y aditivo respectivamente de $\mathbb{F}_q$. La suma de Gauss, denotada por $G(\psi, \chi)$, está definida como*

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

Detalles sobre el siguiente resultado se pueden consultar en [**35**].

TEOREMA 3.2. *Sea $\mathbb{F}_q$ un campo con q elementos, $q = p^n$, p un primo impar, η el caracter cuadrático de $\mathbb{F}_q$, i el número complejo $\sqrt{-1}$ 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 $\mathbb{F}_q$ y sea

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

TEOREMA 3.3. *(*[**17**]*) Sea $n/(n, r)$ impar, $r \in \mathbb{N}$, $0 \neq a \in \mathbb{F}_q$ y $q = p^n$, p impar. 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 $x \neq 0$,

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

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

Por lo tanto

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

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

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

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

□

El siguiente resultado es necesario para la hipótesis del Teorema 3.6.

TEOREMA 3.4. [**17**] *Sea* $0 \neq a \in \mathbb{F}_p$ *y* n *un número natural. Si* $n/(n,r)$ *es impar, entonces* $x \mapsto a^{p^r}x^{p^{2r}} + ax$ *es una permutación en* $\mathbb{F}_q$, $q = p^n$, p *primo impar.*

DEMOSTRACIÓN. Es fácil 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 $(n,r) = d$, y supóngase que $0 \neq x_1 \in \mathbb{F}_q$ 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,

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

luego,

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

Por lo tanto,

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

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

El resultado anterior también es válido en característica par.

TEOREMA 3.5. *(*[**34**]*) Sea* $d = 2^r + 1$, $r \in \mathbb{N}$. *Si* $a \notin \{x^d | x \in \mathbb{F}_{2^n}\}$, *entonces* $x \mapsto a^{2^r}x^{2^{2r}} + ax$ *es una permutación en* $\mathbb{F}_{2^n}$.

DEMOSTRACIÓN. Se tiene 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 $0 \neq x_1 \in \mathbb{F}_{2^n}$ 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

$(2^r-1, 2^r+1) = 1$, el lado izquierdo de la expresión anterior es una d-ésima potencia, y en el lado derecho, 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 3.6. *([**18**]) Sean $q = p^n$, p primo impar y r un entero tal que $n/(n,r)$ es impar. Supóngase que $x_{a,b}$, $a, b \in \mathbb{F}_q$, $(a, b \neq 0)$, es la única solución de la ecuación $a^{p^r}x^{p^{2r}} + ax + b^{p^r} = 0$. Entonces,*

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

DEMOSTRACIÓN. Resolviendo:

$$\begin{aligned} S_r(a,b)S_r(-a,0) &= \sum_{y\in\mathbb{F}_q}\chi_1(-ay^{p^r+1})\sum_{w\in\mathbb{F}_q}\chi_1(aw^{p^r+1}+bw) \\ &= \sum_{y\in\mathbb{F}_q}\chi_1(-ay^{p^r+1})\sum_{x\in\mathbb{F}_q}\chi_1(a(x+y)^{p^r+1}+b(x+y)) \\ &= \sum_{x,y\in\mathbb{F}_q}\chi_1\left(a(x+y)^{p^r+1}+b(x+y)\right)\chi_1(-ay^{p^r+1}) \\ &= \sum_{x,y\in\mathbb{F}_q}\chi_1\left(a(x+y)^{p^r+1}+b(x+y)-ay^{p^r+1}\right) \\ &= \sum_{x,y\in\mathbb{F}_q}\chi_1\left(a(x^{p^r+1}+x^{p^r}y+y^{p^r}x+y^{p^r+1})+bx+by-ay^{p^r+1}\right) \\ &= \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1(ax^{p^r}y+axy^{p^r}+by) \\ &= \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1\left(a^{p^r}x^{p^{2r}}y^{p^r}+axy^{p^r}+b^{p^r}y^{p^r}\right) \\ &= \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^r+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1\left(y^{p^r}(a^{p^r}x^{p^{2r}}+ax+b^{p^r})\right). \end{aligned}$$

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 3.3 se obtiene que,

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

Por lo tanto,

$$S_r(a,b) = (S_r(-a,0))^{-1}\,\overline{q\chi_1(ax_{a,b}^{p^r+1})}$$

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

□

TEOREMA 3.7. *([**55**]) Sea $q = p^n$, p primo impar. Entonces para toda $a \in \mathbb{F}_q$,*

$$|\{x \in \mathbb{F}_q : Tr_{(\mathbb{F}_q/\mathbb{F}_p)}(ax^2) = 0\}|$$

$$= \begin{cases} p^{n-1} & \textit{si n es impar} \\ \frac{1}{p}\left(q - \eta(a)(p-1)q^{1/2}\right) & \textit{si n es par y } p \equiv 1 \textit{ mód } 4 \\ \frac{1}{p}\left(q - i^n\eta(a)(p-1)q^{1/2}\right) & \textit{si n es par y } p \equiv 3 \textit{ mód } 4 \end{cases}.$$

DEMOSTRACIÓN. Resolviendo:

$$|\{x \in \mathbb{F}_q : Tr_{(\mathbb{F}_q/\mathbb{F}_p)}(ax^2) = 0\}| = \frac{1}{p}\sum_{x\in\mathbb{F}_q}\sum_{c\in\mathbb{F}_p} e^{2\pi i Tr_{(\mathbb{F}_q/\mathbb{F}_p)}(acx^2)/p}$$

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

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 tanto,

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

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

De donde se obtiene el resultado dependiendo del caso de la hipótesis que se considere. □

4. Funciones booleanas

Las funciones booleanas son importantes en varias áreas, como en Criptografía y la Teoría de Códigos, por ejemplo en el diseño de algoritmos criptográficos para la elaboración de cifrados de flujo ([**20**]), en la criptografía de llave secreta o simétrica como el criptosistema DES, en donde se encuentran las llamadas S-cajas. Estas funciones también son utilizadas en la construcción de códigos lineales, como por ejemplo los códigos de Reed-Muller binarios ([**37**]). En este trabajo estas funciones son utilizadas para la construcción de códigos lineales con el propósito de construir esquemas de compartición de secretos y esquemas de autenticación.

Sea $n \geq 1$ un número entero, $\mathbb{F}_2$ el campo de los números binarios y $\mathbb{F}_2^n$ el producto cartesiano de $\mathbb{F}_2$, el cual es un $\mathbb{F}_2$-espacio vectorial de dimensión n.

DEFINICIÓN 4.1. *Se llama función booleana a aquellas que tienen dominio $\mathbb{F}_2^n$ y codominio $\mathbb{F}_2$, es decir,*

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

Se denota como $\mathcal{B}_n$ al conjunto de funciones booleanas de n entradas, o sea,

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

EJEMPLO 4.2. *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.

El conjunto de funciones booleanas de n entradas 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 forma de representar a las funciones booleanas es la Forma Algebraica Normal (F.A.N.).

DEFINICIÓN 4.3. *([**5**]) Una función booleana f tiene una F.A.N. si se puede expresar como*

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

Nótese que en el Ejemplo 4.2 la función f está expresada en su F.A.N.

Se tiene la siguiente relación de orden ($\leq_n$) en $\mathbb{F}_2^n$: si $x = (x_1, \ldots, x_n)$ y $u = (u_1, \ldots, u_n)$ son elementos de $\mathbb{F}_2^n$, entonces, $x \leq_n u$ si y sólo si para toda $i \in \{1, \ldots, n\}$, $x_i \leq u_i$, donde $\leq$ es la relación de orden natural en $\mathbb{F}_2$.

Con base en el orden dado en $\mathbb{F}_2^n$ se tiene el siguiente resultado el cual afirma que cualquier función booleana tiene una representación en su F.A.N.

TEOREMA 4.4. *(*[**5**]*) Sea $f : \mathbb{F}_2^n \to \mathbb{F}_2$ una función booleana. Entonces,*

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

□

De aquí el conjunto de representantes de las funciones booleanas en su F.A.N. es el anillo $\mathcal{R}_n := \mathbb{F}_2[x_1, x_2, \ldots, x_n]/\langle x_i^2 - x_i \rangle$, $i = 1, \ldots, n$.

El anillo $\mathcal{R}_n$ 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 su dimensión es

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

y su cardinalidad, 2^{2^n}.

En particular se tienen el siguiente conjunto de funciones booleanas en su F.A.N. el cual será de utilidad en posteriores Capítulos:

DEFINICIÓN 4.5. *Las funciones booleanas básicas son las funciones afines definidas por el conjunto*

$$\mathcal{A}_n = \{f | f(x_1, \ldots, x_n) = a_1 x_1 + \cdots + a_n x_n + a_0 = a \cdot x + a_0\},$$

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

Otra manera de representar a las funciones booleanas es por medio de sus imágenes, para describir esto considérese la función evaluación

$$ev : \mathcal{B}_n \to \mathbb{F}_2^{2^n},$$

definida como

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

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

La función ev es inyectiva y $\mathcal{B}_n$ es isomorfo a $\mathbb{F}_2^{2^n}$ como $\mathbb{F}_2$-espacio vectorial.

Obsérvese que la imagen de un elemento $f \in \mathcal{B}_n$ bajo esta función es un vector de longitud 2^n, esto implica que la cardinalidad y dimensión de $\mathcal{B}_n$ es 2^{2^n} y 2^n respectivamente.

Más aún, una base para $\mathcal{B}_n$ está dada por el siguiente conjunto de funciones booleanas cuyas imágenes son vectores de longitud 2^n las cuales forman una base de $\mathbb{F}_2^{2^n}$:

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

5. La transformada de Fourier

Para mayores detalles de esta Sección ver [**5**] y [**6**].

DEFINICIÓN 5.1. *Se define la transformada de Fourier de la función* $f : \mathbb{F}_2^n \to \mathbb{R}$ *como*

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

El espectro de Fourier de f *es el conjunto* $\{\widehat{f}(a) : a \in \mathbb{F}_2^n\}$, *donde las imágenes de* $\widehat{f}$ *son llamadas coeficientes de Fourier de* f *y* $a \cdot x$ *es el producto punto usual en* $\mathbb{F}_2^n$.

La definición anterior también se puede considerar cuando f es una función booleana.

Sea $f \in \mathcal{B}_n$ y $\zeta_f : \mathbb{F}_2^n \to \mathbb{R}$ definida por $\zeta_f := (-1)^f$. Entonces la transformada de Fourier de ζ_f está dada por

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

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

Considérese ahora el campo finito $\mathbb{F}_q$, donde q es la potencia de un número primo.

DEFINICIÓN 5.2. *Sean* $x, y \in \mathbb{F}_q^n$. *El soporte de* $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ *está definido como*

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

El peso de Hamming de x *está definido por*

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

y la distancia de Hamming entre x *y* y *como*

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

Obsérvese que el peso de Hamming de x indica el número de entradas de x distintas de cero, y la distancia de Hamming entre x y y el número de entradas en donde difieren estos elementos.

La identificación de $\mathcal{B}_n$ con $\mathbb{F}_2^n$ y mas aún considerando $q = p^n$, p un número primo, permite dar la siguiente definición.

DEFINICIÓN 5.3. *Sean $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$. El soporte de f está definido por*

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

El peso de Hamming de f está definido como

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

y la distancia de Hamming entre f, g por

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

Es decir, el peso de Hamming de una función es el número de sus imágenes distintas de cero, y la distancia de Hamming entre dos funciones es el número de sus respectivas imágenes en donde estas funciones difieren.

6. Código lineales

Los códigos lineales sobre un campo finito $\mathbb{F}_q$, donde q es la potencia de un número primo, son subespacios vectoriales de $\mathbb{F}_q^n$. Existen familias de códigos lineales como los códigos de Hamming, los de Reed-Muller, Reed-Solomon, BCH entre otros. Para mayor información consultar por ejemplo [**37**] y [**45**].

Ejemplos de códigos es la clave Morse que representa letras y números, los códigos de barras de los artículos que permite conocerlos de forma única.

A continuación se recuerda la definición de un código lineal:

DEFINICIÓN 6.1. *(*[**37**]*) Un $[n, k, d]_q$ código lineal sobre $\mathbb{F}_q$, donde q es la potencia de un número primo, es un subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k y peso mínimo d, donde*

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

es decir, el peso mínimo de $\mathcal{C}$ es el menor peso de los elementos distintos de cero del código.

Es fácil ver que el peso mínimo de un código lineal es equivalente a la distancia mínima que existe entre las palabras del código, razón por lo cual es llamado también la distancia mínima del código.

Sea $[x]$ el mayor entero menor o igual a x. El peso mínimo o distancia mínima determina el número de errores que puede detectar y corregir un código lineal.

TEOREMA 6.2. *Un $\mathbb{F}_q$-código lineal con peso mínimo d puede corregir $[\frac{1}{2}(d-1)]$ errores. Si d es un número entero par, el código puede detectar $\frac{d}{2}$ errores y corregir $\frac{1}{2}(d-1)$ errores.*

□

Describamos un ejemplo de código lineal: Sea $0 \leq r \leq n$, un número entero, $\mathcal{R}(r, n) := \{f \in \mathcal{R}_n : gr(f) \leq r\}$ y

$$\mathcal{RM}(r, n) = \{ev_r(f) := (f(p_1), f(p_2), \ldots, f(p_{2^n})) \,|\, f \in \mathcal{R}(r, n)\}.$$

Una base para $\mathcal{RM}(r,n)$ está dada por las imágenes, ev_r, de las distintas funciones booleanas en $\mathcal{B}_n$ que corresponden en su F.A.N. al conjunto

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

por lo que la dimensión de este espacio vectorial es ([**37**], [**45**]):

$$k = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}$$

y es llamado el código de Reed-Muller de orden r y longitud 2^n.

El peso mínimo de este código lineal está dado por:

TEOREMA 6.3. *(*[**37**],[**45**]*) El código de Reed-Muller $\mathcal{RM}(r,n)$ tiene peso mínimo 2^{n-r}.*

□

Obsérvese que estos códigos lineales están relacionados con las funciones booleanas. En particular se tiene que,

$$\{ev(f) := (f(p_1), f(p_2), \ldots, f(p_{2^n}))\,|f \in \mathcal{A}_n\} = \mathcal{RM}(1,n),$$

es decir, el código de Reed-Muller de orden uno tiene una correspondencia biyectiva con las funciones booleanas afines.

6.1. La no-linealidad.

DEFINICIÓN 6.4. *La no-linealidad, denotada N_f, de una función booleana $f \in \mathcal{B}_n$, es la distancia de Hamming entre f y el conjunto de las funciones afines, es decir,*

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

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

Una propiedad criptográfica deseable en las funciones booleanas es una no-linealidad máxima ([**15**]). El siguiente resultado proporciona una relación entre la transformada de Fourier y la no-linealidad. Los detalles pueden consultarse en [**37**].

TEOREMA 6.5. *Una caracterización de la no-linealidad de una 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. Sea

$$g_a(x) := f(x) + a\cdot x.$$

Analizando las imágenes de la función g_a se obtiene que,

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

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

$$h_a(x) := f(x) + a \cdot x + 1,$$

se tiene la relación,

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

lo cual implica que

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

Por lo tanto,

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

es decir,

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

□

Capítulo 2

Funciones sobre $\mathbb{F}_q^n$, $q = p^m$, p primo

Las funciones bent fueron introducidas por O. S. Rothaus en l976 ([**44**]). Las funciones bent, casi-bent, perfectamente no-lineales y casi perfectamente no-lineales tienen aplicaciones muy importantes en la Teoría de Códigos y Criptografía, por ejemplo, en los sistemas de cifrado de llave privada tipo DES. Sus propiedades las hacen ideales para resistir ataques lineales y diferenciales, por ejemplo en la implementación de una S-caja. Para los lectores interesados en estas definiciones y aplicaciones pueden consultar [**1**] y [**27**]. En el presente trabajo se estudian las funciones mencionadas y son utilizadas para la construcción de códigos lineales, la construcción de esquemas de compartición de secretos y esquemas de autenticación. Este Capítulo inicia definiendo las funciones bent, caracterizadas por su no-linealidad máxima. Posteriormente se generaliza la definición de una función bent y se dan las funciones perfectamente no-lineales, las casi perfectamente no-lineales y las funciones casi-bent (consúltese [**3**], [**12**] y [**15**]).

1. Funciones bent

En esta Sección se introducen las funciones bent. La definición de una función bent así como varias de sus propiedades podemos encontrarlas en gran cantidad de referencias, por ejemplo en [**5**], [**6**], [**34**], [**37**] y [**44**].

DEFINICIÓN 1.1. *Una función $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (booleana), con n par, es llamada bent si $\widehat{\zeta_f}(a) = \pm 2^{\frac{n}{2}}$ para toda $a \in \mathbb{F}_2^n$.*

Recuérdese que $\widehat{\zeta_f}$ es la transformada de Fourier de la función $\zeta_f = (-1)^f$, es decir,

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

Es inmediato de la definición de la transformada de Fourier que una función bent más una función afín es una función bent:

Sean $b, d, a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$, $b + a = d$ y f una función bent. Entonces,

$$\widehat{\zeta_f}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+b\cdot x+c+a\cdot x} = (-1)^c \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+d\cdot x} = \pm 2^{\frac{n}{2}}.$$

TEOREMA 1.2. *(Identidad de Parseval) ([**37**]) Sea $\widehat{\zeta_f}$ la función definida anteriormente. Se tiene la siguiente identidad,*

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

DEMOSTRACIÓN. El resultado se obtiene de modo directo efectuando las operaciones de suma y producto correspondientes. □

Un resultado interesante de las funciones bent es la siguiente:

COROLARIO 1.3. *([**37**]) Las funciones bent tienen no-linealidad máxima.*

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

Es decir, respecto a la distancia de Hamming, las funciones bent están mas alejadas de las funciones lineales, y de la definición de las funciones bent se tiene que esta no-linealidad está dada por

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

TEOREMA 1.4. *([**37**]) Las funciones booleanas*

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

son bent si 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. Sean $c \in \mathbb{F}_2^m$ y $d \in \mathbb{F}_2^n$. 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, ya que de lo contrario h no satisfaría la identidad de Parseval. □

EJEMPLO 1.5. *La función booleana $(x_1, x_2) \mapsto f(x_1, x_2) = x_1x_2 \in \mathcal{B}_2$ 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

$$N_f = 1.$$

Recuérdese que en general el conjunto de las funciones booleanas con n entradas en el dominio es denotado por $\mathcal{B}_n$

EJEMPLO 1.6. *La función booleana*

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

es bent ya que evaluando en la transformada de Fourier todos los elementos de $\mathbb{F}_2^4$, se obtiene,

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

y su no-linealidad es

$$N_f = 6.$$

Utilizando un programa computacional en Maple, se tiene que para $n = 2$ y $n = 4$ en $\mathcal{B}_n$ existen 8 y 896 funciones bent respectivamente. Es un problema abierto conocer la cardinalidad $\mathcal{B}_n$ para valores grandes de n ([**6**]).

Las funciones bent del ejemplo siguiente forman la llamada clase de Maiorana-Mc-Farland ([**34**]).

EJEMPLO 1.7. *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 la función $f : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2$ definida como*

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

es 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,

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

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

Nótese que la suma interior es cero, a menos que $\pi(y) = a$, es decir, $y = \pi^{-1}(a)$, en cuyo caso la suma interior es 2^k. Por consiguiente,

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

lo cual implica que,

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

□

2. Funciones bent vectoriales y perfectamente no-lineales

En esta Sección se introducen las funciones bent y las perfectamente no-lineales con dominio $\mathbb{F}_2^n$ y rango $\mathbb{F}_2^m$, y se da la equivalencia que existe entre ellas así como la existencia de estas funciones para los distintos valores de n y m (véase [**15**]).

DEFINICIÓN 2.1. *Sea $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ una función y $b \in \mathbb{F}_2^m \backslash \{0\}$, $a \in \mathbb{F}_2^n$. Se definen las siguientes relaciones,*

$$L_F(a, b) := \{x \in \mathbb{F}_2^n |\ b \cdot F(x) + a \cdot x = 0\},$$
$$\lambda_F(a, b) := 2\left(|L_F(a, b)| - 2^{n-1}\right),$$
$$\Lambda_F := \textit{sup}_{a,b\neq 0}|\lambda_F(a, b)|.$$

Nótese que $\lambda_F(a, b) = \widehat{\zeta_{b\cdot F}}(a)$, es decir, $\lambda_F(a, b)$ es la transformada de Fourier de la función booleana $b \cdot F$ evaluada en a.

Obsérvese que

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

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

DEFINICIÓN 2.2. *Sea $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Defínase:*

$$D_aF(x) := F(x+a) - F(x), \text{ para cada } 0 \neq a \in \mathbb{F}_2^n,$$
$$(D_aF)^{-1}(b) = \{x \in \mathbb{F}_2^n | F(x+a) - F(x) = b\},$$
$$(\delta_aF)^{-1}(b) := |(D_aF)^{-1}(b)|,$$
$$\Delta_F := sup_{a \neq 0, b} (\delta_aF)^{-1}(b).$$

$D_aF(x)$ es llamada la función diferencia, derivada o incremento de F. En el caso de n par Λ_F puede tener el menor valor $2^{n/2}$ pues ésta es la menor cantidad que pueden alcanzar las funciones booleanas $b \cdot F$ en caso de que alguna de ellas sea bent.

En general para funciones $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se tiene que $\Delta_F \geq 2$ ya que si el conjunto $(D_aF)^{-1}(b) = \{x \in \mathbb{F}_2^n | F(x+a) - F(x) = b\}$ tiene una solución x_1, entonces también tiene la solución $x_1 + a$.

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

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

donde $\mathcal{A}$ es 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 distintas de cero de las funciones coordenada de F y el conjunto de todas las funciones afines. Nótese que para cada $b \in \mathbb{F}_2^m$ se tiene que $b \cdot F$ es una función booleana, luego dado que la no-linealidad de una función booleana f está caracterizada por

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

entonces la no-linealidad de una función vectorial está dada por la relación

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

ya que también es necesario considerar el máximo respecto a las funciones booleanas $b \cdot F$. De la relación anterior se observa que los menores valores de $\text{sup}_{a,b \neq 0} |\lambda_F(a,b)|$ corresponden a una mayor no-linealidad de F.

Ahora se extenderá la definición de función bent $f : \mathbb{F}_2^n \to \mathbb{F}_2$ a funciones 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 2.3. *Sea n par. Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es bent si para toda $0 \neq b \in \mathbb{F}_2^m$ la función booleana*

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

es bent,

es decir,

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

Sea $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ una función bent. Entonces $\lambda_F(a,b) = \pm 2^{n/2}$, para toda $b \neq 0$, y este es el menor valor que puede alcanzar Λ_F, ya que $\lambda_F(a,b) = \widehat{\zeta_{b\cdot F}}(a)$ y $a \cdot F$ es una función bent, luego la no-linealidad de F es máxima y 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 2.4. *(*[**15**]*) Sea $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ una función. Entonces $\Delta_F \geq 2^{n-m}$.*

DEMOSTRACIÓN. Si $a \in \mathbb{F}_2^n$, entonces $\sum_{b\in\mathbb{F}_2^m} (\delta_a F)^{-1}(b) = 2^n$, ya que en la suma se consideran todos los elementos de $\mathbb{F}_2^m$. Afirmamos que existe un elemento $b \in \mathbb{F}_2^m$ tal que $(\delta_a F)^{-1}(b) \geq 2^{n-m}$, pues en caso contrario, es decir, si $(\delta_a F)^{-1}(b) < 2^{n-m}$, para toda $a \neq 0$ y b, por la relación $2^m 2^{n-m} = 2^n$ se tendría que $\sum_{b\in\mathbb{F}_2^m} (\delta_a F)^{-1}(b) < 2^n$, lo cual es una contradicción. Por lo tanto $\Delta_F \geq 2^{n-m}$. □

DEFINICIÓN 2.5. *Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es perfectamente no-lineal (PN) si $\Delta_F = 2^{n-m}$.*

Observación.

1. Si $n < m$, entonces 2^{n-m} no es un entero, por lo que en este caso no se tiene la existencia de funciones perfectamente no-lineales.
2. Si F es una función perfectamente no-lineal, entonces $(\delta_a F)^{-1}(b) = 2^{n-m}$ para toda $a \in \mathbb{F}_2^n$, $a \neq 0$ y toda $b \in \mathbb{F}_2^m$.

La segunda observación es justificada por la desigualdad $(\delta_a F)^{-1}(b) \leq \Delta_F = 2^{n-m}$ y la relación $2^m 2^{n-m} = 2^n$, ya que si para algún par (a,b) se tiene que $(\delta_a F)^{-1}(b) < 2^{n-m}$, entonces $\sum_{b\in\mathbb{F}_2^m} (\delta_a F)^{-1}(b) < 2^n$, lo cual es una contradicción.

Existe una equivalencia entre funciones bent y funciones perfectamente no-lineales. Es de importancia la equivalencia de estas funciones ya que permite considerarlas desde el punto de vista de su no-linealidad o de su forma diferencial, características importantes contra los ataques criptográficos lineales y diferenciales respectivamente ([**1**], [**27**]).

TEOREMA 2.6. *(*[**15**]*) Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es perfectamente no-lineal si y sólo si es bent.*

□

TEOREMA 2.7. *(*[**15**]*) Las funciones bent, $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, existen únicamente para $n \geq 2m$ y n par.*

□

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

En esta Sección se introducen las funciones casi-bent y casi perfectamente no-lineales, se presentan algunas de sus propiedades como su no-linealidad, y se da la relación que existe entre ellas, así como la existencia de estas funciones para los distintos valores de n y m, donde n, m son enteros positivos.

DEFINICIÓN 3.1. *Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es llamada casi perfectamente no-lineal (CPN) si $\Delta_F = 2$.*

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

Una relación que tienen las funciones CPN, F, respecto a Λ_F es la siguiente:

TEOREMA 3.2. *(*[**15**]*) 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 si y sólo si F es casi perfectamente no-lineal y $\lambda_F(\cdot, \cdot)$ toma los tres valores, $\lambda_F(a, b) = \{0, -\Lambda_F, \Lambda_F\}$, $a \in \mathbb{F}_2^n$, $0 \neq b \in \mathbb{F}_2^m$.

□

Con base en la relación anterior es conveniente definir una función casi-bent como sigue.

DEFINICIÓN 3.3. *Una función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es llamada casi-bent si*

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

Es decir, F es casi-bent si y sólo si F es CPN y $\lambda_F(\cdot, \cdot)$ tiene los tres distintos valores, $\lambda_F(a, b) = \{0, -\Lambda_F, \Lambda_F\}$, $a \in \mathbb{F}_2^n$, $0 \neq b \in \mathbb{F}_2^m$.

