CIMAT Centro de Investigación en Matemáticas, A.C.

CONSTRUCCIÓN DE FUNCIONES BOOLEANAS CON BUENAS PROPIEDADES CRIPTOGRÁFICAS A PARTIR DE CÓDIGOS ALGEBRAICOS

T E S I S

Que para obtener el grado de

Doctor en Ciencias

con Orientación en

Matemáticas Básicas

Presenta

Guillermo Sosa Gómez

Director de Tesis:

Dr. Pedro Luis del Ángel Rodríguez

Dr. Herbert Kanarek Blando

Autorización de la versión final

Guanajuato, Gto., 23 de marzo de 2018

Agradecimientos

Quisiera agradecer:

- Gracias a Dios por brindarme la oportunidad de cerrar este ciclo. Culmino mis estudios de doctorado llevándome en el corazón las múltiples experiencias con las que aprendí a ser una mejor persona a través de la gente con la que tuve el privilegio de interactuar durante este periodo.
- Al Consejo Nacional de Ciencia y Tecnología, por dejar permitir con su apoyo económico mi formación y la de otros jóvenes mexicanos y extranjeros.
- Al Centro de Investigación en Matemáticas, A.C., por brindarme las condiciones optimas para estudiar y su esfuerzo permanente por impartir cursos útiles y de calidad, y por la atención a sus estudiantes. Al Departamento de Servicios Escolares.
- Gracias a mi familia, icono fundamental para alcanzar mis metas, en especial a mis padres y esposa Claudia Vega quien ha sido una persona maravillosa e incondicional.
- A toda la Familia Vega Gutiérrez por dejarme ser parte de esa gran familia y contar con su apoyo.
- Quiero agradecer de manera especial a mis asesores Dr. Herbert Kanarek Blando y Dr. Pedro Luis del Ángel Rodríguez, por todo su apoyo y paciencia durante estos años. Además, de aceptarme para realizar esta tesis doctoral bajo su tutela siendo para mi un honor.
- A un gran ser humano, un profesor, padre y amigo: Dr. Octavio Paez Osuna, por la paciencia y el tiempo infinito que me brindo desde mucho antes de entrar a CIMAT para aclararme dudas y sugerencias.
- A mis compañeros de cubo: Nayelis, Jorge Dávila, Juan, Javier, Hector y Marco por hacer del cubo un lugar agradable.

- A la Revolución Cubana, por los valores que me inculcaron, por darme la oportunidad de tener una excelente educación.
- A mi amada Universidad Central "Marta Abreu"de Las Villas.
- A mi Departamento de Matemáticas en la UCLV, en especial a Lucia, Gerardo, Tamara, Evaristo, Oristela, Antonio y Perfetti.

Abstract

In 2005, [1] Philippe Guillot studied a new form of constructing Boolean functions using linear codes by performing an extension of the construction of Maiorana-McFarland bent functions. We study a class of Boolean functions with cryptographically strong properties in this paper: nonlinearity, propagation criterion, resilient and balance. The construction of cryptographically strong Boolean functions is a daunting task and there is currently a wide range of algebraic and heuristic techniques for constructing such functions, however these methods can be complex, computationally difficult to implement and not always produce a sufficient variety of functions. We present in this paper a construction using algebraic codes.

Índice general

Introducción

0.1 Introducción

Las funciones booleanas aparecen en varias disciplinas científicas incluyendo la Teoría de la Codificación, Combinatoria, Teoría de la Complejidad, Criptografía, Teoría Gráfica, etc. En criptografía, el diseño y análisis de las funciones booleanas que poseen ciertas propiedades han sido a menudo el foco de atención. Además, un terreno productivo de la investigación para la mayoría de estas propiedades criptográficas es el espectro de Walsh-Hadamard, una de las representaciones más utilizadas de la función booleana. Esta tesis hace un análisis de estas propiedades utilizando Teoría de Códigos para construir dichas funciones.

Este capítulo contiene tres partes. En la primera parte, hacemos una breve introducción al tema de las funciones booleanas y énfasis en la necesidad de nuestro objetivo. En la segunda parte, el contenido de los siguientes capítulos de manera resumida. En la última parte, las contribuciones del autor a esta tesis.

0.2 Panorámica de las funciones booleanas

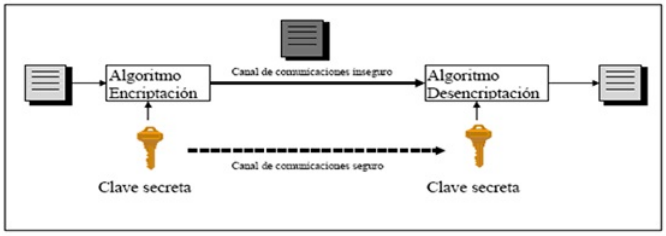
A finales de la década de 1940 en que Claude Shannon [2] publicó los conceptos de confusión y difusión como definiciones fundamentales para lograr una seguridad en los criptosistemas. La confusión se manifiesta en la no linealidad en el interior del criptosistema y del hecho de ocultar la estructura algebraica interna; los sistemas lineales son generalmente fáciles de romper. La difusión se logra mediante poder disipar la estructura estadística del texto en claro en el texto cifrado resultante, además la difusión se relaciona con el criterio de propagación de la función booleana. Las funciones booleanas pueden proporcionar fácilmente confusión y difusión. Un objetivo de esta tesis es la construcción de buenas funciones booleanas para este propósito.

Un importante vínculo entre los criterios de difusión y confusión fue señalado por Meier y Staffelbach. Ellos demostraron que la no linealidad máxima perfecta y los criterios de propagación son requisitos indispensables para las funciones booleanas. Desgraciadamente, las funciones que tienen la difusión y la confusión perfecta (llamadas funciones dobladas, suaves o bent) no son balanceadas; lo que significa que no tienen una distribución de uniforme en la salida. La construcción de funciones booleanas balanceadas que tienen una alta no linealidad y buen criterio de propagación sigue siendo un problema abierto.

La mayoría de los criptosistemas convencionales se interesan por estos principios esenciales: criptosistemas de clave secreta (cifras de bloque y cifrado de flujo), así como funciones de hash.

0.2.1 Criptografía simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma clave tanto para cifrar como para descifrar.



Existe una clasificación de este tipo de criptografía en tres familias, la criptografía simétrica de bloques (block cipher), la criptografía simétrica de flujo (stream cipher) y la criptografía simétrica de resumen (hash functions).

El sistema criptográfico simétrico más conocido DES (Data Encryption Standard) es un sistema criptográfico que toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, con una clave de 56 bits. Este sistema fue tomado como estándar y ha sido uno de los más conocidos, usados y estudiados. Los cifradores de flujo o stream ciphers, son usados donde se cuenta con un ancho de banda restringido, este

tipo de cifradores tiene la característica de ser muy rápido. Los algoritmos más conocidos de este tipo están RC-4, SEAL y WAKE.

Entre los ataques más potentes a la criptografía simétrica están el criptoanálisis diferencial y lineal.

0.2.2 Funciones hash

Una herramienta fundamental en la criptografía son las funciones hash, son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen. Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar pueden ser en general demasiado grandes la función hash les asocia una cadena de longitud 160 bits que son más manejables para el propósito de firma digital. Las funciones hash (o primitivas hash) pueden operar como: **MDC**(Modification Detection Codes) ó **MAC**(Message Authentication Codes).

0.2.2.1 Funciones hash rápidas

Para aprovechar al máximo la tecnología para obtener hash rápidas, hay que ser capaz de diseñar funciones booleanas criptográficamente fuertes en muchas variables que se puede evaluar más rápido usando evaluaciones parciales de las rondas anteriores. En el campo de investigación de las funciones hash se ha introducido una nueva clase de funciones booleanas cuya evaluación es especialmente eficiente y las llaman rotación simétrica.

Teorema 0.2.1. *La clase de funciones de rotación-simétrica incluida en el conjunto de las funciones booleanas* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *tales que* $f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$*, donde* $y_{i+1} = x_i, \forall i = 1, \ldots, n-1$ *y* $y_1 = x_n$ *y podemos escribir a* $f(y) = g_1(x_1, \ldots, x_{n-1}) \oplus y_1 g_0(x_1, \ldots, x_{n-1})$

0.2.3 Ejemplo

Consideremos algunos ejemplos.

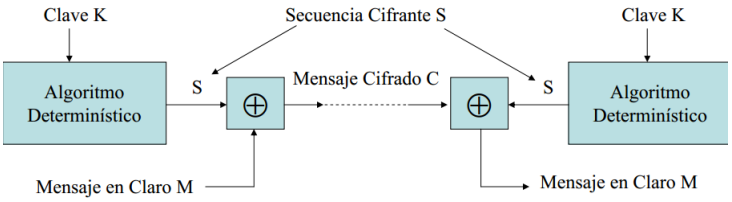
Ejemplo 0.2.2 (1). Sea la función f una de las funciones usadas en MD4. Definida como $f(x_1, x_2, x_3) = x_1x_2 \oplus \overline{x_1}x_3 = x_1x_2 \oplus x_1x_3 \oplus x_3$. Si aplicamos la rotación $y_2 = x_1, y_3 = x_2, y_1 = x_3$ entonces $f(y) = y_2y_3 \oplus y_1y_2 \oplus y_1$. La evaluación de $f(y)$ no puede ser apoyada por evaluaciones parciales de $f(x)$ al máximo.

Ejemplo 0.2.3 (2). Sea la función f definida como $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$. Si aplicamos la rotación $y_2 = x_1, y_3 = x_2, y_1 = x_3$ entonces $f(y) = y_2y_3 \oplus y_3y_1 \oplus y_1y_2$, o sea, $f(x) = f(y)$. Observemos que $f(x) = x_1x_2 \oplus x_3(x_1 \oplus x_2)$ y el valor de $f(y) = x_1x_2 \oplus y_1(x_1 \oplus x_2)$, o sea, que se aprovecha las evaluaciones parciales de x_1x_2 y $x_1 \oplus x_2$

Actualmente dentro de las mejoras que tiene la familia MD es la introducción de este tipo de funciones.

0.2.4 LFSR

El cifrado en flujo es la única solución factible para optimizar el recurso tiempo. Entre las características que se le exigen a una secuencia pseudoaleatoria para ser de utilidad criptográfica destaca la de una alta complejidad lineal. Por eso se hace necesario que a las secuencias generadas con un simple registro de desplazamiento con realimentación lineal (RDRL) se les aplique una transformación no lineal conocida con el nombre de filtrado no lineal.



0.2.4.1 Generadores con registros de desplazamientos

Actualmente en el entorno criptográfico encontrar más generadores que utilizan LFSR, que los que utilizan NLFSR, se ha convertido en algo habitual. La principal característica que influye en la poca utilización de un NLFSR es que resulta difícil de analizar. Es por lo que muchos diseñadores de generadores de secuencia prefieren evitar este tipo de modelo. Estas características son también válidas en el caso de los filtrados no

lineales sobre LFSRs, debido a la utilización de funciones no lineales para el proceso de obtención de bits. Mientras que, por otro lado, por las buenas propiedades estadísticas de los registros de desplazamiento lineales como generadores pseudoaleatorios, estos han sido empleados frecuentemente en el diseño de cifrados de flujo, combinados con alguna función de complejidad no lineal.

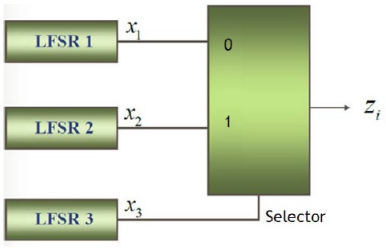
0.2.4.2 Ejemplo

Generador basado en combinaciones no lineales. En estas estructuras, las salidas de los LFSRs constituyen las entradas a la función no lineal. Como ejemplo más representativo de este grupo se analizará el generador de Geffe.

Generador Geffe

Consiste en una combinación de tres registros de desplazamiento donde el tercero de ellos LFSR3 actúa como selector. Las secuencias de LFSR1 y LFSR2, x_1 y x_2, respectivamente, se combinan de forma aleatoria mediante un conmutador(multiplexer) que selecciona una u otra secuencia en función de los bits de $x_3(t)$, secuencia generada por LFSR3, si x_3 es un 1, se selecciona el bit del LFSR2, si es 0 se selecciona el bit del LFSR1. En la forma algebraica normal, la secuencia de salida puede expresarse como,

$z_i = x_1 \oplus x_3x_1 \oplus x_3x_2$



0.2.5 S-cajas

Las cajas de substitución (S-cajas) constituyen la piedra angular en criptografía para lograr que los cifradores por bloque exhiban la ineludible propiedad de no linealidad. En efecto, si la o las S-cajas de un determinado

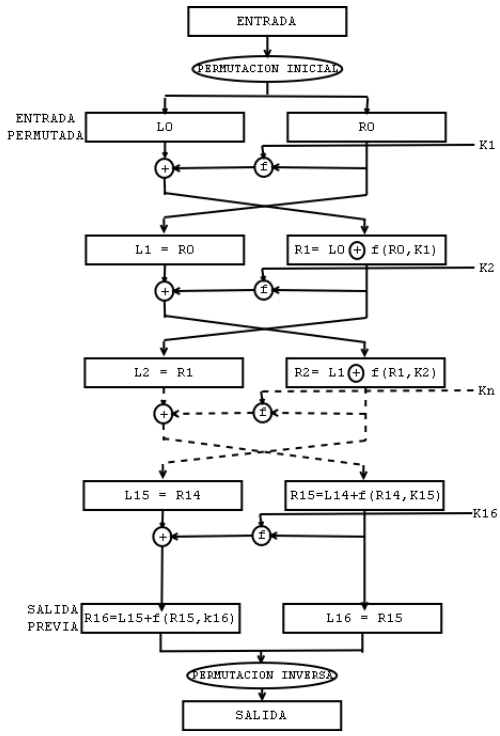
cifrador por bloque no alcanzan una alta no linealidad, entonces se considera que tal algoritmo no podrá ofrecer una seguridad adecuada para impedir que información confidencial pueda ser develada por entidades no autorizadas [3].

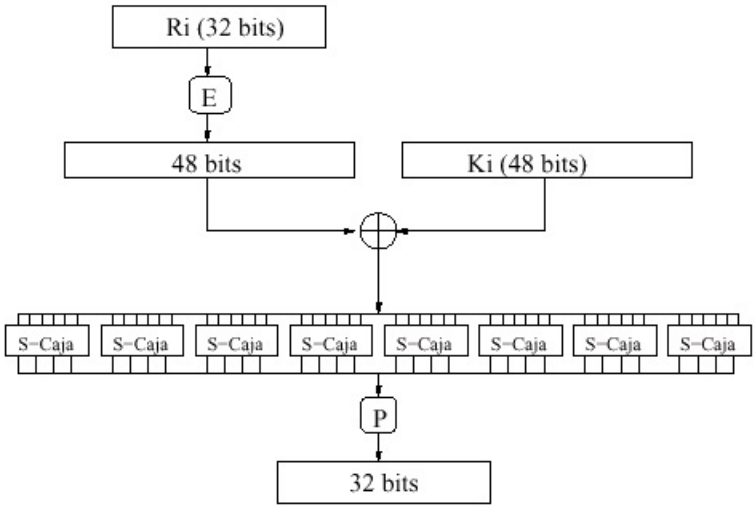
Formalmente, una S-caja es una función o correspondencia de n bits de entrada a m bits de salida, $S : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$, esto es, una S-caja puede ser vista como una función booleana de n bits de entrada y m bits de salida. Cuando $n = m$ la función es reversible y por lo tanto biyectiva. Sin embargo, en muchas ocasiones las S-cajas de los cifradores por bloque no son biyectivas. Por ejemplo, como se describe en la siguiente sección, el estándar de cifrado de datos (DES por sus siglas en inglés) emplea S-cajas en las cuales el número de bits de entrada (seis) es mayor que el número de bits de salida (cuatro). [3]

0.2.5.1 Ejemplo

Data Encryption Standard (DES)

El algoritmo DES cifra un bloque de 64 bits (8 bytes) de texto en claro en un bloque de 64 bits de texto cifrado. Para ello usa una clave externa de 64 bits en los que los bits en las posiciones octavas de cada byte son bits de paridad impar. Consta de 16 iteraciones, y en cada una de ellas se realizan operaciones de o exclusivo, permutaciones y sustituciones. Las permutaciones son de tres tipos: simples, expandidas (se duplican bits) y restringidas (se eliminan bits).





0.3 Contenido de la tesis

A medida que las redes informáticas se desarrollan, utilizar canales públicos para transmitir información segura de un cliente a otro se hace cada vez más importante. El texto cifrado depende de los algoritmos de cifrado. El propósito del estudio de las funciones booleanas y sus propiedades criptográficas es proporcionar

funciones booleanas que apoyen los protocolos de la computadoras y los algoritmos de seguridad de red. La tesis se divide en cinco capítulos y dos anexos, este es el primer capítulo. Hemos tratado de escribir la tesis que sea fácil de leer con un enfoque sistemático.

En el capítulo 1, revisamos el desarrollo del estudio de las funciones booleanas en la criptografía, definiciones principales como el peso y la distancia de Hamming. A continuación, las definiciones generales de las propiedades de las funciones booleanas, tales como balanceo, no linealidad, inmunidad de correlación y criterio de propagación. Además, como las matrices de Hadamard y la transformada de Walsh-Hadamard juegan un papel muy importante en la búsqueda de estas propiedades.

Se analiza la construcción de Maiorana-McFarland(MM), que se utilizará para encontrar las funciones booleanas requeridas. Se describe de manera profunda la vinculación entre las propiedades criptográficas y dicha construcción.

Además, se describe de manera sintética todo lo relacionado con los códigos de Goppa y de Reed-Solomon, en particular, con los códigos hermitianos que se utilizó en la construcción de MM.

En el capítulo 2, se describe toda la propuesta de nuestro trabajo que se resumirá en la próxima sección.

En los anexos A se refiere lo concerniente a la teoría campo de funciones algebraicas pero se tratan como anexo para que todo aquel que vaya a dar lectura a esta tesis y necesite refrescar algunos conceptos tomen como referencia este anexo.

0.4 Contribuciones de la tesis

En el capítulo 2, el autor realiza una descripción exhaustiva de la construcción de MM y de la función π donde se analiza tres casos fundamentales, o sea, se profundiza los casos donde el espacio de las fibras de π es un subespacio afín de dimensión cero, uno y dos. Este último no descrito con anterioridad en ningún artículo revisado. También, se realiza una descripción completa de como debe de elegirse las imágenes de π y h para construir las bien deseadas funciones booleanas.

Se revisa con detenimiento las propiedades criptográficas deseables dada la construcción escogida y describimos las ventajas y desventajas de dicha construcción. Fijamos cuales van a hacer los parámetros óptimos para encontrar las funciones booleanas. Así, se podrá saber cuando las funciones van a hacer balanceadas, que orden de criterio de propagación va a tener, se podrá saber cual es la No linealidad y el orden de resistencia. También es importante señalar que se obtiene un factor no trivial en cuanto al número de funciones distintas obtenidas con las mismas propiedades.

Todo lo anterior, se podrá conocer de antemano por las características y propiedades del código hermitiano que se utilice conforme a la función que se quiera construir de n- variables.

Preliminares

1.1 Funciones booleanas

Es objetivo para nosotros mostrar los principios matemáticos que se utilizan en el problema de búsqueda de funciones booleanas con muy alta no linealidad y otras propiedades criptográficas necesarias para su aplicación en la criptografía de clave simétrica para alcanzar confusión. Por ejemplo, la implementación de una caja de sustitución o S-cajas necesita funciones booleanas no lineales para resistir ataques tales como el criptoanálisis lineal y el diferencial. La construcción de funciones boooleanas criptográficamente fuertes es una tarea ardua. Actualmente, existe una amplia gama de técnicas algebraicas y heurísticas para construir tales funciones, sin embargo estos métodos pueden ser complejos, computacionalmente difíciles para su implementación y no siempre producen una variedad suficiente de funciones.

1.1.1 Definición

Sea $\mathbb{F}_2^n$ el espacio vectorial de dimensión n sobre el campo finito $\mathbb{F}_2$. Para dos vectores a,$b \in \mathbb{F}_2^n$, nosotros definimos el producto escalar $a \cdot b = (a_1 b_1 \oplus \ldots \oplus a_n b_n)$ y la suma $a \oplus b = (a_1 \oplus b_1, \ldots, a_n \oplus b_n)$, dónde la multiplicación y suma $\oplus$ (llamada XOR) son sobre $\mathbb{F}_2$.

Definición 1.1.1. Una función booleana f de n variables es una aplicación que va de $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. El conjunto $\mathcal{B}_n$ de todas las funciones booleanas de n variables es un espacio vectorial sobre $\mathbb{F}_2$ con la adición $\oplus$ dada por $(f \oplus g)(x) = f(x) \oplus g(x)$, para $f, g \in \mathcal{B}_n$.

Definición 1.1.2. Cada función booleana $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ tiene asociada su forma polar o función signo, denotada por $\hat{f} : \mathbb{F}_2^n \longrightarrow \{-1, 1\}$ y definida por $\hat{f}(x) = (-1)^{f(x)}$.

Recordemos que hay una biyección entre los elementos de $\mathbb{F}_2^n = \{0, 1, \ldots, 2^n - 1\}$ y $\mathbb{F}_2^n$ dado por:

Si $j = c_{n-1}2^{n-1} + \ldots + c_1 2 + c_0 \in \{0, 1, \ldots, 2^n - 1\}$ con $c_n \in \mathbb{F}_2$, entonces $v_j = \{c_{n-1}, \ldots, c_1, c_0\}$.

