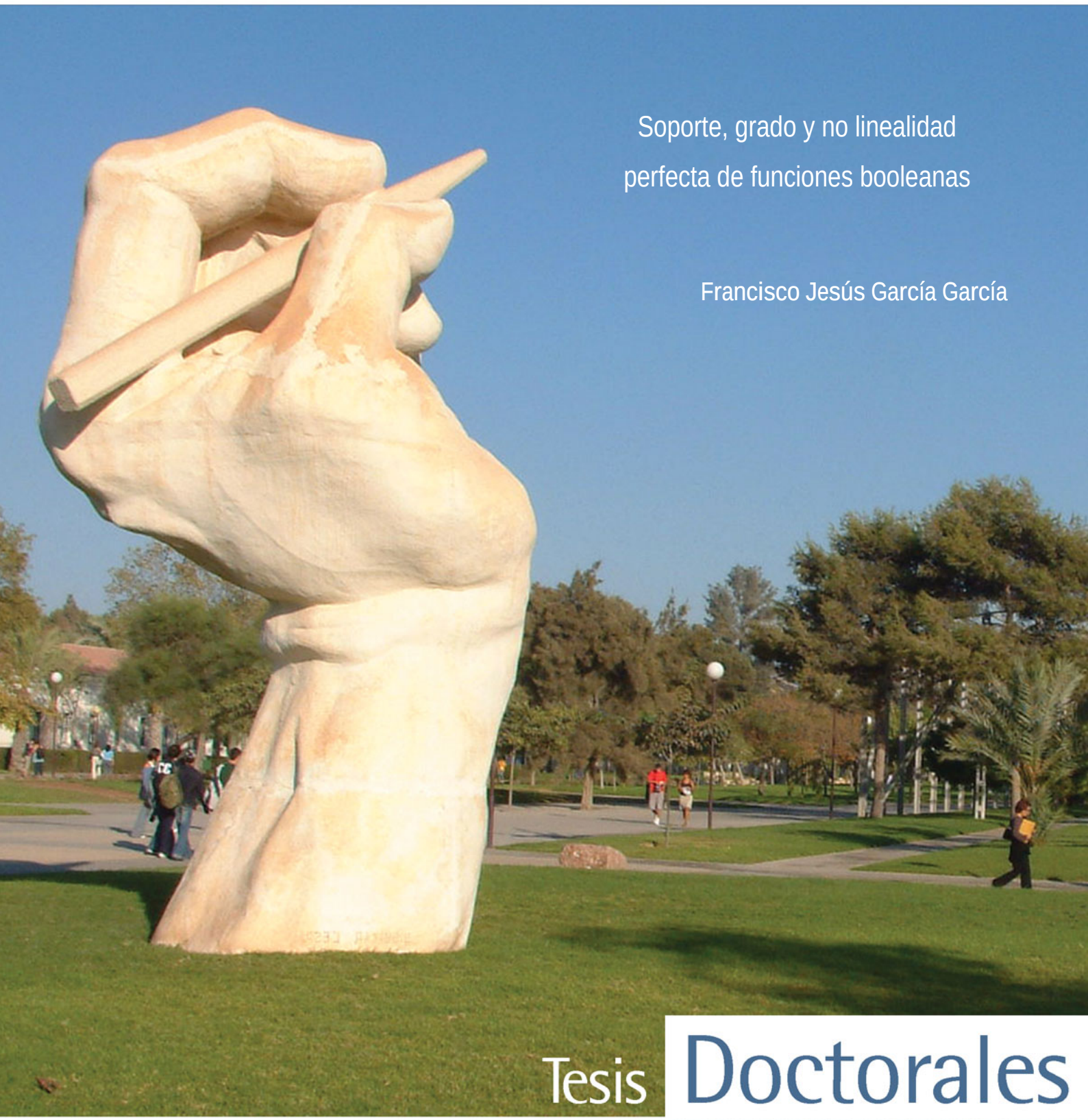
Universitat d'Alacant
Universidad de Alicante

Soporte, grado y no linealidad perfecta de funciones booleanas

Francisco Jesús García García



Tesis Doctorales

www.eltallerdigital.com

UNIVERSIDAD de ALICANTE

Universidad de Alicante

Departamento de Ciencia de la Computación e Inteligencia Artificial

Soporte, grado y no linealidad perfecta de funciones booleanas

TESIS DOCTORAL

Presentada por:
Francisco Jesús García García

Dirigida por:
Joan Josep Climent Coloma

Universidad de Alicante

Departamento de Ciencia de la Computación e Inteligencia Artificial

Soporte, grado y no linealidad perfecta de funciones booleanas

Memoria presentada para optar al grado de doctor por Francisco Jesús García García.

Alicante, mayo de 2014.

A Mati,
que comparte conmigo
una clave secreta
que ningún criptoanálisis
podrá romper jamás

Quiero expresar mi más sincero agradecimiento

- al Dr. Leandro Tortosa, que me puso en contacto con el grupo de criptografía de la Universidad de Alicante.
- a la Dra. Verónica Requena que, llena de ilusión, se incorporó al grupo, aportando una fuente de energía inagotable y el atrevimiento de la juventud temprana, que tan fructífero ha sido para explorar el intrincado campo de las funciones booleanas de no linealidad perfecta. El presente trabajo no es más que un corolario de su tesis doctoral.
- al Dr. Joan Josep Climent, que enseguida me adoptó como discípulo y como amigo, sufriendo como un padre mis pasos descarriados y mi natural tendencia al desánimo. Inasequible al desaliento, prolífico en ideas, perseverante hasta la extenuación, resulta imposible exagerar sus virtudes como director científico.
- a las interminables horas de debate y discusión que me regalaron Vero y Joan Josep, tan duras y, al mismo tiempo, tan excitantes e intelectualmente placenteras y que permanecerán indelebles en mi memoria mientras ésta resista. Los tres formamos durante un tiempo un entrañable equipo de trabajo que, sin ser exactamente ni trino ni tripartito, ni una terna ni un trío, ni una trinca ni un metafórico trinomio, ni siquiera un terceto encadenado; un poco de todo, sin embargo, lo fue sin querer. Ni una sola de las ideas en las que se basa la memoria aquí presentada es ajena a esa particular dialéctica a tres bandas que tuvimos la suerte de orquestar y de la que yo fui el privilegiado que recibió mucho más de lo que aportó. No obstante, y la afirmación no es ningún tópico, solo yo soy responsable de los errores, las erratas y las imprecisiones que puedan haberse infiltrado en el texto.

Índice

Prólogo

El presente trabajo se enmarca en los esfuerzos desarrolados durante las últimas décadas para comprender la estructura de la clase de las *funciones booleanas de no linealidad perfecta*. El evidente interés práctico del tema por sus aplicaciones a la criptografía, disciplina que desde los tiempos de Bletchley Park está irreversiblemente unida a la vertiginosa expansión de las ciencias de la computación, no debe ocultar sin embargo sus dimensiones teóricas. Al fin y al cabo, el origen de las funciones booleanas de no linealidad perfecta se remonta a un trabajo teórico de McFarland ([70] sobre diferencias finitas en grupos finitos no cíclicos.

Grado elevado, no linealidad perfecta y equibrio (conceptos que serán definidos con precisión más adelante) son algunas de las propiedades deseables para las funciones booleanas que intervienen en el diseño de los criptosistemas destinados a incrementar la seguridad en las comunicaciones mediante el uso de cifradores en bloque, cifradores en flujo y funciones *hash*. O, si se nos permite la ironía, para dinamitarla, habida cuenta de la ancestral ambivalencia de los resultados en criptografía, utilizables tanto para mejorar las codificaciones como para romper los códigos.

Dedicamos el capítulo 2 de la presente memoria a analizar el concepto de grado de una función booleana y a explorar sus propiedades con vistas al diseño de algoritmos que aceleren la determinación del grado a partir de la secuencia binaria que define la función. Es sabido que, en igualdad de condiciones para las otras buenas propiedades criptográficas, la eficacia de los sistemas criptográficos mejora al elevar el grado de las funciones booleanas que intervienen en su diseño.

La no linealidad es la propiedad más importante en cualquier criptosistema de clave simétrica para alcanzar confusión y dificultar el criptoanálisis diferencial. Como veremos en el capítulo 1, la no linealidad se puede definir como la mínima distancia —para una precisa definición de distancia— de una función booleana al conjunto

de las funciones afines, que son, en varios sentidos, las funciones más simples. Si el número n de variables es par, existen funciones booleanas que gozan de una no linealidad máxima o perfecta. Estas funciones tienen un grado máximo de $n/2$. Dedicamos tanto el capítulo 3 como el capítulo 4 a detallar diferentes procedimientos para construir funciones de no linealidad perfecta.

Una función booleana se llama *equilibrada* si contiene el mismo número de 1 que de 0 en su *tabla de verdad*. Las funciones equilibradas gozan de buenas propiedades criptográficas en tanto que son el punto de partida para la construcción de las funciones llamadas *resilientes*, que tienen inmunidad frente a la correlación.

Las funciones de no linealidad perfecta no son equilibradas y tienen un grado máximo limitado ($n/2$, como se ha dicho anteriormente), de modo que alto grado, no linealidad y equilibrio, son propiedades que, desgraciadamente, no se pueden alcanzar simultáneamente. En consecuencia, la construcción de funciones criptográficamente buenas no es una tarea fácil. La literatura especializada ha producido una amplia gama de técnicas algebraicas y heurísticas para construir funciones bien dotadas criptográficamente pero estos métodos suelen ser muy complejos, computacionalmente difíciles de implementar (especialmente de modo directo en el *hadware* para comunicaciones seguras) y no siempre producen el número elevado de funciones que requiere la demanda práctica.