Más aún, los valores de n y m para funciones casi-bent se restringen y se obtiene una fórmula breve de modo que es posible advertir la no-linealidad máxima de estas funciones.

TEOREMA 3.4. *(*[**15**]*) Si la función $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es casi-bent, entonces n es impar tal que $n = m$, o $n = 2$ y $m = 1$.*

□

Además se tiene:

TEOREMA 3.5. *(*[**15**]*) Si $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ es una función casi-bent y no bent, entonces $m = n$ y n impar. Además $\Lambda_F = 2^{\frac{n+1}{2}}$ si $m = n$.*

□

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 ([**9**]):

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

Las funciones casi-bent al igual que las funciones bent tienen no-linealidad máxima, y la existencia de estas funciones no coincide en los mismos valores de n, a excepción de $n = 2$ y $m = 1$. Puede observarse que la no-linealidad de las funciones bent indican una mayor no-linealidad a comparación de las funciones casi-bent en el respectivo conjunto de funciones booleanas.

El siguiente resultado es de utilidad para un ejemplo de familia de funciones casi-bent.

TEOREMA 3.6. *([**40**]) Sea G un subcampo con 2^s elementos de $\mathbb{F}_{2^n}$, $s = (k, n)$. Entonces*

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

DEMOSTRACIÓN. Si $x_1 \in \alpha(G \setminus \{0\})$, entonces $x_1 = \alpha e, e \in (G \setminus \{0\})$, 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, $x_1^{2^k-1} = \alpha^{2^k-1}$. Las relaciones anteriores también son equivalencias y de aquí se tiene el resultado. □

TEOREMA 3.7. *([**40**]) Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = x^{2^k+1}$ y $k \in \mathbb{N}$ tal que $s = (k, n)$. Entonces $\Delta_F = 2^s$. Si $\frac{n}{s}$ es impar, luego*

$$d_H(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wF(x)), \mathcal{A}) = 2^{n-1} - 2^{\frac{n+s}{2}-1},$$

para toda $w \in \mathbb{F}_{2^n}^*$, donde $\mathcal{A}$ es el conjunto de las funciones booleanas afines.

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

Sean $x_1 \neq x_2$ dos soluciones. Entonces

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

o de modo equivalente

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

Por otro lado 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, luego tiene exactamente $2^s - 1$ soluciones en $\mathbb{F}_{2^n}^*$ ([**28**]). Sean x_0, x_i soluciones distintas de $(x + a)^{2^k-1} + x^{2^k-1} = b$, por las relaciones anteriores y el Teorema 3.6, $x_0 + x_i \in a(G \setminus \{0\})$, de aquí $x_i \in x_0 + a(G \setminus \{0\})$ lo cual implica, $(\delta_a F)^{-1}(b) = 2^s$ o 0. Nótese que al menos existe un elemento b tal que $\delta_a F^{-1}(b) = 2^s$, por lo que $\Delta_F = 2^s$. Como $n/(n, k)$ es impar, entonces se tiene que $(2^k + 1, 2^n - 1) = 1$, y de aquí $F(x) = x^{2^k+1}$ 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 ([**34**]), se tiene que

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

así,

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

Sea $y\in\mathbb{F}_{2^n}^*$ y 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 el conjunto $\{x\in\mathbb{F}_{2^n}^*|\ x^{2^k-1}=y^{2^k-1}\}\cup\{0\}$, entonces por el Teorema 3.6, el núcleo de H_y es el conjunto yG, lo que implica que E_y tiene dimensión $n-s$. También para cada $y\neq 0$,

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

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 carácter 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 de modo equivalente, 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 $\mathbb{F}_{2^n}$. Ahora 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,

$$\begin{aligned}&(\lambda_F(a,w))^2\\ =\ &2^n+\sum_{y\in\mathbb{F}_{2^n}^*}(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}2^s\sum_{\beta\in E_y}(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(w\beta)}\\ =\ &2^n+\sum_{y\in Y\setminus\{0\}}(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}2^s2^{n-s}\\ =\ &2^n+2^n\sum_{y\in Y\setminus\{0\}}(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)+Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}.\end{aligned}$$

El espacio lineal Y tiene 2^s elementos y la función $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})$ es lineal en Y ([**40**]). Ya que $F(x)$ es una permutación, luego $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}$ es un caracter. Como el número de caracteres es finito, entonces existe $a\in\mathbb{F}_{2^n}$ tal que los caracteres $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ay)}$ y $(-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(wy^{2^k+1})}$ son iguales. Al elegir $a\in\mathbb{F}_{2^n}$ de modo conveniente, 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. □

En particular, si $s=1$, entonces F es una función casi-bent.

EJEMPLO 3.8. *Sea n un número natural impar y $F(x) = x^{2^k+1}$, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, donde k es un entero tal que $(k, n) = 1$. Entonces F es casi-bent.*

Observación. Si $\mathbb{F}_{p^m}$ es un campo finito con p^m elementos y r un entero positivo tal que $(r, p^m - 1) = 1$, entonces la función $f(y) = y^r$ es una permutación en $\mathbb{F}_{p^m}$ ([**28**]). Con base en esta observación la función casi-bent dada en el ejemplo anterior es también una permutación ya que $(k, n) = 1$ implica $(2^k + 1, 2^n - 1) = 1$.

4. Funciones bent y perfectamente no-lineales sobre campos de característica impar

En esta Sección se introducen las funciones $F : \mathbb{F}_q^n \to \mathbb{F}_q$, q impar, y de manera natural se extiende la definición de una función bent a estas funciones. En particular, si $n = 1$, se tienen funciones $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, $q = p^m$, $p \neq 2$, y las funciones bent en este caso pueden ser utilizadas para la construcción de esquemas de compartición de secretos y esquemas de autenticación ([**7**], [**9**]).

Considerando la definición de caracteres aditivos sobre un campo finito de característica impar se tiene la siguiente definición de la transformada de Fourier de una función:

DEFINICIÓN 4.1. *(*[**16**]*) La transformada de Fourier de la función $f : \mathbb{F}_q^n \to \mathbb{F}_q$, $q = p^m$, $p \neq 2$, es la función con valores complejos $c_{f,\chi}(\cdot) : \mathbb{F}_q^n \to \mathbb{C}$, dada 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 distinto del trivial de $\mathbb{F}_q$, $\lambda \cdot x$ el producto interno usual y $\mathbb{F}_q^n$ es el producto cartesiano del campo finito $\mathbb{F}_q$.

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 $a \in \mathbb{F}_q^*$, χ_a definido en la Sección 2 del Capítulo 1.

Ahora se generaliza la definición de una función bent de la siguiente manera:

DEFINICIÓN 4.2. *(*[**16**]*) Sea $q = p^m$, p primo y m un entero positivo. Se dice que la función $f : \mathbb{F}_q^n \to \mathbb{F}_q$ es bent si cada uno sus coeficientes de Fourier tiene magnitud $q^{n/2}$ para cualquier caracter aditivo χ distinto del 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 $\chi \neq \chi_0$.

Si se consideran funciones $F : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^m$, $p \neq 2$, 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 algúna $a \in \mathbb{F}_q^*$, con $\lambda \in \mathbb{F}_q$. De lo anterior se tiene que F es bent si

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

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

De igual modo que en la Definición 2.2 del Capítulo 2, se define $D_a f(x) = f(x + a) - f(x)$, $a, x \in \mathbb{F}_q^n$, tal que $a \neq 0, q = p^m$.

DEFINICIÓN 4.3. *([**16**]) La función $f : \mathbb{F}_q^n \to \mathbb{F}_q$ es perfectamente no-lineal si para toda $a \in \mathbb{F}_q^n \setminus \{0\}$, $b \in \mathbb{F}_q$,*

$$|(D_a)^{-1}(b)| = q^{n-1}.$$

Las funciones perfectamente no-lineales y las funciones bent son equivalentes:

TEOREMA 4.4. *([**16**]) Una función $f : \mathbb{F}_q^n \to \mathbb{F}_q$ es perfectamente no-lineal si y sólo si f es bent.*

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

$\Rightarrow$) Si f es perfectamente no-lineal, entonces

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

donde $z = x_2 - x_1$, por consiguiente, f es bent.

$\Leftarrow$) Sea f una función bent, $0 \neq a \in \mathbb{F}_q$, $z \in \mathbb{F}_q^n$, y

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

Entonces,

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

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

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

la igualdad (I) se expresa como:

$$AB = q^n I, \qquad (II)$$

donde

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

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

Multiplicando por la matriz

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

en ambos lados de la relación (II), se obtiene

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

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

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 distinto del trivial, entonces

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

para cualquier caracter χ distinto del trivial, ya que si suponemos sin pérdida de generalidad $|c_{f,\chi_1}(\lambda)| = q^{n/2}$, entonces al considerar el caracter χ_1 en forma similar a la prueba del Teorema 4.4, f es perfectamente no-lineal, y de aquí nuevamente por el resultado anterior f es bent tal que $|c_{f,\chi_a}(\lambda)| = q^{n/2}$ para toda $a \in \mathbb{F}_q^*$.

EJEMPLO 4.5. *(***[16]**,**[55]***) 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.*

Probemos el primer caso del Ejemplo 4.5.

DEMOSTRACIÓN. Sea $q = p^n$, p primo impar. El polinomio $(x+1)^{p^k+1} - x^{p^k+1} = x^{p^k} + x + 1$ es una permutación sobre $\mathbb{F}_q$ si y sólo si $x^{p^k} + x$ tiene una única raíz en $\mathbb{F}_q$ o de modo equivalente si $x^{p^k-1} \neq -1$ para toda $x \in \mathbb{F}_q^*$. Considérese ahora un elemento primitivo α de $\mathbb{F}_q$. Entonces $\alpha^{i(p^k-1)} \neq \alpha^{(q-1)/2}$ para cualquier entero i. Esta desigualdad ocurre si y sólo si la congruencia $i(p^k-1) \equiv (p^n-1)/2$ mód p^n-1 no tiene una solución entera i. Considérese ahora la equivalencia, $iu \equiv v$ mód m, la cual tiene solución si y sólo si $(u,m)|v$, luego de esto podemos afirmar que el polinomio $(x+1)^{p^k+1} - x^{p^k+1}$ es una permutación si y sólo si $(p^k-1, p^n-1) \nmid (p^n-1)/2$ o de modo equivalente si y sólo si $p^{(k,n)} - 1 \nmid (p^n-1)/2$, es decir, si el orden de p^d-1 es mayor o igual a el orden de p^n-1, donde $d = (k,n)$, pero ya que $p^n - 1 = (p^d-1)(1+p^d+p^{2d}+\cdots+p^{((e/d)-1)d})$, entonces $n/(k,n)$ es un número impar. Nótese que para cualquier $a \in \mathbb{F}_q^*$, $(x+a)^t - x^t = a^t(x/a+1)^t - (x/a)^t$, t número natural, luego, si una de las expresiones es una permutación, la otra también lo es, y de aquí se tiene el resultado. □

Capítulo 3

Funciones bent sobre anillos

La definición de las funciones bent así como algunas propiedades de los anillos de Galois son recordadas en este Capítulo. En la primera Sección se definen las funciones bent sobre los anillos de enteros modulares (veáse [**32**]), en la segunda y tercera Sección se definen los anillos de Galois y las funciones bent sobre estos anillos. Para mayores detalles consúltese por ejemplo [**4**] y [**53**].

En la tercera Sección resalta la construcción de una familia de funciones bent la cual es la base para la determinación de una clase de códigos de autenticación.

1. Funciones bent sobre anillos de enteros modulares

En esta Sección se dan ejemplos de funciones bent sobre el $\mathbb{Z}_q$-módulo, $\mathbb{Z}_q^n$, cuando n es un BN entero positivo par, y cuando n es impar con $q \not\equiv 2$ mód 4 ([**32**]), ya que en el caso, $q \equiv 2$ mód 4 y n impar, no se tiene la existencia de estas funciones ([**32**]). Al igual que para los campos finitos en donde se generaliza la definición de una función bent, en esta Sección se hace sobre los anillos de enteros modulares.

DEFINICIÓN 1.1. *(*[**32**]*) Sean $n \geq 1$ y $q > 1$ enteros y $\mathbb{Z}_q$ el anillo de enteros módulo q. Sea f una función con valores complejos definida en $\mathbb{Z}_q^n$, donde $\mathbb{Z}_q^n$ denota el conjunto de n-tuplas módulo q, q un número natural. La trasformada de Fourier de f se define como*

$$\widehat{f}(a) := \sum_{x \in \mathbb{Z}_q^n} f(x) w^{-a \cdot x},\ a \in \mathbb{Z}_q^n,$$

donde $w = e^{2\pi i/q}$ es una raíz primitiva q-ésima de la unidad e $i = \sqrt{-1}$.

Nótese que la definición de la transformada de Fourier para estas funciones es una generalización natural respecto a las funciones booleanas.

DEFINICIÓN 1.2. *(*[**32**]*) Una función $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ es llamada bent si todas las imágenes de la transformada de Fourier de la función $\xi_{wf} = w^f$ tienen magnitud $q^{\frac{n}{2}}$, es decir,*

$$|\widehat{\xi_{wf}}(a)| = |\sum_{x \in \mathbb{Z}_q^n} w^{f(x) - a \cdot x}| = q^{\frac{n}{2}},$$

n entero positivo, para toda $a \in \mathbb{Z}_q^n$

TEOREMA 1.3. *([**32**]) Sean $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ y $g : \mathbb{Z}_q^n \to \mathbb{Z}_q$ funciones bent. Entonces la función $f + g : \mathbb{Z}_q^{m+n} \to \mathbb{Z}_q$ definida por*

$$(f + g)(x_1, x_2, \ldots, x_{m+n}) := f(x_1, x_2, \ldots, x_m) + g(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$$

$\forall\ (x_1, x_2, \ldots, x_{m+n}) \in \mathbb{Z}_q^{m+n}$ *es una función bent.*

DEMOSTRACIÓN. La prueba es básicamente la misma que en el caso de $\mathbb{F}_2^n$. □

El resultado anterior solo enuncia una implicación a diferencia del Teorema 1.4 que trata el caso sobre $\mathbb{F}_2^n$.

En el caso de funciones booleanas la suma de una función bent más una función afín es una función bent, este resultado es generalizado para funciones sobre enteros modulares:

Si $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ es una función bent, entonces la función $f_{a,b} : \mathbb{Z}_q^n \to \mathbb{Z}_q$ definida por

$$f_{a,b}(x) := f(x) + a \cdot x + b,$$

$a \in \mathbb{Z}_q^n$, $b \in \mathbb{Z}_q$, es una función bent. La prueba es directa utilizando la definición de la transformada de Fourier.

TEOREMA 1.4. *([**32**]) Sea $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ una función bent. Entonces las imágenes de la transformada de Fourier de γ^f tienen magnitud $q^{\frac{n}{2}}$, para toda γ una raíz primitiva q-ésima compleja de la unidad, es decir, $|\widehat{\xi_{\gamma f}}(a)| = q^{\frac{n}{2}}, \forall a \in \mathbb{Z}_q^n$.*

DEMOSTRACIÓN. Si γ es una raíz primitiva q-ésima compleja de la unidad, entonces $\gamma = w^r$ (recordar que $w = e^{2\pi i/q}$ es una raíz primitiva q-ésima de la unidad e $i = \sqrt{-1}$), para algún número entero r, $0 < r < q$, $(r, q) = 1$. Por otro lado existen $\mathbb{Q}$-automorfismos σ y τ tal que $\sigma(w) = \gamma$ y $\tau(z) = \bar{z}$, donde $\bar{z}$ es el conjugado complejo de z. Ya que f es una función bent, entonces el entero algebraico $\sum_{x \in \mathbb{Z}_q^n} w^{f(x)-a\cdot x}$ tiene magnitud igual a $q^{\frac{n}{2}}$, es decir,

$$\sum_{x \in \mathbb{Z}_q^n} w^{f(x)-a\cdot x} \tau\Big(\sum_{x \in \mathbb{Z}_q^n} w^{f(x)-a\cdot x}\Big) = q^n.$$

Como los $\mathbb{Q}$-automorfismos conmutan, entonces

$$\sigma\Big(\sum_{x \in \mathbb{Z}_q^n} w^{f(x)-a\cdot x}\Big)\tau\Big(\sigma\Big(\sum_{x \in \mathbb{Z}_q^n} w^{f(x)-a\cdot x}\Big)\Big) = q^n,$$

o sea,

$$\Big|\sum_{x \in \mathbb{Z}_q^n} \gamma^{f(x)-a\cdot x}\Big| = q^{n/2},$$

de donde se concluye la prueba. □

Como consecuencia del Teorema 1.4, si r es primo relativo con q y f es una función bent, entonces, rf, es una función bent.

Las funciones bent sobre enteros modulares existen para n par, y para n impar con $q \not\equiv 2$ mód 4. La prueba de estos casos serán considerados dependiendo del valor de q y n :

Caso 1: para n par y cualquier entero q mayor que 1.

Caso 2: para n impar tal que

$$q = \begin{cases} q \equiv 1, 3 \text{ mód } 4 \ (q \text{ impar}) \\ q \equiv 0 \text{ mód } 4 = \begin{cases} q = 2^k, & k > 1, k \text{ par} \\ q = 2^k, & k > 1, k \text{ impar} \\ q = 2^k r, & k > 1, r \text{ impar} \end{cases} \end{cases} .$$

El siguiente resultado afirma la existencia de las funciones bent cuando n es par y q cualquier entero mayor que 1:

Sean q, k enteros positivos y $n = 2k$. Considérese $x = (x_1, x_2)$, donde $x_1, x_2 \in \mathbb{Z}_q^k$, π una permutación arbitraria de los elementos de $\mathbb{Z}_q^k$ y una función arbitraria $g : \mathbb{Z}_q^k \to \mathbb{Z}_q$. Con base en la notación anterior se tiene el siguiente resultado:

TEOREMA 1.5. *([**32**]) Sea $f : \mathbb{Z}_q^k \times \mathbb{Z}_q^k \to \mathbb{Z}_q$ una función definida por*

$$f(x) := x_2 \cdot \pi(x_1) + g(x_1), \qquad \forall\, x \in \mathbb{Z}_q^n.$$

Entonces f es una función bent.

DEMOSTRACIÓN. La transformada de Fourier de $\xi_{wf} = w^f$ está dada por

$$\widehat{\xi}_{wf}(a) = \sum_{x \in \mathbb{Z}_q^n} w^{f(x) - a \cdot x}.$$

Si $a = (a_1, a_2) \in \mathbb{Z}_q^n$, $a_1, a_2 \in \mathbb{Z}_q^k$, entonces

$$\widehat{\xi}_{wf}(a) = \sum_{x \in \mathbb{Z}_q^n} w^{f(x) - a \cdot x} = \sum_{x \in \mathbb{Z}_q^n} w^{x_2 \cdot \pi(x_1) + g(x_1) - a \cdot x}$$

$$= \sum_{x_1 \in\, Z_q^k} w^{g(x_1) - a_1 \cdot x_1} \sum_{x_2 \in\, Z_q^k} w^{x_2 \cdot (\pi(x_1) - a_2)}.$$

Nótese que la suma interior es igual a cero a menos que $\pi(x_1) = a_2$, es decir, $x_1 = \pi^{-1}(a_2)$, luego

$$\widehat{\xi}_{wf}(a) = q^k w^{g(\pi^{-1}(a_2)) - a_1 \cdot \pi^{-1}(a_2)}.$$

Por lo tanto

$$|\widehat{\xi}_{wf}(a)| = q^k.$$

□

Las funciones bent del Teorema anterior son conocidas como la clase Maiorana-McFarland.

Por el Teorema 1.3 se tiene que dada una función bent sobre $\mathbb{Z}_q$ se pueden obtener funciones bent sobre $\mathbb{Z}_q^n$ para cualquier valor de n. Por lo tanto en el siguiente resultado se tiene la construcción de funciones bent para el caso $q \equiv 1, 3$ mód 4:

TEOREMA 1.6. *([**32**]) Sea q impar y f una función sobre $\mathbb{Z}_q$ dada por*

$$f(k) := k^2 + ck \qquad \forall\, k \in \mathbb{Z}_q.$$

Entonces f es bent para toda c en $\mathbb{Z}_q$.

DEMOSTRACIÓN. Considérese la relación

$$k^2 + (c-\lambda)k = (k + a(c-\lambda))^2 - a^2(c-\lambda)^2,\ \lambda \in \mathbb{Z}_q.$$

donde $a = 2^{-1}$. La transformada de Fourier de la función $\xi_{wf} = w^f$ está dada por

$$\widehat{\xi}_{wf}(\lambda) = \sum_{k=0}^{q-1} w^{k^2+ck-\lambda k} \qquad \forall\, \lambda \in \mathbb{Z}_q,$$

luego

$$\widehat{\xi}_{wf}(\lambda) = \sum_{k=0}^{q-1} w^{(k+a(c-\lambda))^2 - a^2(c-\lambda)^2} = \frac{1}{2} w^{-a^2(c-\lambda)^2} \sum_{k=0}^{q-1} w^{(k+a(c-\lambda))^2}.$$

Por sumas cuadráticas de Gauss ([**33**]), se tiene

$$\sum_{k=0}^{q-1} w^{(k+a(c-\lambda))^2} = q^{1/2}, \quad \text{si } q \equiv 1 \text{ mód } 4,$$

y

$$\sum_{k=0}^{q-1} w^{(k+a(c-\lambda))^2} = iq^{1/2}, \quad \text{si } q \equiv 3 \text{ mód } 4.$$

Entonces

$$|\widehat{\xi}_{wf}(\lambda)| = q^{1/2}.$$

□

Sea $r \geq 2$ un entero y sea $\mathbb{Z}_q^{(r)} := \{s \in \mathbb{Z}_q |\ 0 \leq s \leq r-1\}$, π una permutación de $\mathbb{Z}_q^{(r)}$ y g una función con valores enteros que está definida en $\mathbb{Z}_q^{(r)}$. Si $q = r^2$ y r es una potencia de 2, entonces es posible expresar q en la forma 2^k, k par, de aquí, utilizando las definiciones anteriores, el siguiente resultado proporciona una construcción de funciones bent cuando n es impar y $q = 2^k$, k par:

TEOREMA 1.7. *([**32**]) Sea $q = r^2$, $r > 1$ entero, y la función f definida por*

$$f(s) := rs_1\pi(s_2) + g(s_2),\ \textit{para toda } s \textit{ en } \mathbb{Z}_q,$$

donde s_1, $s_2 \in \mathbb{Z}_q^{(r)}$, son tales que $s = rs_1 + sk_2$. Entonces f es una función bent.

DEMOSTRACIÓN. Si $s' \in \mathbb{Z}_q$ es un elemento fijo y $s'_1, s'_2 \in \mathbb{Z}_q^{(r)}$ son tales que $s' = rs'_1 + s'_2$, entonces

$$\begin{aligned}
&\widehat{\xi}_{wf}(s') \\
= &\sum_{k=0}^{q-1} w^{f(s)-s's} = \sum_{s_1,s_2\in\mathbb{Z}_q^{(r)}} w^{rs_1\pi(s_2)+g(s_2)-(rs'_1+s'_2)(rs_1+s_2)} \\
= &\sum_{s_1,s_2\in\mathbb{Z}_q^{(r)}} w^{rs_1\pi(s_2)+g(s_2)-r^2s'_1s_1-rs'_1s_2-rs'_2s_1-s'_2s_2} \\
= &\sum_{s_2=0}^{r-1} w^{g(s_2)-rs'_1s_2-s'_2s_2} \sum_{s_1=0}^{r-1} w^{rs_1(\pi(s_2)-s'_2)}.
\end{aligned}$$

Nótese que la suma interior es igual a cero a menos que $\pi(s_2) = s'_2$, es decir, $s_2 = \pi^{-1}(s'_2)$, luego,

$$\widehat{\xi}_{wf}(s') = rw^{g(\pi^{-1}(s'_2))-rs'_1\pi^{-1}(s'_2)-s'_2\pi^{-1}(s'_2)}.$$

Por lo tanto $|\widehat{\xi}_{wf}(s')| = r$. □

Sea $x \in \mathbb{Z}_q$ y su representación binaria

$$x = \sum_{j=0}^{2r} x_j 2^j,$$

donde $j = 0, 1, 2, \ldots, 2r$ son los dígitos de la representación binaria de x. Considérense las sumas parciales y_1, y_2, y_3, dadas por

$$y_1 = \sum_{j=0}^{r-1} x_j 2^j, \quad y_2 = x_k 2^r, \quad y_3 = \sum_{j=k+1}^{2r} x_j 2^j, \text{ respectivamente,}$$

g una función arbitraria con valores enteros definidos en $\mathbb{Z}_q$ y h una función definida por

$$h(z) := 4cz + 2z, \qquad z \in \{0, 1\},$$

donde c es 0 o 1.

Utilizando las definiciones anteriores se tiene la siguiente construcción de funciones bent para el caso $q = 2^k$, $k > 1$, k impar:

TEOREMA 1.8. *([**32**]) Sea $q = 2^{2r+1}$, $r > 0$, entero. Entonces la función f sobre $\mathbb{Z}_q$ definida por*

$$f(x) := g(y_1) + y_1 x + \frac{q}{8} h(x_k), \qquad x \in \mathbb{Z}_q,$$

es una función bent.