1.1.2 Formas de representación de las funciones booleanas

1. La **Tabla de Verdad** de una función booleana f es una tabla unidimensional, indexada por los elementos de $\mathbb{F}_2^n$ (en el orden lexicográfico), o sea, es la secuencia de $(0, 1)$ definida por $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$ es llamada tabla de verdad de f, donde $v_0 = (0, \ldots, 0, 0), v_1 = (0, \ldots, 0, 1), \ldots, v_{2^n-1} = (1, \ldots, 1, 1)$.

2. La **Tabla de Verdad Polar** es la secuencia $(1, -1)$ de f que esta definida por $\left((-1)^{f(v_0}, \ldots, (-1)^{f(v_{2^n-1}}\right)$

3. Una función booleana en $\mathbb{F}_2^n$ puede ser expresada como un polinomio en $\mathbb{F}_2 [x_1, \ldots, x_n] / \left(x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n\right)$ de manera única a través de una **forma normal algebraica**(FNA), es decir,

$$f(x) = \sum_{a \in \mathbb{F}_2^n} c_a x_1^{a_1} \cdots x_n^{a_n}, \tag{1.1}$$

donde $c_a \in \mathbb{F}_2$ y $a = (a_1, \ldots, a_n)$. Siendo, $c_a = \sum_{x \leq a} f(x)$, donde $x \leq a$ significa que $x_i \leq a_i, \forall, 1 \leq i \leq n$. O sea, $c_a = g(a_1, \ldots, a_n)$, g es una función de $\mathbb{F}_2^n$ y es llamada la Transformación de Möbius de f, denotada por $g = \mu(f)$

4. Representación en términos de la función **Traza**: En la teoría de campos finitos, la función traza en el campo finito $\mathbb{F}_{p^n}$ es la función $Tr : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$ definido por $Tr(x) = x + x^p + x^{p^2} + x^{p^3} + \ldots + x^{p^{n-1}}$.

Cada función booleana puede ser escrita en la forma $f(x) = Tr(F(x))$, donde $F(x)$ es un mapeo de $\mathbb{F}_{2^n}$ en $\mathbb{F}_{2^n}$.

1.1.2.1 Ejemplos de formas de representación de las funciones booleanas

Ejemplo 1.1.3. Sea $f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ definida por:

$f(x) = x_2x_1 + x_3x_1 + x_3x_2$.

Calculemos la Tabla de Verdad de esta función

x_1	x_2	x_3	$f(x)$
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	1
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	1

Ejemplo 1.1.4. Denotemos por $TT(f)$ la tabla de verdad de f. La forma normal algebraica de una función booleana f es una transformación lineal definida por $f = A_n \cdot TT(f)$, donde:

$$A_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes A_{n-1} = \begin{bmatrix} A_{n-1} & 0 \\ A_{n-1} & A_{n-1} \end{bmatrix}, A_0 = 1$$

Donde n es el número de variables de la función booleana, y $\otimes$ denota la multiplicación tensor (kronecker) de una matriz

Dada la tabla de verdad $TT(f) = [0, 1, 0, 0, 0, 1, 0, 1]$ de una función booleana f, obtener su expresión FNA:

Primero se obtiene A_n, sabemos que la longitud de la tabla de verdad es 8, por lo que se deduce que $n = 3$ y posteriormente se determina la matriz en la forma:

$$A_0 = 1 \longrightarrow A_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \longrightarrow A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \longrightarrow A_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

De tal modo que ahora se necesita calcular la columna de coeficientes f:

$$f = A_n \cdot TT(f) = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Términos	TT(f)	c_a
1	0	0
x_1	1	1
x_2	0	0
x_1x_2	0	1
x_3	0	0
x_1x_3	1	0
x_2x_3	0	0
$x_1x_2x_3$	1	1

Entonces, $f(x_1, x_2, x_3) = x_1 \oplus x_1x_2 \oplus x_1x_2x_3$

1.1.3 Definiciones básicas

Definición 1.1.5. Llamamos **soporte de f**, y escribimos $Sop(f)$, al conjunto de vectores de $\mathbb{F}_2^n$ cuya imagen por f es 1, es decir, $Sop(f) = \{v_i \in \mathbb{F}_2^n \mid f(v_i) = 1\}$.

Definición 1.1.6. Si $f \in \mathcal{B}_n$, llamamos **peso de f**, y escribimos $w(f)$, al número de 1 de su tabla de verdad; por tanto, $w(f) = card(Sop(f))$.

Definición 1.1.7. Decimos que una función $f \in \mathcal{B}_n$ es **balanceada** si su tabla de verdad contiene el mismo número de 0 que de 1, es decir, si $w(f) = 2^{n-1}$.

Definición 1.1.8. Decimos que $f \in \mathcal{B}_n$ es una **función afín** si podemos escribirla como $f(x) = a \cdot x \oplus b$ para algún $a \in \mathbb{F}_2^n$ y algún $b \in \mathbb{F}_2$. Si $b = 0$, decimos que f es una función lineal. Al conjunto de las funciones afines de $\mathbb{F}_2^n$ a $\mathbb{F}_2$ lo denotamos por $\mathcal{A}_n$.

Definición 1.1.9. Sean $f, g \in \mathcal{B}_n$. Llamamos **distancia entre f y g**, y escribimos $d(f, g)$, al peso de la función $f \oplus g$, es decir, $d(f, g) = w(f \oplus g)$.

Definición 1.1.10. Llamamos **No linealidad** de una función $f \in \mathcal{B}_n$, y escribimos $\mathcal{N}_f$, al mínimo de las distancias entre f y cualquier función afín, es decir, $\mathcal{N}_f = min\{d(f,\varphi) \mid \varphi \in \mathcal{A}_n\}$.

1.1.4 Transformada de Walsh-Hadamard(TWH)

Definición 1.1.11. La **transformada de Walsh-Hadamard** de una función $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ es una aplicación $H(f) : \mathbb{F}_2^n \to \mathbb{Z}$, definida por

$$H(f)(h) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{h \cdot x}. \tag{1.2}$$

Teorema 1.1.12. *Sea $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ y $H(f)$ la transformada de Walsh-Hadamard. Sea S un subespacio arbitrario de $\mathbb{F}_2^n$ y sea $S^\perp$ el dual(aniquilador) de S, es decir, $S^\perp = \{x \in \mathbb{F}_2^n : x \cdot s = 0, \forall s \in S\}$*

Entonces,

$$\sum_{u \in S} H(f)(u) = 2^{dimS} \sum_{u \in S^\perp} f(u). \tag{1.3}$$

Ver demostración en [4]

1.1.5 Matrices de Hadamard

Una **matriz de Hadamard** de orden n es una matriz de $n \times n$ de entradas ± 1 tal que $HH^t = nI_n$.

La forma de construirse las matrices de Hadamard:
$H_0 = (1); H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$, es decir, H_n es el producto de Kronecker $H_n = H_1 \otimes H_{n-1}$

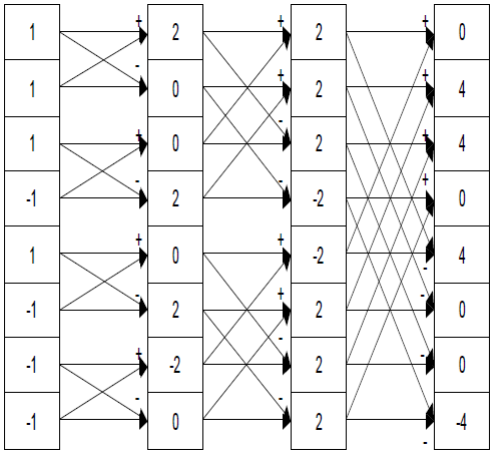
Nosotros podemos expresar la transformada de Walsh-Hadamard en términos de las matrices de Hadamard H_n, o sea, $H(f) = f \cdot H_n$. [4]

1.1.6 Transformada rápida de Walsh-Hadamard

Nótese que un cálculo directo del espectro de Walsh-Hadamard completo implica una complejidad de N^2 *pasos*, *con* $N = 2^n$. Sin embargo, tal y como ocurre con la transformada rápida de Fourier, es posible definir un procedimiento rápido para el cálculo de la transformada de Walsh-Hadamard que puede ser computado con únicamente $N \cdot \log(N)$ pasos. Para lograr esa aceleración, la transformada rápida de Walsh-Hadamard (TRWH) utiliza el concepto de diagrama de mariposa. Un diagrama de mariposa de tamaño 2 (el tamaño más pequeño), toma dos bits de entrada, (x_0, x_1), y produce dos bits de salida (y_0, y_1), de la siguiente manera [3]:

$$\begin{aligned} y_0 &= x_0 + x_1 \\ y_1 &= x_0 - x_1 \end{aligned} \tag{1.4}$$

Veamos un ejemplo para $n = 3$



1.1.7 Ecuación de Parseval

De la definición de la transformada de Walsh-Hadamard se deduce que $H(\hat{f})(u)$ es igual al número de ceros menos el número de unos en el vector binario $f \oplus l_u (l_u \in \mathcal{A}_n)$,o sea, $l_u(v) = \sum_{i=1}^{n} u_i \cdot v_i)$ y tal que

$$H(\hat{f})(u) = 2^n - 2d(f, \sum_{i=1}^{n} u_i \cdot v_i) \tag{1.5}$$

$$d(f, \sum_{i=1}^{n} u_i \cdot v_i) = \frac{1}{2}(2^n - H(\hat{f})(u)) \tag{1.6}$$

$$d(f, 1 \oplus \sum_{i=1}^{n} u_i \cdot v_i) = \frac{1}{2}(2^n + H(\hat{f})(u)) \tag{1.7}$$

Resumiremos estos resultados anteriores en el siguiente teorema

Teorema 1.1.13. *La No linealidad de f es determinado por la transformada de Walsh-Hadamard de f, es decir,*

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |H(\hat{f})(u)| \tag{1.8}$$

1.1.8 Propiedades criptográficas de las funciones booleanas

Los siguientes factores son importantes en el diseño de funciones booleanas con buenas propiedades criptográficas [3]:

1. **Balance**: Una función booleana de n-variables f se dice ser balanceada si $w(f) = 2^{n-1}$. Esta propiedad es deseable para evitar ataques criptodiferenciales tales como los introducidos por A. Shamir contra el algoritmo DES.

2. **No linealidad**: Esta propiedad reduce el efecto de los ataques por criptoanálisis lineal. Como se discutió antes, la No linealidad de una función booleana puede ser calculada directamente de la transformada de Walsh-Hadamard(ver teorema 1.1.13).

3. **Grado algebraico**: Una función booleana f puede ser representada como un polinomio multivariable sobre $\mathbb{F}_2$. Este polinomio es llamado la forma normal algebraica(FNA) de f descrito en la primera

sección de este apartado. Es fácil ver que el grado algebraico máximo de una función balanceada de n-variables es $n-1$.

4. **Inmunidad de correlación**: Una función booleana de n-variables se dice tener inmunidad de correlación de orden l si y solo si $H(\hat{f})(u) = 0$, para todo u con $1 \leq w(u) \leq l$. Una función booleana con orden de inmunidad de correlación l y balanceada es llamada l-resistente. Existe una relación fundamental entre el número de variables n, el grado algebraico d y el orden de inmunidad de correlación l de una función: $l + d \leq n$.

5. **Autocorrelación**: Este valor es proporcional al desbalance de todas las derivadas de primer orden de la función booleana. Valores pequeños son considerados como buenos mientras que un valor grande es considerado un símbolo de debilidad.

   Se define la función de autocorrelación $r_{\hat{f}}(s)$, de una función booleana f a partir de su representación polar como:

   $$r_{\hat{f}}(s) = \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)\hat{f}(x \oplus s)$$

   Además, existen otras propiedades importantes de las funciones booleanas que se usan en las S-cajas.

6. **Criterio de propagación**: Una función booleana tiene criterio de propagación de orden k(PC(k)) si $f(x) \oplus f(x \oplus u)$ es balanceada para toda u con $1 \leq w(u) \leq k$.

7. **Efecto avalancha**(SAC): Está relacionado con la autocorrelación y se define con respecto a un bit específico de entrada tal que al complementarlo resulta en un cambio en el bit de salida con una probabilidad de 1/2. El criterio de avalancha estricto (SAC por sus siglas en inglés), requiere los efectos avalancha de todos los bits de entrada. Una función booleana f se dice que satisface SAC si $f(x) \oplus f(x \oplus u)$ es balanceada para toda u con $w(u) = 1$.

1.1.8.1 Ejemplos

Ejemplo 1.1.14. Sea $f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ definida por:

$f(x) = x_2x_1 + x_3x_1 + x_3x_2$.

Calculemos la tabla de verdad, polar y transformada de Walsh-Hadamard polar de esta función

x_1	x_2	x_3	$f(x)$	$\hat{f}(x)$	$H(\hat{f}(x))$
0	0	0	0	1	0
1	0	0	0	1	4
0	1	0	0	1	4
1	1	0	1	-1	0
0	0	1	0	1	4
1	0	1	1	-1	0
0	1	1	1	-1	0
1	1	1	1	-1	-4

Es balanceada y $\mathcal{N}_f = 2$.

Ejemplo 1.1.15. Veamos ahora una función de 3-variables que satisface el criterio estricto de avalancha(SAC).

Entrada	000	001	010	011	100	101	110	111
Salida	1	1	1	0	0	1	1	1

Calculando su FNA nos da $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3$

Una función f cumple SAC si $f(x) \oplus f(x \oplus a)$, con $w(a) = 1$, es balanceada.

Veamos que el conjunto de las a que cumplen que su peso es 1 son $\{001, 010, 100\}$.

Es desbalanceada y $\mathcal{N}_f = 2$.

Calculemos la tabla de verdad para $f(x) \oplus f(x \oplus a)$ para $a = 001$

x_1	x_2	x_3	$f(x)$	$f(x \oplus 001)$	$f(x) \oplus f(x \oplus 001)$
0	0	0	1	1	0
1	0	0	1	1	0
0	1	0	1	0	1
1	1	0	0	1	1
0	0	1	0	1	1
1	0	1	1	0	1
0	1	1	1	1	0
1	1	1	1	1	0

Como se puede observar $f(x) \oplus f(x \oplus 001)$ es balanceada. Este mismo proceso se hace para las demás a y se comprueba que f satisface el SAC.

Ejemplo 1.1.16. Veamos ahora una función de 3-variables que presenta inmunidad de correlación de orden 1.

Entrada	000	001	010	011	100	101	110	111
Salida	1	1	1	0	0	1	1	1

Calculando su FNA nos da $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3$

Una función f tiene inmunidad de correlación de orden 1 si:

$$H(\hat{f})(h) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus h \cdot x} = 0, \ con \ w(h) = 1 \tag{1.9}$$

Veamos que el conjunto de las h que cumplen que su peso es 1 son $\{001, 010, 100\}$.

Construyamos la tabla correspondiente para ver si cumple con este criterio.

Calculemos la tabla de verdad, forma polar y la transformada de Walsh-Hadamard de la forma polar

x_1	x_2	x_3	$f(x)$	$\hat{f}(x)$	$H(\hat{f}(x))$
0	0	0	1	-1	-4
1	0	0	1	-1	0
0	1	0	1	-1	0
1	1	0	0	1	4
0	0	1	0	1	0
1	0	1	1	-1	-4
0	1	1	1	-1	-4
1	1	1	1	-1	0

Como se puede observar la transformada da cero en los h con peso 1.

1.2 Construcción de Maiorana-McFarland

Las funciones booleanas son una poderosa herramienta para modelar una gran cantidad de procesos de interés en la lógica, la ingeniería, la ciencia o las matemáticas. La utilidad de una función booleana en las aplicaciones criptográficas depende de una buena combinación de las anteriores propiedades mencionadas. Desgraciadamente, una función booleana no puede satisfacer a la vez todas las propiedades plenamente.

1.2.1 Definiciones preliminares

La construcción de **Maiorana-McFarland**(MM) fue originalmente diseñada para construir funciones dobladas y también ha sido extendida para construir funciones resistentes [1].

Para $n \geq 2$ un entero, sea $\mathbb{F}_2^n = E \oplus F$ una descomposición en dos subespacios vectoriales complementarios: E de dimensión p y F de dimensión $q = n - p$.

Para cualquier aplicación $\pi : E \longrightarrow \mathbb{F}_2^n$ y cualquier aplicación $h : E \longrightarrow \mathbb{F}_2$ la construcción Maiorana-McFarland(MM) define una función booleana f como sigue:

$$\begin{array}{rccl} f: & E \oplus F & \longrightarrow & \mathbb{F}_2 \\ & x + y & \mapsto & \pi(x) \cdot y + h(x), \end{array}$$

- La aplicación π está definida sobre $\mathbb{F}_2^n$, pero como $\pi(x)$ está multiplicada por un producto interno con un elemento de F, el valor de f es invariante cuando $\pi(x)$ es trasladado por cualquier vector de $F^\perp$, donde $F^\perp$ se define más adelante.

- Así, podríamos considerar que π esta definida sobre el espacio $\mathbb{F}_2^n / F^\perp \simeq E^\perp$.

- Para cualquier subespacio vectorial $p - dimensional$ E de $\mathbb{F}_2^n$, el dual de E, denotado por $E^\perp$, es el

espacio vectorial $(n-p)-$ *dimensional* de los vectores que se anulan en E.

$$E^{\perp} = \{u \in \mathbb{F}_2^n | \forall x \in E, u \cdot x = 0\}$$

Con el fin de establecer las propiedades de correlación de la función de f, la siguiente proposición expresa la transformada de Walsh-Hadamard.

Proposición 1.2.1. *[1] Para cualquier $w \in \mathbb{F}_2^n$, sea $w = u + v$ la única descomposición de w en la suma directa $E^{\perp} \oplus F^{\perp}$ con $u \in E^{\perp}$ y $v \in F^{\perp}$; entonces*

$$H(\hat{f})(u+v) = 2^q \sum_{x \in \pi^{-1}(u)} (-1)^{h(x)+v\cdot x} \tag{1.10}$$

Demostración:

Por definición de la transformada de Walsh-Hadamard, para cualquier $w \in \mathbb{F}_2^n, w = u + v$

$$H(\hat{f})(w) = \sum_{(x,y) \in E \times F} (-1)^{\pi(x)\cdot y + h(x) + w\cdot(x+y)}$$

$$= \sum_{x \in E} (-1)^{h(x)+w\cdot x} \sum_{y \in F} (-1)^{(\pi(x)+w)\cdot y}$$

La última sumatoria es igual a $|F| = 2^q$ si $\pi(x) + w \in F^{\perp}$ y 0 en otro caso. Por lo tanto, los únicos términos no cero en la suma son donde $\pi(x) \in w + F^{\perp}$. Como $x \in E$ en la suma, $w \cdot x = u \cdot x + v \cdot x = v \cdot x$. Por lo que, $\pi(x) \in w + F^{\perp} \Leftrightarrow x \in \pi^{-1}(u)$ y así queda demostrado. Veamos esto,

$\pi(x) \in w + F^{\perp} \Leftrightarrow x \in \pi^{-1}(u)$

$\Rightarrow$

Recordemos que π esta definida sobre el espacio $\mathbb{F}_2^n/F^{\perp}$, el cual es isomorfo a $E^{\perp}$, o sea, $\pi(x) \in E^{\perp}$

Hipótesis $\pi(x) \in w + F^{\perp}$

Como $w = u + v$ con $u \in E^{\perp}$ y $v \in F^{\perp} \Rightarrow \pi(x) \in u + v + F^{\perp} \Rightarrow \pi(x) \in u + F^{\perp}$

$\Rightarrow \pi(x) = u + f'$ pero como $\pi(x) \in E^{\perp} \Rightarrow u + f' \in E^{\perp}$ como $u \in E^{\perp} \Rightarrow f' \in E^{\perp}$ y

$f' \in F^{\perp} \Rightarrow f' = 0 \Rightarrow \pi(x) = u \Rightarrow x \in \pi^{-1}(u)$

$\Leftarrow$

Hipótesis $x \in \pi^{-1}(u)$

$x \in \pi^{-1}(u) \Rightarrow \pi(x) = u = w + v \in w + F^{\perp}$

■

Con el fin de estudiar la propiedad de resistencia, nos interesa el caso donde la transformada de Walsh-Hadamard es cero. Esto ocurre en dos casos: si $\pi^{-1}(u) = \emptyset$ ó si la función $x \mapsto h(x) + v \cdot x$ es balanceada en el subconjunto $\pi^{-1}(u)$ de E. Esta última propiedad no es fácil de verificar en general. Un caso particular interesante es cuando $\pi^{-1}(u)$ es un subespacio afín de E.

Proposición 1.2.2. *[1] Sea $u \in E^{\perp}$, si la preimagen $\pi^{-1}(u)$ es un subespacio afín de E definida por el subespacio V_u y el elemento x_u, entonces, $\forall v \in F^{\perp}$,*

$$H(\hat{f})(u+v) = 2^q (-1)^{v \cdot x_u} H(\hat{h_u})(v),$$

donde h_u denota la función booleana definida por $t \mapsto h(t + x_u)$.