La presente memoria de investigación pretende contribuir al desarrollo de estas técnicas.

Parte de los resultados aquí expuestos han sido publicados en distintas revistas o actas de congresos [22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 36, 37, 38, 40, 41, 42] y otros están en proceso de evaluación para su publicación [34, 35, 39].

Algunos de los resultados y técnicas han sido presentados y discutidos en jornadas, conferencias o congresos como los siguientes:

- 1st International Conference on Data Management and Security: Applications in Medicine, Sciences and Engineering, Elche, España, 2013.
- Congreso de la Real Sociedad Matemática Española, Santiago de Compostela, España, 2013.
- XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2012), Donsotia-San Sebastián, España, 2012.
- Algebra Lineal, Análisis Matricial y Aplicaciones (ALAMA 2012), Leganés,

España, 2012

- 11th International Conference Computational and Mathematical Methods in Science and Engineering, Benidorm, 2011
- 2010 International Symposium on Information Theory and its Applications (ISITA 2010), Taichung, Taiwan, 2010.
- XI Reunión Española sobre Criptología y Seguridad de la Información, Tarragona, España, 2010.
- 10th International Coference on Computational and Mathematical Methods in Science and Engineering (CMMSE2010), Almería, España, 2010.
- V Congreso Iberoamericano de Seguridad Informática, Motevideo, Uruguay, 2009.
- Congreso de la Real Sociedad Matemática Española, Oviedo, España, 2009.
- Second Workshop on Mathematical Cryptology, Santander, España, 2008.
- X Reunión Española sobre Criptología y Seguridad de la Información (RECSI), Salamanca, España, 2008.
- IV Congreso Iberoamericano de Seguridad Informática, Mar de Plata, Argentina, 2007.
- 2007 International Conference on Boolean Functions: Cryptography and Applications, París, Francia, 2007.

Los estudios que han dado lugar a la presente memoria han sido realizados parcialmente al amparo de los siguientes proyectos:

- Grupo de Álgebra y Geometría (VIGROB-287), 2014.
- Criptología y seguridad computacional (VIGROB-025), 2007, 2008, 2009, 2010, 2011, 2012, 2013.
- Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas (ACOMP/2011/005), 2011.
- Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas (ACOMP/2010/039), 2010.
- Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas (MTM2008-06674-C02-01), 2009, 2010, 2011.
- Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas (ACOMP/2009/142), 2009.

Capítulo 1

Preliminares

1.1 Introducción

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. Por citar un ejemplo, el código genético natural está compuesto de manera única por solo dos pares de bases codificables como secuencias binarias. Particularmente, en *criptografía* se hace un uso intensivo de las mismas en la construcción y análisis de criptosistemas. Las funciones booleanas juegan un papel importante en los cifradores en bloque, los cifradores en flujo,las funciones *hash* [8, 11, 20, 61, 73] y la teoría de códigos,[7, 45, 60, 62, 69], entre otras.

En los modelos más comunes de cifradores en flujo, la clave se produce utilizando una función booleana. La selección de las funciones booleanas atendiendo a una amplia variedad de criterios permite aumentar notablemente la seguridad de las claves producidas. La implementación de una caja de sustitución o *S-box* necesita funciones booleanas no lineales que posean ciertas propiedades criptográficas favorables para garantizar la resistencia a ataques tales como el criptoanálisis lineal y el diferencial [1, 52, 78].

Las siguientes cuatro propiedades han demostrado ser importantes en la construcción de funciones booleanas para las aplicaciones criptográficas:

(a) *Grado algebraico* o grado del polinomio multivariante que representa a la función booleana (véase la definición 1.5).
(b) *No linealidad* o distanciamiento de las funciones afines (véase la definición 1.7).
(c) *Equilibrio* o presencia de la misma cantidad de unos y ceros en su tabla de

verdad (véase la definición 1.3).

(d) *Resilencia* o inmunidad a la correlación, esto es independencia probabilística entre los valores de la función y el conocimiento previo de los valores binarios de algunas de sus variables.

La utilidad de una función booleana en las aplicaciones criptográficas depende de una buena combinación de las anteriores propiedades. Desgraciadamente, una función booleana no puede satisfacer a la vez todas las propiedades plenamente. Las funciones con máxima no linealidad, o *funciones de no linealidad perfecta* tienen un grado algebraico reducido (de hecho como mucho $n/2$, si n es el número de variables de la función) y no son equilibradas. Existe también un límite para el grado algebraico de las funciones resilientes ($n - m - 1$, siendo m el orden de resilencia, que cuanto más elevado es denota mayor inmunidad a la correlación), que son equilibradas pero tienen una no linealidad lejana a la máxima.

Las funciones booleanas pueden ser representadas de diversas maneras. Las representaciones que se emplean más comúnmente en la literatura son la forma polinomial o forma normal algebraica, la secuencia de los valores de la tabla de verdad, o forma secuencial y la forma matricial. En su tesis doctoral [89], precursora e inspiradora de la presente, Verónica Requena utilizó, sin embargo, el concepto clásico de *minterm*, que no ha sido utilizado con frecuencia, a pesar de estar directamente relacionado con la implementación de circuitos lógicos y su complejidad.

Cada una de las formas mencionadas de representar las funciones booleanas presenta ventajas e inconvenientes prácticos y teóricos y ninguna de las representaciones puede sustituir totalmente a las otras. Por ejemplo, la forma normal algebraica proporciona directamente el grado algebraico de la función, pero no su peso. Por otra parte, si conocemos la tabla de verdad, podemos calcular fácilmente el peso de la función, pero no su grado. Peso y grado de una función booleana son propiedades vinculadas a la complejidad lineal, una de las más valiosas propiedades criptográficas de las mismas. Buena parte del presente trabajo está dedicada a establecer propiedades del grado de las funciones booleanas a partir de su forma secuencial. Propiedades diversas del grado de las funciones booleanas desde otras representaciones pueden encontrarse en los artículos de Barrington [4], Nisan [76], Ozols [82], Meier [71], Zhang [98], Strazdins [95], Habib [53] o Gonda [51]

Las funciones *de no linealidad perfecta* son un tipo especial de funciones booleanas,

las que poseen máxima no linealidad. A causa de sus buenas propiedades criptográficas, tales como gozar de la más baja autocorrelación [72, 87], las funciones *de no linealidad perfecta* pueden ser empleadas en cifradores simétricos para resistir los criptoanálisis citados anteriormente. Además, también son utilizadas en comunicación, teoría de códigos y teoría combinatoria, entre otros muchos campos.

Las funciones *de no linealidad perfecta* se utilizan en los *códigos de Reed-Muller* [64]. El *código de Reed-Muller* de primer orden consiste en todas las funciones afines de $\mathbb{F}_2^n$ y, si n es par, las funciones *de no linealidad perfecta* de n variables pueden ser caracterizadas como las funciones que poseen la máxima distancia posible a todas las palabras del *código de Reed-Muller* de primer orden. También los *códigos Kerdock* son construidos utilizando funciones *de no linealidad perfecta*, en este caso de un tipo especial, cuadráticas o de grado 2.

Este tipo de funciones booleanas, que junto con el grado de las funciones booleanas en general son el objeto de nuestro trabajo, han sido estudiadas desde principios de los años 70 del siglo pasado. A continuación daremos un breve repaso a los principales resultados obtenidos sobre ellas.

El origen de las funciones *de no linealidad perfecta* se remonta al año 1973 en un artículo teórico de McFarland [70] sobre conjuntos de diferencias finitas en grupos finitos no cíclicos. Un año más tarde, Dillon [46] en su tesis doctoral sistematizó y extendió las ideas de McFarland, proporcionando una gran cantidad de propiedades de las funciones booleanas de *de no linealidad perfecta*. El nombre *bent* con el que también se conoce a estas funciones se debe a Rothaus [91]. En la actualidad, no existe traducción ni adaptación al castellano de esta palabra que sea aceptada por la comunidad científica. las funciones *de no linealidad perfecta* han sido objeto de un intenso estudio, como se desprende de la abundante literatura acumulada sobre ellas (véase por ejemplo [2, 3, 5, 9, 13, 17, 49, 50, 59, 65, 77, 81] y las referencias en ellas incluidas).

Entre sus propiedades más relevantes cabe citar que solo existen para un número de variables n par, que toda función *de no linealidad perfecta* de n variables, con $n > 2$, tiene grado máximo $n/2$ (véase [91]), que hay funciones *de no linealidad perfecta* con grado igual a $n/2$ y que las únicas funciones *de no linealidad perfecta* simétricas son las cuadráticas, existiendo exactamente cuatro de estas funciones para cada n. No existen funciones *de no linealidad perfecta* para un número impar

de variables, pero sí las hay con una no linealidad muy elevada (no la máxima posible). Estas últimas son denominadas funciones *de no linealidad casi perfecta* [79] o *semibent* [21, 58]. Dobbertin [48] ha resumido, aportando nuevos casos, el estado de la clasificación de las funciones casi perfectamente no lineales sobre $\mathbb{F}_{2^n}$ cuando n es impar.

A partir de las tablas de verdad de las funciones *de no linealidad perfecta* y las funciones lineales, es posible construir funciones *de no linealidad perfecta* con un número mayor de variables concatenando adecuadamente dichas tablas de verdad. Pero no todas las funciones *de no linealidad perfecta* de 6 variables se pueden obtener a partir de funciones *de no linealidad perfecta* y funciones lineales con un número menor de variables, como demostró Chang [18]. Esto no significa que no sea interesante construir funciones *de no linealidad perfecta* a partir de funciones *de no linealidad perfecta* y lineales con un número menor de variables, sino que por esa vía no es posible generarlas *todas*.