DEMOSTRACIÓN. Sea $x' \in \mathbb{Z}_q$ fija, y ${x'}_j, j = 0, 1, \ldots, 2k$, los dígitos binarios en la expansión base 2 de x', es decir,

$$x' = \sum_{j=0}^{2k} {x'}_j 2^j.$$

Si ${y'}_1$, ${y'}_2$ y ${y'}_3$ son tales que ${y'}_1 = \sum_{j=0}^{k-1} {x'}_j 2^j$, ${y'}_2 = {x'}_k 2^k$ y ${y'}_3 = \sum_{j=k+1}^{2k} {x'}_j 2^j$, entonces,

$$\begin{aligned} x'x &= y_1x' + y_2({y'}_1 + {y'}_2) + y_3{y'}_1 + y_2{y'}_3 + y_3 + {y'}_2 + y_3{y'}_3 \\ x'x &\equiv y_1x' + y_2({y'}_1 + {y'}_2) + y_3{y'}_1 \text{ mód } q, \end{aligned}$$

y

$$\widehat{\xi}_{wf}(x') = \sum_{x=0}^{q-1} w^{f(x)-x'x} = \sum_{x_0} \cdots \sum_{x_{k-1}} w^{g(y_1)+y_1^2-y_1x'}$$
$$\sum_{x_k} w^{q/8h(x_k)-y_2({y'}_1+{y'}_2)+y_1y_2} \sum_{x_{k+1}} \cdots \sum_{x_{2k}} w^{y_3(y_1-{y'}_1)}.$$

Nótese que la suma interior es igual a cero, excepto si $y_1 = {y'}_1$, por lo que

$$\widehat{\xi}_{wf}(x') = 2^k w^{g({y'}_1)+{{y'}_1}^2-{y'}_1x'} \sum_{x_k} w^{q/8h(x_k)-{y'}_2y_2}.$$

Sea $\delta = w^{q/8} = e^{2\pi i/8}$. Como $w^{q/2} = -1$ y $2^{2k} = \frac{q}{2}$, entonces,

$$\begin{aligned} \sum_{x_k} w^{q/8h(x_k)-{y'}_2y_2} &= \sum_{x_k=0}^{1} w^{q/8(c4x_k+2x_k)-2^k2^kx_k{x'}_k} \\ = \sum_{x_k=0}^{1} (-1)^{cx_k}\delta^{2x_k} w^{-2^{2k}x_k{x'}_k} &= \sum_{x_k=0}^{1} (-1)^{cx_k}\delta^{2x_k} w^{q/2(-x_k{x'}_k)} \\ = \sum_{x_k=0}^{1} \delta^{2x_k}(-1)^{x_k(c-{x'}_k)} &= 1 + \delta^2(-1)^{c-{x'}_k}. \end{aligned}$$

Por otro lado $1 + \delta^2 = 2^{1/2}\delta$ y $1 - \delta^2 = \delta^6 2^{1/2}\delta$, luego,

$$\widehat{\xi}_{wf}(x') = 2^k w^{g({y'}_1)+{{y'}_1}^2-{y'}_1x'} 2^{1/2} w^{q/8} = q^{1/2} w^{g({y'}_1)+{{y'}_1}^2-{y'}_1x'+q/8},$$

o

$$2^k w^{g({y'}_1)+{{y'}_1}^2-{y'}_1x'} 2^{1/2} (w^{q/8})^7 = q^{1/2} w^{g({y'}_1)+{{y'}_1}^2-{y'}_1x'+7q/8}.$$

Por lo tanto, $|\widehat{\xi}_{wf}(x')| = q^{1/2}$. □

Como último caso a tratar en la construcción de funciones bent se considera $q = 2^k r$, $k > 1$, r impar:

Si $q = 2^k r$, $k > 1$, r impar ($r > 1$), ya que $(2^{k-1}, r) = 1$, existen enteros a_0 y b_0 tales que $a_0 2^{k-1} - b_0 r = 1$. Sea

$$A := \{(a_0 + lr, b_0 + l2^{k-1}) |\ l \in \mathbb{Z}\}.$$

Obsérvese que existe

$$(e, v) \in A, \tag{I}$$

tal que

$$0 < e < r,\ 0 < v < 2^{k-1}, e, v \text{ enteros.} \tag{II}$$

Por otro lado, sea $r > 1$ un entero impar, $q = 2^k r$, (e, v) como en (I) y en (II). Considérese la función $g : \mathbb{Z}_{2^k} \to \mathbb{Z}_q$ definida por

$$g(l) := rh(l) + 2^{k-2}(r+1)^2 e^2 l^2 \qquad \forall\, l \in \mathbb{Z}_{2^k},$$

y sea $h : \mathbb{Z}_{2^k} \to \mathbb{Z}_{2^k}$ una función.

Utilizando la notación anterior se tiene el siguiente resultado:

TEOREMA 1.9. *([**32**]) Sea g, definida anteriormente, y f la función sobre $\mathbb{Z}_q^1$ definida por*

$$f(l) := g(l_2) + 2^k(l_1^2 + el_1 l_2) \qquad \forall\, l \in \mathbb{Z}_q,$$

donde para cada l los números enteros l_1 y l_2 son tales que

$$l = 2^k l_1 + l_2, \qquad 0 \le l_1 < r, \quad 0 \le l_2 < 2^k.$$

Entonces f es una función bent.

DEMOSTRACIÓN. Se tiene que

$$\begin{aligned}
\widehat{\xi}_{wf}(\lambda) &= \sum_{k=0}^{q-1} w^{f(l)-\lambda l} = \sum_{l_1, l_2} w^{g(l_2)+2^k(l_1^2+el_1l_2)-\lambda 2^k l_1 - \lambda l_2} \\
&= \sum_{l_2=0}^{2^k-1} w^{g(l_2)-\lambda l_2} \sum_{l_1=0}^{r-1} w^{2^k(l_1^2 - l_1(\lambda - el_2))} \\
&= \sum_{l_2=0}^{2^k-1} w^{g(l_2)-\lambda l_2} \sum_{l_1=0}^{r-1} w^{2^k(l_1 - \frac{1}{2}(\lambda - el_2))^2 - \frac{1}{4}2^k(\lambda - el_2)^2} \\
&= \sum_{l_2=0}^{2^k-1} w^{g(l_2)-\lambda l_2 - \frac{1}{4}2^k(\lambda - el_2)^2} \sum_{l_1=0}^{r-1} w^{2^k(l_1 - \frac{1}{2}(\lambda - el_2))^2}.
\end{aligned}$$

Sea $a = \frac{r+1}{2} = \frac{1}{2}r + \frac{1}{2}$. Como

$$w^{2^k(\frac{1}{2}r + \frac{1}{2})} = w^{\frac{1}{2}2^k r + 2^k \frac{1}{2}} = w^{2^k \frac{1}{2}},$$

entonces

$$\widehat{\xi}_{wf}(\lambda) = \sum_{l_2=0}^{2^k-1} w^{g(l_2)-\lambda l_2 - 2^k a^2(\lambda - e l_2)^2} \sum_{l_1=0}^{r-1} w^{2^k(l_1 - a(\lambda - e l_2))^2}.$$

Utilizando las sumas de Gauss ([**33**]),

$$\widehat{\xi}_{wf}(\lambda) = \alpha r^{1/2} \sum_{l_2=0}^{2^k-1} w^{g(l_2)-\lambda l_2} w^{-2^k a^2(\lambda - e l_2)^2},$$

donde,

$$\begin{array}{lll} \alpha = 1 & \text{si} & r \equiv 1 \text{ mód } 4 \\ \alpha = i & \text{si} & r \equiv 3 \text{ mód } 4 \end{array}.$$

Ahora por la definición de g se tiene que

$$\widehat{\xi}_{wf}(\lambda) = \alpha r^{1/2} \sum_{l_2=0}^{2^k-1} w^{rh(l_2)+2^{k-2}(r+1)^2(\frac{1+vr}{2^{k-1}})^2 l_2^2 - \lambda l_2} w^{-2^k a^2(\lambda - (\frac{1+vr}{2^{k-1}})l_2)^2},$$

y simplificando:

$$\widehat{\xi}_{wf}(\lambda) = \alpha r^{1/2} w^{-2^k a^2 \lambda^2} \sum_{l_2=0}^{2^k-1} w^{rh(l_2) - r\lambda' l_2},$$

donde $\lambda' \equiv -(vr^2 + 2vr + v + r + 2)\lambda$ mód 2^k. Como h es bent, entonces

$$|\sum_{l_2=0}^{2^k-1} w^{rh(l_2) - r\lambda' l_2}| = 2^{k/2},$$

y por lo tanto,

$$|\widehat{\xi}_{wf}(\lambda)| = (2^k r)^{1/2}.$$

□

2. Anillos de Galois

En esta Sección se definen los anillos de Galois y enuncian sus características mas importantes (para mayores detalles consúltese [**53**]).

Sea p un número primo y $s > 1$ un entero. Considérese el anillo de polinomios con coeficientes los enteros modulares $\mathbb{Z}_{p^s}$, es decir, $\mathbb{Z}_{p^s}[x]$.

DEFINICIÓN 2.1. *([**53**]) Sea $f(x)$ un polinomio mónico en $\mathbb{Z}_{p^s}[x]$. Si $\bar{f}(x)$ es irreducible (primitivo) en $\mathbb{F}_p[x]$, entonces $f(x)$ es llamado un polinomio mónico básico irreducible (primitivo) en $\mathbb{Z}_{p^s}[x]$, donde $\bar{*}$ indica la reducción módulo p.*

Sea $\mathbb{F}_p$ el campo finito con p elementos.

LEMA 2.2. *([**53**]) Sean $f_1(x)$ y $f_2(x)$ dos polinomios en $\mathbb{Z}_{p^s}[x]$. Entonces $f_1(x)$ y $f_2(x)$ son coprimos en $\mathbb{Z}_{p^s}[x]$ si y sólo si $\overline{f}_1(x)$ y $\overline{f}_2(x)$ lo son en $\mathbb{F}_p[x]$.*

□

LEMA 2.3. *(Lema de Hensel)(*[**53**]*) Sea $f(x)$ un polinomio mónico en $\mathbb{Z}_{p^s}[x]$ y supóngase que*

$$\overline{f}(x) = g_1(x)g_2 \text{ en } \mathbb{F}_p[x],$$

donde $g_1(x)$ y $g_2(x)$ son polinomios mónicos coprimos en $\mathbb{F}_p[x]$. Entonces existen polinomios mónicos coprimos $f_1(x)$ y $f_2(x)$ en $\mathbb{Z}_{p^s}[x]$ tal que

$$f(x) = f_1(x)f_2(x) \text{ en } \mathbb{Z}_{p^s}[x],$$

y $\overline{f}_1(x) = g_1(x)$, $\overline{f}_2(x) = g_2(x)$.

□

TEOREMA 2.4. *(*[**53**]*) Sea $m \geq 1$ un entero. Entonces existe un polinomio mónico básico irreducible (primitivo) de grado m en $\mathbb{Z}_{p^s}[x]$ divisor de $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$.*

DEMOSTRACIÓN. Dado $m \geq 1$, existe un polinomio mónico irreducible (primitivo) $f_p(x)$ de grado m sobre $\mathbb{F}_p$ tal que divide al polinomio $x^{p^m-1} - 1$ en $\mathbb{F}_p[x]$ (ver [**35**]). Sea

$$g_p(x) = \left(x^{p^m-1} - 1\right) / f_p(x).$$

Entonces

$$x^{p^m-1} - 1 = f_p(x)g_p(x) \text{ en } \mathbb{F}_p[x].$$

Como $x^{p^m-1} - 1$ no tiene raíces múltiples, $f_p(x)$ y $g_p(x)$ son coprimos en $\mathbb{F}_p[x]$, luego por el Lema de Hensel existen polinomios mónicos $f(x)$ y $g(x)$ en $\mathbb{Z}_{p^s}[x]$ tales que

$$x^{p^m-1} - 1 = f(x)g(x) \text{ en } \mathbb{Z}_{p^s}[x],$$

y además $\overline{f}(x) = f_p(x)$, $\overline{g}(x) = g_p(x)$. Como el grado de $f(x)$ es igual al grado de $f_p(x)$, $f(x)$ es el polinomio buscado. □

DEFINICIÓN 2.5. *(*[**53**]*) El anillo de Galois $GR(p^s, m)$ se define como*

$$GR(p^s, m) := \mathbb{Z}_{p^s}[x]/\left\langle h(x)\right\rangle,$$

donde $h(x)$ es un polinomio mónico básico irreducible (primitivo) de grado m sobre $\mathbb{Z}_{p^s}$ y $\langle h(x)\rangle$ es el ideal de $\mathbb{Z}_{p^s}[x]$ generado por $h(x)$.

Considérese la función

$$\begin{array}{rccc} \gamma: & \mathbb{Z}_{p^s}[x]/\left\langle h(x)\right\rangle & \to & \mathbb{F}_p[x]/\left\langle \overline{h}(x)\right\rangle \\ & a_0 + \cdots + a_{m-1}x^{m-1} + \left\langle h(x)\right\rangle & \to & \overline{a}_0 + \cdots + \overline{a}_{m-1}x^{m-1} + \left\langle \overline{h}(x)\right\rangle \end{array}$$

donde $a_0, \ldots, a_{m-1} \in \mathbb{Z}_{p^s}$ y $\bar{*}$ indica la reducción módulo p.

Es fácil ver que γ es un epimorfismo cuyo núcleo es el ideal generado por $p + \langle h(x)\rangle$ en $\mathbb{Z}_{p^s}[x]/\left\langle h(x)\right\rangle$, de aquí $\langle p + \langle h(x)\rangle\rangle$ es un ideal maximal del anillo de Galois $\mathbb{Z}_{p^s}[x]/\left\langle h(x)\right\rangle$ ya que el cociente del anillo de Galois y este ideal es isomorfo a la imagen de γ, la cual es un campo finito (ver la referencia [**53**]).

También se puede ver que los elementos que no se encuentran en este ideal maximal son unidades, por lo que $\langle p + \langle h(x)\rangle\rangle$ es el único ideal maximal de $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$, es decir, el anillo $R = GR(p^s, m)$ es un anillo local con ideal maximal $\langle p\rangle = pR$ generado por p, y campo residual R/pR (utilizando una notación más sencilla) isomorfo a $\mathbb{F}_{p^m}$. La cardinalidad de R es p^{sm} con característica p^s cuyos elementos del ideal maximal son sus divisores de cero. El anillo $GR(p^s, m)$ es una extensión de $\mathbb{Z}_{p^s}$, más aún, cualquier ideal del anillo de Galois tiene la forma $\langle p^i\rangle$ para $1 \leq i \leq s$, y se tiene una cadena de ideales

$$\langle 0\rangle = \langle p^s\rangle \subset \left\langle p^{s-1}\right\rangle \subset \cdots \subset \langle p\rangle \subset \langle 1\rangle .$$

Sea $S = GR(p^s, mn)$ una extensión de $R = GR(p^s, m)$ tal que $S = R[x]/\langle h(x)\rangle$, donde $h(x)$ es un polinomio mónico básico irreducible (primitivo) de grado n sobre $R[x]$. En este trabajo S denotará una extensión del anillo de Galois R y el grupo de unidades de un anillo de Galois R por U_R. Para mas detalles de las observaciones anteriores puede consultarse [**53**].

EJEMPLO 2.6. *Ejemplos de anillos de Galois incluyen los siguientes:*

1. $GR(p^s, 1) = \mathbb{Z}_{p^s}$ *y* $GR(p, m) = \mathbb{F}_{p^m}$([**53**]).
2. *Sea* $f(x) = x^3 + x + 1 \in \mathbb{Z}_4$ *el cual es mónico básico irreducible. Entonces* $GR(2^2, 3) = \mathbb{Z}_4[x]/\langle f(x)\rangle$ ([**53**]).

Considérese nuevamente al anillo de Galois

$$GR(p^s, m) = \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle ,$$

donde $h(x)$ es un polinomio mónico básico primitivo de grado m sobre $\mathbb{Z}_{p^s}$:

Sea $\xi = x + \langle h(x)\rangle$. Entonces $h(\xi) = 0$ y

$$a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + \langle h(x)\rangle = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1},$$

$a_i \in \mathbb{Z}_{p^s}$, $i = 0, \ldots, m-1$, luego

$$\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle = \{a_0 + a_1\xi + \cdots + a_{n-1}\xi^{m-1} : a_i \in \mathbb{Z}_{p^s},\ i = 0, 1, \ldots, m-1\} = \mathbb{Z}_{p^s}[\xi].$$

Por otro lado $\overline{\xi} = x + \left\langle \overline{h}(x)\right\rangle$ es raíz del polinomio primitivo $\overline{h}(x)$ sobre $\mathbb{F}_p$ y

$$\mathbb{F}_p[x]/\left\langle \overline{h}(x)\right\rangle = \mathbb{F}_{p^m} = \mathbb{F}_p[\overline{\xi}].$$

Como $\overline{h}(x)$ es un polinomio primitivo sobre $\mathbb{F}_p[x]$ de grado m, entonces $\mathbb{F}_{p^m}\backslash\{0\} = \left\langle \overline{\xi}\right\rangle$, y de aquí ξ es un elemento de $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ de orden $p^m - 1$.

En general estas observaciones se enuncian en el siguiente resultado en donde se representa de dos maneras a los elementos de un anillo de Galois:

TEOREMA 2.7. *(*[**53**]*) Sea* $S = GR(p^s, mn)$ *una extensión del anillo de Galois* $R = GR(p^s, m)$. *Existe un elemento* $\xi \in S$ *distinto de cero de orden* $p^{mn} - 1$, *el cual es raíz de un polinomio mónico básico primitivo* $h(x)$ *de grado* n *sobre* R *tal que* $h(x)$ *divide a* $x^{p^n-1} - 1$ *sobre el anillo* R. *Más aún*

$$S = \{a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} : a_i \in R,\ i = 0, 1, \ldots, n-1\}$$

y

$$S = \{a_0 + a_1 p + \cdots + a_{s-1} p^{s-1} : a_i \in \mathcal{T}_S,\ i = 0, 1, \ldots, s-1\},$$

donde $\mathcal{T}_S := \{0, 1, \xi, \xi^2, \ldots, \xi^{p^{mn}-2}\}$, *es el conjunto de Teichmüller de* S.

□

Un automorfismo ψ de S tal que $\psi(r) = r$ para todo elemento de R es llamado un automorfismo de S sobre R.

DEFINICIÓN 2.8. *(*[**53**]*) Se define la función* $\phi : S \longrightarrow S$ *como*

$$\phi(a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}) := a_0 + a_1\xi^q + \cdots + a_{n-1}\xi^{(n-1)q},$$

$a_0, a_1, \ldots, a_{n-1} \in R$.

La función ϕ es un automorfismo de S sobre R llamado el automorfismo de Frobenius generalizado, nombre recibido por su generalización respecto al automorfismo de Frobenius sobre campos finitos.

Considérense los automorfismos $\phi^0 = 1$ y $\phi^{i+1} = \phi^i \circ \phi,\ i = 0, 1, 2, \ldots$, dados por

$$\phi^i\left(a_0 + a_1 p + \cdots + a_{s-1} p^{s-1}\right) = a_0^{q^i} + a_1^{q^i} p + \cdots + a_{s-1}^{q^i} p^{s-1},$$

donde $a_i \in \mathcal{T}_S$. El grado de la extensión de S sobre R indica el número de automorfismos de S sobre R, por lo que los automorfismos $\phi^i,\ i = 0, 1, 2, \ldots, n-1$, son todos los automorfismos de S sobre R ya que estos son todos distintos.

DEFINICIÓN 2.9. *(*[**53**]*) La función traza de* S *sobre* R, $T_{S/R} : S \to R$, *está definida por*

$$T_{S/R}(\alpha) := \alpha + \phi(\alpha) + \cdots + \phi^{n-1}(\alpha).$$

Las siguientes propiedades de la traza se siguen de la definición y su demostración es similar a las del Teorema 1.2.

TEOREMA 2.10. *(*[**53**]*) Sean* $\alpha, \beta \in S$ *y* $a \in R$. *Entonces,*

- $T_{S/R}(\alpha) \in R$,
- $T_{S/R}$ *es un epimorfismo de* R*-módulos (considerando* S *y* R *como* R*-módulos),*
- $T_{S/R}(a) = na$,
- $T_{S/R}(\phi(\alpha)) = T_{S/R}(\alpha)$.
- *(Transitividad de la traza) Sean* R, R' *y* R'' *anillos de Galois tal que* R *es un subanillo de* R' *y* R' *un subanillo de* R''. *Entonces*

  $$T_{R''/R}(\alpha) = T_{R'/R}(T_{R''/R'}(\alpha)),$$

  para toda $\alpha \in R''$.

□

Una vez generalizada la definición de la traza sobre anillos de Galois es posible considerar caracteres sobre el grupo aditivo de un anillos de Galois.

Sea $R = GR(p^s, m)$ un anillo de Galois, la función χ_1 definida por

$$\chi_1(c) := e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(c)/p^s} \qquad \text{para toda } c \in R,$$

es un caracter del grupo aditivo de R que al igual que los campos finitos es llamado caracter aditivo de R.

Sea $a \in R$. La función χ_a definida por $\chi_a(c) := \chi_1(ac)$ es un caracter aditivo de R.

LEMA 2.11. *(*[**23**]*) El conjunto* $\{\chi_a | a \in R\}$ *introducidos anteriormente son todos los caracteres aditivos de un anillo de Galois* R.

DEMOSTRACIÓN. En primer lugar probemos que para $0 \neq a \in R$, existe $c \in R$ tal que $T_{R/\mathbb{Z}_{p^s}}(ac) \neq 0$:

Sea $a = p^r u$, $u \in U_R$, $1 \leq r \leq s-1$, y supóngase que $T_{R/\mathbb{Z}_{p^s}}(ac) = 0$ para toda $c \in R$. Entonces $p^r T_{R/\mathbb{Z}_{p^s}}(uc) = 0$ para toda $c \in R$, por lo que se tiene que $p^r T_{R/\mathbb{Z}_{p^s}}(b) = 0$ para toda $b \in R$. Por otro lado, como $T_{R/\mathbb{Z}_{p^s}}$ es una función suprayectiva se tiene que existe $d \in R$ tal que $T_{R/\mathbb{Z}_{p^s}}(d) = 1$. Por lo tanto $p^r = 0$, lo cual es una contradicción.

Procediendo de modo similar al caso de campos finitos, si $a, b \in R, a \neq b$, 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 alguna $c \in R$, por lo que χ_a y χ_b son caracteres distintos. Considerando todos los elementos $b \in R$ se concluye el resultado. □

3. Funciones bent sobre anillos de Galois

En esta Sección se definen las funciones bent sobre anillos de Galois y se dedica la Sección a la construcción de una familia de funciones bent sobre anillos de Galois de característica p^2, p un número primo.

Definamos las funciones bent sobre los anillos de Galois.

DEFINICIÓN 3.1. *(*[**4**]*) Una función* $f : GR(p^s, m)^n \longrightarrow GR(p^s, m)$ *es llamada bent si*

$$\left| \sum_{x \in GR(p^s,m)^n} e^{2\pi i (T_{GR(p^s,m)/\mathbb{Z}_{p^s}}(f(x) - \lambda \cdot x))/p^t} \right| = |GR(p^s, m)|^{n/2},$$

para toda $\lambda \in GR(p^s, m)^n$, *donde* $\lambda \cdot x$ *denota el producto punto usual.*

En términos de caracteres, la función f es bent si

$$\left| \sum_{x \in GR(p^s,m)^n} \chi_1(f(x) - \lambda \cdot x) \right| = |GR(p^s, m)|^{n/2},$$

para toda $\lambda \in GR(p^s, m)^n$.

EJEMPLO 3.2. *Considérese el anillo de Galois $GR(4,2)$ y α una raíz del polinomio mónico básico primitivo x^2+x+1. Entonces $f(x)=x^3+\alpha x^2$, $x\in GR(4,2)$, es una función bent.*

Es fácil ver que

$$\begin{aligned} GR(4,2) = \quad & \{0,2,2\alpha,2\alpha^2,1,3,1+2\alpha,1+2\alpha^2,\alpha,2+\alpha,3\alpha,\alpha+2\alpha^2,\alpha^2,2+\alpha^2,\\ & 2\alpha+\alpha^2,3\alpha^2\}. \end{aligned}$$

Siguiendo el orden anterior de los elementos de $GR(4,2)$ y tomando en particular $\lambda=\alpha$, se tiene:

$$\begin{aligned} &\sum_{x\in GR(4,2)} e^{2\pi i T_{R/\mathbb{Z}_4}(f(x)-\alpha\cdot x)/4}\\ &= e^{2\pi i T_{R/\mathbb{Z}_4}(0)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(2\alpha)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(2+2\alpha)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(1)/4}\\ &+e^{2\pi i T_{R/\mathbb{Z}_4}(1+2\alpha^2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(3)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(1+2\alpha)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2+2\alpha)/4}\\ &+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2+2\alpha^2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2+2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2)/4}\\ &+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(\alpha^2)/4}\\ &= e^{2\pi i(0)/4}+e^{2\pi i T_{R/\mathbb{Z}_4}(2)/4}+e^{2\pi i(2)/4}+e^{2\pi i(0)/4}+e^{2\pi i(2)/4}+e^{2\pi i(0)/4}+e^{2\pi i(2)/4}\\ &+e^{2\pi i(0)/4}+e^{2\pi i(1)/4}+e^{2\pi i(1)/4}+e^{2\pi i(3)/4}+e^{2\pi i(3)/4}+e^{2\pi i(3)/4}+e^{2\pi i(3)/4}\\ &+e^{2\pi i(3)/4}+e^{2\pi i(3)/4}\\ &= 4+4e^{\pi i}+2e^{\pi i/2}+6e^{3\pi i/2}=-4i. \end{aligned}$$

El ejemplo anterior pertenece a una familia de funciones bent. Para probar la existencia de esta familia considérense las siguientes observaciones:

Observación 1. Sea $R=GR(p^2,m)$ y u una unidad de R. Entonces

$$\sum_{x\in T_R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(xu)/p}=\sum_{x\in T_R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(pxu)/p^2}=\sum_{x\in pR} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(xu)/p^2}=0.$$

Nótese que la última suma es igual a cero ya que u es una unidad y al multiplicarse por todos los elementos del ideal pR se obtienen nuevamente los elementos del ideal, por lo que la traza en la suma evalúa todos los elementos de pR y al considerar el caracter sobre el grupo aditivo pR se obtiene el resultado.

Observación 2. Si $\mathbb{F}_{p^m}$ es un campo finito con p^m elementos y r es un entero positivo tal que $(r,p^m-1)=1$, entonces la función $f(y)=y^r$ es una permutación (polinomial) en $\mathbb{F}_{p^m}$ ([**28**]). Así, bajo las mismas condiciones, la función $g(x)=x^r$ es una permutación en el conjunto de Teichmüller $\mathcal{T}_R$ del anillo de Galois R.

Sean r un entero positivo y las funciones $\varphi,\psi: R\longrightarrow R$ definidas por $\varphi(x)=x^{p^r}$ y $\psi(x)=x^p$ respectivamente. Obsérvese que estas funciones tienen la siguiente propiedad:

Si $x=x_0+px_1$ es cualquier elemento de R con $x_0,x_1\in\mathcal{T}_R$, entonces

$$\varphi(x)=\varphi(x_0)\text{ y }\psi(x)=\psi(x_0).$$

El siguiente resultado es el objetivo principal de esta Sección, la construcción de una familia de funciones bent:

TEOREMA 3.3. *([**10**]) Considérese el anillo de Galois $R = GR(p^2, m)$. Con la notación anterior, sea r un entero positivo tal que $(r, p^m - 1) = 1$ y la función f definida por $f(x) := x\varphi(x) + \alpha\psi(x)$, donde $\alpha \in R$. Entonces para cualquier $u \in U_R$, $uf(x)$ es una función bent en R.*

DEMOSTRACIÓN. Sea $x = x_0 + px_1 \in R$ con $x_i \in \mathcal{T}_R$, $d \in R$, $u \in U_R$ y sea $b = ud$.