Demostración:

Hacemos la sustitución $x = t + x_u$ en la suma de la expresión de la proposición 1.2.1, o sea,

$$H(\hat{f})(u+v) = 2^q \sum_{x \in \pi^{-1}(u)} (-1)^{h(x)+v \cdot x} = 2^q \sum_{x \in \pi^{-1}(u)} (-1)^{h(t+x_u)+v \cdot (t+x_u)} \tag{1.11}$$

$$= 2^q \sum_{x \in \pi^{-1}(u)} (-1)^{h(t+x_u)+v \cdot t + v \cdot x_u} \tag{1.12}$$

$$= 2^q (-1)^{v \cdot x_u} \sum_{x \in \pi^{-1}(u)} (-1)^{h(t+x_u)+v \cdot t} = 2^q (-1)^{v \cdot x_u} H(\hat{h_u})(v)$$

■

Veamos que Guillot en [1] asume que $\pi^{-1}(u)$ es un subespacio afín de E de dimensión 0 ó 1. O sea, como sabemos hay un único subespacio vectorial de dimensión 0, el $\{0\}$. Cualquier punto $x_u \in E$ traslada al $\{0\}$,

$\{x_u\} = x_u + \{0\}$, así decimos que x_u es un subespacio afín de dimensión 0. Igualmente, si desplazamos una recta vectorial tenemos una recta afín, o sea, tenemos a V_u un subespacio vectorial de dimensión 1, por lo que, $x_u + \langle V_u \rangle$ es un subespacio afín de dimensión 1,es decir, $x_u + V_u = \{x_u + t : t \in V_u\}$

1.2.2 Autocorrelación

A fin de establecer propiedades de propagación de la función f, la siguiente proposición expresa la función de autocorrelación.

Proposición 1.2.3. *Para cualquier $z \in \mathbb{F}_2^n$, sea $z = x + y$ la única descomposición de z en la suma directa $E \oplus F$ con $x \in E$ e $y \in F$.*

$$r_f(x+y) = 2^q \sum_{t \in E | \pi(t)+\pi(t+x) \in F^\perp} (-1)^{h(t)+h(t+x)+\pi(t+x)\cdot y} \tag{1.13}$$

Demostración:

$$r_f(x+y) = \sum_{(t,s)\in E\times F} (-1)^{\pi(t)\cdot s + h(t)+\pi(t+x)\cdot(s+y)+h(t+x)}$$

$$= \sum_{t\in E} (-1)^{h(t)+h(t+x)+\pi(t+x)\cdot y} \sum_{s\in F} (-1)^{(\pi(t)+\pi(t+x))\cdot s}$$

La última suma es igual $|F| = 2^q$ si $\pi(t)$ y $\pi(t+x)$ pertenecen a la misma $F^\perp-$ clase lateral, y 0 en otro caso.

■

En particular para cualquier $y \in F$,

$$r_f(y) = 2^q \sum_{t\in E} (-1)^{\pi(t)\cdot y}.$$

Tomando $u = \pi(t)$, para cualquier $y \in F$,

$$r_f(y) = 2^q \sum_{t \in E} (-1)^{\pi(t) \cdot y} \tag{1.14}$$

$$r_f(y) = 2^q \sum_{u \in E^\perp} \psi(u)(-1)^{u \cdot y} \tag{1.15}$$

donde, para cualquier $u \in E^\perp$, el valor $\psi(u)$ es el número de elementos de la preimagen $\pi^{-1}(u)$.

1.2.3 Construcciones prácticas de π

Las subsecciones 1 y 2 fueron estudiadas y vistas por Guillot en [1]

1.2.3.1 π es uno a uno

Asumimos que para cualquier $u \in E^\perp$, la preimagen $\pi^{-1}(u)$ contiene a lo sumo un elemento. Esto es solo posible si $2^q =\mid E^\perp \mid \geq \mid E \mid = 2^p \Rightarrow p \leq q$. Si la preimagen es no vacía, entonces el espacio vectorial V_u de la proposición 1.2.2 es siempre el espacio vectorial nulo y $H(\hat{h_u})(u) = \pm 1$. Consecuentemente, $\forall (u, v) \in E^\perp \times F^\perp$

$$H(\hat{f})(u+v) = \begin{cases} \pm 2^q & , si \quad \pi^{-1}(u) \neq \emptyset \\ 0 & , \quad en\, otro\, caso \end{cases} \tag{1.16}$$

Lo supuesto sobre π implica que $\forall t, x \in E$,

$\pi(t) + \pi(t+x) \in F^\perp \Leftrightarrow x = 0$.

Por la proposición 1.2.3, si $x \neq 0$ entonces $r_f(x+y) = 0$. Finalmente, por la relación 1.15, $\forall (x, y) \in E \times F$,

$$r_f(x+y) = \begin{cases} 2^q H(\varphi_{\hat{\pi(E)}})(y) & , si \quad x = 0 \\ 0 & , \quad en\, otro\, caso \end{cases} \tag{1.17}$$

donde $\varphi_{\pi(E)}$ denota el índice de la imagen $\pi(E) \in E^\perp$

Las siguientes propiedades de correlación de f son deducidas:

- f es balanceada $\Leftrightarrow H(\hat{f})(0) = 0$, es decir, $0 \notin \pi(E)$. Esto requiere en particular que $p < q$.
- Si $\forall x \in E$, las clases laterales de $\pi(x) + F^{\perp}$, las cuales son, por definición, el elemento de peso mínimo, tiene peso al menos $l + 1$, entonces $H(\hat{f})$ es cero para todos los vectores de peso $< l + 1$. Por tanto, f es (l)-resistente.
- Como $H(\hat{f})$ tiene magnitud constante igual a 2^q o cero, la No linealidad de f es $\mathcal{N}_f = 2^{n-1} - 2^{q-1}$.
- Como $r_f(z)$ no es cero solamente para $z \in F$, si F tiene distancia mínima d, entonces f satisface el criterio de propagación $PC(d-1)$.

1.2.3.2 π es dos a uno

Asumimos que π es una aplicación dos a uno, esto quiere decir, para cualquier $u \in \pi(E)$, la preimagen $\pi^{-1}(u)$, contiene exactamente dos elementos, llamémoslos x_u y x'_u. Esto implica que $\mid E^{\perp} \mid \geq \frac{|E|}{2} \Rightarrow 2^q \geq \frac{2^p}{2} \Rightarrow q \geq p-1$. Primero examinaremos la transformada de Walsh-Hadamard de f en tal caso. Como cualquier par es un subespacio afín de dimensión uno, la proposición 1.2.2 es aplicable. Con la notación de la proposición 1.2.2, V_u es el espacio vectorial $\{0, x_u + x'_u\}$ y para cualquier $v \in F^{\perp}$,

$$H(\hat{h_u})(v) = (-1)^{h(x_u)+v\cdot x_u} + (-1)^{h(x'_u)+v\cdot x'_u}$$

$$= \begin{cases} 0 & , si \quad h(x_u) + h(x'_u) \neq v \cdot (x_u + x'_u) \\ \pm 2 & , \quad en\, otro\, caso \end{cases}$$

Por conveniencia, denotamos por T a la aplicación booleana en $F^{\perp}$ definida por $T : x \mapsto h(x_u) + h(x'_u)$. La transformada de Walsh-Hadamard de f queda expresada, para cualquier $u \in E^{\perp}$ y cualquier $v \in F^{\perp}$:

$$H(\hat{f})(u+v) = \begin{cases} 0 & , si \quad \pi^{-1}(u) = \emptyset\, o\, T(u) \neq v \cdot (x_u + x'_u) \\ \pm 2^{q+1} & , \quad en\, otro\, caso \end{cases}$$

En particular, f es balanceada si bien no existe un vector de E que cuando se le aplica π devuelve 0 ó $T(0) \neq 0$

Ahora estudiemos la función de autocorrelación de f.

Para cualquier $t, x \in E$, si $x \neq 0$, entonces indica que $\pi(t)$ y $\pi(t+x)$ pertenece a la misma clase lateral $F^{\perp}$ definida por el vector $u \in E^{\perp}$ esto significa que $\{t, t+x\}$ es precisamente el par x_u, x'_u para esta clase lateral, y $x_u + x'_u = x$. Por lo que, usando la proposición 1.2.3 y como el par x_u, x'_u aparece para ambos $x_u = t$ y $x'_u = t + x$, para cualquier $x \in E \setminus \{0\}$ y cualquier $y \in F$,

$$r_f(x+y) = 2^{q+1} \sum_{u \in E^{\perp} | x_u + x'_u = x} (-1)^{H(u)+u\cdot y} \tag{1.18}$$

1.2.3.3 π es cuatro a uno

Asumimos que π es una aplicación cuatro a uno, esto quiere decir, para cualquier $u \in \pi(E)$, la preimagen $\pi^{-1}(u)$, contiene exactamente cuatro elementos. Esto implica que $\mid E^{\perp} \mid \geq \frac{|E|}{4} \Rightarrow 2^q \geq \frac{2^p}{4} \Rightarrow q \geq p - 2$.

Primero examinaremos la transformada de Walsh-Hadamard de f en tal caso. Por hipótesis $\pi^{-1}(u) = \{t, t + x_0, t + y_0, t + x_0 + y_0\}$ es un subespacio afín de dimensión dos, la proposición 1.2.2 es aplicable. Con la notación de la proposición 1.2.2, V_u es el espacio vectorial $\{0, x_0, y_0, x_0 + y_0\}$ y para cualquier $v \in F^{\perp}$,

$$H(\hat{h_u})(v) = (-1)^{h(t)+v\cdot t} + (-1)^{h(x_0+t)+v\cdot(x_0+t)} + (-1)^{h(y_0+t)+v\cdot(y_0+t)} + (-1)^{h(x_0+y_0+t)+v\cdot(x_0+y_0+t)}$$

$$= \begin{cases} 0 \\ \pm 2 \\ \pm 4 \end{cases}$$

Por conveniencia, queremos construir una función booleana con No linealidad lo más alta posible por lo que elegiremos para que tres de lo exponentes sean iguales y el cuarto diferente, tenemos que:

La transformada de Walsh-Hadamard de f queda expresada, para cualquier $u \in E^{\perp}$ y cualquier $v \in F^{\perp}$:

$$H(\hat{f})(u+v) = \begin{cases} \pm 2^{q+1} & , si \quad (h(t) + h(x_0+t) = v \cdot x_0) \wedge (h(x_0+t) + h(x_0+y_0+t) \neq v \cdot x_0) \\ 0 & , si \quad \pi^{-1}(u) = \emptyset \end{cases}$$

1.3 Códigos algebraicos

La notación que estamos usando es del libro de Henning y ver Anexos para más detalle. Denotamos $\mathbb{F}_\sigma$ como el campo finito de σ elementos.

1.3.1 Códigos de Goppa

[5] Sea F/K un campo de funciones algebraicas de género g y sean $P_1, \ldots, P_n \in \mathbb{P}_F$ n lugares distintos de grado 1 de F; definimos el divisor

$$D := P_1 + \cdots + P_n \in \mathcal{D}_F,$$

y sea $G \in \mathcal{D}_F$ un divisor tal que $soporte(G) \cap soporte(D) = \emptyset$. El **código de Goppa** o **código geométrico** $C_{\mathcal{L}}(D, G)$ asociado a los divisores D y G se define como

$$C_{\mathcal{L}}(D, G) := \{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_\sigma^n.$$

Notemos que toda $f \in \mathcal{L}(G)$ está definida en P_i $(v_{P_i}(f) \geq 0)$, $i = 1, \ldots, n$, por lo que $f(P_i) \in \mathbb{F}_\sigma$. De esta manera $C_\mathcal{L}(D, G)$ es simplemente la imagen del espacio $\mathcal{L}(G)$ bajo el mapeo lineal evaluación

$$ev_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_\sigma^n$$

dado por $ev_D(f) := (f(P_1), \ldots, f(P_n))$.

Esta definición es análoga a la de los códigos de Reed-Solomon. De hecho, en el caso del código Reed-Solomon $RS(k, \sigma)$ tenemos que $F = K = k(x)$,

$$D = P_0 + P_1 + P_\alpha + \cdots + P_{\alpha^{\sigma-2}}$$

y

$$G = m \cdot P_\infty.$$

Se sigue que $Ker(ev_D) = \mathcal{L}(G - D)$ por lo que, usando Riemann-Roch

$$dim(C_\mathcal{L}(D, G)) = dim(G) - dim(G - D).$$

Ahora sea $f \in \mathcal{L}(G)$ tal que $d = peso(ev_D(f))$. Entonces f tiene exactamente $n - d$ ceros $P_{i_1}, \ldots, P_{i_{n-d}} \in soporte(D)$. Esto último nos dice que

$$f \in \mathcal{L}(G - (P_{i_1} + \ldots + P_{i_{n-d}})),$$

de donde

$$0 \leq grado(G - (P_{i_1} + \ldots + P_{i_{n-d}})) = grado(G) - (n - d).$$

Por lo que $d \geq n - grado(G)$. Entonces $C_\mathcal{L}(D, G)$ es un código con parámetros

$$[n, dim(G) - dim(G - D), \geq n - grado(G)]_q.$$

1.3.1.1 Ejemplo de Códigos de Goppa

Ejemplo para $m = 3$

En este ejemplo usaremos como campo base a $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ donde $\alpha^2 + \alpha + 1 = 0$.

Consideremos el campo de funciones $F := \mathbb{F}_4(x, y)$ con $y^2 + y = x^3$.

Los lugares para D son: $(0,0), (0,1), (1,\alpha), (1,\alpha^2), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,\alpha), (\alpha^2,\alpha^2)$. Podemos ahora construir un código de Goppa: Por ejemplo, definimos los divisores $D, G \in \mathcal{D}_F$

$D := (0,0) + (0,1) + (1,\alpha) + (1,\alpha^2) + (\alpha,\alpha) + (\alpha,\alpha^2) + (\alpha^2,\alpha) + (\alpha^2,\alpha^2)$

y

$G := 3 \cdot P_\infty$

Las funciones $\{1, x, y\}$ son una base para $\mathcal{L}(G)$. Una matriz generadora para el código de Goppa asociado a los divisores D y G es

	$(0,0)$	$(0,1)$	$(1,\alpha)$	$(1,\alpha^2)$	(α,α)	(α,α^2)	(α^2,α)	(α^2,α^2)
1	1	1	1	1	1	1	1	1
x	0	0	1	1	α	α	α^2	α^2
y	0	1	α	α^2	α	α^2	α	α^2

El código obtenido tiene parámetros $[8, 3, 5]_4$

1.3.2 Códigos hermitianos

La curva hermitiana sobre $\mathbb{F}_{\sigma^2}$ en coordenadas afines es:

$$C : u^{\sigma+1} + v^{\sigma+1} + 1 = 0 \tag{1.19}$$

Con el cambio de coordenadas $x = b/(v - bu)$ e $y = ux - a$ donde $a^\sigma + a = b^{\sigma+1} = -1$, la curva Hermitiana C es equivalente a la curva

$$y^{\sigma} + y = x^{\sigma+1} \tag{1.20}$$

Lema 1.3.1. *[5] El campo de funciones hermitiano sobre $\mathbb{F}_{\sigma^2}$, σ es una potencia prima, puede ser definida por*

$$H = \mathbb{F}_{\sigma^2}(x, y) \text{ con } y^{\sigma} + y = x^{\sigma+1}$$

La curva H tiene las siguientes propiedades:

- *a) Es no singular*
- *b) Tiene genero $g = \sigma(\sigma - 1)/2$*
- *c) Tiene $\sigma^3 + 1$ lugares de grado uno sobre $\mathbb{F}_{\sigma^2}$.*
  - *1. P_{∞} es el polo común de x e y*
  - *2. Para cada $\alpha \in \mathbb{F}_{\sigma^2}$, existen σ elementos $\beta \in \mathbb{F}_{\sigma^2}$ tales que $\beta^{\sigma} + \beta = \alpha^{\sigma+1}$ y respecto a todos los pares (α, β) hay un único lugar $P_{\alpha,\beta} \in \mathbb{P}_H$ de grado uno con $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$*

Demostración:

(a) Tomando $F = X^{\sigma+1} - Y^{\sigma}Z - YZ^{\sigma}$, tenemos las siguientes derivadas parciales: $F_X = X^{\sigma}, F_Y = Z^{\sigma} y F_Z = Y^{\sigma}$. Observe que no existe punto P de X tal que $F_X(P) = F_Y(P) = F_Z(P) = 0$. Con esto se prueba, C es una curva no-singular.

(b) Siendo C una curva no-singular y plana, se sigue por el teorema de Riemann-Hurwitz que $g = d(d-1)/2$.

(c) Una generalización de Hasse ligada a las curvas algebraicas es el límite de Hasse-Weil. Esto proporciona un límite en el número de puntos en una curva sobre un campo finito. Si la cantidad de puntos en la curva C del género g sobre el campo finito $\mathbb{F}_{\sigma}$ de orden σ es $\#C(\mathbb{F}_{\sigma})$, entonces

$|\#C(\mathbb{F}_{\sigma}) - (\sigma + 1)| \leq 2g\sqrt{\sigma}$.

Ahora en nuestro caso $\#C(\mathbb{F}_{\sigma^2}) = 1 + \sigma^2 + 2 \cdot \frac{\sigma(\sigma-1)}{2} \cdot \sqrt{\sigma^2} = 1 + \sigma^2 + \sigma^3 - \sigma^2 = 1 + \sigma^3$

■

De acuerdo con el lema anterior, tenemos σ^3+1 puntos en la curva hermitiana, denotemos por $P_1,\ldots,P_n$ los lugares de grado uno distintos de P_∞ , donde $n=\sigma^3$ y consideremos el divisor $D=\sum_{i=1}^{n}P_i$

Para cada $m\in\mathbb{Z}$, definimos el m-ésimo código hermitiano sobre F_{σ^2} o código AG, $C_m := C(D;mP_\infty)$ cuyos parámetros son $[n;k_m;d_m]_{\sigma^2}$.

Proposición 1.3.2. *[5] Una $\mathbb{F}_{\sigma^2}$-base de $\mathcal{L}(mP_\infty), m\geq 0$, esta dada por*

$$A(m)=\{x^iy^j : i\sigma+j(\sigma+1)\leq m; i\geq 0; 0\leq j\leq \sigma-1\} \tag{1.21}$$

$v(m)=\#(A(m))$

Demostración:

Los elementos $1,y,\ldots,y^{\sigma-1}$ forman una base de $F/K(x)$ para todos los lugares $P\in\mathbb{P}_{K(x)}$ diferente de P_∞.

Esto implica que $d(P_i\mid P)=v_{P_i}(\varphi'(y))$, donde $\varphi(T)=T^\sigma+\mu T-f(x)$ es el polinomio minimal de y sobre $K(x)$ está en $\mathcal{O}_P[T]$ y para todo $Q\mid P$, $v_Q(\varphi'(y))=v_Q(\mu)=0=d(Q\mid P)$.

Sea $z\in\mathcal{L}(mQ_\infty)$. Como P_∞ es el único polo de z, z es integral sobre $\mathcal{O}_P$ para todo $P\in\mathbb{P}_{K(x)}, P\neq P_\infty$, así $z=\sum_{j=0}^{\sigma-1}z_jy^j$ con $z_j\in K(x)$ y z_j no tiene polos distintos de P_∞. Por tanto, z_j es un polinomio en $K[x]$, es decir,

$$z=\sum_{j=0}^{\sigma-1}\sum_{i\geq 0}a_{ij}x^iy^j \; con\, a_{ij}\in K \tag{1.22}$$

Los elementos x^iy^j con $0\leq j\leq\sigma-1$ tienen pares de orden de polo distinto porque $v_{P_\infty}(x)=-\sigma$, $v_{P_\infty}(y)=-(\sigma+1)$ y $\sigma+1$ y σ son primos relativos. Por tanto, aplicando la desigualdad triangular estricta implica que: $v_{P_\infty}(z)=min\{-i\sigma-(\sigma+1)j\mid a_{ij}\neq 0\}$.

Por tanto, como resultado de lo anterior

$$dim_{F_{\sigma^2}}(\mathcal{L}(G)) = \#\{x^i y^j : i\sigma + j(\sigma+1) \leq m; i \geq 0; 0 \leq j \leq \sigma - 1\}$$

■

Teorema 1.3.3. *Asumamos que* $0 \leqslant m < \sigma^3$. *Entonces*

$$dim\ C_m = \begin{cases} v(m) & si \quad m \leqslant \sigma^2 - \sigma - 2 \\ m + 1 - (\sigma^2 - \sigma)/2 & si \quad \sigma^2 - \sigma - 2 < m < \sigma^3 \end{cases}$$

Ver demostración en [6]

Observación: Los códigos hermitianos tiene por parámetros $\left[\sigma^3, dim\ C_m, \geq \sigma^3 - dim\ C_m\right]_{\sigma^2}$

Proposición 1.3.4. *El código dual de un código hermitiano* C_m *es* $C_m^{\perp} = C_{\sigma^3+\sigma^2-\sigma-2-m}$.

Si $2m \leq \sigma^3 + \sigma^2 - \sigma - 2$, *entonces* C_m *es auto-ortogonal y si* $m = \frac{\sigma^3+\sigma^2-\sigma-2}{2}$, *entonces es auto-dual.*

1.3.2.1 Ejemplo de códigos hermitianos

El mismo ejemplo anterior sobre códigos de Goppa nos sirve, lo que en este caso tomaremos $m = 6$

En este ejemplo usaremos como campo base a $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ donde $\alpha^2 + \alpha + 1 = 0$.

Consideremos el campo de funciones $F := \mathbb{F}_4(x, y)$ con $y^2 + y = x^3$.

