Universidad del Atlántico	**CÓDIGO:** FOR-DO-109
	VERSIÓN: 0
	FECHA: 03/06/2020

AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO

Puerto Colombia, **20 de Marzo de 2021**

Señores
DEPARTAMENTO DE BIBLIOTECAS
Universidad del Atlántico

Asunto: Autorización Trabajo de Grado

Cordial saludo,

Yo, **RAFAEL EDUARDO GONZALEZ PUGLIESE**, identificado(a) con **C.C. No. 1.043.023.028** de **SABANALARGA**, autor(a) del trabajo de grado titulado **FUNCIONES BENT Y ALGUNAS DE SUS APLICACIONES** presentado y aprobado en el año **2020** como requisito para optar al título Profesional de **MATEMÁTICO**; autorizo al Departamento de Bibliotecas de la Universidad del Atlántico para que, con fines académicos, la producción académica, literaria, intelectual de la Universidad del Atlántico sea divulgada a nivel nacional e internacional a través de la visibilidad de su contenido de la siguiente manera:

- Los usuarios del Departamento de Bibliotecas de la Universidad del Atlántico pueden consultar el contenido de este trabajo de grado en la página Web institucional, en el Repositorio Digital y en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad del Atlántico.
- Permitir consulta, reproducción y citación a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato CD-ROM o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

Esto de conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, “Los derechos morales sobre el trabajo son propiedad de los autores”, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.
Atentamente,

Firma Rafael Gonzalez P.
RAFAEL EDUARDO GONZALEZ PUGLIESE
C.C. No. 1.043.023.028 de SABANALARGA

Universidad del Atlántico	CÓDIGO: FOR-DO-110
	VERSIÓN: 01
	FECHA: 02/DIC/2020

DECLARACIÓN DE AUSENCIA DE PLAGIO EN TRABAJO ACADÉMICO PARA GRADO

Este documento debe ser diligenciado de manera clara y completa, sin tachaduras o enmendaduras y las firmas consignadas deben corresponder al (los) autor (es) identificado en el mismo.

Puerto Colombia, **20 de Marzo de 2021**

Una vez obtenido el visto bueno del director del trabajo y los evaluadores, presento al **Departamento de Bibliotecas** el resultado académico de mi formación profesional o posgradual. Asimismo, declaro y entiendo lo siguiente:

- El trabajo académico es original y se realizó sin violar o usurpar derechos de autor de terceros, en consecuencia, la obra es de mi exclusiva autoría y detento la titularidad sobre la misma.
- Asumo total responsabilidad por el contenido del trabajo académico.
- Eximo a la Universidad del Atlántico, quien actúa como un tercero de buena fe, contra cualquier daño o perjuicio originado en la reclamación de los derechos de este documento, por parte de terceros.
- Las fuentes citadas han sido debidamente referenciadas en el mismo.
- El (los) autor (es) declara (n) que conoce (n) lo consignado en el trabajo académico debido a que contribuyeron en su elaboración y aprobaron esta versión adjunta.

Título del trabajo académico:	**FUNCIONES BENT Y ALGUNAS DE SUS APLICACIONES**
Programa académico:	**MATEMÁTICAS**

Firma de Autor 1:								
Nombres y Apellidos:	**RAFAEL EDUARDO GONZALEZ PUGLIESE**							
Documento de Identificación:	**CC**	**X**	**CE**		**PA**		**Número:**	**1.043.023.028**
Nacionalidad:					**Lugar de residencia:**			
Dirección de residencia:								
Teléfono:					**Celular:**			

Universidad del Atlántico	**CÓDIGO:** FOR-DO-111
	VERSIÓN: 0
	FECHA: 03/06/2020

FORMULARIO DESCRIPTIVO DEL TRABAJO DE GRADO

TÍTULO COMPLETO DEL TRABAJO DE GRADO	**FUNCIONES BENT Y ALGUNAS DE SUS APLICACIONES**
AUTOR(A) (ES)	**RAFAEL EDUARDO GONZALEZ PUGLIESE**
DIRECTOR (A)	**TOVIAS CASTRO POLO**
CO-DIRECTOR (A)	**-**
JURADOS	**CARLOS ADOLFO ARAUJO MARTÍNEZ** **GABRIEL MAURICIO VERGARA RÍOS**
TRABAJO DE GRADO PARA OPTAR AL TITULO DE	**MATEMÁTICO**
PROGRAMA	**MATEMÁTICAS**
PREGRADO / POSTGRADO	**PREGRADO**
FACULTAD	**CIENCIAS BÁSICAS**
SEDE INSTITUCIONAL	**SEDE NORTE**
AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO	**2020**
NÚMERO DE PÁGINAS	**123**
TIPO DE ILUSTRACIONES	**DIAGRAMAS**
MATERIAL ANEXO (VÍDEO, AUDIO, MULTIMEDIA O PRODUCCIÓN ELECTRÓNICA)	**NO APLICA**
PREMIO O RECONOMIENTO	**NO APLICA**

Funciones bent y algunas de sus aplicaciones.

Rafael E. Gonzalez Pugliese

Tesis De Pregrado

Barranquilla, Diciembre 2020

Funciones bent y algunas de sus aplicaciones.

Rafael E. Gonzalez Pugliese

Trabajo de Pregrado

Barranquilla, Diciembre 2020

UNIVERSIDAD DEL ATLÁNTICO

PROGRAMA DE MATEMÁTICAS

PREGRADO EN MATEMÁTICAS

Funciones bent y algunas de sus aplicaciones

Estudiante: Rafael E. Gonzalez pugliese

Este trabajo de grado ha sido aprobado en nombre de la Universidad del Atlántico por el siguiente jurado examinador:

Carlos Adolfo Araujo Martinez

Nombre- Filiacion -País

Gabriel Mauricio Vergara Rios

Nombre- Filiacion -País

Diciembre del 2020

Contenido

Resumen

En este trabajo de grado se hace un estudio de las funciones Booleanas y en especifico las Booleanas tipo bent. Inicialmente se construye una base teórica de conceptos algebraicos luego se definen las funciones Booleanas. Más adelante se estudia de manera detallada, destacando aspectos y características para así, poder llegar a las de tipo bent, de las funciones bent, se caracterizan y definen características importantes. Por último, se exponen algunas aplicaciones de estas funciones y problemas abiertos relacionados con ellas.

Palabras Claves: Función Booleana, función bent.

Agradecimientos

En primer lugar quiero agradecer a mi tutor PhD. Tovias Castro, quien con sus conocimientos y apoyo me guió a través de cada una de las etapas de este proyecto para alcanzar los resultados que buscaba.
A todos los profesores que me sirvieron como guía durante todo el pregrado, enseñándome un mundo nuevo para mi, un mundo que ni en el mejor de mis sueños cuando niño pensé que existiera, ayudándome a conocer y entender ese nuevo mundo llamado matemáticas, tal mundo con el que he soñado despierto los últimos años.
Por último, quiero agradecer a todos mis compañeros y a mi familia, por apoyarme y creer en mi. En especial, quiero hacer mención de mis padres, que siempre estuvieron ahí para brindarme su apoyo.

Capítulo 1

Introducción

La presente investigación se refiere al tema de las funciones Booleanas y las funciones Booleanas tipo bent, que se definen como aquellas funciones definidas de $\mathbb{F}_2^n$ a $\mathbb{F}_2$, donde n define el número de variables de la función. Para el caso donde n es un entero par, las funciones Booleanas que alcanzan la máxima no linealidad posible, funciones con la característica anterior son las que mejor resisten los ataques basados en el criptoanálisis lineal, estas se conocen como funciones bent. El nombre de funciones bent se debe a Oscar Rothaus, quien escribió un famoso articulo llamado *On bent functions*. Las funciones Booleanas y las Booleanas bent son un tema de mucho interés en la criptografía, una muestra de esto es la gran bibliografía existente sobre ellas, pero hay gran desconocimiento sobre sus propiedades, construcciones y aplicaciones.

En este trabajo se hace un estudio detallado de las funciones Booleanas en aspectos como: Definiciones, propiedades , caracterizaciones y aplicaciones.

Este trabajo se organiza de la siguiente manera: Primero, se presentan los temas previos necesarios para la comprensión del trabajo. Segundo, un análisis detallado de las funciones Booleanas basado en sus propiedades . Tercero, como preparación para las aplicaciones, se estudia la independencia de las variables de las funciones Booleanas. Cuarto, se estudia algunas aplicaciones relevantes de las funciones Booleanas. Por último, se enuncian algunos problemas abiertos relacionados con la temática abordada en este trabajo.

Capítulo 2

Preliminares

En este capítulo se definen los conceptos necesarios para que el lector pueda encontrar este trabajo de investigación de una forma autocontenida.

2.1 Teoría de anillos y cuerpos

DEFINICIÓN 2.1. **Grupo**
Un grupo G es un par $(G, \cdot)$, donde G es un conjunto no vacío y $*$ es una operación binaria que satisface la ley de asocitividad, existencia del elemento inverso y existencia del elemento identidad. Si los elementos bajo la operación binaria conmutan, entonces diremos que G es un grupo abeliano.

DEFINICIÓN 2.2. **Subgrupo**
Sea $(G, \cdot)$ un grupo. Un subgrupo de G es un subconjunto H de G cerrado para el producto,y tal que $(H, \cdot)$ un grupo.

DEFINICIÓN 2.3. **Anillo**
Un anillo es una tripleta $(R, +, \cdot)$ donde R es un conjunto no vacío; $+, \cdot$ son dos operaciones binarias en R llamadas usualmente como suma y producto que satisfacen los siguientes axiomas: $(R, +)$ es un grupo abeliano, $\cdot$ es una operación asociativa y distributiva bilateral respecto a $+$.
En un anillo con elemento identidad, para $a \in R$, decimos que a es una unidad (o un elemento invertible) si existe un $b \in R$ tal que si $ab = 1 = ba$.

DEFINICIÓN 2.4. **Subanillo**
Si $(R, +, \cdot)$ es un anillo, un subconjunto $S \subset R$ es un subanillo de R si S cerrado para la suma y el producto, $1 \in S$ y $(S, +, \cdot)$ es un anillo.

DEFINICIÓN 2.5. **Centro de un anillo**
Sea R un anillo, el centro de R denotado por $Cen\ R$ se define como:

$$Cen\ R = \{r \in R | \ rx = xr \ (x \in R)\}.$$

DEFINICIÓN 2.6. **Ideal**
Un subconjunto I de un anillo R se dice que es un ideal de R, si cumple:I es diferente de vacío, es cerrado bajo la adición para todos loe elementos en I, $ra \in I$ para todo $r \in R$ y $a \in I$.

DEFINICIÓN 2.7. **Homomorfismo de grupos**
Sean G y G' dos grupos. Se dice que aplicación $f : G \longrightarrow G'$ es un homomorfismo de grupos si cumple:

$$f(ab) = f(a)f(b) \ \ \forall\ a, b \in G.$$

DEFINICIÓN 2.8. **Homomorfismo de anillos**
Sean R y R' dos anillos. Se dice que aplicación $f : R \longrightarrow R'$ es un homomorfismo de anillos si cumple:

(1) $f(a + b) = f(a) + f(b) \ \ \forall\ a, b \in R.$

(2) $f(ab) = f(a)f(b) \ \ \forall\ a, b \in R.$

DEFINICIÓN 2.9. **Álgebra**
Sea R un anillo, y K un anillo conmutativo, y $\phi : K \longrightarrow Cen\ R$ es un homomorfismo de anillos. El sistema resultante (R, K, ϕ) es llamada una $K-$álgebra. En la practica, se tiende a suprimir ϕ y se habla de R como $K-$álgebra o como una álgebra sobre K.

DEFINICIÓN 2.10. **Endomorfismo, isomorfismo y automorfismo**
Un homomorfismo de grupos (respectivamente para anillos y cuerpos) en sí mismo es llamado endomorfismo.
Un homomorfismo de grupos (respectivamente para anillos y cuerpos) biyectivo es llamado isomorfismo.
A un isomorfismo de un grupo (respectivamente para anillos y cuerpos) en si mismo es llamado automorfismo.

DEFINICIÓN 2.11. **Núcleo e imagen**
Sea $f : G \longrightarrow G'$ una aplicación. Se define el núcleo de f y se denotará $Ker\ f$ al conjunto

$$Ker\ f = \{a \in G : f(a) = 0\}.$$

Se llama imagen de f y se denotará $Img\, f$ al conjunto

$$Img\, f = \{b \in G' : b = f(a) \text{ para cierto } \ a \in G\}.$$

DEFINICIÓN 2.12. **Elemento idempotente**
Sea a un elemento de un anillo R, decimos que a es idempotente si $a^2 = a$.

DEFINICIÓN 2.13. **Anillo Booleano**
Un anillo R es llamado Booleano si todos sus elementos son idempotentes.

DEFINICIÓN 2.14. **Característica de un anillo**
Sea R un anillo, supongamos que existe $m \in \mathbb{N}$ tal que $ma = 0$, $\forall a \in R$. Definimos la característica del anillo como :

$$Car(R) = \min\{m \in \mathbb{N} | ma = 0, \forall a \in R\}.$$

Si tal entero no existe diremos que R tiene característica cero.

OBSERVACIÓN 2.1.1. Con un cálculo sencillo se demuestra que los anillos Booleano son abeliano y tienen característica dos.

DEFINICIÓN 2.15. **Dominio entero**
Sea R un anillo con elemento identidad ($e \in R$ tal que $ae = ea = a \ \forall a \in R$) y conmutativo. Decimos que R es un dominio entero, si R no tiene divisores de cero. Es decir si $a, b \in R$ y $ab = 0$ entonces $a = 0$ o $b = 0$.

DEFINICIÓN 2.16. Sea R un anillo con elemento identidad, decimos que R es un anillo con división si cada elemento no cero en R es una unidad (si $a \in R$ y existe un $b \in R$ tal que $ab = 1 = ba$ luego a es una unidad o un elemento invertible).

LEMA 2.1. [8] Sea R un anillo con característica p con p primo. Entonces se verifican las siguientes relaciones

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \text{ y } (a - b)^{p^n} = a^{p^n} - b^{p^n}.$$

para todo $n \in \mathbb{N}$ y $a, b \in R$.

DEFINICIÓN 2.17. **Elemento asociado**
Sea R un anillo conmutativo con elemento identidad. Sean $a, b \in R$, se dice que b divide a a, si existe $c \in R$ tal que $a = cb$.
Un elemento $a \neq 0 \in R$ es asociado de un elemento $b \in R$, $b \neq 0$, si $a = \nu b$ para alguna unidad $\nu \in R$.

DEFINICIÓN 2.18. **Elemento irreducible**
Sea R un anillo conmutativo y con elemento identidad. Un elemento $p \in R$ es llamado irreducible si p es no cero y no es una unidad, además se tiene que si $p = ab$ con $a, b \in R$ implica que a o b es una unidad.

DEFINICIÓN 2.19. Un elemento $a \neq 0$ que no es una unidad en un dominio entero D, se dice que que tiene una factorización si puede ser expresado como $a = p_1 p_2 \cdots p_n$, donde $p_1 p_2 \cdots p_n$ son elementos irreducibles en D. La expresión $p_1 p_2 \cdots p_n$ se llama factorización de a.

DEFINICIÓN 2.20. **Dominio de factorización única (DFU)**
Un dominio entero es un dominio de factorización única (DFU), si cada elemento no cero, no unidad tiene una factorización única salvo en el orden. Si existen dos factorizaciones, una es asociada de la otra

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

entonces $n = m$.

DEFINICIÓN 2.21. **Cuerpo (o campo)**
Sea R un anillo, decimos que R es un cuerpo (o campo) si R es un anillo con división.

TEOREMA 2.1. [1] Si R es un anillo conmutativo finito con más de un elemento y sin divisores de cero, entonces R es un cuerpo.

COROLARIO 2.1. [1] Todo dominio entero finito es un cuerpo.

El siguiente resultado es un ejercicio clásico, en nuestro caso sirve para conocer el tipo de conjuntos en donde vamos a definir más adelante las funciones Booleanas.

TEOREMA 2.2. Un anillo Booleano R es un cuerpo si y solo si contiene al 0 y el 1.

Demostración. Supongamos que R es un cuerpo, veamos que no puede tener elementos diferentes del 0 y 1. Supongamos que existe $a \in R$ con $a \neq 0$ y $a \neq 1$, como R es Booleano entonces $a^2 = a$ luego $a^2 - a = 0$, simplificando $a(a-1) = 0$, entonces $a = 0$ o $a = 1$ lo cual es absurdo, entonces R solo puede contener al 0 y el 1. Veamos el reciproco, supongamos que R solo contiene al 0 y el 1, luego R es un cuerpo ya que es un dominio entero finito. □

PROPOSICIÓN 2.1.1. [2] $\mathbb{Z}_n$ es un cuerpo si y solo si n es un número entero primo.

DEFINICIÓN 2.22. **Subuerpo**
Un subanillo de un anillo R que sea además un cuerpo se denominará subcuerpo de R.

DEFINICIÓN 2.23. **Extensión de cuerpo**
Una extensión de cuerpos es un par (K, F) donde F es un cuerpo y K es un subcuerpo de F. Se denotará por F/K.
Llamaremos cuerpo intermedio de la extensión a todo subcuerpo de F que contenga a K.

DEFINICIÓN 2.24. Sea F/K una extensión de cuerpos y S un subconjunto de F. A la intersección de todos los cuerpos intermedios de la extensión que contienen a S, que es el menor cuerpo intermedio de la extensión que contiene al conjunto S, lo denominaremos cuerpo intermedio generado por S. Y lo denotaremos por $K(S)$.
Diremos que una extensión de cuerpos F/K es una extensión simple si existe algún $\alpha \in F$ tal que $F = K(\alpha)$.

TEOREMA 2.3. Sea F/K una extensión de cuerpos, entonces F es un espacio vectorial sobre K.

Demostración. Es claro que la suma en F y el producto en F de elementos de K por elementos de F dotan a F de estructura de $K-$ espacio vectorial. □

DEFINICIÓN 2.25. A la dimensión de F como $K-$ espacio vectorial se le llama grado de F sobre K.

DEFINICIÓN 2.26. Diremos que una extensión de cuerpos F/K es finita si F como espacio vectorial sobre K tiene dimensión m, en cuyo caso llamaremos a m grado de la extensión y se denotara como $[F : K] = m$.

DEFINICIÓN 2.27. **Elemento algebraico**
Sea una extensión de cuerpos F/K. Un elemento $\theta \in F$ Se dice algebraico sobre K si existe un polinomio no nulo $P(x) \in K[x]$ tal que $P(\theta) = 0$.
Una extensión de cuerpos F/K Se dice algebraica si todo elemento de F es algebraico sobre K.

TEOREMA 2.4. **Multiplicidad del grado** [2]
Sea F/K una extensión de cuerpos y L un cuerpo intermedio. Entonces F/K es finita si y solo si F/L y L/K son ambas finitas. Y, en este caso, se verifica:

$$[F : K] = [F : L] \cdot [L : K].$$

PROPOSICIÓN 2.1.2. [2] Sea $K(\alpha)/K$ una extensión simple con α algebraico sobre K, entonces

(1) Existe un polinomio mónico irreducible $f(x) \in K[x]$, único, tal que $f(\alpha) = 0$. A este polinomio se le denominara polinomio mínimo de α sobre K.

(2) $[K(\alpha) : K] = n = deg(f(x))$ (Grado del polinomio mínimo de α sobre K).

(3) Si $g(x) \in K[x]$ y $g(\alpha) = 0$, entonces $f(x)$ divide a $g(x)$.

(4) $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base de $K(\alpha)$ sobre K.

(5) Todo elemento de $K(\alpha)$ se escribe de forma única como $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ con $a_i \in K$.

DEFINICIÓN 2.28. Un cuerpo F se llama algebraicamente cerrado si no existen extensiones algebraicas propias de F. es decir, si L/F es un extensión algebraica ella obliga a que $L = F$.

DEFINICIÓN 2.29. **Clausura algebraica**
Sea K un cuerpo una extensión L/F se dice una clausura algebraica de K cuando se verifica:

(1) F es algebraicamente cerrado.

(2) F/K es una extensión algebraica.

TEOREMA 2.5. [3] Para todo cuerpo K existe una clausura algebraica de K y además es única salvo K− isomorfismos.

OBSERVACIÓN 2.1.2. Como consecuencia de la existencia y unicidad de la clausura algebraica de cualquier cuerpo K, se tiene que, para cada polinomio $f(x) \in K[x]$ existe una determinada extensión de K en la que dicho polinomio tiene todas sus raíces. El cuerpo generado sobre K por dichas raíces, denominado el cuerpo de descomposición de $f(x)$ sobre es, además único salvo K– isomorfismos.

TEOREMA 2.6. [2] Sea F un cuerpo finito y K un subcuerpo de F con q elementos entonces $|F| = q^m$, donde m es la dimensión de F como K–espacio vectorial.

TEOREMA 2.7. [2, 4] Sea F un cuerpo finito el cardinal de F es p^m donde , p es la característica de F y m es el grado de F sobre su subcuerpo primo.

LEMA 2.2. [2] Si F es un cuerpo finito con q elementos se tiene la siguiente factorización del polinomio $x^q - x \in F[x]$

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

TEOREMA 2.8. **Existencia y unicidad de cuerpos finitos** [2]
Para cada numero primo p y cada entero positivo $n \geq 1$ existe un cuerpo finito con p^n elementos. Además cualquier cuerpo finito con p^n elementos es isomorfo al cuerpo de descomposición del polinomio $x^{p^n} - x$ sobre $\mathbb{Z}_p$.

OBSERVACIÓN 2.1.3. (1) Se sabe que $\mathbb{Z}_p$ es un cuerpo si y solo si p es primo, esto junto con el teorema de existencia y unicidad de cuerpos finitos muestra que el cuerpo F_{p^m} es isomorfo a $\mathbb{Z}_{p^m}$ si y solo si $m = 1$ en caso contrario $\mathbb{Z}_{p^m}$ no será un cuerpo.

(2) En lo sucesivo denotaremos (al menos que se indique lo contrario), como q al número de elementos de un cuerpo finito, teniendo presente que $q = p^r$, con p un número primo y $r \in \mathbb{N}$.

LEMA 2.3. [2] Si F es un cuerpo finito con q elementos y $a \in F$ es un elemento no nulo entonces $a^{q-1} = 1$, por tanto $a^q = a$ para cada a no nulo.

LEMA 2.4. [2] Sean $m, n \in \mathbb{N}$ y sea p un entero primo positivo, entonces si m es divisor de n el polinomio $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$.

TEOREMA 2.9. Estructura de subcuerpos [2]
Sea F_{p^n} un cuerpo finito con p^n elementos. Se verifica que cada subcuerpo de F_{p^n} tiene p^m elementos para algún entero positivo m divisor de n. Recíprocamente para cualquier entero positivo m divisor de n existe un único subcuerpo de F_{p^n} de orden p^m.

COROLARIO 2.2. [2] El grupo multiplicativo $(F_q^*, \cdot)$ de las unidades de un cuerpo es cíclico.

DEFINICIÓN 2.30. Un elemento de F_q que genere el grupo multiplicativo F_q^* de las unidades recibirá el nombre de elemento primitivo.

PROPOSICIÓN 2.1.3. [2] Sea F_r/F_q Una extensión finita de cuerpos, se tiene que $F_r \backslash F_q$ es una extensión simple y algebraica y además para cualquier elemento primitivo $\theta \in F_r$ se cumple $F_r = F_q(\theta)$.

LEMA 2.5. [2] Sea $f(x) \in F_q[x]$ es un polinomio irreducible de grado m, entonces f divide al polinomio $x^{q^n} - x$ si y solo si m divide a n.

PROPOSICIÓN 2.1.4. [2] Si $f(x) \in F_q[x]$ es un polinomio irreducible de grado m sobre F_q entonces $f(x)$ tiene alguna raíz $\alpha \in F_{q^m}$. Es más, todas la raíces de f son simples y son exactamente $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$.

COROLARIO 2.3. Si $f(x) \in F_q[x]$ un polinomio irreducible de grado m, se tiene que F_{q^m} es el cuerpo de descomposición de f sobre F_q.

DEFINICIÓN 2.31. Sea una extensión de cuerpos F_{q^m}/F_q y sea $\alpha \in F_{q^m}$. A los elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ se les denomina conjugados de α sobre F_q.

TEOREMA 2.10. [2] Los distintos F_q- automorfismos de F_{q^m} vienen dados por las funciones $\sigma_0, ..., \sigma_{m-1}$ donde $\sigma_j : F_{q^m} \longrightarrow F_{q^m}$ está definida por $\sigma_j(\alpha) = \alpha^{q^j}$ para cada $\alpha \in F_{q^m}$ con $0 \leq j \leq m-1$.

DEFINICIÓN 2.32. sea una extensión de cuerpos F/K. Se le llama grupo de Galois de dicha extensión y se denotara $Gal(F/K)$ al conjunto de $K-$automorfismo de f con la composición de aplicaciones.

El grupo de Galois de una extensión de cuerpos finita es cíclico algo que no ocurre para las extensiones de cuerpos arbitrarias

DEFINICIÓN 2.33. sea una extensión algebraica de cuerpos F/K, sea $f(x) \in K[x]$ un polinomio no constante y $\alpha \in F$ un elemento arbitrario, diremos que:

(1) El polinomio f es separable si no tiene raíces múltiples en su clausura algebraica de K.

(2) α es un elemento separable sobre K si su polinomio mínimo es un polinomio separable.

(3) La extensión F/K es separable si todo elemento de F es separable sobre K.

DEFINICIÓN 2.34. **Cuerpo perfecto**
Un cuerpo K se dice perfecto cuando todo polinomio irreducible de $K[x]$ es separable, o cuando toda extensión algebraica F/K es separable.

DEFINICIÓN 2.35. **Extensión normal**
Sea F/K una extensión algebraica y sea L una clausura algebraica de F. Decimos que F/K es una extensión normal si todo $K-$ homomorfismo $\sigma(F) \subseteq F$.

PROPOSICIÓN 2.1.5. [5] Sea F/K una extensión algebraica. Las siguientes condiciones son equivalentes:

(1) F/K es una extensión normal.

(2) Todo polinomio irreducible sobre $f(x) \in K[x]$ que tenga una raíz en F escinde (o descompone) sobre F.

(3) F es cuerpo de descomposición sobre K de algún conjunto de polinomios no constante de $K[x]$.

DEFINICIÓN 2.36. **Extensión de Galois**
Sea F/K una extensión algebraica. Se dice que F/K es una extensión de Galois si es normal y separable.

PROPOSICIÓN 2.1.6. [3] Sea F/K una extensión de Galois y sea M un cuerpo intermedio de la misma. Entonces la extensión F/M es de Galois.

PROPOSICIÓN 2.1.7. [5] Sea F/K una extensión finita. Los siguientes enunciados son equivalentes.

(1) F/K es de Galois.

(2) $[F : K] = |Gal(F/K)|$.

DEFINICIÓN 2.37. **Extensión cíclica**
Una extensión de cuerpos F/K se dice cíclica cuando es finita, de Galois y su grupo $Gal(F/K)$ es cíclico.

TEOREMA 2.11. [2] Toda extensión de cuerpos finitos es una extensión cíclica.

OBSERVACIÓN 2.1.4. Si tenemos una extensión de cuerpos finitos arbitraria F_{q^m}/F_q, entonces el F_q–automorfismo $\sigma : F_{q^m} \longrightarrow F_{q^m}$ dado por $\sigma(\alpha) = \alpha^q$ genera el grupo $Gal(F_{q^m}/F_q)$ dicho automorfismo recibirá el nombre de automorfismo de Frobenius. Los conjugados de un elemento $\alpha \in F_{q^m}$ serán por tanto los elementos obtenidos de la aplicación sucesiva del automorfismo de Frobenius sobre α.

2.2 Traza

Con el objeto de simplificar la notación, convendremos salvo que se indique lo contrario que $K := F_q$ y $F := F_{q^m}$ donde $m \geq 1$ corresponde al grado de la extensión.

DEFINICIÓN 2.38. **Traza**
Para cada $\alpha \in F$ se define la traza de α sobre K y se denotará $Tr_{F/K}(\alpha)$ como

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{m-1}}$$

Es decir, la traza de α sobre K es la suma de los conjugados de α.

DEFINICIÓN 2.39. Sea K un cuerpo, un polinomio $P \in K[x_1, ..., x_n]$ se dice que es simétrico si para toda permutación $\sigma \in S_n$ la aplicación φ_σ de $K[x_1, ..., x_n]$ en sí mismo que es la identidad sobre K y actúa en las variables x_i como $\varphi_\sigma(x_i) = x_{\sigma_{(i)}}$ verifica que $\varphi_\sigma(f) = f$. Se llaman polinomios simétricos elementales en n indeterminadas a los polinomios:

$$s_r^n(x_1, ..., x_n) = \sum_{1 \leq i_1 \leq ... \leq i_r \leq n} x_{i_1}...x_{i_r} \text{ con } 0 \leq r \leq n$$

PROPOSICIÓN 2.2.1. **Formulas de Cardano Vieta** [3]
Sea D un dominio de factorización única. Sea

$$f = \sum_{i=0}^{n} a_i x^i \in D[x]$$

Un polinomio mónico , es decir , $a_n = 1$. Supongamos que f se factoriza en $D[x]$ como $f = (x - \alpha_1)\cdots(x-\alpha_n)$. Entonces si $s_1, ..., s_1$ denota los polinomios simétricos elementales en n indeterminadas sobre D, se tiene:

$$a_{n-r} = (-1)^r s_r(\alpha_1, ..., \alpha_n) \text{ para cada } r = 1, ..., n$$

LEMA 2.6. [2] Para cualquier $\alpha \in F$ se verifica que $Tr_{F/K}(\alpha) \in K$

Demostración. Sea $f(x)$ el polinomio mínimo de $\alpha \in F$ sobre K y sea $d = deg(f)$. Consideremos ahora el polinomio $g(x) = f(x)^{\frac{m}{d}}$ con $m = [F : K]$. Así las raíces de $g(x)$ serán las mismas que las de $f(x)$ pero repetidas $\frac{m}{d}$ veces cada una. Entonces por definición, $Tr_{F/K}(\alpha)$ sera exactamente la suma de las raíces de $g(x)$, y a su vez por las formulas de Cardano Vieta $Tr_{F/K}(\alpha)$ sera igual al cociente de la variable x^{m-1} en $g(x)$, que es un polinomio de $K[x]$. □

PROPOSICIÓN 2.2.2. [2] La traza de un elemento verifica las siguientes propiedades

(1) $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ para cada $\alpha, \beta \in F$.

(2) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ para cada $\alpha \in F$,$c \in K$.

(3) La traza es una aplicación lineal sobreyectiva de de F en K.

(4) $Tr_{F/K}(\alpha) = m\alpha$ para todo $\alpha \in K$, donde $m = [F : K]$.

(5) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$ para cada $\alpha \in F$.

Demostración. (1) Sean $\alpha, \beta \in F$

$$\begin{aligned} Tr_{F/K}(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^q + \cdots + (\alpha + \beta)^{q-1} \\ &= (\alpha + \beta) + (\alpha^q + \beta^q) + \cdots + (\alpha^{q-1} + \beta^{q-1}) \\ &= Tr_{F/K}(\alpha) + Tr_{F/K}(\beta) \end{aligned}$$

donde la segunda igualdad se deduce del lema (2.1).

(2) Sea $\alpha \in F$, $c \in K$

$$\begin{aligned} Tr_{F/K}(c\alpha) &= (c\alpha) + (c\alpha)^q + \cdots + (c\alpha)^{q-1} \\ &= c\alpha + c\alpha^q + \cdots + c\alpha^{q-1} \\ &= cTr_{F/K}(\alpha). \end{aligned}$$

Para obtener la tercera igualdad se tuvo en cuenta el lema (2.3).