Nótese que,

$$\begin{aligned} & uf(x) - bx \\ &= u(x\phi(x) + \alpha\psi(x)) - bx = ux^{pr+1} + u\alpha x^p - bx \\ &= ux_0^{pr+1} + upx_0^{pr}x_1 + u\alpha x_0^p - udx_0 - pudx_1 \\ &= u(x_0^{pr+1} + \alpha x_0^p - dx_0) + up(x_0^{pr} - d)x_1 \\ &= (uf(x_0) - bx_0) + up(x_0^{pr} - d)x_1. \end{aligned}$$

Si $d = d_o + d_1 p$ con $d_i \in \mathcal{T}_R$, entonces:

$$\sum_{x\in R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(uf(x)-bx)/p^2} \tag{1}$$

$$= \sum_{x_0\in\mathcal{T}_R} \sum_{x_1\in\mathcal{T}_R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}\left((uf(x_0)-bx_0)+up(x_0^{pr}-d)x_1\right)/p^2} \tag{2}$$

$$= \sum_{x_0\in\mathcal{T}_R} \left(e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(uf(x_0)-bx_0)/p^2} \times [\sum_{x_1\in\mathcal{T}_R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}\left(u\left(x_0^{pr}-d\right)x_1\right)/p}] \right) \tag{3}$$

$$= \sum_{x_0\in\mathcal{T}_R} \left(e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(uf(x_0)-bx_0)/p^2} \times [\sum_{x_1\in\mathcal{T}_R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}\left(u\left(x_0^{pr}-d_0\right)x_1\right)/p}] \right) \tag{4}$$

$$= p^m \left(e^{2\pi i T_{R/\mathbb{Z}_{p^2}}\left(u(d_0^{\frac{pr+1}{pr}} + \alpha d_0^{\frac{p}{pr}}) - bd_0^{\frac{1}{pr}}\right)/p^2} \right). \tag{5}$$

La relación (5) se sigue de la relación (4) observando que si $x_0^{pr} = d_0$, entonces la suma respecto a x_1 es $|\mathcal{T}_R| = p^m$. Si $x_0^{pr} \neq d_0$, ya que u es una unidad y la diferencia de dos elementos distintos de $\mathcal{T}_R$ es una unidad, entonces $u\,(x_0{}^{pr} - d_0)$ es también una unidad, por lo que se sigue de la Observación 1 que la suma respecto a x_1 es cero. Si $(r, p^m - 1) = 1$, entonces $(pr, p^m - 1) = 1$ y la función x_0^{pr} es una permutación en $\mathcal{T}_R$ (Observación 2). Así existe un único elemento $x_0 \in \mathcal{T}_R$ tal que $x_0^{pr} = d_0$, es decir, $x_0 = d_0^{\frac{1}{pr}}$. Por lo tanto todas las sumas respecto a x_1 son cero con una excepción, la cual es p^m.

Como la exponencial en la relación (5) es una raíz de la unidad, el resultado se sigue. □

Capítulo 4

Funciones perfectamente no-lineales y esquemas de compartición de secretos

En este Capítulo se presenta una construcción de códigos lineales y esquemas de compartición de secretos utilizando funciones perfectamente no-lineales $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ basados en los trabajos [**7**] y [**55**], y se hace un recuento de los resultados ahí obtenidos.

Se introduce 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 (para mayor información consúltese [**39**] o [**7**]). En el siguiente Capítulo se abordan estos temas considerando el caso $p = 2$, es decir, al utilizar las funciones casi-bent, el cual no aparece en la literatura.

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

En esta Sección se da una construcción de códigos lineales basados en funciones perfectamente no-lineales $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $p \neq 2$ primo ([**7**]). Al referirnos a funciones perfectamente no-lineales se entiende que también son funciones bent dada la equivalencia que existe entre ellas (Capítulo 2, Teorema 4.4).

Se da una primera construcción de un código lineal y posteriormente se describen sus parámetros ([**7**]).

DEFINICIÓN 1.1. *Sea $p \neq 2$ un número primo, $n > 1$ un entero y h un divisor de n. $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ una función bent tal que $F(0) = 0$ y $a, b \in \mathbb{F}_{p^n}$. Sea*

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

y

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

Es fácil verificar que $\mathcal{C}$ es un código lineal sobre $\mathbb{F}_{p^h}$. Nótese que las funciones $F_{a,b}$ y $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^h}}(F_{a,b}(x))$ son también funciones bent si $a \neq 0$, ya que las funciones bent multiplicadas por un elemento del grupo de unidades es bent, y este al sumarse con una función afín también lo es. Veamos cuales son los parámetros de este código.

Para el peso de las palabras del código se tiene una cota, y el siguiente resultado ([**21**]) nos permite encontrarla.

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,

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

□

COROLARIO 1.3. *(*[**7**]*) Sea* $\mathcal{C}$ *el código lineal de la Definición 1.1 y* w *un elemento distinto de cero de* $\mathcal{C}$. *Entonces,*

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

□

TEOREMA 1.4. *(*[**7**]*) Sea* $\mathcal{C}$ *el código de la Definición 1.1 y* $\mathcal{C}^\perp$ *su código dual con distancia mínima* $d^\perp$. *Entonces* $\mathcal{C}$ *es un* $[p^n - 1, 2n/h, d]_{p^h}$*- código lineal y si* $p \geq 3$ *y* $n > 1$,

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

□

De este modo se tienen los parámetros del código lineal introducido anteriormente, sin embargo, no ha sido posible hallar la distribución de pesos. La siguiente definición es la de un código lineal en donde esto sí es posible ([**7**]).

DEFINICIÓN 1.5. *Sea* $p \neq 2$ *primo,* $r > 1$ *un entero y* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *la función definida por* $F(x) = x^{p^r+1}$, *donde* $n/(n, r)$ *es impar, la cual es una función bent. Si* $a, b \in \mathbb{F}_{p^n}$, *sea*

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

y

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

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

El siguiente resultado proporciona la longitud, dimensión y distribución de pesos del código anterior para el caso n impar, así como una relación con su código dual.

TEOREMA 1.6. *(*[**55**]*) Sea* $\mathcal{C}$ *el código introducido en la Definición 1.5 y* $\mathcal{C}^\perp$ *su código dual. Entonces* $\mathcal{C}^\perp$ *tiene peso mínimo* $d^\perp = 3$ *ó* 4. *Si* n *es impar los parámetros de* $\mathcal{C}$ *son*

$$[p^n - 1, 2n, (p-1)p^{n-1} - p^{\frac{n-1}{2}}]_p \text{ - código lineal.}$$

Más aún, los distintos pesos de las palabras distintas de 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 para determinar la longitud y la dimensión del código lineal se sigue del caso $h = 1$ de la Definición 1.1.

Veamos que $d^{\perp} = 3$ o 4: si $d^{\perp} = 2$, entonces existe $\mathbf{c} = (c_1, \ldots, c_m) \in \mathcal{C}^{\perp}$, tal que $c_1 = \cdots = c_m = 0$, excepto un par de elementos $c_i, c_j \neq 0$, $i, j \in \{1, \ldots, m\}$, $i \neq j$. Luego,

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

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

$$Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(aF(x_i) + bx_i) = c(Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(aF(x_j) + bx_j)),\ \forall\ (a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$$

tal que $x_i \neq x_j$ y $c \in \mathbb{F}_p^*$, o equivalentemente,

$$aF(x_i) + bx_i = c(aF(x_j) + bx_j)\ \forall (a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$$

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

Sea $C_{a,b} \in \mathcal{C}$, considérense los distintos casos para a y b, ya que de este modo se encontrarán los distintos pesos de las palabras del código:

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 3.7 del Capítulo 1,

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

Entonces,

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

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

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

donde $S_r(ac, bc)$ es dado en (I) Sección 3 del Capítulo 1. Por otro lado para cualquier elemento $c \in \mathbb{F}_p^*$, la ecuación $(ac)^{p^r}x^{p^{2r}} + acx + (bc)^{p^r} = 0$, es equivalente a $a^{p^r}x^{p^{2r}} +$

$ax + b^{p^r} = 0$, ya que $c^{p^r} = c$. Por el Teorema 3.4 del Capítulo 1, esta ecuación tiene una única solución $x_{a,b}$, y por el Teorema 3.6 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,

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

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

En el caso del código lineal de la Definición 1.5 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. 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 1.7. *(Relaciones de Pless,* [**43**]*) Sea C un $[n, k]$ - código lineal sobre $\mathbb{F}_2$, A_i es el número de palabras de peso i de C y B_i el número de palabras de peso i en $C^\perp$. Si $r \geq 1$ es un entero y*

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

entonces

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

□

TEOREMA 1.8. *([**55**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.5 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 1.6 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. Entonces de las relaciones de Pless se obtienen las siguientes 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 este sistema lineal se prueba la afirmación. □

TEOREMA 1.9. *([**55**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.5. 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, $w(C_{0,b}) = (p-1)p^{n-1}$. De estas palabras existen p^n-1 elementos en el código.

Si $a\neq 0, b=0$, sea $q=p^n$. Por el Teorema 3.7 del Capítulo 1,

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

dependiendo del valor de $\eta(a)$, se tiene que:

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

Entonces, para cada uno de esos casos existen $\frac{p^n-1}{2}$ palabras con ese peso.

Si $a \neq 0, b \neq 0$, un argumento similar a la prueba del Teorema 1.6 muestra 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 3.6 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 $\eta(c) = 1$, o $\eta(-c) = 1$ y

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

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

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

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 cada elemento $a \in \mathbb{F}_q^*$ fijo, existe un único $x_{a,b}$ el cual satisface $a^{p^r}x^{p^{2r}} + ax = -b^{p^r}$ para cada $b \in \mathbb{F}_q^*$. Estos valores $x_{a,b}$ 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 recorre los elementos de $\mathbb{F}_q^*$ son los mismos de ay^{p^r+1} cuando y recorre todos los elementos de $\mathbb{F}_q^*$, y éstos a su vez son los mismos de az^2 cuando z toma todos los valores de $\mathbb{F}_q^*$.

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 3.7 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 y

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

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, nótese que solo ocurre un cambio de signo en los valores de $R_{a,b}$. Aplicando nuevamente el Teorema 3.7 del Capítulo 1, para $\eta(a)=-1$, y procediendo de manera similar a lo anterior, 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. De modo similar,

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

aparece

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

veces.
La prueba del caso $p\equiv 3$ mód 4 es semejante 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 lo tanto 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 ([**46**]) 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 éstas el secreto puede ser recuperado, y no con un número menor de entidades. 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 no es posible recuperar la imagen. Existen varios esquemas de compartición de secretos, por ejemplo, el esquema de umbral ("Threshold") de Shamir (ver también [**52**] y [**50**]).

2.1. Esquemas de compartición de secretos, método de Massey.

Existen varias maneras de utilizar los códigos lineales para construir un esquema de compartición de secretos, una de ellas es descrita por James L. Massey (para mayor información consúltese [**39**] y [**7**]), la cual se menciona a continuación:

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 $\mathcal{C}$ sobre $\mathbb{F}_q$, recuérdese, n la longitud, k la dimensión y d el peso mínimo. Se consideran distintos de cero los vectores columna de la matriz generadora.
- En el esquema de compartición de secretos basado en $\mathcal{C}$ el secreto es un elemento del campo finito $\mathbb{F}_q$ elegido aleatoriamente. Este campo finito es llamado el espacio de secretos.
- Se consideran $n-1$ entidades $P_1, P_2, \ldots, P_{n-1}$ y un encargado P_0.
- Para calcular los fragmentos (partes del secreto s), el encargado elige aleatoriamente un vector
$$u = (u_0, \ldots, u_{k-1}) \in \mathbb{F}_q^k$$
tal que $s = u\mathbf{g}_0$. Se tienen 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 considera 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 a la entidad P_i como su fragmento para cada $i \geq 1$.

Nótese que $t_0 = u\mathbf{g}_0 = s$.

Nótese que al considerar distintos valores de $u \in \mathbb{F}_q^k$, que satisfagan $= u\mathbf{g}_0 = s$, los conjuntos de fragmentos
$$\{t_{i_1}, \ldots, t_{i_m}\},$$
no necesariamente son iguales, pero el conjunto de entidades, sí lo es.

El siguiente resultado proporciona una relación entre los fragmentos y las columnas de la matriz generadora del código lineal considerado.

TEOREMA 2.1. *(*[**39**],[**7**]*) Los fragmentos*
$$(t_{i_1}, t_{i_2}, \ldots, t_{i_m}) = u(\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_m}),$$

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

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

Por lo tanto,

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

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

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

luego

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

Entonces,

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

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

Utilizando el Teorema anterior se tiene el siguiente resultado, el cual describe una relación con el código dual del código en consideración.

COROLARIO 2.2. *(*[**39**],[**7**]*) 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 fragmentos*

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

determina el secreto si 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* $c_{i_j} \neq 0$ *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,

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

si y sólo si,

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

o equivalentemente

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

Utilizando el Teorema 2.1 se tiene el resultado. □

Si un grupo de entidades puede recuperar el secreto combinando sus fragmentos, entonces cualquier grupo de entidades conteniendo este grupo puede también recuperar el secreto.

Es posible una relación más estrecha con el código dual, para esto se requieren los siguientes conceptos ([**7**]):

- Un grupo de entidades es llamado "conjunto mínimo de acceso" si cualesquiera entidades en él pueden recuperar el secreto con sus fragmentos, pero cualquier subgrupo propio de éste no lo puede hacer.
- El soporte de un vector $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ está 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 distintos de cero de ella.

COROLARIO 2.3. *(*[**39**]*,*[**7**]*) 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 mínimos de acceso y el conjunto de palabras mínimas del código dual $\mathcal{C}^\perp$ cuya primera entrada es* 1.

DEMOSTRACIÓN. Sea A un conjunto mínimo de acceso y $t = \{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ su respectivo conjunto de fragmentos, es decir, t determina el secreto. Entonces por el Corolario 2.2 existe una palabra

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

en el código dual $\mathcal{C}^\perp$ 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 los fragmentos correspondientes a conjuntos mínimos de acceso siempre son distintos de cero, ya que si un coeficiente c_{i_j} es cero, es posible suprimir la entidad 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 2.2 existe un conjunto de fragmentos $t = \{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ que determinan el secreto s considerado. A este conjunto le corresponde un conjunto mínimo de acceso, ya que si se prescinde de una de estas entidades, nuevamente por el Corolario 2.2, se tiene una palabra contenida propiamente en $\mathbf{c}$. □

Los conceptos anteriores se ilustran 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 ahora un esquema sobre $\mathcal{H}^{\perp}$ y elíjase $u = (1, 0, 1)$. Como H es una matriz generadora para $\mathcal{H}^{\perp}$, entonces $s = (1, 0, 1) \cdot (1, 1, 0) = 1$. Si se desean conocer los conjuntos mínimos de acceso, una manera 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 $\{t_1, t_2, t_3, t_4, t_5, t_6\}$ los fragmentos de las respectivas entidades $\{P_1, P_2, P_3, P_4, P_5, P_6\}$. Entonces,

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

son las combinaciones de todos los conjuntos mínimos de acceso. Para este elemento $u = (1, 0, 1)$, se tiene $t_1 = 0, t_2 = 1, t_3 = 0, t_4 = 1, t_5 = 0, t_6 = 1$. Nótese que no es posible suprimir t_3 en la primera combinación, pues si se considera $u = (1, 0, 0)$, entonces, $1 = s = (1, 0, 0) \cdot (1, 1, 0)$ y $t_3 = 1$ y $t_6 = 0$ (aún cuando para $u = (1, 0, 1)$ se tenga $t_3 = 0$). Este ejemplo es ilustrativo, sin embargo no es un buen ejemplo, ya que cualquier atacante tiene probabilidad $1/2$ de descubrir el secreto.

La estructura de acceso de un esquema de compartición de secretos son los conjuntos mínimos de acceso 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 conocer el conjunto de todas las palabras mínimas de un código lineal ([**7**]).

2.2. La estructura del mínimo acceso 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 2.4. *([**7**]) 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 distinta de cero de $\mathcal{C}$ es mínima, entonces en el esquema de compartición de secretos basado en $\mathcal{C}^{\perp}$ se tiene que:

1. *Existen en total q^{k-1} conjuntos mínimos de acceso.*
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 la entidad P_i, está incluida en todo conjunto mínimo de acceso.

   b) Si $\mathbf{g}_i$ no es un múltiplo de $\mathbf{g}_0$, $1 \leq i \leq n-1$, entonces la entidad P_i está incluida en $(q-1)q^{k-2}$ conjuntos mínimos de acceso.
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 entidades está incluido en

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

   conjuntos mínimos de acceso.

DEMOSTRACIÓN. Probemos el primer punto, es decir, que el número total de conjuntos mínimos de acceso 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 mínimos de acceso 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, por lo que $\mathbf{g}_0 \neq \mathbf{0}$. Por lo tanto el producto interior $u\mathbf{g}_0$ toma cada elemento de $\mathbb{F}_q^*$ exactamente q^{k-1} veces cuando u recorre los elementos distintos de cero de $\mathbb{F}_q^k$, pues este es una función lineal.

Probemos ahora el segundo punto. Supóngase que $d^{\perp} = 2$. Determinemos la estructura del mínimo acceso 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 mínimo de acceso por el Corolario 2.3, 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. Nótese que, $d^{\perp} = 2$, asegura la existencia de palabras mínimas con uno en la primera entrada con al menos dos elementos distintos de cero.

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 recorre los elementos de $\mathbb{F}_q^k$ (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

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

Recuérdese 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 $\mathcal{C}$, por el Corolario anterior existen precisamente $(q-1)q^{k-2}$ conjuntos mínimos de acceso en el cual P_i está implicado.

Demostración del tercer punto: supóngase la condición $d^\perp \geq 3$ y $1 \leq t \leq$ mín$\{k-1, d^\perp - 2\}$. Considérese $1 \leq i_1 < i_2 < \cdots \leq n-1$ 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 ya que $t \leq k-1 \leq d-1$ y $d-1$ columnas cualesquiera de una matriz generadora son linealmente independientes. Además,

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

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

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

De modo similar a las observaciones anteriores se puede concluir que todo grupo de t participantes está incluido en

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

conjuntos mínimos de acceso. □

En relación al resultado anterior, hay un interesante problema, el de construir códigos donde cada palabra distinta de cero sea una palabra mínima.

TEOREMA 2.5. *([7]) Sea $\mathcal{C}$ un $[n,k]_q$ código lineal, $w_{\textbf{mín}}$ y $w_{\textbf{máx}}$ los pesos mínimo y máximo distintos de cero respectivamente de las palabras del código. Si*

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

entonces cada palabra distinta de cero de $\mathcal{C}$ es una palabra mínima.

DEMOSTRACIÓN. Supóngase que

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

tal que $\mathbf{u}$ no es un múltiplo de $\mathbf{v}$, luego,

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

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

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

por lo que existe $t \in \mathbb{F}_q^*$ tal que $m_t \geq \frac{w(\mathbf{v})}{q-1}$, pues se divide $w(\mathbf{v})$ en $q-1$ partes y se tienen $q-1$ 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 tiene la igualdad anterior, pues $\mathbf{u}$ cubre a $\mathbf{v}$, y de aquí,

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

$$< \frac{q}{q-1} w_{\textbf{mín}} - \frac{w_{\textbf{mín}}}{q-1} = w_{\textbf{mín}},$$

lo cual es una contradicción. Luego si $\mathbf{u}$ cubre a $\mathbf{v}$, $\mathbf{u}$ es múltiplo de $\mathbf{v}$, para $\mathbf{u}$ y $\mathbf{v}$ arbitrarios con esta propiedad. Por lo tanto cada palabra distinta de cero de $\mathcal{C}$ es una palabra mínima. □

2.3. Esquemas de compartición de secretos.

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

TEOREMA 2.6. *([7]) Considérese $\mathcal{C}$ 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.

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

Por otro lado,

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

entonces,

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

lo cual implica,

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

de esta expresión se tiene,

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

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 2.5, todas las palabras son mínimas. □

El resultado anterior nos brinda una condición para asegurar que todas las palabras del código $\mathcal{C}$ de la definición 1.1 son mínimas, de esta manera considerando el esquema sobre el código dual $\mathcal{C}^\perp$ y aplicando el Teorema 2.4 se tiene el siguente resultado.

TEOREMA 2.7. *([7]) Sea $\mathcal{C}$ el código lineal de la definición 1.1 y una matriz generadora $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, g_{p^n-2})$ de $\mathcal{C}$. 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 se tienen en total p^{2n-h} conjuntos mínimos de acceso.*

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 mínimo de acceso.*

   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 mínimos de acceso.
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 mínimos de acceso.

DEMOSTRACIÓN. La afirmación se sigue del Teorema 2.6 y el Teorema 2.4. □

Considérese el siguiente ejemplo:

Sea $\mathcal{C}$ el código lineal de la Definición 1.1, considerando los campos finitos $\mathbb{F}_{3^3}$, $\mathbb{F}_3$ y la función bent $F(x) = x^2$. Una matriz generadora del código $\mathcal{C}$ está dada de la siguiente

forma:

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

la cual está expresada con la representación $(I_6|A)$, donde I_6 es la matriz identidad de orden 6×6. Entonces una matriz generadora del código $\mathcal{C}^{\perp}$ está dada por

$$H = (I_{20}, -A^t) = \left(\begin{array}{c|cccccc} & 2 & 2 & 0 & 2 & 0 & 1 \\ & 1 & 0 & 2 & 1 & 2 & 2 \\ & 2 & 0 & 0 & 1 & 1 & 0 \\ & 0 & 2 & 0 & 0 & 1 & 1 \\ & 1 & 1 & 2 & 1 & 0 & 0 \\ & 0 & 1 & 1 & 2 & 1 & 0 \\ & 0 & 0 & 1 & 1 & 2 & 1 \\ & 1 & 1 & 0 & 2 & 1 & 1 \\ I_{20} & 1 & 2 & 1 & 1 & 2 & 0 \\ & 0 & 1 & 2 & 1 & 1 & 2 \\ & 2 & 2 & 1 & 1 & 1 & 2 \\ & 2 & 1 & 2 & 0 & 1 & 2 \\ & 2 & 1 & 1 & 1 & 0 & 2 \\ & 2 & 1 & 1 & 0 & 1 & 1 \\ & 1 & 0 & 1 & 2 & 0 & 0 \\ & 0 & 1 & 0 & 1 & 2 & 0 \\ & 0 & 0 & 1 & 0 & 1 & 2 \\ & 2 & 2 & 0 & 0 & 0 & 2 \\ & 2 & 1 & 2 & 2 & 0 & 1 \\ & 1 & 0 & 1 & 0 & 2 & 2 \end{array}\right),$$

donde I_{20} es la matriz identidad de orden 20×20. Considérese el esquema sobre $\mathcal{C}^{\perp}$. Si se desean conocer los conjuntos mínimos de acceso, una manera es determinando las palabras mínimas con uno en la primera entrada del código lineal $\mathcal{C}$. Por medio del programa computacional Maple, hemos observado que el código lineal $\mathcal{C}$ tiene 243 palabras mínimas con uno en la primera entrada, por lo que es el número de conjuntos mínimos de acceso que se tiene en el esquema. Aquí se listan 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 2.3 para cada palabra mínima con uno en la primera entrada se tiene un conjunto mínimo de acceso, el cual está formado por las acciones correspondientes a las entradas distintas de cero. Al expresar el secreto s como combinación lineal de los fragmentos, como coeficientes de esta combinación lineal 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 mínimo de acceso:

$\{t_1, t_2, t_3, t_6, t_7, t_8, t_9, t_{15}, t_{16}, t_{17}, t_{19}, t_{22}, t_{23}, t_{25}\}$, es decir, para cada entrada distinta de cero se considera un fragmento en el correspondiente conjunto mínimo de acceso.

Si s es un secreto (elegido de $\mathbb{F}_3$), entonces las combinaciones lineales de los fragmentos, corresponden respecto a los conjuntos mínimos de acceso, como sigue, para las primeras tres palabras de la lista anterior.

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

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

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

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 los fragmentos no son los mismos, pues con la misma u, al multiplicarse por cada una de las columnas de la matriz generadora de $\mathcal{C}^{\perp}$, se obtiene un correspondiente fragmento. 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 todos los fragmentos 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 todos los fragmentos 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 todos los fragmentos 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 fragmentos anteriores satisface las combinaciones antes escritas si $s = 1$.

Capítulo 5

Funciones casi-bent y esquemas de compartición de secretos

En este Capítulo se presenta la construcción de esquemas de compartición de secretos utilizando funciones casi-bent sobre campos de característica 2. Estos resultados pueden encontrarse en [**31**]. De esta manera se tienen esquemas de compartición de secretos basados en funciones $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, para cualquier número primo p.

Se introduce el Capítulo con la construcción de códigos lineales con base en las funciones casi-bent sobre campos de característica 2 obteniendo sus parámetros y posteriormente se da la construcción de esquemas de compartición de secretos utilizando estos códigos lineales siguiendo el método de Massey. Además se presentan dos extensiones de estos esquemas cuando el espacio de secretos es $\mathbb{F}_2$.

1. Construcción de códigos lineales con base en 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. *([**31**]) Sea $n = hr$ un entero impar. $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent, $a, b \in \mathbb{F}_{2^n}$. Sea*

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

y

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

Es fácil ver que $\mathcal{C}$ es 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. *([**31**]) El código $\mathcal{C}$ de la Definición 1.1 es un $[2^n - 1, 2n/h]_{2^h}$-código lineal, 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. Encontremos la dimensión del código. Para esto probemos 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 a $\mathcal{C}$ es equivalente a demostrar 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

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

La prueba es directa.

Probar que el conjunto D es linealmente independiente es equivalente a demostrar que el conjunto E lo es 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

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

entonces,

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

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,

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

$\forall x \in \mathbb{F}_{2^n}^*$, esto es una contradicción, pues como F es casi-bent,

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

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

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

y

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

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,

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

Como un último caso, 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 es una contradicción, pues como F es casi-bent, entonces,

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

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 utilizando el método de Massey a partir de este código.

TEOREMA 1.3. *([**31**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.1. Entonces $\mathcal{C}^\perp$ es un $[2^n - 1, 2^n - 1 - 2r, d^\perp]$-código lineal, donde $d^\perp \geq 2$.*

DEMOSTRACIÓN. Se sabe 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 una columna cero, ya que si se supone que la columna $j+1$, $j = 0, \ldots, 2^n - 2$, es 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 $\mathbb{F}_{2^n}^*$,

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

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

lo cual implica que $\alpha^j = 0$, siendo esto una contradicción.