Los lugares para D son: $(0,0), (0,1), (1,\alpha), (1,\alpha^2), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,\alpha), (\alpha^2,\alpha^2)$. Podemos ahora construir un código de Goppa: Por ejemplo, definimos los divisores $D, G \in \mathcal{D}_F$

$D := (0,0) + (0,1) + (1,\alpha) + (1,\alpha^2) + (\alpha,\alpha) + (\alpha,\alpha^2) + (\alpha^2,\alpha) + (\alpha^2,\alpha^2)$

y

$G := 6 \cdot P_\infty$

Las funciones $\left\{1, x, x^2, x^3, y, xy\right\}$ son una base para $\mathcal{L}(G)$. Una matriz generadora para el código de Goppa asociado a los divisores D y G es

	$(0,0)$	$(0,1)$	$(1,\alpha)$	$(1,\alpha^2)$	(α,α)	(α,α^2)	(α^2,α)	(α^2,α^2)
1	1	1	1	1	1	1	1	1
x	0	0	1	1	α	α	$\alpha+1$	$\alpha+1$
x^2	0	0	1	1	$\alpha+1$	$\alpha+1$	α	α
x^3	0	0	1	1	1	1	1	1
y	0	1	α	$\alpha+1$	α	$\alpha+1$	α	$\alpha+1$
xy	0	0	α	$\alpha+1$	$\alpha+1$	1	1	α

El código obtenido tiene parámetros $[8,6,2]_4$

Tenemos por matriz generadora

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

1.4 Concatenación

La concatenación de códigos fue propuesta por Forney [7] en 1965. Sea $Q = \sigma^h$. El método de encadenamiento construye a partir de un código sobre $\mathbb{F}_Q$, un nuevo código sobre $\mathbb{F}_\sigma$: Sea C un código con parámetros $[N,K,D]_Q$ y supongamos que existe un código I con parámetros $[n,h,d]_\sigma$. Supongamos un isomorfismo $\phi : \mathbb{F}_Q \longrightarrow I \subseteq \mathbb{F}_\sigma^n$, en nuestro caso usaremos el isomorfismo del epígrafe anterior, entonces

$$F = \{(\phi(c_1)), \ldots, \phi(x_N))|(x_1, \ldots, x_N) \in C\}.$$

El código F tiene parámetros

$$[N \cdot n, K \cdot h, D \cdot d]_\sigma.$$

1.4.1 Isomorfismo para la concatenación

Para la concatenación ocupamos un isomorfismo entre el campo finito donde vive nuestro código algebraico $\mathbb{F}_{\sigma^2} \cong \mathbb{F}_{2^{2k}}$ haciendo $\sigma = 2^k$ y un código binario de todas las palabras de peso par en $\mathbb{F}_2^{2k+1}$, los parámetros de este código son $[2k+1, 2k, 2]$.

$\phi : \mathbb{F}_{2^{2k}} \longrightarrow \mathbb{F}_2^{2k+1}$

Como se muestra en el Anexo A en su sección 3, el campo $\mathbb{F}_{2^{2k}}$ tiene su representación

$$\mathbb{F}_{2^{2k}} = \{a_{2k-1}x^{2k-1} + a_{2k-2}x^{2k-2} + \cdots + a_1x + a_0 : a_i \in \mathbb{F}_2\}$$

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

$$\mathbb{F}_2^{2k} = \{(a_{2k-1}a_{2k-2}\cdots a_1a_0) : a_i \in \{0,1\}\}$$

Por otra parte, consideremos el espacio vectorial

$\mathbb{F}_2^{2k+1} = \{(a_{2k-1}a_{2k-2}\cdots a_1a_0) : a_i \in \{0,1\} \wedge \sum_{i=0}^{2k-1} a_i \equiv 0 \mod 2\}$

Para obtener el vector de dimensión $2k+1$ completamos la derecha con cero o uno en dependencia de si las suma de las coordenadas del vector $2k-$*dimensional* es par o impar.

$$\phi(a_{2k-1}a_{2k-2}\cdots a_1a_0) = \begin{cases} (a_{2k-1}a_{2k-2}\cdots a_1a_00) & si \quad \sum_{i=0}^{2k-1} a_i \equiv 0 \mod 2 \\ (a_{2k-1}a_{2k-2}\cdots a_1a_01) & si \quad \sum_{i=0}^{2k-1} a_i \equiv 1 \mod 2 \end{cases}$$

Denotaremos al conjunto imagen de ϕ por I,que se puede ver como un código binario con parámetros $[2k+1, 2k, 2]$

1.4.1.1 Ejemplo 1

El campo finito $\mathbb{F}_{2^2}$ construido como extensión del campo finito $\mathbb{F}_2$, utilizando el polinomio primitivo $P(x) = x^2 + x + 1$ $\mathbb{F}_{2^2} = \{0, 1, \alpha, 1+\alpha\}$

Si consideramos el espacio vectorial $(A)^3$

$(A)^3 = \{(a_2, a_1, a_0) \mid a_i \in \mathbb{F}_2 \wedge \sum_{i=0}^{2}(a_i \equiv 0 \mod 2\}$

$$\mathbb{F}_{2^2} \longrightarrow (A)^3$$

	Elemento	Vector de dimensión 2	Vector de dimensión 3 de peso par
0	1	$(0,1)$	$(0,1,1)$
1	α	$(1,0)$	$(1,0,1)$
2	$1+\alpha$	$(1,1)$	$(1,1,0)$
	0	$(0,0)$	$(0,0,0)$

1.4.1.2 Ejemplo 2

El campo finito $\mathbb{F}_{2^4}$ construido como extensión del campo finito $\mathbb{F}_2$, utilizando el polinomio primitivo $P(x) = x^4 + x + 1$ $\mathbb{F}_{2^4} = \{0, 1, \alpha, \alpha^2, \alpha^3, 1+\alpha, \alpha+\alpha^2, 1+\alpha+\alpha^3, 1+\alpha^2, \alpha+\alpha^3, 1+\alpha+\alpha^2, \alpha+\alpha^2+\alpha^3, 1+\alpha+\alpha^2+\alpha^3, \alpha^2+\alpha^3, 1+\alpha^3, 1+\alpha^2+\alpha^3\}$

Si consideramos el espacio vectorial $(A)^5$

$(A)^5 = \{(a_4, a_3, a_2, a_1, a_0) \mid a_i \in \mathbb{F}_2 \wedge \sum_{i=0}^{4}(a_i \equiv 0 \mod 2\}$

$$\mathbb{F}_{2^4} \longrightarrow (A)^5$$

	Elemento	Vector de dimensión 4	Vector de dimensión 5 de peso par
0	1	$(0,0,0,1)$	$(0,0,0,1,1)$
1	α	$(0,0,1,0)$	$(0,0,1,0,1)$
2	α^2	$(0,1,0,0)$	$(0,1,0,0,1)$
3	α^3	$(1,0,0,0)$	$(1,0,0,0,1)$
4	$1+\alpha$	$(0,0,1,1)$	$(0,0,1,1,0)$
5	$\alpha+\alpha^2$	$(0,1,1,0)$	$(0,1,1,0,0)$
6	$\alpha^2+\alpha^3$	$(1,1,0,0)$	$(1,1,0,0,0)$
7	$1+\alpha+\alpha^3$	$(1,0,1,1)$	$(1,0,1,1,1)$
8	$1+\alpha^2$	$(0,1,0,1)$	$(0,1,0,1,0)$
9	$\alpha+\alpha^3$	$(1,0,1,0)$	$(1,0,1,0,0)$
10	$1+\alpha+\alpha^2$	$(0,1,1,1)$	$(0,1,1,1,1)$
11	$\alpha+\alpha^2+\alpha^3$	$(1,1,1,0)$	$(1,1,1,0,1)$
12	$1+\alpha+\alpha^2+\alpha^3$	$(1,1,1,1)$	$(1,1,1,1,0)$
13	$1+\alpha^2+\alpha^3$	$(1,1,0,1)$	$(1,1,0,1,1)$
14	$1+\alpha^3$	$(1,0,0,1)$	$(1,0,0,1,0)$
	0	$(0,0,0,0)$	$(0,0,0,0,0)$

Veamos si se preservan las operaciones, por ejemplo,

$\phi((1,0,0,1)+(0,1,0,1)) = \phi(1,1,0,0) = (1,1,0,0,0)$

$\phi((1,0,0,1)) + \phi((0,1,0,1)) = (1,0,0,1,0) + (0,1,0,1,0) = (1,1,0,0,0)$

1.4.2 Ejemplo de concatenación

Utilizando el isomorfismo y la concatenación descrita en la sección anterior. Además, tomemos el ejemplo de la sección 1.3.2.1, donde se obtuvo la matriz generadora para un código hermitiano para $m = 6$. La matriz

$$G_F = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 0 & 0 & 1 & 1 & \alpha+1 & \alpha+1 & \alpha & \alpha \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha+1 & \alpha & \alpha+1 & \alpha & \alpha+1 \\ 0 & 0 & \alpha & \alpha+1 & \alpha+1 & 1 & 1 & \alpha \end{pmatrix}$$

Le aplicamos el isomorfismo del ejemplo 1 de la sección 1.4.1.1 y obtenemos una nueva matriz generadora binaria que es con la que se construye el subespacio F, o sea,

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

Propiedades criptográficas de funciones booleanas provenientes de códigos hermitianos.

2.1 Introducción

Nuestra propuesta esta determinada por el orden de la resistencia que podamos y queramos tener para construir nuestra función booleana:

$$\begin{array}{rccl} f: & E \oplus F & \longrightarrow & \mathbb{F}_2 \\ & x+y & \mapsto & \pi(x)\cdot y + h(x), \end{array}$$

En general es muy difícil calcular propiedades criptográficas de funciones booleanas de la forma anterior si no se conoce nada acerca de las funciones π y h. El caso más sencillo (y menos interesante porque se obtienen funciones no balanceadas) es por supuesto el caso en que π es una transformación lineal. El siguiente caso sencillo es cuando $\pi^{-1}(\pi(x)) = x + V$ para algún espacio vectorial V fijo, pero introduciendo la hipótesis adicional de que $\pi^{-1}(0) = \emptyset$.

Guillot calcula la autocorrelación de f y la transformada de Walsh-Hadamard de f en el caso en que π es uno a uno o bien si π es dos a uno y $\pi^{-1}(\pi(x)) = \{x, x + x_0\}$ para todo $x \in E$, con $x_0 \in E$ fijo, siempre bajo la hipótesis de que $\pi^{-1}(0) = \emptyset$.

En esta sección calcularemos la nolinealidad de f y daremos una cota para la resistencia de f en estos casos, así como en el caso en que π es cuatro a uno, suponiendo que $\pi^{-1}(0) = \emptyset$ y que $\pi^{-1}(\pi(x)) = x + V$ para toda $x \in E$ con $V < E$ un subespacio vectorial fijo. Supondremos además que el código F es un código de Reed-Solomon o un código hermitiano.

Observe que si π es dos a uno, entonces $V = \{0, x_0\}$ para algún $x_0 \in E$ y la resistencia y el criterio de propagación de f dependen de x_0. Si F es un código de Reed-Solomon es fácil proponer un x_0 adecuado. Si F

es un código hermitiano es deseable describir un modo de construir x_0 a partir de la curva hermitiana asociada.

Finalmente, si π es cuatro a uno el espacio vectorial V es de la forma $\{0, x_0, y_0, x_0 + y_0\}$, donde $x_0, y_0 \in E$ son linealmente independientes. En general necesitaríamos construir x_0 e y_0, sin embargo en este trabajo proponemos una función h de tal modo que el valor específico de y_0 es irrelevante.
En lo que sigue usaremos todos estos supuestos.
De manera particular, queremos trabajar con dos tipos de códigos especiales pertenecientes a la familia de los códigos de Goppa que son los códigos Reed-Solomon y códigos hermitianos. Analizaremos por separado estos casos hasta cierto punto.

2.1.1 Reed-Solomon

Asumamos que tenemos $C = RS(r, 2^m)$, I es un código binario porque $q = 2$. Definamos al conjunto I como las palabras de peso par que definimos en el capítulo 1 como el espacio vectorial de llegada del isomorfismo ϕ, entonces $I \subseteq \mathbb{F}_2^{m+1}$ y como código I tiene parámetros $[m+1, m, 2]_2$. Por lo que, el código concatenado F tiene parámetros $[(m+1)2^m, m \cdot r, 2(2^m - r + 1)]_2$. Denotemos para mayor comodidad los parámetros F por $[n, q, d_F)]_2$.

2.1.2 Códigos hermitianos

Al igual que en el caso anterior asumamos que tenemos un código hermitiano C_m con parámetros $\left[\sigma^3, dim\ C_m, \sigma^3 - k_m\right]_{\sigma^2}$, asumiendo que $\sigma = 2^k$, tenemos $\left[2^{3k}, k_m = dim\ C_m, 2^{3k} - k_m\right]_{2^{2k}}$. Para el isomorfismo seguimos con lo que se formalizó en el capítulo 1, tomando a I como el conjunto imagen de $\phi : \mathbb{F}_{2^{2k}} \longrightarrow \mathbb{F}_2^{2k+1}$ y visto como código tiene parámetros $[2k+1, 2k, 2]_2$. Por lo que, el código concatenado F tiene parámetros $\left[(2k+1)2^{3k}, 2k_m \cdot k, 2(2^{3k} - k_m)\right]_2$. Denotemos para mayor comodidad los parámetros F por $[n, q, d_F)]_2$.

2.1.3 Observaciones

En ambos casos ya tenemos nuestro código F que a su vez será nuestro subespacio complementario F de 2.1 pero el código F lo reescribiremos de manera sistemática.

El subespacio complementario E tendrá por lo tanto, dimensión $p = n - q$ y será de la forma
$E = \{(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n : x_1 = 0, x_2 = 0, \ldots, x_q = 0\}$.

2.2 Obteniendo x_0

Una de las propiedades que nos interesa de las funciones booleanas es el criterio de propagación, en su artículo Guillot muestra que si π es dos a uno, la función booleana tiene criterio de propagación de orden k si la clase laterial $x_0 + F$ tiene $w(x_0 + F) >> k$. En principio como queremos encontrar una función booleana con $PC(k-1)$ tenemos que seleccionar un x_0 apropiado.

2.2.1 Reed-Solomon

Supongamos que tenemos la clase lateral x_0+F, F esta construida con todos los polinomios de grado menores que r sobre $\mathbb{F}_{2^m}[x]$, también podemos suponer que x_0 es generado por un polinomio $L(x)$ sobre $\mathbb{F}_{2^m}[x]$. $L(x)$ se obtiene usando el polinomio de interpolación de Lagrange.
Sea $a_1, ..., a_t$ el conjunto de coordenadas de información para el código $RS(r, 2^m)$ por interpolación de Lagrange, podemos obtener un polinomio de grado $< t$ tal que $L(a_i) = 0$ for $i = 1, ..., t$. El vector $ev(L)$ es un vector en el complemento de F como espacio vectorial sobre $\mathbb{F}_{2^m}$. Sea $x_0 = ev(L)$ la concatenación de x_0 dado un vector en el complemento de F.
Como $x_0 \in E$, entonces $x_0 = (0, 0, \ldots, 0, x_{q+1}, \ldots, x_n)$, particionamos a x_0 en 2^m partes de tamaño $m + 1$. Nos regresamos a $\mathbb{F}_{2^m}$ mediante la función ϕ^{-1} de la concatenación.

Entonces obtenemos $x_0 = (A_1, A_2, \ldots, A_{2^m}) \in \mathbb{F}_{2^m}^{2^m}$ Usamos ahora Lagrange para encontrar un polinomio $L(x)$ tal que:
$L(a_i) = A_i$, con $a_i \in \mathbb{F}_{2^m}$ e $i = 1 \ldots 2^m$

2.2.2 Códigos hermitianos

Para el caso de las curvas hermitianas, si a es un elemento de $\mathbb{F}_{\sigma^2}$, ¿qué quiere decir que $v_P(L - a) > 0$?
Si $v_P(L - a) > 0$ quiere decir que P es un cero de la función $L - a$. Es decir, usando el mapeo natural

$(L-a)(P)=0$ como el mapeo natural es un homomorfismo tenemos que:

$(L-a)(P)=L(P)-a(P)$

Pero como el campo de constantes, $\mathbb{F}_{\sigma^2} \subset K(H)$, mediante las funciones constantes $a(P)=a$ tenemos $L(P)-a=0$ o bien $L(P)=a$, es decir, podemos preescribir el valor de nuestra función L en el punto P. Entonces estamos buscando una función L tal que $L(P_1)=L(P_2)=\ldots=L(P_q)=0$, de preferencia que esos sean sus únicos ceros. Por lo que, podríamos reescribir sus polos, por ejemplo, si P_∞ es el lugar al infinito de la curva, entonces pidamos que $v_{P_\infty}(L)=-q$ y por tanto L pertenece al espacio $\mathcal{L}(qP_\infty)$ y es una combinación lineal de las funciones de una base para $\mathcal{L}(qP_\infty)$

2.2.2.1 Construyendo x_0

Con el teorema de aproximación fuerte podemos construir una función L que tome valores prescritos en lugares prescritos, utilizaremos una idea explicada en el libro [5], la cual es la siguiente:
Como queremos que nuestro x_0 tenga q ceros en las primeras coordenadas, siendo q la dimensión del subespacio F. Dividamos el problema de la construcción de L en tres casos:

Caso 1: Si $q=\sigma^3-\sigma^2$. Escojamos $i=\sigma^2-\sigma$ elementos diferentes $\alpha_1,\ldots,\alpha_i \in \mathbb{F}_{\sigma^2}$. Entonces la L se construye de la manera

$$L=\prod_{\nu=1}^{i}(x-\alpha_\nu)$$

$\mathbb{P}'_D=\{(\alpha_\nu,\delta)\in\mathbb{P}_D \; con \; \delta\in\mathbb{F}_{\sigma^2} \; y \; \nu=1\ldots i\}$

Reescribimos $D=(D')\bigcup(D-D')$

En este caso L tendrá exactamente $\sigma\cdot i=q$ ceros distintos $P_{\alpha,\beta}$ de grado uno distintos de P_∞ , por lo que la $ev_D(L)$ es un vector con peso menor o igual σ^3-q.

Caso 2: Si $q<\sigma^3-\sigma^2$. Escribimos $q=i\sigma+j(\sigma+1)$ con $i\geqslant 0$ y $0\leqslant j\leqslant \sigma-1$, tal que $i\leqslant\sigma^2-\sigma-1$. Fijamos un elemento $0\neq\gamma\in\mathbb{F}_\sigma$ y consideremos el conjunto $A=\{\alpha\in\mathbb{F}_{\sigma^2}\mid \alpha^{\sigma+1}\neq\gamma\}$. Entonces $\#A=\sigma^2-(\sigma+1)\geqslant i$, y podemos escoger elementos distintos $\alpha_1,\ldots,\alpha_i\in A$. Escojamos un subconjunto $I\subseteq A \; con \; \#I=i$. Por lo que, la función

$$L_1 = \prod_{\nu \in I} (x - \alpha_\nu)$$

tiene $i\sigma$ ceros distintos. Próximo paso escojamos ahora j elementos distintos $\beta_1, \ldots, \beta_j \in \mathbb{F}_{\sigma^2}$ con $\beta_\mu^\sigma + \beta_\mu = \gamma$ y definamos ahora

$$L_2 = \prod_{\mu=1}^{j} (y - \beta_\mu)$$

entonces L_2 tiene $j(\sigma + 1)$ ceros, y todos estos son dintintos de los ceros de L_1 por que $\beta_\mu^\sigma + \beta_\mu = \gamma \neq \alpha_\nu^{\sigma+1}$ para $\mu = 1, \ldots, j$ y $\nu = 1, \ldots, i$. Por tanto, $L = L_1 \cdot L_2$

Hagamos un paréntesis, definamos el conjunto $\mathbb{P}_A = \{(\alpha_\nu, \delta) \in \mathbb{P}_D \; con \; \delta \in \mathbb{F}_{\sigma^2} \; y \; \nu = 1 \ldots i\}$ y

$\mathbb{P}_B = \{(\epsilon, \beta_\mu) \in \mathbb{P}_D \; con \; \epsilon \in \mathbb{F}_{\sigma^2} \; \mu = 1 \ldots j\}$

Reescribimos $D = \{\mathbb{P}_A \cup \mathbb{P}_B \cup \{D - (\mathbb{P}_A \cup \mathbb{P}_B)\}\}$ y evaluemos $ev_D(L)$ nos dará un vector con $\sigma^3 - q$ ceros en las primeras coordenadas.

Caso 3: Si $\sigma^3 - \sigma^2 < q < \sigma^3$. Por suposición, $s = \sigma^3 - q$ y $0 < s < \sigma^2 \leqslant \sigma^3 - \sigma^2$. Por el Caso 2 existe una función L' con divisor principal $(L') = \hat{D} - sP_\infty$ donde $0 \leqslant \hat{D} \leqslant D$ y el $grad(\hat{D}) = s$. La función $u = x^{\sigma^2} - x$ tiene el divisor $(u) = D - \sigma^3 P_\infty$, por tanto,

$(L'^{-1} \cdot u) = (D - \hat{D}) - (\sigma^3 - s)P_\infty = (D - \hat{D}) - (q)P_\infty$

Por lo que mi función es $L = L'^{-1} \cdot u$, como lo hemos hecho hasta ahora reescribimos $D = \hat{D} \bigcup (D - \hat{D})$.

Si $q > dim(F)$ entonces $L \in \mathcal{L}(qP_\infty) \setminus \mathcal{L}(dim(F)P_\infty)$.

2.2.3 Ejemplo

Tomemos el caso de la curva hermitiana $y^2 + y = x^3$ sobre $\mathbb{F}_{2^2} = \mathbb{F}_4$, el subcampo base esta compuesto por $\mathbb{F}_2 = \{0, 1\}$ y $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ donde $\alpha^2 + \alpha + 1 = 0$.