(3) En las dos propiedades anteriores se ha visto la linealidad de la traza. Además se verifica que $Tr_{F/K}(0) = 0$, vamos a ver también que $Tr_{F/K}(\alpha) \neq 0$ para algún $\alpha \in F$, y por tanto que la imagen de la función $Tr_{F/K}$ es todo $K = F_q$.
El núcleo de la aplicación traza es precisamente el conjunto de raíces del polinomio $P(x) = \sum_{i=0}^{m-1} x^{q^i}$ que tiene grado q^{m-1} y por tanto a lo sumo q^{m-1} raíces distintas. Pero el cuerpo $F = F_{q^m}$ contiene q^m elementos, por lo que alguna de ellas no pertenece al núcleo.

(4) Supongamos $\alpha \in K$, entonces

$$\begin{aligned} Tr_{F/K}(\alpha) &= \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\ &= \alpha + \alpha + \cdots + \alpha = m\alpha \end{aligned}$$

Para obtener la segunda igualdad se tuvo en cuenta el lema (2.3).

(5) Sea $\alpha \in K$

$$\begin{aligned} Tr_{F/K}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha^{q^m} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha = Tr_{F/K}(\alpha) \end{aligned}$$

Para obtener la última igualdad se tuvo en cuenta el lema (2.3).

□

EJEMPLO 2.2.1. Para $n = 3$, sea F_{2^3} construido con el polinomio irreducible $g(x) = x^3 + x + 1$. El elemento $x+1$ es primitivo, con un cálculo, se verifica que sus potencias son distintas. Denotemos con α a $x + 1$; a continuación, calcularemos la traza de cada elemento del campo F_{2^3}.

Vector	Polinomio	α^k	Traza $Tr(c) = c + c^2 + c^4$	$f = Tr$
(000)	0		0	0
(001)	1	α^0	$\alpha^0 + \alpha^{0\cdot 2} + \alpha^{0\cdot 4} = 1$	1
(010)	x	α^5	$\alpha^5 + \alpha^{5\cdot 2} + \alpha^{5\cdot 4} = \alpha^5 + \alpha^3 + \alpha^6 = 0$	0
(011)	$x+1$	α^1	$\alpha^1 + \alpha^{1\cdot 2} + \alpha^{1\cdot 4} = 1$	1
(100)	x^2	α^3	$\alpha^3 + \alpha^{3\cdot 2} + \alpha^{3\cdot 4} = \alpha^3 + \alpha^6 + \alpha^5 = 0$	0
(101)	x^2+1	α^2	$\alpha^2 + \alpha^{2\cdot 2} + \alpha^{2\cdot 4} = \alpha^2 + \alpha^4 + \alpha^1 = 1$	1
(110)	x^2+x	α^6	$\alpha^6 + \alpha^{6\cdot 2} + \alpha^{6\cdot 4} = \alpha^6 + \alpha^5 + \alpha^3 = 0$	0
(111)	x^2+x+1	α^4	$\alpha^4 + \alpha^{4\cdot 2} + \alpha^{4\cdot 4} = \alpha^4 + \alpha^1 + \alpha^2 = 1$	1

Tabla 2.1 Ejemplo del calculo de la traza de un elemento

PROPOSICIÓN 2.2.3. [2] Para cualquier $\alpha \in K$ se tiene que

$$|\{\beta \in F : Tr_{F/K}(\beta) = \alpha\}| = q^{m-1}.$$

Demostración. Sabemos por la proposición (2.2.2), que la aplicación traza $Tr_{F/K} : F \longrightarrow K$ es lineal y sobre. Luego teniendo en cuenta que $[F : K] = m$ y que K visto como K–espacio vectorial tiene dimensión 1, obtenemos de (2.2.2) $\dim(Ker(Tr_{F/K})) = m - 1$. Además se tiene que

$$\{\beta \in F : Tr_{F/K}(\beta) = \alpha\} = \{\beta_0 + \gamma : \gamma \in Ker(Tr_{F/K})\}.$$

Donde $\beta_0 \in F$ es un elemento fijo que cumple $Tr_{F/K}(\beta_0) = \alpha$, el cual debe existir por la sobreyectividad de la traza. Por tanto

$$|\{\beta \in F : Tr_{F/K}(\beta) = \alpha\}| = |Ker(Tr_{F/K})| = q^{m-1}.$$

□

TEOREMA 2.12. [2] Sea F una extensión finita de K. Entonces para $\alpha \in F$ tenemos $Tr_{F/K}(\alpha) = 0$ si y solo si $\alpha = \beta^q - \beta$ para algún $\beta^q \in F$.

Demostración. La condición de suficiencia es obvia por la propiedad (5) de la traza. Para probar el otro sentido. Supongamos $\alpha \in F = F_{q^m}$ con $Tr_{F/K}(\alpha) = 0$ y sea β una raíz de $x^q - x - \alpha$ en alguna

extensión finita de F. Entonces $\beta^q - \beta = \alpha$ y

$$\begin{aligned} 0 = \mathrm{Tr}_{F/K}(\alpha) &= \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta. \end{aligned}$$

□

2.3 Bases

Anteriormente se vio que todo cuerpo finito se puede considerado como un espacio vectorial sobre cada subcuerpo y por tanto existe una base sobre dichos subcuerpos.
A continuación, se definen diferentes tipos bases y se proporciona un método de comprobación para ver si un determinado conjunto es una base.

DEFINICIÓN 2.40. Sea F/K una extensión finita de cuerpos y sea $\{\alpha_1, \cdots, \alpha_m\}$ un conjunto de m elementos de F visto como espacio vectorial sobre K. Se define el discriminante de $\alpha_1, \cdots, \alpha_m$ y se denotará $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m)$ como el determinante

$$\Delta_{F/K}(\alpha_1, ..., \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \cdots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

PROPOSICIÓN 2.3.1. [2] Sea F/K una extensión de cuerpos y sea $\alpha_1, ..., \alpha_m \in F$, donde m es la dimensión de F sobre K. El conjunto de $\{\alpha_1, ..., \alpha_m\}$ es una base de F sobre K si y solo si $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ es no nulo.

Demostración. Supongamos que $\{\alpha_1, ..., \alpha_m\}$ es una base, veamos que su discriminante es distinto de cero. Comprobando que las m columnas de la matriz en la definición de discriminante son linealmante independiente.
Denotemos con $C_1, ..., C_m$ las columnas de la matriz correspondiente al discriminante $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ y supongamos que existen $a_1, ..., a_m \in K$ tales que $a_1C_1 + ... + a_mC_m = 0$; es decir, para cada $1 \leq j \leq m$ se tendrá que

$$a_1\mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + ... + a_m\mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0$$

Tomemos ahora $\beta = a_1\alpha_1 + ... + a_m\alpha_m$. Entonces por la relación anterior y teniendo en cuenta la linealidad de la traza, se tiene que $Tr_{F/K}(\alpha\beta) = 0$ para todo $\alpha \in F$, pero esto solo ocurre si $\beta = 0$, es decir $a_1 = ... = a_1 = 0$ pues por hipótesis $\{\alpha_1, ..., \alpha_m\}$ es una base de F sobre K.
Supongamos ahora $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ y que $a_1\alpha_1 + ... + a_m\alpha_m = 0$ para ciertos $a_1, ..., a_m \in K$. Pero entonces se verificará también

$$\beta := a_1\alpha_1\alpha_j + ... + a_m\alpha_m\alpha_j = 0 \text{ donde } 1 \leq j \leq m$$

Tomando la traza de β y por propiedades vistas en la proposición (2.2.2) tenemos

$$a_1 Tr_{F/K}(\alpha_1\alpha_j) + ... + a_m Tr_{F/K}(\alpha_m\alpha_j) = 0 \text{ con } 1 \leq j \leq m$$

Pero hemos supuesto que $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ y por tanto las columnas de la matriz son linealmante independiente por lo que

$$a_1\alpha_1 C_j + ... + a_m C_m\alpha_j = 0 \text{ entonces } \ a_1 = ... = a_m = 0$$

Obtenemos así que $\alpha_1, ..., \alpha_m$ son m elementos linealmante independientes; por tanto una base de F sobre K. □

DEFINICIÓN 2.41. Sea $\theta \in F_{q^m}$ una raíz de un polinomio irreducible de grado m sobre F_q. Entonces a una base $\left\{1, \theta, \cdots, \theta^{m-1}\right\}$ de F_{q^m} sobre F_q es llamada una base polinómica.

DEFINICIÓN 2.42. Supongamos que $\theta \in F_{q^m}$ es tal que le conjunto

$$\left\{\theta^{q^i} : 0 \leq i \leq m-1\right\}.$$

es una base de F_{q^m} sobre F_q . Entonces a una base de esta forma es llamada una base normal de F_{q^m} sobre F_q.

DEFINICIÓN 2.43. Sea una extensión de cuerpos F_{q^m}/F_q. Diremos que una base es primitiva normal si es de la forma $\left\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\right\}$ donde α es un elemento primitivo de F_{q^m}.

2.4 Campo finito $\mathbb{F}_p$

DEFINICIÓN 2.44. Sea p un número primo, $\mathbb{F}_p$, el denominado un campo primo, está compuesto por el conjunto de enteros $\{0, 1, ..., p-1\}$ con las operaciones aritméticas:

(1) Adición: Si $a, b \in \mathbb{F}_p$ entonces $a + b = r$, donde r es el residuo de la división de $a + b$ entre p y $0 \leq r \leq p - 1$. Esta operación es conocida como suma módulo p.

(2) Multiplicación: Si $a, b \in \mathbb{F}_p$, entonces $a \cdot b = s$, donde s es el residuo de la división de $a \cdot b$ entre p. Esta operación es conocida como multiplicación módulo p.

(3) Inversión: si a es un elemento de $\mathbb{F}_p$ diferente de cero, el inverso de a módulo p, denotado por a^{-1}, es el entero único $c \in \mathbb{F}_p$ tal que $a \cdot c = 1$.

2.5 Campo finito $\mathbb{F}_{2^m}$

El campo finito $\mathbb{F}_{2^m}$, denominado campo finito de característica 2 o campo binario, por lo que hemos visto anteriormente lo podemos ver como espacio vectorial de dimensión m sobre el campo $\mathbb{F}_2$. Luego, existen elementos $\alpha_0, ..., \alpha_{m-1}$ en $\mathbb{F}_{2^m}$ tales que cada $\alpha \in \mathbb{F}_{2^m}$ puede ser escrito en forma única como:

$$\alpha = a_0\alpha_0 + ... + a_{m-1}\alpha_{m-1}$$

donde $a_i \in \{0, 1\}$. Al conjunto $\{\alpha_0, ..., \alpha_{m-1}\}$ se le denomina una base de $\mathbb{F}_{2^m}$.
Dada una base, un elemento α del campo puede ser representado por la cadena de bits $(a_0a_1, \cdots, a_{m-1})$, (bits: acronimo de binary digit, unidad mas pequeña de información). La adición de elementos en el campo se realiza mediante XOR bit a bit de sus representaciones vectoriales (XOR: disyunción exclusiva).

2.6 Representación en bases polinomiales

Sea

$$f(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + f_0$$

donde $f_i \in \{0, 1\}$, para $i = 0, ..., m - 1$ un polinomio irreducible de grado m sobre $\mathbb{F}_2$, entonces $f(x)$ define una representación de base polinomial de $\mathbb{F}_{2^m}$, la cual se describirá a continuación:
El campo $\mathbb{F}_{2^m}$ está compuesto por todos los polinomios sobre $\mathbb{F}_2$ de grado menor a m,

$$\mathbb{F}_{2^m} = \left\{ a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 : a_i \in \{0, 1\} \right\}.$$

Al elemento $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0$ usualmente se le denota por la cadena de bits $(a_{m-1}a_{m-2}, \cdots, a_1a_0)$ de longitud m, de modo que

$$\mathbb{F}_{2^m} = \{(a_{m-1}a_{m-2}, \cdots, a_1a_0) : a_i \in \{0, 1\}\}$$

Se define las operaciones aritméticas sobre los elementos de $\mathbb{F}_{2^m}$ cuando se tiene una representación de base polinomial con reducción polinomial $f(x)$:

(1) Adición: si $(a_{m-1}a_{m-2}, \cdots, a_1a_0)$ y $(b_{m-1}b_{m-2}, \cdots, b_1b_0)$ son elementos de $\mathbb{F}_{2^m}$ entonces, $a + b = c = (c_{m-1}c_{m-2}, \cdots, c_1c_0)$ donde $c_i = a_i + b_i$ módulo 2.

(2) Multiplicación: si $(a_{m-1}a_{m-2}, \cdots, a_1a_0)$ y $(b_{m-1}b_{m-2}, \cdots, b_1b_0)$ son elementos de $\mathbb{F}_{2^m}$ entonces, $a \cdot b = r = (r_{m-1}r_{m-2}, \cdots, r_1r_0)$, donde el polinomio $r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + \cdots + r_1x + r_0$ es el residuo de la división de

$$(a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0) \cdot (b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0)$$

entre $f(x)$

(3) Sea $a \in \mathbb{F}_{2^m}$, con $a \neq 0$, el inverso de a que se denota por a^{-1}, es el elemento $c \in \mathbb{F}_{2^m}$ tal que $c \cdot a = 1$.

EJEMPLO 2.6.1. Una representación en base polinomial para $\mathbb{F}_{2^4}$. Sea $f(x) = x^4 + x + 1$ la reducción polinomial. Entonces los 16 elementos de $\mathbb{F}_{2^4}$ son los siguientes

$0 = (0000)$	$1 = (0001)$	$x = (0010)$	$x + 1 = (0011)$
$x^2 = (0100)$	$x^2 + 1 = (0101)$	$x^2x = (0110)$	$x^2 + x + 1 = (0111)$
$x^3 = (1000)$	$x^3 + 1 = (1001)$	$x^3 + x = (1010)$	$x^3 + x + 1 = (1011)$
$x^3 + x^2 = (1100)$	$x^3 + x^2 + 1 = (1101)$	$x^3 + x^2 + x = (1110)$	$x^3 + x^2 + x + 1 = (1111)$

Tabla 2.2 Representación en base polinomial

Algunos ejemplos de operaciones aritméticas sobre $\mathbb{F}_{2^4}$ son los siguientes

(1) $(1011) + (0001) = (1010)$.

(2) $(1010) \cdot (1100) = (0001)$.

(3) $(1101)^{-1} = (0100)$.

Capítulo 3

Análisis de Fourier Funciones y Mapeos Booleanos

3.1 Función y mapeo Booleano

DEFINICIÓN 3.1. **Función Booleana**
Una función Booleana de n variables es una función definida de la siguiente forma:
$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, donde $\mathbb{F}_2$ denota el cuerpo con dos elementos, y $\mathbb{F}_2^n$ denota el espacio vectorial $n-$dimensional sobre $\mathbb{F}_2$.
Toda función Booleana puede ser definida por su tabla de verdad (esta tabla está en un orden canónico o lexicográfico), de la siguiente manera:

$x_1 \cdots x_n$	$f(x_1, \cdots, x_n)$
$0 \cdots 0$	$*$
.	.
.	.
.	.
$1 \cdots 1$	$*$

Donde en la primera columna se encuentran todos los posibles vectores de $\mathbb{F}_2^n$ y en la segunda columna están los valores que toma la función Booleana denotada en este caso por $*$.

EJEMPLO 3.1.1. Sea $g : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, donde $g(00) = g(11) = 0$ y $g(01) = g(10) = 1$, luego, la anterior función es representada en la tabla (3.1).

$x_1\ x_2$	$g(x_1, x_2)$
00	0
01	1
10	1
11	0

Tabla 3.1 Función Booleana representada en tabla de verdad , ejemplo (3.1.1)

Es fácil ver el número de funciones Booleanas es 2^{2^n}, al construir una función, podemos escoger 2^n valores posibles para $f(x)$ donde x corre a través de $\mathbb{F}_2^n$. Una función Booleana vectorial o un mapeo Booleano es una función de la forma $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, donde q es un entero.
Denotaremos con $\mathcal{F}_n$ al conjunto de todas las funciones Booleanas en $\mathbb{F}_2^n$. La negación lógica de la función $f \in \mathcal{F}_n$ es la función $\bar{f} = f + 1$.
Sea $\mathcal{L}_n$ el conjunto de todas formas lineales, que es el espacio dual de $\mathbb{F}_2^n$. Sea $\{e_1, ..., e_n\}$ la base canónica de $\mathbb{F}_2^n$ y $\cdot$ el producto punto canónico, identificando una forma lineal como $x \longmapsto u \cdot x$ con el vector $u \in \mathbb{F}_2^n$ da el isomorfismo $\mathbb{F}_2^n \cong \mathcal{L}_n$.
Sea $\mathcal{A}_n$ el conjunto de todas funciones afines de $\mathbb{F}_2^n$ a $\mathbb{F}_2$ hay 2^{n+1} de ellas que son las formas lineales y sus negaciones, las funciones afines son de la forma:
$f(x) = \alpha(x) + c$ donde $\alpha \in \mathcal{L}_n$ y $c \in \mathbb{F}_2$.

Ahora, definamos $\chi : \mathbb{F}_2 \longrightarrow \mathbb{C}$ con $\chi(0) = 1$ y $\chi(1) = -1$ que es lo mismo
$\chi(a) = -1^a = 1 - 2a$ (identificando con $1 \in \mathbb{F}_2$ con $1 \in \mathbb{R}$) en particular χ es una función de valor real. Ahora para cada función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ asociamos su forma característica como:
$\chi_f := \chi \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{R}$, $\chi_f(x) = (-1)^{f(x)}$, esta función tiene las dos siguientes propiedades:
1) $\chi_{f+g} = \chi_f \chi_g$, ya que $\chi_{(f+g)(x)} = (-1)^{f(x)+g(x)} = (-1)^{f(x)}(-1)^{g(x)} = \chi_{f(x)}\chi_{g(x)}$
2) $2\chi_{fg} = 1 + \chi_f + \chi_g - \chi_{fg}$.
construyamos la siguiente tabla

a	b	$a+b$	ab	χ_a	χ_b	χ_{a+b}	χ_{ab}
0	0	0	0	1	1	1	1
0	1	1	0	1	-1	-1	1
1	0	1	0	-1	1	-1	1
1	1	1	1	-1	-1	1	-1

observando la tabla podemos deducir la siguiente formula:
$\chi_{a+b} + 2\chi_{ab} = 1 + \chi_a + \chi_b$ para todo $a, b \in \mathbb{F}_2$, por tanto para $f, g \in \mathcal{F}_n$ se tiene la formula del

producto $2\chi_{fg} = 1 + \chi_f + \chi_g - \chi_{fg}$.

DEFINICIÓN 3.2. **Distancia de Hamming**
Para dos funciones Booleanas $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ la distancia de Hamming es el número de argumentos donde las funciones difieren:

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

en otras palabras es el numero de unos en la tabla de verdad de $f + g$.

Veamos que d es una métrica en $\mathcal{F}_n$; para eso, d debe cumplir los 4 axiomas dela definición de métrica, los tres primeros es evidente que se cumplen, ya que dado dos vectores diferentes su distancia de Hamming será mayor que cero, y la distancia de Hamming entre dos vectores es cero si y solo si los vectores son el mismo, la simetría también es evidente, nos falta probar la desigualdad triangular, para eso definiremos unos conceptos previos para poder hacer la prueba.

DEFINICIÓN 3.3. **Peso de un vector**
Para cualquier elemento $X = x_1x_2 \cdots x_n \in \mathbb{Z}_2^n$, para un entero $n \geq 0$, el peso de X que denotaremos por $P(X)$ es el número de componentes X_i de X tales que $X_i = 1$ para $1 \leq i \leq n$. Si $Y \in \mathbb{Z}_2^n$ la distancia entre X e Y denotada por $d(X, Y)$ es el número de componentes tales que $X_i \neq Y_i$ para $1 \leq i \leq n$.

EJEMPLO 3.1.2. Para $n = 5$ $X = 01001$ y $Y = 11101$ entonces $P(X) = 2$ y $P(Y) = 4$, $d(X, Y) = 2$, además $X + Y = 10100$; de modo que $P(X + Y) = 2$, en este momento nos surge una pregunta , ¿ será que $d(X, Y) = P(X + Y)$? para cada $1 \leq i \leq 5$.
Tenemos que $X_i + Y_i$ contribuye con una unidad a $P(X + Y)$ si y solo si $X_i \neq Y_i$ si y solo si X_i, Y_i contribuye con una unidad a $d(X, Y)$.

TEOREMA 3.1. Para todo $x, y \in \mathbb{Z}_2^n$ se tiene que $P(x + y) \leq P(x) + P(y)$.

Demostración. Para cada $1 \leq i \leq n$ de las componentes de x_i,y_i,$x_i + y_i$ de x, y respectivamente solamente una situación haría que la desigualdad fuera falsa, si $x_i + y_i = 1$ mientras que $x_i = 0$ y $y_i = 0$ para algún $1 \leq i \leq n$ pero esto nunca ocurre, ya que si $x_i + y_i = 1$ implica que exactamente una de las variables de x_i o y_i es 1 entonces $P(x + y) \leq P(x) + P(y)$. □

Con base al teorema anterior (3.1) probaremos la desigualdad triangular.
Para $x, y, z \in \mathbb{Z}_2^n$ $d(x, z) = P(x + z)$ por otro lado sabemos que $\mathbb{Z}_2^n$ tiene característica dos entonces $y + y = 0$, luego $d(x, z) = P(x + z) = P(x + (y + y) + z) = P((x + y) + (y + z)) \leq P(x + y) + P(y + z) = d(x, y) + d(y, z)$. Así, d es una métrica.

TEOREMA 3.2. [6] Sean f y g funciones Booleanas luego

$$d(f, \bar{g}) = 2^n - d(f, g). \tag{3.1}$$

Demostración. Supongamos que dadas dos funciones Booleanas $f \neq g$ tales que :
$g = k - unos$ y $f = j - unos$ con $k, j \leq n$.

(1) **Caso 1.** Supongamos que los unos en f y g están en distintas posiciones, luego $d(f, g) = P(f + g) = k + j$ entonces $\bar{g} = 2^n - (k - unos)$, luego
$d(f, \bar{g}) = 2^n - (k + j)$
ya que los $j - unos$ estarán en la misma posición en $\bar{g}$ entonces se convertirán en ceros de $d(f, \bar{g})$, luego por otro lado tenemos $d(f, \bar{g}) + d(f, g) = 2^n - k - j + k + j = 2^n$.

(2) **Caso 2.** Consideremos ahora que puede existir al menos un 1 en la misma posición tanto en f como en g. Sean f, g funciones Booleanas tales que:
$g = k - unos$ y $f = j - unos$ con $k, j \leq n$.
Pero existe al menos un 1 en la misma posición $1 \leq N \leq n$ tanto en f como en g, luego
$d(f, g) = k + j - N$; donde N es el número de 1 en la misma posición
$\bar{g} = 2^n - (k - unos)$
$d(f, \bar{g}) = 2^n - k - j + N$, entonces
$d(f, \bar{g}) + d(f, g) = 2^n - k - j + N + k + j - N = 2^n$.

□

3.2 Representación de funciones Booleanas

3.2.1 Forma Normal Algebraica (FNA)

En la sección anterior conocimos las funciones Booleanas, son aquellas funciones del espacio vectorial $\mathbb{F}_2^n$ al campo finito $\mathbb{F}_2$. Las funciones Booleanas se pueden representar de formas distintas, pero por ahora solo estudiaremos la forma normal algebraica.
Una de las principales características de esta forma de representación, es, que permite definir el grado algebraico de una función Booleana.
En criptografía, se requiere que las funciones criptográficas tengan grado algebraico grande, por lo

que el grado algebraico de una función Booleana juega un papel muy importante en los criptosistemas que usan funciones Booleanas.

DEFINICIÓN 3.4. **Orden monomial**
Un orden monomial sobre $\mathbb{Z}_{\geq 0}^n$, es cualquier relación $>$ que satisface lo siguiente:

(1) $>$ es un orden total sobre $\mathbb{Z}_{\geq 0}^n$.

(2) Si $\alpha > \beta$ y $\gamma \in \mathbb{Z}_{\geq 0}^n$ entonces $\alpha + \gamma > \beta + \gamma$.

(3) $>$ es un buen orden sobre $\mathbb{Z}_{\geq 0}^n$.

La condición 3) es equivalente a : Para cada cadena infinita estrictamente decreciente $\alpha_1 > \alpha_2 > \cdots$ en $\mathbb{Z}_{\geq 0}^n$, existe un entero positivo k tal que $\alpha_k = \alpha_{k+1} = \cdots$.
El orden usual en $\mathbb{Z}_{\geq 0}^n$, $\cdots > m+1 > m > \cdots > 1 > 0$, satisface las tres condiciones de la definición anterior. Por lo tanto, el orden dado con respecto al grado para monomios en $K[x]$ es un orden monomial.
Daremos a continuación un orden sobre $\mathbb{Z}_{\geq 0}^n$ (con $n > 1$).

NOTA 1. (1) **Orden total:** Un orden total en un conjunto A, es un orden parcial (hay una relación de orden parcial en A) en A más la propiedad de que todo par de elementos son comparables bajo la relación.

(2) **Buen orden:** Sea A un conjunto ordenado tal que todo subconjunto de A tiene un primer elemento. Entonces A es un conjunto bien ordenado.

LEMA 3.1. [11] Una relación de orden $>$ en $\mathbb{Z}_{\geq 0}^n$ es un buen orden si y solo si cada sucesión estrictamente decreciente en $\mathbb{Z}_{\geq 0}^n$

$$\alpha(1) > \alpha(2) > \alpha(3) \cdots$$

eventualmente termina.

Demostración. Realizaremos la prueba por contraposición: Si $>$ no es un buen orden si y solo si hay una secuencia infinita estrictamente decreciente en $\mathbb{Z}_{\geq 0}^n$. Si $>$ no es un buen orden, entonces algún subconjunto no vacío $S \subset \mathbb{Z}_{\geq 0}^n$ no tiene elemento mínimo. Ahora tomando $\alpha(1) \in S$. Ya que $\alpha(1)$ no es el elemento mínimo, podemos definir $\alpha(1) > \alpha(2) \in S$. Entonces $\alpha(2)$ tampoco es el elemento mínimo, de modo que hay $\alpha(2) > \alpha(3) \in S$. Continuando de esta manera, se obtiene una sucesión infinita estrictamente decreciente

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots .$$

Recíprocamente, dada una sucesión infinita, entonces $\{\alpha(1), \alpha(2), \alpha(3), \cdots\}$ es un subconjunto no vació de $\mathbb{Z}^n_{\geq 0}$ sin elemento mínimo y por tanto, $<$ no es un buen orden. □

DEFINICIÓN 3.5. **Orden lexicográfico**
Sean $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Diremos que $\alpha >_{lex} \beta$ si, en el vector diferencia $\alpha - \beta \in \mathbb{Z}^n$, la primera entrada distinta de cero más a la izquierda es positiva. Escribiremos $x^\alpha >_{lex} x^\beta$ si $\alpha >_{lex} \beta$.
Se llama orden lexicográfico por que es análogo a la manera como se ordenan las palabras en un diccionario.

EJEMPLO 3.2.1. En $\mathbb{Z}^3_{\geq 0}$ $\alpha = (1, 2, 0) >_{lex} \beta = (0, 4, 5)$ ya que $\alpha - \beta = (1, -2, -5)$.

PROPOSICIÓN 3.2.1. [11] El orden lexicográfico $>_{lex}$ es un orden monomial sobre $\mathbb{Z}^n_{\geq 0}$.

Demostración. (1) Que $>_{lex}$ es un orden total, se deriva directamente de la definición y del hecho de que el orden numérico usual en $\mathbb{Z}_{\geq 0}$ es un orden total.

(2) Si $\alpha >_{lex} \beta$, entonces se tiene que la entrada más a la izquierda es diferente de cero en $\alpha - \beta$, digamos $\alpha_k - \beta_k$ es positiva. Pero $x^\alpha \cdot y^\gamma = x^{\alpha+\gamma}$ y $x^\beta \cdot y^\gamma = x^{\beta+\gamma}$. Entonces en $(\alpha+\gamma)-(\beta+\gamma) = \alpha + \beta$, la entrada más a la izquierda diferente de cero es otra vez $\alpha_k - \beta_k > 0$.

(3) Supongamos que $>_{lex}$ no es un buen orden. Entonces por el lema (3.1), habría una secuencia infinita estrictamente decreciente $\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \cdots$ de elementos de $\mathbb{Z}^n_{\geq 0}$. Mostraremos que lo anterior lleva a una contradicción. Consideremos las primeras entradas de los vectores $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Por la definición de orden lexicográfico, estas primeras entradas forman una sucesión no creciente de enteros no negativos. Ya que $\mathbb{Z}_{\geq 0}$ es bien ordenado, las primeras entradas de $\alpha(i)$ deben estabilizarse eventualmente. Es decir, existe un k tal que todas las primeras componentes de $\alpha(i)$ con $i \geq k$ son iguales. Comenzando en $\alpha(k)$, las segundas entradas y las siguientes entradas en juego para determinar el orden lexicográfico. Las segundas entradas de $\alpha(k), \alpha(k+1), \cdots$ forman una sucesión no creciente. Por el mismo razonamiento anterior, las segundas entradas estabilizan también eventualmente. Continuando de la misma manera, vemos que para algunos l, el $\alpha(l), \alpha(l+1), \cdots$ son todos iguales. Esto contradice el hecho de que $\alpha(l) >_{lex} \alpha(l+1)$.

□

Es importante notar que existen $n!$ ordenes lexicográficos sobre $\mathbb{Z}^n_{\geq 0}$, que corresponden a como los vectores $e_1 = (1, 0, ..., 0)$, $e_2 = (0, 1, ..., 0)$, ..., $e_n = (0, 0, ..., n)$ son asignadas a las variables $x_1, x_2, \cdots, x_n$. Por ejemplo, las variables $x_1, x_2, \cdots, x_n$ pueden ser ordenadas en forma usual asignando $e_i \longmapsto x_i$, pero cualquier permutación $\sigma \in S_n$ da lugar a un orden lexicográfico: $e_i \longmapsto x_{\sigma(i)}$ con $i = 1, ..., n$.

LEMA 3.2. [10] Sea $>$ cualquier orden monomial. Entonces $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$. Además, si x^α divide a x^β se tiene que $x^\alpha \leq x^\beta$.

Demostración. Si $0 > \alpha$ para algún $\alpha \in \mathbb{Z}^n_{\geq 0}$, entonces $0 > \alpha > 2\alpha > 3\alpha > \cdots$ es una cadena infinita estrictamente decreciente en $\mathbb{Z}^n_{\geq 0}$ para la cual no existe k talque $k\alpha = (k+1)\alpha = \cdots$; lo cual contradice que $>$ es un buen orden. Además, si x^α divide a x^β entonces $\beta = \alpha + \gamma$ para algún $\gamma \in \mathbb{Z}^n_{\geq 0}$. Ya que $\gamma \geq 0$, tenemos que $\beta = \alpha + \gamma \geq \alpha + 0 = \alpha$. □

Como consecuencia del lema anterior se tiene $x_i^2 \geq x_i$ para cualquier orden monomial $>$ sobre $\mathbb{Z}^n_{\geq 0}$, ya que, en $K[x_1, \cdots, x_n]$, x_i siempre divide a x_i^2.

DEFINICIÓN 3.6. Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio distinto de cero en $K[x_1, \cdots, x_n]$ y sea $>$ un orden monomial, se define lo siguiente.

(1) El exponente principal de f es $EP(f) = \text{máx}\left\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\right\}$.

(2) El coeficiente principal de f es $CP(f) = a_{EP(f)} \in K$.

(3) El monomio principal de f es $MP(f) = x^{EP(f)}$.

(4) El término principal de f es $TP(f) = CP(f)MP(f)$.

EJEMPLO 3.2.2. Sea $f = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4 \in K[x, y, z]$ y $>_{lex}$ el orden lexicográfico con $x >_{lex} y >_{lex} z$. Entonces $EP(f) = (2, 8, 0)$, $CP(f) = (-3)$, $MP(f) = x^5yz^4$ y $TP(f) = -3x^5yz^4$.

El exponente principal tiene las siguientes propiedades útiles, similares a las que tiene el grado de un polinomio de una sola variable.