Como G es una matriz generadora para $\mathcal{C}$, G es también una matriz verificadora de paridad para $\mathcal{C}^\perp$, es decir,

$$x \in \mathcal{C}^\perp \text{ si y sólo si } Gx^t = 0.$$

Por lo tanto si $x \in \mathcal{C}^\perp$ tiene peso 1, alguna de las columnas de G es cero, lo cual no es posible por la observación anterior, y de aquí se concluye la prueba. □

El siguiente resultado, el cual puede consultarse en [**9**], proporciona información 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,

$$\begin{aligned} & N(F; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) \\ := \; & |\{x \in \mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) = u_i, i = 1, \ldots, l\}|. \end{aligned}$$

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. Sea $\chi(\cdot) := (-1)^{Tr_{\mathbb{F}_{2^h}/\mathbb{F}_2}(\cdot)}$ 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,

$$\begin{aligned} & 2^{lh} N(F; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) \\ = \; & \sum_{x \in \mathbb{F}_{2^n}} \left[\sum_{y_1 \in \mathbb{F}_{2^h}} \chi(y_1(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_1 F(x) + b_1 x) - u_1)) \right] \cdots \\ \cdots \; & \left[\sum_{y_l \in \mathbb{F}_{2^h}} \chi(y_l(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_l F(x) + b_l x) - u_l)) \right] \\ = \; & \sum_{x \in \mathbb{F}_{2^n}} \sum_{y_1 \in \mathbb{F}_{2^h}} \cdots \sum_{y_l \in \mathbb{F}_{2^h}} \prod_{i=1}^{l} \chi\left(y_i(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) - u_i)\right) \\ = \; & \sum_{x \in \mathbb{F}_{2^n}} \sum_{y_1 \in \mathbb{F}_{2^h}} \cdots \sum_{y_l \in \mathbb{F}_{2^h}} \chi\left(\sum_{i=1}^{l} y_i(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) - u_i)\right) \\ = \; & 2^n + \sum_{\substack{y_1, \ldots, y_l \in \mathbb{F}_{2^h} \\ (y_1, \ldots, y_l) \neq (0, \ldots, 0)}} \\ & \sum_{x \in \mathbb{F}_{2^n}} \chi\left(\sum_{i=1}^{l} y_i(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(a_i F(x) + b_i x) - u_i)\right) \end{aligned}$$

$$
\begin{aligned}
&= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \\
&\quad \sum_{x\in\mathbb{F}_{2^n}} \chi\left(\sum_{i=1}^{l} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(y_i a_i F(x) + b_i x) - y_i u_i\right) \\
&= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \\
&\quad \sum_{x\in\mathbb{F}_{2^n}} \chi\left(\sum_{i=1}^{l} Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(y_i a_i F(x) + b_i x)\right) \chi\left(\sum_{i=1}^{l} y_i u_i\right) \\
&= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \\
&\quad \chi\left(\sum_{i=1}^{l} y_i u_i\right) \sum_{x\in\mathbb{F}_{2^n}} \chi\left(Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}\left(\sum_{i=1}^{l}(y_i a_i F(x) + b_i x)\right)\right) \\
&= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \\
&\quad \chi\left(\sum_{i=1}^{l} y_i u_i\right) \sum_{x\in\mathbb{F}_{2^n}} \psi\left(\sum_{i=1}^{l}(y_i a_i F(x) + b_i x)\right)
\end{aligned}
$$

$$
= 2^n + \sum_{\substack{y_1,\ldots,y_l \in \mathbb{F}_{2^h} \\ (y_1,\ldots,y_l) \neq (0,\ldots,0)}} \chi\left(\sum_{i=1}^{l} y_i u_i\right) \mu_{y_1 a_1 + \cdots + y_l a_l, y_1 b_1 + \cdots + y_l b_l}(F),
$$

donde $\mu_{c,d} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2(cF(x)+dx)}}$.

Ahora se fija $(y_1,\ldots,y_l) \neq (0,\ldots,0)$. Si $y_1 a_1 + \cdots + y_l a_l = 0$, entonces $y_1 b_1 + \cdots + y_l b_l \neq 0$ ya que $(a_1, b_1),\ldots,(a_l, b_l)$ son linealmente independientes sobre $\mathbb{F}_{2^h}$. Por lo tanto

$$
\mu_{y_1 a_1 + \cdots + y_l a_l, y_1 b_1 + \cdots + y_l b_l}(F) = 0.
$$

Supóngase ahora que $y_1a_1 + \cdots + y_la_l \neq 0$. Se sabe por $(*)$ del Capítulo 2 que la no-linealidad de una función vectorial es 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

$$\begin{aligned} & 2^{lh}N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l) - 2^n \\ = & \sum_{\substack{y_1,\ldots,y_l\in\mathbb{F}_{2^h} \\ (y_1,\ldots,y_l)\neq(0,\ldots,0)}} \chi\left(\sum_{i=1}^{l} y_iu_i\right)\mu_{y_1a_1+\cdots+y_la_l,y_1b_1+\cdots+y_lb_l}(F), \end{aligned}$$

lo cual implica que,

$$\begin{aligned} & |2^{lh}N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l) - 2^n| \\ \leq & \ | \sum_{\substack{y_1,\ldots,y_l\in\mathbb{F}_{2^h} \\ (y_1,\ldots,y_l)\neq(0,\ldots,0)}} \mu_{y_1a_1+\cdots+y_la_l,y_1b_1+\cdots+y_lb_l}(F)| \\ \leq & \sum_{\substack{y_1,\ldots,y_l\in\mathbb{F}_{2^h} \\ (y_1,\ldots,y_l)\neq(0,\ldots,0)}} 2^n - 2N_F \\ = & \ (2^n - 2N_F)|\{(y_1,\ldots,y_l)\in\mathbb{F}_{2^h}^l : y_1a_1+\cdots+y_la_l\neq 0\}| \\ \leq & \ (2^n - 2N_F)(2^{lh} - 2^{(l-1)h}). \end{aligned}$$

Por lo tanto,

$$|2^{lh}N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l) - 2^n| \leq (2^n - 2N_F)(2^{lh} - 2^{(l-1)h}),$$

de donde se concluye,

$$|N(F;a_1,b_1,\ldots,a_l,b_l;u_1,\ldots,u_l) - 2^{n-lh}| \leq (1 - \frac{1}{2^h})(2^n - 2N_F),$$

y el resultado queda probado. □

En las siguientes afirmaciones se considera a $\mathbb{F}_{2^h}$ un subcampo de $\mathbb{F}_{2^n}$.

COROLARIO 1.5. *([**31**]) Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función y $u_1, \ldots, u_{2^h-1}$ todos los elementos de $\mathbb{F}_{2^h}^*$. Entonces*

$$(2^h-1)\left(2^{n-h} - (1-\frac{1}{2^h})(2^n - 2N_F)\right) \leq |\{x \in \mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) \in \mathbb{F}_{2^h}^*\}|$$
$$\leq (2^h-1)\left(2^{n-h} + (1-\frac{1}{2^h})(2^n - 2N_F)\right).$$

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
$$\left||\{x \in \mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) \in \mathbb{F}_{2^h}^*\}| - (2^h-1)(2^{n-h})\right|$$
$$= \left|N_{u_1} - 2^{n-h} + N_{u_2} - 2^{n-h} + \cdots + N_{u_{2^h-1}} - 2^{n-h}\right|$$
$$\leq |N_{u_1} - 2^{n-h}| + \cdots + |N_{u_{2^h-1}} - 2^{n-h}| \leq (2^h-1)(1-\tfrac{1}{2^h})(2^n - 2N_F),$$

de donde se concluye el resultado. □

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. *([**31**]) Si $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ es una función casi-bent, entonces,*

$$(2^h-1)\left(2^{n-h} - (1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right) \leq |\{x \in \mathbb{F}_{2^n} : Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(x)+bx) \in \mathbb{F}_{2^h}^*\}|$$
$$\leq \quad (2^h-1)\left(2^{n-h} + (1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right).$$

DEMOSTRACIÓN. Como F es casi-bent, el resultado se sigue del Corolario 1.5 y del hecho que $N_F = 2^{n-1} - 2^{\frac{n-1}{2}}$. □

Lo siguiente, consecuencia inmediata del Corolario 1.6, proporciona una cota para los pesos del código lineal de la Definición 1.1.

COROLARIO 1.7. *([**31**]) Sea $\mathcal{C}$ el código de la Definición 1.1 y w el peso de una palabra distinta de cero de $\mathcal{C}$. Entonces,*

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

□

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 distintas de cero del código de la Definición 1.1.

COROLARIO 1.8. *([31]) Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función, tal que $F(0) = 0$. 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 $F(0) = 0$, 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. *([31]) Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent tal que $F(0) = 0$. 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. Dado que $N_F = 2^{n-1} - 2^{\frac{n-1}{2}}$, la afirmación se sigue del Corolario 1.8. □

Hasta el momento se ha usado el código de la Definición 1.1, en donde se considera a $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent la cual genera un código lineal. Respecto a este código se tiene lo siguiente:

COROLARIO 1.10. *([31]) 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. Entonces el peso w de cualquier*

palabra distinta de cero de $\mathcal{C}$ es tal que,

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

□

De este modo, con respecto al código lineal de la Definición 1.1 se ha determinado la longitud, dimensión, una cota para los pesos de las palabras distintas de cero y una cota para el peso mínimo del código dual.

Construcción $n = hr$, $h = 1$.

Ahora se da 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, en particular la distribución de pesos, a comparación del código definido anteriormente.

DEFINICIÓN 1.11. *([**31**]) Sea n impar, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent y $a, b \in \mathbb{F}_{2^n}$. Se define*

$$F_{a,b}(x) := aF(x) + bx \ , \ C_{a,b} := (Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(F_{a,b}(\gamma))_{\gamma \in \mathbb{F}_{2^n}^*})$$

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 $\mathbb{F}_2$ y su dimensión está dada por el siguiente resultado.

TEOREMA 1.12. *([**31**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.11. $\mathcal{C}$ es un $[2^n - 1, 2n]_2$-código lineal, 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 demostración se sigue del Teorema 1.2, tomando en cuenta que es un caso particular de ese resultado. □

Estamos interesados en conocer la distribución de pesos de este código lineal, el 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 ([**43**]).

TEOREMA 1.13. *([**31**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Entonces $\mathcal{C}^\perp$ tiene peso mínimo mayor o igual que 3.*

DEMOSTRACIÓN. El caso cuando $d^\perp$ tiene peso mínimo mayor o igual a 2 se sigue del Teorema 1.3 cuando $h = 1$. Veamos lo que resta de la prueba. Si dos columnas de G son

iguales, digamos las columnas $i+1$ y $j+1$, sin pérdida de generalidad se puede suponer que $i<j$, entonces,

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

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

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

por lo que,

$$\begin{aligned}&Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}((\alpha^j-\alpha^i)x)=e_0Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^j-\alpha^i)+e_1Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+1}-\alpha^{i+1})\\&+\cdots+e_{r-1}Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(\alpha^{j+r-1}-\alpha^{i+r-1})=0,\ \forall x.\end{aligned}$$

De aquí se sigue que $\alpha^j-\alpha^i=0$, lo que implica, $\alpha^j=\alpha^i$, lo cual es una contradicción. Ahora, si una palabra $x\in\mathcal{C}^\perp$ tiene peso 2, entonces 2 columnas de G son iguales (Teorema 1.3), luego, por lo anterior se tiene una contradicción. Por lo tanto el código lineal $\mathcal{C}$ tiene peso mínimo mayor que 2. □

TEOREMA 1.14. *(*[**31**]*) Sea $\mathcal{C}$ el código lineal binario de la Definición 1.11. Si w es el peso de una palabra distinta de cero de $\mathcal{C}$, entonces*

$$w\in\{2^{n-1}-2^{\frac{n-1}{2}},\ 2^{n-1}+2^{\frac{n-1}{2}},\ 2^{n-1}\}.$$

DEMOSTRACIÓN. Si $\lambda_F(b,a)=\widehat{\zeta_{a\cdot F}}(b)=2^{\frac{n+1}{2}}$, se define

$$\begin{aligned}A&=|\{x\in\mathbb{F}_{2^n}:x\in Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x)+bx)=1\}|\ \text{ y}\\B&=|\{x\in\mathbb{F}_{2^n}:Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(aF(x)+bx)=0\}|.\end{aligned}$$

Entonces,

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

luego,

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

y por consiguiente

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

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

$$B-A=\widehat{\chi}_{bF}(a)=-2^{\frac{n+1}{2}},$$

entonces,

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

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 $B=A$. Por lo tanto $A=2^{n-1}$ y de aquí se prueba la afirmación. □

Con base en los resultados anteriores es posible obtener la distribución de pesos del código lineal de la Definición 1.11.

TEOREMA 1.15. *([**31**]) Los parámetros del código lineal binario $\mathcal{C}$ de la Definición 1.11, son los de un*

$$[2^n - 1, 2n, 2^{n-1} - 2^{\frac{n-1}{2}}]_2 \text{ - código lineal.}$$

Si A_i es el número de palabras de peso i del código $\mathcal{C}$, entonces $A_i = 0$, para toda i, 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. Del Teorema 1.7 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 representan 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,

$A_a + A_b + A_c = 2^{2n} - 1,$
$2^{n-1}A_a + (2^{n-1} - 2^{\frac{n-1}{2}})A_b + (2^{n-1} + 2^{\frac{n-1}{2}})A_c = 2^{2n-1}(2^n - 1)$
$(2^{n-1})^2 A_a + (2^{n-1} - 2^{\frac{n-1}{2}})^2 A_b + (2^{n-1} + 2^{\frac{n-1}{2}})^2 A_c = 2^{3n-2}(2^n - 1).$

Resolviendo el sistema se tiene el resultado deseado. □

Obsérvese que $\mathcal{C}$ es un código con solo tres pesos.

De acuerdo a las condiciones del código $\mathcal{C}$, el Teorema 1.15 se puede ver como un caso especial de la siguiente afirmación ([**13**]):

TEOREMA 1.16. *Sea $\mathcal{D}$ un $[2^n - 1, 2n, d]$ - código lineal binario tal que $\mathbf{1} = (1, \ldots, 1) \notin \mathcal{D}$. Sea $d^{\perp} \geq 3$ y w_0 el más pequeño valor de 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 tiene si 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 de interes, $\mathcal{C}$, 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 además $2^{n-1} - 2^{\frac{n-1}{2}}$ 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 sobre el campo $\mathbb{F}_{p^n}$, $2 \neq p$ primo y n un entero positivo. En esta Sección se presentan esquemas similares a los anteriores, ahora utilizando funciones casi-bent, es decir, el caso sobre campos finitos de característica 2. Una vez construidos los códigos lineales con base en funciones casi-bent en la Sección anterior, ya es posible utilizarlos 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. *([**31**]) 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,

$$\frac{w_{\textbf{mín}}}{w_{\textbf{máx}}} \geq \frac{(2^h-1)\left(2^{n-h} - (1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right)}{(2^h-1)\left(2^{n-h} + (1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right)} = \frac{2^{n-h} - \frac{2^h-1}{2^h}(2^{\frac{n+1}{2}})}{2^{n-h} + \frac{2^h-1}{2^h}(2^{\frac{n+1}{2}})}$$

$$= \frac{2^n - (2^h-1)(2^{\frac{n+1}{2}})}{2^n + (2^h-1)(2^{\frac{n+1}{2}})} = \frac{2^{\frac{n-1}{2}} - (2^h-1)}{2^{\frac{n-1}{2}} + (2^h-1)}.$$

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,

$$\frac{w_{\mathbf{mín}}}{w_{\mathbf{máx}}}>\frac{2^h-1}{2^h},$$

y el resultado se sigue del Teorema 2.5 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 $\frac{w_{\mathbf{mín}}}{w_{\mathbf{máx}}}$ 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. *([**31**]) 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 distinta cero del código es mínima.*

DEMOSTRACIÓN. Del Corolario 1.10 se sigue que,

$$\frac{w_{\mathbf{mín}}}{w_{\mathbf{máx}}}\geq\frac{\frac{2^h-1}{2^h}(2^n-2^{\frac{n+1}{2}})}{\frac{2^h-1}{2^h}(2^n+2^{\frac{n+1}{2}})}=\frac{2^{\frac{n+1}{2}}(2^{\frac{n-1}{2}}-1)}{2^{\frac{n+1}{2}}(2^{\frac{n-1}{2}}+1)}=\frac{2^{\frac{n-1}{2}}-1}{2^{\frac{n-1}{2}}+1}.$$

Si $n\geq 3h$, $h\geq 3$,

$$2^{h+1}=2^h2=(2^{2h}2^2)^{1/2}=(\frac{2^{2h}2^3}{2})^{1/2}\leq(\frac{2^{2h}2^h}{2})^{1/2}=(\frac{2^{3h}}{2})^{1/2}=2^{\frac{3h-1}{2}}\leq 2^{\frac{n-1}{2}},$$

luego,

$$2^{h+1}-1<2^{\frac{n-1}{2}},$$

por lo que,

$$2^h2^{\frac{n-1}{2}}-2^h>2^h2^{\frac{n-1}{2}}+2^h-2^{\frac{n-1}{2}}-1,$$

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,

$$\frac{w_{\textbf{mín}}}{w_{\textbf{máx}}} > \frac{2^h-1}{2^h},$$

y el resultado se sigue del Teorema 2.5 del Capítulo 4. □

TEOREMA 2.3. *([**31**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Si $n > 3$, entonces toda palabra distinta de cero de $\mathcal{C}$ es una palabra mínima.*

DEMOSTRACIÓN. Por el Teorema 1.14,

$$w_{\textbf{mín}} = 2^{n-1} - 2^{\frac{n-1}{2}} \text{ y } w_{\textbf{máx}} = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

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,

$$\frac{2^{n-1} - 2^{\frac{n-1}{2}}}{2^{n-1} + 2^{\frac{n-1}{2}}} > \frac{1}{2},$$

y el resultado se sigue del Teorema 2.5 del Capítulo 4. □

Obsérvese que si $n = 1$, entonces se contradice la desigualdad del resultado anterior.

Ahora ya es posible dar un esquema de compartición de secretos proporcionando resultados similares a los descritos en [**7**], para el caso $p \neq 2$, utilizando el código lineal basado en la función casi-bent $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ de la Definición 1.1:

TEOREMA 2.4. *([**31**]) Sea $\mathcal{C}$ el código lineal de la Definición 1.11. Sea n impar tal que $n \geq 5h$, $h \geq 3$, 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 mínimos de acceso.*
- *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 mínimos de acceso.

DEMOSTRACIÓN. La prueba se sigue del Teorema 2.1, Teorema 2.2, Teorema 2.4 del Capítulo 4 y utilizando el hecho de que $d^\perp > 2$. □

TEOREMA 2.5. *([**31**]) 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 mínimos de acceso.*
- *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 mínimos de acceso.*

DEMOSTRACIÓN. La afirmación se sigue del Teorema 2.3 y el Teorema 2.4 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 número cero o el uno, 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 nuevo esquema es un elemento de
$$s = (s_1, s_2, \ldots, s_l) \in \mathbb{F}_2^l.$$
- 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 el fragmento $t_{i,j}$ 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 el fragmento $(t_{i,1}, t_{i,2}, \ldots, t_{i,l})$.

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 el fragmento $(t_{i,1}, t_{i,2}, \ldots, t_{i,l})$, 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 pueden utilizar son $\mathbb{F}_{2^3}$ y $\mathbb{F}_{2^{15}}$. Esto es por la condición $h \geq 3$ y $n \geq 5h$ al considerar $\mathbb{F}_{2^h}$ y $\mathbb{F}_{2^n}$, la cual asegura que todas las palabras del código son mínimas.

Capítulo 6

Esquemas de autenticación con base en funciones bent y casi-bent sobre campos finitos

En este Capítulo se introduce la definición de una clase de esquemas de autenticación, y posteriormente utilizando las funciones bent y las casi-bent construcciones de estos esquemas son dadas.

Un esquema de autenticación provee un método para 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 el transmisor como el 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 existe el riesgo de que un intruso pueda deliberadamente observar, y más aún, causar un disturbio en la comunicación. Se supone que el intruso 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 intruso deliberadamente elige un mensaje y lo inserta en el canal esperando que el receptor lo acepte como auténtico. Sea P_I la máxima probabilidad de que en este ataque se acepte el nuevo mensaje. En el ataque por substitución el intruso 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. Sea P_S la máxima probabilidad de que en este ataque se acepte el nuevo mensaje. En este trabajo se asume que todos los elementos del espacio fuente y del espacio llave son igualmente probables de ser elegidos. Para mayores detalles sugerimos al lector consultar, por ejemplo, [**50**].

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 ([**21**]):

$$P_I = \max_{s \in \mathcal{S}, t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : E_k(s) = t\}|}{|\mathcal{K}|}.$$

Como en el ataque por substitución el oponente observa el mensaje dado por $m = (s, t)$ y lo reemplaza con otro mensaje $m' = (s', t')$, donde $s \neq s'$, y ya que las llaves y los elementos del espacio fuente son igualmente probables, entonces ([**21**]):

$$P_S = \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|}.$$

El intruso 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 las más pequeñas posibles.

Ya que

$$|\mathcal{T}|P_I \geq \sum_{t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : E_k(s) = t\}|}{|\mathcal{K}|} = 1,$$

y en forma análoga para P_S, se tienen las siguientes cotas generales para P_I y P_S ([**21**]):

$$P_I \geq \frac{1}{|\mathcal{T}|} \text{ y } P_S \geq \frac{1}{|\mathcal{T}|}.$$

Por lo tanto el objetivo es tener P_I y P_S lo más cercano posible a $\frac{1}{|\mathcal{T}|}$.

EJEMPLO 0.1. *(*[**50**]*) Considérese la siguiente construcción de un esquema de autenticación:*

$$\begin{aligned} \mathcal{S} &= \mathbb{Z}_3 \\ \mathcal{T} &= \mathbb{Z}_3, \\ \mathcal{K} &= \mathbb{Z}_3 \times \mathbb{Z}_3, \\ \mathcal{E} &= \{e_{i,j} : (i, j) \in \mathcal{K}\}, \end{aligned}$$

donde $e_{ij}(s) = is + j$ *mód* 3.

Analicemos el ejemplo anterior. 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 intruso inserte en el canal, $P_I = \frac{3}{9} = \frac{1}{3}$, 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 intruso observa el mensaje $(0,0)$ en el canal. Esto le proporciona información acerca de la llave. Él sabe que la llave k_0 se encuentra en el conjunto,

$$\{(0,0),(1,0),(2,0)\}.$$

Si el intruso remplaza el mensaje $(0,0)$ con el mensaje $(1,1)$, el intruso 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, es decir, para cada elección (s',t') del enemigo siempre existe una única llave de las tres posibles que autentica el mensaje.

En el resto del Capítulo se da la construcción de esquemas de autenticación, una utilizando funciones bent $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, q la potencia de un primo, y otra utilizando funciones casi-bent $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. 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 ([**21**]).

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

$$E_k(s) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k_1) + bk_1) + k_2,$$

$k = (k_1, k_2) \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

Es importante conocer la relación entre las llaves y las reglas de codificación.

TEOREMA 1.2. *([**21**]) La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H(k) = E_k$ es una biyección.*

□

El siguiente resultado da aproximaciones para P_I y P_S :

TEOREMA 1.3. *([**21**]) 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, $|\mathcal{S}| = q^{2n}, |\mathcal{T}| = q, |\mathcal{K}| = |\mathcal{E}| = q^{n+1}$.

□

En el esquema anterior P_I y su cota coinciden. Para valores de P_I pequeños se consideran valores grandes de q. Para obtener un valor pequeño de P_S se puede considerar una extensión de orden considerable entre $\mathbb{F}_{q^n}$ y $\mathbb{F}_q$.

Analicemos el siguiente ejemplo: Considérese $\mathbb{F}_{3^2}$, $\mathbb{F}_3$ y la función bent $F(x) = x^2$. Utilizando el esquema anterior, con la fórmula de las cotas se tiene que $P_I = 1/3$ y $P_S \leq 5/9$. Por medio de un programa computacional en Maple se ha probado 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 $\mathbb{F}_3$, ya que cualquier elemento del campo $\mathbb{F}_3$ se obtiene 9 veces al aplicarle la traza a los elementos del campo $\mathbb{F}_{3^2}$, por ejemplo,

$$\begin{aligned}&|\{(k_1, k_2) \in \mathbb{F}_{3^2} : E_k(\alpha, \alpha + 2) = 1\}|\\ = \ &|\{(k_1, k_2) : Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha F(k_1) + (\alpha + 2)k_1) + k_2 = 1\}| = 9,\end{aligned}$$

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.

1.2. Construcción 2.

Ahora se define un esquema de autenticación basado en funciones bent ([**21**]),

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

$$E_k(s) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(aF(k) + bk),$$

$k \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

TEOREMA 1.5. *([**21**]) La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección.*

□

El siguiente resultado ([**21**]) es de importancia para la obtención de cotas para 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*

$$N(a_1, b_1, a_2, b_2; u_1, u_2) = |\{x \in \mathbb{F}_{q^n} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_i F(x) + b_i x) = u_i, i = 1, 2\}|.$$

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 $\mathbb{F}_q$. Sea $\chi(\cdot) := e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(\cdot)/p}$ el caracter aditivo canónico de $\mathbb{F}_q$ y $\psi(\cdot) := e^{2\pi i Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\cdot)/p}$ el caracter aditivo canónico de $\mathbb{F}_{q^n}$. Entonces

$$\begin{aligned}
&q^2 N(F; a_1, b_1, a_2, b_2; u_1, u_2)\\
= &\sum_{x \in \mathbb{F}_{q^n}} \left[\sum_{y_1 \in \mathbb{F}_q} \chi(y_1(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_1 F(x) + b_1 x) - u_1)) \right]\\
&\left[\sum_{y_2 \in \mathbb{F}_q} \chi(y_2(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_2 F(x) + b_2 x) - u_2)) \right]
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{x\in\mathbb{F}_{q^n}}\sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\prod_{i=1}^{2}\chi\left(y_i(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_iF(x)+b_ix)-u_i)\right)\\
&= \sum_{x\in\mathbb{F}_{q^n}}\sum_{y_1\in\mathbb{F}_q}\sum_{y_2\in\mathbb{F}_q}\chi\left(\sum_{i=1}^{2}y_i(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_iF(x)+b_ix)-u_i)\right)\\
&= q^n+\sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}}\sum_{x\in\mathbb{F}_{q^n}}\chi\left(\sum_{i=1}^{2}y_i(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_iF(x)+b_ix)-u_i)\right)\\
&= q^n+\sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}}\sum_{x\in\mathbb{F}_{q^n}}\chi\left(\sum_{i=1}^{2}Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y_ia_iF(x)+b_ix)-y_iu_i\right)\\
&= q^n+\sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}}\sum_{x\in\mathbb{F}_{q^n}}\chi\left(\sum_{i=1}^{2}Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y_ia_iF(x)+b_ix)\right)\chi\left(-\sum_{i=1}^{2}y_iu_i\right)\\
&= q^n+\sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}}\chi\left(-\sum_{i=1}^{2}y_iu_i\right)\sum_{x\in\mathbb{F}_{q^n}}\chi\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\sum_{i=1}^{2}(y_ia_iF(x)+b_ix)\right)\right)\\
&= q^n+\sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}}\chi\left(-\sum_{i=1}^{2}y_iu_i\right)\sum_{x\in\mathbb{F}_{q^n}}\psi\left(\sum_{i=1}^{2}(y_ia_iF(x)+b_ix)\right)\\
&= q^n+\sum_{\substack{y_1,y_2\in\mathbb{F}_q\\(y_1,y_2)\neq(0,0)}}\chi\left(-\sum_{i=1}^{2}y_iu_i\right)\mu_{y_1a_1+y_2a_2,y_1b_1+y_2b_2}(F),
\end{aligned}
$$

$$\text{donde } \mu_{c,d}=\sum_{x\in\mathbb{F}_{q^n}}e^{2\pi iTr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(cF(x)+dx)/p}.$$

Sea $(y_1,y_2)\neq(0,0)$ un elemento constante. 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,

$$|q^2N(F; a_1, b_1, a_2, b_2; u_1, u_2) - q^n| \leq \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}} |\mu_{y_1a_1+y_2a_2, y_1b_1+y_2b_2}(F)|$$

$$\leq \sum_{\substack{y_1, y_2 \in \mathbb{F}_q \\ (y_1, y_2) \neq (0,0)}} q^{n/2} = (q^2 - q)q^{n/2}.$$

De aquí se tiene el resultado. □

En el siguiente resultado se obtienen cotas superiores para P_I y P_S.