De hecho, gracias a Canteaut y Charpin [9] conocemos dos familias infinitas de funciones *de no linealidad perfecta* de n variables que no se pueden obtener a partir de funciones *de no linealidad perfecta* con un número menor de variables. En dicho artículo, los autores también describen un método para construir, partiendo de una función *de no linealidad perfecta* de n variables, funciones booleanas de $n-1$ y $n-2$ variables con bastante alta no linealidad.

Siguiendo una estrategia diferente, Hou y Langevin [57] describieron cómo a partir de una función *de no linealidad perfecta* conocida podemos obtener, de modo efectivo, funciones *de no linealidad perfecta* nuevas con el mismo número de variables que la de partida.

Yarlagadda y Hershey [97] realizan una aproximación distinta al análisis y la construcción de funciones *de no linealidad perfecta*, utilizando la secuencia de 0 y 1 formada por su tabla de verdad. Esta es una de las cuatro vías de estudio de las funciones booleanas más utilizadas en la literatura. Otras dos recurren respectivamente a la representación polinómica y a la matricial de una función booleana.

La cuarta manera de analizar funciones *de no linealidad perfecta* consiste en explorar las propiedades de determinadas estructuras algebraicas sobre $\mathbb{F}_{2^n}$. Esta es la opción metodológica que hemos adoptado en nuestro trabajo. Tal es el caso, también, de Carlet y Guillot [16] o de Hou [54, 56]. Los resultados obtenidos de este

modo son teóricamente interesantes puesto que permiten generar caracterizaciones y teoremas de existencia, y en muchas ocasiones también se obtienen métodos efectivos de construcción de las funciones que postulan. Con esta metodología se han podido determinar todas las funciones *de no linealidad perfecta* cúbicas de 8 variables a partir de las funciones *de no linealidad perfecta* cúbicas de 6 variables (véase [55]).

Una función booleana se llama *homogénea* cuando todos los términos de su expresión polinómica son del mismo grado. Las funciones homogéneas son más fáciles de implementar y, lógicamente, son mucho menos numerosas que las no homogéneas, con lo que es más asequible determinar sus propiedades. Eso es lo que han hecho Qu, Seberry y Pieprzyk [88], caracterizando las funciones homogéneas de 6 variables y grado 3 que son *de no linealidad perfecta* y las que son *equilibradas*. En el mismo artículo, los autores también discuten por qué las funciones homogéneas podrían ser muy útiles para el diseño de funciones *hash*. Posteriormente, Charnes, Rötteler y Beth [19, 20] encontraron algunas funciones *de no linealidad perfecta* homogéneas de grado 3 con 8 o 10 variables.

Maity y Maitra [68] estudiaron la mínima distancia entre el conjunto de las funciones *de no linealidad perfecta* y el conjunto de las funciones booleanas 1-resilientes. Estas funciones son equilibradas y tienen la máxima inmunidad a la autocorrelación (su transformada de Walsh es 0 para vectores de peso 1) mientras que las funciones *bent* tienen la máxima no linealidad. Como consecuencia de dicho estudio establecieron un procedimiento para generar funciones 1-resilientes con altas cotas de no linealidad a partir de funciones *de no linealidad perfecta* de 8 variables.

En la misma línea, Borissov [6] ha estudiado la relación entre las funciones m-resilientes y los códigos de Red-Muller. Las funciones resilientes con alta no linealidad son más resistentes a los criptoanálisis cuanto mayor es su grado algebraico. Pasalic [83] ha generalizado un método, modificando la clase de funciones *de no linealidad perfecta* de Maiorana-McFarland, para construir *S-boxes* en las que cada una de las componentes, en definitiva una función booleana, sea m-resiliente y con elevado grado algebraico.

Una función *de no linealidad perfecta* de n variables se llama *normal* si es constante cuando se restringen sus n entradas a cierto subespacio vectorial de dimensión $n/2$ [47]. Hasta muy recientemente, todas las construcciones *concretas* conocidas proporcionaban funciones *de no linealidad perfecta normales*. Ahora se sabe ya que

todas las funciones *de no linealidad perfecta* de 2, 4 y 6 variables son *normales*. Para mayor número de variables, Carlet, Dobbertin y Leander [15] han demostrado que la suma de una función *de no linealidad perfecta normal* y una función *de no linealidad perfecta no normal*, de las que ahora se sabe su existencia, es siempre *no normal*.

Millan, Clark y Dawson [74, 75] han explorado la posibilidad de diseñar métodos para probar sistemáticamente la no linealidad de *S-boxes* biyectivas, mostrando también cómo pueden obtenerse *S-boxes* altamente no lineales con resultados mejores que los obtenidos por generación aleatoria. Como consecuencia de dicho estudio, han diseñado un algoritmo genético capaz de generar funciones booleanas equilibradas con alta no linealidad y satisfaciendo el criterio de inmunidad por correlación y el criterio de estricta avalancha, cuya definición y generalización es discutida con amplitud en [87]. La base del método consiste en modificar una función equilibrada previamente conocida en dos posiciones de su tabla de verdad para obtener una nueva función también equilibrada con no linealidad más alta.

La construcción de familias de funciones *de no linealidad perfecta* particulares es importante, por un lado, para satisfacer la necesidad práctica de disponer de funciones de máxima no linealidad para implementar cifradores y, por otro lado, para explorar teóricamente propiedades de las mismas que permitan contrastar conjeturas y desvelar más características de las todavía no bien conocidas *funciones de no linealidad perfecta*.

La ya mencionada tesis de Verónica Requena [89] se centra, principalmente, en la generación de funciones *de no linealidad perfecta* utilizando la representación de funciones booleanas como suma de *minterms*. Así, usando dicho concepto, Climent, García y Requena [22, 23, 24, 26, 27, 29, 34, 35, 42] han obtenido funciones *de no linealidad perfecta* de cualquier número de variables partiendo de funciones *de no linealidad perfecta* de menor número de variables .

Un método general para generar todas las funciones *de no linealidad perfecta* aún no es conocido, excepto para algunos casos particulares. Cabe destacar que para $n = 2$ hay 8 funciones *de no linealidad perfecta*, para $n = 4$ hay 896 funciones *de no linealidad perfecta* (que se pueden obtener fácilmente mediante una búsqueda exhaustiva por ordenador), para $n = 6$ Preneel [86] (véase también [18]) probó que el número de funciones *de no linealidad perfecta* es de $5\,425\,430\,528$ y para $n = 8$, Langevin y Leander [63] probaron recientemente que el número de funciones *de no*

linealidad perfecta es 99 270 589 265 934 370 305 785 861 242 880. Sin embargo, para $n > 8$, la clasificación, así como el número de funciones *de no linealidad perfecta*, continúa siendo un problema abierto.

En esta memoria nos centraremos, principalmente, en el estudio de la estructura algebraica de las funciones booleanas en general y, en particular, de las funciones *de no linealidad perfecta*. aprovechando que la representación en forma de secuencia de bits (o tabla de verdad) es equivalente a un determinado subconjunto de vectores del espacio vectorial $\mathbb{F}_2^n$. El objetivo principal de este trabajo es doble. Por una parte la construcción de funciones *de no linealidad perfecta* partiendo de bases de $\mathbb{F}_2^n$, donde $\mathbb{F}_2$ es el cuerpo de Galois de dos elementos, 0 y 1, y, por otra parte, investigar las propiedades del grado de las funciones booleanas en general, sean o no funciones *de no linealidad perfecta*, con el propósito de generar algoritmos que determinen el grado de una función booleana de forma efectiva.

La tesis se divide en tres capítulos principales, además del presente, en el que repasamos brevemente la historia de las funciones *bent* a lo largo de estas últimas cuatro décadas y recopilamos los resultados preliminares necesarios para la comprensión y entendimiento de la tesis y de la notación utilizada. En el segundo capítulo demostramos una serie de propiedades del grado de las funciones booleanas cualesquiera y construimos algoritmos basados en ellas, útiles para determinar computacionalmente el grado partiendo del soporte o tabla de verdad que define a la función. En el tercer capítulo presentamos construcciones de funciones *de no linealidad perfecta* de $2k$ variables teniendo como punto de partida una base del espacio vectorial $\mathbb{F}_2^{2k}$. Y por último, en el cuarto capítulo introducimos construcciones de una clase especial de funciones *de no linealidad perfecta*, conocidas como Partial Spread ($\mathcal{PS}$), planteando una serie de cuestiones abiertas que merecería la pena investigar en el futuro.

1.2 Resultados previos

Denotamos por $\mathbb{F}_2$ el cuerpo de Galois de dos elementos, 0 y 1, con la adición (denotada por $\oplus$) y la multiplicación (denotada por yuxtaposición). Para cada entero positivo n, $\mathbb{F}_2^n$ es un espacio vectorial de dimensión n sobre $\mathbb{F}_2$ con la adición (denotada también por $\oplus$) dada por

$$\boldsymbol{a} \oplus \boldsymbol{b} = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n)$$

para $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ y $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$ en $\mathbb{F}_2^n$. Consideramos también el producto interno

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle = a_1 b_1 \oplus a_2 b_2 \oplus \cdots \oplus a_n b_n$$

de $\boldsymbol{a}$ y $\boldsymbol{b}$.

Cada $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{F}_2^n$, tiene asociado el entero positivo

$$a = a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_{n-1} 2^1 + a_n 2^0 \ \in \mathbb{Z}_{2^n}.$$

Decimos entonces que $\boldsymbol{a}$ es la **expansión binaria** de n dígitos de a. Dado que la aplicación

$$\Phi : \mathbb{F}_2^n \longrightarrow \mathbb{Z}_{2^n} \quad \text{definida por} \quad \Phi(\boldsymbol{a}) = a$$

es biyectiva, podemos identificar $\mathbb{F}_2^n$ con $\mathbb{Z}_{2^n}$ y así escribir $\boldsymbol{a}$ o a, según convenga, para denotar los elementos de $\mathbb{F}_2^n$, es decir,

$$\mathbb{F}_2^n = \{\boldsymbol{a} \mid 0 \leq a \leq 2^n - 1\}.$$

Además, denotamos por $\text{Env}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ el subespacio vectorial de $\mathbb{F}_2^n$ generado por los vectores $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \in \mathbb{F}_2^n$.