LEMA 3.3. [10] Sea $f, g \in K[x_1, \cdots, x_n]$ polinomios no cero. Entonces $EP(fg) = EP(f) + EP(g)$. Además si $f + g \neq 0$, $EP(f + g) \leq \max\{EP(f), EP(g)\}$ y la igualdad se cumple si $EP(f) \neq EP(g)$.

Demostración. La igualdad se sigue de la parte (2) de la definición de orden monomial y de que la multiplicación en $K[x_1, \cdots, x_n]$ es distributiva con respecto a la adición. Para demostrar la desigualdad, basta observar que al ordenar los términos en $f+g$, el término que queda como principal es $TP(f)$ o $TP(g)$. Ya que éstos se pueden cancelar la desigualdad ocurre. □

Ahora estamos listos para formular el algoritmo de la división en $K[x_1, \cdots, x_n]$, el cual extiende al algoritmo para $K[x]$. El objetivo de éste es dividir al polinomio $f \in K[x_1, \cdots, x_n]$ entre una s–ada

ordenada $F = (f_1, f_2, \cdots, f_s)$ de polinomios $f_1, f_2, \cdots, f_s \in K[x]$; esto significa expresar a f en la forma :

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$$

Donde los coeficientes $a_1, a_2, \cdots, a_s$ y el residuo r están en $K[x_1, \cdots, x_n]$.

TEOREMA 3.3. **Algoritmo de la división en** $K[x_1, \cdots, x_n]$ [11]
Sea $>$ un orden monomial fijo sobre $\mathbb{Z}^n_{\geq 0}$ y $F = (f_1, f_2, ..., f_s)$ una s–ada ordenada de polinomios en $K[x_1, ..., x_n]$. Entonces cada $f \in K[x_1, ..., x_n]$ puede ser escrito como

$$f = a_1 f_1 + a_2 f_2 + ... + a_s f_s + r$$

donde $a_i, r \in K[x_1, ..., x_n]$ y $r = 0$ ó r es una combinación lineal, con coeficientes en K, de monomios, ninguno de los cuales es divisible por cualquier $TP(f_1), TP(f_2), ..., TP(f_s)$. Llamaremos a $r = 0$ el residuo de f po F. además, si $r \neq 0$, $EP(f) \geq EP(r)$ y si $a_i f_i \neq 0$, entonces tenemos que $EP(f) \geq EP(a_i f_i)$.

Demostración. Probaremos la existencia de $a_1, ..., a_s$ y r dando un algoritmo para su construcción y mostrando en cualquier entrada dada
Entrada: $f_1, ..., f_s, f$
Salida: $a_1, ..., a_s, r$
$a_1 := 0; ...; a_s := 0; r := 0$
$p := f$
Mientras: $p \neq 0$ ***Hacer***
$i := 1$
$divisiónocurrida ::= falsa$
Mientras $i \leq s$ ***y*** $divisiónocurrida := falsa$ ***Hacer***
Si $TP(f_i)$ $divide$ $TP(p)$ ***Entonces***
$a_i := a_i + TP(p)/TP(f_i)$
$p := p - (TP(p)/TP(f_i))f_i$
$divisiónocurrida := verdadero$
De otro modo:
$i := i + 1$
Si $divisiónocurrida := falsa$ ***Entonces***
$r := r + TP(p)$
$p = p - TP(p)$
la variable Booleana *divisiónocurrida* nos dice cuándo algunos $TP(f_i)$ divide el término principal del

dividendo intermedio. Se debe comprobar eso cada vez que se pasa por el bucle *Mientras...Hacer*, precisamente sucede una de dos cosas:

(1) **Paso división:** Si algún $TP(f_i)$ divide $TP(P)$, entonces el algoritmo procede como en el caso de una variable.

(2) **Paso restante:** Si ningún $TP(f_i)$ divide a $LT(p)$, entonces el algoritmo agrega $TP(p)$ al recordatorio.

Para probar que el algoritmo funciona, primero mostraremos que

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{3.2}$$

se mantiene en cada etapa. Esto es cierto para los valores iniciales de $a_1, ..., a_s, p$ y r. Ahora, supongamos que (3.2) se cumple en un paso del algoritmo. Si el siguiente paso es un paso de la división; entonces algún $TP(f_i)$ divide $TP(p)$ y la igualdad

$$a_i f_i + p = (a_i + TP(p)/TP(f_i))f_i + (p - (TP(p)/TP(f_i))f_i).$$

Muestra que $a_i f_i + p$ no ha cambiado. Como todas las demás variables no se ven afectadas, (3.2) permanece cierto en este caso. Por otro lado, si el siguiente caso es un paso restante, entonces p y r serán cambiado, pero la suma $p + r$ no ha cambiado desde

$$p + r = (p - TP(p)) + (r + TP(p)).$$

Como antes, la igualdad (3.2) aún se conserva.
Luego, se observa que el algoritmo se detiene cuando $p = 0$. En esta situación, (3.2) se convierte

$$f = a_1 f_1 + \cdots + a_s f_s + r.$$

Dado que los términos se agregan a r solo cuando son divisibles por ninguno de los $TP(f_i)$, se deduce que $a_1, ..., a_s$ y r tienen las propiedades deseadas cuando el algoritmo termina.
Finalmente, tenemos que mostrar que el algoritmo finalmente termina. La clave es, que cada vez que redefinimos la variables p, cada uno de los descensos del exponente principal (en relación con nuestro orden de término) o se convierte en 0. Para ver esto, supongamos que durante un paso de división, p se redefine para ser

$$p' = p - \frac{TP(p)}{TP(f_i)} f_i.$$

Por el lema (3.3), se tiene

$$\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}f_i\right) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\mathrm{LT}(f_i) = \mathrm{LT}(P),$$

de modo que p y $(\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$ tengan el mismo término principal. Por lo tanto su diferencia p' debe tener exponente principal más pequeño cando $p' \neq 0$. Luego, supongamos que durante un paso restante, p se redefine para ser $p' = p - \mathrm{LT}(p)$. Aquí, es obvio que $\mathrm{EP}(p') < \mathrm{EP}(p)$ cuando $p' \neq 0$. Por lo tanto, en cualquier caso, exponente principal debe disminuir. Si el algoritmo nunca terminará, abtendríamos una sucesión infinita decreciente de exponentes principales. La propiedad de buen orden de $>$, como se indica en el lema (3.1), muestra que esto no puede ocurrir. Por lo tanto, $p = 0$ debe suceder eventualmente, para que el algoritmo termine después de finitos pasos.
Queda por estudiar la relación entre $\mathrm{EP}(f)$ y $\mathrm{EP}(a_i f_i)$. Cada término en a_i es de la forma $\mathrm{TP}(p)/\mathrm{TP}(f_i)$ para algún valor de la variable p. El algoritmo comienza con $p = f$, y se acaba de probar que el exponente principal de p disminuye. Esto muestra que $\mathrm{TP}(p) \leq \mathrm{TP}(f)$, luego se sigue usando la condición (2) de la definición de orden monomial que $\mathrm{EP}(a_i f_i) \leq \mathrm{EP}(f)$ cuando $a_i f_i \neq 0$. □

EJEMPLO 3.2.3. Dividiremos $f = -x^2y - x^2z + x^3 + x + xyz$ entre $F = (f_1, f_2)$, donde $f_1 = x^2y - z$ y $f_2 = xy - 1$. Usaremos el orden $>_{lex}$ con $x >_{lex} y >_{lex} z$. El primer paso es escribir los términos de los polinomios en orden decreciente con respecto a $>_{lex}$:

$$\begin{aligned} f &= x^3 - x^2y - x^2z + xyz + x \\ f_1 &= x^2y - z \\ f_2 &= xy - 1 \end{aligned}$$

Ahora coloquemos los divisores de f_1 y f_2; los cocientes a_1, a_2 y el residuo r en el siguiente esquema

$$\begin{array}{ll} a_1: & \\ a_2: & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad r \\ x^2y - z \quad & /x^3 - x^2y - x^2z + xyz + x \\ xy - 1 & \end{array}$$

Los términos principales $\mathrm{TP}(f_1) = x^2y$ y $\mathrm{TP}(f_2) = xy$ no dividen al término principal $\mathrm{TP}(f) = x^3$, sin embargo, a diferencia de lo que ocurre con el algoritmo de la división en $K[x]$, $x^3 - x^2y - x^2z + xyz + x$ no es el residuo ya que $\mathrm{TP}(f_1) = x^2y$ y $\mathrm{TP}(f_2) = xy$ dividen a $-x^2y$.
Así que, moviendo x^3 al residuo, podemos continuar dividiendo

$$\begin{array}{lll} a_1: & & \\ a_2: & & r \\ x^2y-z & /\underline{x^3-x^2y-x^2z+xyz+x} & \\ xy-1 & \quad -x^2y-x^2z+xyz+x & \rightarrow\ x^3 \end{array}$$

Ahora, ambos términos $TP(f_1)$ y $TP(f_2)$ dividen a $TP(-x^2y-x^2z+xyz+x) = -x^2y$ pero ya que f_1 está listado primero, usamos f_1. Procedemos a dividir $-x^2y$ entre x^2y, y obtenemos $a_1 = -1$, y a restar $(-1)f$ de $-x^2y-x^2z+xyz+x$.

$$\begin{array}{lll} a_1: & -1 & \\ a_2: & & r \\ x^2y-z & /\underline{x^3-x^2y-x^2z+xyz+x} & \\ xy-1 & \quad -x^2y-x^2z+xyz+x & \rightarrow\ x^3 \\ & \quad \underline{-x^2y+z} & \\ & \quad -x^2z+xyz+x-z & \end{array}$$

Continuando con la división vemos que $TP(f_1) = x^2y$ y $TP(f_2) = xy$ no dividen a $TP(-x^2z+xyz+x-z) = -x^2z$, así que movemos $-x^2z$ al residuo y continuamos dividiendo. El término $TP(f_1) = x^2y$ no divide a $TP(xyz+x-z) = -xyz$ pero $TP(f_2) = xy$ si. El resultado de esta división es $a_2 = z$ y por tanto restamos zf_2 de $xyz+x+z$.

$$\begin{array}{lll} a_1: & -1 & \\ a_2: & z & r \\ x^2y-z & /\underline{x^3-x^2y-x^2z+xyz+x} & \\ xy-1 & \quad -x^2y-x^2z+xyz+x & \rightarrow\ x^3 \\ & \quad \underline{-x^2y+z} & \\ & \quad \underline{-x^2z+xyz+x-z} & \\ & \quad xyx+x-z & \rightarrow\ x^3-x^2z \\ & \quad \underline{xyz-z} & \\ & \quad x & \rightarrow\ x^3-x^2z+x \\ & \quad \overline{0} & \end{array}$$

Claramente ninguno de los términos principales de f_1 y f_2 dividen a x; por ello lo movemos al residuo. Por tanto

$$f = (-1)(x^2y-z) + z(xy-1) + (x^3-x^2z+x). \tag{3.3}$$

Se puede verificar que si dividimos f entre $G = (f_1, f_2)$ obtenemos

$$f = (-x + z)(xy - 1) + 0(x^2y - z) + (x^3 - x^2z - z).$$

Comparando con la ecuación (3.3), vemos que los a_i y el residuo son diferentes. Esto muestra que ellos pueden cambiar con sólo reordenar los f_i.

En la sección anterior se definió lo que es el peso de un elemento. Ahora definiremos el peso de una función Booleana $f \in \mathcal{F}_n$.

DEFINICIÓN 3.7. **Peso de una función Booleana**
Sea f una función Booleana en $\mathcal{F}_n$. Se define el peso de f como:

$$w(f) = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|$$

Ahora definamos la distancia de Hamming de $f \in \mathcal{F}_n$ en función del peso como $d(f, g) = w(f \oplus g)$ (recordemos que $\oplus$ es la suma usual entre funciones Booleanas, en módulo 2).

A continuación, describiremos dos representaciones de las funciones Booleanas que, en general, son usadas en criptografía y teoría de códigos.
La primera fue mencionada anteriormente, conocida como la tabla de verdad o vector característico de $f \in \mathcal{F}_n$. Ahora, la definiremos de forma más detallada como

$$V_f = (f(v_0), f(v_1), \cdots, f(v_{2^n-1})) \in \mathbb{F}_2^{2^n} \text{ donde } \mathbb{F}_2^n = \{v_0, v_1, \cdots, v_{2^n-1}\}$$

Note que V_f depende de la biyección $i \longmapsto v_i$ mientras que el peso de f no. Las ventajas de esta representación son la simplicidad además de que :

(1) Establece un isomorfismo entre los $\mathbb{F}_2$–espacios vectoriales y $\mathcal{F}_n$ y $\mathbb{F}_2^{2^n}$. De aquí que la dimensión de $\mathcal{F}_n$ es 2^n.

(2) El peso de f calculado directamente de su tabla de verdad como $w(f) = \sum_{a \in \mathbb{F}_2^n} f(a)$, donde el símbolo $\sum$ denota a la suma ordinaria de enteros.

EJEMPLO 3.2.4. Para $n = 2$ consideremos

(x_1, x_2)	$f(x_1, x_2)$	$g(x_1, x_2)$	$(f \oplus g)(x_1, x_2)$	$(f \otimes g)(x_1, x_2)$
$v_0 = (0, 0)$	1	0	1	0
$v_1 = (0, 1)$	1	0	1	0
$v_2 = (1, 0)$	1	0	1	0
$v_3 = (1, 1)$	0	1	1	0

Notemos que f y g son ambas diferentes de la función cero, sin embargo, $(f \otimes g)$ es la función cero, con lo anterior podemos deducir que $\mathcal{F}_n$ no es un dominio entero. De la tabla podemos ver que $V_f = (1, 1, 1, 0)$, $w(f) = 3$ y $d(f, g) = w(f \oplus g) = 4$.

También podemos representar una función Booleana en $\mathcal{F}_n$ por medio de un polinomio en n variables. Por ejemplo, la función $f(x_1, x_2) = x_1^2 x_2 \oplus 1$ es una expresión polinomial de la función f del ejemplo anterior. Pero no es obvio que para cada función Booleana se tenga una representación polinomial y que además sea única, ya que también el polinomio $p(x_1, x_2) = x_1 x_2 \oplus 1$ representa a f.

TEOREMA 3.4. [10] El anillo $\mathcal{F}_n$ es isomorfo al anillo cociente $\mathbb{F}_2[x_1, \cdots, x_n]/I$, donde $I = \langle x_1^2 \oplus x_1, \cdots, x_n^2 \oplus x_n \rangle$ es el ideal en $\mathbb{F}_2[x_1, \cdots, x_n]$ generado por los polinomios $x_1^2 \oplus x_1, \cdots, x_n^2 \oplus x_n$.

Demostración. Sea $\phi : \mathbb{F}_2[x_1, \cdots, x_n]/I \longrightarrow \mathcal{F}_n$ dada por $(p + I) \longmapsto f$, donde $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es tal que $\alpha \longrightarrow p(\alpha)$. Veamos que ϕ esta bien definida. Si tomamos dos representantes diferentes p y p', del mismo elemento de $\mathbb{F}_2[x_1, \cdots, x_n]/I$ la igualdad $\phi(p) = \phi(p')$ se debe cumplir. Supongamos que $p + I = p' + I$ en $\mathbb{F}_2[x_1, ..., x_n]/I$, entonces $p \oplus p' \in I$ y por tanto $p \oplus p' = \bigoplus_{i=1}^{n} h_i(x_i^2 \oplus x_i)$ donde $h_i \in \mathbb{F}_2[x_1, ..., x_n]$ para todo $i = 1, ..., n$. Sea $\alpha \in \mathbb{F}_2^n$; por la definición de la función ϕ tenemos que $\phi(p \oplus p') = f$, donde $f(\alpha) = (p \oplus p')(\alpha) = p(\alpha) \oplus p'(\alpha) = 0$ para todo $\alpha \in \mathbb{F}_2^n$; de aquí que $p(\alpha) = p'(\alpha)$ para todo $\alpha \in \mathbb{F}_2^n$. Entonces $\phi(p) = \phi(p')$ y por tanto ϕ está bien definida.
Por la forma en que está definida ϕ se deduce que es un homomorfismo de anillos. (También ϕ es una transformación lineal entre estos $\mathbb{F}_2$–espacios vectoriales).
Ahora veamos que ϕ es inyectiva, para eso veamos que $\ker \phi = I$.
Es claro que $I \subseteq \ker \phi$. Ahora sea $p + I \in \ker \phi$, entonces $\phi(p + I) = 0$; es decir, $p(\alpha) = 0$ para todo $\alpha \in \mathbb{F}_2^n$. Sea $>$ cualquier orden monomial sobre $\mathbb{Z}_{\geq 0}^n$. Dividamos al polinomio p, de acuerdo al algoritmo de la división en $K[x_1, \cdots, x_n]$, entre la n–ada ordenada de polinomios $F = (x_1^2 \oplus x_1, x_2^2 \oplus x_2, \cdots, x_n^2 \oplus x_n)$. Entonces

$$p = \bigoplus_{i=1}^{n} h_i(x_i^2 \oplus x_i) \oplus r(x_1, x_2, \cdots, x_n)$$

donde ningún x_i^2 divide a ningún monomio del polinomio $r(x_1, x_2, ..., x_n)$ ya que $TP(x_i^2 \oplus x_i) = x_i^2$ (ver lema (3.2)). Por lo tanto, los monomios de r son de la forma x_i o $x_{i_1} x_{i_2} \cdots x_{i_k}$ para algún $k \in \mathbb{Z}$. Ya

que $h_i(x_i^2 \oplus x_i) \in I$ y $p(\alpha) = 0$, tenemos que $r(\alpha) = 0$ para todo $\alpha \in \mathbb{F}_2^n$. Si el monomio x_i aparece en el polinomio r, entonces evaluando r en el vector $e_i \in \mathbb{F}_2^n$, obtenemos precisamente el coeficiente del monomio x_i en r, digamos a_i. Como $r(e_i) = 0$, vemos que $a_i = 0$. Así, el polinomio r no tiene monomios de la forma x_i. De manera similar, si algún monomio de la forma $x_{i_1}x_{i_2}$ aparece en el polinomio r, entonces evaluando r en el vector $\alpha \in \mathbb{F}_2^n$ que tiene unos en las coordenadas i_1 e i_2 y ceros en las restantes, obtenemos como resultado el coeficiente del monomio $x_{i_1}x_{i_2}$, digamos a_{i_1,i_2}. Nuevamente como $r(\alpha) = 0$, tenemos que $a_{i_1,i_2} = 0$. Procediendo de esta manera, vemos que r es el polinomio cero. Por tanto , $p = \bigoplus_{i=1}^n h_i(x_i^2 \oplus x_i)$; o sea, $p \in I$ y de esta forma hemos demostrado que $ker\,\phi \subseteq I$. Entonces , $I = ker\,\phi$, así ϕ es inyectiva.
Por otro lado, sea $f \in \mathcal{F}_n$. Necesitamos un elemento $p + I \in K[x_1, x_2, \cdots, x_n]/I$ tal que $\phi(p + I) = f$. Para construir tal elemento usemos el siguiente algoritmo:

(1) ***Entrada: la función Booleana*** $f \in \mathcal{F}_n$.

(2) ***Haga*** $p_0(x_1, x_2, \cdots, x_n) = f(0, 0, \cdots, 0)$.

(3) ***para*** $k = 1$ ***a*** $2^n - 1$ ***haga***
Calcule la representación binaria del entero k***,***
$k = b_0 + b_1 2 + b_2 2^2 + ... + b_{n-1}2^{n-1}$
si $p_{k-1}(b_0, b_1, \cdots, b_{n-1}) \neq f(b_0, b_1, \cdots, b_{n-1})$ ***entonces***
$p_k(x_1, x_2, \cdots, x_n) = p_{k-1}(x_1, x_2, \cdots, x_n) \oplus \prod_{i=1}^n (x_i^{b_{i-1}})$
De otra manera,
$p_k(x_1, x_2, \cdots, x_n) = p_{k-1}(x_1, x_2, \cdots, x_n)$.

(4) ***Salida:*** $p_{2^n-1}(x_1, x_2, \cdots, x_n)$.

Afirmamos que $p = p_{2^n-1}(x_1, x_2, \cdots, x_n)$ es tal que $\phi(p + I)$, es decir, para todo $\alpha \in \mathbb{F}_2^n$ tenemos que $p(\alpha) = f(\alpha)$. Para demostrar lo anterior, supongamos que estamos en el j–esimo paso del algoritmo, $1 \leq j \leq 2^n - 1$, y que $p_{j-1} = f$ para toda representación binaria de k con $0 \leq k \leq j - 1$. Si en este paso no se suma ningún monomio, $p_j = p_{j-1}$ y por lo tanto $p_j = f$ para toda representación binaria de k con $0 \leq k \leq j$. Por el contrario, si añadimos el monomio $\prod_{i=1}^n x_i^{b_{i-1}}$, donde $(b_0, b_1, ..., b_{n-1})$ es la representación binaria de j, sean $b_{i_1}, ..., b_{i_s}$ las coordenadas diferentes de cero del vector $(b_0, b_1, \cdots, b_{n-1})$. El monomio $x_{i_1}^{b_{i_1}} \cdots x_{i_s}^{b_{i_s}}$ al ser evaluado en las representaciones binarios de los enteros menores estrictos que j es cero; si esto no fuese así, entonces existe un vector $v \in \mathbb{F}_2^n$ correspondiente a la representación binaria de un entero no negativo menor estricto que j, el cual tiene $1's$ en las posiciones $i_1, ..., i_s$ y probablemente en otras. Pero esto implica que este entero es mayor o igual que j, lo cual no es posible. Entonces $p_j = p_{j-1} = f$ para toda representación binaria de k con $0 \leq k < j$.

Ahora, el monomio $x_{i_1}^{b_{i_1}} \cdots x_{i_s}^{b_{i_s}}$ es 1 cuando es evaluado en la representación binaria de j, la cual hace que p_j coincida con f en la representación binaria de j. Por lo tanto, $p_j = f$ para toda representación binaria de k con $0 \leq k \leq j$. □

Del teorema anterior tenemos, que toda función Booleana $f \in \mathcal{F}_n$ tiene una única representación polinomial, módulo el ideal I,

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x^{u_i} \right), \ \lambda_u \in \mathbb{F}_2, \ u = (u_1, u_2, \cdots, u_n)$$

Esta representación de f es llamada la forma normal algebraica de f (FNA). El grado total $deg(f)$ de la forma normal algebraica es llamado el grado algebraico de la función.

Una desventaja de la tabla de verdad es, que no da información acerca del grado algebraico de la función y sobre el número de términos de f en su FNA. La tabla de verdad puede ser recuperada de la FNA, y recíprocamente, la FNA puede ser calculada por medio de la tabla de verdad usando el algoritmo usado en la prueba del teorema anterior.

EJEMPLO 3.2.5. Para cada $k \in \{0, 1, ..., 7\}$ calcule su representación binaria $k = b_0 + 2b_1 + 4b_2$ y sea $v_k = (b_0, b_1, b_2)$ el vector asociado a k. Considere la función $f \in \mathcal{F}_3$ dada por la tabla de verdad $V_f = (0, 1, 1, 1, 0, 1, 0, 1)$.
Para calcular la FNA de f primero hacemos $p_0(x_1, x_2, x_3) = f(0, 0, 0) = 0$. Luego, comparamos los valores de p_0 y f en v_1. Vemos que $p_0(v_1) = 0$ y $f(v_1) = 1$ no coinciden, de acuerdo al algoritmo hacemos

$$p_1(x_1, x_2, x_3) = p_0(x_1, x_2, x_3) \oplus x_1^1 x_2^0 x_3^0 = 0 \oplus x_1 = x_1$$

Ahora comparamos p_1 y f en v_2, ya que $p_1(v_2) = 0$ y $f(v_2) = 0$ son iguales, entonces tenemos que $p_2 = p_1$, ahora evaluemos $p_2(v_3) = 1$ y $f(v_3) = 0$; son diferentes entonces para obtener p_3 añadimos un término a p_2

$$p_3(x_1, x_2, x_3) = p_2(x_1, x_2, x_3) \oplus x_1^1 x_2^1 x_3^0 = x_1 \oplus x_1 x_2$$

El procedimiento se resume en la siguiente tabla:

k	$k = b_0 + 2b_1 + 2^2b_2$	$f(b_0, b_1, b_2)$	$p_k(x_1, x_2, x_3)$
0	$(0,0,0)$	0	0
1	$(1,0,0)$	1	$0 \oplus x_1$
2	$(0,1,0)$	0	x_1
3	$(1,1,0)$	0	$x_1 \oplus x_1x_2$
4	$(0,0,1)$	0	$x_1 \oplus x_1x_2$
5	$(1,0,1)$	1	$x_1 \oplus x_1x_2$
6	$(0,1,1)$	0	$x_1 \oplus x_1x_2$
7	$(1,1,1)$	1	$x_1 \oplus x_1x_2 \oplus x_1x_2x_3$

Por tanto la FNA de f es $p(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3$, el $deg(f) = 3$ y el número de términos en su forma normal algebraica es 3.

3.2.2 Representación polinomial de una función Booleana

Cada función Booleana vectorial f en n variables, es una función (o mapeo) de $\mathbb{F}_{2^n}$ a $\mathbb{F}_{2^n}$. Estas funciones se pueden representar de forma única haciendo uso de la forma polinomial univariada (o representación polinomica) sobre $\mathbb{F}_{2^n}$ de grado a lo más $2^n - 1$.

$$f(x) = \sum_{i=0}^{2^n-1} \delta_i x^i$$

Cualquier función Booleana de $\mathbb{F}_{2^n}$ es un caso particular de una función vectorial de $\mathbb{F}_{2^n}$ (ya que $\mathbb{F}_2$ es un subcuerpo de $\mathbb{F}_{2^n}$) y admite por tanto una única representación, que llamaremos univariada de f. Para todo $u, v \in \mathbb{F}_{2^n}$ tenemos que $(u+v)^2 = u^2 + v^2$ y $u^{2^n} = u$. Un polinomio univariado $\sum_{i=0}^{2^n-1} \delta_i x^i$, $\delta_i \in \mathbb{F}_{2^n}$, es entonces la representación univariada de una función Booleana si y solo si

$$\left(\sum_{i=0}^{2^n-1} \delta_i x^i\right)^2 = \sum_{i=0}^{2^n-1} \delta_i^2 x^{2i} = \sum_{i=0}^{2^n-1} \delta_i x^i \left[\text{módulo } x^{2^n} + x\right]$$

esto es, $\delta_0, \delta_{2^n-1} \in \mathbb{F}_2$ para todo $i = 1, ..., 2^n - 2$, $\delta_{2i} = \delta_i^2$ donde los indices $2i$ toman mod $2^n - 1$.

3.2.3 Representación por traza

DEFINICIÓN 3.8. **Coclase ciclotómica**
Sea $\mathbb{Z}_{2^L-1}$ el conjunto de números enteros $[1, ..., 2^L - 1]$, se considerara la siguiente relación de equivalencia, denotada por R_e, definida sobre sus elementos: $e_1\ R_e\ e_2$ con $e_1, e_2 \in \mathbb{Z}_{2^L-1}$ si existe un entero j, $0 \leq j < L$, tal que

$$2^j \cdot e_1 = e_2 \bmod(2^L - 1)$$

R_e divide al conjunto $\mathbb{Z}_{2^L-1}$ en clases de equivalencia que denominaremos coclases ciclotómicas $\bmod(2^L - 1)$.

La función definida en $\mathbb{F}_{2^n}$ por $Tr_n = u + u^2 + u^{2^2} + \cdots + u^{2^{n-1}}$ es lineal y satisface $(Tr_n(u))^2 = Tr_n(u^2) = Tr_n(u^2)$ (proposición (2.2.2)).
La función $(u, v) \longmapsto Tr_n(u, v)$ es un producto interno en $\mathbb{F}_{2^n}$ que es simétrico para todo $u \neq 0$, la función $u \longmapsto Tr_n(uv)$ es una forma lineal no cero en $\mathbb{F}_{2^n}$.
Toda función Booleana puede ser escrita en la forma $f(x) = Tr_n(F(x))$ donde F es un mapeo de $\mathbb{F}_{2^n}$ en $\mathbb{F}_{2^n}$, es decir, demostrar que para una función Booleana arbitraria f siempre hay un función Booleana vectorial F tal que $f(x) = Tr_n(F(x))$. Realmente, en cuanto a la traza, es una función lineal no constante, hay un vector b distinto de cero tal que por cada x $Tr(x) = \langle b, x\rangle = b_1x_1 \oplus \cdots \oplus b_nx_n$. Toma cualquier i tal que $b_i = 1$. Considere un función Booleana vectorial $F : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ con funciones coordenadas $f_j(x) = 0$ si $j \neq i$, y $f_i(x) = f(x)$, entonces obviamente $f(x) = Tr_n(F(x))$. Un ejemplo de un mapeo F esta definido por $F(x) = \lambda f(x)$ donde $Tr_n(\lambda) = 1$ y $f(x)$ es la representación univariada. Así, toda función Booleana puede ser representada en la forma

$$Tr_n\left(\sum_{i=0}^{2^n-1} \beta_i x^i\right),$$

donde $\beta_i \in \mathbb{F}_{2^n}$. Esta representación no es única. Ahora, gracias al hecho de que $Tr_n(u^2) = Tr_n(u^2)$ para todo $u \in \mathbb{F}_{2^n}$, podemos restringir los exponentes i con coeficientes no ceros β_i tal que hay a lo más un exponente en cada clase ciclotomica $\left\{i \times 2^j [\bmod(2^n - 1); j \in \mathbb{N}]\right\}$ de 2 $\bmod(2^n - 1)$. Pero esto, todavía no hace única esta representación . Llamaremos esta expresión la representación absoluta de la traza de f.

Volviendo a la representación univariada. Veremos como podemos obtener de la tabla de verdad de la función y representarla en una forma conveniente usando la notación Tr_n. Denotando

por α a un elemento primitivo en el cuerpo $\mathbb{F}_{2^n}$. El polinomio Mattson– Solomon del vector $(f(1), f(\alpha), ..., f(\alpha^{2^n-2}))$ es el polinomio

$$A(x) = \sum_{j=1}^{2^n-1} A_j x^{2^n-1-j} = \sum_{j=0}^{2^n-2} A_{-j} x^j \text{ con } A_j = \sum_{k=0}^{2^n-2} f(\alpha^k)\alpha^{kj}.$$

Tenemos, para todo $0 \leq i \leq 2^n - 2$

$$A(\alpha^i) = \sum_{j=1}^{2^n-1} A_j \alpha^{-ij} = \sum_{j=1}^{2^n-1} \sum_{k=0}^{2^n-2} f(\alpha^k)\alpha^{(k-i)j} = f(\alpha^i).$$

Ya que

$$\sum_{j=1}^{2^n-1} \alpha^{(k-i)j} = \sum_{j=0}^{2^n-2} \alpha^{(k-i)j} = \frac{\alpha^{(k-i)(2^n-1)}}{\alpha^{k-i}+1}$$

es igual a cero si $1 \leq k \neq i \leq 2^n - 2$., y A es por tanto la representación univariada de f, si $f(0) = A_0 = \sum_{j=1}^{2^n-2} f(\alpha^i)$ eso es, si f tiene peso par, esto es, si su grado algebraico es exactamente menor que n.

De lo contrario, tenemos $f(x) = A(x) + 1 + x^{2^n-1}$, ya que $1 + x^{2^n-1}$ toma valor 1 en 0 y 0 en cada elemento distinto de cero de $\mathbb{F}_{2^n}$.