TEOREMA 1.7. *([**21**]) Para el esquema de autenticación definido anteriormente,*

$$P_I \leq \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{n/2}},\ P_S \leq \frac{1}{q} + \frac{q^2-1}{q(q^{n/2} - q + 1)}.$$

Más aún, $|\mathcal{S}| = q^n + 1, |\mathcal{T}| = q, |\mathcal{K}| = |\mathcal{E}| = q^n$.

DEMOSTRACIÓN. Para cualquier elemento $(a, b) \in \mathcal{S}$, 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,

$$\begin{aligned} P_I &= \text{máx}_{s \in \mathcal{S}, t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(af(k) + bk) = t\}}{|\mathcal{K}|} \\ &\leq \frac{q^n + (q-1)q^{n/2}}{q^{n+1}} = \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{n/2}}. \end{aligned}$$

Ahora realicemos el análisis respectivo para 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,

$$\begin{aligned} P_S = & \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|} \\ & \leq \frac{q^n + (q^2 - q)q^{n/2}}{(q^n - (q-1)q^{n/2})q} = \frac{1}{q} + \frac{q^2 - 1}{q(q^{n/2} - q + 1)}. \end{aligned}$$

□

Un análisis similar al caso anterior se puede hacer respecto a este esquema.

Veamos los siguientes ejemplos, los cuales fueron hechos utilizando el programa computacional Maple:

Considérese $\mathbb{F}_{3^2}$ y $\mathbb{F}_3$ y la función bent $F(x) = x^2$. Utilizando el esquema anterior se tiene, $P_I \leq 0.5555$ y $P_S \leq 3$ (con la fórmula de las cotas). Por medio del programa 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 $\mathbb{F}_{3^2}$. Nótese que P_S no es una buena cota. Más aún, con ayuda del programa, $P_S = 2/2 = 1$, ya que

$$|\{k \in \mathbb{F}_{3^2} : E_k(1, \alpha^5) = 1,\ E_k(1, \alpha^2) = 2\}| = 2$$

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 este valor, lo cual no es recomendable, pues el objetivo es encontrar el menor valor 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, $P_I \leq 0.4074$ y $P_S \leq 0.7142$ (con la fórmula de las cotas). Por medio del programa, $P_I = 30/81 = 0.3703$. Este resultado se puede obtener 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,

$$|\{k \in \mathbb{F}_{3^4} : E_k(0, 1) = 1,\ E_k(1, \alpha^{16}) = 2\}| = 12.$$

Como $|\{k \in \mathbb{F}_{3^4} : E_k(0, 1) = 1\}| = 27$, entonces $P_S = 12/27 = 0.4444$, pues es la mayor razón que se puede determinar. En este caso la cota de P_I disminuye respecto al

ejemplo anterior y mejor aún, P_I no alcanza la respectiva cota. Por otro lado la cota de P_S ya es algo significativa, aunque P_S no la alcanza.

Cabe mencionar que estos 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 ([**9**]), en el cual un parámetro revelante es la no-linealidad de la función. A continuación se presentan 2 construcciones basadas en funciones casi-bent. Para mayores detalles consúltese [**9**].

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. Considérese el 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

$$E_k(s) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(af(k_1) + bk_1) + k_2,$$

$k = (k_1, k_2) \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

TEOREMA 2.2. *La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección.*

□

En el siguiente resultado se obtienen cotas para P_I y P_S ([**9**]):

TEOREMA 2.3. *Sea el esquema de autenticación de la Definición 2.1. Entonces*

$$P_I = \frac{1}{2^h} \text{ y } P_S \leq \frac{1}{2^h} + \left(1 - \frac{1}{2^h}\right)\left(1 - \frac{N_F}{2^{n-1}}\right).$$

Más aún,

$$|\mathcal{S}| = 2^{2n}, |\mathcal{T}| = 2^h, |\mathcal{K}| = |\mathcal{E}| = 2^{n+h}.$$

□

TEOREMA 2.4. *([**9**]) Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent, en este caso, para el esquema de autenticación definido anteriormente,*

$$P_I = \frac{1}{2^h} \text{ y } P_S \leq \frac{1}{2^h} + \frac{1 - 2^{-h}}{2^{\frac{n-1}{2}}}.$$

□

Se omitieron ejemplos en este caso, debido a 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 ([**9**]):

DEFINICIÓN 2.5. *Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función. Se da el siguiente 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

$$E_k(s) = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_{2^h}}(aF(k) + bk),$$

$k \in \mathcal{K}$, $s = (a, b) \in \mathcal{S}$.

TEOREMA 2.6. *([**9**]) La función $H : \mathcal{K} \to \mathcal{E}$ definida por $H : k \to E_k$ es una biyección*

□

TEOREMA 2.7. *([**9**]) Considérese el esquema de autenticación anterior. Entonces,*

$$P_I \leq \frac{1}{2^h} + \left(1 - \frac{1}{2^h}\right)\left(1 - \frac{N_F}{2^{n-1}}\right),\ P_S \leq \frac{1}{2^h} + \frac{(2^h - 2^{-h})(2^n - 2N_F)}{2^n - (2^h - 1)(2^n - 2N_F)}.$$

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. *([**9**]) Sea $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ una función casi-bent. Entonces en el esquema de autenticación definido anteriormente,*

$$P_I \leq \frac{1}{2^h} + \left(\frac{2^h - 1}{2^h}\right)\frac{1}{2^{\frac{n-1}{2}}}\ y\ P_S \leq \frac{1}{2^h} + \frac{2^{2h} - 1}{2^h\left(2^{\frac{n-1}{2}} - 2^h + 1\right)}.$$

□

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, $P_I \leq 0.1796$ y $P_S \leq 1$ (con la fórmula de las cotas). En este caso también se omitieron ejemplos. Para obtener un valor pequeño de P_S se puede considerar una extensión de orden considerable entre $\mathbb{F}_{2^n}$ y $\mathbb{F}_{2^h}$.

Capítulo 7

Esquemas de autenticación con base en funciones bent sobre anillos de Galois

En este Capítulo se presenta la construcción de esquemas de autenticación utilizando las funciones bent sobre anillos de Galois de característica p^2, p un número primo, y la función de Gray sobre estos anillos. En un caso el esquema propuesto es sobre anillos de Galois ([**10**]) y en otro sobre campos finitos ([**30**]), ya que al utilizar la función de Gray ([**25**]) para elementos de un anillo de Galois se obtienen elementos en el campo finito correspondiente.

Las cotas obtenidas para el esquema de autenticación utilizando la función de Gray son mejores respecto a las obtenidas en [**21**], [**9**] y [**42**] (que es en estos trabajos de donde se generaron las ideas para los esquemas que aquí se construyen), y se dan las comparaciones así como ejemplos de funciones bent los cuales no puede ser utilizados para la construcción de los códigos de autenticación presentados en este Capítulo, resaltando de este modo la importancia de la familia de funciones bent encontrada en el Capítulo 3. Los resultados aquí presentados aparecen en [**10**].

1. Definiciones y conceptos previos

Algunas operaciones con caracteres sobre anillos de Galois, definición de peso homogéneo y función de Gray son dados en esta Sección.

Los siguientes resultados son importantes para la construción de los esquemas de autenticación

LEMA 1.1. *([**42**]) Sea* $\chi_u = e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(ux)/p^s}$ *(ver Capítulo 3),* $R = GR(p^s, m)$. *Si* $u \in R$, *entonces*

$$\sum_{x \in R} \chi_u(x) = \begin{cases} q^s & si \quad u = 0 \\ 0 & si \quad u \neq 0 \end{cases}.$$

DEMOSTRACIÓN. El primer caso es fácil de demostrar. Para el segundo caso se utiliza parte de la prueba del Lema 2.11 del Capítulo 3, por la cual se sabe que para un elemento $u \in R$ distinto de cero existe un elemento $x \in R$ tal que $T_{R/\mathbb{Z}_{p^s}}(ux) \neq 0$, de esta manera procediendo de modo similar a la prueba del Lema 2.11 se obtiene el resultado deseado. □

En adelante se denotará por R al anillo de Galois $GR(p^s, m)$.

LEMA 1.2. *([**42**]) Si $u \in R$,*

$$\sum_{x \in pR} \chi_u(x) = \begin{cases} q^{s-1} & si \quad u \in p^{s-1}R \\ 0 & si \quad u \in R \backslash p^{s-1}R \end{cases}.$$

DEMOSTRACIÓN. El primer caso es claro. Ahora para el segundo caso si se considera un elemento $u \in R\backslash p^{s-1}R$, entonces la suprayectividad de la función traza implica la existencia de un elemento $y \in p^{s-1}R$ tal que $T_{R/\mathbb{Z}_{p^s}}(uy) \neq 0$. La prueba es finalizada utilizando el Lema anterior. □

LEMA 1.3. *([**42**]) Si $u \in R$,*

$$\sum_{x \in R \backslash pR} \chi_u(x) = \begin{cases} q^s - q^{s-1} & si \quad u = 0 \\ -q^{s-1} & si \quad u \in p^{s-1}R\backslash\{0\} \\ 0 & si \quad u \in R\backslash p^{s-1}R \end{cases}.$$

DEMOSTRACIÓN. La prueba se sigue de los Lemas anteriores. □

DEFINICIÓN 1.4. *([**42**]) Sea $u \in R$,*

$$s(u) := \sum_{x \in R \backslash pR} e^{2\pi i T_{R/\mathbb{Z}_{p^s}}(ux)/p^s} \text{ y } w_h(u) := -\frac{1}{q}s(u) + (q^{s-1} - q^{s-2}).$$

w_h es llamado el peso homogéneo en R.

Con base en los resultados anteriores el peso homogéneo en R está dado por,

$$w_h(u) = \begin{cases} 0 & \text{si} \quad u = 0 \\ q^{s-1} & \text{si} \quad u \in p^{s-1}R\backslash\{0\} \\ q^{s-1} - q^{s-2} & \text{si} \quad u \in R\backslash p^{s-1}R \end{cases}.$$

Una herramienta muy importante ya que proporciona una relación entre los anillos de Galois y los campos finitos es la función de Gray sobre los anillos de Galois.

DEFINICIÓN 1.5. *([**25**]) La función de Gray sobre R está definida como*

$$\begin{array}{rccc} \Phi : & R & \to & \mathbb{F}_q^{q^{s-1}} \\ & r_0 + r_1 p + \cdots + r_{s-1}p^{s-1} & \to & \overline{r}_0 c_0 + \overline{r}_1 c_1 + \cdots + \overline{r}_{s-1} c_{s-1} \end{array},$$

donde

$$\mathcal{T}_R := \{0, 1, \eta, \ldots, \eta^{q-1}\},$$

$$c_i := (v + \delta_{i0}(u - v) \otimes \cdots \otimes v + \delta_{is-2}(u - v)), \quad i = 0, \ldots, s-1,$$

y

$$v := (1, \ldots, 1) \in \mathbb{F}_q^q, u := (0, \overline{\eta}, \overline{\eta}^2, \ldots, \overline{\eta}^{q-1}) \in \mathbb{F}_q^q.$$

$\mathcal{T}_R$ está definido en el Teorema 2.7 del Capítulo 3 y $\overline{*}$ es la reducción módulo p.

Una manera más clara de expresar los elementos c_i, $i = 1, \cdots, s-1$, es:

$$\begin{aligned} c_0 &= (u \otimes v \otimes \cdots \otimes v) \in \mathbb{F}_q^{q^{s-1}} \\ c_1 &= (v \otimes u \otimes \cdots \otimes v) \in \mathbb{F}_q^{q^{s-1}} \\ &\cdots \\ c_{s-2} &= (v \otimes v \otimes \cdots \otimes u) \in \mathbb{F}_q^{q^{s-1}} \\ c_{s-1} &= (v \otimes v \otimes \cdots \otimes v) \in \mathbb{F}_q^{q^{s-1}} \end{aligned}$$

En particular para un anillo de Galois de característica p^2 ([**42**]),

$$\begin{array}{rccc} \Phi: & GR(p^2, m) & \to & \mathbb{F}_q^q \\ & r_0 + r_1 p & \to & \left(\overline{r_1}, \overline{r_1 + \eta r_0}, \overline{r_1 + \eta^2 r_0}, \ldots, \overline{r_1 + \eta^{q-1} r_0}\right), \end{array}$$

donde $\mathcal{T}_{GR(p^2,m)} := \{0, 1, \eta, \ldots, \eta^{q-1}\}$.

Sea

$$d_h(u, v) = w_h(u - v)$$

la distancia homogénea inducida por el peso homogéneo, $u, v \in R$.

TEOREMA 1.6. *([**25**]) Sean $u, v \in R$. Entonces*

$$d_h(u, v) = d_H(\Phi(u), \Phi(v)),$$

donde d_H es la distancia de Hamming.

□

Obsérvese que se tiene una isometría entre los anillos de Galois y los campos finitos, considerando la distancia homogénea y la distancia de Hamming respectivamente, esta importante propiedad será de utilidad para un esquema propuesto.

2. Esquemas de autenticación sobre anillos de Galois

Se ha construido una familia de funciones bent sobre anillos de Galois de característica p^2, en el Capítulo 3, Sección 3, Teorema 3.3, la cual satisface que cuando u es una unidad y f es una función bent, entonces la funcion uf también es bent. En el transcurso de este Capítulo también se probará que si f es una función bent de $R = GR(p^2, m)$ a R y u una unidad de $\mathbb{Z}_{p^2}$, entonces uf es también una función bent.

En lo que resta de esta Sección se considera $S = GR(p^2, mn)$ y $R = GR(p^2, m)$ tal que S es una extensión de R. La siguiente construcción de un esquema es basada en funciones bent donde dada una función bent $f : S \to S$ y u una unidad de S, entonces uf es también una función bent. En particular los resultados obtenidos son válidos para la familia de funciones bent encontrada en el Capítulo 3.

2.1. Esquema 1.

Utilizando la notación del Capítulo 6 y considerando una función bent $f : S \longrightarrow S$ tal que uf es bent para cualquier $u \in U_S$, donde U_S es el grupo de unidades del anillo de Galois S, se propone el siguiente esquema de autenticación:

$$\begin{aligned}
&\mathcal{S} := \mathcal{T}_S \times S,\\
&\mathcal{T} := R,\\
&\mathcal{K} := S \times R,\\
&\mathcal{E} := \{E_k(s) = T_{S/R}(af(x) + bx) + y,\ k = (x, y) \in \mathcal{K}, s = (a, b) \in \mathcal{S}\},
\end{aligned}$$

donde $S = GR(p^2, mn)$ y $R = GR(p^2, m)$. Recuérdese que $\mathcal{T}_S$ es el conjunto de Teichmüller del anillo S.

Para poder encontrar cotas superiores para P_I y P_S se da el siguiente resultado.

TEOREMA 2.1. *([**10**]) Sean $q = p^m$, S y R como antes y $f : S \longrightarrow S$ una función bent tal que uf es también bent para toda $u \in U_S$. Para $(a, b) \in \mathcal{T}_S \times S$ con $(a, b) \neq (0, 0)$ y $y \in R$, sea*

$$N(a, b, y) := \left|\{x \in S : T_{S/R}(af(x) + bx) = y\}\right|.$$

Entonces,

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

DEMOSTRACIÓN. Obsérvese que si $T_{S/R}(af(x) + bx) - y = 0$,

$$\sum_{r \in R\backslash pR} e^{2\pi i T_{R/\mathbb{Z}_{p^t}}((T_{S/R}(af(x)+bx)-y)r)/p^t} = |R\backslash pR|,$$

y si $T_{S/R}(af(x) + bx) - y \neq 0$, del Lema 1.3 se sigue que,

$$\sum_{r \in R\backslash pR} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}((T_{S/R}(af(x)+bx)-y)r)/p^2} \geq -q.$$

Entonces,

$$\begin{aligned}
&|R\backslash pR|N(a, b, y) + (|S| - N(a, b, y))(-q)\\
\leq\ &\sum_{x \in S}\sum_{r \in R\backslash pR} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}\left(\left(T_{S/R}(af(x)+bx)-y\right)r\right)/p^2}\\
=\ &\sum_{r \in R\backslash pR}\sum_{x \in S} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}\left(\left(T_{S/R}(af(x)+bx)-y\right)r\right)/p^2}\\
=\ &\sum_{r \in R\backslash pR}\left(e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(-yr)/p^2}\sum_{x \in S} e^{2\pi i T_{S/\mathbb{Z}_{p^2}}((af(x)+bx)r)/p^2}\right).
\end{aligned}$$

De las propiedades de la suma y de que (arf) es una función bent en S, si $a \neq 0$ se tiene que,

$$\begin{aligned} & |R\backslash pR|N(a,b,y) + (|S| - N(a,b,y))\,(-q) \\ \leq & \sum_{r\in R\backslash pR} \left| e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(-yr)/p^2} \right| \left| \sum_{x\in S} e^{2\pi i T_{S/\mathbb{Z}_{p^2}}((af(x)+bx)r)/p^2} \right| \\ = & \ (q^2-q)q^n. \end{aligned}$$

Por lo tanto,

$$(q^2-q)N(a,b,y) + (q^{2n} - N(a,b,y))(-q) \leq (q^2-q)q^n,$$

lo cual implica,

$$N(a,b,y)q^2 - q^{2n+1} \leq (q^2-q)q^n,$$

y la afirmación del Teorema se sigue en este caso.

Si $a = 0$, ya que $(a,b) \neq (0,0)$, luego $b \neq 0$ y $br \neq 0$ pues $r \in R\backslash pR$. Entonces por el Lema 1.1,

$$\sum_{x\in S} e^{2\pi i T_{S/\mathbb{Z}_{p^2}}((af(x)+bx)r)/p^2} = 0,$$

por lo que $N(a,b,y) = \frac{q^{2n}}{q} < \frac{q^{2n}+q^n(q-1)}{q}$, probando así la afirmación. □

Si la función $H : \mathcal{K} \longrightarrow \mathcal{E},\ H(k) = E_k$ es inyectiva, entonces las reglas de codificación son igualmente probables a ser elegidas. Veamos que este es el caso en el esquema propuesto:

TEOREMA 2.2. *([**10**]) La función $H : \mathcal{K} \longrightarrow \mathcal{E},\ H(k) = E_k$, es biyectiva.*

DEMOSTRACIÓN. Si $E_k = E_{k'}$, $k = (x,y)$, $k' = (x',y')$, entonces

$$T_{S/R}(0f(x) + 0x) + y = T_{S/R}(0f(x') + 0x') + y'$$

implica $y = y'$ y así,

$$T_{S/R}(a(f(x) - f(x')) + b(x - x')) = 0, \text{ para toda } (a,b) \in \mathcal{S}.$$

Considerando $a = 0$,

$$T_{S/R}(b(x - x')) = 0 \text{ para toda } b \in S,$$

implica $x = x'$, por lo qué $k = k'$. El resto de la afirmación se sigue de modo directo. □

Ahora ya es posible determinar las cotas P_I y P_S del esquema de autenticación propuesto.

TEOREMA 2.3. *([**10**]) Con la notación anterior, los parámetros P_I y P_S del esquema de autenticación propuesto son tales que*

$$P_I = \frac{1}{q^2} \ \ y \ \ P_S \leq \frac{1}{q} + \frac{q-1}{q^{n+1}}.$$

Más aún,

$$|\mathcal{S}| = q^{3n}, |\mathcal{T}| = q^2, |\mathcal{K}| = |\mathcal{E}| = q^{2(n+1)}.$$

DEMOSTRACIÓN. Determinemos primero el valor de P_I. Sea $s = (a, b) \in \mathcal{S}$ y $z \in \mathcal{T} = R$. Dado $x \in S$ existe un único elemento $y \in R$ tal que $T_{S/R}(af(x) + bx) + y = z$, es decir, $E_{(x,y)}(s) = z$, de aquí se sigue que $|\{k \in \mathcal{K} : E_k(s) = z\}| = |S| = q^{2n}$. Como $|\mathcal{K}| = q^{2n}q^2$, entonces $P_I = \frac{q^{2n}}{q^{2n}q^2} = \frac{1}{q^2}$. En este caso P_I tiene el mínimo valor posible, o sea, $\frac{1}{|\mathcal{T}|}$.
Ahora determinemos una cota superior para P_S. Si $s = (a, b)$, $s' = (a', b')$ son elementos de $\mathcal{S}$ y $k = (k_1, k_2) \in \mathcal{K}$, sea T el numerador de la relación,

$$P_S = \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|}.$$

Entonces

$$\begin{aligned} T &= |\{k \in \mathcal{K} : E_k(s) = y, E_k(s') = y'\}| \\ &= \left| \left\{ k \in \mathcal{K} : \begin{array}{c} T_{S/R}(af(k_1) + bk_1) + k_2 = y \\ T_{S/R}(a'f(k_1) + b'k_1) + k_2 = y' \end{array} \right\} \right| \\ &= \left| \left\{ k \in \mathcal{K} : \begin{array}{c} T_{S/R}(af(k_1) + bk_1) + k_2 = y \\ T_{S/R}\left((a-a')f(k_1) + (b-b')k_1\right) = y - y' \end{array} \right\} \right| \\ &= \left| \left\{ k_1 \in S : T_{S/R}\left((a-a')f(k_1) + (b-b')k_1\right) = y - y' \right\} \right|. \end{aligned}$$

Como $N(a - a', b - b', y - y') = T$ y $|\{k \in \mathcal{K} : E_k(s) = y\}| = q^{2n}$, por el Teorema 2.1 se sigue que,

$$P_S \leq \frac{q^{2n-1} + q^{n-1}(q-1)}{q^{2n}} = \frac{1}{q} + \frac{q-1}{q^{n+1}},$$

probando así la afirmación. □

Un caso especial del resultado anterior es el siguiente:
CASO 1. Si $t = 1$ y $q = p^m$, entonces $S = \mathbb{F}_{q^n}$ y $R = \mathbb{F}_q$. En este caso por el Teorema 2.3,

$$P_I = \frac{1}{q} \ \text{ y } \ P_S \leq \frac{1}{q} + \frac{q-1}{q^{\frac{n+2}{2}}},$$

las cuales son las cotas del esquema de autenticación de la Definición 1.1 del Capítulo 6.

De este modo el resultado anterior es una generalización para el correspondiente resultado para campos finitos:

$$\begin{array}{ccc} GR(p^2, mn) & \longrightarrow & \mathbb{F}_{q^n} \\ | & & | \\ GR(p^2, m) & \longrightarrow & \mathbb{F}_q \end{array}.$$

Con el fin de proporcionar otro Caso del Teorema 2.3 se da lo siguiente:

PROPOSICIÓN 2.4. *([**10**]) Sea $R = GR(p^2, m)$ un anillo de Galois de característica p^2 y sea $f : R \longrightarrow R$ una función bent. Entonces (af) es también una función bent para cualquier unidad a de $\mathbb{Z}_{p^2}$.*

DEMOSTRACIÓN. Si $b \in R$, sea

$$I = \sum_{x \in R} e^{2\pi i T_{R/\mathbb{Z}_{p^t}}(f(x)-bx)/p^2}.$$

Sean $\omega = e^{2\pi i/p^2}$, $G = Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ el grupo de Galois de $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$, a una unidad de $\mathbb{Z}_{p^2}$ y $\sigma, \tau \in G$ tal que $\sigma(\omega) = \omega^a$ y $\tau(z) = \overline{z}$, respectivamente, donde $\overline{z}$ es el conjugado de z.