Decimos que el conjunto $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ es una **base de Gauss-Jordan** de cardinalidad k si la matriz cuyas filas son $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ están en forma escalonada reducida [10, 44].

Si $F \subseteq \mathbb{F}_2^n$ y $\boldsymbol{a} \oplus F = \{\boldsymbol{a} \oplus \boldsymbol{u} \mid \boldsymbol{u} \in F\}$ para $\boldsymbol{a} \in \mathbb{F}_2^n$, es evidente que

$$\text{Card}\,(\boldsymbol{a} \oplus F) = \text{Card}\,(F)\,.$$

Cuando F es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$ decimos que $\boldsymbol{a} \oplus F$ es el **subespacio afín** de dimensión k de $\mathbb{F}_2^n$ que pasa por $\boldsymbol{a}$ en la dirección de F.

Para un vector $\boldsymbol{u} \in \mathbb{F}_2^n$ denotamos por $S(\boldsymbol{u})$ al subespacio vectorial de $\mathbb{F}_2^n$ generado por los vectores de la base canónica de $\mathbb{F}_2^n$ correspondiente a las componentes no nulas de $\boldsymbol{u}$; es decir, si $u_{i_1}, u_{i_2}, \ldots, u_{i_k}$, con $1 \leq i_1 < i_2 < \cdots < i_k \leq n$,, son las componentes no nulas de $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, entonces

$$\boldsymbol{u} = \boldsymbol{2^{n-i_1}} \oplus \boldsymbol{2^{n-i_2}} \oplus \cdots \oplus \boldsymbol{2^{n-i_k}} \quad \text{y} \quad S(\boldsymbol{u}) = \text{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_k}}\right\}.$$

Decimos que k, es decir, el número de componentes no nulas de un vector $\boldsymbol{u}$, es el **peso** de $\boldsymbol{u}$ y lo denotamos por $w(\boldsymbol{u})$. Es evidente que $\dim S(\boldsymbol{u}) = w(\boldsymbol{u})$.

Para $1 \leq k < n$, consideraremos que $\mathbb{F}_2^n = \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$. Así que, si $\boldsymbol{u} \in \mathbb{F}_2^n$, entonces $\boldsymbol{u} = (\boldsymbol{v}, \boldsymbol{w})$ con $\boldsymbol{v} \in \mathbb{F}_2^k$ y $\boldsymbol{w} \in \mathbb{F}_2^{n-k}$. Por lo tanto, si v y w son números enteros cuyas expansiones binarias de k y $n-k$ dígitos son respectivamente los vectores $\boldsymbol{v}$ y $\boldsymbol{w}$, entonces $u = v\,2^{n-k} + w$ es el número entero cuya expansión binaria de n dígitos es el vector $\boldsymbol{u}$. En particular, si $\boldsymbol{a} \in \mathbb{F}_2^{n-k}$, también denotamos por $\boldsymbol{a}$ al vector $(\boldsymbol{0}, \boldsymbol{a}) \in \mathbb{F}_2^n$.

Una **función booleana** de n variables es una aplicación $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Denotamos por $\mathcal{B}_n$ el conjunto de todas las funciones booleanas de n variables. Es bien conocido que $\mathcal{B}_n$, con la adición usual de funciones (que también denotamos $\oplus$), definida por

$$(f \oplus g)(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus g(\boldsymbol{x}), \quad \text{para } f, g \in \mathcal{B}_n.$$

es un espacio vectorial de dimensión 2^n sobre $\mathbb{F}_2$, así que $\mathrm{Card}\,(\mathcal{B}_n) = 2^{2^n}$.

Si $f \in \mathcal{B}_n$, llamamos **tabla de verdad** de f (véase [80, 84]) a la secuencia binaria de longitud 2^n dada por

$$\boldsymbol{\xi}_f = (f(\boldsymbol{0}),\ f(\boldsymbol{1}),\ \ldots,\ f(\boldsymbol{2^n - 1})),$$

es decir, la i-ésima componente de $\boldsymbol{\xi}_f$, coincide con $f(\boldsymbol{i})$, para $\boldsymbol{i} = \boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, \ldots, \boldsymbol{2^n - 1}$.

Definición 1.1: Llamamos **soporte** de f, y escribimos $\mathrm{Sop}\,(f)$, al conjunto de vectores de $\mathbb{F}_2^n$ cuya imagen por f es distinta de 0, es decir,

$$\mathrm{Sop}\,(f) = \{\boldsymbol{i} \in \mathbb{F}_2^n \mid f(\boldsymbol{i}) \neq 0\},$$

o equivalentemente,

$$\mathrm{Sop}\,(f) = \{\boldsymbol{i} \in \mathbb{F}_2^n \mid f(\boldsymbol{i}) = 1\}.$$

Por tanto, $\mathrm{Sop}\,(f)$ está formado por los vectores de $\mathbb{F}_2^n$ correspondientes a las expansiones binarias de las componentes de $\boldsymbol{\xi}_f$ que son iguales a 1. De acuerdo con la identificación que hemos hecho de los elementos de $\mathbb{F}_2^n$ y $\mathbb{Z}_{2^n}$, también podemos escribir

$$\mathrm{Sop}\,(f) = \{i \in \mathbb{Z}_{2^n} \mid f(\boldsymbol{i}) = 1\}.$$

Definición 1.2: 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,

$$w(f) = \mathrm{Card}\left(\mathrm{Sop}\left(f\right)\right).$$

Además, si consideramos 0 y 1 como elementos de $\mathbb{F}_2$ y de $\mathbb{Z}$ indistintamente, entonces

$$w(f) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} f(\boldsymbol{x}).$$

Obviamente, f es la función nula si y sólo si $\mathrm{Sop}\left(f\right) = \emptyset$ y entonces $w(f) = 0$. Análogamente, f es la función constante 1 si y sólo si $\mathrm{Sop}\left(f\right) = \mathbb{F}_2^n$ y, en este caso, $w(f) = 2^n$.

Si $f \in \mathcal{B}_n$, llamamos **función complementaria** de f a la función $g \in \mathcal{B}_n$ dada por $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$ para todo $\boldsymbol{x} \in \mathbb{F}_2^n$. Escribimos $1 \oplus f$ para denotar la función complementaria de f. Es evidente que

$$\mathrm{Sop}\left(1 \oplus f\right) = \mathbb{F}_2^n \setminus \mathrm{Sop}\left(f\right)$$

y, por tanto, $w(1 \oplus f) = 2^n - w(f)$.

El soporte de una función booleana cumple las siguientes propiedades.

Teorema 1.1: *Si $f \in \mathcal{B}_n$ y $\boldsymbol{a} \in \mathbb{F}_2^n$, entonces*

(a) $\boldsymbol{a} \oplus \mathrm{Sop}\left(f\right) = \{\boldsymbol{a} \oplus \boldsymbol{b} \mid \boldsymbol{b} \in \mathrm{Sop}\left(f\right)\}$ *es el soporte de la función booleana* $f(\boldsymbol{a} \oplus \boldsymbol{x})$,

(b) $\mathrm{Sop}\left(f\right) \Delta (\boldsymbol{a} \oplus \mathrm{Sop}\left(f\right))$ *es el soporte de la función booleana* $f(\boldsymbol{x}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{x})$ *donde* Δ *denota la diferencia simétrica de conjuntos.*

Demostración:

(a) Consideramos la función $g(\boldsymbol{x}) = f(\boldsymbol{a} \oplus \boldsymbol{x})$.

Probaremos que $\mathrm{Sop}\left(g\right) = \boldsymbol{a} \oplus \mathrm{Sop}\left(f\right)$. Supongamos que $\boldsymbol{c} \in \mathbb{F}_2^n$. Tenemos que $\boldsymbol{c} \in \boldsymbol{a} \oplus \mathrm{Sop}\left(f\right)$ si y sólo si existe $\boldsymbol{b} \in \mathrm{Sop}\left(f\right)$ tal que $\boldsymbol{c} = \boldsymbol{a} \oplus \boldsymbol{b}$, pero entonces $\boldsymbol{b} = \boldsymbol{a} \oplus \boldsymbol{c}$, con lo que $f(\boldsymbol{a} \oplus \boldsymbol{c}) = 1$, esto es, $\boldsymbol{c} \in \mathrm{Sop}\left(g\right)$.