Note que $A_{2j} = A_j^2$, (A es un polinomio univariado). Denotando por $\Gamma(n)$ el conjunto obtenido al elegir un elemento en cada clase ciclotómica de 2 mod $2^n - 1$ (la opción más habitual para k es el elemento más pequeño en su clase ciclotómica, llamado el líder coclase de la clase), esto permite representar a $f(x)$ en la forma

$$\sum_{j \in \Gamma(n)} Tr_{n_j}(A_{-J} x^j) + \varepsilon(1 + x^{2^n-1})$$

donde $\varepsilon = wt(f)[\text{mod } 2]$ y donde n_j es el tamaño de la clase ciclotómica que contiene j. Note que, para cada $j \in \Gamma(n)$ y cada $x \in \mathbb{F}_{2^n}$ tenemos que $A_j \in \mathbb{F}_{2^{n_j}}$ (ya que $A_j^{2^{n_j}} = A_j$) y $x^j \in \mathbb{F}_{2^{n_j}}$ también. A esta expresión la llamaremos representación traza de f. Obviamente, no es más que una expresión alternativa para la representación univariada. Por esta razón, es única (si restringimos el coeficiente de x^j para vivir en $\mathbb{F}_{2^{n_j}}$).

EJEMPLO 3.2.6. En el siguiente ejemplo, obtendremos la representación por traza de una función Booleana usando su forma normal algebraica.

Al igual que en el ejemplo (2.2.1), consideremos $n = 3$ y el cuerpo $\mathbb{F}_{2^3}$, que se construye usando el polinomio irreducible $g(x) = x^3 + x + 1$ como generador. Representamos al elemento primitivo $x + 1$

con α.
Consideremos la función $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$, esta función es lineal, su representación por traza se puede encontrar como $Tr(a \cdot c)$ donde $a \in \mathbb{F}_{2^3}$. Notemos que $f(0001) = 1$, esto significa que $Tr(a \cdot 1)$ debe ser igual a 1. Ya que $Tr(\alpha^3)$ es 0 (ver tabla (2.1) del ejemplo (2.2.1)); deducimos que no puede ser $\alpha^3, \alpha^6, \alpha^5$ y 0. Ahora, usaremos el siguiente valor de f, $f(010) = 1$. Por tanto, $Tr(a \cdot \alpha^5)$ debería ser igual a 1 ya que el vector (010) corresponde a α^5. Entonces vemos que a a no puede ser igual a 1 y α ya que $Tr(\alpha^5) = Tr(\alpha^6) = 0$; así, solo hay dos posibilidades restantes, estas son $a = \alpha^2$ y $a = \alpha^4$. Vemos que $f(100) = 1$, y por tanto $Tr(a\alpha^3)$ debería ser igual a 1. Pero como $Tr(a\alpha^2 \cdot \alpha^3) = 0$, se concluye que no es igual a α^2. Por tanto, $a = \alpha^4$ y $f(x) = Tr(\alpha^4 \cdot x)$.

Es más difícil encontrar una representación por traza para una función no lineal. Por ejemplo sea $g(x_1, x_2, x_3) = x_1x_2$, ya que $\Gamma(n) = \{0, 1, 3\}$ y $x^0 = 1$ para todo $x \in \mathbb{F}_{2^3}$, entonces la representación por traza para g es de la forma $Tr(a_0) + Tr(a_1x) + Tr(a_3x^3) + 2(1 + x^7)$, para los $a_0, a_1, a_3, a_7 \in \mathbb{F}_{2^3}$ apropiados. Ya que $g(000) = 0$, a_0 se toma como cero, y $2(1 + x^7)$ también es cero. Después de algunas cálculos de a_1 y a_3, podemos encontrar una variante para la representación dada por $g(x) = Tr(\alpha^4x) + Tr(x^3)$.

3.3 La Transformada Walsh

Ahora consideraremos funciones de valor real de la forma $\varphi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$. Estas componen la $\mathbb{R}-$álgebra $\mathcal{C}_n = \mathbb{R}^{\mathbb{F}_2^n}$.

DEFINICIÓN 3.9. **La transformada de Walsh o transformada Hadamard-Walsh**.
La transformada de Walsh o transformada Hadamard-Walsh se define como:

$$\Phi : \mathcal{C}_n \longrightarrow \mathcal{C}_n, \ \varphi \longrightarrow \hat{\varphi},$$

con la formula

$$\hat{\varphi}(u) := \sum_{x \in \mathbb{F}_2^n} \varphi(x) \cdot (-1)^{u \cdot x}$$

donde $u \cdot x$ es el producto punto canónico en $\mathbb{F}_2^n$.

Claramente Φ es un mapeo $\mathbb{R}-$lineal, y $\hat{0} = 0$ para la función constante $0 \in \mathcal{C}_n$, la otra fun-

ción constante 1 transforma a $\hat{1}$ en 0:

$$\hat{1}(0) = 2^n$$
$$\hat{1}(0) = 0 \quad \text{otro}$$

LEMA 3.4. [7] Para $u \in \mathbb{F}_2^n$ tenemos :

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} = \begin{cases} 2^n, & \text{si} \quad u = 0 \\ 0, & \text{otro caso} \end{cases}$$

Demostración. Si $u = 0$ entonces, todos los exponentes son 0, todos los sumandos 1 y tenemos 2^n de ellos. Cuando $u \neq 0$, consideremos los siguientes conjuntos,$H = \{x \in \mathbb{F}_2^n | x \cdot u = 0\}$ y $\bar{H} = \{x \in \mathbb{F}_2^n | x \cdot u = 1\}$ que es el complemento de H, por tanto $\mathbb{F}_2^n = H \cup \bar{H}$ y $H \cap \bar{H} = \varnothing$, y el número de H es el mismo que $\bar{H}$ que es 2^{n-1}, luego para todo $x \in H$ la suma es positiva, y para todo $y \in \bar{H}$ la suma es negativa por tanto al sumar ambas cantidades la suma total es 0. □

DEFINICIÓN 3.10. **Espectro Walsh**
Dada una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ la función transformación $\hat{\chi_f} : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ de la forma característica χ_f es llamado el espectro Walsh de f. El cual tiene la forma

$$\hat{\chi_f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x}$$

donde es 1 si $f(x) = u \cdot x$ y -1 si $f(x) \neq u \cdot x$, entonces

$$\hat{\chi_f}(u) = \#\{x | f(x) = u \cdot x\} - \#\{x | f(x) \neq u \cdot x\}.$$

Denotaremos el primero de los conjuntos por :

$$L_f(u) := \#\{x | f(x) = u \cdot x\}$$

COROLARIO 3.1. [7] El espectro de una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es igual a

$$\hat{\chi_f}(u) = 2\,\#\,L_f(u) - 2^n$$

en particular $\chi_f(u)$ es siempre par y $-2^n \leq \hat{\chi_f}(u) \leq 2^n$.

Demostración. De (3.1) tenemos que $d(f, \bar{g}) = 2^n - d(f, g)$ despejando tenemos $d(f, g) = 2^n - d(f, \bar{g})$,

remplazando tenemos :

$$\hat{\chi_f}(u) = \#\, L_f(u) - (2^n - \#\, L_f(u)) = 2\,\#\, L_f(u) - 2^n.$$

Es claro que $\hat{\chi_f}(u)$ es múltiplo de 2 y que está acotado por 2^n. □

En general el espectro refleja la coincidencia o desviación entre una función Booleana y todas sus funciones afines.

COROLARIO 3.2. [7] Sea α una forma lineal $\alpha(x) = u \cdot x$ correspondiente a u entonces:

$$d(f, \alpha) = 2^n - \#\, L_f(u) = 2^{n-1} - \frac{1}{2}\hat{\chi_f}(u).$$

Demostración. La primera igualdad se deduce de $d(f, \bar{g}) = 2^n - d(f, g)$, despejando tenemos $d(f, g) = 2^n - d(f, \bar{g})$, en nuestro caso $\bar{g}$ es $\alpha(x) = u \cdot x$.
Veamos la segunda igualdad, del corolario (3.1) tenemos $\hat{\chi_f}(u) = 2\,\#\, L_f(u) - 2^n$, despejando tenemos: $\#\, L_f(u) = \dfrac{\hat{\chi_f}(u) + 2^n}{2}$, remplazando tenemos lo siguiente

$$\begin{aligned} d(f, \alpha) &= 2^n - \left(\frac{\chi_f(u) + 2^n}{2}\right) \\ d(f, \alpha) &= 2^n - \frac{\hat{\chi_f}(u)}{2} - \frac{2^n}{2} \\ d(f, \alpha) &= 2^{n-1} - \frac{\hat{\chi_f}(u)}{2} \end{aligned}$$

□

EJEMPLO 3.3.1. Sea f una función Booleana tal que $f(x_1, x_2) = x_1x_2$, calculemos su espectro.

$$\hat{\chi_f}(00) = (-1)^{(00)\cdot(00)+0} + (-1)^{(00)\cdot(01)+0} + (-1)^{(00)\cdot(10)+0} + (-1)^{(00)\cdot(11)+1} = 2.$$

$$\hat{\chi_f}(01) = (-1)^{(01)\cdot(00)+0} + (-1)^{(01)\cdot(01)+0} + (-1)^{(01)\cdot(10)+0} + (-1)^{(01)\cdot(11)+1} = 2.$$

$$\hat{\chi_f}(10) = (-1)^{(10)\cdot(00)+0} + (-1)^{(10)\cdot(01)+0} + (-1)^{(10)\cdot(10)+0} + (-1)^{(10)\cdot(11)+1} = 2.$$

$$\hat{\chi_f}(11) = (-1)^{(11)\cdot(00)+0} + (-1)^{(11)\cdot(01)+0} + (-1)^{(11)\cdot(10)+0} + (-1)^{(11)\cdot(11)+1} = -2.$$

Así el espectro de f es $\{2, 2, 2, -2\}$.

3.4 Formula de inversión

Aplicaremos la transformación Walsh Φ otra vez a una función ya transformada $\hat{\varphi}$:

$$\begin{aligned}\hat{\hat{\varphi}}(w) &= \sum_{u\in\mathbb{F}_2^n} \hat{\varphi}(u)\cdot(-1)^{u\cdot w} \\ &= \sum_{x\in\mathbb{F}_2^n}\sum_{u\in\mathbb{F}_2^n} \varphi(x)\cdot(-1)^{u\cdot x}\cdot(-1)^{u\cdot w} \\ &= \sum_{x\in\mathbb{F}_2^n} \varphi(x)\left[\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot(x+w)}\right]\end{aligned}$$

Donde lo que esta dentro de los corchetes es 2^n si $(x+w)=0$ o 0 en otro caso, entonces $\hat{\hat{\varphi}}(w) = 2^n\varphi(w)$. Así, hemos demostrado que

$$\Phi\circ\Phi(\varphi) = 2^n\varphi \quad \text{para todo } \varphi\in\mathcal{C}_n. \tag{3.4}$$

PROPOSICIÓN 3.4.1. [7] La transformada Walsh Φ es biyectiva y su transformación inversa está dada por

$$\Phi^{-1} = \frac{1}{2}\Phi.$$

Demostración. De la formula de inversión (3.4) se tiene que $\hat{\varphi}=0$, implica que $\varphi=0$. La sobreyectividad se tiene ya que estamos trabajando en un espacio de dimensión finita y tenemos una inyectividad sobre el, entonces Φ es biyectiva. Que la inversa tenga esa forma, se deduce de (3.4). □

COROLARIO 3.3. [7]

$$\varphi(0) = \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}\hat{\varphi}(u)$$

Demostración. La prueba se deduce de la definición de la transformada Walsh. □

COROLARIO 3.4. [7] Para toda función Booleana $f:\mathbb{F}_2^n\longrightarrow\mathbb{F}_2$ tenemos :

$$\sum_{u\in\mathbb{F}_2^n}\hat{\chi_f}(u)\begin{cases}2^n, & \text{si} \quad f(0)=0\\ -2^n, & \text{otro caso}\end{cases}$$

Demostración. La prueba es clara por la definición de $\hat{\chi_f}(u)$. □

3.5 Convolución

DEFINICIÓN 3.11. Para $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ la Convolución $\varphi * \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ está definida por :

$$\varphi * \psi(w) := \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(w - x)$$

está dada por el mapeo bilineal $* : \mathcal{C}_n \times \mathcal{C}_n \longrightarrow \mathcal{C}_n$.

Calcularemos el valor en 0 para la convolución de las formas características de dos funciones Booleanas $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$.

$$\begin{aligned} \chi_f * \chi_g(0) &= \sum_{x \in \mathbb{F}_2^n} \chi_f(x)\chi_g(x) \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} \\ &= 2^n - 2d(f, g). \end{aligned}$$

Donde la última igualdad se deduce del corolario (3.2).
Ahora, del razonamiento anterior podemos enunciar el siguiente corolario.

COROLARIO 3.5. [7] La distancia Hamming entre dos funciones Booleanas f, g en $\mathbb{F}_2^n$ es :

$$d(f, g) = 2^{n-1} - \frac{1}{2}\chi_f * \chi_g(0).$$

Otra forma de expresar este resultado es en término de la correlación

$$\begin{aligned} \kappa(f, g) &= \frac{1}{2^n} \left[\#\{x | f(x) = g(x)\} - \#\{x | f(x) \neq g(x)\} \right] \\ &= \frac{1}{2^{n-1}} \left[\#\{x | f(x) = g(x)\} \right] - 1 \end{aligned}$$

En efecto, sabemos que $d(f, \bar{g}) = 2^n - d(f, g)$, despejando tenemos $d(f, g) = 2^n - d(f, \bar{g})$. Remplazando en $\kappa(f, g)$ se tiene lo siguiente:

$$\begin{aligned}\kappa(f,g) &= \frac{1}{2^n}d(f,\bar{g}) - \left(\frac{2^n - d(f,\bar{g})}{2^n}\right)\\ &= \frac{1}{2^n}d(f,\bar{g}) - 1 + \frac{d(f,\bar{g})}{2^n}\\ &= \frac{1}{2^{n-1}}d(f,\bar{g}) - 1.\end{aligned}$$

COROLARIO 3.6. [7] La correlación de la función f y g es $\kappa(f,g) = \frac{1}{2^n}\chi_f * \chi_g(0)$.

Demostración. Sabemos $\chi_f * \chi_g(0) = 2^n - 2d(f,g)$ remplazando se tiene lo siguiente

$$\begin{aligned}\chi_f * \chi_g(0) &= 2^n - 2(2^n - d(f,\bar{g}))\\ &= 2^n - 22^n + 2d(f,\bar{g})\\ &= d(f,g) + d(f,\bar{g}) - 22^n + 2d(f,\bar{g})\\ &= d(f,g) + d(f,\bar{g}) + 2d(f,\bar{g}) - 2d(f,g) - 2d(f,\bar{g})\\ &= d(f,\bar{g}) - d(f,g)\end{aligned}$$

Multiplicando por $\frac{1}{2^n}$ en ambos lados de la igualdad anterior se obtiene el resultado deseado. □

DEFINICIÓN 3.12. La autocorrelación de una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ con respecto a el shift $x \in \mathbb{F}_2^n$ es:

$$\kappa_f := \frac{1}{2^n}\left[\#\{u \in \mathbb{F}_2^n | f(x+u) = f(x)\} - \#\{u \in \mathbb{F}_2^n | f(x+u) \neq f(x)\}\right]$$

Por tanto tenemos

$$\kappa_f(x) = \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}(-1)^{f(x+u)+f(x)} = \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}\chi_f(x+u)\chi_f(u)$$

Por tanto

LEMA 3.5. [7] La autocorrelación de f es

$$\kappa_f = \frac{1}{2^n}\chi_f * \chi_f.$$

Ahora calcularemos la transformada Walsh de una convolución.

$$\begin{aligned}
\widehat{\varphi * \psi}(u) &= \sum_{w \in \mathbb{F}_2^n} (\varphi * \psi)(w)(-1)^{u \cdot w} \\
&= \sum_{w \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(w+x)(-1)^{u \cdot w} \\
&= \sum_{x \in \mathbb{F}_2^n} \varphi(x) \left[\sum_{w \in \mathbb{F}_2^n} \psi(w+x)(-1)^{u \cdot w} \right] \\
&= \sum_{x \in \mathbb{F}_2^n} \varphi(x) \sum_{v \in \mathbb{F}_2^n} (-1)^{u \cdot (v+x)} \quad (\text{tomando } v = w + x, \text{ luego } v + x = w + x + x = w) \\
&= \sum_{x \in \mathbb{F}_2^n} \varphi(x) \left[\sum_{v \in \mathbb{F}_2^n} \psi(v)(-1)^{u \cdot v} \right] (-1)^{u \cdot x} \\
&= \left[\sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{u \cdot x} \right] \hat{\psi}(u) \\
&= \hat{\varphi}(u)\hat{\psi}(u)
\end{aligned}$$

TEOREMA 3.5. **Convolución** [7]
Para $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ se tiene lo siguiente $\widehat{\varphi * \psi}(u) = \hat{\varphi}(u)\hat{\psi}(u)$.

COROLARIO 3.7. [7] Para $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ tenemos $\widehat{\varphi\psi} = \frac{1}{2^n}\hat{\varphi} * \hat{\psi}$.

Demostración. Por el teorema de convolución (3.5) se tiene $\widehat{\varphi * \psi}(u) = \hat{\varphi}(u)\hat{\psi}(u)$.
Cambiemos la notación por: $\Phi(f * g) = \Phi(f)\Phi(g)$. Con $\hat{f}$ y $\hat{g}$ en lugar de f y g se tiene lo siguiente:

$$\Phi(\hat{f} * \hat{g}) = \Phi(\Phi(f))\Phi(\Phi(g)) = 2^n(fg) = 2^n\Phi(\Phi(fg)). \tag{3.5}$$

aplicando Φ^{-1} en ambos lados de la ecuación (3.5), se obtiene el resultado deseado. □

COROLARIO 3.8. [7] La transformación Walsh de la autocorrelación κ_f está dada por $\widehat{\kappa_f} = \frac{1}{2^n}\widehat{\chi_f}^2$.

Demostración. Por el lema (3.5) se sebe que $\kappa_f = \frac{1}{2^n}\chi_f * \chi_f$. Tomando la transformada Walsh se obtiene lo siguiente

$$\widehat{\kappa_f} = \frac{1}{2^n}\widehat{\chi_f * \chi_f} = \frac{1}{2^n}\widehat{\chi_f}\widehat{\chi_f} = \frac{1}{2^n}\widehat{\chi_f}^2$$

□

Hay dos formas de calcular el valor de un producto de una convolución en 0

(1) Por definición

$$\varphi * \psi(0) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(x),$$

(2) Aplicando el corolario (3.3) y el teorema de convolución (3.5).

$$\varphi * \psi(0) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \widehat{\varphi * \psi}(u) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\varphi}(u)\hat{\psi}(u). \tag{3.6}$$

PROPOSICIÓN 3.5.1. **Ecuación de Parseval** [7]
Para $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$

$$\sum_{u \in \mathbb{F}_2^n} \hat{\varphi}\hat{\psi}(u) = 2^n \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(x).$$

Demostración. De la igualdad (3.6) se tiene lo siguiente

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^n} \hat{\varphi}\hat{\psi}(u) &= 2^n \varphi * \psi(0) \\ &= 2^n \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(x). \end{aligned}$$

□

3.6 Funciones bent

Las funciones bent son un tipo especial de funciones Booleanas. Esto significa que toman varias entradas y da una salida (como 0 y 1, verdadero y falso). Las funciones bent se llaman así porque son lo más diferente posible a todas las funciones lineales y a todas las funciones afines; esto hace que las funciones bent sean naturalmente difíciles de aproximar. Las funciones bent han sido ampliamente estudiadas por su aplicación en la criptografía.

La ecuación de Parseval aplicada a la forma característica de una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ da el siguiente resultado:

$$\sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^2 = 2^n \sum_{x \in \mathbb{F}_2^n} \chi_f(x)^2 = 2^{2n}. \tag{3.7}$$

En efecto

$$\begin{aligned}
\sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^2 &= \sum_{u \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{2f(x)+2(u\cdot x)} \\
&= \sum_{u \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{2f(x)} (-1)^{2(u\cdot x)} \\
&= \sum_{u \in \mathbb{F}_2^n} (-1)^{2(u\cdot x)} \sum_{x \in \mathbb{F}_2^n} (-1)^{2f(x)} \\
&= 2^n \sum_{x \in \mathbb{F}_2^n} \chi_f(x)^2.
\end{aligned}$$

Por otro lado

$$\begin{aligned}
2^n \sum_{x \in \mathbb{F}_2^n} \chi_f(x)^2 &= 2^n \left[\sum_{x \in \mathbb{F}_2^n} \chi_f(x) \chi_f(x) \right] \\
&= 2^n \left[\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u\cdot v+f(x)+u\cdot v} \right] \\
&= 2^n \left[\sum_{x \in \mathbb{F}_2^n} (-1)^{2f(x)+2u\cdot v} \right] \\
&= 2^n \left[\sum_{x \in \mathbb{F}_2^n} (-1)^{2(f(x)+u\cdot v)} \right] \\
&= 2^n 2^n = 2^{2n}.
\end{aligned}$$

En la última suma de (3.7) todos los sumandos son 1. Por lo tanto, en la primera suma debe haber al menos uno de los 2^n sumandos $\hat{\chi_f}^2 \geq 2^n$.

PROPOSICIÓN 3.6.1. [7] Para toda función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ tenemos

$$\max |\hat{\chi_f}| \geq 2^{\frac{n}{2}}$$

Con la igualdad si y solo si $\hat{\chi_f}^2 = 2^n$.

Demostración. El resultado se deduce de la ecuación (3.7). □

DEFINICIÓN 3.13. **Función bent**
Una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es llamada Bent si $(\hat{\chi_f})^2 = 2^n$.

En particular el espectro $\hat{\chi_f}$ de una función bent puede solo asumir los valores $\pm 2^{\frac{n}{2}}$; estos deben ser enteros, es decir

$$\hat{\chi_f}(u) = \sum_{x \in \mathbb{F}_2^n} \hat{\chi_f}(x)(-1)^{u \cdot x} \in \mathbb{Z}.$$

El siguiente corolario es una consecuencia de la definición de una función bent.

COROLARIO 3.9. [7] Si f es una función bent entonces n debe ser par.

A continuación, ilustraremos la definición de función bent con unos ejemplos.

EJEMPLO 3.6.1. La función Booleana del ejemplo (3.3.1) es una función bent, ya que su espectro es de la forma $\pm 2^{\frac{n}{2}}$. Ahora veamos el caso de función Booleana que no sea bent.
Sea $h : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ una función Booleana tal que $h(x) = 1$ si y solo si x tiene dos coordenadas diferentes de cero.

$x_1x_2x_3$	$h(x_1x_2x_3)$
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	0

Calculemos el espectro de h.
$\hat{\chi_h}(000) = (-1)^{(000)\cdot(000)+0} + (-1)^{(000)\cdot(001)+0} + (-1)^{(000)\cdot(010)+0} + (-1)^{(000)\cdot(011)+1} + (-1)^{(000)\cdot(100)+0} + (-1)^{(000)\cdot(101)+1} + (-1)^{(000)\cdot(110)+1} + (-1)^{(000)\cdot(111)+0} = 2.$

$\hat{\chi_h}(001) = (-1)^{(001)\cdot(000)+0} + (-1)^{(001)\cdot(001)+0} + (-1)^{(001)\cdot(010)+0} + (-1)^{(001)\cdot(011)+1} + (-1)^{(001)\cdot(100)+0} + (-1)^{(001)\cdot(101)+1} + (-1)^{(001)\cdot(110)+1} + (-1)^{(001)\cdot(111)+0} = 2.$

$$\widehat{\chi_h}(010) = (-1)^{(010)\cdot(000)+0} + (-1)^{(010)\cdot(001)+0} + (-1)^{(010)\cdot(010)+0} + (-1)^{(010)\cdot(011)+1} + (-1)^{(010)\cdot(100)+0} + (-1)^{(010)\cdot(101)+1} + (-1)^{(010)\cdot(110)+1} + (-1)^{(010)\cdot(111)+0} = 2.$$

$$\widehat{\chi_h}(011) = (-1)^{(011)\cdot(000)+0} + (-1)^{(011)\cdot(001)+0} + (-1)^{(011)\cdot(010)+0} + (-1)^{(011)\cdot(011)+1} + (-1)^{(011)\cdot(100)+0} + (-1)^{(011)\cdot(101)+1} + (-1)^{(011)\cdot(110)+1} + (-1)^{(011)\cdot(111)+0} = 2.$$

$$\widehat{\chi_h}(100) = (-1)^{(100)\cdot(000)+0} + (-1)^{(100)\cdot(001)+0} + (-1)^{(100)\cdot(010)+0} + (-1)^{(100)\cdot(011)+1} + (-1)^{(100)\cdot(100)+0} + (-1)^{(100)\cdot(101)+1} + (-1)^{(100)\cdot(110)+1} + (-1)^{(100)\cdot(111)+0} = 2.$$

$$\widehat{\chi_h}(101) = (-1)^{(101)\cdot(000)+0} + (-1)^{(101)\cdot(001)+0} + (-1)^{(101)\cdot(010)+0} + (-1)^{(101)\cdot(011)+1} + (-1)^{(101)\cdot(100)+0} + (-1)^{(101)\cdot(101)+1} + (-1)^{(101)\cdot(110)+1} + (-1)^{(101)\cdot(111)+0} = 2.$$

$$\widehat{\chi_h}(110) = (-1)^{(110)\cdot(000)+0} + (-1)^{(110)\cdot(001)+0} + (-1)^{(110)\cdot(010)+0} + (-1)^{(110)\cdot(011)+1} + (-1)^{(110)\cdot(100)+0} + (-1)^{(110)\cdot(101)+1} + (-1)^{(110)\cdot(110)+1} + (-1)^{(110)\cdot(111)+0} = 2.$$

$$\widehat{\chi_h}(111) = (-1)^{(111)\cdot(000)+0} + (-1)^{(111)\cdot(001)+0} + (-1)^{(111)\cdot(010)+0} + (-1)^{(111)\cdot(011)+1} + (-1)^{(111)\cdot(100)+0} + (-1)^{(111)\cdot(101)+1} + (-1)^{(111)\cdot(110)+1} + (-1)^{(111)\cdot(111)+0} = -7.$$

El espectro de h es $\{2, 2, 2, 2, 2, 2, 2, -7\}$ luego h no es bent ya que el espectro no es de la forma $\pm 2^{\frac{n}{2}}$.

EJEMPLO 3.6.2. En general, para cualquier $n \geq 4$ par, una función Booleana $f(x) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n$ es un ejemplo clásico de una función bent, probemos que en efecto es bent, sea $x' = (x_1, x_3, \cdots, x_{n-1})$ y $x'' = (x_2, x_4, \cdots, x_n)$ vectores binarios de longitud $n/2$ con coordenadas impares y pares respectivamente. Entonces $f(x) = f(x', x'') = \langle x', x'' \rangle$ para todo x. Consideremos la trasformada Walsh de los coeficientes de f; entonces

$$\begin{aligned}
\chi_f(y) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+y\cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,y\rangle} = \sum_{x',x'' \in \mathbb{F}_2^{n/2}} (-1)^{\langle x',y'\rangle\oplus\langle x'',y''\rangle\oplus\langle x',x''\rangle} \\
&= \sum_{x'' \in \mathbb{F}_2^{n/2}} (-1)^{\langle x'',y''\rangle} \sum_{x'' \in \mathbb{F}_2^{n/2}} (-1)^{\langle x',y'\oplus x''\rangle} = \sum_{x''=y'} (-1)^{\langle x'',y''\rangle} 2^{n/2} \\
&= (-1)^{\langle y',y''\rangle} 2^{n/2}.
\end{aligned}$$

En virtud del lema (3.4), se tiene que f es una función bent.

3.7 Propiedades de las funciones bent

DEFINICIÓN 3.14. **Grado algebraico**
El grado de un mapeo Booleano f como un polinomio es

$$deg(f) = \max\{|u| : \lambda_u \neq 0\}$$

es decir, el número de variables en el item más grande de su FNA, es llamado grado (algebraico) de f.

OBSERVACIÓN 3.7.1. (1) En general el $deg(f) \leq n$.

(2) f es afín si y solo si $deg(f) \leq 1$.

PROPOSICIÓN 3.7.1. [8] El grado algebraico es un invariante afín (es un invariante bajo la acción del grupo afín general) para cada isomorfismo afín $L : x \in \mathbb{F}_2^n \longmapsto M \times x \oplus a \in \mathbb{F}_2^n$, donde M es una matriz no singular sobre $\mathbb{F}_2$, tenemos que $deg(f \circ L) = deg(f)$.

Demostración. La composición por L no puede incrementar el grado algebraico, ya que las coordenadas de $L(x)$ tienen grado 1, por tanto tenemos $deg(f \circ L) \leq deg(f)$.
Aplicando esta desigualdad a $f \circ L$ en lugar de f y a L^{-1} en lugar de L, muestra la desigualdad inversa. □

TEOREMA 3.6. [6] Para $n = 2$, el grado de una función bent en $\mathbb{V}_n$ es 2. Para $n > 2$ (n par), el grado de una función bent es a lo más $\frac{n}{2}$.

Antes de dar una prueba al teorema anterior, veamos los siguientes resultados que son necesarios para la realización de la demostración.
Realizaremos algunos cambios en la notación, estos nuevos son los que usualmente se usan en los textos.
$\mathbb{V}_n :=$ es el espacio vectorial de dimensión n sobre el campo de dos elementos $\mathbb{F}_n$.

DEFINICIÓN 3.15. El peso de Hamming de un vector $x \in \mathbb{V}_n$, denotado por $wt(x)$ es el número de unos del vector x.

TEOREMA 3.7. [6] Sea $f : \mathbb{V}_n \longrightarrow \mathbb{R}$ y $\widehat{f}$ es su transformación Walsh, si S es un subespacio arbitrario y $S^\perp$ el dual (aniquilador) de S, es decir

$$S^\perp = \{x \in \mathbb{V}_n : x \cdot s = 0 \ \forall s \in S\}.$$

Entonces

$$\sum_{u\in S}\widehat{f}(u) = 2^{\dim S}\sum_{u\in S^{\perp}} f(u).$$

Demostración.

$$\begin{aligned}\sum_{u\in S}\widehat{f}(u) &= \sum_{u\in S}\left(\sum_{v\in\mathbb{V}_n} f(v)(-1)^{u\cdot v}\right)\\ &= \sum_{v\in\mathbb{V}_n} f(v)\left(\sum_{u\in S}(-1)^{u\cdot v}\right)\\ &= 2^{\dim S}\sum_{v\in S^{\perp}} f(v).\end{aligned}$$

Donde la ultima igualdad se tiene en virtud del lema (3.4). □

COROLARIO 3.10. [6] Para cualquier función Booleana $f : \mathbb{V}_n \longrightarrow \mathbb{F}_2$ se tiene lo siguiente

$$\sum_{u\leq v}\widehat{f}(u) = 2^{wt(v)}\sum_{u\leq \overline{v}} f(u)$$

donde $u \leq v$ significa que $u_i = 1$, entonces $v_i = 1$, $1 \leq i \leq n$.

Demostración. La prueba se tiene como una consecuencia directa del teorema anterior (3.7). □

DEFINICIÓN 3.16. Para una función bent f, definamos una función Booleana $\widetilde{f}$ tal que

$$\frac{\widehat{\chi_f}(u)}{2^{\frac{n}{2}}} = (-1)^{\widetilde{f}(u)} = \chi_{\widetilde{f}}(u).$$

Llamaremos a esa función el dual de f. Para un a función Booleana tenemos que $\chi_f(u) = (-1)^{f(u)} = 1 - 2f(u)$, donde la segunda igualdad se cumple si consideramos las funciones como funciones reales. Del teorema (3.7), sabemos que para un subespacio arbitrario S de $\mathbb{V}_n$ tenemos; usando χ_f en lugar de f

$$\sum_{u\in S}\widehat{\chi_f}(u) = 2^{\dim S}\sum_{u\in S^{\perp}}\chi_f(u)$$

Tomando S como el conjunto de todos los vectores u incluidos en v, es decir $u \leq v$, la ecuación

anterior se transforma en (en virtud del corolario (3.10)) :

$$\sum_{u\leq v}\widehat{\chi_f}(u)=2^{wt(v)}\sum_{u\leq \overline{v}}\chi_f(u)$$

Además , si f es bent y teniendo en cuenta la definición del dual $\widetilde{f}$

$$\widehat{\chi_f}(u)=2^{\frac{n}{2}}\chi_{\widetilde{f}}(u)=2^{\frac{n}{2}}(1-\widetilde{f}(u))$$

luego, obtenemos

$$2^{wt(v)}-2\sum_{u\leq v}f(u)=2^{-wt(v)}\sum_{u\leq \overline{v}}(2^{\frac{n}{2}}-2^{\frac{n}{2}+1})\widetilde{f}(u).$$

Ahora enunciemos el razonamiento descrito anteriormente como un lema

LEMA 3.6. [6] Si f es una función bent en $\mathbb{V}_n$, entonces con respecto a f como una función real tenemos

$$\sum_{u\leq v}f(u)=2^{wt(v)-1}-2^{\frac{n}{2}-1}+2^{wt(v)-\frac{n}{2}}\sum_{u\leq \overline{v}}\widetilde{f}(u). \tag{3.8}$$

TEOREMA 3.8. [9] Cualquier función Booleana f puede expandirse en potencias de v_i como

$$f(v_1,\cdots,v_n)=\sum_{u\in\mathbb{V}_n}g(a)v_1^{a_1}\cdots v_n^{a_n}. \tag{3.9}$$

donde los coeficientes están dados por

$$g(a)=\sum_{b\subset a}f(b_1\cdots b_n) \tag{3.10}$$

y $b\subset a$ significa que unos en b son un subconjunto de unos en a.