Como f es una función bent, $|I| = p^m$, lo cual es equivalente a, $I \cdot \tau(I) = p^m$. Entonces,

$$[I \cdot \tau(I)]^2 = (I \cdot \tau(I))(I \cdot \tau(I)) = p^{2m}.$$

Aplicando la función σ en ambos lados de expresión anterior y observando que σ y τ conmutan,

$$\sigma[(I \cdot \tau(I))(I \cdot \tau(I))] = [\sigma(I)\tau(\sigma(I))][\sigma(I)\tau(\sigma(I))] = |\sigma(I)||\sigma(I)| = p^{2m},$$

es decir,

$$|\sigma(I)| = p^m.$$

Si $h = T_{R/\mathbb{Z}_{p^2}}(f(x) - bx)$, cálculos directos muestran que

$$\sigma(I) = \sum_{x \in R} \sigma(e^{2\pi i h/p^2}) = \sum_{x \in R} e^{2\pi i a h/p^2} = \sum_{x \in R} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(af(x)-abx)/p^2},$$

de lo cual se sigue que (af) es una función bent. □

CASO 2. Sea $R = GR(p^2, m)$ y $f : R \longrightarrow R$ una función bent. Por la Proposición previa (af) es también una función bent cuando a es una unidad de $\mathbb{Z}_{p^2}$. En este caso el

Teorema 2.1 es válido al remplazar q por p, y si

$$\begin{aligned}
&\mathcal{S} := \mathcal{T}_{\mathbb{Z}_{p^2}} \times R,\\
&\mathcal{T} := \mathbb{Z}_{p^2},\\
&\mathcal{K} := R \times \mathbb{Z}_{p^2},\\
&\mathcal{E} := \{E_k(s) = T_{R/\mathbb{Z}_{p^2}}(af(x) + bx) + y,\ k = (x, y) \in \mathcal{K}, s = (a, b) \in \mathcal{S}\},
\end{aligned}$$

entonces,

$$P_I = \frac{1}{p^2} \text{ y } P_S \leq \frac{1}{p} + \frac{p-1}{p^{n+1}}.$$

CASO 3. Esta es una situación particular del CASO 2 donde $f : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ es una función bent, por lo que (af) es también una función bent para cualquier unidad a de $\mathbb{Z}_{p^2}$. En este caso el resultado del Teorema 2.1 también es válido remplazando q por p y notando que $n = 1$. Entonces,

$$\begin{aligned}
&\mathcal{S} := \mathcal{T}_{\mathbb{Z}_{p^2}} \times \mathbb{Z}_{p^2},\\
&\mathcal{T} := \mathbb{Z}_{p^2},\\
&\mathcal{K} := \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2},\\
&\mathcal{E} := \{E_k(s) = af(x) + bx + y,\ k = (x, y) \in \mathcal{K}, s = (a, b) \in \mathcal{S}\}
\end{aligned}$$

y

$$P_I = \frac{1}{p^2} \text{ y } P_S \leq \frac{1}{p} + \frac{p-1}{p^2}.$$

Las cotas obtenidas en el esquema de la siguiente Sección, son mejores.

3. Esquemas de autenticación utilizando la función de Gray

La función de Gray relaciona un anillo de Galois con su campo residual, es decir, los elementos de los anillos de Galois $GR(p^s, m)$ con los campos finitos $\mathbb{F}_q$, $q = p^m$, p primo.

Se modifica ligeramente la notación de la expansión p-ádica de los elementos de un anillo de Galois para definir de un modo claro la función de Gray sobre R^n, donde $R = GR(p^s, m)$.

Sea n un entero positivo y $A = (a_0, a_1, ..., a_{n-1})$ un elemento de R^n. Si $a_i = \rho_0(a_i) + p\rho_1(a_i) + \cdots + p^{s-1}\rho_{s-1}(a_i)$, donde $\rho_j(a_i) \in \mathcal{T}_R$ es la expansión p-ádica de a_i con $i = 0, 1, ..., n-1$ y $\rho_j(A) = (\rho_j(a_0), ..., \rho_j(a_{n-1}))$, $j = 0, 1, ..., s-1$ (recuérdese que $\mathcal{T}_R$ es el conjunto de Teichmüller de R), entonces es posible escribir $A = \rho_0(A) + p\rho_1(A) + \cdots + p^{s-1}\rho_{s-1}(A)$. Sea

$$r_j(A) = (r_j(a_0), ..., r_j(a_{n-1})),\ j = 0, 1, ..., s-1,$$

donde $r_j(a_i) = \overline{\rho_j(a_i)} \in \mathbb{F}_q$ es la reducción módulo p de los elementos de $\rho_j(a_i)$. Entonces la función de Gray en R^n está definida como ([**25**]):

$$\Phi : R^n \longrightarrow \mathbb{F}_q^{nq^{s-1}}, \Phi(A) = c_0 \otimes r_0(A) + c_1 \otimes r_1(A) + \cdots + c_s \otimes r_s(A).$$

Los resultados que en esta Sección se dan, aparecen en [**30**].

Las siguientes propiedades de la función de Gray serán utilizadas posteriormente.

LEMA 3.1. *Sea Φ la función de Gray sobre R. Entonces,*

$$\Phi(a+b) = \Phi(a) + \Phi(b),$$

para toda $a \in R$ y $b \in p^{s-1}R$.

DEMOSTRACIÓN. Sea $a = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}$ y $b = b_{s-1}p^{s-1}$, donde

$$a_0, a_1, \ldots, a_{s-1}, b_{s-1} \in \mathcal{T}_R$$

y $a_0 \neq 0$. Si $[x]_k = (x, x, ..., x)$, k-veces, entonces de la definición de la función de Gray,

$$\Phi(a) = \overline{a}_0 c_0 + \overline{a}_1 c_1 + \cdots + \overline{a}_{s-1}c_{s-1} + \left[\overline{a}_{s-1}\right]_{q^{s-1}},$$

y

$$\Phi(b) = \overline{b}_{s-1}c_{s-1} = \left[\overline{b}_{s-1}\right]_{q^{s-1}},$$

por lo que,

$$\Phi(a) + \Phi(b) = \overline{a}_0 c_0 + \overline{a}_1 c_1 + \cdots + \overline{a}_{s-2}c_{s-2} + \left[\overline{a}_{s-1} + \overline{b}_{s-1}\right]_{q^{s-1}}.$$

Por otro lado,

$$\begin{aligned} a + b &= a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + (a_{s-1} + b_{s-1})p^{s-1} \\ &= a_0 + a_1 p + \cdots + a_{s-2}p^{s-2} + r_{s-1}p^{s-1}, r_{s-1} \in \mathcal{T}_R, \end{aligned}$$

donde $\overline{r}_{s-1} = \overline{a}_{s-1} + \overline{b}_{s-1}$. Se concluye la prueba comparando $\Phi(a) + \Phi(b)$ y $\Phi(a+b)$. □

3.1. Esquema 2.

En particular, trabajando sobre anillos de Galois de característica p^2, considérese $R = GR(p^2, m)$ y $S = GR(p^2, mn)$ en el resto de esta Sección. Utilizando la notación del Capítulo 6 y considerando funciones bent $f : S \longrightarrow S$, donde $S = GR(p^2, mn)$, tal que uf es bent para cualquier $u \in U_S$, donde U_S es el grupo de unidades del anillo de Galois S. Sea Φ la función de Gray en $R = GR(p^2, m)$, se propone el siguiente esquema de autenticación, $\mathcal{A} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E})$:

$$\begin{aligned} \mathcal{S} &:= \{(a, b, c) \in \mathcal{T}_S \times S \times \mathcal{T}_R \mid (a, b) \neq (0, 0)\}, \\ \mathcal{T} &:= \mathbb{F}_q, \\ \mathcal{K} &:= \mathbb{Z}_{q^{2(n+1)}}, \\ \mathcal{E} &:= \{E_k(s) = pr_k(u_s),\ k \in \mathcal{K}, s \in \mathcal{S}\}. \end{aligned}$$

donde $s = (a, b, c) \in \mathcal{S}$, $\beta \in pR = \{\beta_1, \beta_2, \ldots, \beta_q\}$,

$$\begin{aligned} v_{s,\beta}(x) &= \beta + T_{S/R}(af(x) + bx) + c, \\ u_{s,\beta} &= \left(\Phi(v_{s,\beta}(x))\right)_{x \in S}, \\ u_s &= \left(u_{s,\beta}\right)_{\beta \in pR}, \end{aligned}$$

y pr_k es la función proyección de $\mathbb{F}_q^{q^{2(n+1)}}$ sobre $\mathbb{F}_q$, enviando u_s a su k-ésima coordenada.

Sea el conjunto V definido como:

$$V = \{c \in S : T_{S/R}(c) \in \mathcal{T}_R\}.$$

Con la notación anterior se propone otro esquema, $\mathcal{A}' = (\mathcal{S}', \mathcal{T}', \mathcal{K}', \mathcal{E}')$:

$$\begin{aligned}
\mathcal{S}' &:= \{(a, b, c) \in \mathcal{T}_S \times S \times V \mid (a, b) \neq (0, 0)\},\\
\mathcal{T}' &:= \mathbb{F}_q,\\
\mathcal{K}' &:= \mathbb{Z}_{q^{2(n+1)}},\\
\mathcal{E}' &:= \{E_k(s) = pr_k(u_s),\ k \in \mathcal{K}', s \in \mathcal{S}'\},
\end{aligned}$$

Nótese que este esquema tiene una ligera modificación respecto al esquema $\mathcal{A}$: en la definición de $\mathcal{A}$, en el espacio fuente $\mathcal{S}$ el conjunto $\mathcal{T}_R$ es considerado, mientras que en la definición del espacio fuente $\mathcal{S}'$ para $\mathcal{A}'$ el conjunto V es utilizado.

En el resto de este Capítulo una cota superior para los parámetros P_I y P_S serán determinados para el esquema propuesto $\mathcal{A}$.

TEOREMA 3.2. *Sea d_H la distancia de Hamming en $\mathbb{F}_q^{q^{2(n+1)}}$. Utilizando la notación anterior, para cualquier $s_1 = (a_1, b_1, c_1), s_2 = (a_2, b_2, c_2) \in \mathcal{S}, s_1 \neq s_2$, y cualesquiera elementos $\beta_1, \beta_2 \in pR$, se tiene que,*

$$(q-1)(q^{2n} - q^n) \leq d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right) \leq (q-1)(q^{2n} + q^n).$$

DEMOSTRACIÓN. Sean $a = a_1 - a_2, b = b_1 - b_2, c = c_1 - c_2$ y $\beta = \beta_1 - \beta_2$, y recuérdese que $v_{s,\beta} = (\beta + T_{S/R}(af(x) + bx) + c)$. De la definición de peso homogéneo (Definición 1.4), para el esquema $\mathcal{A} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E})$ se tiene que,

$$\begin{aligned}
& d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right) = \sum_{x \in S} d_H\left(\Phi(v_{s_1,\beta_1})(x), \Phi(v_{s_2,\beta_2}(x))\right)\\
= \ & \sum_{x \in S} w_h\left((v_{s_1,\beta_1}(x)) - (v_{s_2,\beta_2}(x))\right) = \sum_{x \in S} w_h\left(v_{s,\beta}(x)\right)\\
= \ & \sum_{x \in S}\left(-\frac{1}{q}\sigma\left(v_{s,\beta}(x)\right) + q - 1\right)\\
= \ & q^{tn}(q-1) - \frac{1}{q}\sum_{x \in S}\sum_{r \in R \setminus pR} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}((v_{s,\beta}(x))r)/p^2} = q^{2n}(q-1)\\
- \ & \frac{1}{q}\sum_{r \in R \setminus pR} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(\beta r)/p^2} e^{2\pi i T_{R/\mathbb{Z}_{p^2}}(cr)/p^2} \sum_{x \in S} e^{2\pi i T_{S/\mathbb{Z}_{p^2}}(raf(x) + rbx)/p^2}.
\end{aligned}$$

Si $(a, b) \neq (0, 0)$, ya que la función f en S es bent, de la relación anterior se obtiene:

$$\left|d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right) - q^{2n}(q-1)\right| \leq \frac{1}{q}q^n(q^2 - q),$$

y la afirmación se sigue.

Si $(a, b) = (0, 0)$, entonces,

$$d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right) = \sum_{x\in S} w_h\left(v_{s,\beta}\right) = \sum_{x\in S} w_h\left(\beta + c)\right) = q^{2n}(q-1).$$

La última desigualdad se sigue pues $\beta + c \in R\backslash pR$ y de la definición de peso homogéneo en R. En este caso se puede ver que $c \neq 0$, ya que como $s_1 \neq s_2$, $a_1 = a_2$ y $b_1 = b_2$, entonces $c_1 \neq c_2$, y de aquí $\beta + c \in R\backslash pR$ pues $c_1 - c_2 \in R \setminus p$. Por las discusiones anteriores el resultado se sigue.

El mismo resultado es válido para el esquema $\mathcal{A}'$. Si $s = (a, b, c) \in \mathcal{S}'$, sea $v_{s,\beta}(x) = (T_{S/R}(af(x) + bx + c) + \beta)$. De la definición de peso homogéneo se tiene que,

$$d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right) = \sum_{x\in S} w_h\left(v_{s_1,\beta_1}(x) - v_{s_2,\beta_2}(x)\right) = \sum_{x\in S} w_h\left(v_{s,\beta}(x)\right).$$

Como la función f es bent el resto de la prueba es similar al caso anterior. □

Recuérdese que en un esquema de autenticación, si la función $H : \mathcal{K} \to \mathcal{E}$ dada por $H(k) = E_k$ es inyectiva, entonces las reglas de codificación son igualmente probables, veamos que este es el caso en el esquema propuesto.

TEOREMA 3.3. *Sea la función $H : \mathcal{K} \longrightarrow \mathcal{E}$ con la notación anterior, dada por $H(k) = E_k$. H es biyectiva.*

DEMOSTRACIÓN. La prueba del Teorema será dada considerando varios casos. Sean $s = (a, b, c) \in \mathcal{S}$ y $\beta \in pR$, y considérese como antes, $v_{s,\beta}(x) = (\beta + T_{S/R}(af(x) + bx) + c)$, $u_{s,\beta} = (\Phi(v_{s,\beta}(x)))_{x\in S}$ y $u_s = (u_{s,\beta})_{\beta\in pR}$.

Obsérvese que es posible probar que la función H es biyectiva si se consideran dos distintas coordenadas de u_s, sean estas k_1 y k_2 y considérense dos funciones E_{k_1} y E_{k_2}, es decir, dos distintas proyecciones con imágenes en las coordenadas k_1 y k_2 respectivamente.

Si se tiene al menos un elemento $s \in S$ tal que $pr_{k_1}(u_s) \neq pr_k(u_{s_2})$, entonces se tienen dos funciones proyección distintas, y de aquí H es una función biyectiva.

Se compararán todas las coordenadas de u_s considerando la longitud de u_s por partes, para esto dividimos en tres casos:

Caso 1: Considérese dos coordenadas de $\Phi(v_{s,\beta}(x))$.

Case 2: Considérese una coordenada de $\Phi(v_{s,\beta}(x))$ y una de $\Phi(v_{s,\beta}(y))$, con $x \neq y$.

Case 3: Considérese $\beta_i \neq \beta_j$, una coordenada de $\Phi(v_{s,\beta_i}(x))$ y una de $\Phi(v_{s,\beta_j}(y))$. Este caso es subdividido cuando $x = y$ y cuando $x \neq y$.

Caso 1: Si $(a, b) \in \{\mathcal{T}_S \times S |\ a = 0, b \in pS \setminus \{0\}\}$, entonces $\beta + T_{S/R}(bx) \in pR$, y $\Phi(\beta + T_{S/R}(bx))$ tienen los mismos elementos en todas las coordenadas. Más aún, del Lema 3.1 se sigue que $\Phi(\beta + T_{S/R}(bx)) = \Phi(\beta + T_{S/R}(bx)) + \Phi(c)$ para toda $c \in \mathcal{T}_R$.

Considérese ahora dos distintas coordenadas j y k. Eligiendo un elemento c de $\mathcal{T}_R$ distinto de cero, se tiene que los elementos de la k-ésima y j-ésima coordenadas de $\Phi(c)$ son

diferentes. Considerando $s = (a, b, c)$ se pueden obtener distintos elementos en cualquier par de coordenadas de $\Phi(v_{s,\beta}(x))$.

Caso 2: En este caso elegimos una coordenada de $\Phi(v_{s,\beta}(x))$ y una de $\Phi(v_{s,\beta}(y))$, $x \neq y$.

Sea $b \in S\backslash\{0\}$ tal que $T_{S/R}(b(x-y)) \in pR\backslash\{0\}$. Si $T_{S/R}(bx) = a_0 + a_1 p$ y $T_{S/R}(by) = b_0 + b_1 p$, esto implica, $(a_0 - b_0) + (a_1 - b_1)p \in pR\backslash\{0\}$, luego $a_0 - b_0 = 0$, por lo que $(a_1 - b_1)p \in pR\backslash\{0\}$, de aquí $a_1 - b_1 \neq 0$, por lo que $a_1 \neq b_1$. Si se elige $\beta \in pR$, $a = 0$ y $c \in \mathcal{T}_R$, sea $s = (a, b, c)$ y $\Phi_w(\cdot)$ la w-ésima proyección, enviando $\Phi(\cdot)$ a su w-ésima coordenada. Si se considera la misma coordenada w en $\Phi(v_{s,\beta}(x))$ y en $\Phi(v_{s,\beta}(y))$, entonces los elementos en esas coordenadas son distintos:

$$\begin{aligned} & \Phi_w(v_{s,\beta}(x)) = \Phi_w(\beta + T_{S/R}(bx) + c) \\ = \ & \Phi_w(\beta + c + a_0) + \Phi_w(a_1 p) \\ \neq \ & \Phi_w(\beta + c + a_0) + \Phi_w(b_1 p) = \Phi_w(\beta + T_{S/R}(by) + c) \\ = \ & \Phi_w(v_{s,\beta}(y)) \end{aligned}$$

Esta desigualdad se tiene ya que $\Phi_w(a_1 p) \neq \Phi_w(b_1 p)$.

Considérense ahora elementos arbitrarios a y b de $\mathcal{T}_S$ y S respectivamente tal que $(a, b) \neq (0, 0)$. Si se toman distintas coordenadas r, w de $\Phi(\beta + T_{S/R}(af(x) + bx))$ y $\Phi(\beta + T_{S/R}(af(y) + by))$ respectivamente, y suponiendo que

$$\Phi_r(\beta + T_{S/R}(af(x) + bx)) \neq \Phi_w(\beta + T_{S/R}(af(y) + by)),$$

se elige $s = (a, b, c)$, donde $c = 0$, y se tiene que $\Phi_r(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$.

Si se supone que

$$\Phi_r(\beta + T_{S/R}(af(x) + bx)) = \Phi_w(\beta + T_{S/R}(af(y) + by)),$$

entonces se elige c y $s = (a, b, c) \in S$ tal que $\Phi_r(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$. La desigualdad anterior es posible si se considera a c como en el Caso 1.

Caso 3: Sea $\beta_i \neq \beta_j$, $\beta_i, \beta_j \in pR$, $(a, b, c) \in \mathcal{S}$. En este caso, si $x = y$, $x, y \in S$, entonces,

$\Phi_w(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$ ya que de lo contrario se tendría $\beta_i = \beta_j$.

Considérense ahora a, b, elementos arbitrarios de $\mathcal{T}_S$ y S respectivamente tal que $(a, b) \neq (0, 0)$, $x = y$. Si se eligen coordenadas distintas r, w en $\Phi(\beta_i + T_{S/R}(af(x) + bx))$ y $\Phi(\beta_j + T_{S/R}(af(y) + by))$ respectivamente y suponiendo que

$$\Phi_r(\beta_i + T_{S/R}(af(x) + bx)) \neq \Phi_w(\beta_j + T_{S/R}(af(y) + by)),$$

tomando $s = (a, b, c)$, donde $c = 0$, se obtiene $\Phi_r(v_{s,\beta_i}(x)) \neq \Phi_w(v_{s,\beta_j}(y))$.

Si suponemos que

$$\Phi_r(\beta_i + T_{S/R}(af(x) + bx)) = \Phi_w(\beta_j + T_{S/R}(af(y) + by)),$$

entonces elegimos c y $s = (a, b, c) \in S$ tal que $\Phi_r(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$. La desigualdad anterior es posible si se considera a $c \in \mathcal{T}_R$ distinto de cero.

Si $x \neq y$, entonces existe $b \in S\backslash\{0\}$ tal que $T_{S/R}(b(x-y)) = 0$, luego considerando $a = 0$,

$$\Phi_r(\beta_i + T_{S/R}(bx) + c) \neq \Phi_r(\beta_j + T_{S/R}(by) + c).$$

Considérense ahora a, b, elementos arbitrarios de $\mathcal{T}_S$ y S respectivamente tal que $(a,b) \neq (0,0)$, $x = y$. Si tomamos distintas coordenadas r, w en $\Phi(\beta_i + T_{S/R}(af(x)+bx))$ y $\Phi(\beta_j + T_{S/R}(af(y)+by))$, $x \neq y$, respectivamente y suponiendo que

$$\Phi_r(\beta_i + T_{S/R}(af(x)+bx)) \neq \Phi_w(\beta_j + T_{S/R}(af(y)+by)),$$

tomando $s = (a,b,c)$, donde $c = 0$, se obtiene $\Phi_r(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$.

Si suponemos que

$$\Phi_r(\beta_i + T_{S/R}(af(x)+bx)) = \Phi_w(\beta_j + T_{S/R}(af(y)+by)),$$

entonces elegimos c y $s = (a,b,c) \in S$ tal que $\Phi_r(v_{s,\beta}(x)) \neq \Phi_w(v_{s,\beta}(y))$. La desigualdad anterior es posible si se elige a $c \in \mathcal{T}_R$ distinto de cero.

Los casos discutidos anteriormente prueban la afirmación. □

Ahora se determina una cota superior para los parámetros P_I y P_S del esquema propuesto $\mathcal{A}$. El mismo resultado es obtenido para el esquema $\mathcal{A}'$.

TEOREMA 3.4. *Sea $\mathcal{A}$ el esquema de autenticación definido anteriormente. Entonces,*

$$P_I = \frac{1}{q} \;\; y \;\; P_S \leq \frac{1}{q} + \frac{q-1}{q^{n+1}}.$$

DEMOSTRACIÓN. Sea $x \in S$, $s = (a,b,c) \in \mathcal{S}$, β_i, $\beta_j \in pR$. Si $\beta_i \neq \beta_j$, del Teorema 3.3 se sigue que la k-ésima coordenada de

$$\Phi(\beta_i + T_{S/R}(af(x)+bx)+c) \text{ y } \Phi(\beta_j + T_{S/R}(af(x)+bx)+c)$$

son distintas y de aquí $|\{k \in \mathcal{K} : pr_k(u_s) = t\}| = q^{2n+1}$. Como $|\mathcal{K}| = q^{2(n+1)}$, de la definición de P_I se sigue que, $P_I = \frac{1}{q}$.

Ahora se determina una cota superior para P_S. Sea M el numerador de la relación,

$$P_S = \max_{\substack{s \in \mathcal{S} \\ t \in \mathcal{T}}} \max_{\substack{s' \in \mathcal{S}, s' \neq s \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathcal{K} : E_k(s) = t\}|},$$

donde $s_1 = (a_1, b_1, c_1)$, $s_2 = (a_2, b_2, c_2) \in \mathcal{S}$, $s_1 \neq s_2$. Entonces,

$$
\begin{aligned}
M &= |\{k \in \mathcal{K} : pr_k(u_{s_1}) = t_1, pr_k(u_{s_2}) = t_2\}| \\
&= \left| \left\{ k \in \mathcal{K} : \begin{array}{c} pr_k(u_{s_1}) = t_1 \\ pr_k(u_{s_1}) - pr_k(u_{s_2}) = t_1 - t_2 \end{array} \right\} \right| \\
&= |\{k \in \mathcal{K} : pr_k[(\Phi(\beta_i + T_{S/R}(a_1 f(x_j) + b_1 x_j) + c_1))_{j=1}^{q^{2n}}]_{i=1}^{q} = t_1, \\
&\quad pr_k[(\Phi(T_{S/R}(a_1 f(x_j) + b_1 x_j) + c_1) - \Phi(T_{S/R}(a_2 f(x_j) + b_2 x_j) + c_2))_{j=1}^{q^{2n}}]_q \\
&\quad = t_1 - t_2\}| \\
&= |\{k \in \mathcal{K} : pr_k[(\Phi(T_{S/R}(a_1 f(x_j) + b_1 x_j) + c_1) - \Phi(T_{S/R}(a_2 f(x_j) + b_2 x_j) + c_2))_{j=1}^{q^{2n}}] \\
&\quad = t_1 - t_2\}| \\
&= |\{k \in \mathcal{K} : pr_k[\Phi(T_{S/R}(a_1 f(x_1) + b_1 x_1) + c_1) - \hat{t}_1 - \Phi(T_{S/R}(a_2 f(x_1) + b_2 x_1) + c_2) \\
&\quad + \hat{t}_2, \ldots, \Phi(T_{S/R}(a_1 f(x_{q^{2n}}) + b_1 x_{q^{2n}}) + c_1) - \hat{t}_1 \\
&\quad - \Phi(T_{S/R}(a_2 f(x_{q^{2n}}) + b_2 x_{q^{2n}}) + c_2) + \hat{t}_2] = 0\}| \\
&= |\{k \in \mathcal{K} : pr_k[\Phi(T_{S/R}(a_1 f(x_1) + b_1 x_1) + c_1 + \beta_1) \\
&\quad - \Phi(T_{S/R}(a_2 f(x_1) + b_2 x_1) + c_2 + \beta_2), \ldots, \Phi(T_{S/R}(a_1 f(x_{q^{2n}}) + b_1 x_{q^{2n}}) + c_1 + \beta_1) \\
&\quad - \Phi(T_{S/R}(a_2 f(x_{q^{2n}}) + b_2 x_{q^{2n}}) + c_2 + \beta_2)] = 0\}| = q^{n+1} - d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right),
\end{aligned}
$$

donde

$$
\begin{aligned}
-\Phi(\beta_1) = \hat{t}_1 = (t_1, \ldots, t_1), q-\text{veces}, \\
-\Phi(\beta_2) = \hat{t}_2 = (t_2, \ldots, t_2), q-\text{veces}.
\end{aligned}
$$

En la relación anterior la tercera igualdad se sigue de la siguiente observación: sea $x \in S$ y $t \in \mathbb{F}_q$, entonces existe un único elemento $\beta_j \in pR$ tal que $pr_k[\Phi(\beta_i + T_{S/R}(a_1 f(x) + b_1 x) + c_1))] = t$. Por lo tanto

$$
\begin{aligned}
&|\{k \in \mathcal{K} : pr_k[(\Phi(\beta_i + T_{S/R}(a_1 f(x) + b_1 x) + c_1))]_{i=1}^{q} = t_1, \\
&pr_k[(\Phi(T_{S/R}(a_1 f(x) + b_1 x) + c_1) - \Phi(T_{S/R}(a_2 f(x) + b_2 x) + c_2))]_q = t_1 - t_2\}| \\
= \; &|\{k \in \mathcal{K} : pr_k[(\Phi(T_{S/R}(a_1 f(x_j) + b_1 x_j) + c_1) - \Phi(T_{S/R}(a_2 f(x_j) + b_2 x_j) + c_2))_{j=1}^{q^{2n}}] \\
&= t_1 - t_2\}|.
\end{aligned}
$$

Ahora del Teorema 3.2 se sigue que,

$$
\begin{aligned}
P_S &= \frac{q^{2n+1} - d_H\left(u_{s_1,\beta_1}, u_{s_2,\beta_2}\right)}{q^{2n+1}} \leq \frac{q^{2n+1} - (q-1)(q^{2n} - q^n)}{q^{2n+1}} \\
&= \frac{q^{n+1} + q^{2n} - q^n}{q^{2n+1}} = \frac{1}{q} + \frac{q^n(q-1)}{q^{2n+1}} = \frac{1}{q} + \frac{q-1}{q^{n+1}},
\end{aligned}
$$

y de aquí se tiene el resultado. □

Las cotas obtenidas en este esquema son mejores que todas las obtenidas en los esquemas de los trabajos [**21**] y [**9**] en el cual se consideran campos finitos y funciones bent y casi-bent sobre estos campos, del mismo modo se obtienen mejores cotas que las obtenidas en[**42**] en el cual trabajan con polinomios no-degenerados y funciones racionales sobre anillos de Galois y la función de Gray. Estas comparaciones serán dadas en la siguiente Sección.