(b) Supongamos que $\boldsymbol{b} \in \mathbb{F}_2^n$. Tenemos que $f(\boldsymbol{b}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{b}) = 1$ si y sólo si $f(\boldsymbol{b}) = 1$ o $f(\boldsymbol{a} \oplus \boldsymbol{b}) = 1$ pero $f(\boldsymbol{b}) \neq f(\boldsymbol{a} \oplus \boldsymbol{b})$, por tanto, de acuerdo con el apartado (a), tenemos que $\boldsymbol{b} \in \mathrm{Sop}\,(f)$ o $\boldsymbol{b} \in \boldsymbol{a} \oplus \mathrm{Sop}\,(f)$ y $\boldsymbol{b} \notin \mathrm{Sop}\,(f) \cap (\boldsymbol{a} \oplus \mathrm{Sop}\,(f))$, por lo que $\boldsymbol{b} \in \mathrm{Sop}\,(f)\,\Delta(\boldsymbol{a} \oplus \mathrm{Sop}\,(f))$. □

Análogamente podemos comprobar que, de modo más general, si $f, g \in \mathcal{B}_n$, entonces $\mathrm{Sop}\,(f \oplus g) = \mathrm{Sop}\,(f)\,\Delta\,\mathrm{Sop}\,(g)$, donde, como en el caso anterior, Δ denota la diferencia simétrica de conjuntos. Consecuentemente

$$w(f \oplus g) \equiv w(f) + w(g) \pmod 2.$$

En general, si $f_j \in \mathcal{B}_n$, para $j = 1, 2, \ldots, m$, entonces

$$\mathrm{Sop}\left(\bigoplus_{j=1}^{m} f_j\right) = \bigtriangleup_{j=1}^{m} \mathrm{Sop}\,(f_j) \tag{1.1}$$

y, por tanto,

$$w\left(\bigoplus_{j=1}^{m} f_j\right) \equiv \sum_{j=1}^{m} w(f_j) \pmod 2. \tag{1.2}$$

Definición 1.3: Decimos que una función $f \in \mathcal{B}_n$ es **equilibrada** si su tabla de verdad contiene el mismo número de 0 que de 1, es decir, si $w(f) = 2^{n-1}$.

Es evidente que f es equilibrada si y sólo si $1 \oplus f$ es equilibrada.

Definición 1.4: Decimos que $f \in \mathcal{B}_n$ es una **función afín** si

$$f(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle \oplus b$$

donde $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \mathbf{0}$ y $b \in \mathbb{F}_2$. Si $b = 0$, decimos que f es una **función lineal**.

En todo lo que sigue denotamos por $l_{\boldsymbol{a}}(\boldsymbol{x})$ la función lineal definida por $\boldsymbol{a} \in \mathbb{F}_2^n$, es decir $l_{\boldsymbol{a}}(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle$ para todo $\boldsymbol{x} \in \mathbb{F}_2^n$. Denotamos por $\mathcal{A}_n$ el conjunto de todas las funciones afines de n variables. Puede comprobarse que cualquier función afín es equilibrada, pero la proposición recíproca no es cierta.

Supongamos ahora que $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ donde cada x_j, para $j = 1, 2, \ldots, n$, es una variable binaria. Si $f \in \mathcal{B}_n$, entonces podemos escribir $f(\boldsymbol{x})$ unívocamente como (ver, por ejemplo, [60, 80, 84, 87, 88])

$$f(\boldsymbol{x}) = \bigoplus_{\boldsymbol{u} \in \mathbb{F}_2^n} \mu_f(\boldsymbol{u}) \boldsymbol{x}^{\boldsymbol{u}} \tag{1.3}$$

donde $\mu_f(\boldsymbol{u}) \in \mathbb{F}_2$ y si, $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, entonces

$$\boldsymbol{x}^{\boldsymbol{u}} = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n} \quad \text{con} \quad x_j^{u_j} = \begin{cases} x_j, & \text{si } u_j = 1, \\ 1, & \text{si } u_j = 0. \end{cases}$$

La expresión (1.3), donde cada término $\boldsymbol{x}^{\boldsymbol{u}}$ se denomina **monomio**, se llama la **forma normal algebraica** de $f(\boldsymbol{x})$, más conocida por sus siglas en inglés ANF *(algebraic normal form)*, que utilizaremos en lo sucesivo. Notemos que μ_f es también una función booleana de n variables, conocida con el nombre de **transformada de Möbius** de f.

Definición 1.5: Llamamos **grado** del monomio $\boldsymbol{x}^{\boldsymbol{u}}$ al peso del vector $\boldsymbol{u}$, esto es a $w(\boldsymbol{u})$.

Para $f \in \mathcal{B}_n$, llamamos **grado** de f, denotado por $\operatorname{gr}(f)$, al grado máximo de los monomios de su ANF. Así que,

$$\operatorname{gr}(f) = \max\{w(\boldsymbol{u}) \mid \mu_f(\boldsymbol{u}) = 1\}. \tag{1.4}$$

Obviamente, $\operatorname{gr}(1 \oplus f) = \operatorname{gr}(f)$ y $\operatorname{gr}(1) = 0$. Como es habitual, decimos que $\operatorname{gr}(0) = -\infty$.

Si $f \in \mathcal{B}_n$ es una **función afín** la expresión (1.3) se convierte en

$$f(\boldsymbol{x}) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$$

con $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n \setminus \mathbf{0}$, y $a_0 \in \mathbb{F}_2$, con lo que $\operatorname{gr}(f) = 1$.

Por otra parte, si $f \in \mathcal{B}_n$ y denotamos por $\boldsymbol{\mu}_f$ la tabla de verdad de la transformada de Möbious μ_f de f; esto es,

$$\boldsymbol{\mu}_f = (\mu_f(\mathbf{0}), \mu_f(\mathbf{1}), \ldots, \mu_f(\mathbf{2^n - 1})),$$

y $\boldsymbol{\xi}_f$ es la tabla de verdad de f, entonces (ver, por ejemplo, [87])

$$\boldsymbol{\mu}_f = \boldsymbol{\xi}_f A_n$$

donde

$$A_n = \begin{bmatrix} A_{n-1} & A_{n-1} \\ O & A_{n-1} \end{bmatrix} \text{ para } n \geq 1, \quad \text{con } A_0 = [1].$$

Finalmente, si $f \in \mathcal{B}_n$ y para todo $\boldsymbol{a} \in \mathbb{F}_2^n$ consideramos $g_{\boldsymbol{a}} \in \mathcal{B}_n$ tal que $g_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{a})$, es difícil establecer una relación entre $\boldsymbol{\mu}_f$ y $\boldsymbol{\mu}_{g_{\boldsymbol{a}}}$. Sin embargo, resulta claro que $\mathrm{gr}\,(g_{\boldsymbol{a}}) = \mathrm{gr}\,(f)$, para todo $\boldsymbol{a} \in \mathbb{F}_2^n$, y es fácil apreciar que

$$\mathrm{Sop}\,(g_{\boldsymbol{a}}) = \boldsymbol{a} \oplus \mathrm{Sop}\,(f), \quad \text{para todo } \boldsymbol{a} \in \mathbb{F}_2^n.$$

Definición 1.6: 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,

$$d(f, g) = w(f \oplus g).$$

La no linealidad, que definimos a continuación, fue introducida por Pieprzyk y Finkelstein [85].

Definición 1.7: Llamamos **no linealidad** de una función $f \in \mathcal{B}_n$, y escribimos $\mathrm{NL}(f)$, al mínimo de las distancias entre f y cualquier función afín, es decir,

$$\mathrm{NL}(f) = \min\{d(f, \varphi) \mid \varphi \in \mathcal{A}_n\}.$$

La no linealidad de una función $f \in \mathcal{B}_n$ está acotada superiormente (véase [14, 43, 73, 94]) por

$$\mathrm{NL}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Las funciones booleanas que alcanzan la máxima no linealidad posible se conocen con el nombre de *funciones de no linealidad perfecta* (véase [14, 43, 73, 94]), también denominadas funciones *bent* (véase [94]). Más formalmente,

Definición 1.8: Sea $f \in \mathcal{B}_n$. Decimos que f es una **función de no linealidad perfecta** o **función bent** si

$$\mathrm{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Por tanto, de acuerdo con la definición anterior, las funciones *bent* solamente existen para n par.

El resultado siguiente (véase [73, 93, 94]), que enunciamos para futuras referencias, nos proporciona una caracterización de las funciones *bent*.

Teorema 1.2: *Sea $f(\boldsymbol{x})$ una función booleana de n variables (con n par). Las condiciones siguientes son equivalentes.*

(a) *$f(\boldsymbol{x})$ es una función bent,*
(b) *$f(\boldsymbol{x}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{x})$ es equilibrada para todo $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$.*
(c) *El número de 1 de la tabla de verdad de $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ es $2^{n-1} \pm 2^{\frac{n}{2}-1}$ para todo $\boldsymbol{a} \in \mathbb{F}_2^n$.*

Una consecuencia inmediata del teorema anterior es que si $f(\boldsymbol{x})$ es una función *bent* de n variables, entonces tomando $\boldsymbol{a} = \mathbf{0}$ en el apartado (c), tenemos que el número de 1 de su tabla de verdad, es decir, su peso, es $2^{n-1} \pm 2^{\frac{n}{2}-1}$ y, por tanto, $f(\boldsymbol{x})$ no es equilibrada.

Una función *bent*, siendo no equilibrada, se puede utilizar en la construcción de funciones booleanas equilibradas con alta no linealidad, considerándose una buena herramienta para la obtención de potentes *S-boxes* [78].

Otra consecuencia inmediata del teorema anterior es que si $f(\boldsymbol{x})$ es una función *bent* de n variables de peso $2^{n-1} \pm 2^{\frac{n}{2}-1}$, entonces su función complementaria $1 \oplus f(\boldsymbol{x})$ es también una función *bent* de n variables, aunque su peso es $2^{n-1} \mp 2^{\frac{n}{2}-1}$.

Finalmente (véase [92]), si $f(\boldsymbol{x})$ es una función *bent* de n variables, entonces $f(\boldsymbol{x} \oplus \boldsymbol{a})$, para todo $\boldsymbol{a} \in \mathbb{F}_2^n$, es también una función *bent* de n variables con el mismo peso que $f(\boldsymbol{x})$. También (véase [92]), $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ es una función *bent* de n variables para todo $\boldsymbol{a} \in \mathbb{F}_2^n$, aunque el peso de esta función no coincide necesariamente con el peso de $f(\boldsymbol{x})$.