Estos son los puntos que están sobre la curva: $(0,0), (0,1), (1,\alpha), (1,\alpha^2), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,\alpha), (\alpha^2,\alpha^2)$

Caso 1: Si $q = 4 = 2^3 - 2^2$ y $\sigma = 2$,entonces $i = 2$. Basta con tomar los primeros 2 elementos de $\mathbb{F}_4$ para construir L

$L(x) = x(x-1) = x^2 + x$

$eva_D(L(x)) = \{0, 0, 0, 0, 1, 1, 1, 1\}$

Caso 2: Tomemos $q = 3 = 0 \cdot \sigma + 1 \cdot (\sigma + 1) < 2^3 - 2^2$, o sea, que $i = 0, j = 1$. Entonces, definamos el conjunto B para $\gamma = 1$ (es importante aclarar que A no se define porque $i = 0$)

$B = \{\alpha\}$

$\mathbb{P}_B = \{(1, \alpha), (\alpha, \alpha), (\alpha^2, \alpha)\}$

Ahora, de B el primero para conformar nuestra función L.

$L(x, y) = (y - \alpha) = y + \alpha$

Redefinamos $D = \{\mathbb{P}_B, D - \mathbb{P}_B\}$

$D = \{(1, \alpha), (\alpha, \alpha), (\alpha^2, \alpha), (0, 0), (0, 1), (1, \alpha^2), (\alpha, \alpha^2), (\alpha^2, \alpha^2)\}$

$ev_D(L(x, y)) = \{0, 0, 0, \alpha, \alpha^2, 1, 1, 1\}$

Caso 3: Asumamos $q = 5 > 2^3 - 2^2$, por lo que, $s = 8 - 5 = 3$ y se aplica el Caso 2 pero con $s = 3$, que ya tenemos construido del ejemplo anterior.

$L'(y) = (y + \alpha)$

Ahora $D' = \mathbb{P}_B = \{(1, \alpha), (\alpha, \alpha), (\alpha^2, \alpha)\}$

Redefinamos $D = \{\mathbb{P}_B, D - \mathbb{P}_B\}$

$ev_D(L'(y)) = \{0, 0, 0, \alpha, \alpha^2, 1, 1, 1\}$ Definamos $L(x, y) = \frac{x^4+x}{L'(y)} = \frac{x^4+x}{(y-\alpha)}$

Redefinamos $D = \{D - D', D'\} = \{(0, 0), (0, 1), (1, \alpha^2), (\alpha, \alpha^2), (\alpha^2, \alpha^2), (1, \alpha), (\alpha, \alpha), (\alpha^2, \alpha)\}$

$ev_D(L(x, y)) = \{0, 0, 0, 0, 0, 1, 1, 1\}$

2.3 Construcción de π y h

Algunas de las ideas planteadas en esta sección y demostraciones fueron tomadas del artículo [8].

Lema 2.3.1. *Si $w \in \mathbb{F}_2^n$, tenemos que*

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

Demostración:

Primero, si $w = 0$, entonces todos los sumandos son 1. Ahora, asumamos que $w \neq 0$, y consideremos los hiperplanos $H = \{u \in \mathbb{F}_2^n : u \cdot w = 0\}$, $\bar{H} = \{u \in \mathbb{F}_2^n : u \cdot w = 1\}$. Obviamente, estos hiperplanos generan una partición de $\mathbb{F}_2^n$. Por otra parte, para cualquier $u \in H$, los sumandos son 1, y para cualquier $u \in \bar{H}$, los sumandos son -1. Ya que las cardinalidades de $H, \bar{H}$ son las mismas, es decir, 2^{n-1}, tenemos el lema.

■

Con las notación introducida en la introducción del capítulo sobre la construcción de MM.

Teorema 2.3.2. *Si $\mathbb{F}_2^n = E \oplus F$ con $dim(E) = p$, $dim(F) = q$ y $f : \mathbb{F}_2^n \Longrightarrow \mathbb{F}_2$ es de la forma $f(z) = f(x, y) = \pi(x) \cdot y + h(x)$, con $z = (z_1, \ldots, z_n) \in \mathbb{F}_2^n$, donde $z = x + y$ con $x \in E$ e $y \in F$ entonces,*
Sea

$$\lambda = min\{w(\pi(x)) : x \in E\} \geq 1 \tag{2.1}$$

.

Entonces $f(z)$ tiene una resistencia de orden l con $l \leq \lambda - 1$.

Demostración:

Recordemos que una función booleana tiene resistencia de orden l si $H(\hat{f})(u) = 0$, con $0 \leq w(u) \leq l$.

Ahora, $H(\hat{f})(u) = \sum_{z \in \mathbb{F}_2^n} (-1)^{f(z)+u\cdot z}$.
Primero analicemos el caso que $w(u) = 0 \Rightarrow u = 0$.
Tenemos $\sum_{z \in \mathbb{F}_2^n} (-1)^{f(z)} = \sum_{x \in E} (-1)^{h(x)} \sum_{y \in F} (-1)^{\pi(x)\cdot y} = 0$,
ya que las sumas sobre y son siempre cero porque $\pi(x) \neq 0$ por (5.1) y usando el lema 2.3.1. Así, $f(z)$ es balanceada. Para cualquier, $l \leqslant \lambda - 1$ y cualquier elección u con $1 \leq w(u) \leq l$, tenemos

$$H(\hat{f})(u) = \sum_{(x,y) \in E \times F} (-1)^{\pi(x)\cdot y + h(x) + u\cdot(x+y)}$$

$$= \sum_{x \in E} (-1)^{h(x)+u\cdot x} \sum_{y \in F} (-1)^{(\pi(x)+u)\cdot y}$$

Ya que $w(u) \leq l$ y $w(\pi(x)) \geq \lambda \geq l + 1$, obtenemos $\pi(x) \oplus u \neq 0$, por lo que las sumas sobre y son cero. Así $H(\hat{f})(u) = 0$ para toda u con $0 \leq w(u) \leq l$ por tanto, f tiene resistencia de orden l. ■

Como se requiere construir una función booleana l resistente, la cardinalidad del conjunto $\{z \in E^{\perp} : w(z) \geq l+1\}$ es

$$\sum_{i=1}^{q} \binom{q}{l+i}$$

Teorema 2.3.3. *Sea n, p, q tres enteros positivos con la condición $n = p + q$. Sea $t_u = \#\{x \in E \mid \pi(x) = u\}$ y $t = \max_u t_u$. La $\mathcal{N}_f \geq 2^{n-1} - t2^{q-1}$, donde f proviene de la construcción MM.*

Demostración:

Sea $f(x, y) = \pi(x) \cdot y + h(x)$ que proviene de la construcción de MM con todos los supuestos planteados a principios del capítulo.

Se ha analizado anteriormente en el capítulo 1, por definición de la transformada de Walsh-Hadamard, para cualquier $w \in \mathbb{F}_2^n, w = u + v$ con $u \in E^{\perp}$ y $v \in F^{\perp}$

$$H(\hat{f})(w) = \sum_{(x,y) \in E \times F} (-1)^{\pi(x)\cdot y + h(x) + w\cdot(x+y)}$$

$$= \sum_{x \in E} (-1)^{h(x)+v\cdot x} \sum_{y \in F} (-1)^{(\pi(x)+u)\cdot y}$$

Ahora, si $\pi(x) = u$ la suma de la derecha es 2^q y será cero en otro caso. Por lo que,

$$= 2^q \sum_{\{x \in E \mid \pi(x) = u\}} (-1)^{h(x)+v\cdot x}$$

Así, $\max_w |H(\hat{f})(w)| = \max_{u,v} |H(\hat{f})(u, v)| \leq 2^q max_u t_u = t2^q$. Por el teorema 2.8.1, sustituimos

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |H(\hat{f})(w)| \geq 2^{n-1} - \frac{1}{2} t2^q = 2^{n-1} - t2^{q-1}.$$

■

Teorema 2.3.4. *Dados enteros positivos n, l $(n \geq 4, 1 \leq l \leq n-3)$ y cualquier entero positivo t, sea q_t el menor q tal que*

$$t\left\{\binom{q}{l+1} + \binom{q}{l+2} + \cdots + \binom{q}{q}\right\} \geq 2^{n-q},$$

entonces tenemos $2^{q_1} \leq t2^{q_t}$, es decir, $min\{t2^{q_t} \mid t = 1, 2, \cdots\} = 2^{q_1}$

Para probar el teorema anterior, necesitamos algunos lemas. El lema siguiente es bien conocido y omitiremos

su demostración.

Lema 2.3.5. *Para enteros positivos n, k, tenemos la siguiente igualdad*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Lema 2.3.6. *Para enteros positivos n, k, tenemos la siguiente desigualdad*

$$2\left\{\binom{n}{k+1} + \binom{n}{k+2} + \cdots + \binom{n}{n}\right\} \leq \binom{n+1}{k+1} + \binom{n+1}{k+2} + \cdots + \binom{n+1}{n+1}$$

Demostración:

Por el lema anterior, tenemos

$$\binom{n+1}{k+1}+\binom{n+1}{k+2}+\cdots+\binom{n+1}{n}+\binom{n+1}{n+1} = \left\{\binom{n}{k+1} + \binom{n}{k}\right\}+\left\{\binom{n}{k+2} + \binom{n}{k+1}\right\}+\left\{\binom{n}{n} + \binom{n}{n-1}\right\}+1$$

Reagrupamos,

$$\left\{\binom{n}{k+1} + \binom{n}{k+2} + \cdots + \binom{n}{n}\right\} + \left\{\binom{n}{k} + \binom{n}{k+1} + \binom{n}{n-1} + \binom{n}{n}\right\}$$
$$= 2\left\{\binom{n}{k+1} + \binom{n}{k+2} + \cdots + \binom{n}{n}\right\} + \binom{n}{k}$$

■

Lema 2.3.7. *Si $q \geq q_t$, entonces*

$$t\left\{\binom{q}{l+1} + \binom{q}{l+2} + \cdots + \binom{q}{q}\right\} \geq 2^{n-q},$$

donde q_t es el valor definido en el teorema 2.3.4

Demostración:

Por la definición de q_t,

$$t\left\{\binom{q_t}{l+1} + \binom{q_t}{l+2} + \cdots + \binom{q_t}{q_t}\right\} \geq 2^{n-q_t},$$

Pues $q \geq q_t$, tenemos

$$t\left\{\binom{q}{l+1} + \binom{q}{l+2} + \cdots + \binom{q}{q_t} + \cdots + \binom{q}{q}\right\} \geq t\left\{\binom{q_t}{l+1} + \binom{q_t}{l+2} + \cdots + \binom{q_t}{q_t}\right\} \geq 2^{n-q_t} \geq 2^{n-q}$$

■

Ahora, probemos el teorema anterior,

Si $t = 1$, entonces $t2^{q_t} = 2^{q_1}$. Así que vamos a demostrar que $t2^{q_t} \geq 2^{q_1}$ cuando $t \geq 2$. Si $t \geq 2$, entonces hay un $r(r \geq 1)$ tal que $2^r \leq t < 2^{r+1}$. Si $q_1 - r \leq q_t$, entonces $t2^{q_t} \geq t2^{q_1-r} \geq 2^r 2^{q_1-r} = 2^{q_1}$. La demostración queda completada si $q_1 - r \leq q_t$. Queda por demostrar que el caso $q_t < q_1 - r$ no ocurre. Supongamos que $q_t < q_1 - r$, es decir, $q_t \leq q_1 - r - 1$. Entonces, por el lema 2.3.7,

$$t\left\{\binom{q_1-r-1}{l+1}+\binom{q_1-r-1}{l+2}+\cdots+\binom{q_1-r-1}{q_1-r-1}\right\} \geq 2^{n-(q_1-r-1)} \tag{2.2}$$

Por el lema 2.3.6,

$$\begin{aligned} &t\left\{\binom{q_1-r-1}{l+1}+\binom{q_1-r-1}{l+2}+\cdots+\binom{q_1-r-1}{q_1-r-1}\right\} \\ &\leq 2^{r+1}\left\{\binom{q_1-r-1}{l+1}+\binom{q_1-r-1}{l+2}+\cdots+\binom{q_1-r-1}{q_1-r-1}\right\} \\ &\leq 2^{r}\left\{\binom{q_1-r}{l+1}+\binom{q_1-r}{l+2}+\cdots+\binom{q_1-r}{q_1-r}\right\}. \end{aligned}$$

Aplicando el lema 2.3.6 en esta última desigualdad, obtenemos

$$\begin{aligned} &t\left\{\binom{q_1-r-1}{l+1}+\binom{q_1-r-1}{l+2}+\cdots+\binom{q_1-r-1}{q_1-r-1}\right\} \\ &\leq 2\left\{\binom{q_1-1}{l+1}+\binom{q_1-1}{l+2}+\cdots+\binom{q_1-1}{q_1-1}\right\} \end{aligned}$$

Por la desigualdad 2.2,

$$2\left\{\binom{q_1-1}{l+1}+\binom{q_1-1}{l+2}+\cdots+\binom{q_1-1}{q_1-1}\right\} \geq 2^{n-(q_1-r-1)}$$

Si $r \geq 1$, tenemos

$$\left\{\binom{q_1-1}{l+1}+\binom{q_1-1}{l+2}+\cdots+\binom{q_1-1}{q_1-1}\right\} \geq 2^{n-(q_1-r)} \geq 2^{n-(q_1-1)}$$

Por la definición de q_1, $q_1 \leq q_1 - 1$ pero esto es una contradicción.

2.3.1 π uno a uno

Siguiendo las ideas de Guillot, observamos que necesitamos tener todos los valores de $\pi(E)$. Para $u \in E^{\perp}$ construiremos la clase lateral $u+F^{\perp}$ y calculamos el peso mínimo de esta clase para cada u. Guardemos estos pesos en el conjunto $U(l) = \{u \in E^{\perp} : w(u+F^{\perp}) \geq l+1\}$. Para poder construir π uno a uno, debemos tener $q > p$ porque de paso queremos que nuestra función booleana sea balanceada. Para construir una función booleana con un orden (l) de resistencia alta debemos cuidar que la cardinalidad de $U(l) \geq 2^p$. Tomamos para construir la imagen de $\pi(E)$, 2^p elementos distintos de cero de $U(l)$, y lo asignamos de manera aleatoria. De igual manera generamos de forma aleatoria los valores de $h(E)$ usando cualquier generador pseudo-aleatorio.

Como π es uno a uno implica que $t = 1$, por lo que $\mathcal{N}_f = 2^{n-1} - 2^{q-1}$ en el teorema 2.3.3.

Teorema 2.3.8. *Para $f \in \mathbb{B}_n$, la máxima no linealidad de f es $\mathcal{N}_f = 2^{n-1} - 2^{q_1-1}$ y podemos obtenerlo si $t = 1$.*

Demostración:

Por el lema 2.3.7 tenemos que

$$t\left\{\binom{q}{l+1} + \binom{q}{l+2} + \cdots + \binom{q}{q}\right\} \geq 2^{n-q},$$

y además

$\mathcal{N}_f \geq 2^{n-1} - t2^{q-1}$.

Por lo tanto, para cada t (t = 1,2, ...), la máxima no linealidad se obtiene si q es el valor más pequeño que satisface la desigualdad anterior. Es decir, $max_q \mathcal{N}_f \geq 2^{n-1} - t2^{q_t-1}$. Por lo tanto, por el teorema 2.3.4, es decir, $max_{q,t}\mathcal{N}_f = 2^{n-1} - t2^{q_t-1} = 2^{n-1} - min_t t2^{q_t-1} = 2^{n-1} - 2^{q_1-1}$.

■

Lema 2.3.9. *Sean n, l, q_1 dados como el teorema 2.3.8. Entonces $q_1 \geq \lceil \frac{n}{2} \rceil + 1$*

Demostración:

Por la definición de q_1,

$$\binom{q_1}{l+1}+\binom{q_1}{l+2}+\cdots+\binom{q_1}{q_1}\geq 2^{n-q_1}.$$

Así,

$$\binom{q_1}{0}+\binom{q_1}{1}+\cdots+\binom{q_1}{l}+\binom{q_1}{l+1}+\binom{q_1}{l+2}+\cdots+\binom{q_1}{q_1}\geq \binom{q_1}{0}+\binom{q_1}{1}+\cdots+\binom{q_1}{l}+2^{n-q_1}$$

$$2^{q_1}\geq \binom{q_1}{0}+\binom{q_1}{1}+\cdots+\binom{q_1}{l}+2^{n-q_1}$$

$$2^{q_1}-2^{n-q_1}\geq \binom{q_1}{0}+\binom{q_1}{1}+\cdots+\binom{q_1}{l}$$

Como la parte derecha de la desigualdad anterior es positiva, $q_1 > n-q_1 \Rightarrow 2q_1 > n \Rightarrow q_1 \geq \lceil \frac{n}{2} \rceil + 1$ ■

Teorema 2.3.10. *Sea n un entero par, $n \geq 4$ y sea $q_1 = \frac{n}{2}+1$. Entonces la No linealidad de f es $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}}$*

Demostración:

La demostración es simple basta con sustituir el valor de $q_1 = \frac{n}{2}+1$ en el teorema 2.3.8 ■

Corolario 2.3.11. *Si n es par y $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}}$ entonces el limite superior del orden de la resistencia es*

$$l \leq \left\lfloor \frac{n}{4} + 0.238468\sqrt{n+2} \right\rfloor$$

Demostración:

Comencemos con el hecho que el teorema 2.3.8 habíamos obtenido que,

$$\binom{q_1}{l+1}+\binom{q_1}{l+2}+\cdots+\binom{q_1}{q_1}\geq 2^{n-q_1}.$$

Sustituimos $q_1 = \frac{n}{2}+1$ y nos queda

$$\binom{\frac{n}{2}+1}{l+1}+\binom{\frac{n}{2}+1}{l+2}+\cdots+\binom{\frac{n}{2}+1}{\frac{n}{2}+1}\geq 2^{\frac{n}{2}-1}. \tag{2.3}$$

Ahora recordemos que en estadística una de las distribuciones que se estudia es la distribución Binomial. Si X una variable aleatoria y tiene una distribución Binomial, es decir, $X \sim B\left(n, \frac{1}{2}\right)$ donde n es la cantidad de ensayos de Bernoulli entonces,

$$P(X \geq l) = \sum_{k=l}^{n} \binom{n}{k} \left(\frac{1}{2}\right)^n$$

Si tenemos ahora que $X \sim B\left(\frac{n}{2}+1, \frac{1}{2}\right)$, entonces

$$P(X \geq l+1) = \sum_{k=l+1}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{k} \left(\frac{1}{2}\right)^{\frac{n}{2}+1} = \left(\frac{1}{2}\right)^{\frac{n}{2}+1} \sum_{k=l+1}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{k}$$

Queda

$$2^{\frac{n}{2}+1} P(X \geq l+1) = \sum_{k=l+1}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{k}$$

Y por la ecuación 2.3 tenemos que $P(X \geq l+1) \geq \frac{1}{4}$.

Como $P(X \geq l+1) = 1 - P(X < l+1) = 1 - P(X \leq l) \geq \frac{1}{4} \Rightarrow P(X \leq l) \leq \frac{3}{4}$.

Recordemos que Abraham de Moivre demostró que bajo ciertas condiciones una distribución Binomial se puede aproximar a una distribución Normal de media $\mu = n \cdot a$ y desviación típica $\sigma = \sqrt{n \cdot a \cdot b}$, o sea, $X \sim B(n, a) \cong N(n \cdot a, \sqrt{n \cdot a \cdot b})$. (Nota: Recordemos que n es el tamaño de la muestra y $a = 1 - b$)

La bondad de la aproximación es tanto mejor cuanto mayor sea $n \geq 10$ y cuanto más próximo esté a de 0.5 con una corrección de $-\frac{1}{2}$ porque es ajustar una distribución discreta a una continua.

Decidimos dar una aproximación con la distribución Normal $B\left(\frac{n}{2}+1, \frac{1}{2}\right) \cong N\left(\frac{n}{4}+\frac{1}{2}, \sqrt{\frac{n}{8}+\frac{1}{4}}\right)$, o sea, $X \sim N\left(\frac{n}{4}+\frac{1}{2}, \sqrt{\frac{n}{8}+\frac{1}{4}}\right)$ y queremos ver que cuantil satisface que: $P(X \leq l) \leq \frac{3}{4}$, para esto usamos el paquete de estadística que trae el Mathematica 10.4 y nos arrojo que $l \leq \left\lfloor \frac{n}{4} + 0.238468\sqrt{n+2} \right\rfloor$. ■

2.3.2 π dos a uno

Para este caso es distinta la metodología, observamos que necesitamos tener todos los valores de $\pi(E)$ para $u \in E^{\perp}$.