Como casos particulares del resultado anterior se tienen los siguientes:

CASO 1: Sea $R = GR(p^2, m)$ y $f : R \to R$ una función bent. Se sabe que la función uf es también una función bent para cualquier unidad u del anillo $\mathbb{Z}_{p^2}$. El resultado del Teorema 3.2 también se obtiene al remplazar q por p, en este caso:

$$\begin{aligned}
&\mathcal{S} := \{(a, b, c) \in \mathcal{T}_R \times R \times \mathcal{T}_R \mid (a, b) \neq (0, 0)\},\\
&\mathcal{T} := \mathbb{F}_p,\\
&\mathcal{K} := \mathbb{Z}_{p^{2(n+1)}},\\
&\mathcal{E} := \{E_k(s) = pr_k(u_s),\ k \in \mathcal{K}, s \in \mathcal{S}\},\\
&\qquad P_I = \frac{1}{p} \text{ y } P_S \leq \frac{1}{p} + \frac{p-1}{p^{m+1}}.
\end{aligned}$$

CASO 2: Este es un caso particular de la situación anterior donde $m = 1$, es decir, $R = \mathbb{Z}_{p^2}$ y $f : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ es una función bent. En este caso uf también es bent para cualquier unidad u del anillo $\mathbb{Z}_{p^2}$. El resultado del Teorema 3.2 es garantizado, en esta situación se remplaza q por p y se obtiene,

$$\begin{aligned}
&\mathcal{S} := \{(a, b, c) \in \mathcal{T}_{\mathbb{Z}_{p^2}} \times \mathbb{Z}_{p^2} \times \mathcal{T}_{\mathbb{Z}_{p^2}} \mid (a, b) \neq (0, 0)\},\\
&\mathcal{T} := \mathbb{F}_p,\\
&\mathcal{K} := \mathbb{Z}_{p^4},\\
&\mathcal{E} := \{E_k(s) = pr_k(u_s),\ k \in \mathcal{K}, s \in \mathcal{S}\}.\\
&\qquad P_I = \frac{1}{p} \text{ y } P_S \leq \frac{1}{p} + \frac{p-1}{p^2}.
\end{aligned}$$

Obsevación. Es fácil ver que los resultados de este Capítulo son también válidos sobre anillos de Galois de característica p^s, $s > 2$ sobre el cual se tengan funciones bent, f, con la propiedad que uf también es bent para toda unidad u del anillo. Sin embargo no hemos detectado en la literatura tales funciones ni tampoco hemos encontrado alguna.

4. Comparación de cotas de P_I y P_S respecto a otros trabajos

Las cotas obtenidas en el Esquema 2, refiriéndonos con esto siempre al Esquema de autenticación 2 dado en este Capítulo, resultan ser mejores que las obtenidas en [**21**], [**9**] y [**42**] como se verá a continuación.

En la siguiente tabla se presentan las cotas superiores de P_I y P_S obtenidas en los distintos trabajos antes mencionados. Para mayor detalle de los esquemas presentados en la tabla consúltese las respectivas referencias que en éstas aparecen.

	Cota de P_I	Cota de P_S
Esquema 2, $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q}$	$\frac{1}{q} + \frac{q-1}{q^{n+1}}$
Teorema 2 de [**21**], $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q}$	$\frac{1}{q} + \frac{q-1}{q^{\frac{n+2}{2}}}$
Teorema 4 de [**21**], $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{n/2}}$	$\frac{1}{q} + \frac{q^2-1}{q(q^{m/2}-q+1)}$
Teorema 7 de [**21**], $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q}$	$\frac{1}{q} + \frac{1+2(q-1)(1+q^{m/2})}{q^{m+1}}$
Teorema 9 de [**21**], $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q} + \frac{(q-1)(1+2q^{m/2})}{q^{m+1}}$	$\frac{1}{q} + \frac{2(q^2+q-2)q^{m/2}+q^2}{q\left(q^m-2(q-1)q^{m/2}-1\right)}$
Ejemplo 1 de [**9**], $\mathcal{T} := \mathbb{F}_{2^h}$	$\frac{1}{2^h}$	$\frac{1}{2^h} + \frac{1-2^{-h}}{2^{\frac{n-1}{2}}}$
Ejemplo 2 de [**9**], $\mathcal{T} := \mathbb{F}_{2^h}$	$\frac{1}{2^h} + \left(1 - \frac{1}{2^h}\right) \frac{1}{2^{(n-1)/2}}$	$\frac{1}{2^h} + \frac{2^h-2^{-h}}{2^{(n-1)/2}-2^h+1}$
Proposición 3.2 de [**42**], $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q}$	$\frac{1}{q} + \frac{q-1}{q} \cdot \frac{D-1}{q^{n/2}}$
Proposición 3.5 de [**42**], $\mathcal{T} := \mathbb{F}_q$	$\frac{1}{q}$	$\frac{1}{q} + \frac{(q-1)}{q} \cdot \frac{(p(N+1)+N-1)q^{n/2}}{q^n-N}$
Proposición 4.5 de [**42**], $\mathcal{T} = \mathbb{F}_p$	$\frac{1}{p} + \frac{(p-1)}{p} \cdot \frac{(D-1)}{\sqrt{p^n}}$	$\frac{1}{p} + \frac{(p^2+p-2)(D-1)}{p(\sqrt{p^n}-(p-1)(D-1))}$

En [**21**] los esquemas de autenticación son contruidos utilizando funciones bent sobre campos finitos, en [**9**] los esquemas son construidos utilizando funciones casi-bent sobre campos finitos y en la referencia [**42**] se utilizan funciones racionales y polinomios no-degenerados sobre anillos de Galois y la función de Gray sobre estos anillos.

En la tabla anterior $n > m$, n, m, h, D y N enteros positivos. En el Esquema 2, $\mathbb{F}_q$ es un campo con $q = p^n$ elementos, p primo, en los Teoremas 2, 4, 7 y 9 de [**21**] se considera $\mathbb{F}_q$ un campo con $q = p^n$ elementos, p un número primo impar, en los Ejemplos 1 y 2 de [**9**], $\mathbb{F}_{2^h}$ es un campo con 2^h elementos, en las Proposiciones 3.2 y 3.5 de [**42**], $\mathbb{F}_q$ es un campo con $q = p^n$ elementos, p un número primo y en la Proposición 4.5, también de [**42**], $\mathbb{F}_p$ es un campo finito donde p es un número primo.

Las operaciones para comparar las cotas del Esquema 2 con los resultados de la tabla anterior son fáciles, veamos algunas de ellas.

Dado que $P_I = \frac{1}{q}$ en el Esquema 2 descrito en este trabajo, esta cota resulta mejor o igual que en los casos mencionados. Nos enfocamos entonces a comparar las cotas para P_S.

En el Esquema 2 de este trabajo la relación entre $\frac{1}{|\mathcal{T}|}$ y la cota obtenida para P_S está dada por

$$\frac{1}{q} \longleftrightarrow \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^n}.$$

En el caso de la cota para P_S en el Teorema 2 de [**21**] la relación mínima cota y cota obtenida está dada por:

$$\frac{1}{q} \longleftrightarrow \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^{n/2}}.$$

Dado que $\frac{1}{q^n} < \frac{1}{q^{n/2}}$ se tiene que la cota para P_S del Esquema 2 es mejor que la proporcionada en [**21**].

Ahora comparemos el Esquema 2 con el Ejemplo 1 de [**9**]. En este caso $\mathcal{T} := \mathbb{F}_{2^h}$, y $P_S \leq \frac{1}{2^h} + \frac{1-2^{-h}}{2^{\frac{n-1}{2}}}$. Sea $\tilde{q} = 2^h$, luego $\frac{1-2^{-h}}{2^{\frac{n-1}{2}}} = \frac{\tilde{q}-1}{\tilde{q}2^{\frac{n-1}{2}}} = \frac{\tilde{q}-1}{\tilde{q}} \cdot \frac{1}{2^{\frac{n-1}{2}}}$. Como $\frac{1}{2^{\frac{n-1}{2}}} > \frac{1}{\tilde{q}^n}$, entonces

$$\frac{1}{\tilde{q}} + \frac{\tilde{q}-1}{\tilde{q}} \cdot \frac{1}{2^{\frac{n-1}{2}}} > \frac{1}{\tilde{q}} + \frac{\tilde{q}-1}{\tilde{q}} \cdot \frac{1}{\tilde{q}^n},$$

de donde se puede observar que en el lado derecho de la desigualdad se tiene la forma de la cota del Esquema 2 de este trabajo, luego la cota de P_S es mejor en este caso. Recuérdese que la comparación es respecto al menor valor que puede alcanzar P_S el cual es $\frac{1}{\tilde{q}}$ en el Ejemplo 1 de [**9**] y $\frac{1}{q}$ en el Esquema 2.

Por último comparemos el Esquema 2 con la Proposición 3.2 de [**42**]. En el Esquema de la Proposición 3.2 de [**42**], $\mathcal{T} := \mathbb{F}_q$ y $P_S \leq \frac{1}{q} + \frac{q-1}{q} \cdot \frac{D-1}{q^{n/2}}$, D un entero positivo. Nótese que $\frac{1}{q^n} < \frac{D-1}{q^{n/2}}$, por lo que la cota para P_S del esquema 2 es mejor, ya que ésta es dada por $P_S \leq \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q^n}$.

Para los restantes esquemas haciendo un análisis similar se puede notar que las cotas de nuestro Esquema 2 son mejores.

5. Acerca de las funciones bent

En el Capítulo 3 se construyeron funciones bent sobre el anillo de Galois $GR(p^2, m)$ con la propiedad de que al ser multiplicadas por cualquier unidad del anillo se obtienen también funciones bent, funciones bent con esta propiedad no parece haber muchas, esto permitió construir los esquemas de autenticación dados en este Capítulo. En las siguientes líneas veremos que algunas funciones bent que aparecen en la literatura no tienen esta propiedad.

Consideremos el anillo de Galois R como un anillo de característica 4, es decir, $R = GR(4, m)$. Sea $\mathcal{T}_R$ el conjuto de Teichmüller de R y $f, g : \mathcal{T}_R \to \mathbb{Z}_4$ funciones bent. Sea $H : R \to \mathbb{Z}_4$ definida por $H(x + 2y) = f(x) + g(y)$, $x, y \in \mathcal{T}_R$. Veamos que H es una función bent:

Sean $w = x + 2y$ y $\lambda = \lambda_1 + 2\lambda_2$ elementos de R. Entonces

$$\left| \sum_{w \in R} e^{2\pi i T_{R/\mathbb{Z}_4}(H(w) - \lambda w)/4} \right| = \left| \sum_{x,y \in \mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(H(x+2y) - ((\lambda_1 + 2\lambda_2)(x+2y)))/2} \right|$$

$$= \left| \sum_{x,y \in \mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(f(x) - x(\lambda_1 - 2\lambda_2) + g(y) - 2y\lambda_1)/2} \right|$$

$$= \left| \sum_{x,y \in \mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(f(x) - x(\lambda_1 - 2\lambda_2))/2} e^{\pi i T_{R/\mathbb{Z}_4}(g(y) - 2y\lambda_1)/2} \right|$$

$$= \left|\sum_{x\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(f(x)-x(\lambda_1-2\lambda_2))/2}\right| \left|\sum_{y\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(g(y)-2y\lambda_1)/2}\right| = 2^{n/2}2^{n/2} = 2^n.$$

Por lo tanto H es una función bent sobre R.

En [**49**] se muestra que la función $f : \mathcal{T}_R \to \mathbb{Z}_4$ definida por $f(x) = \epsilon + T_{R/\mathbb{Z}_4}(cx)$ es una función bent para cualquier elemento $\epsilon \in \mathbb{Z}_4$ y c una unidad del anillo R cuando $m \geq 3$. Por lo tanto la función $H(x + 2y) := \epsilon_1 + T_{R/\mathbb{Z}_4}(c_1x) + \epsilon_2 + T_{R/\mathbb{Z}_4}(c_2y) = (\epsilon_1 + \epsilon_2) + T_{R/\mathbb{Z}_4}(c_1x + c_2y)$, $\epsilon_1, \epsilon_2 \in \mathbb{Z}_4$ y c_1, c_2 unidades de R, es un ejemplo de función bent.

En el caso particular $c = 1$ y $m = 3$, es decir, $R = GR(4, 3)$, determinado por el polinomio mónico básico primito $x^3 + 2x^2 + x + 3 \in \mathbb{Z}_4[x]$, sea ξ una raíz primitiva de este polinomio y $f(x) = T_{R/\mathbb{Z}_4}(x)$. Veamos que la función uf no es bent para cualquier unidad u del anillo de Galois R.

Si $\lambda = 0$,

$$\left|\sum_{x\in\mathcal{T}_R} e^{2\pi i T_{R/\mathbb{Z}_4}(\xi(f(x)-\lambda x))/4}\right| = \left|\sum_{x\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(\xi T_{R/\mathbb{Z}_4}(x))/2}\right| = \left|\sum_{x\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(\xi)T_{R/\mathbb{Z}_4}(x)/2}\right|.$$

Por otro lado $T_{R/\mathbb{Z}_4}(0) = 0, T_{R/\mathbb{Z}_4}(\xi) = 2, T_{R/\mathbb{Z}_4}(\xi^2) = 2, T_{R/\mathbb{Z}_4}(\xi^3) = 1, T_{R/\mathbb{Z}_4}(\xi^4) = 2$, $T_{R/\mathbb{Z}_4}(\xi^5) = 1$, $T_{R/\mathbb{Z}_4}(\xi^6) = 1$, $T_{R/\mathbb{Z}_4}(\xi^7) = 3$, por lo que la suma anterior es igual a cero, lo cual implica que la función ξf no es una función bent sobre $\mathcal{T}_R$.

El mismo resultado se obtiene si se considera nuevamente la función bent $H : R \to \mathbb{Z}_4$, $H(x + 2y) = f(x) + g(y)$ con $R = GR(4, 3)$ y $f = g = T_{R/\mathbb{Z}_4}$. En el caso particular $\lambda = 0$, para la suma $\sum_{w\in R} e^{2\pi i T_{R/\mathbb{Z}_4}(\xi H(w)-\lambda w)/4}$, $w = x + 2y$, se tiene que

$$\left|\sum_{w\in R} e^{2\pi i T_{R/\mathbb{Z}_4}(\xi H(w))/4}\right| = \left|\sum_{x\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(\xi)T_{R/\mathbb{Z}_4}(x)/2}\right| \left|\sum_{y\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(\xi)T_{R/\mathbb{Z}_4}(y)/2}\right|$$
$$= (0)(0) = 0,$$

por lo tanto la función uH no es bent para toda unidad de R.

A fin de proporcionar un ejemplo mas de funciones bent sobre anillos de Galois con la característica del ejemplo anterior se da la siguiente Proposición.

PROPOSICIÓN 5.1. [**49**] *Sea μ la reducción módulo 2 de $R = GR(4, n)$ a $\mathbb{F}_{2^n}$, $n \geq 3$. Entonces la función booleana definida para $x \in \mathcal{T}_R$ por $f(x) = \epsilon + T_{R/\mathbb{Z}_4}(sx + 2tx^3)$, $\epsilon \in \mathbb{Z}_4$, $s \in R$, $t \in \mathcal{T}_R\backslash\{0\}$, es bent si $\mu(s) = 0$ y la ecuación $\mu(t)z^3 + 1 = 0$ no tiene solución en $\mathbb{F}_{2^n}$, o si $\mu(s) \neq 0$ y la ecuación $z^3 + z + \frac{\mu(t)^2}{\mu(t)^6} = 0$ no tiene solución en $\mathbb{F}_{2^n}$.*

Considérese nuevamente R como el anillo de Galois $GR(4, 3)$ determinado por el polinomio mónico básico primitivo $x^3 + 2x^2 + x + 3 \in \mathbb{Z}_4[x]$ y ξ una raíz primitiva de este polinomio. Sea $\xi^3 \in \mathcal{T}_R$, luego $\frac{\mu(\xi^3)^2}{\mu(\xi^3)^6} = \overline{\xi}^2$ y la ecuación $z^3 + z + \overline{\xi}^2 = 0$ no tiene solución en $\mathbb{F}_{2^3}$, donde $\mu(\xi) = \overline{\xi}$. Entonces por la Proposición anterior las funciones

$f(x) = \epsilon + T_{R/\mathbb{Z}_4}(sx + 2\xi^3 x^3)$, $\epsilon \in \mathbb{Z}_4$, $\mu(s) \neq 0$, son bent, de éstas considérese en particular $g(x) = 1 + T_{R/\mathbb{Z}_4}(x + 2\xi^3 x^3)$. La función ug no siempre es bent para toda u unidad de $\mathcal{T}_R$, ya que si se considera $\xi g(x) = \xi + \xi T_{R/\mathbb{Z}_4}(x + 2\xi^3 x^3)$, ésta no es bent, pues $\left|\sum_{x\in\mathcal{T}_R} e^{2\pi i T_{R/\mathbb{Z}_4}(\xi(g(x)-\lambda x))/4}\right| = 2$ si $\lambda = 0$. Ahora de modo similar al primer ejemplo dado, si se considera nuevamente la función bent $H : R \to \mathbb{Z}_4$, $H(x+2y) = f(x)+g(y)$ y $f(x) = g(x) = 1 + T_{R/\mathbb{Z}_4}(x + 2\xi^3 x^3)$. En el caso particular $\lambda = 0$, para la suma $\sum_{w\in R} e^{2\pi i T_{R/\mathbb{Z}_4}(\xi H(w)-\lambda w)/4}$, $w = x + 2y$, se tiene que

$$\left|\sum_{w\in R} e^{2\pi i T_{R/\mathbb{Z}_4}(\xi H(w))/4}\right| = \left|\sum_{x\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(\xi)(1+T_{R/\mathbb{Z}_4}(x+2\xi^3 x^3))/2}\right|$$

$$\left|\sum_{y\in\mathcal{T}_R} e^{\pi i T_{R/\mathbb{Z}_4}(\xi)(1+T_{R/\mathbb{Z}_4}(y+2\xi^3 y^3))/2}\right| = (2)(2) = 4.$$

Por lo tanto la función ξH no es bent.

Con base en los ejemplos anteriores concluimos que la familia de funciones bent obtenida en el Teorema 3.3 es una clase especial de estas funciones.

Conclusiones

Las funciones perfectamente no-lineales y casi perfectamente no-lineales tienen propiedades criptográficas usadas en cifrados tipo DES y también son utilizadas para la construcción de esquemas de compartición de secretos y esquemas de autenticación sobre campos finitos como se ha presentado en este trabajo. Más aún al generalizar la definición de funciones bent sobre anillos de Galois de característica p^2, p primo, una clase especial de funciones bent son obtenidas sobre estos anillos (introducido en el Capítulo 3) que permite la construcción de esquemas de autenticación sobre estos anillos, y también sobre campos finitos al utilizar la función de Gray.

Las cotas respecto a la probabilidad de aceptar como auténticos, mensajes insertados en el canal de comunicación por algún intruso, obtenidas en el esquema de autenticación 2 del Capítulo 7, son mejores que las que se obtienen en los trabajos [**21**], [**9**] y [**30**], en donde se usan funciones bent y casi-bent sobre campos finitos, y polinomios no-degenerados y funciones racionales sobre anillos de Galois.

Resulta natural preguntarse acerca de la existencia de funciones bent sobre anillos de Galois de característica p^s, $s > 2$, y más aún con la propiedad de obtener siempre una función bent al ser multiplicada por una unidad del anillo correspondiente. Respecto a los esquemas de autenticación dados en el Capítulo 7, esto sería muy conveniente, ya que las operaciones que se han realizado pueden ser generalizadas y hemos observado que las cotas que se obtienen son mejores. Por lo que una pregunta abierta es la existencia de funciones bent sobre anillos de Galois de característica p^s, $s > 2$ con la propiedad antes mencionada.

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. "More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings", Advances in Cryptology-EUROCRYPT 97, Vol. 1233, 1997, pp. 422-433.

[5] Carlet, C. and Guillot, Ph. "A new representation of Boolean Functions", Springer-Verlag Berlin Heidelberg, 1999, Proceedings of AAEC-C 13, LNCS 1719, pp. 94-103.

[6] Carlet, C. and Guillot, Ph. "Bent, resilient functions and the Numerical Normal Form", DIMACS SDMTCS, 56, 2001, pp. 87-96

[7] 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.

[8] 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.

[9] Carlet, C.; Ding, C. and Niederreiter, H. "Authentication schemes from highly nonlinear functions", Designs, Codes and Cryptography, 2006, pp. 71-79.

[10] Carlet, C.; Ku-Cauich, J. C. and Tapia-Recillas, H. "Bent Functions on a Galois Ring and Systematic Authentication Codes", Advances in Mathematics of Communications, vol. 6, no 2, 2012, pp. 249-258.

[11] 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, .

[12] 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.

[13] 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 .

[14] Carter, J. L. and Wegman, M. N."Universal classes of hash functions", J. Comput. Syst. Sci., vol 18, 1979, pp. 143-154.

[15] 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.

[16] Coulter, R. S. and Matthews, R. W. "Bent Polynomials Over Finite Fields", Bull. Austral. Math. Soc. 56, 1997, pp. 429-437.

[17] Coulter, R. S. "Explicit evaluations of some Weil sums", Acta Arith. 83, 1998, pp. 241-251.

[18] Coulter, R. S. "Further evaluations of Weil sums", Acta Arith. 86, 1998, pp. 217-226.

[19] Coulter, R. S. "The Number of Rational Points of a Class of Artin-Schreier Curves", Finite Fields and Their Applications, vol. 8, 2002, pp. 397-413.

[20] Courtois, N. and Meier, W. "Algebraic attacks on stream ciphers with linear feedback", In Advances in Cryptology-EUROCRYPT 2003, Springer Verlag 2003, pp. 346-359.
[21] Ding, C. and Niederreiter, H. "Systematic Authentication Codes From Highly Nonlinear Functions", IEEE Transactions on Information Theory, vol. 50, no. 10, October 2004, pp. 2421-2428.
[22] 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.
[23] Fan, S. and Han, W. "Character sums over Galois rings and primitive polynomials over finite fields", Finite Fields and Their Applications, vol. 10, 2004, pp 36–52.
[24] Gilbert, E. N.; MacWilliams, F. J. and Sloane, N. J. "Codes which detect deception", The Bell System Technical Journal, 1974, pp. 405-424.
[25] Greferath, M. and Schmidt, S. E. "Gray isometries for finite chain rings and non-linear ternary $(36, 3^{12}, 15)$ code", IEEE Transactions on Information Theory, Vol. 45, 1999, pp. 2522-2524.
[26] Gutiérrez N. and Tapia-Recillas, H. "Systematic authentication codes based on affine transformations", C. Numerantium, Canada, 2005, pp. 123-128.
[27] 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.
[28] Ireland, K. and Rosen, M. *"A Classical Introduction to Modern Number Theory"*, Springer-Verlag New York, Inc, second edition, 1990.
[29] Jitman, S. and Udomkavanich, P. "The Gray Image of Codes over Finite Chain Rings", Int. J. Contemp. Math. Sciences, vol 5, no. 10, 2010, pp. 449-458.
[30] Ku-Cauich, J. C. and Tapia-Recillas, H. "A Class of Systematic Authentication Codes Based on Bent Functions and the Gray Map on a Galois Ring". En preparación.
[31] Ku-Cauich, J. C. and Tapia-Recillas, H. "Secret Sharing Schemes Based on Almost-Bent Functions", International Journal of Pure and Applied Mathematics , vol. 57, no. 1, 2009, pp. 87-102.
[32] Kumar, P. V.; Scholtz, R. A. and Welch, L. R. "Generalized bent functions and their properties", J. Comb. Theory, Vol. 40, 1985, pp. 90-107.
[33] Lang S. *"Algebraic Number Theory"*, Reading Mass; Addison-Wesley, 1968.
[34] Leander, N. "Monomial Bent Functions", IEEE Transactions on Information Theory, vol. 52, Feb. 2006, pp. 738-743.
[35] Lidl, R. and Niederreiter, H. *"Finite Fields"*, vol. 20 of Encyclopedia of Mathematics and Its Applications. Reading, Mass; Addison-Wesley (now distributed by Cambridge Univ. Press), vol 20, 1997.
[36] McEliece, R. J. and Sarwate, D. V. "On sharing secrets and reed-solomon codes", Commun. Association Computing Machinery, vol. 24, 1981, pp. 583-584.
[37] 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.
[38] Mc Donald, B. R. *"Finite Rings with Identity"*, Marcel Dekker Inc., New York, 1974
[39] 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.
[40] 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.
[41] 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.
[42] 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.
[43] Pless, V. "Power moments identities on weight distributions in error correcting codes", Info. and Control, vol. 6, 1963, pp. 147-152.

[44] Rothaus, O. S. “On bent functions”, J. Comb. Theory, 20A, 1976, pp. 300-305.
[45] Roman, Steven *“Coding and Information Theory”*, Graduate Texts in Mathematics, Springer-Verlag, 1992.
[46] Shamir, A. “How to share a secret”, Commun. ACM, vol. 22, Dec. 1979, pp. 612-613.
[47] Simmons, G. J. “Authentication theory/coding theory”, In advances in Cryptology-Crypto 84, 1984, pp. 411-431.
[48] Simmons, G. J. “A survey of information authentication”, in Contemporary Cryptology, The Science of Information Integrity, Ed. Piscataway, IEEE Press, 1992, pp. 379-419.
[49] Sole, P. and Tokareva, N. “Connections between Quaternary and Binary Bent Functions”, Cryptology ePrint Archives, 2009 (http://www.eprint.iacr.org/2009/544).
[50] Stinson, D. R. *“Cryptography Theory and Practice”*, CRC Press, LCC, 1995.
[51] 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.
[52] Tapia-Recillas, H. “A secret sharing scheme from a chain ring linear code”, C. Numerantium 186, 2007, pp. 33-39.
[53] Wan, Zhe-Xian *“Lectures on Finite Fields and Galois Rings”*, World Scientific Publishing Co. Pte. Ltd., 2003.
[54] 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.
[55] 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.