1.3 Algunas construcciones clásicas de funciones *bent*

Como hemos dicho en la sección 1.1, no se conoce ningún método que proporcione todas las funciones *bent* de n variables para cualquier entero positivo par n. Sin embargo, existen distintos métodos que permiten obtener funciones *bent* de $n+2$ variables a partir de funciones *bent* de n variables, o bien funciones *bent* de n variables a partir de funciones (no necesariamente *bent*) de $n/2$ variables. En esta sección comentamos brevemente cuatro de tales métodos: la construcción de Rothaus, la de Maiorana-McFarland, la de Carlet y la de Dillon, que podemos considerar como construcciones clásicas.

Rothaus [91, página 303] presenta dos construcciones de funciones *bent* que recogemos en el teorema siguiente:

Teorema 1.3: *Supongamos que* $n = 2k$.

(a) *Si* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^k$ *y* f *es una función booleana de* k *variables, entonces*

$$Q(\boldsymbol{x}, \boldsymbol{y}) = \langle \boldsymbol{x}, \boldsymbol{y} \rangle \oplus f(\boldsymbol{y})$$

es una función bent de n *variables.*

(b) *Si* $A(\boldsymbol{x})$, $B(\boldsymbol{x})$ *y* $C(\boldsymbol{x})$ *son funciones bent de* n *variables tales que* $A(\boldsymbol{x}) \oplus B(\boldsymbol{x}) \oplus C(\boldsymbol{x})$ *es también una función bent de* n *variables, entonces*

$$\begin{aligned} R(\boldsymbol{x}, x_{n+1}, x_{n+2}) = {} & A(\boldsymbol{x})\, B(\boldsymbol{x}) \oplus B(\boldsymbol{x})\, C(\boldsymbol{x}) \oplus C(\boldsymbol{x})\, A(\boldsymbol{x}) \\ & \oplus (A(\boldsymbol{x}) \oplus B(\boldsymbol{x}))\, x_{n+1} \oplus (A(\boldsymbol{x}) \oplus C(\boldsymbol{x}))\, x_{n+2} \oplus x_{n+1}\, x_{n+2} \end{aligned}$$

es una función bent de $n+2$ *variables.*

Como veremos seguidamente, la construcción (a) es un caso particular de la construcción de Maiorana-McFarland, por tanto, nos referiremos únicamente a la construcción (b) como la construcción de Rothaus. Esta construcción presenta el inconveniente de la inexistencia hasta el momento de una caracterización general de las ternas $(A(\boldsymbol{x}), B(\boldsymbol{x}), C(\boldsymbol{x}))$ de funciones *bent* de n variables tales que $A(\boldsymbol{x}) \oplus$

$B(\boldsymbol{x}) \oplus C(\boldsymbol{x})$ es también una función *bent* de n variables, excepto solamente para algunos casos particulares (véase [91]); por tanto, no es posible contar directamente cuántas funciones *bent* de esta clase existen para cada valor de n.

El resultado siguiente (que puede encontrarse, por ejemplo en [46, 59]) recoge la construcción de Maiorana-McFarland de funciones *bent*.

Teorema 1.4: *Supongamos que $n = 2k$. Si $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^k$, π es una permutación cualquiera de $\mathbb{F}_2^k$, y f es una función booleana de k variables, entonces*

$$M(\boldsymbol{x}, \boldsymbol{y}) = \langle \boldsymbol{x}, \pi(\boldsymbol{y}) \rangle \oplus f(\boldsymbol{y})$$

es una función bent de n variables.

Notemos que si π es la permutación identidad, entonces la construcción de Maiorana-McFarland coincide con la primera construcción de Rothaus definida en el teorema 1.3(a). Es fácil comprobar que el número de funciones *bent* que podemos construir de acuerdo con el resultado anterior es $(2^k)!\, 2^{2^k}$.

El resultado siguiente (que puede encontrarse, por ejemplo en [12]) recoge la construcción de Carlet de funciones *bent*.

Teorema 1.5: *Si $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ son funciones bent de n variables y $g_0(\boldsymbol{y})$ y $g_1(\boldsymbol{y})$ son funciones bent de m variables, entonces*

$$C(\boldsymbol{y}, \boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus g_0(\boldsymbol{y}) \oplus (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}))\,(g_0(\boldsymbol{y}) \oplus g_1(\boldsymbol{y}))$$

es una función bent de $n + m$ variables.

A diferencia de la construcción de Maiorana-McFarland, en la construcción de funciones *bent* de Carlet no podemos contabilizar cuántas funciones *bent* de esta clase podemos construir. Esto se debe a que partiendo de dos cuaternas de funciones *bent* distintas,

$$(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), g_0(\boldsymbol{y}), g_1(\boldsymbol{y})) \quad \text{y} \quad (f_0'(\boldsymbol{x}), f_1'(\boldsymbol{x}), g_0'(\boldsymbol{y}), g_1'(\boldsymbol{y})),$$

y construyendo las correspondientes funciones *bent* a partir del teorema anterior,

podemos obtener la misma función *bent*, es decir, puede ocurrir que

$$\begin{aligned} C(\boldsymbol{y},\boldsymbol{x}) &= f_0(\boldsymbol{x}) \oplus g_0(\boldsymbol{y}) \oplus (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}))\,(g_0(\boldsymbol{y}) \oplus g_1(\boldsymbol{y})) \\ &= f_0'(\boldsymbol{x}) \oplus g_0'(\boldsymbol{y}) \oplus (f_0'(\boldsymbol{x}) \oplus f_1'(\boldsymbol{x}))\,(g_0'(\boldsymbol{y}) \oplus g_1'(\boldsymbol{y})) = C'(\boldsymbol{y},\boldsymbol{x}) \end{aligned}$$

En [89, Ejemplo 1.4] puede encontrarse un ejemplo en el que se pone de manifiesto lo dicho anteriormente.

El siguiente teorema introduce la clase $\mathcal{PS}$ de funciones *bent* dada por Dillon (véase [46]).

Teorema 1.6: *Supongamos que $G_1, G_2, \ldots, G_t$ son subespacios vectoriales de $\mathbb{F}_2^n$ de dimensión $n/2$ tal que $G_i \cap G_j = \{\mathbf{0}\}$ para $i, j = 1, 2, \ldots, t$ con $i \neq j$, y consideremos el conjunto*

$$B = \begin{cases} \bigcup_{i=1}^{t} G_i^*, & si \;\; t = 2^{\frac{n}{2}-1}, \\ \{\mathbf{0}\} \cup \bigcup_{i=1}^{t} G_i^*, & si \;\; t = 2^{\frac{n}{2}-1}+1, \end{cases}$$

con $G_i^* = G_i \setminus \{\mathbf{0}\}$. Entonces, B es el soporte de una función bent de n variables.

Dillon denotó por $\mathcal{PS}^-$ (respectivamente, $\mathcal{PS}^+$), la clase de funciones *bent* para la cual $t = 2^{\frac{n}{2}-1}$ (respectivamente, $t = 2^{\frac{n}{2}-1}+1$).

Capítulo 2

Propiedades algebraicas del soporte de una función booleana y de su grado

2.1 Introducción

En este capítulo empleamos el soporte de una función booleana para establecer algunas propiedades algebraicas que nos van a permitir obtener el grado de una función booleana sin necesidad de calcular explícitamente su forma normal algebraica. La determinación completa de la forma normal algebraica de una función booleana cuya tabla de verdad (equivalentemente, su soporte) es conocida, requiere la computación simultánea de todos los coeficientes del polinomio que la define, pero si queremos saber sólo su grado y no necesitamos conocer todos sus monomios, es posible reducir sustancialmente el número de operaciones necesarias empleando las propiedades que introducimos en este capítulo. Además, utilizando dichas propiedades, construimos algunos algoritmos y calculamos el tiempo medio necesario para la obtención del grado de funciones booleanas a partir de su su soporte.

Más concretamente, en la sección 2.2, introducimos algunas definiciones y notaciones básicas que emplearemos en lo sucesivo, en la sección 2.3, proporcionamos los resultados principales del capítulo; en particular, enunciamos y demostramos algunas propiedades que permiten determinar el grado de una función booleana de n variables a partir de su suporte. En la sección 2.4, introducimos algunas propiedades del álgebra lineal que nos permiten mejorar el proceso descrito en la sección 2.3.

Asimismo, describimos algunos algoritmos basados en las propiedades introducidas y evaluamos el tiempo requerido en un ordenador personal estándar para obtener el grado de algunas funciones booleanas a partir de su soporte. Una versión preliminar de algunos de los resultados de las secciones 2.3 y 2.4, fue publicada en [32, 36]. La sección 2.5 está dedicada a los resultados numéricos y, finalmente, presentamos las conclusiones en la sección 2.6

2.2 Propiedades básicas

Comenzamos esta sección introduciendo el siguiente teorema, que es una reformulación de un resultado bien conocido de la teoría de códigos (véase [67, teorema 1, página 372]).

Teorema 2.1: *Si $f \in \mathcal{B}_n$, entonces los coeficientes $\mu_f(\boldsymbol{u})$ de la ANF de f pueden ser calculados como*

$$\mu_f(\boldsymbol{u}) = \bigoplus_{\boldsymbol{a} \in S(\boldsymbol{u})} f(\boldsymbol{a}), \quad \text{para todo } \boldsymbol{u} \in \mathbb{F}_2^n. \tag{2.1}$$

Demostración: Supongamos que $u_{i_1}, u_{i_2}, \ldots, u_{i_k}$, con $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, son componentes no nulas de $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$. Análogamente, supongamos que $v_{j_1}, v_{j_2}, \ldots, v_{j_l}$, con $1 \leq j_1 < j_2 < \cdots < j_l \leq n$, son componentes no nulas de $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. Ahora no es difícil demostrar que $\boldsymbol{v} \in S(\boldsymbol{u})$ si y sólo si $\{j_1, j_2, \ldots, j_l\} \subseteq \{i_1, i_2, \ldots, i_k\}$. El resultado se sigue entonces de [67, teorema 1, página 372]. □

Como consecuencia del resultado anterior, obtenemos el siguiente corolario.