Demostración. Para $n=1$, la forma normal disyuntiva para f es

$$f(v_1)=f(0)(1+v_1)+f(1)v_1=f(0)1+(f(0)+f(1))v_1$$

lo que prueba (3.9) y (3.10) .

Similarmente para $n = 2$ tenemos

$$\begin{aligned} f(v_1, v_2) &= f(0,0)(1+v_1)(1+v_2) + f(0,1)(1+v_1)v_2 + f(1,0)v_1(1+v_2) + f(1,1)v_1v_2 \\ &= f(0,1)1 + \{f(0,0) + f(1,0)\}v_1 + \{f(0,0) + f(0,1)\}v_2 + \\ &\{f(0,0) + f(0,1) + f(1,0) + f(1,1)\}v_1v_1 \end{aligned}$$

lo que nuevamente prueba (3.9) y (3.10) , continuando de esta manera se tiene el resultado. □

Ahora procedamos a realizar la prueba del teorema (3.6).

NOTA 2. La forma normal disyuntiva (DNF) es la normalización de una fórmula lógica en matemáticas booleanas. En otras palabras, se dice que una fórmula lógica está en forma normal disyuntiva si es una disyunción de conjunciones con cada variable y su negación está presente una vez en cada conjunción.

TEOREMA 3.9. [6] Para $n = 2$, el grado de una función bent en $\mathbb{V}_n$ es 2. Para $n > 2$ (n par), el grado de una función bent es a lo más $\frac{n}{2}$.

Demostración. La primera parte es clara. Ahora, sea f una función bent y $n > 2$, por el teorema (3.8) se tiene

$$f(x) = \sum_{u \in \mathbb{V}_n} g(v) x_1^{v_1} \cdots x_n^{v_n}$$

donde los coeficientes están dados por

$$g(v) = \sum_{u \in \mathbb{V}_n} f(u)$$

así, el monomio $x_1^{v_1} \cdots x_n^{v_n}$ está presente en $f(x)$ si y solo si $g(v)$ es impar. Pero si $wt(v) > \frac{n}{2}$ y $n > 2$, entonces la última suma en la ecuación (3.8) también es par y $g(v)$ es cero en $\mathbb{F}_2$. Por tanto f tiene grado a lo sumo $\frac{n}{2}$. □

3.8 Aproximación por relaciones lineales

En esta sección estudiaremos a la linealidad oculta de un mapeo Booleano, mirando para combinaciones lineales de los bits de salida que dependen linealmente de una combinación lineal de los bits de entrada al menos para algunos argumentos.

3.8.0.1 Transformación de funciones indicadoras

DEFINICIÓN 3.17. **Función indicador**
Para $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ la función $\vartheta : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$,

$$\vartheta(x, y) := = \begin{cases} 1, & \text{si } y = f(x) \\ 0, & \text{otro caso} \end{cases}$$

Es llamada la función indicador de f.

Calcularemos la transformada Walsh de una función indicador; encontraremos el conjunto

$$L_f(u, v) := \{x \in \mathbb{F}_2^n | u \cdot x = v \cdot f(x)\}.$$

Donde la función $v \cdot f$ coincide con la forma lineal correspondiente a u. El más grande $L_f(u, v)$, el más cercano es la aproximación lineal de f por (u, v).

$$\begin{aligned} \widehat{\vartheta}(x, y) &= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^q} \vartheta(x, y)(-1)^{u \cdot x + v \cdot y} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot f(x)} \\ &= \#\ L_f(u, v) - \#\ \{x \in \mathbb{F}_2^n | u \cdot x \neq v \cdot f(x)\} \\ &= \#\ L_f(u, v) - (2^n - \#\ L_f(u, v)). \end{aligned}$$

Del razonamiento anterior, podemos enunciar el siguiente teorema.

TEOREMA 3.10. [7] Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ la transformación de la función indicador es:

$$\widehat{\vartheta}(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot f(x)} = 2\#\ L_f(u, v) - 2^n.$$

En particular $-2^n \leq \widehat{\vartheta} \leq 2^n$, y todos los valores de $\widehat{\vartheta}$ son par.

COROLARIO 3.11. [7] Sea $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ la forma lineal correspondiente a v. Entonces

$$\widehat{\vartheta}(u, v) = \widehat{\chi}_{\beta \circ f}(u).$$

Demostración. La prueba es clara, se deduce de la definición de $\widehat{\chi}_{\beta \circ f}(u)$. □

DEFINICIÓN 3.18. **Espectro (Walsh)** Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ la función transformada $\widehat{\vartheta}_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$ de la función indicador ϑ_f es llamada el espectro (Walsh) de f.

Imagine el espectro $\widehat{\vartheta}_f$ de f como una matriz de $2^n \times 2^q$ cuyas filas están indexadas por $u \in \mathbb{F}_2^n$ y las columnas por $v \in \mathbb{F}_2^q$ en el orden canónico. Por el corolario (3.11) las columnas son solo es espectro de las funciones Booleanas $\beta \circ f$ para todas las formas lineales $\beta \in \mathcal{L}_q$.

COROLARIO 3.12. **Suma de columnas del espectro** [7]
Sea $v \in \mathbb{F}_2^q$ entonces

$$\sum_{u \in \mathbb{F}_2^q} \widehat{\vartheta}_f(u, v) = \begin{cases} 2^n, & \text{si } v \cdot f(0) = 0 \\ -2^n, & \text{otro caso} \end{cases}$$

$$\sum_{u \in \mathbb{F}_2^q} \widehat{\vartheta}_f(u, v)^2 = 2^{2n}.$$

Demostración. Tenemos

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^q} \widehat{\vartheta}_f(u, v) &= \sum_{u \in \mathbb{F}_2^n} \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot f(x)} \\ &= \sum_{u \in \mathbb{F}_2^n} \widehat{\chi}_f(u) \end{aligned}$$

Por corolario (3.4) sabemos que la última igualdad es 2^n si $f(0) = 0$ y -2^n en otro caso.
Para la segunda igualdad usaremos el corolario (3.12) y la ecuación de Parseval (proposición 3.5.1)

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^n} \widehat{\vartheta}_f(u, v)^2 &= \sum_{x \in \mathbb{F}_2^n} \widehat{\chi}_{\beta \circ f}(u)^2 = 2^n \sum_{x \in \mathbb{F}_2^n} \widehat{\chi}_{\beta \circ f}(x)^2 \\ &= 2^{2n}. \end{aligned}$$

□

OBSERVACIÓN 3.8.1. Sabemos que para toda función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ tenemos que $\max|\widehat{\chi}_f| \geq 2^{\frac{n}{2}}$ donde la igualdad se da si y solo si $\widehat{\chi}_f^2 = 2^n$ es constante, luego $\max|\widehat{\vartheta}_f(u, v)| = \max|\widehat{\chi}_{\beta \circ f}| \geq 2^{\frac{n}{2}}$ para todo vector $v \in \mathbb{F}_2^q$ donde la igualdad se da si y solo si $\beta \circ f$ es Bent.

De lo anterior, enunciamos el siguiente corolario.

COROLARIO 3.13. [7] Sea $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ un mapeo Booleano, entonces $\max|\hat{\vartheta}_f| \geq 2^{\frac{n}{2}}$ la igualdad se da si y solo si $\beta \circ f$ es bent para cada $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ con $\beta \neq 0$.

Ahora, tenemos otra forma de definir las funciones bent, dada en la siguiente definición.

DEFINICIÓN 3.19. Un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ es llamado bent si para toda forma lineal $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$ la función $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es bent.

OBSERVACIÓN 3.8.2. (1) Ya que $L_f(0,0) = \mathbb{F}_2^n$ tenemos que $\hat{\vartheta}_f(0,0) = 2^n$.

(2) Si $u \neq 0$, tenemos

$$\hat{\vartheta}_f(u,0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x}$$

luego por lema (3.4) tenemos

$$\hat{\vartheta}_f(u,0) = 0$$

Por tanto tenemos la primera columna del espectro (columna 0) es $(2^n, 0, ..., 0)^t$.

(3) Por el teorema (3.10) y los corolarios anteriores, un mapeo Booleano es bent si y solo si $\hat{\vartheta}_f(u,v) = \pm 2^{\frac{n}{2}}$ para todo $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^q - \{0\}$, y esto es, que el espectro toma valores solamente $\pm 2^{\frac{n}{2}}$ (excepto en la columna 0).

(4) Si un mapeo bent $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ existe entonces n es par, lo anterior se tiene como consecuencia de la proposición (3.6.1) junto con el corolario (3.9).

Sea $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ afín, $f(x) = Ax + b$ donde $A \in M_{n,q}(\mathbb{F}_2)$ y $b \in \mathbb{F}_2^q$ entonces

$$\begin{aligned} L_f(u,v) &= \{x \in \mathbb{F}_2^n | u^t x = v^t A x + v^t b\} \\ &= \{x \in \mathbb{F}_2^n | (u^t - v^t)x = v^t b\} \end{aligned}$$

Esto es, el kernel de la forma lineal $u^t - v^t A$, si $v^t b = 0$, esto es un hiperplano paralelo, si $v^t b = 1$. Nosotros, distinguiremos los siguientes casos:

$$\#\, L_f(u,v) = \begin{cases} 2^n, & si \quad v^t A = u^t \quad y \quad v^t b = 0 \\ 0, & v^t A = u^t \quad y \quad v^t b = 1 \\ 2^{n-1}, & si \quad v^t A \neq u^t \end{cases}$$

Por tanto

$$\hat{\vartheta}_f(u,v) = 2\,\#\, L_f(u,v) - 2^n = \begin{cases} 2^n, & si \quad v^t A = u^t \quad y \quad v^t b = 0 \\ -2^n, & v^t A = u^t \quad y \quad v^t b = 1 \\ 0, & si \quad v^t A \neq u^t \end{cases}$$

Por lo tanto, el espectro contiene exactamente una entrada $\pm 2^n$ en cada columna (para ν constante), y solo ceros en las otras.

3.9 Mapeos Balanceados y la Preimagen contadora

Anteriormente conocimos la primera columna del espectro, ahora estudiaremos la primera fila; para eso, estudiaremos la preimagen contadora.

$$\begin{aligned} v_f(y) := \#\ f^{-1}(y) &= \#\{x \in \mathbb{F}_2^n | f(x) = y\} \\ &= \sum_{x \in \mathbb{F}_2^n} \vartheta_f(x, y) \end{aligned}$$

tenemos

$$\begin{aligned} \hat{\vartheta}_f(0, \nu) &= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^q} \vartheta_f(x, y)(-1)^{\nu \cdot y} \\ &= \sum_{y \in \mathbb{F}_2^q} v_f(y)(-1)^{\nu \cdot y} \\ &= \hat{v}_f(y) \end{aligned}$$

Sumando en ambos lados tenemos

$$\sum_{\nu \in \mathbb{F}_2^q} \hat{\vartheta}_f(0, \nu) = \sum_{\nu \in \mathbb{F}_2^q} \hat{v}_f(y) = 2^q v_f(0).$$

Note que $v_f(0)$ es el número de ceros de f. De lo anterior, podemos enunciar el siguiente lema.

LEMA 3.7. [7] Si $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ un mapeo Booleano, entonces

$$\begin{aligned} \hat{\vartheta}_f(0, \nu) &= \hat{v}_f(\nu) \\ \sum_{\nu \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0, \nu) &= 2^q v_f(0) - 2^n. \end{aligned}$$

Demostración. Teniendo en cuenta la definición de la transformada Walsh y el ítem (1) de la obser-

vación (3.8.2) se tiene lo siguiente:

$$\begin{aligned}\sum_{v\in\mathbb{F}_2^q-\{0\}}\hat{\vartheta}_f(0,v) &= \sum_{v\in\mathbb{F}_2^q}\hat{\vartheta}_f(0,v)-\hat{\vartheta}_f(0,0)\\ &= \sum_{v\in\mathbb{F}_2^q}\sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot f(x)}-2^n\\ &= \sum_{x\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q}(-1)^{b\cdot f(x)}-2^n = 2^q v_f(0)-2^n.\end{aligned}$$

□

Para la criptología, una de las propiedades más importantes de las funciones Booleanas, es el ser balanceada o equilibrada (que sin embargo no tiene nada que ver con la no linealidad). los mapeos que no son balanceados dan una distribución no uniforme de su salida y facilitan ataques estadísticos.

DEFINICIÓN 3.20. **Fibra**
La fibra del elemento y bajo f es el conjunto de elementos en el dominio de f que están mapeados a y.

DEFINICIÓN 3.21. **Mapeo balanceado o equilibrado**
Un mapeo $f:\mathbb{F}_2^n\longrightarrow\mathbb{F}_2^q$ es llamado balanceado (o equilibrado) si todos sus fibras para $y\in\mathbb{F}_2^q$ tienen el mismo tamaño.

OBSERVACIÓN 3.9.1. (1) f es balanceada si y solo si la preimagen contadora es constante.

(2) si f es balanceado entonces f es sobreyectiva, en particular $n\geq q$, y el valor constante de la preimagen contadora es $v_f=2^{n-q}$; si $n=q$ entonces los mapeos biyectivos son balanceados.

(3) f es balanceada si y solo si $v_f(0)=2^n$ y $v_f(v)=0$, para $v\neq 0$ por el lema (3.7) esto ocurre si y solo si

$$\hat{\vartheta}_f(0,v)=\begin{cases}2^n, \text{ para } v=0\\ 0 \text{ otro caso}\end{cases}$$

De esta manera el ser balanceado esta sujeto a la primera fila del espectro.

(4) Una función $f:\mathbb{F}_2^n\longrightarrow\mathbb{F}_2$ es balanceada si toma valores de 0 y 1 cada exactamente 2^{n-1} veces, en otras palabras, si su tabla de verdad contiene exactamente 2^{n-1} ceros o $d(f,0)=2^{n-1}$, por el corolario (3.2), se tiene $d(f,\alpha)=2^{n-1}-\frac{1}{2}\hat{\chi}_f(u)$, luego f es balanceada si y solo si $\hat{\chi}_f(0)=0$.

(5) Como el número total de preimágenes es 2^n, tenemos

$$\sum_{y \in \mathbb{F}_2^q} v_f(y) = 2^n.$$

TEOREMA 3.11. [7] Un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ es balanceado si y solo si para cada forma lineal $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2, \beta \neq 0$ la forma lineal $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es balanceado.

Demostración. Si f es balanceada, entonces cada función componente $f_1, ..., f_q : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es balanceada. Una forma lineal $\beta \neq 0$ se puede transformar a la primera función de coordenadas por un automorfismo lineal de $\mathbb{F}_2^q$; por tanto $\beta \circ f$ es también balanceada.
Para el regreso necesitamos mostrar que la preimagen contadora es constante, $v_f(0) = 2^{n-q}$. Por el corolario (3.13) tenemos

$$\begin{aligned} \hat{\vartheta}_f(u, v) &= \hat{\chi}_{\beta \circ f}(u), \quad \text{entonces} \\ \hat{\vartheta}_f(0, v) &= \hat{\chi}_{\ v \cdot f}(0) = 0, \quad \forall \quad v \in \mathbb{F}_2^q - \{0\} \end{aligned}$$

más aun $\hat{\vartheta}_f(0, 0) = 2^n$,teniendo en cuenta la observación (3) se tiene el resultado. □

Se puede expresar lo balanceado de una función Booleana por el cuadrado de convolución de la preimagen contadora.

PROPOSICIÓN 3.9.1. [7] Si $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ un mapeo Booleano, las siguientes afirmaciones son equivalentes:

(1) f es balanceada.

(2) $v_f * v_f = 2^{2n-q}$ constante.

(3) $v_f * v_f(0) = 2^{2n-q}$.

Demostración. (1) (1) $\Rightarrow$ (2)

$$v_f * v_f(v) = \sum_{y \in \mathbb{F}_2^q} v_f(y) v_f(v + y)$$

$$= 2^q 2^{n-q} 2^{n-q} = 2^{2n-q}.$$

(2) (2) $\Rightarrow$ (3) Es un caso particular.

(3) (3) $\Rightarrow$ (1) tenemos

$$2^{2n-q}v_f * v_f(0) = \sum_{y\in\mathbb{F}_2^q} v_f(y)^2.$$

Por la desigualdad de Cauchy tenemos

$$2^{2n} = \left[\sum_{y\in\mathbb{F}_2^q} 1v_f(y)^2\right] \leq \sum_{y\in\mathbb{F}_2^q} 1 \quad \sum_{y\in\mathbb{F}_2^q} v_f(y)^2 = 2^q 2^{2n-q}.$$

□

3.10 La no Linealidad de un Mapeo Booleano

DEFINICIÓN 3.22. **No linealidad de un mapeo Booleano**
La no linealidad de f es el mínimo número de entradas en la tabla de verdad que deben cambiarse para convertir a f en una función afín.
De manera formal, la no linealidad de una función Booleana $f \in \mathcal{F}_n$ es la distancia de Hamming

$$\sigma_f := d(f, \mathcal{A}_n)$$

entre f y el subespacio de las funciones afines.
Otra forma de definir la no linealidad siguiente:
Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ la no linealidad es

$$\sigma_f := \min\left\{\sigma_{\beta\circ f} | \beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2, \quad \text{afín } \beta \neq 0\right\}.$$

EJEMPLO 3.10.1. Entre funciones de 3 variables, la función $f(x) = x_1x_2x_3$, que no es afín, tiene no linealidad 1, ya que la conversión del único 1 en su tabla de verdad a 0 crea la función constante 0, que es una función afín.

TEOREMA 3.12. [7]La no linealidad de una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es:

$$\sigma_f = 2^{n-1} - \frac{1}{2}\text{máx}|\hat{\chi}_f|.$$

Demostración. Sea α una forma lineal, y $\tilde{\alpha}$ la función afín correspondiente a $u \in \mathbb{F}_2^n$, por el corolario

(3.2) se tiene lo siguiente:

$$\begin{aligned} d(f,\alpha) &= 2^{n-1} - \frac{1}{2}\hat{\chi_f}(u) \\ d(f,\bar{\alpha}) &= 2^n - 2^{n-1} + \frac{1}{2}\hat{\chi_f}(u) = 2^{n-1} + \frac{1}{2}\hat{\chi_f}(u) \\ d(f,\{\alpha,\bar{\alpha}\}) &= 2^{n-1} - |\frac{1}{2}\hat{\chi_f}(u)|. \end{aligned}$$

□

OBSERVACIÓN 3.10.1. (1) Si w' es un valor tal que

$$|\hat{\chi}_f(w')| = \text{máx}_w|\hat{\chi}_f(w)|,$$

entonces si $\hat{\chi}_f(w') > 0$, tenemos $d(f(x),\langle w,x\rangle) = \min_{a(x)\in\mathcal{L}_n} d(f,a)$ y por tanto $\ell(x) = \langle w,x\rangle$ es la mejor aproximación lineal (BLA). Donde $a(x) = a_0 + \ell(x)$ es una función afín.

(2) Claramente $\sigma_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ se deduce del teorema (3.12) y del hecho que $\text{máx}|\hat{\chi_f}| \geq 2^{\frac{n}{2}}$ luego

$$\begin{aligned} \sigma_f &= 2^{n-1} - \frac{1}{2}\text{máx}|\hat{\chi}_f| \\ \sigma_f &\leq 2^{n-1} - \frac{1}{2}2^{\frac{n}{2}} \\ \sigma_f &\leq 2^{n-1} - 2^{\frac{n}{2}-1}. \end{aligned}$$

Una función Booleana f en n variables es llamada no lineal maximal, si el parámetro σ_f toma su máximo valor posible.

Las funciones bent tienen la propiedad, de que están a una distancia máxima de todas las funciones afines. De esto, se tiene el siguiente corolario.

COROLARIO 3.14. [7] Si f es una función Bent y α una función afín, entonces $d(f,\alpha) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.

Demostración. Es claro que si f es bent entonces $\hat{\chi_f}(u) = 2^{\frac{n}{2}}$. □

EJEMPLO 3.10.2. Sea $f(x) = x_1x_2 \oplus x_3x_4$ es una función bent en 4 variables. Está a una distancia 6 de 16 de las 32 funciones afines en 4 variables y a una distancia de 10 de las otras funciones afines. Es decir, se deben cambiar al menos 6 entradas de la tabla de verdad para convertirla en una función afín. ya que no hay funciones de 4 variables cuya distancia mínima a una función afín es 7 o mayor, se sigue que f es bent.

COROLARIO 3.15. [7] Si f es bent, entonces f tiene $2^{n-1} \pm 2^{\frac{n}{2}-1}$ ceros; en particular f es no balanceada.

Demostración. $d(f,0) = 2^{n-1} \pm 2^{\frac{n}{2}-1} \neq 2^{n-1}$; entonces f es no balanceada. □

3.11 Aproximación por estructuras lineales

Mapeo diferencial

DEFINICIÓN 3.23. Sea $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ un mapeo Booleano, y $u \in \mathbb{F}_2^n$, entonces el mapeo diferencial está definido por:

$$\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$$
$$\Delta_u f(x) := f(x+u) - f(x) \text{ para todo } x \in \mathbb{F}_2^n.$$

LEMA 3.8. [7] Sean $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ y $u \in \mathbb{F}_2^n$ entonces

(1) $\Delta_u(f+g) = \Delta_u f + \Delta_u g$.

(2) $Deg\Delta_u f \leq Deg f - 1$.

Demostración. (1) $\Delta_u(f+g) = (f+g)(x+u)-(f+g)(x) = f(x+u)+g(x+u)-f(x)-g(x) = \Delta_u f+\Delta_u g$.

(2) Asumimos sin perdida de generalidad que , $q = 1$, $f = T^I$ es un monomio y $f = T_1 ... T_r$ entonces $Deg\Delta_u f(x) = (x_1+u_1)...(x_1+u_r) - x_1...u_r$; es claro que el grado es menor o igual a $r-1$.

□

Los siguientes corolarios, su demostración se deduce de la definición de mapeo diferencial.

COROLARIO 3.16. [7] Si f es contante entonces $\Delta_u f = 0$ para todo $u \in \mathbb{F}_2^n$.

COROLARIO 3.17. [7] Si f es afín entonces $\Delta_u f$ es constante para todo $u \in \mathbb{F}_2^n$.

DEFINICIÓN 3.24. **Estructura lineal**
Un vector $u \in \mathbb{F}_2^n$ es llamado estructura lineal de $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ si $\Delta_u f$ es constante.

OBSERVACIÓN 3.11.1. (1) $\Delta_{u+v} f(x) = f(x+u+v) - f(x) = f(x+u+v) - f(x+v) + f(x+v) - f(x) = \Delta_u f(x+v) + \Delta_v f(x)$.

(2) Si f es afín, entonces todo vector es una estructura lineal de f.

(3) El 0 siempre es una estructura lineal de f.

(4) Si u y v son estructuras lineales , entonces también lo es $u+v$ (por (1)) por tanto , las estructuras lineales de f forman un subespacio vectorial de $\mathbb{F}_2^n$. En este subespacio f es afín. Concluimos que el reciproco de la observación (2) es verdadero.

(5) Si $g : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ es lineal, entonces $\Delta_u(g \circ f) = g \circ \Delta_u f$.
En efecto, ya que $\Delta_u(g \circ f)(x) = (g \circ f)(x+u) - (g \circ f)(x) = g(f(x+u)) - g(f(x)) = g \circ \Delta_u f$.

DEFINICIÓN 3.25. **Radical**
Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ el espacio vectorial de sus estructuras lineales es llamado el Radical $Radf$,y su dimensión, dimensión de linealidad de f, y su codimensión, rango de f, $Rankf$.

3.12 Perfil Diferencial

Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, $u \in \mathbb{F}_2^n$ y $v \in \mathbb{F}_2^q$ sea

$$D_f(u,v) := \{x \in \mathbb{F}_2^n | \Delta_u f(x) = v\}$$
$$\delta_f(u,v) := \frac{1}{2^n} \#D_f(u,v)$$

DEFINICIÓN 3.26. **Perfil diferencial**
La función $\delta_f : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{R}$ es llamado el perfil diferencial de f.

OBSERVACIÓN 3.12.1. (1) Si f es afín , $f(x) = Ax + b$, entonces $\Delta_u f(x) = Au$. Es claro, se deduce de la definición de mapeo diferencial, por tanto

$$D_f(u,v) = \{x \in \mathbb{F}_2^n | Au = v\} = \begin{cases} \mathbb{F}_2^n, \text{ si } \quad Au = v \\ \varnothing, \text{ en otro caso} \end{cases}$$
$$\delta_f(u,v) = \begin{cases} 1, \text{ si } \quad Au = v \\ 0, \text{ en otro caso} \end{cases}$$

La primera igualdad se tiene ya que si f es afín entonces su mapeo diferencial es contante.
Cada fila del perfil diferencial contiene exactamente un 1, y 0 en el resto.

(2) Las siguientes afirmaciones son equivalentes:

u es una estructura lineal de f si y solo si

$$D_f(u,v) = \begin{cases} \mathbb{F}_2^n, & \text{para un } v \\ \varnothing, & \text{en otro caso} \end{cases}$$

si y solo si

$$\delta_f(u,v) = \begin{cases} 1, & para\ un\ v \\ 0, & \text{en otro caso} \end{cases}$$

La fila u del perfil diferencial es 0 excepto exactamente en la 1 entrada.

(3) Para una f arbitraria, y $u = 0$, tenemos

$$\delta_f(0,v) = \begin{cases} 1, & \text{si } v = 0 \\ 0, & \text{otro caso} \end{cases}$$

Lo anterior es claro, solo remplazar en la definición de perfil diferencial.
(fila 0 del perfil diferencial).

(4)

$$\sum_{v \in \mathbb{F}_2^q} \delta_f(u,v) = 1$$

(Suma de las filas del perfil diferencial).
En particular para cada vector $u \in \mathbb{F}_2^n$ hay $v \in \mathbb{F}_2^q$ tal que $\delta_f(u,v) \geq \frac{1}{2^q}$.

De las observaciones anteriores, se deduce la siguiente proposición.

PROPOSICIÓN 3.12.1. [7] Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ los siguientes enunciados son equivalentes :

(1) f es afín.

(2) Cada vector $u \in \mathbb{F}_2^n$ es una estructura lineal de f.

(3) Cada fila del perfil diferencial contiene exactamente una entrada diferente de 0.

OBSERVACIÓN 3.12.2. (5) Si $x \in D_f(u,v)$ si y solo si $x + u \in D_f(u,v)$.
Sabemos que si $x \in D_f(u,v)$ entonces se cumple que $f(x+u) - f(x) = v$ que es lo mismo que $f(x) - f(x+u) = -v$, por otro lado consideremos $x+u$; por definición tenemos $f(x+u+u) - f(x+u) = f(x) - f(x+u) = -v$ que es igual a $f(x+u) - f(x) = v$.

Ahora, supongamos que $x \notin D_f(u,v)$, luego $f(x+u)-f(x) \neq v$. Suponemos que $f(x+u)-f(x) = k$,con $k \neq v$, tenemos que $f(x+u)-f(x) = k$ que es igual a $-(f(x+u+u)-f(x+u)) = k$ así , $-v = k$ lo cual es absurdo ya que si $-v = k$ entonces $v+k = 0$ ya que el cuerpo tiene característica 2 .

(6) Todos los valores del $\#\, D_f(u,v)$ son par: Para $u = 0$ se sigue de la observación (3). Los otros casos se siguen de la observación (5) (ya que estarían en parejas x y $x+u$). Por tanto todos los $\delta_f(u,v)$ son enteros múltiplos de $\frac{1}{2^{n-1}}$.

(7) En el caso $q = 1$, la autocorrelación se pueden expresar como:

$$\kappa_f(x) = \delta_f(x,0) - \delta_f(x,1).$$

Lo cual es claro, ya que

$$\delta_f(x,0) = \frac{1}{2^n}\,\#\{u \in \mathbb{F}_2^n | f(x+u)-f(x) = 0\}$$
$$\delta_f(x,1) = \frac{1}{2^n}\,\#\{u \in \mathbb{F}_2^n | f(x+u)-f(x) = 1\}$$

Tomando factor común $\frac{1}{2^n}$ y restando tenemos la definición de $\kappa_f(x)$.

3.13 Calculo eficiente del perfil diferencial

LEMA 3.9. [7] Para todo mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, se tiene

$$\delta_f = \frac{1}{2^n}\vartheta_f * \vartheta_f.$$

Demostración.

$$\begin{aligned}\vartheta_f * \vartheta_f(u,v) &= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)\vartheta_f(x+u,y+v)\\ &= \sum_{x\in\mathbb{F}_2^n} \vartheta_f(x+u,f(x)+v)\\ &= \#\{x \in \mathbb{F}_2^n | f(x+u) = f(x)+v\}\end{aligned}$$

Entonces, $\vartheta_f * \vartheta_f(u,v) = \#\{x \in \mathbb{F}_2^n | f(x+u) - f(x) = v\} = \#D_f(u,v)$ multiplicando lo anterior por $\frac{1}{2^n}$:

$$\frac{1}{2^n}\vartheta_f * \vartheta_f(u,v) = \frac{1}{2^n} \# D_f(u,v) = \delta_f.$$

□

Por el teorema de convolución (3.5), se tiene:

$$\widehat{\delta_f} = \frac{1}{2^n}\widehat{\vartheta_f}^2 = 2^n\lambda_f.$$

Se sabe que:

$$\begin{aligned}
&\delta_f = \frac{1}{2^n}\vartheta_f * \vartheta_f; \text{ luego} \\
&\widehat{\delta_f} = \frac{1}{2^n}\widehat{\vartheta_f * \vartheta_f} = \frac{1}{2^n}\widehat{\vartheta_f}\,\widehat{\vartheta_f} = \frac{1}{2^n}\widehat{\vartheta_f}^2.
\end{aligned}$$

Por otro lado sabemos :

$$\lambda_f(u,v) = \frac{1}{2^{2n}}\,\widehat{\vartheta_f}(u,v)^2 = \frac{1}{2^n 2^n}\widehat{\vartheta_f}(u,v)^2.$$

Despejando se tiene lo siguiente

$$2^n\lambda_f(u,v) = \frac{1}{2^n}\widehat{\vartheta_f}(u,v)^2 = \widehat{\delta_f}. \tag{3.11}$$

Con base al razonamiento anterior, enunciamos el siguiente teorema.

TEOREMA 3.13. [7] El perfil diferencial, es un factor constante del la transformada Walsh del perfil lineal

(1) $\lambda_f = \frac{1}{2^n}\widehat{\delta_f}$.

(2) $\delta_f = \frac{1}{2^q}\widehat{\lambda_f}$.

Demostración. (1) Para la prueba de (1) solo basta con despejar en la ecuación (3.11).

(2) Se sabe que $\frac{1}{2^{2n}}\widehat{\vartheta_f}\,\widehat{\vartheta_f} = \frac{1}{2^{2n}}\widehat{\vartheta_f * \vartheta_f}$.