Construiremos la clase lateral $u + F^{\perp}$, la misma clase lateral se divide en dos partes según la función lineal

$$v \mapsto v \cdot x_0.$$

Definimos $E_0 = \{v \in u + F^{\perp} \mid v \cdot x_0 = 0\}$ y $E_1 = \{v \in u + F^{\perp} \mid v \cdot x_0 = 1\}$. Calculamos el peso mínimo de E_0 y E_1, lo denotaremos por $w(E_0)$ y $w(E_1)$

Para cada $u \in E^{\perp}$ determinamos $w(E_0)$ y $w(E_1)$, si queremos construir una function booleana (l)-resistente,

necesitamos que máx$\{w(E_0), w(E_1)\} \geq l+1$. Después guardamos u con esta propiedad, es decir, guardamos el par $(u, 0/1)$(El $0/1$ corresponde al hecho de donde se alcanza el máximo en E_0 ó E_1) para definir después la función h, llamaremos a este conjunto U_l, esta claro que $U_l \subseteq E^{\perp}$. Con estos elementos de U_l construiremos la imagen de $\pi(E)$ y la imagen de $h(E)$. Al igual que en la sección anterior debemos cuidar que la cardinalidad de $U_l \geq 2^{p-1}$ y el valor de l debe satisfacer la siguiente condición:

$$\sum_{i=1}^{q} \binom{q}{l+i} \geq 2^{n-q-1}.$$

Por el teorema 2.3.3, como π es dos a uno, $t=2$, si sustituimos este valor en los resultados del teorema 2.3.3 y en el lema 2.3.7, nos queda que $\mathcal{N}_f \geq 2^{n-1} - 2^{q_2}$ y $\sum_{i=1}^{q_2} \binom{q_2}{l+i} \geq 2^{n-q_2-1}$.

Usando la primera parte de la demostración del teorema 2.3.4, para estimar q_2, como $t=2$ y $r=1$, entonces $q_1 - 1 \leq q_2$, ya habíamos calculado anteriormente $q_1 \geq \frac{n}{2}+1$, esto implica que $q_2 \geq \frac{n}{2}$.

Queremos encontrar valores de l de manera que $q_2 = \frac{n}{2}$, en particular se debe cumplir que:

$\left\{ \binom{\frac{n}{2}}{l+1} + \binom{\frac{n}{2}}{l+2} + \cdots + \binom{\frac{n}{2}}{\frac{n}{2}} \right\} \geq 2^{\frac{n}{2}-1}$,

Corolario 2.3.12. *Si n es par y $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}}$ entonces el limite superior del orden de resistencia es*

$$l \leq \left\lfloor \frac{n}{4} - \frac{1}{2} \right\rfloor$$

Demostración:

Siguiendo el procedimiento de la sesión anterior para encontrar una cota para el valor de la resistencia usando estadística y encontrar la desigual a partir de la distribución Binomial.

Si X una variable aleatoria y tiene una distribución Binomial, es decir, $X \sim B\left(\frac{n}{2}, \frac{1}{2}\right)$ donde $\frac{n}{2}$ es la cantidad de ensayos de Bernoulli entonces,

$$P(X \geq l+1) = \sum_{k=l+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} \left(\frac{1}{2}\right)^{\frac{n}{2}}$$

Queda

$$2^{\frac{n}{2}} P(X \geq l+1) = \sum_{k=l+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{k}$$

Y por la ecuación 2.3 tenemos que $P(X \geq l+1) \geq \frac{1}{2}$.

Como $P(X \geq l+1) = 1 - P(X < l+1) = 1 - P(X \leq l) \geq \frac{1}{2} \Rightarrow P(X \leq l) \leq \frac{1}{2}$

Decidimos dar una aproximación con la distribución Normal $B\left(\frac{n}{2},\frac{1}{2}\right) \cong N\left(\frac{n}{4},\sqrt{\frac{n}{8}}\right)$, o sea, $X \sim N\left(\frac{n}{4},\sqrt{\frac{n}{8}}\right)$ y queremos ver que cuantil satisface que: $P(X \leq l) \leq \frac{1}{2}$, para esto usamos el paquete de estadística que trae el Mathematica 10.4 y nos arrojo que $l \leq \left\lfloor \frac{n}{4} - \frac{1}{2} \right\rfloor$. ■

Del conjunto U_l tomemos exactamente 2^{p-1} y que ninguno sea el elemento cero para asegurar el balance. Construimos la imagen de π de tal manera que $\pi(x) = \pi(x + x_0)$.

La construcción de h la realizamos de tal manera que el valor de $h(x)$ es aleatorio y el valor de $h(x + x_0) = h(x) + h_u$, el valor h_u esta asociado al valor de la imagen de $\pi(x) = u$. Recordemos que en el capítulo 1, en la construcción de π dos a uno se llegó a la conclusión 1.2.3.2, la cual plantea que $h(x) + h(x + x_0) \neq v \cdot x_0 \Rightarrow h_u \neq v \cdot x_0$

Por otra parte, si el espacio vectorial F y la clase lateral $x_0 + F$ tienen peso mayor igual que k, entonces f satisface $PC(k-1)$.

2.3.3 π cuatro a uno

De igual manera, que el epígrafe anterior. Por hipótesis, $\pi^{-1}(u) = \{t, t+x_0, t+y_0, t+x_0+y_0\}$ es un subespacio afín de dimensión dos, $t \in V_u$ es el espacio vectorial $\{0, x_0, y_0, x_0 + y_0\}$ y para cualquier $v \in F^{\perp}$

Para $u \in E^{\perp}$ construimos la clase lateral $u + F^{\perp}$, la misma clase lateral queda partida en dos partes de acuerdo al funcional lineal

$$v \mapsto v \cdot x_0.$$

Definimos $E_0 = \left\{v \in u + F^{\perp} \mid \ v \cdot x_0 = 0\right\}$ y $E_1 = \left\{v \in u + F^{\perp} \mid \ v \cdot x_0 = 1\right\}$. Calculamos el peso mínimo de E_0 y E_1, lo denotaremos por $w(E_0)$ y $w(E_1)$

Para cada $u \in E^{\perp}$ determinamos $w(E_0)$ y $w(E_1)$, si queremos construir una function booleana (l)-resistente, necesitamos que máx$\{w(E_0), w(E_1)\} \geq l + 1$ y además $w(E_0) \geq l + 1$ $w(E_1) \geq l + 1$. Después guardamos u con esta propiedad, es decir, guardamos el par $(u, 0/1)$ para definir después la función h, llamaremos a este conjunto U_l, esta claro que $U_l \subseteq E^{\perp}$. Con estos elementos de U_l construiremos la imagen de $\pi(E)$ y la imagen de $h(E)$. Al igual que en la sección anterior debemos cuidar que la cardinalidad de $U_l \geq 2^{p-2}$. El valor de l para este caso debe satisfacer que:

$$\sum_{i=1}^{q} \binom{q}{l+i} \geq 2^{n-q-2}$$

Esto sucede por el hecho del teorema 2.3.3, como π es cuatro a uno, $t = 4$, si sustituimos este valor en los

resultados del teorema 2.3.3 y en el lema 2.3.7, nos queda que $\mathcal{N}_f \geq 2^{n-1} - 2^{q_4+1}$ y $\sum_{i=1}^{q_4} \binom{q_4}{l+i} \geq 2^{n-q_4-2}$.
Como parte de la demostración del teorema 2.3.4, para estimar q_4, como $t = 4$ y $r = 2$, entonces $q_1 - 2 \leq q_4$, ya habíamos calculado anteriormente $q_1 \geq \frac{n}{2} + 1$, esto implica que $q_4 \geq \frac{n}{2} - 1$ pero $q_2 \leq q_4$,por lo que para la desigualdad del lema 2.3.7 usaremos $q_4 = \frac{n}{2}$

Si tomamos $q_4 = \frac{n}{2}$ y sustituimos
$\left\{ \binom{\frac{n}{2}}{l+1} + \binom{\frac{n}{2}}{l+2} + \cdots + \binom{\frac{n}{2}}{\frac{n}{2}} \right\} \geq 2^{\frac{n}{2}-2}$,

Corolario 2.3.13. *Si n es par y $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}} \geq 2^{n-1} - 2^{\frac{n}{2}+1}$ entonces el limite superior del orden de resistencia es*

$$l \leq \left\lfloor \frac{n}{4} + 0.238468\sqrt{n} - \frac{1}{2} \right\rfloor$$

Demostración:

Siguiendo el procedimiento de la sesión anterior para encontrar una cota para el valor de la resistencia usando estadística y encontrar la desigual a partir de la distribución Binomial.
Si X una variable aleatoria y tiene una distribución Binomial, es decir, $X \sim B(\frac{n}{2}, \frac{1}{2})$ donde $\frac{n}{2}$ es la cantidad de ensayos de Bernoulli entonces,

$$P(X \geq l+1) = \sum_{k=l+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} \left(\frac{1}{2}\right)^{\frac{n}{2}}$$

Queda

$$2^{\frac{n}{2}} P(X \geq l+1) = \sum_{k=l+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{k}$$

Y por el lema 2.3 tenemos que $P(X \geq l+1) \geq \frac{1}{4}$

Como $P(X \geq l+1) = 1 - P(X < l+1) = 1 - P(X \leq l) \geq \frac{1}{4} \Rightarrow P(X \leq l) \leq \frac{3}{4}$
Decidimos dar una aproximación con la distribución Normal $B\left(\frac{n}{2}, \frac{1}{2}\right) \cong N\left(\frac{n}{4}, \sqrt{\frac{n}{8}}\right)$, o sea, $X \sim N\left(\frac{n}{4}, \sqrt{\frac{n}{8}}\right)$ y queremos ver que cuantil satisface que: $P(X \leq l) \leq \frac{3}{4}$, para esto usamos el paquete de estadística que trae el Mathematica 10.4 y nos arrojo que $l \leq \left\lfloor \frac{n}{4} + 0.238468\sqrt{n} - \frac{1}{2} \right\rfloor$. ■

Al conjunto U_l tomemos exactamente 2^{p-2} y que ninguno sea el elemento cero para asegurar el balance. Construimos la imagen de π de tal manera que $\pi(t) = \pi(t + x_0) = \pi(t + y_0) = \pi(t + x_0 + y_0)$.
La construcción de h la realizamos de tal manera que los valores de $h(t)$ y $h(t + y_0)$ sean aleatorios. Los valores de $h(t + x_0) = h(t) + h_u$ y $h(t + x_0 + y_0) = h(t + y_0) + h_u + 1$, el valor h_u esta asociado al valor de la

imagen de $\pi(t) = u$.

La construcción de h esta dada por los condiciones impuestas en el capítulo 1 en la construcción de π cuatro a uno.

Al igual que el el epígrafe anterior, si el espacio vectorial F y la clase lateral $x_0 + F$ tienen peso mayor o igual que k, entonces f satisface $PC(k-1)$.

2.4 Construcción de f

Ya con esto tenemos todos los ingredientes para construir la función booleana.

Recordemos que $f(z) = \pi(x) \cdot y + h(x)$ con $z = x + y = u + v$; $x \in E, y \in F, u \in E^{\perp}$ y $v \in F^{\perp}$, o sea, $z = \{z_1, z_2, \ldots, z_q, z_{q+1}, \ldots, z_n\}, x = \{0, 0, \ldots, 0, x_{q+1}, \ldots, x_n\}, F \ni y = (z_1, z_2, \ldots, z_q) \cdot G_F = (z_1, z_2, \ldots, z_q) \cdot (I \mid A)$, donde G_F es la matriz generadora de F con dimensiones $q \times n$, $I_{q\times q}$ es la matriz idéntica y $A_{q,n-q} = \begin{pmatrix} A_1 \\ A_2 \\ \cdots \\ A_q \end{pmatrix}$.

¿Cómo determino x e y a partir de z?

- Tomo las q primeras coordenadas de z, o sea, $\hat{z} = (z_1, z_2, \ldots, z_q)$.
- Tenemos a G_F la matriz generadora de F por lo que para obtener $F \ni y = (z_1, z_2, \ldots, z_q) \cdot G_F = (z_1, z_2, \ldots, z_q, 0, 0, \ldots, 0) \cdot (I \mid A) = (z_1, z_2, \ldots, z_q) + (z_1, z_2, \ldots, z_q) \cdot A)$.
- Ya tenemos y, conocemos a z por lo que

  $x = y+z = (z_1, z_2, \ldots, z_q, (z_1, z_2, \ldots, z_q)A_1, (z_1, z_2, \ldots, z_q)A_2, \ldots, (z_1, z_2, \ldots, z_q)A_q)+(z_1, z_2, \ldots, z_q, z_{q+1}, \ldots, z_n) =$

  $(0_1, 0_2, \ldots, 0_q, z_{q+1} + (z_1, z_2, \ldots, z_q)A_1, z_{q+2} + (z_1, z_2, \ldots, z_q)A_2, \ldots, z_{q+n-q} + (z_1, z_2, \ldots, z_q)A_q) \in E.$
- Tenemos ya calculado todas las imágenes de π y de h. Por tanto, ya podemos construir f

2.5 Sobre el número de funciones en esta nueva construcción

En la introducción de la tesis se había comentado dentro de las contribuciones que se obtuvo un factor no trivial en cuanto al número de funciones que se pueden obtener con la construcción propuesta.

Como se ha podido constatar en este trabajo las propiedades criptográficas de f solo dependen de la propiedades del código F y de la imagen de $\pi(E)$. Una vez que se haya elegido la imagen $\pi(E)$ y el código, tenemos a elegir una permutación y la función booleana h nos lleva a $2^p! \times 2^{2^p}$ diferentes funciones con propiedades criptográficas similares. A esto hay que adicionarle por el isomorfismo de concatenación $\phi : \mathbb{F}_{2^{2k}} \longrightarrow \mathbb{F}_2^{2k+1}$, o sea, existen 2^{2k} maneras distintas de construir este isomorfismo, quitemos de aquí el cero y serían $2^{2k} - 1$. Por lo que, el número de funciones que se puede construir con esta nueva construcción fijando la imagen de π y eligiendo el código F tenemos que es un número no trivial $2^p! \times 2^{2^p} \times (2^{2k} - 1)$

2.6 Ejemplos

2.6.1 π uno a uno

Para este ejemplo tomaremos $n = 12$, por lo que la $dim(F) = 7$ y la $dim(E) = 5$ fue la que se selecciono. Ahora

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

$$G_{F^\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

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

$$G_{E^\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Construimos todas las clases laterales de la forma $u + F^\perp$ donde $u \in E^\perp$ y calculamos los pesos mínimos de cada clase.

En este ejemplo se tiene que $\text{mín}_{u \in E^\perp}(u + F^\perp) = \{0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, 1, 1, 2, 2,$
$2, 2, 3, 3, 2, 2, 3, 3, 3, 3, 4, 4, 1, 2, 2, 3, 2, 3, 3, 4, 2, 2, 3, 3, 3, 3, 4, 4, 2, 2, 3, 3, 3, 3, 4, 4, 2, 1, 3, 2,$
$3, 2, 4, 3, 1, 2, 2, 3, 2, 3, 3, 4, 2, 3, 3, 4, 3, 4, 4, 5, 2, 2, 3, 3, 3, 3, 4, 4, 3, 3, 4, 4, 4, 4, 5, 5, 2, 3, 3, 4,$
$3, 4, 4, 5, 3, 3, 4, 4, 4, 4, 5, 5, 3, 3, 4, 4, 4, 4, 5, 5, 3, 2, 4, 3, 4, 3, 5, 4\}$

Por el corolario 2.3.11 sustituyendo $n = 12$ la máxima resistencia a la que podemos aspirar es $l = 3$, entonces como E tiene 32 elementos, escogemos exactamente de $E^\perp$ de manera que $\text{mín}_{u \in E^\perp}(u + F^\perp) \geq 4$ pero con $u \neq 0$ para asegurar que la función sea balanceada y a su vez estos vectores serán las imágenes de π, o sea,
$\pi(E) = \{\{0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0\}, \{0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0\}, \{0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0\},$
$\{0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0\}, \{0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0\}, \{0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0\},$
$\{0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0\}, \{0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0\}, \{0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0\},$
$\{1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0\}, \{1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0\}, \{1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0\},$

$\{1,0,0,1,1,1,0,0,0,0,0,0\},\{1,0,1,0,1,1,0,0,0,0,0,0\},\{1,0,1,0,1,1,1,0,0,0,0,0\},$
$\{1,0,1,1,0,1,0,0,0,0,0,0\},\{1,0,1,1,0,1,1,0,0,0,0,0\},\{1,0,1,1,1,0,0,0,0,0,0,0\},$
$\{1,0,1,1,1,0,1,0,0,0,0,0\},\{1,1,0,0,0,1,1,0,0,0,0,0\},\{1,1,0,0,1,0,1,0,0,0,0,0\},$
$\{1,1,0,0,1,1,0,0,0,0,0,0\},\{1,1,0,1,0,1,0,0,0,0,0,0\},\{1,1,0,1,0,1,1,0,0,0,0,0\},$
$\{1,1,0,1,1,0,0,0,0,0,0,0\},\{1,1,0,1,1,0,1,0,0,0,0,0\},\{1,1,1,0,0,1,0,0,0,0,0,0\},$
$\{1,1,1,0,0,1,1,0,0,0,0,0\},\{1,1,1,0,1,0,0,0,0,0,0,0\},\{1,1,1,0,1,0,1,0,0,0,0,0\},$
$\{1,1,1,1,0,1,0,0,0,0,0,0\},\{1,1,1,1,1,0,0,0,0,0,0,0\}\}$

Ahora los valores $h(E)$ los obtengo de manera aleatoria usando cualquier generador pseudo-aleatorio binario. En resumen nuestra función tendrá las siguientes propiedades,

- Balanceada
- $\mathcal{N}_f = 1984$
- 3-resistente
- $grad(f) = 6$
- Inmunidad algebraica de orden 5

2.6.2 π dos a uno

Para este ejemplo seguimos construyendo funciones booleanas de 12 variables. Para este caso $dim(E) = 6$ y $dim(F) = 6$ y las matrices generadoras fueron:

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

$$G_{F^\perp} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

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

$$G_{E^\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Tomamos $x_0 = \{0,0,0,0,0,0,1,0,1,1,1,1\}$

Construimos las clases laterales de la forma $u + F^\perp$ donde $u \in E^\perp$ y para cada $\{v \in u + F^\perp : v \cdot x_0 = \mathbb{F}_2 = \{0,1\}\}$, lo dividimos en dos subconjuntos y calculamos los pesos mínimos de cada subconjunto.

En este ejemplo se tiene que

u	E_0	E_1
1	0	2
2	1	3
3	1	1
4	2	2
5	1	1
6	2	2
7	2	2
8	3	3
9	1	3
10	2	3
11	2	2
12	3	3
13	2	2
14	3	2
15	3	3
16	3	3
17	1	3
18	2	3
19	2	2
20	3	3
21	2	2
22	3	2
23	3	1
24	3	2
25	2	3

u	E_0	E_1
26	3	4
27	3	3
28	3	4
29	3	2
30	4	3
31	3	2
32	4	3
33	1	3
34	2	3
35	2	2
36	2	3
37	2	2
38	3	2
39	3	3
40	3	2
41	2	3
42	2	2
43	3	3
44	3	3
45	3	2
46	3	1
47	3	3
48	2	2
49	2	3
50	1	2

u	E_0	E_1
51	3	3
52	2	2
53	3	2
54	2	1
55	3	2
56	2	2
57	3	4
58	2	3
59	3	4
60	2	3
61	4	3
62	3	2
63	4	3
64	3	3

Ahora seleccionamos aquellas posiciones que el peso sea mayor o igual que 3, ya que en las funciones booleanas a las cuales puedo aspirar a construir son 2-resistentes según se vio en el corolario 2.3.11. En el caso que el peso este en E_0 se guarda $(u, 0)$ y en caso que el peso se alcance en E_1 se guarda $(u, 1)$. Sin perdida de generalidad se tomó

$$\begin{pmatrix} u & h \\ \{0,0,0,1,1,1,0,0,0,0,0,0\} & 0 \\ \{0,0,1,0,0,0,0,0,0,0,0,0\} & 1 \\ \{0,0,1,0,0,1,0,0,0,0,0,0\} & 1 \\ \{0,0,1,0,1,1,0,0,0,0,0,0\} & 0 \\ \{0,0,1,1,0,1,0,0,0,0,0,0\} & 0 \\ \{0,0,1,1,1,0,0,0,0,0,0,0\} & 0 \\ \{0,0,1,1,1,1,0,0,0,0,0,0\} & 0 \\ \{0,1,0,0,0,0,0,0,0,0,0,0\} & 1 \\ \{0,1,0,0,0,1,0,0,0,0,0,0\} & 1 \\ \{0,1,0,0,1,1,0,0,0,0,0,0\} & 0 \\ \{0,1,0,1,0,1,0,0,0,0,0,0\} & 0 \\ \{0,1,0,1,1,0,0,0,0,0,0,0\} & 0 \\ \{0,1,0,1,1,1,0,0,0,0,0,0\} & 0 \\ \{0,1,1,0,0,0,0,0,0,0,0,0\} & 1 \\ \{0,1,1,0,0,1,0,0,0,0,0,0\} & 1 \\ \{0,1,1,0,1,0,0,0,0,0,0,0\} & 0 \end{pmatrix} \begin{pmatrix} u & h \\ \{0,1,1,0,1,1,0,0,0,0,0,0\} & 1 \\ \{0,1,1,1,0,0,0,0,0,0,0,0\} & 0 \\ \{0,1,1,1,0,1,0,0,0,0,0,0\} & 0 \\ \{0,1,1,1,1,0,0,0,0,0,0,0\} & 0 \\ \{0,1,1,1,1,1,0,0,0,0,0,0\} & 0 \\ \{1,0,0,0,0,0,0,0,0,0,0,0\} & 1 \\ \{1,0,0,0,0,1,0,0,0,0,0,0\} & 1 \\ \{1,0,0,0,1,1,0,0,0,0,0,0\} & 1 \\ \{1,0,0,1,0,1,0,0,0,0,0,0\} & 0 \\ \{1,0,0,1,1,0,0,0,0,0,0,0\} & 0 \\ \{1,0,0,1,1,1,0,0,0,0,0,0\} & 0 \\ \{1,0,1,0,0,0,0,0,0,0,0,0\} & 1 \\ \{1,0,1,0,1,0,0,0,0,0,0,0\} & 0 \\ \{1,0,1,0,1,1,0,0,0,0,0,0\} & 0 \\ \{1,0,1,1,0,0,0,0,0,0,0,0\} & 0 \\ \{1,0,1,1,0,1,0,0,0,0,0,0\} & 0 \end{pmatrix}$$

Estos serán los valores de π y h que usaremos para construir la función booleana.