Corolario 2.1: *Sea $f \in \mathcal{B}_n$.*

(a) *Supongamos que $\boldsymbol{u} \in \mathbb{F}_2^n$. El monomio $\boldsymbol{x}^{\boldsymbol{u}}$ está en la ANF de f si y sólo si*

$$\operatorname{Card}(\operatorname{Sop}(f) \cap S(\boldsymbol{u})) \equiv 1 \pmod 2.$$

(b) $\operatorname{gr}(f) = \max\{w(\boldsymbol{u}) \mid \boldsymbol{u} \in \mathbb{F}_2^n \text{ y } \operatorname{Card}(\operatorname{Sop}(f) \cap S(\boldsymbol{u})) \equiv 1 \pmod 2\}$.

DEMOSTRACIÓN: Sea $\boldsymbol{u} \in \mathbb{F}_2^n$. Como consecuencia del teorema 2.1 y la expresión (1.3) tenemos que el monomio $\boldsymbol{x}^{\boldsymbol{u}}$ está en la ANF de f si y sólo si $\bigoplus_{\boldsymbol{a} \in S(\boldsymbol{u})} f(\boldsymbol{a}) = 1$. Ahora, teniendo en cuenta que

$$\bigoplus_{\boldsymbol{a} \in S(\boldsymbol{u})} f(\boldsymbol{a}) = \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(f) \cap S(\boldsymbol{u})} f(\boldsymbol{a})$$

tenemos que $\boldsymbol{x}^{\boldsymbol{u}}$ está en la ANF de f si y sólo si $\mathrm{Card}\left(\mathrm{Sop}\left(f\right) \cap S(\boldsymbol{u})\right) \equiv 1 \pmod 2$. Ésto prueba la parte (a).

La parte (b) se sigue de la parte (a), del teorema 2.1 y de la expresión (1.4). □

Un resultado análogo al corolario 2.1(a) fue obtenido en [99, corolario 5].

Una consecuencia inmediata que podemos deducir del corolario 2.1(a) es el corolario que sigue.

Corolario 2.2: *Sea $f \in \mathcal{B}_n$. Entonces $\mathrm{gr}\left(f\right) = n$ si y sólo si $w(f)$ es un número impar.*

DEMOSTRACIÓN: Consideremos el vector $\boldsymbol{u} = \bigoplus_{i=1}^{n} \boldsymbol{2^{n-i}} \in \mathbb{F}_2^n$; esto es, $\boldsymbol{u}$ es el vector con todas sus componentes iguales a 1. Claramente $S(\boldsymbol{u}) = \mathbb{F}_2^n$ y por tanto

$$\mathrm{Sop}\left(f\right) \cap S(\boldsymbol{u}) = \mathrm{Sop}\left(f\right)$$

El resultado se sigue ahora del corolario 2.1(a) porque $\mathrm{gr}\left(f\right) = n$ si y sólo si el monomio $\boldsymbol{x}^{\boldsymbol{u}}$ está en la ANF de f, y $w(f) = \mathrm{Card}\left(\mathrm{Sop}\left(f\right)\right)$. □

Como consecuencia inmediata de los corolarios 2.1 y 2.2 obtenemos el siguiente algoritmo que nos permite calcular el grado de la función booleana cuyo soporte es un conjunto dado.

Algoritmo 2.1: Supongamos que F es un subconjunto de $\mathbb{F}_2^n$ y sea $f \in \mathcal{B}_n$ tal que $F = \mathrm{Sop}\left(f\right)$

Este algoritmo calcula $\mathrm{gr}\left(f\right)$.

(a) Si $\mathrm{Card}\,(F)$ es impar entonces $\mathrm{gr}\,(f) = n$. Ir al paso (d)
(b) Para $\boldsymbol{u} \in \mathbb{F}_2^n$ calcula $w(\boldsymbol{u})$ y $\mathrm{Card}\,(F \cap S(\boldsymbol{u}))$.
(c) $\mathrm{gr}\,(f) = \max\{w(\boldsymbol{u}) \mid \boldsymbol{u} \in \mathbb{F}_2^n \text{ y } \mathrm{Card}\,(\mathrm{Sop}\,(f) \cap S(\boldsymbol{u})) \equiv 1 \pmod 2\}$
(d) Fin.

Para $k = 0, 1, 2, \ldots, 2^n$, es evidente que el número de funciones booleanas de n variables cuyo soporte tiene k elementos es $\binom{2^n}{k}$, mientras que el número de funciones booleanas de n variables cuyo soporte contiene un número impar de elementos es

$$\sum_{i=1}^{2^{n-1}} \binom{2^n}{2i-1} = 2^{2^n-1}.$$

Entonces, por el corolario 2.2, exactamente la mitad de las funciones booleanas de n variables tienen grado n y, para tales funciones, determinar su grado a partir de su soporte es inmediato (ver el paso (a) del algoritmo 2.1).

Otra consecuencia inmediata del corolario 2.1(a) es que el número de monomios en la ANF de $f \in \mathcal{B}_n$ viene dado por

$$\mathrm{Card}\left(\{\boldsymbol{u} \in \mathbb{F}_2^n \mid \mathrm{Card}\,(\mathrm{Sop}\,(f) \cap S(\boldsymbol{u})) \equiv 1 \pmod 2\}\right).$$

Un resultado similar al corolario 2.1(b) fue introducido también en [99, teorema 16] donde los autores establecieron que

$$\mathrm{gr}\,(f) = \max\{\dim U \mid U \text{ es un subespacio vectorial de } \mathbb{F}_2^n \text{ y } w(f_U) \text{ es impar}\} \quad (2.2)$$

donde f_U denota la restricción de f a U. Sin embargo, nuestro resultado es mejor que éste, como podemos ver en el siguiente ejemplo.

Observemos previamente que para cualquier conjunto U de $\mathbb{F}_2^n$ (no necesariamente un subespacio vectorial), tenemos que

$$w(f_U) = \mathrm{Card}\,(\mathrm{Sop}\,(f) \cap U)$$

Ejemplo 2.1: Sea $f \in \mathcal{B}_4$ tal que $\mathrm{Sop}\,(f) = \{\mathbf{2}, \mathbf{4}, \mathbf{5}, \mathbf{7}, \mathbf{8}, \mathbf{9}, \mathbf{11}, \mathbf{12}, \mathbf{13}, \mathbf{15}\}$.

Sólo hay un subespacio vectorial de dimensión 4 de $\mathbb{F}_2^4$ que se corresponde con el vector $\mathbf{15} = (1, 1, 1, 1)$; que es $S(\mathbf{15}) = \mathbb{F}_2^4$. Para este vector tenemos, obviamente,

que $\mathrm{Card}\,(\mathrm{Sop}\,(f) \cap S(\boldsymbol{u})) = 10$ que no es un número impar. Ésto quiere decir, por el corolario 2.1(b), que $\mathrm{gr}\,(f) < 4$. Notemos que éste es exactamente el argumento usado en la demostración del corolario 2.2.

Los únicos vectores de peso 3 en $\mathbb{F}_2^4$ son **7**, **11**, **13** y **14**, para los que tenemos

$$S(\mathbf{7}) = \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{5},\mathbf{6},\mathbf{7}\}, \qquad S(\mathbf{11}) = \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{8},\mathbf{9},\mathbf{10},\mathbf{11}\},$$

$$S(\mathbf{13}) = \{\mathbf{0},\mathbf{1},\mathbf{4},\mathbf{5},\mathbf{8},\mathbf{9},\mathbf{12},\mathbf{13}\} \quad \text{y} \quad S(\mathbf{14}) = \{\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6},\mathbf{8},\mathbf{10},\mathbf{12},\mathbf{14}\}.$$

Luego

$$\mathrm{Sop}\,(f) \cap S(\mathbf{7}) = \{\mathbf{2},\mathbf{4},\mathbf{5},\mathbf{7}\}, \qquad \mathrm{Sop}\,(f) \cap S(\mathbf{11}) = \{\mathbf{2},\mathbf{8},\mathbf{9},\mathbf{11}\},$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{13}) = \{\mathbf{4},\mathbf{5},\mathbf{8},\mathbf{9},\mathbf{12},\mathbf{13}\} \quad \text{y} \quad \mathrm{Sop}\,(f) \cap S(\mathbf{14}) = \{\mathbf{2},\mathbf{4},\mathbf{8},\mathbf{12}\}.$$

Ahora, de nuevo por el corolario 2.1(a), tenemos que $\mathrm{gr}\,(f) < 3$.

Observemos que para obtener el mismo resultado empleando la expresión (2.2), necesitaríamos calcular $\mathrm{Card}\,(\mathrm{Sop}\,(f) \cap U)$ para cada uno de los 35 subespacios vectoriales U de $\mathbb{F}_2^4$ de dimensión 3 (véase, por ejemplo, [96, pág 46] para el número de subespacios vectoriales de dimensión k en $\mathbb{F}_q^n$).

Finalmente, como $S(\mathbf{3}) = \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}$, tenemos que $\mathrm{Sop}\,(f) \cap S(\mathbf{3}) = \{\mathbf{2}\}$ y, dado que $w(\mathbf{3}) = 2$, una vez más por el corolario 2.1(b), concluimos que $\mathrm{gr}\,(f) = 2$.

Si queremos obtener la ANF de $f(\boldsymbol{x})$, necesitamos saber qué monomios de grado 2 y 1 contiene.