Luego

$$\begin{aligned}\widehat{\lambda_f} &= \frac{1}{2^{2n}}\widehat{\widehat{\vartheta_f * \vartheta_f}} = \frac{2^n 2^q}{2^{2n}}\vartheta_f * \vartheta_f \\ &= 2^q \frac{1}{2^n}\vartheta_f * \vartheta_f \\ &= 2^q \delta_f.\end{aligned}$$

Las igualdades anteriores son posibles debido a la ecuación de Parseval (3.5.1).

□

COROLARIO 3.18. [7] Para todo mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ se tiene

$$2^n \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q} \lambda_f(u,v)^2 = 2^q \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \delta_f(x,y)^2.$$

Demostración. Por la ecuación de Parseval (3.5.1) tenemos lo siguiente

$$\begin{aligned}2^n \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q} \lambda_f(u,v)^2 &= 2^n \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q} \left(\frac{1}{2^n}\widehat{\delta_f}(u,v)\right)^2 \\ &= 2^n \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q} \left(\frac{1}{2^{2n}}\widehat{\delta_f}(u,v)^2\right) \\ &= 2^n 2^n 2^q \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \left(\frac{1}{2^{2n}}\delta_f(u,v)\right) \\ &= 2^q \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \delta_f(u,v).\end{aligned}$$

□

3.14 Potencial diferencial

DEFINICIÓN 3.27. **Potencial diferencial**
Para un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$

$$\Omega_f := \max\{\delta_f(u,v) | u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q, (u,v) \neq 0\}.$$

Es llamado el potencial diferencial de f.

OBSERVACIÓN 3.14.1. (1) por la observación (4) en (3.12.1) tenemos

$$\frac{1}{2^q} \leq \Omega_f \leq 1.$$

(2) Ω_f está acotado inferiormente por 2^{-q} si y solo si $\delta_f(u,v) = 2^{-q}$ para $u \neq 0$; esto es, todos los mapeos diferenciales $\triangle_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ son balanceados (toda fila u del perfil diferencial es constante).

(3) Para $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ todos los valores del perfil diferencial δ_f son múltiplos de $\frac{1}{2^{n-1}}$, el potencial diferencial $\Omega_f \geq \frac{1}{2^{n-1}}$.

(4) Si f tiene una estructura lineal diferente de 0; esto es , si $Rad_f \neq 0$, entonces $\Omega_f = 1$.

DEFINICIÓN 3.28. **Mapeo perfectamente no lineal**
Un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ es llamado perfectamente no lineal, si su potencial diferencial tiene el (el más pequeño posible) valor $\Omega_f = 2^{-q}$.

OBSERVACIÓN 3.14.2. (5) Por la observación (5) de (3.11.1) y además, por proposición (3.11) que un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ si y solo si para cada forma lineal $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, la forma lineal $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es balanceada si y solo si $\beta \circ f$ es perfectamente no lineal para cada forma lineal $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$.

(6) Un mapeo perfectamente no lineal $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ no puede tener alguna estructura lineal $u \neq 0$.

(7) Si un mapeo perfectamente no lineal existe, entonces $q \leq n-1$, (se tiene por la observación (3) de (3.14.1)).

De la observación (2) en (3.14.1) se tiene la siguiente caracterización de los mapeos perfectamente no lineal relacionada con el perfil diferencial.

PROPOSICIÓN 3.14.1. [7] $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ es perfectamente no lineal si y solo si el perfil diferencial es constante $\delta_f = 2^{-q}$ en $(\mathbb{F}_2^n - \{0\}) \times \mathbb{F}_2^q$.

3.15 Buena Difusión

DEFINICIÓN 3.29. **Buena difusión**
Un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ tiene buena difusión con respecto a $u \in \mathbb{F}_2^n$ si la función diferencia

$\Delta_u f$ es balanceada.

OBSERVACIÓN 3.15.1. (1) Para $q = 1$ esto significa $f(x+u) - f(x) = 0$ o 1 para exactamente 2^{n-1} vectores $x \in \mathbb{F}_2^n$. Denotaremos el número de ceros de la función diferencia por $\eta_f := \#\{x \in \mathbb{F}_2^n | \Delta_u f(x) = 0\} = 2^n \delta_f(u, 0)$. La buena difusión con respecto a u es equivalente $\eta_f(u) = 2^{n-1}$.
La última igualdad se deduce de la observación (1) de (3.14.1).

(2) Para q general la buena difusión significa que $\# D_f(u, v) = 2^{n-q}$ y $\delta_f(u, v) = \dfrac{1}{2^q}$ para todo $v \in \mathbb{F}_2^q$. Esto es , que la fila u del perfil diferencial es constante.

(3) Con respecto a 0 ningún mapeo tiene buena difusión. En caso contrario se contradice la observación anterior.

(4) Los mapeos afines no tienen buena difusión con respecto a cualquier vector u.
Se deduce de la observación (1) de (3.12.1) .

(5) Un mapeo Booleano f es perfectamente no lineal, si y solo si tiene buena difusión con respecto a todos los vectores $u \in \mathbb{F}_2^n - \{0\}$.

DEFINICIÓN 3.30. Una función Booleana f cumple el criterio estricto de avalancha (SAC), si f tiene buena difusión con respecto a todos los vectores de la base canónica.
Esto significa: voltear un bit de entrada cambia exactamente la mitad de los valores de f.

OBSERVACIÓN 3.15.2. (6) Cada función perfectamente no lineal cumple el SAC.
Se deduce de la observación (2) de (3.14.1).

(7) En criptografía, el efecto avalancha es la propiedad deseable de los algoritmos criptográficos, en donde si una entrada cambia ligeramente (por ejemplo, permutando un solo bit), la salida cambia significativamente (por ejemplo, la mitad de los bits de salida).
El criterio de avalancha estricto (SAC, por sus siglas en inglés) es una formalización del efecto de avalancha. Se satisface si, cada vez que se complementa un solo bit de entrada, cada uno de los bits de salida cambia con un 50 por ciento de probabilidad. Fue introducido por Webster y Tavares en 1985. Las funciones Booleanas que satisfacen el orden más alto de SAC son siempre funciones bent.

Podemos expresar una buena difusión de una función Booleana f por la convolución de la forma

característica consigo misma.

$$\begin{aligned}\chi_f * \chi_f &= 2^n \kappa_f(u) \\ &= 2^n \left[\delta_f(u,0) - \delta_f(u,1)\right] \\ &= 2\eta_f(u) - 2^n.\end{aligned}$$

Donde κ_f es la autocorrelación.

LEMA 3.10. [7] Una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ tiene buena difusión con respecto a u si y solo si $\chi_f * \chi_f(u) = 0$ o en otras palabras $\kappa_f(u) = 0$.
Además u es una estructura lineal de f si y solo si
$\chi_f * \chi_f(u) = \pm 2^n$; en otras palabras $\kappa_f(u) = \pm 1$.

Demostración. Si tomamos $u = 0$ en $\chi_f * \chi_f = 2^n \left[\delta_f(u,0) - \delta_f(u,1)\right]$, tenemos como resultado que $\chi_f * \chi_f = 2^n$. Por otro lado tenemos que $\eta_f(u) = 2^n$. Por tanto f es perfectamente no lineal si y solo si $\chi_f * \chi_f(u) = \widehat{1}$, o si $(\widehat{\chi_f})^2 = \widehat{\chi_f * \chi_f} = 2^n$ constante. □

Lo anterior fue la definición de una función bent. De lo anterior, tenemos el siguiente corolario cuya prueba se tiene del lema anterior.

COROLARIO 3.19. [7] Una función Booleana f es perfectamente no lineal si y solo si f es bent.

COROLARIO 3.20. [7] Un mapeo Booleano $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ es perfectamente no lineal si y solo si f es bent.

Demostración. Cada una de estas propiedades es una afirmación equivalentemente para todas las funciones $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ donde $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ es una forma lineal arbitraria diferente de 0. □

Una expresión para una difusión (tan buena como sea posible) de una función Booleana es la autocorrelación global

$$\tau_f := \sum_{x \in \mathbb{F}_2^n} \kappa_f^2(x) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \widehat{\kappa_f}^2(u) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \widehat{\chi_f}(u)^4$$

Las igualdades anteriores se tienen en virtud de la igualdad de Parseval (3.5.1) y del corolario (3.8). En particular $\tau_f \geq \kappa_f(0)^2 = 1$, Así sabemos, que f es perfectamente no lineal si y solo si $\tau_f = 1$. Además

$$\tau_f = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \widehat{\chi_f}(u)^4 \leq \frac{1}{2^n} \left[\sum_{u \in \mathbb{F}_2^n} \widehat{\chi_f}(u)^2 \right]^2. \tag{3.12}$$

Porque todos los sumandos son ≥ 0 la igualdad se cumple si y solo si a lo sumo uno de los sumandos es > 0 . Además $\tau_f \leq 2^n$, y la igualdad se mantiene si y solo si al menos uno $\widehat{\chi_f}(u)^2 > 0$. Este término debe ser igual a la suma total de la suma de los cuadrados 2^{2n}, por tanto $\widehat{\chi_f}(u) = \pm 2^n$,$L_f(u) = \varnothing$ o $\mathbb{F}_2^n$, por tanto $f(x) = u \cdot x + 1$ o $f(x) = u \cdot x$ para todo x.
Así, hemos mostrado lo siguiente.

PROPOSICIÓN 3.15.1. [7] Sea τ_f la autocorrelación global de una función Booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ entonces :

(1) $1 \leq \tau_f \leq 2^n$.

(2) $\tau_f = 1$ si y solo si f es perfectamente no lineal.

(3) $\tau_f = 2^n$ si y solo si f es afín.

3.16 Otras caracterizaciones de las funciones bent

En el estudio de las funciones bent existen muchas preguntas abiertas, una de ellas es, buscar nuevas formas de caracterizarlas. A continuación daremos algunas caracterizaciones conocidas de las funciones bent.

PROPOSICIÓN 3.16.1. [14] Las funciones Booleanas $f(x_1, \cdot, x_m)$ y $g(x_1, \cdot, x_n)$ son bent si y solo si la función Booleana $h(x_1, \cdot, x_m, x_1, \cdot, x_n) = f(x_1, \cdot, x_m) + g(x_1, \cdot, x_n)$ es bent.

Demostración. Sea $c \in \mathbb{F}_2^m$ y $d \in \mathbb{F}_2^n$. De la definición de transformada Walsh tenemos lo siguiente

$$\widehat{\chi_h}(a) = \widehat{\chi_f}(c)\widehat{\chi_g}(d);\ a = (c, d).$$

Si h es bent, entonces f y g también lo son, de lo contrario h no satisfaría la ecuación de Parseval (3.5.1). Si f y g son bent, es claro que h es bent. □

PROPOSICIÓN 3.16.2. [15] Una función Booleana en n variables es bent si y solo si

$$\sum_{a \in \mathbb{F}_2^n} \widehat{\chi_f}^4(a) = 2^{3n}.$$

Demostración. Se tiene de la autocorrelación, ecuación (3.12) lo siguiente:

$$\tau_f = \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}\widehat{\chi_f}(u)^4 \leq \frac{1}{2^n}\left[\sum_{u\in\mathbb{F}_2^n}\widehat{\chi_f}(u)^2\right]^2 \leq \frac{1}{2^n}\left[\sum_{u\in\mathbb{F}_2^n}\widehat{\chi_f}(u)^2\right]\left[\sum_{u\in\mathbb{F}_2^n}\widehat{\chi_f}(u)^2\right].$$

Por la ecuación de Parseval (3.5.1) se tiene el resultado. □

TEOREMA 3.14. [15] Para funciones Booleanas f y f' en n variables se tiene

$$\sum_{x,y\in\mathbb{F}_2^n}(-1)^{f(x)+f'(y)+x\cdot y} \leq 2^{\frac{3n}{2}}.$$

Se tiene la igualdad si y solo si ambas funciones son bent y son duales una de la otra.

Demostración. Sean f y f' funciones Booleanas en n variables, tenemos lo siguiente

$$\begin{aligned}\sum_{x,y\in\mathbb{F}_2^n}(-1)^{f(x)+f'(y)+x\cdot y} &= 2^{-n}\sum_{x,y,z\in\mathbb{F}_2^n}(-1)^{f(x)+(x+z)\cdot y}\widehat{\chi_{f'}}(z)\\ &= \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}\widehat{\chi_{f'}}(x) \leq \sum_{x\in\mathbb{F}_2^n}|\widehat{\chi_{f'}}(x)|\\ &\leq \sqrt{2^n\sum_{x\in\mathbb{F}_2^n}\widehat{\chi_{f'}}(x)} = 2^{\frac{3n}{2}}.\end{aligned}$$

Se tiene la igualdad si y solo si ambas desigualdades de arriba son iguales. Esto es , si y solo si $|\widehat{\chi_{f'}}(x)|$ es constante y $(-1)^{f(x)}$ es el signo de $\widehat{\chi_{f'}}(x)$ para todo x, esto es si y solo si f' es bent y $\tilde{f} = f$. □

DEFINICIÓN 3.31. **La clase de Maiorana- Mcfarland**
El conjunto de todas la funciones Booleanas en el espacio vectorial $\mathbb{F}_2^n = \{(x,y) : x,y \in \mathbb{F}_2^m\}$ (n par) de la forma

$$f(x,y) = x\cdot\pi(y) + g(y) = \sum_{i=1}^{m} x_i\pi_i(y) + g(y)$$

donde π es cualquier permutación en $\mathbb{F}_2^m$, donde $\pi_i, ..., \pi_m$ son sus funciones coordenadas y donde g es cualquier función Booleana en $\mathbb{F}_2^m$.

Ahora, veamos que las funciones Booleanas descritas en la clase de Maiorana- Mcfarland son bent.

PROPOSICIÓN 3.16.3. [14] Las funciones descritas en la clase de Maiorana- Mcfarland son bent.

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

$$\begin{aligned}\widehat{\chi_f}(c) &= \sum_{z \in \mathbb{F}_2^m \times \mathbb{F}_2^m} (-1)^{f(z)+c\cdot z} = \sum_{x,y \in \mathbb{F}_2^m} (-1)^{x\cdot\pi(y)+g(y)+(a,b)\cdot(x,y)} \\ &= \sum_{y \in \mathbb{F}_2^m} (-1)^{g(y)+b\cdot y} \sum_{x \in \mathbb{F}_2^m} (-1)^{x\cdot(\pi(y)+y)}.\end{aligned}$$

Note que la suma anterior es cero, a menos que $\pi(y) = a$, es decir , $y = \pi^{-1}(a)$; en cuyo caso la suma anterior es 2^m. Entonces

$$\widehat{\chi_f}(c) = 2^m(-1)^{g(\pi^{-1}(a))+b\cdot\pi^{-1}(a)}$$

lo que implica que

$$|\widehat{\chi_f}(c)| = 2^m.$$

□

PROPOSICIÓN 3.16.4. [7] Un mapeo bent $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ existe, si y solo si n es un entero par y $n \geq 2q$.

Demostración. Supongamos que f es bent, por el corolario (3.13) se tiene que $\hat{\vartheta}_f$ tomo los valores $\pm 2^{\frac{n}{2}}$ para $v \neq 0$, definamos el siguiente conjunto:

$$r := \#\{v \in \mathbb{F}_2^q - \{0\} | \, \hat{\vartheta}_f(0, v) = +2^{\frac{n}{2}}\}.$$

Y la suma $S := \sum_{v \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0, v)$, luego se tiene $S = 2^{\frac{n}{2}} \cdot [r - (2^q - 1 - r)] = 2^{\frac{n}{2}} \cdot [2r - 2^q + 1]$. Por el lema (3.7) se tiene que $S = 2^q v_f(0) - 2^n$. Despejando $v_f(0)$ se tiene que

$$v_f(0) = \frac{S + 2^n}{2^q} = 2^{\frac{n}{2}-q} \cdot [2r - 2^q + 2^{\frac{n}{2}} + 1].$$

Ya que el factor entre los corchetes es impar, y $v_f(0)$ es un número entero entonces, $2^{\frac{n}{2}-q}$ debe ser entero. por tanto, $\frac{n}{2} \geq q$.

Para la prueba en la otra dirección, supongamos que $n = 2m \geq 2q$. sea $a_1, ..., a_q \in \mathbb{F}_2^m$ sobre $\mathbb{F}_2$ linealmente independiente. Las funciones componentes $f_1, ..., f_q$ de $f : \mathbb{F}_2^m \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ están definidas como $f_i(x, y) = a_i x \cdot y$ para $x, y \in \mathbb{F}_2^m$, como el producto $a_i x \in \mathbb{F}_2^m$, este es un caso especial de la construcción Maiorana- Mcfarland (las cuales son bent ver proposición (3.16.3)). En particular las funciones f_i son bent. Ahora, consideremos la forma lineal $\beta \neq 0$ definida $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, con $\beta(z) = b_1 z_1 + \cdots + b_q z_q$, así se tiene que $\beta \circ f(x, y) = (b_1 a_1 + \cdots + b_q a_q)x \cdot y$ también es una función de la clase Maiorana- Mcfarland. Así, se concluye que f es bent. □

DEFINICIÓN 3.32. **Derivada de una función Booleana**
La primera derivada de una función f en la dirección de $a \in \mathbb{F}_2^n$ está definida como:

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

PROPOSICIÓN 3.16.5. [6] Cualquier función Booleana es Bent si y solo si para cualquier vector a diferente de cero $D_a f(x)$ es balanceada.

Demostración. Veamos que $D_a f(x)$ es balanceada para $a \neq 0$, debemos ver que $d(D_a f(x), 0) = 2^{n-1}$, por el corolario (3.2) sabemos que $d(D_a f(x), 0) = 2^{n-1} - \frac{1}{2}\hat{\chi}_{D_a f}(x)$.
Pero

$$\begin{aligned}
\hat{\chi}_{D_a f}(x) &= \sum_{a \in \mathbb{F}_2^n} \left((-1)^{a\cdot b} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)} \right) \\
&= \sum_{a \in \mathbb{F}_2^n} \left((-1)^{a\cdot b} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{f(x+a)} \right) \\
&= \sum_{a \in \mathbb{F}_2^n} (-1)^{a\cdot b} \chi_f \chi_f.
\end{aligned}$$

Teniendo en cuenta que $a \neq 0$, por lema (3.4) se tiene lo buscado. Luego $d(D_a f(x), 0) = 2^{n-1}$. □

Capítulo 4

Independencia de las variables de funciones Booleanas

Al considerar una función Booleana como una red con n entradas y una salida, entonces podría haber una relación entre las entradas y la salida. La relación entre las entradas y salida de una función Booleana puede proporcionar información útil al romper un algoritmo de cifrado cuando dicha función Booleana es un componente del núcleo del algoritmo. Esta relación puede ser fuertemente dependiente, o ligeramente dependiente o incluso independiente en algún sentido.

Para una función Booleana $f(x)$ en n variables, puede no depender de todas sus variables de entrada, es decir, alguna de las variables pueden no contribuir a la salida de $f(x)$. En este caso la función se dice que es algebraicamente independiente de esas variables.

DEFINICIÓN 4.1. Sea $f(x) \in \mathcal{F}_n$, si el valor de $f(x)$ no se ve afectado por el valor de x_i, esto es

$$f(x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n) = f(x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n)$$

se tiene para cualquier $(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n) \in \mathbb{F}_2^{n-1}$, entonces $f(x)$ se dice que es algebraicamente independiente de x_i o simplemente independiente de x_i

La definición anterior, puede ser generalizada de la siguiente manera.

DEFINICIÓN 4.2. Sea $f(x) \in \mathcal{F}_n$. Denotamos por

$$\Delta(i_1, i_2, ..., i_k) = \{x \in \mathbb{F}_2^n : x_j = 0 \text{ si } j \notin \{i_1, i_2, ..., i_k\}\}.$$

Si $f(x \oplus \alpha) = f(x)$ se tiene para todo $\alpha \in \Delta(i_1, i_2, ..., i_k)$, entonces $f(x)$ se dice independiente de las variables $x_{i_1}, x_{i_2}, ..., x_{i_k}$. Por simplicidad simplemente llamamos a la función independiente de $x_{i_1}, x_{i_2}, ..., x_{i_k}$.

EJEMPLO 4.0.1. Sea $f(x) = x_1$, f es independiente de las variables $x_2, x_3, ..., x_n$. Ya que cualquier asignación de estas variables no afectará el valor de $f(x)$.

OBSERVACIÓN 4.0.1. Un registro de desplazamiento es un sistema, circuito o memoria de n celdas donde se almacena un bit en su estado inicial, la secuencia inicial se conoce como semilla. Al ritmo que marca un reloj el contenido de cada celda se desplaza y envía ese bit a la celda siguiente; así, la última celda de la cadena pierde su valor y la primera celda de la cadena se queda vacía. El bit que se pierde formará parte de un secuencia de bits que se transmiten. Por su parte la celda vacía se rellenará con el resultado de una operación de alimentación que se ejecuta antes de ese desplazamiento con los bits de un conjunto de celdas del registro conectas a esa función de realimentación.
Si la operación consiste solo en la puerta lógica XOR, entonces se habla de un registro de desplazamiento realimentado linealmante (LSFR). Este se usa en criptografía para generar secuencias cifrantes al ser más simple, rápidas y eficientes.

4.0.1 La independencia estadística de las variables de funciones Booleanas

Una variable binaria $x \in \mathbb{F}_2^n$ puede tomar todos los 2^n valores posibles. Sin embargo, en muchos casos, solo se toma un cierto número de sus valores. En situaciones es importante que valor se necesita. Entonces, en general suponemos que la variable puede tomar cualquier valor posible en $\mathbb{F}_2^n$ con igual probabilidad. Esto significa que tratamos a x como una variable probabilística con distribución de probabilidad uniforme. Por este tratamiento, cualquier función Booleana con esta variable también es un evento probabilístico que tiene cierta probabilidad de ser verdadero (cuando su valor es igual a 1) o falso (cuando su valor es igual a 0). Del mismo modo, podemos estudiar las probabilidades condicionales, por ejemplo, cuando la condición previa es que la variable toma un conjunto particular de valores en $\mathbb{F}_2^n$; la probabilidad de que $f(x)$ tenga valor 0 o 1 es una probabilidad condicional. Existen tales funciones Booleanas, aunque no son independientes de ninguna de sus variables; sin embargo, estadísticamente parecen no verse afectadas por algunas de sus variables; es decir, la probabilidad de que tal función tomó un cierto valor (0 o 1) no se ve afectado por ningún valor predefinido de estas variables. En este caso, se dice que la función es estadísticamente independiente de estas variables.
Por ejemplo, la función Booleana en 3 variables $f(x) = x_1x_2 \oplus x_3$ toma el valor de 1 si y solo si $x \in \{(110), (001), (101), (011)\}$. Así, $\mathrm{Prob}(f(x) = 1) = \mathrm{Prob}(f(x) = 0) = 1/2$, esto es , $f(x)$ es balanceada

donde $Prob(A)$ representa la probabilidad de que ocurra el evento A.
Cuando $x_1 = 1$ es fijado, entonces $f(x)$ toma valor de 1 si y solo si $x = (110)$ o $x = (101)$ y $f(x) = 0$ si y solo si $x = (100)$ o $x = (111)$. Obviamente, bajo la condición que $x_1 = 1$, sea x_2 y x_3 variables libres, entonces $f(x)$ sigue balanceada, esto es

$$Prob(f(x) = 1|x_1 = 1) = Prob(f(x) = 0|x_1 = 1) = 1/2.$$

Donde la $Pro(A|B)$ representa la probabilidad que el evento A ocurra dado la condición que B ha ocurrido. Es fácil verificar que $f(x)$ es también balanceada bajo la condición que $x_1 = 0$. Esto significa que independientemente de cualquier valor fijo asignado a x_1, la probabilidad de que $f(x)$ tome un cierto valor (0 o 1) sigue siendo la misma; esto es

$$Prob(f(x) = a|x_1 = b) = Prob(f(x) = a)$$

se tiene para cualquier $a, b \in \{0, 1\}$. Por tanto, la función $f(x)$ es estadísticamente independiente de x_1. Con un calculo, se puede verificar que $f(x)$ es estadísticamente independiente de x_2 pero no de x_3. Aparentemente $f(x)$ no es independiente de ninguna de sus variables, ya que todas las variables aparecen en la forma normal algebraica.

DEFINICIÓN 4.3. Sea $f(x) \in \mathcal{F}_n$. Consideremos cada x_i como una variable independiente que toma valores de $\mathbb{F}_2$ al azar. Si la probabilidad de $f(x)$ de tomar un valor particular no se afectado por la precondición de que x_i tiene asignado cierto valor. Esto es ,

$$Prob(f(x) = b|x_i = a) = Prob(f(x) = b),$$

donde $a, b \in \{0, 1\}$, $Prob(Z)$ significa la probabilidad que el evento Z ocurra, y $P(A|B)$ significa la probabilidad condicional para que ocurra el evento A dado que el evento B ocurrió; entonces $f(x)$ es llamada estadísticamente independiente de x_i.
De forma general, si para algún $1 \leq i_1 < i_2 < \cdots < i_k \leq n$,

$$Prob(f(x) = b|(x_{i_1}, x_{i_2}, ..., x_{i_k}) = (a_1, a_2, ..., a_k)) = Prob(f(x) = b)$$

se tiene para cualquier $b \in \mathbb{F}_2$ y $(a_1, a_2, ..., a_k) \in \mathbb{F}_2^k$, entonces $f(x)$ es llamada estadísticamente independiente de las variables $x_{i_1}, x_{i_2}, ..., x_{i_k}$.

Como en la definición anterior, si $f(x)$ es estadísticamente independiente de $x_{i_1}, x_{i_2}, ..., x_{i_k}$, entonces cualquier asignación de valores a $x_{i_1}, x_{i_2}, ..., x_{i_k}$ no afectará la probabilidad de $f(x)$ para tomar un

cierto valor. Esto significa que para cualquier función Booleana no constante $f(x) \in \mathbb{F}_n$ se tiene lo siguiente

$$\text{Prob}(f(x) = b|(x_{i_1}, x_{i_2}, ..., x_{i_k}) = (a_1, a_2, ..., a_k)) = \text{Prob}(f(x) = b) \neq 0$$

donde $b \in \{0, 1\}$ y $(a_1, a_2, ..., a_k) \in \mathbb{F}_2^k$.
Note que una función puede ser estadísticamente independiente de sus variables $x_{i_1}, x_{i_2}, ..., x_{i_k}$ individualmente pero aun, no ser estadísticamente independiente del conjunto de variables $x_{i_1}, x_{i_2}, ..., x_{i_k}$. Por ejemplo, $f(x_1, x_2, x_3) = x_1x_3 \oplus x_2x_3 \oplus x_3$ es estadísticamente independiente de x_1 y de x_2 individualmente, pero no estadísticamente independiente de x_1, x_2 como grupo.

4.0.2 Independencia estadística de dos funciones Booleanas individuales

Hasta este momento, se ha definido la independencia de las variables de funciones Booleanas. Como generalización de esta relación, podemos considerar la independencia de dos distintas funciones Booleanas. Sean $f(x)$ y $g(x)$ dos funciones Booleanas del mismo número de variables. La probabilidad condicional $\text{Prob}(f(x) = a|g(x) = b)$ donde $a, b \in \{0, 1\}$, significa que entre el conjunto de entradas x que satisfacen $g(x) = b$, la probabilidad de que x también satisfaga $f(x) = a$. Por ejemplo, cuando $g(x)$ tiene un valor fijo, digamos $g(x) = 1$, entonces la probabilidad de que $f(x)$ tome el valor 1 es una probabilidad condicional, denotado por $\text{Prob}(f(x) = 1|g(x) = 1)$.

DEFINICIÓN 4.4. **Independencia entre dos funciones Booleanas**
Sea $f(x)$ y $g(x)$ dos funciones Booleanas en n variables. Se considera a x como una variable aleatoria sobre $\mathbb{F}_2^n$ si para cualquier $a, b \in \{0, 1\}$ se tiene lo siguiente

$$\text{Prob}(f(x) = a|g(x) = b) = \text{Prob}(f(x) = a)$$

entonces $f(x)$ es llamada estadísticamente independiente de $g(x)$.

4.0.3 Independencia estadística de un grupo de funciones Booleanas

DEFINICIÓN 4.5. **Independencia estadística de un grupo de funciones Booleanas**
Sea $f_1(x), f_2(x), ..., f_m(x) \in \mathcal{F}_n$. Tratando a x como una variable aleatoria sobre $\mathbb{F}_2^n$ con distribución de

probabilidad uniforme si

$$\begin{aligned}&\text{Prob}((f_1(x), f_2(x), ..., f_m(x))) = (a_1, a_2, ..., a_m) = \\ &\text{Prob}(f_1(x) = a_1)\text{Prob}(f_2(x) = a_2) \cdots \text{Prob}(f_m(x) = a_m)\end{aligned}$$

se cumple para todos $(a_1, a_2, ..., a_m) \in \mathbb{F}_2^m$, entonces el grupo de funciones

$$\{f_1(x), f_2(x), ..., f_m(x)\}$$

es llamada una familia de funciones Booleanas estadísticamente independiente.

TEOREMA 4.1. [13] Sea $\{f_1(x), f_2(x), \cdot, f_m(x)\}$ una familia estadísticamente independiente de funciones Booleanas en $\mathcal{F}_n$. Entonces cualquiera de sus subconjuntos es una familia estadísticamente independiente de funciones Booleanas.

Demostración. Sin perdida de generalidad, probemos que $\{f_1(x), f_2(x), \cdot, f_k(x)\}$ forma una familia de funciones Booleanas estadísticamente independiente, donde $k < n$. Para cualquier $(a_1, a_2, ..., a_k) \in \mathbb{F}_2^k$, ya que $\{f_1(x), f_2(x), \cdot, f_m(x)\}$ forma una familia de funciones Booleanas estadísticamente independiente, tenemos

$$\begin{aligned}&\text{Prob}((f_1(x), f_2(x), \cdot, f_k(x)) = (a_1, a_2, ..., a_k)) \\ &= \sum_{(a_{k+1},...,a_m)\in\mathbb{F}_2^{m-k}} \text{Prob}((f_1(x), \cdot, f_k(x)) = (a_1, ..., a_k), f_{k+1}(x), \cdot, f_m(x)) = (a_{k+1}, ..., a_m) \\ &= \sum_{(a_{k+1},...,a_m)\in\mathbb{F}_2^{m-k}} \prod_{i=1}^{k} \text{Prob}(f_i(x) = a_i) \prod_{j=k+1}^{m} \text{Prob}(f_j(x) = a_j) \\ &= \prod_{i=1}^{k} \text{Prob}(f_i(x) = a_i) \sum_{(a_{k+1},...,a_m)\in\mathbb{F}_2^{m-k}} \prod_{j=k+1}^{m} \text{Prob}(f_j(x) = a_j) \\ &= \prod_{i=1}^{k} \text{Prob}(f_i(x) = a_i) \begin{bmatrix} \sum_{a_{k+1}\in\{0,1\}} \text{Prob}(f_{k+1}(x) = a_{k+1}) \cdots \\ \sum_{a_m\in\{0,1\}} \text{Prob}(f_m(x) = a_m) \end{bmatrix} \\ &= \prod_{i=1}^{k} \text{Prob}(f_i(x) = a_i)\end{aligned}$$

Por la definición (4.5), $\{f_1(x), f_2(x), \cdot, f_k(x)\}$ forman una familia de funciones Booleanas estadísticamente independiente. □

TEOREMA 4.2. [13] El número de funciones booleanas no constantes (miembros) en una familia de funciones Booleanas estadísticamente independiente en n variables es como máximo n y en este caso, todas las funciones miembro deben ser balanceadas.