Ahora construyó a π de manera que $\pi(t) = \pi(t + x_0)$ donde $t \in E$. Después, construimos los valores de $h(t)$ de manera aleatoria y de manera que $h(x_0 + t) = h(t) + h_u$, el valor h_u esta asociado al valor de la imagen de $\pi(t) = u$.

Ya tenemos todos los valores de $\pi(E)$ y $h(E)$. Ahora,

En resumen nuestra función tendrá las siguientes propiedades,

- Balanceada
- $\mathcal{N}_f = 1984$
- 2-resistente
- $grad(f) = 6$
- Inmunidad algebraica de orden 5

2.6.3 π cuatro a uno.

Construyamos también una función de 12 variables, siguiendo la metodología descrita en este trabajo, pongamos a $dimE = 6$ y $dimF = 6$ al igual que en el ejemplo anterior. Tenemos a

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

$$G_{F^\perp} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

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

$$G_{E^\perp} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$x_0 = \{0,0,0,0,0,0,1,0,1,1,1,1\}$, $y_0 = \{0,0,0,0,0,0,1,1,1,0,0,0\}$,

Construimos las clases laterales de la forma $u + F^{\perp}$ donde $u \in E^{\perp}$ y para cada $\{v \in u + F^{\perp} : v \cdot x_0 = \mathbb{F}_2 = \{0, 1\}\}$, lo dividimos en dos subconjuntos y calculamos los pesos mínimos de cada subconjunto.

En este ejemplo se tiene que

#	E_0	E_1
1	0	2
2	1	3
3	1	1
4	2	2
5	1	1
6	2	2
7	2	2
8	3	3
9	1	2
10	2	3
11	2	2
12	3	3
13	2	2
14	3	3
15	3	3
16	4	4
17	1	3
18	2	4
19	2	2
20	3	3

21	2	2
22	3	3
23	3	3
24	4	4
25	2	3
26	3	4
27	3	3
28	4	4
29	3	3
30	4	4
31	4	4
32	5	5
33	1	2
34	2	3
35	2	2
36	3	3
37	2	2
38	3	3
39	3	3
40	4	4

41	1	1
42	2	2
43	2	2
44	3	3
45	2	2
46	3	3
47	3	3
48	4	4
49	2	3
50	3	4
51	3	3
52	4	4
53	3	3
54	4	4
55	4	4
56	5	5
57	2	2
58	3	3
59	3	3
60	4	4
61	3	3
62	4	4
63	4	4
64	5	5

Cabe aclarar que aquí cambia cambia un poco los criterios para la resistencia, en este ejemplo, debemos construir π cuatro a uno. Además, queremos construir una función l-resistente, entonces los vectores que escojamos de E_0 y E_1 tienen que cumplir $E_0 \geq E_1 \geq l + 1$ o $E_1 \geq E_0 \geq l + 1$

Queremos construir una función 3-resistente entonces escojamos los vectores de $u \in E^{\perp}$ no vacíos que en la

tabla anterior en la segunda y tercera columna sea su peso mayor o igual que 4.

Así nos queda $u, 0/1$

$$\begin{pmatrix} & & & & & & & u & & & & & h \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$E = \{t, x_0 + y_0 + t, x_0 + t, y_0 + t\}, cont \in E$ en ese orden.

A π la construimos de manera que $\pi(t) = \pi(x_0 + y_0 + t) = \pi(x_0 + t) = \pi(y_0 + t)$ donde $t \in E$. Los valores para cada t y $y_0 + t$ los generamos de manera aleatoria.

Me explico los 16 primeros de manera aleatoria y los 16 últimos también, o sea, $h(t)$ y $h(t + y_0)$ los genero aleatoriamente. Los valores de $h(t + x_0) = h(t) + h_u$ y los valores de $h(x_0 + y_o + t) = h(t) + h_u + 1$, sabiendo el valor h_u esta asociado al valor de la imagen de $\pi(x) = u$.

Entonces, $h(t) = \{0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0\}$ y $h(t + y_0) = \{0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1\}$, como la columna última de la matriz anterior 2.6.3 todos sus elementos son ceros, por lo que, $h(t + x_0) = h(t)$ y $h(t + x_0 + y_0) = \{1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0\}$.

Así ya tenemos todos los valores de $\pi(E)$ y $h(E)$, el próximo paso es construir la función booleana.

Mi función booleana tendrá las siguientes propiedades:

- Balanceada
- $\mathcal{N}_f = 1984$
- 3-resistente
- $grad(f) = 5$
- Inmunidad algebraica de orden 4

π cuatro a uno.

$n = 8$

Construyamos también una función de 8 variables, siguiendo la metodología descrita en este trabajo, pongamos a $dimE = 4$ y $dimF = 4$ al igual que en el ejemplo anterior.

Tenemos a

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

$$F^{\perp} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

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

$$E^{\perp} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$x_0 = \{0,0,0,0,1,0,0,0\}$, $y_0 = \{0,0,0,0,0,1,0,0\}$,

$V = \{\{0,0,0,0,0,0,0,0\}, \{0,0,0,0,0,0,0,1\}, \{0,0,0,0,0,0,1,0\}, \{0,0,0,0,0,0,1,1\}\}$

Construimos las clases laterales de la forma $u + F^{\perp}$ donde $u \in E^{\perp}$ y para cada $\{v \in u + F^{\perp} : v \cdot x_0 = \mathbb{F}_2 = \{0,1\}\}$, lo dividimos en dos subconjuntos y calculamos los pesos mínimos de cada subconjunto.

En este ejemplo se tiene que

$$\begin{pmatrix} E^{\perp} & E_0 & E_1 \\ \{1\} & 0 & 3 \\ \{2\} & 1 & 2 \\ \{3\} & 1 & 3 \\ \{4\} & 2 & 2 \\ \{5\} & 1 & 2 \\ \{6\} & 2 & 1 \\ \{7\} & 1 & 3 \\ \{8\} & 2 & 2 \\ \{9\} & 1 & 3 \\ \{10\} & 2 & 2 \\ \{11\} & 2 & 4 \\ \{12\} & 3 & 3 \\ \{13\} & 1 & 3 \\ \{14\} & 2 & 2 \\ \{15\} & 2 & 4 \\ \{16\} & 3 & 3 \end{pmatrix}$$

Cabe aclarar que aquí cambia un poco los criterios para la resistencia, en este ejemplo, debemos construir π cuatro a uno. Además, queremos construir una función l-resistente, entonces los vectores que escojamos de E_0 y E_1 tienen que cumplir $E_0 \geq E_1 \geq l+1$ o $E_1 \geq E_0 \geq l+1$

Para construir una función 1-resistente, entonces escojamos $4, 8, 11, 16$

Así nos queda $u, 0/1$

$$\begin{pmatrix} u & h \\ \{0,0,0,0,0,0,0,0\} & 1 \\ \{0,0,0,1,0,0,0,0\} & 1 \\ \{0,0,1,0,0,0,0,0\} & 1 \\ \{0,0,1,1,0,0,0,0\} & 0 \\ \{0,1,0,0,0,0,0,0\} & 1 \\ \{0,1,0,1,0,0,0,0\} & 0 \\ \{0,1,1,0,0,0,0,0\} & 1 \\ \{0,1,1,1,0,0,0,0\} & 0 \\ \{1,0,0,0,0,0,0,0\} & 1 \\ \{1,0,0,1,0,0,0,0\} & 0 \\ \{1,0,1,0,0,0,0,0\} & 1 \\ \{1,0,1,1,0,0,0,0\} & 0 \\ \{1,1,0,0,0,0,0,0\} & 1 \\ \{1,1,0,1,0,0,0,0\} & 0 \\ \{1,1,1,0,0,0,0,0\} & 1 \\ \{1,1,1,1,0,0,0,0\} & 0 \end{pmatrix}$$

$E = \{t, y_0 + t, x_0 + t, x_0 + y_0 + t\}, cont \in E$ en ese orden.

Los elementos de t y $y_0 + t$ los genero de manera aleatoria.

Las u que escogimos son:

$\{0,0,1,1,0,0,0,0\}, \{0,1,1,1,0,0,0,0\}, \{1,0,1,0,0,0,0,0\}, \{1,1,1,1,0,0,0,0\}$ y los valores de h correspondientes son: $0,0,1,0$

$h = \{1,0,0,1,1,0,1,0,1,0,1,1,0,1,1,1\}$

O sea, los 8 primeros de manera aleatoria los cuatro siguientes los sumo con $\{0,0,1,0\}$ y los cuatro últimos también los sumo con $\{0,0,1,0\}$ pero le asigno lo contrario, o sea, cada elemento de la última suma, le adiciono uno modulo dos.

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

Ahora construyo f cuya tabla de verdad es

$\{1,0,0,1,1,0,1,0,1,0,1,1,0,1,1,1,1,1,0,0,1,1,0,1,0,0,0,0,1,1,1,0,1,1,0,0,1,1,0,1,0,1,0,$
$0,0,0,1,0,0,1,0,0,1,1,0,1,0,1,1,0,1,0,0,0,1,0,0,0,1,1,1,0,1,1,1,1,1,1,1,0,0,0,1,0,0,1,0,$
$0,0,1,1,1,1,1,1,0,0,1,1,0,1,0,0,0,1,0,0,0,0,0,0,1,1,0,1,1,1,1,0,1,1,0,0,0,0,0,0,1,1,1,0,$
$0,1,1,0,1,0,0,1,0,0,1,0,0,0,0,1,1,0,0,1,0,1,0,0,0,1,1,1,0,1,1,0,0,1,1,0,1,0,0,1,1,1,1,1,$
$0,1,1,0,1,1,0,0,1,0,1,1,1,0,1,0,0,0,1,1,1,1,0,0,0,1,0,1,1,1,1,1,1,0,0,0,1,0,0,1,0,0,0,$
$0,0,0,0,0,0,1,1,0,0,1,0,1,1,1,0,0,0,0,0,0,0,1,1,0,1,1,1,1,0,1,1,1,1,1,1,1,1,0,0\}$

- Balanceada
- $\mathcal{N}_f = 112$
- 1-resistente
- $grad(f) = 3$
- Inmunidad algebraica de orden 3

Anexos

Campo de funciones algebraicas

A.1 Introducción

El contenido de este anexo se tomó de los libros [5] y [29]. Además de aportaciones del autor.

- Sea K un campo. Un campo F se dice que es una **extensión** de K si K es un subcampo de F.
- Sea F una extensión de K y sea S un subconjunto de F. Denotaremos por $K(S)$ al subcampo mas pequeño de F que contiene a K y a S.
- El campo $K(S)$ es una extensión de K y diremos que es el campo que se obtiene de K *pegándole* los elementos de S.
- Si S es un conjunto finito, digamos $S = \{a_1, \ldots, a_n\}$, denotaremos a $K(S)$ por $K(a_1, \ldots, a_n)$.
- Si F es una extensión de K entonces F es un espacio vectorial sobre K. Llamaremos a la dimensión de F sobre K el **grado de la extensión** de F sobre K y lo denotaremos por

$$[F : K].$$

- Por comodidad usaremos la notación F/K para indicar que F es una extensión de K. Diremos que una extensón F/K es **simple** si $F = K(a)$ para alguna $a \in F$.

Nota que el grado puede ser finito o infinito. Diremos que F es una extensión finita de K si $[F : K]$ es finito

A.2 Definición

- Sea F/K una extensión y sea $a \in F$. Decimos que el elemento a es **algebraico** sobre K si existe un polinomio $f(x) \in K[x]$ tal que $f(a) = 0$, en caso contrario decimos que a es **trascendente** sobre K.

- Diremos que la extensión F/K es una **extensión algebraica** de K si todo elemento de F es algebraico sobre K. En caso de existir al menos un elemento $x \in F$ que sea trascendente sobre K diremos que F/K es una **extensión trascendente** de K.

- Cada elemento algebraico $a \in F$ le podemos asociar, de manera única, el polinomio mónico irreducible $p(x) \in K[x]$ que tiene como raíz a a. Denotaremos a dicho polinomio por $Irr(K, a)$ y le llamaremos el **polinomio mínimo de** a sobre K.

- Si $a, b \in F$ son elementos algebraicos sobre K entonces $a - b$ y ab^{-1} tambien lo son, pues pertenecen al campo $K(a, b)$ el cual es una extensión algebraica de K.

- Definimos la **cerradura algebraica** de K en F como el subcampo

$$\tilde{K} := \{a \in F | a \text{ es algebraico sobre } K\}.$$

  Si $K = \tilde{K}$ decimos que K es **algebraicamente cerrado** en F.

A.3 Campos finitos

- Sea p un primo. Entonces $\mathbb{Z}/p\mathbb{Z}$ es un campo finito con p elementos. Lo denotaremos por $\mathbb{F}_p$. Sea F cualquier campo finito.

- Llamaremos a p la **característica** de F y a $\mathbb{F}_p$, el subcampo generado por 1, su **campo primo**.

- Por definición F es un espacio vectorial sobre $\mathbb{F}_p$, por lo que el número de elementos de F es p^n para alguna n (de hecho, $n = [F : \mathbb{F}_p]$).

- Sea $q = p^n$, p un primo, n un natural. El campo de descomposición del polinomio $f = x^q - x \in \mathbb{F}_p[x]$ es un campo finito con q elementos. Los elementos de $\mathbb{F}_q$ son las raíces (todas distintas) de f.

- Para construir directamente campos finitos hacemos uso de polinomios mónicos irreducibles: Sea $f(x) \in \mathbb{F}_p[x]$ un polinomio mónico irreducible de grado n.

A.3.1 El campo finito $\mathbb{F}_{2^n}$

El campo $\mathbb{F}_{2^n}$, denominado un campo finito de característica dos o campo finito binario, puede ser visto como un espacio vectorial de dimensión n sobre el campo $\mathbb{F}_2$.
Sea

$$f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0$$

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

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

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

$$\mathbb{F}_2^n = \{(a_{n-1}a_{n-2}\cdots a_1a_0) : a_i \in \{0,1\}\}$$

A.3.2 Ejemplos

Ejemplo 1: En el anillo $\mathbb{F}_2[x]$ existe un único polinomio irreducible de grado dos: $x^2 + x + 1$. Tenemos que

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1).$$

Podemos listar todos los elementos de $\mathbb{F}_4$:

$$\mathbb{F}_4 = \{aX + b | a, b \in \mathbb{F}_2\} = \{0, 1, X, X + 1\},$$

donde X es la imagen de x mod (x^2+x+1). En algunos casos es conveniente describir los elementos utilizando un generador del grupo cíclico: sea α tal que $\alpha^2 + \alpha + 1 = 0$. Vemos que $\alpha^2 = \alpha + 1$ por lo que

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}.$$

Ejemplo 2: Los polinomios x^3+x+1 y x^3+x^2+1 son los únicos polinomios cúbicos irreducibles en $\mathbb{F}_2[x]$. Entonces, si α es tal que $\alpha^3+\alpha^2+1=0$, tenemos que $\mathbb{F}_8=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$.

A.4 El campo de funciones racionales K(x)

Sea K un campo y x un elemento trascendente sobre K. Sea $K[x]$ el anillo de polinomios en la "variable" x con coeficientes en K. El campo de funciones racionales $K(x)$ se define como

$$K(x) := \{\frac{f(x)}{q(x)} |\ f(x), q(x) \in K[x],\ q(x) \neq 0\}.$$

Sea $p(x) \in K[x]$ un polinomio irreducible. Definimos

$$\mathcal{O}_{p(x)} := \{\frac{f(x)}{q(x)} \in K(x) |\ p(x)\ \not| q(x)\}$$

y

$$P_{p(x)} := \{\frac{f(x)}{q(x)} \in K(x) |\ p(x) | f(x),\ p(x)\ \not| q(x)\}.$$

Definimos una función

$$\begin{array}{rccc} v_{p(x)}: & K(x) & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ & z & \mapsto & n_{p(x)}, \end{array}$$

donde, $n_{p(x)} = i$ si $z = p(x)^i h$ y $v_{p(x)}(0) := \infty$. Podemos verificar que

$$\mathcal{O}_{p(x)} = \{z \in K(x) | v_{p(x)}(z) \geq 0\}$$

y que

$$P_{p(x)} = \{z \in K(x) | v_{p(x)}(z) > 0\}.$$

Nota: Al anillo $\mathcal{O}_{p(x)}$ **anillo de valoración** y a $P_{p(x)}$ le llamaremos **lugar**. Asociamos al polinomio irreducible $p(x)$ el campo $K_{p(x)} \subset K(x)$: Al ser $P_{p(x)}$ un ideal maximal del anillo $\mathcal{O}_{p(x)}$ podemos definir el **campo residual** $K_{p(x)} := \mathcal{O}_{p(x)}/P_{p(x)}$. Definimos el **grado de un lugar** $P_{p(x)}$ como

$$grado(P_{p(x)}) := [K_{p(x)} : K],$$

el grado de la extensión $K_{p(x)}/K$. Notemos que $grado(P_{p(x)}) = grado(p(x)) < \infty$. **Ejemplo:** Los dos lugares

de $\mathbb{F}_2(x)$ de grado 3 son P_{x^3+x+1} y $P_{x^3+x^2+1}$. En ambos casos su campo residual es $\mathbb{F}_8$

En $K(x)$ existe otro anillo de valoración:

$$\mathcal{O}_\infty := \{\frac{f(x)}{q(x)} \in K(x) | grado(f(x)) \leq grado(q(x))\}$$

con ideal maximal

$$P_\infty = \{\frac{f(x)}{g(x)} \in K(x) | grado(f(x)) < grado(q(x))\}.$$

El lugar P_∞ es llamado el **lugar infinito** de $K(x)$.

A.5 Lugares y valoraciones

Definición A.5.1. Un **anillo de valoración** de F/K es un anillo $\mathcal{O} \subseteq F$ tal que

1. $K \subsetneqq \mathcal{O} \subsetneqq F$, y
2. para cualquier $z \in F$, $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Teorema A.5.2. *Sea $\mathcal{O}$ un anillo de valoración de F/K, P su ideal maximal. Entonces*

1. *P es un ideal principal.*
2. *si $P = t\mathcal{O}$ entonces toda $0 \neq z \in F$ tiene una representación única de la forma $z = t^n u$ para alguna $n \in \mathbb{Z}$, y $u \in \mathcal{O}^*$.*
3. *$\mathcal{O}$ es un dominio de ideales principales. De manera más precisa, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal entonces $I = t^n\mathcal{O}$ para alguna $n \in \mathbb{N}$.*

Definición A.5.3. Un anillo $\mathcal{O}$ de un campo de funciones F/K con las propiedades del teorema anterior se le llama **anillo de valoración discreta**.

Definición A.5.4.
1. Un **lugar** de un campo de funciones F/K es el ideal maximal de un anillo de valoración $\mathcal{O}$ de F/K. Todo elemento $t \in P$ tal que $P = t\mathcal{O}$ es llamado, dependiendo del contexto, **elemento primo**, **parámetro local** o **variable de uniformización**.
2. $\mathbb{P}_F := \{P | P$ es un lugar de F/K$\}$.

$$\mathcal{O} = \{z \in F | z^{-1} \notin P\}.$$

Diremos entonces que $\mathcal{O}_P := \mathcal{O}$ es el **anillo de valoración del lugar** P.

Definición A.5.5. Una **valoración discreta** de F/K es una función

$$v : F \to \mathbb{Z} \cup \{\infty\}$$

con las siguientes propiedades:

1. $v(x) = \infty$ si y solo si $x = 0$.
2. $v(xy) = v(x) + v(y)$ para toda $x, y \in F$.
3. $v(x + y) \geq min\{v(x), v(y)\}$.
4. Existe un elemento $z \in F$ tal que $v(z) = 1$.
5. $v(a) = 0$ para toda $a \in K\backslash\{0\}$.

En este contexto $\infty + \infty = \infty + n = n + \infty = \infty$ y $\infty > m$ para toda $n, m \in \mathbb{Z}$.

Ejemplo A.5.6. Sea p un número primo. Todo racional no nulo a/b se puede escribir de forma única $p^r(x/y)$ con x e y primos con p, donde $r \in \mathbb{Z}$. Sea $v_p : \mathbb{Q}\backslash\{0\} \longrightarrow \mathbb{Z}$ la aplicación que asocia a cada a/b el entero r. Entonces v_p es una valoración discreta de $\mathbb{Q}$.

A.6 El teorema de aproximación débil

Teorema A.6.1 (Teorema de aproximación débil)**.** *Sean F/K un campo de funciones, $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares de F/K distintos dos a dos, $x_1, \ldots, x_n \in F$ y $r_1, \ldots, r_n \in \mathbb{Z}$. Entonces existe una $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \text{ for } i = 1, \ldots, n.$$

Nota: El teorema de aproximación débil es una generalización del teorema chino de los restos.

A.7 Divisores

Como el campo $\mathcal{K}$ de constantes de una extensión algebraica F/K es una extensión finita de K, y F se puede ver como un campo de funciones sobre $\mathcal{K}$, entonces podemos suponer que F/K es un campo de funciones tal

que K es el campo de constantes.

Definición A.7.1. Denotaremos por $\mathcal{D}_F$, al grupo abeliano libre generado por los lugares de F/K. Le llamaremos el **grupo de divisores** de F/K.