Demostración. Primero se probará que el número de funciones miembro en una familia de funciones Booleanas estadísticamente independiente en n variables es como máximo n. Asumamos lo contrario; por el teorema (4.1), podemos asumir que hay $n+1$ funciones Booleanas $f_1(x), f_2(x), \cdot, f_{n+1}(x) \in \mathcal{F}_{n+1}$ que forman una familia de funciones Booleanas estadísticamente independiente. Por la definición (4.5), para cualquier $(a_1, a_2, ..., a_{n+1}) \in \mathbb{F}_2^{n+1}$, tenemos

$$\text{Prob}((f_1(x), f_2(x), \cdot, f_{n+1}(x)) = (a_1, a_2, ..., a_{n+1})) = \prod_{i=1}^{n+1} \text{Prb}(f_i(x) = a_i).$$

Sin embrago, ya que $x \in \mathbb{F}_2^n$ tiene solo 2^n valores posibles, y las salida de $f_1(x), f_2(x), \cdot,$ $f_{n+1}(x)$ no puede cubrir todos los vectores en $\mathbb{F}_2^{n+1}$, de ahí que debe existir $(a_1, a_2, ..., a_{n+1}) \in \mathbb{F}_2^{n+1}$ tal que

$$\text{Prob}((f_1(x), f_2(x), \cdot, f_{n+1}(x)) = (a_1, a_2, ..., a_{n+1})) = 0.$$

Sin embargo, para cualquier función miembro no constante $f_i(x)$ y cualquier $a_i \in \mathbb{F}_2$, tenemos $\text{Prob}(f_i(x) = a_i) \neq 0$, por tanto

$$\prod_{i=1}^{n+1} \text{Prob}(f_i(x) = a_i) \neq 0.$$

Esto conduce a una contradicción. Esto significa que la suposición de que $n+1$ funciones forman una familia de funciones estadísticamente independientes no es cierta.
Ahora probaremos que, si hay n funciones miembro en una familia de funciones estadísticamente independientes, entonces cada función debe ser balanceada.
Asumamos que $f_1(x), f_2(x), \cdot, f_n(x)$ forman una familia de funciones estadísticamente independientes. Entonces para cualquier $(a_1, a_2, ..., a_n) \in \mathbb{F}_2^n$, tenemos

$$\text{Prob}((f_1(x), f_2(x), \cdot, f_n(x)) = (a_1, a_2, ..., a_n)) = \prod_{i=1}^{n} \text{Prob}(f_i(x) = a_i).$$

Ya que cada miembro es una función no constante, por tanto, para cualquier $a_i \in \mathbb{F}_2$, $\text{Prob}(f_i(x) =$

$a_i) \neq 0$ se cumple. Esto significa que para cualquier $(a_1, a_2, ..., a_n) \in \mathbb{F}_2^n$, se tiene

$$\text{Prob}((f_1(x), f_2(x), \cdot, f_n(x)) = (a_1, a_2, ..., a_n)) \neq 0.$$

Note que $x \in \mathbb{F}_2^n$ tiene exactamente 2^n valores posibles; por tanto, para cualquier $(a_1, a_2, ..., a_n) \in \mathbb{F}_2^n$, hay exactamente un $x \in \mathbb{F}_2^n$ tal que

$$(f_1(x), f_2(x), \cdot, f_n(x)) = (a_1, a_2, ..., a_n)$$

por tanto, cuando x pasa por todos los valores posibles en $\mathbb{F}_2^n$, $(f_1(x), f_2(x), ..., f_n(x)) = (a_1, a_2, ..., a_n)$ también pasará por todos los valores posibles en $\mathbb{F}_2^n$. Cuando x cambia sus valores en un cierto orden, todos los posibles valores de a_i de la tabla de verdad de $f_i(x)$. Se sabe que, cuando $(a_1, a_2, ..., a_n)$ pasa por todos los valores posibles en $\mathbb{F}_2^n$, cada una de sus coordenadas a_i tiene el mismo número de 0 y 1 lo que significa que $f_i(x)$ es balanceada. □

4.1 Permutaciones Booleanas

4.1.0.1 Funciones Booleanas vectoriales en la representación de S−boxes

En el diseño de algoritmos criptográficos, particularmente en algoritmo de cifrado de bloque los S−box juegan un papel esencial para garantizar la seguridad de los algoritmos.
Por ejemplo, los algoritmos de cifrado DES y AES (cifrado de bloque) usan S−box como sus componentes no lineales de transformaciones. Se sabe que muchos algoritmos de cifrado de flujo también usan S−box como componentes importantes no lineales.
Una S−box se puede representar mediante una función Booleana vectorial , las propiedades criptográficas pueden ser representadas por las propiedades correspondientes de funciones Booleanas vectoriales, aunque está no siempre es la mejor representación en términos de complejidad tanto en presentación e implementación.

DEFINICIÓN 4.6. S−**box**
Una S−box criptográfica o simplemente llamada una S−box es una función que toma como entrada una cadena de longitud n y genera otra cadena de longitud m. Esto significa que una S−box es un mapeo $F(x)$ de $\mathbb{F}_2^n$ a $\mathbb{F}_2^m$, por ese motivo una S−box también es llamada una (n, m)−función Booleana.

Notemos que una (n, m)−función Booleana puede ser representada como una colección de m fun-

ciones Booleanas de $\mathcal{F}_n$, de la siguiente forma

$$F(x) = [f_1(x), f_2(x), \cdots, f_m(x)],$$

donde cada $f_i \in \mathcal{F}_n$, $i = 1, 2, ..., m$, es una función Booleana en n variables, y las f_i son llamadas funciones coordenadas de $F(x)$. De lo anterior, las (n, m) funciones Booleanas se puede convertir en el estudio de funciones coordenadas individuales; sin embargo, la función (n, m) Booleana puede tener muchas propiedades que no pueden reflejarse desde ninguna de sus funciones Booleanas de coordenadas individuales. Considerando la salida de una $(n, m)-$función Booleana, cualquier salida de este tipo es un vector en $\mathbb{F}_2^m$. Entonces hay una probabilidad de que cada uno de los vectores sea la salida de la función cuando la variable de entrada x pasa por todos los valores posibles en $\mathbb{F}_2^n$. Si $n < m$ entonces el espacio de entrada es más pequeño que el espacio de salida, es decir, la $(n, m)-$función Booleana $F(x)$ mapea $\mathbb{F}_2^n$ en un subconjunto de $\mathbb{F}_2^m$; en este caso, la salida de $F(x)$ no tiene las mismas posibilidades de tener ningún valor en $\mathbb{F}_2^m$. Este tipo de S$-$box es llamada S$-$box de expansión.
En el caso $n > m$, entonces es espacio de entrada es mayor que el espacio de salida; esto significa que un subconjunto de la entrada puede dar como resultado todas las posibles salidas en $\mathbb{F}_2^m$. Se observa que incluso en tal caso, la salida de $F(x)$, también puede tener más posibilidades de ser parte de vectores en $\mathbb{F}_2^m$ en menos posibilidades de ser algunos otros vectores. Este tipo de S$-$box es llamada S$-$box de compresión.
Para $n = m$, entonces este caso especial puede llamarse de comprensión o una S$-$box de expansión donde sea conveniente.

Desde un punto de vista criptográfico, se espera que una S$-$box segura tenga la propiedad que cualquier subconjunto de salida no proporciona información sobre otros bits de la salida. Esto significa que una (n, m) función Booleana que representa una S$-$box tiene la propiedad que las m funciones de salida $f_1(x), f_2(x), \cdots, f_m(x)$ son estadísticamente independientes de cada otro. Por el teorema (4.2) sabemos que esto solo ocurre cuando $n \geq m$.

DEFINICIÓN 4.7. S$-$**box imparcial**
Sea una S$-$box representada por una (n, m) función Booleana $F(x)$. Si $n \geq m$, entonces $F(x)$ (y por tanto la S$-$box) es llamada imparcial si para cualquier $(a_1, a_2, \cdots, a_{n-m})$ la siguiente igualdad siempre se cumple

$$\text{Prob}(F(x) = (a_1, a_2, \cdots, a_{n-m})) = \frac{1}{2^m}$$

si $n < m$, entonces $F(x)$ (y por tanto la S$-$box) es llamada imparcial, si cualquier n funciones coorde-

nadas de $F(x)$ forman una (n, n)-función Booleana imparcial.

TEOREMA 4.3. [13] Sea $F(x) = [f_1(x), f_2(x), \cdots, f_m(x)]$ una (n, n)-función Booleana que representa una $S-$box, donde $n \geq m$. Entonces F es imparcial si y solo si :

(1) $f_1(x), f_2(x), \cdots, f_m(x)$ forman una familia de funciones Booleanas estadísticamente independiente.

(2) $f_1(x), f_2(x), \cdots, f_m(x)$ son todas balanceadas.

Demostración. Probemos la necesidad.
Ya que $[f_1(x), f_2(x), \cdots, f_m(x)]$ es imparcial, por la definición (4.7), para cualquier $(a_1, a_2, ..., a_m) \in \mathbb{F}_2^m$,

$$prob((f_1(x), f_2(x), \cdots, f_m(x)) = (a_1, a_2, ..., a_m)) = \frac{1}{2^n}$$

es una constante fija.
Ahora, dejando que x pase por todos los vectores en $\mathbb{F}_2^n$; entonces para cada $(a_1, a_2, ..., a_m) \in \mathbb{F}_2^m$, hay 2^{n-m} valores de x tales que

$$(f_1(x), f_2(x), \cdots, f_m(x)) = (a_1, a_2, ..., a_m)$$

se cumple. Esto significa que cuando x pasa por todos los valores en $\mathbb{F}_2^n$,
$(f_1(x), f_2(x), \cdots, f_m(x))$ también pasa por cada vector en $\mathbb{F}_2^m$ por exactamente 2^{n-m} veces. Se sabe que cuando $(a_1, a_2, ..., a_m)$ va a través de todos los vectores en $\mathbb{F}_2^m$, cada una de sus coordenadas a_i tiene las mismas posibilidades de ser 0 o 1. Esto es lo mismo cuando $(a_1, a_2, ..., a_m)$ pasa por todos los valores en $\mathbb{F}_2^m$ para 2^{n-m} veces. Esto prueba que cada $f_i(x)$ es balanceada, y es fácil verificar que en este caso, tenemos

$$\begin{aligned} prob((f_1(x), f_2(x), \cdots, f_m(x)) &= (a_1, a_2, ..., a_m)) \\ &= \prod_{i=1}^{m} prob(f_i(x) = a_i) = 2^{-m} \end{aligned}$$

se cumple.
Así, $(f_1(x), f_2(x), \cdots, f_m(x))$ forman una familia estadística independiente de funciones Booleanas.

Veamos ahora la suficiencia. Para cualquier $(a_1, a_2, ..., a_m) \in \mathbb{F}_2^m$, por definición tenemos

$$\begin{aligned} \text{prob}((f_1(x), f_2(x), \cdots, f_m(x)) &= (a_1, a_2, ..., a_m)) \\ &= \prod_{i=1}^{m} \text{prob}(f_i(x) = a_i) = 2^{-m} \end{aligned}$$

esto significa que $(f_1(x), f_2(x), \cdots, f_m(x))$ tiene las mismas posibilidades de tomar cualquier valor en $\mathbb{F}_2^m$. Porque

$$\sum_{a_1, a_2, ..., a_m \in \mathbb{F}_2^m} \text{Prob}((f_1(x), f_2(x), \cdots, f_m(x)) = (a_1, a_2, ..., a_m)) = 1$$

entonces para cada $(a_1, a_2, ..., a_m) \in \mathbb{F}_2^m$ se tiene que $\text{Prob}((f_1(x), f_2(x), \cdots, f_m(x)) = (a_1, a_2, ..., a_m) = 2^{-m}$ por definición (4.7) $[f_1(x), f_2(x), \cdots, f_m(x)]$ es imparcial. □

DEFINICIÓN 4.8. **Permutación Booleana**
Sea $F(x)$ una (n, m) función Booleana; en el caso que $m = n$ y la función es imparcial, diferentes entradas producen diferentes salidas. Al tratar cada entrada-salida como la representación binaria de un número entero dentro de $S = \{0, 1, ..., 2^n - 1\}$, lo anterior, la función F realiza una permutación en S. Nos referimos a tal permutación en S en representación como una (n, m)—permutación Booleana, por simplicidad, también la llamamos una permutación Booleana en n—variables.

Ya que cualquier permutación Booleana se puede representar como una colección de funciones Booleanas en n variables, la escribimos como:

$$F(x) = [f_1(x), f_2(x), \cdots, f_n(x)].$$

Hay que tener en cuenta que no todas las colecciones de funciones Booleanas forman una permutación Booleana ; para eso deben satisfacer ciertas condiciones.
A continuación, se enunciaran y demostraran dos lemas necesarios para la prueba de un teorema que establece condiciones necesarias y suficientes para que una colección de funciones Booleanas sea una permutación Booleana.

LEMA 4.1. [13] Sea $f(x) \in \mathcal{F}_n$ una función Booleana en n variables. Denotamos con $f^0(x) = 1 \oplus f(x)$, $f^1(x) = f(x)$. Entonces para cualquier $a \in \{0, 1\}$, tenemos que $f^a(x) = a$ se cumple si y solo si $f(x) = 1$. Similarmente se tiene que $f^a(x) = 1$ si y solo si $f(a) = a$.

Demostración. El lema se puede verificar tomando los casos cuando $a = 0$ y $a = 1$. □

LEMA 4.2. [13] Sea $f_i \in \mathcal{F}_n$, $i = 1, 2, ..., n$. Entonces $f_1(x)$, $f_2(x)$,$\cdots$,$f_n(x)$ satisface que para cualquier vector diferente de cero $c = (c_1, c_2, \cdots, c_n) \in \{0,1\}^n$

$$wt\left(\bigoplus_{i=1}^{n} c_i f_i\right) = 2^{n-1} \tag{4.1}$$

si y solo si para cualquier $a \in \{0,1\}$ y para cualquier $i \in \{1, 2, ..., n\}$, las funciones

$$f_1(x), \cdots, f_{i-1}(x) f_1^a(x), f_{i+1}(x), \cdots, f_n(x)$$

también satisfacen (4.1).

Demostración. Según el lema (4.1), la suficiencia y la necesidad del lema son simétricas. Entonces, solo tenemos que demostrar la necesidad. Cuando $a = 1$, la conclusión es verdadera. Sea $a = 0$; entonces para cualquier i con $1 \leq i \leq n$ tenemos

$$\begin{aligned} wt\left(\bigoplus_{k,k\ nei} c_k f_k \oplus c_i f_i^0\right) &= wt\left(\bigoplus_{k=1}^{n} c_k f_k \oplus c_i\right) \\ &= \begin{cases} wt\left(\bigoplus_{k=1}^{n} c_k f_k \oplus\right), & \text{si } c_i = 0 \\ 2^n - wt\left(\bigoplus_{k=1}^{n} c_k f_k \oplus\right), & \text{si } c_i = 1 \end{cases} \\ &= 2^{n-1} \end{aligned}$$

entonces la conclusión del lema se sigue. □

TEOREMA 4.4. [13] Sea $F(x) = [f_1(x), f_2(x), \cdots, f_n(x)]$ una $(n,n)-$función Booleana, donde $f_i(x) \in \mathcal{F}_n$, $i = 1, 2, ..., n$. Entonces $F(x)$ es una permutación Booleana si y solo si cualquier combinación lineal diferente de creo de $f_1(x), f_2(x), \cdots, f_n(x)$ es una función Booleana balanceada, esto es, para cualquier vector diferente de cero $c = (c_1, c_2, \cdots, c_n) \in \{0,1\}^n$ se tiene

$$wt\left(\bigoplus_{i=1}^{n} c_i f_i\right) = 2^{n-1}.$$

Demostración. Tratemos cada salida de $(f_1(x), f_2(x), \cdots, f_n(x))$ como la representación binaria de un entero $S = \{0, 1, ..., 2^n-1\}$; entonces la salida de $f_i(x)$ es la $i-$esima coordenada de la representación binaria de este entero. Cuando x va de 0 a 2^n-1, ya que $F(x)$ es una permutación Booleana la cual es una $(n,n)-$función Booleana , por definición dada anteriormente, la salida de $F(x)$ también pasa por cada elemento de S exactamente una vez. Entonces la tabla de verdad de $F(x) = [f_1(x), f_2(x), \cdots, f_n(x)]$

es una permutación de la tabla de verdad de $x = [x_1, x_2, ..., x_n]$. Por tanto, la tabla de verdad de $f'(x) = \bigoplus_{i=1}^{n} c_i f_i$, es una combinación lineal diferente de cero de $f_1(x), f_2(x), \cdots, f_n(x)$, es una permutación de la tabla de verdad de $\bigoplus_{i=1}^{n} c_i f_i$, la misma combinación lineal diferente de cero de $x_1, x_2, ..., x_n$, que obviamente es una función Booleana balanceada. Esto implica la necesidad del teorema.

Ahora , realizaremos la prueba en la otra dirección. Por la ecuación (4.1) y eligiendo el vector de coeficientes para ser el caso especial cuyo peso de Hamming es 1, tenemos

$$wt(f_i) = 2^{n-1}, \quad i = 1, 2, ..., n$$

ya que $wt(f_i \oplus f_j) = wt(f_i) + wt(f_j) - 2wt(f_i f_i)$, tenemos $wt(f_i f_i) = 2^{n-2}$, $i \neq j$. Asuma que $wt(f_{i_1}, f_{i_2}, \cdots, f_{i_t}) = 2^{n-t}$ para $t = 1, 2..., k$, donde $1 \leq i_1 < i_2 < \cdots < i_t \leq n$, ya que

$$\begin{aligned} wt(f_1 \oplus f_2 \oplus \cdots \oplus f_{k+1}) = &\sum_{i=1}^{k+1} wt(f_i) - 2 \sum_{1 \leq i \leq j \leq n} wt(f_i f_j) + \cdots \\ &+ (-1)^k 2^k wt(f_1 f_2 \cdots f_{k+1}) \end{aligned}$$

que es equivalente a

$$\begin{aligned} 2^{n-1} = &(k+1)2^{n-1} - \binom{k+1}{2} 2^{n-1} + \cdots + (-1)^{k-1} \binom{k+1}{k} 2^{n-1} + \\ &(-1)^k wt(f_1 f_2 \cdots f_{k+1}) \end{aligned}$$

tenemos por tanto

$$wt(f_1 f_2 \cdots f_{k+1}) = 2^{n-(k+1)}.$$

Se observa que el orden de las funciones $f_1(x), f_2(x), \cdots, f_n(x)$ que satisfacen la ecuación (4.1) no importa; por tanto, lo anterior significa que para cualquier $k+1$ función de coordenadas de $F(x)$, tenemos

$$wt(f_{i_1} f_{i_2} \cdots f_{i_{k+1}}) = 2^{n-(k+1)}$$

de acuerdo con el principio de inducción, tenemos para el caso $k = n-1$, lo siguiente también es válido $wt(f_1 f_2 \cdots f_n) = 2^{n-n} = 1$.

Esto significa que solo existe una x que satisface $f_1(x) f_2(x) \cdots f_n(x) = 1$. Para cualquier $(a_1, a_2, \cdots, a_n) \in \{0,1\}^n$, usando el lema (4.2), se sabe que $f_1^{a_1}, f_2^{a_2}, \cdots, f_n^{a_n}$ también satisface la ecuación (4.1). Esto significa que existe solo un x tal que $f_1^{a_1}(x), f_2^{a_2}(x), \cdots, f_n^{a_n}(x) = 1$ esto es,

$f_i^{a_i}(x) = 1$ se cumple por el lema (4.1) tenemos $f_i(x) = a_i$. Esto muestra que la salida de $F(x) = [f_1(x), f_2(x), \cdots, f_n(x)]$ tiene exactamente una posibilidad de ser cualquier valor de S cuando x pasa por todos los valores posibles en S, por tanto $F(x)$ es una permutación en S. □

4.1.1 Propiedades de las Permutaciones Booleanas

A continuación veremos algunas propiedades relacionadas con las permutaciones Booleanas.
El siguiente teorema establece que una permutación en el indice de una permutación Booleana produce otra permutación Booleana. Su prueba se deduce de la definición de permutación (Una permutación de un conjunto S es una función biyectiva de dicho conjunto en sí mismo) y de permutación Booleana.

TEOREMA 4.5. [13] Sea $P = [f_1, f_2, \cdots, f_n]$ una permutación Booleana y σ_n una permutación en el conjunto $\{0, 1, 2, ...n\}$. Entonces

$$\sigma_n(P) = [f_{\sigma_n(1)}, f_{\sigma_n(2)}, \cdots, f_{\sigma_n(n)}]$$

es también una permutación Booleana.

TEOREMA 4.6. [13] Sea $P = [f_1, f_2, \cdots, f_n]$ una permutación Booleana, $D = (d_{ij})$ una matriz binaria $n \times n$, y $C = (c_1, c_2, ..., c_n) \in \mathbb{F}_2^n$. Entonces

$$PD \oplus C = \left[\bigoplus_{i=1}^{n} d_{i1} f_i \oplus c_1, \bigoplus_{i=1}^{n} d_{i2} f_i \oplus c_2, \cdots, \bigoplus_{i=1}^{n} d_{in} f_i \oplus c_n\right]$$

es una permutación Booleana si y solo si D es no singular.

Demostración. $P = [f_1, f_2, \cdots, f_n]$ es una permutación Booleana si y solo si para cualquier vector $\alpha = (a_1, a_2, ..., a_n)$, $P \oplus \alpha = [f_1 \oplus a_1, f_2 \oplus a_2, ..., f_n \oplus a_n]$ es también una permutación Booleana .
Entonces solo necesitamos probar el caso $C = 0$. Supongamos que D es una matriz singular. Entonces debe existir un vector diferente de cero $B = (b_1, b_2, ..., b_n)$ tal que $DB^T = 0$; por tanto

$$[f_1, f_2, \cdots, f_n]DB^T = \sum_{j=1}^{n} b_j \sum_{i=1}^{n} d_{i,j} f_i = 0$$

esto indica que la combinación lineal distinta de cero de las coordenadas de
$[f_1, f_2, \cdots, f_n]D$ con el vector de coeficiente B es cero en lugar de una función lineal balanceada. Luego

por teorema (4.4) sabemos que $[f_1, f_2, \cdots, f_n]D$ no es una permutación Booleana.
Ahora vemos el reciproco. Supongamos que D es no singular. Entonces para cualquier vector diferente de cero $B \in \mathbb{F}_2^n$, $DB^T \neq 0$. Por tanto

$$[f_1, f_2, \cdots, f_n]DB^T = \sum_{i=1}^{n} f_i \sum_{j=1}^{n} d_{i,j} b_j$$

es una combinación lineal diferente de cero (con las coordenadas de DB^T como coeficientes) de f_i. Ya que P es una permutación Booleana, por teorema (4.4), tenemos

$$wt\left(\sum_{i=1}^{n} f_i \sum_{j=1}^{n} d_{i,j} b_j\right) = 2^{n-1}.$$

Dada la arbitrariedad de B y el uso del teorema (4.4), sabemos que $[f_1, f_2, \cdots, f_n]D$ es una permutación Booleana. □

TEOREMA 4.7. [13] Sea $P = [f_1, f_2, \cdots, f_n]$ una permutación Booleana, $D = (d_{ij})$ una matriz binaria $n \times n$, y $C = (c_1, c_2, ..., c_n) \in \mathbb{F}_2^n$. Entonces

$$P(xD \oplus C) = [f_1(xD \oplus C), f_2(xD \oplus C), ..., f_n(xD \oplus C)]$$

es una permutación Booleana si y solo si D es no singular.

Demostración. Denotemos $y = (y_1, y_2, ..., y_n) = (x_1, x_2, ..., x_n)D \oplus C$. Entonces vemos que $y_1, y_2, ..., y_n$ son n variables independientes si y solo si D es no singular. Ya que $P = [f_1, f_2, \cdots, f_n]$ es una permutación Booleana, $[f_1(y), f_2(y), \cdots, f_n(y)]$ es también una permutación Booleana si y solo si $y_1, y_2, ..., y_n$ son n variables independientes. □

Ahora veremos que las permutaciones Booleanas también se puede hacer la composición entre ellas.

TEOREMA 4.8. [13] Sean $P = [f_1, f_2, \cdots, f_n]$ y $Q = [g_1, g_2, \cdots, g_n]$ dos permutaciones Booleanas. Entonce su composición

$$P(Q) = [f_1(g_1, g_2, \cdots, g_n), f_2(g_1, g_2, \cdots, g_n), \cdots f_n(g_1, g_2, \cdots, g_n)]$$

es una nueva permutación Booleana.

4.1.2 La inversa de una permutación Booleana

Como cualquier permutación, las permutaciones Booleanas tienen una inversa. Esta inversa es también una permutación Booleana. Las permutaciones Booleanas y su inversa juegan un papel importante en las aplicaciones de funciones Booleanas. Como es el caso de los criptosistemas de clave pública que se estudiarán más adelante.
Dada una permutación Booleana $P = [f_1, f_2, \cdots, f_n]$, la inversa P es una solución de la siguiente ecuación:

$$\begin{cases} z_1 = f_1(x_1, x_2, \cdots, x_n) \\ z_2 = f_2(x_1, x_2, \cdots, x_n) \\ \cdots \\ z_n = f_n(x_1, x_2, \cdots, x_n) \end{cases} \tag{4.2}$$

esto es, una expresión de cada x_i en términos de z_j. Supongamos que tenemos una solución de la ecuación (4.2) en la forma

$$\begin{cases} x_1 = f_1^{-1}(z_1, z_2, \cdots, z_n) \\ x_2 = f_2^{-1}(z_1, z_2, \cdots, z_n) \\ \cdots \\ x_n = f_n^{-1}(z_1, z_2, \cdots, z_n) \end{cases} \tag{4.3}$$

Entonces $P^{-1} = [f_1^{-1}, f_2^{-1}, \cdots, f_n^{-1}]$ es la permutación inversa de la permutación Booleana P.

El siguiente lema es una herramienta usada para verificar si dos permutaciones Booleanas son inversas entre si, especialmente cuando el número de variables de las permutaciones Booleanas es bastante grande, por lo que es computacionalmente inviable verificar todos los pares de entradas y salidas.

LEMA 4.3. [13] Sea $P = [f_1, f_2, \cdots, f_n]$ y $Q = [g_1, g_2, \cdots, g_n]$ dos permutaciones Booleanas. Entonces son inversas entre sí si y solo si para cada $i \in \{1, 2, ..., n\}$, se tiene que $g_i(f_1, f_2, \cdots, f_n) = x_i$ y $f_i(g_1, g_2, \cdots, g_n) = x_i$.

Demostración. la prueba de este lema se deduce de las ecuaciones (4.2),(4.3) y del teorema (4.8). □

Capítulo 5

Aplicaciones

Para Codificar un mensaje de texto sin formato (plaintext) en texto cifrado (cypertext) se usa una clave de 7 bits para 7 bit ASCII y aplicar el bitwise exclusivo OR a cada letra. De esta manera, cada letra del mensaje del texto sin formato se convierte en una letra diferente en el texto cifrado. El descifrado es simple, se aplica la misma clave al texto cifrado. Desde la segunda aplicación de la clave `aniquila` la primera aplicación, nos queda la letra del texto sin formato. El problema con esto es, que la distribución de letras en el texto plano también se produce en el texto cifrado. Esto puede ser explotado por alguien escuchando el texto cifrado. Por ejemplo, las letras más frecuentes en el texto cifrado pueden, se supone que e o t y se puede suponer que las menos frecuentes son z o q.
Para evitar el descifrado por un extraño, se busca una secuencia clave que sea aleatoria. Sin embargo, las computadoras paralelas se pueden utilizar para explotar variaciones de aleatoriedad en la secuencia de claves. Por ejemplo, en un ataque lineal, se intenta una secuencia de claves que se genera a partir de una función Booleana lineal. Si el flujo de clave real utilizado en el cifrado es casi lineal, habrá errores, pero tal ataque puede ser finalmente exitoso.
Contra tales ataques, se busca una función que sea tan lineal como sea posible. Estas son las funciones bent.
Las funciones bent son importantes debido a una técnica de criptoanálisis, en la que las funciones no lineales utilizadas en el proceso de encriptación son aproximadas por funciones lineales. Es decir, cuando el cifrado es lineal, es descifrado es sencillo. Cuando el cifrado es ligeramente no lineal, entonces una aproximación lineal se puede usar, entendiendo que el descifrado es erróneo pero potencialmente corregible. Las funciones bent son altamente valoradas porque son las más difíciles de aproximar por funciones lineales.

5.1 Aplicaciones criptográficas de las funciones Booleanas

Las aplicaciones criptográficas de las funciones Booleanas están destinadas a tener algunas propiedades criptográficas. Esas propiedades están construidas para frustrar el criptoanálisis de ciertos tipos, y generalmente se requieren múltiples propiedades criptográficas para una función que se utilizará en el diseño de algoritmos criptográficos, que se espera que resista algunos ataques conocidos a los algoritmos criptográficos. Por lo tanto las aplicaciones principales (criptográficas) de las funciones Booleanas son el diseño de algoritmos criptográficos, particularmente algoritmos de cifrado de flujo y cifrado de bloque.

DEFINICIÓN 5.1. **Cifrado**
Un cifrado es un conjunto de reglas matemáticas, o algoritmo, utilizado para convertir un texto que se puede leer, o texto sin formato, en un texto que no se puede leer conocido como texto cifrado.

Las funciones Booleanas tienen aplicabilidad en el cifrado de flujo y en el de bloque. Estos tipos de cifrado se definen de la siguiente manera.

DEFINICIÓN 5.2. **Cifrado de flujo**
Consiste en dividir el texto en bloques pequeños, de un bit o byte de largo, y codificar cada bloque dependiendo de muchos bloques anteriores. El cifrado de flujo utiliza una clave de codificación diferente, un valor que debe ser alimentado en el algoritmo, por cada bit o byte para que este mismo produzca un texto cifrado diferente cada vez que se codifica. El cifrado lleva a cabo una operación Booleana conocida como OR exclusiva, entre los bits en el flujo de claves y los bits en el texto sin formato para producir texto cifrado.

DEFINICIÓN 5.3. **Cifrado de bloque**
Consiste en dividir el texto en bloques relativamente largos, normalmente de 64 0 28 bits; y codificar cada bloque por separado. En este tipo de cifrado, Se utiliza la misma clave de cifrado por cada bloque y es la clave de cifrado la que determina el orden en qué se llevan a cabo la sustitución, el transporte y otras funciones matemáticas en cada bloque.

5.1.1 Aplicaciones de las funciones Booleanas degeneradas a la representación lógica de un circuito

Una de las aplicaciones de las funciones Booleanas en el cifrado de flujo es actuar como una función de combinación o similar. Por consideraciones de seguridad las funciones de combinación deberían

ser no lineales e idealmente deberían tener alta no linealidad. Sin embargo, desde un punto de vista diferente, una función no lineal puede tratarse como una composición de una colección de funciones lineales y una no lineal. Por la composición de funciones queremos decir que la salida de una o más funciones se convierte en la entrada de otra. Para esta función deposición (el proceso inverso de composición), puede ser posible encontrar una componente no lineal más simple de las funciones. Si el número de funciones lineales puede ser menor que el número de entradas originales, entonces se dice que la función original es degenerada.

DEFINICIÓN 5.4. **Función algebraicamente degenerada**
Sea $f(x) \in \mathcal{F}_n$. Si existe una $n \times k$ matriz D sobre $\mathbb{F}_2$ y $g(y) \in \mathcal{F}_k$ tal que

$$f(x) = g(xD) = g(y)$$

donde $k < n$, entonces $f(x)$ se dice que es algebraicamente degenerada.
Si k es el mínimo valor tal que $f(x) = g(xD) = g(y)$, esto es, si no existe una $n \times (k-1)$ matriz D' y una función Booleana $h(y) \in \mathcal{F}_{k-1}$ tal que $f(x) = h(xD')$, entonces $g(y)$ es llamada una función algebraicamente degenerada de $f(x)$ o función degenerada de $f(x)$. El valor $n-k$ es llamado el grado de degeneración de $f(x)$ y se denota por $AD(f) = n-k$.
Si no existe una $n \times k$ matriz D con $k < n$ tal que se cumpla $f(x) = g(xD)$, esto es, el mínimo valor de k es $k = n$; entonces $f(x)$ se dice algebraicamente no degenerada.

Cabe señalar que una función Booleana en n variables no puede ser igual a una función Booleana en k $(k < n)$ variables, por lo que la igualdad de la definición anterior solo significa la representación algebraica. Un ejemplo simple es la función $f(x) = x_1$, la cual puede ser tratada como función Booleana en cualquier número de variables dependiendo de donde este definido, pero siempre es equivalente a una función Booleana en una variable, en términos de representación algebraica en el sentido de transformación lineal en sus variables. Otro ejemplo de este tipo es , $f(x) = x_1 \otimes x_2 \otimes, ..., \oplus x_n$, en el que también es equivalente a una función Booleana en una variable, y nuevamente esta equivalencia es en el sentido de representación algebraica mediante una transformación lineal en sus variables.

DEFINICIÓN 5.5. **Coset**
Sea V un subespacio vectorial de $\mathbb{F}_2^n$. Para cualquier $\alpha \in \mathbb{F}_2^n \setminus V$; sea

$$V_1 = \alpha \oplus V = \{\alpha \oplus x : x \in V\}$$

es llamado el coset de V. La descomposición

$$\mathbb{F}_2^n = \bigcup_{\alpha \in \mathbb{F}_2^n \setminus V} \alpha \oplus V$$

es llamada la descomposición coset de $\mathbb{F}_2^n$ con respecto a V, y α es llamado un representante (o líder) del coset de V para el coset V_1.

TEOREMA 5.1. [13] Sea $f(x) \in \mathcal{F}_n$. Denotemos

$$V = \langle \{w : \widehat{f}(w) \neq 0\} \rangle$$

al span lineal de los puntos del espectro distinto de cero de $f(x)$. Asumamos que $\dim(V) = k$, y sea $h_1, h_2, ..., h_k$ una base de V. Denotemos por $H = [h_1^T, h_2^T, ..., h_k^T]$ que es una matriz $n \times k$. Entonces existe una función Booleana $g(y)$ en k variables tal que

$$g(y) = g(xH) = f(x).$$

Demostración. Por la expresión inversa de la transformada Walsh podemos escribir $f(x)$ como:

$$\widehat{f}(w) = \sum_{x=0}^{2^n-1} f(x)(-1)^{\langle w,x \rangle}$$

la transformada correspondientes es :

$$f(x) = 2^{-n} \sum_{x=0}^{2^n-1} \widehat{f}(w)(-1)^{\langle w,x \rangle} = 2^{-n} \sum_{w \in V} \widehat{f}(w)(-1)^{\langle w,x \rangle}.$$

donde V es un subespacio vectorial de $\mathbb{F}_2^n$.
En lo anterior, solo se debe considerar $w \in V$; por tanto, para cualquier $x \in V^\perp$, $\langle w, x \rangle = 0$ siempre se cumple. Por tanto, para cualquier $\alpha \in \mathbb{F}_2^n$ y $x \in V^\perp$, se tiene lo siguiente

$$f(x \oplus \alpha) = 2^{-n} \sum_{w \in V} \widehat{f}(w)(-1)^{\langle w,(x \oplus \alpha) \rangle} = 2^{-n}(-1)^{\langle w,\alpha \rangle} \sum_{w \in V} \widehat{f}(w)$$

esto significa que $f(x)$ es una constante en cada coset de $V^\perp$. Sea S el conjunto de todos los lideres cosets de $V^\perp$. Entonces podemos establecer un mapeo φ de S a $\mathbb{F}_2^n$ como

$$\varphi(\alpha) = \alpha H.$$

donde H es la matriz que se describe en el teorema. Es fácil ver que para cualquier $\alpha_1, \alpha_2 \in S$, si $\varphi(\alpha_1) = \varphi(\alpha_2)$ entonces $(\alpha_1 - \alpha_2)H = 0$. Esto significa que $(\alpha_1 - \alpha_2) \in V^{\perp}$; por tanto, $\alpha_1 = \alpha_2$. Por otro lado, ya que $|S| = 2^k = |\mathbb{F}_2^k|$, así φ es una biyección. Por tanto, la función $g(y)$ se puede definir como

$$g(y) = f(\varphi^{-1}(y)), \quad y \in \mathbb{F}_2^k$$

entonces para cualquier $\alpha \in S$, tenemos

$$g(\alpha H) = f(\varphi^{-1}(\alpha H)) = f(\alpha)$$

por tanto, para cualquier $x \in \mathbb{F}_2^n$, debe existir $\alpha \in S$ y $\beta \in V^{\perp}$ tal que $x = \alpha \oplus \beta$; por tanto, $xH = (\alpha \oplus \beta)H = \alpha H$, y en consecuencia se tiene

$$f(x) = f(\alpha) = g(\alpha H) = g(xH).$$

□

La propiedad de degeneración de funciones Booleana es utilizada para simplificar circuitos lógicos. Las operaciones Booleanas XOR y la multiplicación módulo 2, tienen puertas correspondientes XOR y AND. Representaremos con la letra D el operador multiplicación modulo 2 y $\oplus$ para la adición modulo 2.
En virtud del teorema (5.1), sabemos que si una función Booleana $f(x) \in \mathcal{F}_n$ es degenerada, existe $g(y) \in \mathcal{F}_k$ y una $n \times k$ matriz binaria D tal que $f(x) = g(xD)$ se cumple para todo $x \in \mathbb{F}_2^n$. La prueba del teorema (5.1), en realidad da cómo encontrar la función degenerada $g(y)$ de una función degenerada $f(x)$. Aquí, no daremos el proceso de como calcular la función degenerada si la función Booleana dada es degenerada; en lugar de eso, afirmamos que hay una buena posibilidad de que la implementación del circuito de $g(xD)$ sea más simple que el de $f(x)$. A continuación, ilustraremos lo descrito anteriormente en el siguiente ejemplo.

EJEMPLO 5.1.1. Sea f una función Booleana, tal que $f(x) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3$; f representa un circuito lógico (asumimos la disponibilidad de la compuerta XOR, aunque esto puede ser equivalente implementándose en compuertas AND y OR. La multiplicación representa una compuerta AND como en la figura (5.1)). Se puede ver que el span lineal de los puntos de espectro distintos de cero de $f(x)$ tienen dimensión 2. Por tanto $f(x)$ se puede degenerar en una función de dos variables.
En efecto, podemos encontrar la función degenerada $g(y_1, y_2) = y_1y_2$, ya que

$$g(y_1, y_2) = g((x_1, x_2, x_3)D) = f(x)$$

Donde

$$D = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

por tanto, $y_1 = x_1 \oplus x_3$ y $y_2 = x_2 \oplus x_3$. De acuerdo con la función degenerada, el circuito lógico puede diseñarse como en la figura (5.2).

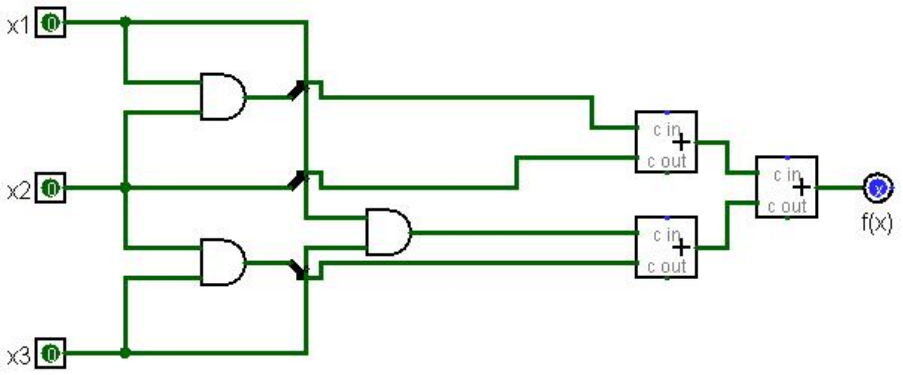

Figura 5.1 circuito lógico de $f(x)$

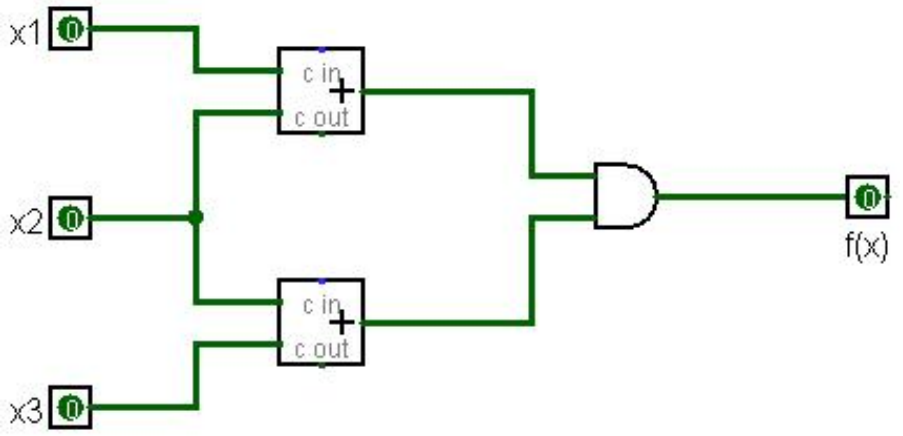

Figura 5.2 Circuito simplificado de $f(x)$

5.2 Una aplicación de las permutaciones Booleanas al diseño de criptosistemas de clave pública

La criptografía de clave pública (o PKC), designa el sistema criptográfico que hace uso de un par de claves: una pública y otra privada. Las dos claves están matemáticamente vinculadas y pueden ser empleadas tanto para encriptación de datos como para firmas digitales.
Como herramienta de encriptación, la PKC es más segura que los métodos más rudimentarios de la encriptación simétrica. Mientras los sistemas más antiguos se apoyan en la misma clave para cifrar y descifrar la información, la PKC permite encriptar los datos mediante la clave pública, y des encriptarlos utilizando la correspondiente clave privada.
Aparte de eso, el esquema PKC puede ser aplicado para la generación de firmas digitales.
Las permutaciones Booleanas se tratan como representaciones de funciones Booleanas de S−boxes criptográficas, y sus aplicaciones principales están en el diseño de cifrados de flujo y cifrado de bloque. Veremos como las permutaciones Booleanas se pueden usar como bloques primarios en la construcción para el diseño de criptosistemas de clave pública. Esencialmente, cualquier algoritmo de cifrado sin expansión de la información es una permutación. En el caso de los sistemas de clave simétrica la permutación está oculta por una clave secreta. En el caso de criptosistemas de clave asimétrica la permutación está oculta por alguna estructura especial.
En criptografía de clave pública donde los algoritmos de cifrado y descifrado son requerido, la idea básica para diseñar los algoritmos implica el uso funciones de trapdoor unidireccional. Una función $y = f_\lambda(x)$ se denomina función de trapdoor unidireccional con parámetro trapdoor λ si cumple las siguientes propiedades:

(1) **Computable:** Dada cualquier entrada x, es computacionalmente fácil para obtener la salida y.

(2) **Sentido único:** Dado cualquier resultado y, sin el conocimiento del parámetro trapdoor λ u otra información adicional, es computacionalmente inviable rastrear hasta la entrada x.

(3) **Tradoor:** Con el conocimiento de λ, es computacionalmente fácil encontrar el correspondiente x dada cualquier salida y.

Una función trapdoor unidireccional también se conoce como una función unidireccional si el parámetro trapdoor es desconocido y, por lo tanto, la función es difícil de invertir. Una función se llama una función de dos vías si es computacionalmente fácil encontrar su inverso. A partir de estos requisitos, vemos que una función de trapdoor debe ser una inyección (no necesariamente una biyección) del dominio de entrada al dominio de salida. El parámetro trapdoor podrían ser datos, o un

algoritmo.

5.2.1 Criptosistemas de clave pública 1 (PKC1)

Una permutación Booleana se puede usar directamente para diseñar un criptosistema de clave pública si cumple las siguientes propiedades como una función trapdoor unidireccional.

- Sin conocimiento adicional es computacionalmente inviable encontrar el inverso de la permutación Booleana dada (unidireccional).
- Con un conocimiento especial, es fácil encontrar el inverso de la permutación Booleana (existe trapdoor).
- El número de elementos en todas las funciones de coordenadas de la permutación Booleana es razonablemente pequeño (aplicable).

Una permutación Booleana que cumpla con las dos primeras propiedades es en realidad una función trapdoor. El conocimiento especial para encontrar el inverso es la trapdoor. Una forma construir tales permutaciones Booleanas implica el uso de la composición de permutaciones Booleanas.
Sea $P = [f_1, f_2, \cdots, f_n]$ una permutación Booleana con las propiedades de arriba. El usuario U elige a P como la clave pública y mantiene la permutación inversa P^{-1} como su clave privada. Un plaintext (texto sin formato) m es una cadena binaria de longitud n, y el ciphertext (texto cifrado) correspondiente viene dado por $c = P(m)$. El descifrado viene dado por $m = P^{-1}(c)$.

El tamaño de la clave pública se basa en el número de términos en la permutación P, y el tamaño de la clave privada se basa en el número de términos en P^{-1}. Entonces el número de términos de P, y P^{-1} deben ser razonablemente pequeños para que el sistema sea practico. La mejor manera de atacar este sistema parece ser la determinación de la mejor aproximación lineal.
En general, el sistema de cifrado se puede asegurar eligiendo una permutación Booleana con baja linealidad.

5.2.2 Criptosistemas de clave pública 2 (PKC2)

Sea A una $k \times n$ matriz binaria arbitraria con rango k. Entonces debe existir una $n \times k$ matriz binaria X y una $(n-k) \times n$ matriz binara B tal que $AX = I_k$ y $BX = 0$; donde I_k es la $k \times k$ matriz identidad.

Denotaremos esto como un triple (A, B, X). Es mejor elegir matrices sin una fila que sea toda cero ni una columna que sea toda cero. Una manera de hacer esto es eligiendo una matriz $n \times n$ C no singular arbitraria; entonces A está compuesta por las primeras k filas de C y B se compondrá del resto de $n - k$ filas de C. Sea X compuesta por las primeras k columnas más a la izquierda de C^{-1}.
Sea $P = [f_1, f_2, \cdots, f_k]$ una permutación Booleana de orden k, para la cual el inverso P^{-1} es conocido solo por el usuario. Sea (A, B, X) un triple que satisface las propiedades anteriores.
Sea $R[r_1, \cdots, r_{n-k}]$ una colección arbitraria de funciones de $\mathcal{F}_k$ (debe tener un número pequeño de términos) y sea $Q = PA \oplus RB$ la clave pública. Note con $P = QX$, la clave privada correspondiente viene dada por $P^{-1}(zX)$. Por tanto, el criptosistema de clave pública es el siguiente:

- **Pública:** $Q = PA \oplus RB$.
- **Privada:** $P^{-1}(zX)$.
- **Mensaje** m **:** cadena binaria de longitud k.
- **Cifrado:** $c = Q(m)$.
- **Descifrado:** $m = P^{-1}(cX)$.

En este sistema criptografico, la clave pública es una colección de k funciones Booleanas en n variables, si alguna de las componentes k de la clave pública forma una permutación Booleana que es fácil de invertir, entonces el criptosistema puede romperse fácilmente. Sin embargo, determinando si alguna de las coordenadas k de Q forman una permutación Booleana es un problema NP−completo. Aunque si tal permutación Booleana se encuentra ocasionalmente, para encontrar su inverso parece ser tan difícil como para romper PKC1. Por lo tanto, no es factible obtener m de c cuando k es bastante grande. Para minimizar la extensión de la información, se propone que n es ligeramente más grande que k. Cuando tanto la permutación Booleana P como la función arbitraria R se elige correctamente, el tamaño de la clave puede ser razonablemente pequeño.

5.2.3 Criptosistema de clave pública 3 (PKC3)

Similar a PKC2, en PKC3 se utiliza una matriz generadora G de un $[n, k, d]$ código lineal con un conocido algoritmo de decodificación rápida (por ejemplo código Goppa). Sea $P(x) = [f_1(x), f_2(x), \cdots, f_k(x)]$ una permutación Booleana de orden k para la que el inverso P^{-1} es conocido solo por el usuario U. Sea $P(x)G$ una colección de n funciones Booleanas en k variables. Note

que para cualquier $m \in \mathbb{F}_2^k$, $G(m)$ es la palabra código correspondiente al mensaje $P(m)$. Sea $E(x) = [e_1(x), ..., e_n(x)]$ una colección de n funciones Booleanas arbitrarias en k variables que satisfacen para cualquier x , $wt(E(x)) \leq t = [d-1]/2$. Entonces $C(x) = G(x) \oplus E(x)$ está configurado para ser la clave pública y P^{-1} y el algoritmo de decodificación rápida se mantienen privados. El criptosistema de clave pública es le siguiente:

- **Pública:** $C(x)$.
- **Privada:** $P^{-1}(x)$ y algoritmo de decodificación.
- **Mensaje** m **:** Cadena binaria de longitud k.
- **Cifrado:** $c = C(m)$.
- **Descifrado:**

  (1) decodificando c para obtener $m' = P(m)$

  (2) $m = P^{-1}(m')$.

Similar como en el caso PKC2, si k componentes de la clave pública forman una permutación Booleana, entonces el criptosistema puede romperse. Sin embargo, este es un problema NP− completo y es difícil cuando k es grande.

5.3 Aplicación de permutaciones Booleanas a firmas digital

Una firma digital es un mecanismo criptográfico empleado para verificar la autenticidad e integridad de datos digitales. Podemos considerarla una versión digital de las firmas escritas a mano ordinarias, pero con un nivel más elevado de complejidad y seguridad.
En términos sencillos, podríamos describir una firma digital como código vinculado a un mensaje o documento. Después de ser generado, dicho código ejerce como prueba de que el mensaje no ha sido manipulado durante el proceso que lo lleva del emisor al receptor.
A pesar de que el concepto de proteger las comunicaciones mediante el uso de criptografía se remonta a la antigüedad, los esquemas de firma digital se convirtieron en una posibilidad real en los años 70 gracias al desarrollo de la Criptografía de Clave Pública (PKC). Los criptosistemas de clave pública a menudo se usan en el diseño de esquemas de firma digital. Un sistema de firma digital debe cumplir las siguientes condiciones:

- La generación y verificación de firmas debe ser computacionalmente eficiente.
- Solo el propietario puede crear sus firmas válidas.
- Cualquier persona debería poder verificar la validez de la forma digital.

Consideremos ahora cómo los criptosistemas de clave pública basados en una permutación Booleana como se propuso en la sección anterior, se puede utilizar para obtener firmas digitales.
Se puede ver que PKC1 se puede utilizar para obtener firmas de conducta directa. Aquí una firma es lo mismo que descifrar un mensaje, mientras que verificar una firma es lo mismo que encriptar un mensaje.
Con PKC2 las firmas se pueden lograr dejando que $P^{-1}(zX)$ sea la clave pública y dejando que $Q(x)$ sea la clave privada. Entonces la clave privada se puede usar para crear firmas, mientras que la clave pública se puede utilizar para verificarlas.
Ahora consideremos cómo se puede utilizar PKC3 para obtener firmas. Sin perdida de generalidad, suponemos que las primeras k columnas de G forman una matriz no singular G'. Luego por teorema (4.6), sabemos que $PG' = [G_1, \cdots, G_K]$ es una permutación Booleana para la cual el inverso $[G_1^{-1}, \cdots, G_K^{-1}]$ puede ser obtenido fácilmente por el propietario de la calve pública. Para un mensaje m que es una cadena binaria de longitud k, la firma del usuario U es el par (m', e'), donde

$$m' = (G_1^{-1}(m), \cdots, G_K^{-1}(m)),$$
$$e' = (e_1(m'), \cdots, e_k(m')).$$

Al recibir la firma, el verificador puede validar la firma calculando

$$(C_1(m'), \cdots, C_K(m')) = (G_1^{-1}(m), \cdots, G_K^{-1}(m)) \oplus (e_1(m'), \cdots, e_k(m')) = m \oplus e',$$
$$(C_1(m'), \cdots, C_K(m')) \oplus e' = (m \oplus e') \oplus e' = m.$$

5.4 Aplicación de permutaciones Booleanas al compartido de firmas

Supongamos que hay una compañía que tiene un clave privada para firmar documentos. Cada miembro de la compañía comparte una parte de la información relacionada con la clave privada tal que una sola persona no pueda crear una firma válida; solo un grupo autorizado puede generar una firma válida. Esto es una combinación de un esquema de firma normal y un esquema de intercambio secreto.

Cuando el esquema de intercambio secreto es un esquema de umbral, produce una firma de umbral. Se debe tener en cuenta que la principal diferencia entre los esquemas de intercambio secreto y las firmas compartidas es que, en un esquema de intercambio secreto, una vez que se recupera la información secreta, el secreto se revela para siempre y todos los accionistas no pueden usar sus acciones más adelante. Sin embrago, en un esquema de firma compartida, los accionistas pueden usar repetidamente sus acciones para firmar mensajes sin revelar la clave secreta.
Suponga que hay una autoridad confiable de una compañía que puede generar claves públicas para la compañía. Sea S una colección de k funciones Booleanas que es la clave privada de la compañía.
Sea A una $k \times n$ matriz donde $n > k$. Sea α_i^T que denota la $i-$esima columna de A. Entonces la autoridad distribuye α_i^T y $S\alpha_i^T$ a miembro U_i de la compañía. Para un mensaje $m \in \mathbb{F}_2^k$, la firma de U_i es α_i^T y $S(m)\alpha_i^T$. Se puede ver que cuando k tales firmas se recogen de manera que $k\alpha_i^T$ son linealmente independiente, el mensaje original m se puede recuperar y por tanto, se genera una firma válidada. Entonces una colección de U_i es un grupo autorizado si y solo si sus α_i forman una matriz con rango k. Cuando k es grande y se quiere que el grupo sea pequeño, cada persona puede tener más de una columna de A. Debe tenerse en cuenta que cuando se firma un mensaje, la firma junto con el mensaje en sí debe enviarse al receptor, cuando el receptor recibe la firma, el/ella comprueba si algunas de las α_i pueden formar una matriz no singular para que $S(m)$ pueda recuperarse. Luego, usando la clave pública, m se recupera. Al comparar el mensaje adjunto con el recuperado, se reconoce la validez del firma. Esta firma compartida tiene las siguientes propiedades.

- Solo un grupo autorizado puede generar firmas válidas.
- Firmar un mensaje no reduce la seguridad de otras firmas.
- Las firmas se pueden verificar fácilmente.
- Cuando se agregan nuevos miembros al grupo, sus claves pueden ser asignadas por la autoridad sin la colaboración de otros miembros.
- Cuando los miembros abandonan la compañía, para que sus acciones ya no sean válidas, todas las acciones de los miembros así como la clave pública debe modificarse.

NOTA 3. Con base en el concepto de cifrado, decimos que un cifrado es *con umbral* si para descifrar un mensaje se requiere que cooperen un número de entidades superior al umbral requerido. Este tipo de sistemas solo es posible con clave pública. En estos sistemas el mensaje se cifra usando una clave pública y la clave privada es compartida de tal forma que permite la funcionalidad descrita. La criptografía con umbral (threshold cryptography) tiene como objetivo distribuir alguna funcionalidad criptográfica entre muchos usuarios de tal forma que:

(1) Cualquier conjunto con $t + 1$ usuarios pueda colectivamente calcular la funcionalidad.

(2) Ningún conjunto con solo t usuarios pueda realizar la funcionalidad.

En los sistemas de firma digital con umbral solo t o más miembros del grupo pueden generar firmas del grupo con n miembros. Por otro lado $t - 1$ o menos miembros no pueden hacerlo. Además cualquiera puede usar la clave pública para verificar la firma.

5.5 Funciones Bent en el Criptografía

Las propiedades de las funciones bent son naturalmente interesantes en la criptografía digital moderna. Para 1988 Forré reconoció que la transformación de Walsh de una función puede ser utilizada para demostrar que cumple con el Criterio estricto de avalancha (SAC) , y recomendó esta herramienta para seleccionar buenos candidatos S-box que logran una difusión casi perfecta. De hecho, funciones que satisfacen el SAC para el orden más alto posible siempre son bent. Además, las funciones bent son como lo más lejos posible de tener lo que se llama estructuras lineales, es decir, vectores distintos de cero a tal que $f(x + a) + f(x)$ es una constante.
En el lenguaje del criptoanálisis diferencial (introducido después de que se descubrió esta propiedad) la derivada de una función bent f en cada punto a distinto de cero (es decir, $D_a(x) = f(x + a) + f(x)$) es una función Booleana balanceada , tomando cada valor exactamente la mitad de veces. Esta propiedad se llama perfecta no linealidad. Dadas tan buenas propiedades de difusión, resistencia aparentemente perfecta a criptoanálisis diferencial y resistencia por definición al criptoanálisis lineal, al principio las funciones bent parecen ser la opción ideal para funciones criptográficas seguras como las S-box. Su defecto fatal es que no pueden ser balanceadas. En particular, una S-box invertible no se puede construir directamente a partir de funciones bent. En cambio, uno podría comenzar con una función bent y complementar aleatoriamente los valores apropiados hasta el resultado balanceado. La función modificada todavía tiene una alta no linealidad, y como tal las funciones son muy raras, el proceso debería ser mucho más rápido que una búsqueda de fuerza bruta. Pero las funciones producidas de esta manera pueden perder otras propiedades deseables, incluso fallando para satisfacer el SAC, es necesario realizar pruebas cuidadosas. Una serie de criptógrafos han trabajado en técnicas para generar funciones balanceadas que preserven tantas de las buenas cualidades criptográficas de las funciones bent como sea posible. Algunos de estas investigaciones teóricas se han incorporado a algoritmos criptográficos reales.

Desde un punto de vista criptográfico, las funciones bent tienen dos principales intereses:

(1) Sus derivadas $D_a f : x \longmapsto f(x) + f(x + a)$ son balanceadas por lo tanto cualquier adición de un vector distinto de cero a la entrada de f induce 2^{n-1} cambios entre las 2^n salidas; esto tiene una relación importante con el ataque diferencial en cifrados de bloque.

(2) La distancia de Hamming entre f y el conjunto de funciones Booleanas afines toma valor óptimo $2^{n-1} - 2^{\frac{n}{2}-1}$ (n par); esto tiene una relación directa con el ataque de correlación rápido en cifrados de flujo y el ataque lineal en cifrados de bloque.

Sin embargo, las funciones bent tienen dos inconvenientes:

(1) Las funciones bent no son balanceadas, por lo tanto, difícilmente pueden usarse, por ejemplo, en cifrados de flujo.

(2) Un generador pseudoaleatorio que utiliza una función bent como combinador o filtro es débil contra algunos ataques, como el ataque algebraico rápido, incluso si la función bent ha sido modificada para hacerla balanceada.

Capítulo 6

Problemas abiertos

Las funciones Booleanas son una fuente de preguntas a un sin respuesta. Las funciones Booleanas y las tipos bent, a pesar de tener un gran desarrollo teórico todavía resta encontrar respuesta a muchas preguntas. A continuación, presentaremos algunos problemas abiertos relacionados con los temas abordados en este trabajo.

(1) El número exacto de funciones bent. Se sabe que hay exactamente $8,896,5\,425\,430\,528 \simeq 2^{32.2}$ y $2^9 \times 193\,887\,869\,660\,028\,067\,003\,488\,010\,240 \simeq 2^{106.29}$ de funciones bent en dos, cuatro, seis y ocho variables respectivamente. Pero ¿cuál es el número exacto de funciones bent si $n \geq 10$?.

(2) Construcciones. Proponer nuevas construcciones directas de funciones bent. Por ahora la clase constructiva más simple de funciones bent es la clase Maiorana- Mcfarland; ¿hay otras clases (más grandes) de funciones bent con ejemplos que se construyen fácilmente?.

(3) Problema de la descomposición bent. ¿Para cualquier $n \geq 4$ par, cada función Booleana en n variables de grado algebraico a lo sumo $\frac{n}{2}$ es igual a la suma (mod 2) de dos funciones bent?

(4) Enfoque algebraico general. Proponer una caracterización algebraica de funciones bent, es decir, encontrar condiciones necesarias y suficientes en la forma traza (o forma polinómica) de una función Booleana que va a bent. Pensar en otras representaciones algebraicas de funciones bent.

(5) Generalizaciones de funciones bent con respecto a sus propiedades algebraicas y criptográficas, que son cada vez más numerosas y ampliamente estudiadas de año en año.

Capítulo 7

Conclusiones

Durante el desarrollo de este trabajo de disertación podemos resaltar los siguientes aspectos:

(1) Se pudo crear un documento detallado con los conceptos bases sobre la teoría de las funciones Booleanas y las Booleanas tipo bent.

(2) Se pudo mostrar parte del alcance que tienen las funciones Booleanas y las bent en aplicaciones en el campo de la criptografía.

(3) Los aportes del autor fueron los siguientes: Detallar y en algunos casos demostrar los resultados mostrados, los cuales algunos tiene demostraciones muy reducidas y otros no presentan demostraciones en el texto [7].

Bibliografía

[1] D. S. MALIK, JOHN M. MORDESON, M. K. SEN, *Fundamentals of Abstract Algebra* Mcgraw-Hill College (1996)

[2] DAVID GÓMEZ SAURA, *Trabajo fin de grado, cuerpos finitos*

[3] J. ASENSIO MAYOR, J.R. CARUNCHO CASTRO, J. MARTÍNEZ HERNÁNDEZ, *Ecuaciones Algebraicas*,DM, Murcia, 2002.

[4] A. DEL RÍO MATEOS, J.J SIMÓN PINERO, A. DEL VALLE ROBLES, *Álgebra Básica*DM, Murcia, 2006.

[5] P.B. BHATTACHARYA, S.K. JAIN, S.R. NAGPAUL, *Basic abstract algebra*, Cambridge University Press, Cambridge, 1986.

[6] CUSICK, THOMAS W AND STANICA, PANTELIMON, *Cryptographic Boolean functions and applications*, Academic Press, 2017.

[7] POMMERENING, KLAUS, *Fourier Analysis of Boolean Maps–A Tutorial–*, manuscript, 2005.

[8] CARLET, CLAUDE AND CRAMA, YVES AND HAMMER, PETER L, *Boolean Functions for Cryptography and Error-Correcting Codes*, 2010.

[9] MACWILLIAMS, FLORENCE JESSIE AND SLOANE, NEIL JAMES ALEXANDER, *The theory of error correcting codes*, Amsterdam: North-Holland Publishing Company, 1978.

[10] DZUL, HENRY CHIMAL AND VARGAS, JAVIER DIAZ, *La forma normal algebraica de una función booleana*, journal vol 48, pag 47-57, 2009.

[11] COX, DAVID AND LITTLE, JOHN AND OSHEA, DONAL, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*,third edition. Springer. New York. 2007.

[12] CARLET, CLAUDE AND CRAMA, YVES AND HAMMER, PETER L, *Boolean Functions for Cryptography and Error-Correcting Codes*, 2010.

[13] WU, CHUAN-KUN AND FENG, DENGGUO AND OTHERS, *Boolean functions and their applications in cryptography*,Springer , 2016.

[14] CAUICH, JUAN CARLOS KU AND EN CIENCIAS, DOCTOR AND RECILLAS, HORACIO TAPIA, *Comparticion de secretos sobre campos finitos y esquemas de autenticacion sobre anillos de Galois basados en funciones casi bent y bent* , 2012.

[15] CARLET, CLAUDE, *Open problems in mathematics and computational science*, Springer, pag 203-241, 2014.

Rafael E. Gonzalez Pugliese

En este trabajo de grado se propone el estudio de las funciones Booleanas y en especifico las Booleanas tipo bent. Inicialmente se construye una base teórica de conceptos algebraicos y luego se definen las funciones Booleanas. Más adelante se hace un estudio de manera detallada, destacando aspectos y características para así, poder llegar a las de tipo bent, se definen y clasifican características importantes de estas funciones. Por último, se abordan algunas aplicaciones de estas funciones y problemas abiertos relacionados con ellas.

Departamento De Matemáticas

Universidad Del Atlántico