Llamaremos a los elementos de $\mathcal{D}_F$ **divisores** de F/K. En otras palabras un divisor D es una suma formal de lugares

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ con } n_P \in \mathbb{Z}, \text{ y casi todas las } n_P = 0.$$

El **soporte** de un divisor $D \in \mathcal{D}_F$ se define como

$$supp(D) := \{P \in \mathbb{P}_F | n_P \neq 0\}.$$

A veces es conveniente escribir

$$D = \sum_{P \in S} n_P P,$$

El **grado de un divisor** se define como

$$grado(D) := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot grado(P)$$

Definición A.7.2. Sea $0 \neq x \in F$ y sean Z el conjunto de ceros y N el conjunto de polos de x en $\mathbb{P}_F$. Definimos

$$(x)_0 := \sum_{P \in Z} v_P(x) P, \text{ el divisor de ceros de } x,$$

$$(x)_\infty := -\sum_{P \in N} v_P(x) P, \text{ el divisor de polos de } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ el divisor principal de } x.$$

Claramente $(x)_0$ y $(x)_\infty$ son divisores positivos. Y

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P. \tag{A.1}$$

Definición A.7.3. Dado un divisor $A \in \mathcal{D}_F$ definimos

$$\mathcal{L}(A) := \{x \in F | (x) + A \geq 0\} \cup \{0\}.$$

Definición A.7.4. Dado $A \in \mathcal{D}_F$, al entero $dim(A) := dim(\mathcal{L}(A))$ le llamaremos **la dimensión de el**

divisor A.

Se sigue que $x \in \mathcal{L}(A)$ si y solo si $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$

Definición A.7.5. El **género** g of F/K está definido como

$$g := max\{grado(A) - dim(A) + 1 | A \in \mathcal{D}_F\}.$$

A.8 El teorema de Riemann-Roch

En esta sección F/K denota un campo de funciones algebraico de género g.

Definición A.8.1. Para $A \in \mathcal{D}_F$ definimos el **índice de especialidad** de A como el entero

$$i(A) := dim(A) - grado(A) + g - 1.$$

Definición A.8.2. Un **adele** de F/K es una aplicación

$$\alpha : \begin{cases} \mathbb{P}_F & \to & F, \\ P & \mapsto & \alpha_P, \end{cases}$$

tal que $\alpha_P \in \mathcal{O}_P$ excepto en un número finito de lugares$P \in \mathbb{P}_F$. Consideraremos a los adeles como elementos del producto directo $\prod_{P \in \mathbb{P}_F} F$. Usaremos la notación $\alpha = (\alpha_P)$.

La suma de adeles (coordenada a coordenada) es cerrada, y la multiplicación de un adele por un elemento de K es un adele. Así que al conjunto

$$\mathcal{A}_F := \{\alpha | \alpha \text{ es un adele de } F/K\}$$

le llamaremos el **espacio de adeles** de F/K.

El **adele principal** de un elemento $x \in F$ es el adele cuyas componentes son todas iguales a x. Esta última definición tiene sentido pues toda $x \in F$ tiene un número finito de ceros y polos.

Las valoraciones v_P de F/K se extienden de manera natural a $\mathcal{A}_F$ como

$$v_P(\alpha) := v_P(\alpha_P),$$

aquí α_P es la P-componente de el adele α. Entonces, por definición de α, $v_P(\alpha) \geq 0$ excepto en un número finito de lugares.

Definición A.8.3. Dado $A \in \mathcal{D}_F$ definimos

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F | v_P(\alpha) \geq -v_P(A) \text{ para todo } P \in \mathbb{P}_F\}$$

Definición A.8.4. Un **diferencial de Weil** de F/K es una aplicación K-lineal $\omega : \mathcal{A}_F \to K$ que se anula en $\mathcal{A}_F(A) + F$ para algún divisor $A \in \mathcal{D}_F$. Llamaremos al conjunto

$$\Omega_F := \{\omega | \omega \text{ es un diferencial de Weil de } F/K\}$$

el **módulo de diferenciales de Weil** de F/K. Sea $A \in \mathcal{D}_F$, definimos

$$\Omega_F(A) := \{\omega \in \Omega_F | \omega \text{ se anula en } \mathcal{A}_F(A) + F\}.$$

Lema A.8.5. *Para todo $A \in \mathcal{D}_F$ tenemos que $dim(\Omega_F(A)) = i(A)$.*

Definición A.8.6. (a) El divisor (ω) de un diferencial de Weil $\omega \neq 0$ es el divisor de F/K determinado de manera única que satisface

1. ω se anula en $\mathcal{A}_F((\omega)) + F$.
2. Si ω se anula en $\mathcal{A}_F(A) + F$ entonces $A \leq (\omega)$.

(b) Dado $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$ definimos $v_P(\omega) := v_p((\omega))$.

(c) Decimos que un lugar P es un cero (resp. polo) si $v_P((\omega)) > 0$ (resp. $v_P((\omega)) < 0$). ω se dice que es **regular** en P si $v_P((\omega)) \geq 0$, ω se dice **regular** si es regular en todo $P \in \mathbb{P}_F$.

(d) Se dice que un divisor W es **divisor canónico** de F/K si $W = (\omega)$ para algún $\omega \in \Omega_F$.

Teorema A.8.7 (Riemann-Roch)**.** *Sea W un divisor canónico de F/K. Entonces para todo $A \in \mathcal{D}_F$,*

$$dim(A) = grado(A) + 1 - g + dim(W - A).\blacksquare$$

Corolario A.8.8. *Para un divisor canónico W, tenemos que*

$$grado(W) = 2g - 2 \text{ y } dim(W) = g.$$

Teorema A.8.9 (Teorema fuerte de aproximación)**.** *Sea $S \subsetneq \mathbb{P}_F$ un subconjunto propio de $\mathbb{P}_F$ y $P_1, \ldots, P_r \in S$. Supongamos que son dados $x_1, \ldots, x_r \in F$ y $n_1, \ldots, n_r \in \mathbb{Z}$. Entonces existe un elemento $x \in F$ tal que*

$$v_{P_i}(x - x_i) = n_i (i = 1, \ldots, r)$$

y

$$v_P(x) \geq 0, \forall P \in S \setminus \{P_1, \ldots, P_r\}.$$

A.9 Curvas algebraicas

Sea K un campo, y sea C el plano proyectivo de la curva definida por $H = 0$, donde $H = H(X, Y, Z) \in K[X, Y, Z]$ es un polinomio homogéneo. Para cualquier campo F que contiene a K, definimos un F-punto racional en C a un punto $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(F)$ tal que $H(X_0, Y_0, Z_0) = 0$. El conjunto de todos los puntos racionales en C es denotado por $C(F)$. Los elementos de $C(K)$ son llamados **puntos de grado uno** o simplemente puntos racionales.
Como caso particular, tomemos $K = \mathbb{F}_q$ un campo finito, el campo finito $F = \mathbb{F}_{q^n}$ y $\mathbb{F}_q \subset \mathbb{F}_{q^n}$

Definición A.9.1. Sea C una curva no singular en el plano proyectivo. Un *punto de grado n* en C sobre $\mathbb{F}_q$ es un conjunto $P = \{P_0, \ldots, P_{n-1}\}$ de n puntos distintos en $C(\mathbb{F}_q)$ tal que $P_i = \sigma^i_{q,n}(P_0)$ para $i = 1, \ldots, n-1$, donde $\sigma^i_{q,n} : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ es el automorfismo de Frobenius con $\sigma_{q,n}(\alpha) = \alpha^q$

A.9.1 Ejemplo

Sea C_0 una curva del plano proyectivo sobre $\mathbb{F}_3$ correspondiendo a

$$h(x, y) = y^2 - x^3 - 2x - 2 \in \mathbb{F}_3[x, y].$$

Homogeneizando, $H(X,Y,Z) = ZY^2 - X^3 - 2XZ^2 - 2Z^3 = 0$

$$H_X = -4Z = 2Z = 0, H_Y = 2YZ = 0, H_Z = Y^2 - 4XZ = Y^2 + 2XZ = 0$$

$$\Longrightarrow X = Y = Z = 0$$

entonces C_0 es no singular.

Ahora vamos a encontrar los puntos de grado 1(puntos racionales) en $C_0(\mathbb{F}_3)$.

$y^2 - x^3 - 2x - 2 = 0$, donde $\mathbb{F}_3 = \{0, 1, 2\}$.

Si $x = 0$ entonces $y^2 = 2 \Longrightarrow$ no hay elementos en $\mathbb{F}_3$

Si $x = 1$ entonces $y^2 = 2 \Longrightarrow$ no hay elementos en $\mathbb{F}_3$

Si $x = 2$ entonces $y^2 = 2 \Longrightarrow$ no hay elementos en $\mathbb{F}_3$

Y cuando $Z = 0$, también $X = 0$, por lo que tenemos, $P_\infty = (0, 1)$ Entonces, los puntos de grado 1 son $C_0(\mathbb{F}_3) = \{P_\infty\}$

Para encontrar los puntos de grado 2, tenemos que calcularlo en $C_0(\mathbb{F}_{3^2})$.

Entonces, $\mathbb{F}_9 = \mathbb{F}_3[t]/(t^2 + 1)$. Sea $\alpha \in \mathbb{F}_9$ correspondiente a t. Entonces, $\mathbb{F}_9 = \{a + b\alpha \,|\, a, b \in \mathbb{F}_3\}$, donde $\alpha^2 = -1 = 2$.

Cuando $Z = 1$, tenemos $Y^2 - X^3 - 2X - 2 = 0$

Si $X = 0$, entonces $y^2 = 2 \Longrightarrow y = \alpha$ o $y = 2\alpha$.

Por lo que, $(0 : \alpha : 1), (0 : 2\alpha : 1) \in C_0(F_9)$.

Si $X = 1$, entonces $y^2 = 2 \Longrightarrow y = \alpha$ o y=2 α.

Por lo que, $(1 : \alpha : 1), (1 : 2\alpha : 1) \in C_0(F_9)$

Si $X = 2$, entonces $y^2 = 2 \Longrightarrow y = \alpha$ o $y = 2\alpha$.

Por lo que, $(2 : \alpha : 1), (2 : 2\alpha : 1) \in C_0(F_9)$

La aplicación de Frobenius $\sigma_{3,2} : \mathbb{F}_9 \longrightarrow \mathbb{F}_9; \alpha \mapsto \alpha^3 = 2\alpha$.

$\sigma_{3,2}(0 : \alpha : 1) = (0 : 2\alpha : 1)$. Por lo que tenemos un punto $Q_1 = \{(0 : \alpha : 1), (0 : 2\alpha : 1)\}$ de grado 2.

Similarmente, $Q_2 = \{(1 : \alpha : 1), (1 : 2\alpha : 1)\}$ y $Q_3 = \{(2 : \alpha : 1), (2 : 2\alpha : 1)\}$. Por lo tanto, tenemos tres puntos de grado 2 wn C_0. $C_0(\mathbb{F}_9) = \{(0 : \alpha : 1), (0 : 2\alpha : 1), (1 : \alpha : 1), (1 : 2\alpha : 1), (2 : \alpha : 1), (2 : 2\alpha : 1), P_\infty\}$

Similarmente, $\mathbb{F}_{3^3} = \mathbb{F}_3[t]/(t^3 + 2t + 2)$ y sea $w \in \mathbb{F}_{27}$ correspondiente a t.

Entonces, tenemos $C_0(\mathbb{F}_{27}) = \{(w : 0 : 1), (1 + w : 0 : 1), \ldots, (1 + 2w + 2w^2 : 1 + 2w + 2w^2 : 1), P_\infty\}$ con 28 $\mathbb{F}_{27}$-puntos racionales.

Se puede ver que $C_0(\mathbb{F}_{27}) = R_1 \cup \cdots \cup R_9 \cup \{P_\infty\}$, donde $R_1, \ldots, R_9$ son los nueve puntos de grado 3 en C_0.

Por ejemplo, $R_1 = \{(w:0:1),(1+w:0:1),(2+w:0:1)\}$

Si establecemos $D = 5P_\infty - 2Q_3 + 7R_1$, entonces D es un divisor en C_0 sobre $\mathbb{F}_3$ de grado $5(1)-2(2)+7(3) = 22$ con soporte $\{P_\infty, Q_3, R_1\}$

Definición A.9.2. Sea $H(X,Y,Z)$ el polinomio el cual define el plano proyectivo no singular sobre la curva C en el campo $\mathbb{F}_q$. El campo de funciones racionales en C es
$\mathbb{F}_q(C) := (\{\frac{g(X,Y,Z)}{h(X,Y,Z)} \mid g,h \in \mathbb{F}_q(X,Y,Z)$ hgéneo del mismo grado $\} \cup \{0\})/\backsim$,
donde $g/h \backsim g'/h'$ si y solo si $gh' - g'h \in \langle H \rangle \subset \mathbb{F}_q(X,Y,Z)$

Ejemplo, $H(X,Y,Z) = Y^2Z - X^3 - 2XZ^2 - 2Z^32 \in \mathbb{F}_3[X,Y,Z]$. Entonces, $X^2/Z^2 = (Y^2 + XZ + Z^2)/XZ \in \mathbb{F}_3(C_0)$

Definición A.9.3. Sea G un divisor de la curva no singular sobre el plano proyectivo de la curva C definida sobre el campo $\mathbb{F}_q$. Entonces, el espacio de funciones racionales asociadas a G es

$$L(G) := \{f \in \mathbb{F}_q(C) | (f) + G \geq 0\} \cup \{0\}.$$

Teorema A.9.4 (Teorema de Riemann-Roch)**.** *Sea C la curva no singular del plano proyectivo de genero g definida sobre el campo $\mathbb{F}_q$ y sea G un divisor en $\mathbb{F}_q$. Entonces, $dimL(G) \geq grado(G) + 1 - g$. Además, si $grado(G) > 2g - 2$, entonces $dimL(G) = grado(G) + 1 - g$.*

Podemos ver en nuestro ejemplo que el divisor de la función racional X/Z en C_0 es $Q_1 - 2P_\infty$. También, es fácil ver que el divisor de la función racional Y/Z es $R_1 - 3P_\infty$. Por lo que, para cualquiera $i,j \geq 0$, tenemos que $div(X^iY^j/Z^{i+j}) = iQ_1 + jR_1 - (2i+3j)P_\infty$

Ahora si tomamos un entero positivo m y tomamos a $G = mP_\infty$. Usando el teorema de Riemann-Roch, sabemos que$dimL(G) = grado(G) + 1 - g = m + 1 - 1 = m$. Cuando $m = 1$, tenemos $L(G) = \mathbb{F}_3$, entonces $\{1\}$ es una base para $L(G)$. Cuando $m = 2$, tenemos $X/Z \in L(G)$ por lo antes visto, y tenemos que $\{1, X/Z\}$ son independientes y por tanto una base para $L(G)$. Cuando $m = 3$, vemos que $div(Y/Z) + G = R_1 - 3P_\infty + 3P_\infty = R_1 \geq 0$ y así $\{1, X/Z, Y/Z\}$ es una base para $L(G)$

Bibliografía

[1] Philippe Guillot. "Cryptographical Boolean Functions Construction From Linear Codes". *Proceedings of BFCA'05 Conference*. 2005, pp. 1–14.

[2] Claude E. Shannon. "Communication Theory of Secrecy Systems.pdf". *Bell Labs Technical Journal* 28.4, 1949, pp. 657–715. ISSN: 0724-6811.

[3] Francisco Rodr\'\iguez. "De la Búsqueda de Funciones Booleanas con Buenas Propiedades Criptográficas". *México. Disponible en l{\ \'i}nea: http://delta. cs. cinvestav. mx/˜ francisco/cajass. pdf (Acceso: 28/05/2010)*, 2007.

[4] Thomas W Cusick and Pantelimon Stanica. *Cryptographic Boolean functions and applications*. Academic Press, 2017.

[5] Henning Stichtenoth. *Algebraic function fields and codes*. Vol. 254. Springer Science & Business Media, 2009.

[6] Henning Stichtenoth. "A Note on Hermitian Codes Over GF(q2)". *IEEE Transactions on Information Theory* 34.5, 1988, pp. 1345–1348. ISSN: 15579654. DOI: 10.1109/18.21267.

[7] G D Forney. *Jr.. concatenated codes*. 1966.

[8] Seongtaek Chee, Sangjin Lee, Daiki Lee, et al. "On the correlation immune functions and their nonlinearity". *AsiaCrypt*. Springer Verlag. 1996, pp. 232–243. ISBN: 978-3-540-61872-0 978-3-540-70707-3 SV - 1163. DOI: 10.1007/BFb0034850. URL: http://link.springer.com/10.1007/BFb0034850.

[9] Kishan Chand Gupta, Yassir Nawaz, and Guang Gong. "Upper bound for algebraic immunity on a subclass of Maiorana McFarland class of bent functions". *Information Processing Letters* 111.5, 2011, pp. 247–249. ISSN: 00200190. DOI: 10.1016/j.ipl.2010.10.013.

[10] Paul Camion, Claude Carlet, Pascale Charpin, et al. "On Correlation-Immune Functions." *Crypto*. Vol. 91. Springer. 1991, pp. 86–100.

[11] C. Munuera, A. Sepúlveda, and F. Torres. "Generalized hermitian codes". *Designs, Codes, and Cryptography* 69.1, 2013, pp. 123–130. ISSN: 09251022. DOI: 10.1007/s10623-012-9627-0.

[12] Deng Tang, Claude Carlet, and Xiaohu Tang. "Highly nonlinear boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks". *IEEE Transactions on Information Theory* 59.1, 2013, pp. 653–664. ISSN: 00189448. DOI: 10.1109/TIT.2012.2217476.

[13] John Little, Keith Saints, and Chris Heegard. "On the structure of Hermitian codes". *Journal of Pure and Applied Algebra* 121.3, 1997, pp. 293–314. ISSN: 00224049. DOI: 10.1016/S0022-4049(96)00067-9.

[14] Claude Carlet. "Vectorial Boolean functions for cryptography". *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* 134, 2010, p. 398. ISSN: 19323166. DOI: http://dx.doi.org/10.1017/CBO9780511780448.

[15] E Pasalic. "Degree optimized resilient Boolean functions from Maiorana-McFarland class". *Cryptography and Coding, Proceedings* 2898, 2003, pp. 93–114. ISSN: 0302-9743.

[16] Wei Guo Zhang and Enes Pasalic. "Generalized Maiorana-McFarland construction of resilient boolean functions with high nonlinearity and good algebraic properties". *IEEE Transactions on Information Theory* 60.10, 2014, pp. 6681–6695. ISSN: 00189448. DOI: 10.1109/TIT.2014.2345772.

[17] Claude Carlet. "A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction". *\ifnum\shortbib=1{CRYPTO}\else{Advances in Cryptology – {CRYPTO}}\fi˜2002*. Vol. 2442. Springer. 2002, pp. 549–564. ISBN: 3-540-44050-X. DOI: 10.1007/3-540-45708-9_35. URL: http://link.springer.com/10.1007/3-540-45708-9{_}35.

[18] Hans Georg Rück and Henning Stichtenoth. "A characterization of Hermitian function fields over finite fields". *Journal fur die Reine und Angewandte Mathematik* 1994.457, 1994, pp. 185–188. ISSN: 14355345. DOI: 10.1515/crll.1994.457.185.

[19] V. D. Goppa. "Codes on Algebraic Curves". *Soviet Mathematics Doklady*. Vol. 24. 1. 1981, pp. 170–172. ISBN: 1461547857.

[20] Kyeongcheol Yang and P.V. Kumar. "On the true minimum distance of Hermitian codes". *Coding theory and algebraic geometry* 1518, 1991, pp. 99–107. URL: http://www.springerlink.com/index/6628247r5636h244.pdf.

[21] Claude Carlet, Deepak Kumar Dalai, Kishan Chand Gupta, et al. "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction". *IEEE Transactions on Information Theory* 52.7, 2006, pp. 3105–3121. ISSN: 00189448. DOI: 10.1109/TIT.2006.876253.

[22] S. V. Bulygin. "Generalized hermitian codes over GF (2r)". *IEEE Transactions on Information Theory* 52.10, 2006, pp. 4664–4669. ISSN: 00189448. DOI: 10.1109/TIT.2006.881831.

[23] Lilya Budaghyan, Claude Carlet, Tor Helleseth, et al. "Generalized bent functions and their relation to Maiorana-McFarland class". *IEEE International Symposium on Information Theory - Proceedings*. IEEE. 2012, pp. 1212–1215. ISBN: 9781467325790. DOI: 10.1109/ISIT.2012.6283049.

[24] Oliver Pretzel. *Codes and algebraic curves*. Vol. 8. Clarendon Press, 1998, pp. xii+192. ISBN: 0-19-850039-4.

[25] Wei Guo Zhang and Guo Zhen Xiao. "Construction of almost optimal resilient Boolean functions via concatenating Maiorana-McFarland functions". *Science China Information Sciences* 54.4, 2011, pp. 909–912. ISSN: 1674733X. DOI: 10.1007/s11432-011-4230-y.

[26] Palash Sarkar and Subhamoy Maitra. "Nonlinearity bounds and constructions of resilient Boolean functions". *Advances in Cryptology—CRYPTO 2000*. Springer. 2000, pp. 515–532.

[27] Carlos Moreno. *Algebraic curves over finite fields*. 97. Cambridge University Press, 1993.

[28] Claude Carlet. "Boolean functions for cryptography and error correcting codes". *Boolean models and methods in mathematics, computer science, and engineering* 2, 2010, pp. 257–397.

[29] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Vol. 20. Cambridge university press, 1997.