Primero, observemos que los vectores de peso 2 en $\mathbb{F}_2^4$, además del vector **3** anteriormente considerado, son los vectores **5**, **6**, **9**, **10** y **12** para los que tenemos

$$S(\mathbf{5}) = \{\mathbf{0},\mathbf{1},\mathbf{4},\mathbf{5}\}, \qquad S(\mathbf{6}) = \{\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6}\}, \qquad S(\mathbf{9}) = \{\mathbf{0},\mathbf{1},\mathbf{8},\mathbf{9}\},$$

$$S(\mathbf{10}) = \{\mathbf{0},\mathbf{2},\mathbf{8},\mathbf{10}\} \qquad \text{y} \qquad S(\mathbf{12}) = \{\mathbf{0},\mathbf{4},\mathbf{8},\mathbf{12}\}.$$

Luego

$$\mathrm{Sop}\,(f) \cap S(\mathbf{5}) = \{\mathbf{4},\mathbf{5}\}, \qquad \mathrm{Sop}\,(f) \cap S(\mathbf{6}) = \{\mathbf{2},\mathbf{4}\}, \qquad \mathrm{Sop}\,(f) \cap S(\mathbf{9}) = \{\mathbf{8},\mathbf{9}\},$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{10}) = \{\mathbf{2},\mathbf{8}\} \quad \text{y} \quad \mathrm{Sop}\,(f) \cap S(\mathbf{12}) = \{\mathbf{4},\mathbf{8},\mathbf{12}\}.$$

Entonces, por el corolario 2.1(a) tenemos que los monomios definidos por los vectores **3** y **12**, esto es, los monomios x_3x_4 y x_1x_2 respectivamente, están en la ANF de f.

En segundo lugar, los vectores de peso 1 en $\mathbb{F}_2^4$ son $\mathbf{1}$, $\mathbf{2}$, $\mathbf{4}$ y $\mathbf{8}$ para los que tenemos

$$S(\mathbf{1}) = \{\mathbf{0}, \mathbf{1}\}, \qquad S(\mathbf{2}) = \{\mathbf{0}, \mathbf{2}\}, \qquad S(\mathbf{4}) = \{\mathbf{0}, \mathbf{4}\} \qquad \text{y} \qquad S(\mathbf{8}) = \{\mathbf{0}, \mathbf{8}\}.$$

Luego

$$\operatorname{Sop}(f) \cap S(\mathbf{1}) = \emptyset, \qquad \operatorname{Sop}(f) \cap S(\mathbf{2}) = \{\mathbf{2}\},$$
$$\operatorname{Sop}(f) \cap S(\mathbf{4}) = \{\mathbf{4}\} \qquad \text{y} \qquad \operatorname{Sop}(f) \cap S(\mathbf{8}) = \{\mathbf{8}\}.$$

Entonces, por el corolario 2.1(a) tenemos que los monomios definidos por los vectores $\mathbf{2}$, $\mathbf{4}$ y $\mathbf{8}$, esto es, los monomios x_3, x_2 y x_1 respectivamente, están en la ANF de f.

Finalmente, como $S(\mathbf{0}) = \{\mathbf{0}\}$ y $\mathbf{0} \notin \operatorname{Sop}(f)$, tenemos que el monomio $\boldsymbol{x}^{\mathbf{0}}$, esto es, el término constante 1, no está en la ANF de $f(\boldsymbol{x})$.

Consecuentemente, la ANF de $f(\boldsymbol{x})$ es

$$f(\boldsymbol{x}) = x_2 \oplus x_3 \oplus x_4 \oplus x_1x_2 \oplus x_3x_4. \qquad \blacksquare$$

Como podemos observar en el ejemplo anterior, para determinar completamente la ANF de $f(\boldsymbol{x})$ a partir de $\operatorname{Sop}(f)$, necesitamos calcular, para todo $\boldsymbol{u} \in \mathbb{F}_2^n$ el subespacio vectorial $S(\boldsymbol{u})$ y después la cardinalidad del conjunto $\operatorname{Sop}(f) \cap S(\boldsymbol{u})$. Es decir, necesitamos calcular 2^n subespacios vectoriales y la cardinalidad de la intersección del soporte de la función booleana con este subespacio vectorial. Por tanto, este procedimiento (es decir, el algoritmo 2.1) no constituye, en general, un algoritmo eficiente.

El siguiente resultado nos permite determinar explícitamente el soporte y el peso de cualquier monomio.

Teorema 2.2: *Supongamos que* $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ *y consideremos los vectores* $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$ *dados por*

$$\boldsymbol{u} = \bigoplus_{j=1}^{k} \mathbf{2}^{\mathbf{n-i_j}} \qquad y \qquad \boldsymbol{v} = \bigoplus_{\substack{l=1 \\ l \notin \{i_1, i_2, \ldots, i_k\}}}^{n} \mathbf{2}^{\mathbf{n-l}}$$

Si $f \in \mathcal{B}_n$ es el monomio definido por $\boldsymbol{u}$; esto es, $f(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{u}}$, entonces

$$\mathrm{Sop}\,(f) = \boldsymbol{u} \oplus S(\boldsymbol{v}). \tag{2.3}$$

En particular, $w(f) = 2^{n-k}$.

DEMOSTRACIÓN: Observemos que las componentes $i_1, i_2, \ldots, i_k$ de los vestores en $S(\boldsymbol{v})$ son iguales a cero, mientras que los componentes restantes pueden ser 0 o 1.

Primero, supongamos que $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in \mathrm{Sop}\,(f)$. Entonces

$$1 = \boldsymbol{a}^{\boldsymbol{u}} = a_{i_1} a_{i_2} \cdots a_{i_k}$$

y por tanto $a_{i_1} = a_{i_2} = \cdots = a_{i_k} = 1$. Las componentes restantes de $\boldsymbol{a}$ pueden ser 0 o 1 y en consecuencia, $\boldsymbol{a} \in \boldsymbol{u} \oplus S(\boldsymbol{v})$, de modo que $\mathrm{Sop}\,(f) \subseteq \boldsymbol{u} \oplus S(\boldsymbol{v})$.

Recíprocamente, supongamos ahora que $\boldsymbol{a} \in \boldsymbol{u} \oplus S(\boldsymbol{v})$. Entonces $\boldsymbol{a} = \boldsymbol{u} \oplus \boldsymbol{v}$ y teniendo en cuenta cómo están definidos $\boldsymbol{u}$ y $\boldsymbol{v}$, resulta evidente que $\boldsymbol{a}^{\boldsymbol{u}} = 1$; esto es, $\boldsymbol{a} \in \mathrm{Sop}\,(f)$. Por tanto $\boldsymbol{u} \oplus S(\boldsymbol{v}) \subseteq \mathrm{Sop}\,(f)$.

Ahora, de esta inclusión y la anterior, obtenemos la expresión (2.3).

Además, de la expresión (2.3), tenemos que $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = \mathrm{Card}\,(S(\boldsymbol{v}))$; esto es, $w(f) = 2^{n-k}$ porque $S(\boldsymbol{v})$ es un subespacio vectorial de $\mathbb{F}_2^n$ cuya dimensión es $w(\boldsymbol{v}) = n - k$. □

Una consecuencia inmediata del teorema anterior es que el peso del monomio formado por todas las variables (es decir, cuando $k = n$) es 1, mientras que el peso de cualquier otro monomio es una potencia de 2 con exponente positivo y, por lo tanto, un número par. Notemos también que la expresión (2.3) nos dice que el soporte de un monomio de grado k es un subespacio afín de dimensión $n - k$ de $\mathbb{F}_2^n$. El recíproco no es cierto; es decir, si el soporte de una función booleana es un subespacio afín, entonces la función booleana no es necesariamente un monomio, tal y como podemos ver en el siguiente ejemplo.

Ejemplo 2.2: Consideremos el subespacio afín de dimensión 2 de $\mathbb{F}_2^4$ definido por

$$\mathbf{10} \oplus \mathrm{Env}\,\{\mathbf{3}, \mathbf{6}\} = \{\mathbf{9}, \mathbf{10}, \mathbf{12}, \mathbf{15}\}$$

y sea $f \in \mathcal{B}_4$ tal que $\mathrm{Sop}\,(f) = \mathbf{10} \oplus \mathrm{Env}\,\{\mathbf{3}, \mathbf{6}\}$. Procediendo como en el ejemplo 2.1 tenemos que

$$\mathrm{Sop}\,(f) \cap S(\mathbf{0}) = \emptyset, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{1}) = \emptyset, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{2}) = \emptyset,$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{3}) = \emptyset, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{4}) = \emptyset, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{5}) = \emptyset,$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{6}) = \emptyset, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{7}) = \emptyset, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{8}) = \emptyset,$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{9}) = \{\mathbf{9}\}, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{10}) = \{\mathbf{10}\}, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{11}) = \{\mathbf{9}, \mathbf{10}\},$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{12}) = \{\mathbf{12}\}, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{13}) = \{\mathbf{9}, \mathbf{12}\},$$

$$\mathrm{Sop}\,(f) \cap S(\mathbf{14}) = \{\mathbf{10}, \mathbf{12}\}, \quad \mathrm{Sop}\,(f) \cap S(\mathbf{15}) = \{\mathbf{9}, \mathbf{10}, \mathbf{12}, \mathbf{15}\}.$$

Entonces, por el corolario 2.1(a) la ANF de f es

$$f(\boldsymbol{x}) = \boldsymbol{x}^{\mathbf{9}} \oplus \boldsymbol{x}^{\mathbf{10}} \oplus \boldsymbol{x}^{\mathbf{12}} = x_1x_4 \oplus x_1x_3 \oplus x_1x_2$$

que no es un monomio. ■

Otra consecuencia del teorema 2.2 es que si el grado de una función booleana de n variables es menor o igual que $n-2$, entonces la suma de elementos de su soporte es el vector nulo.

Antes de demostrar este resultado, introducimos el siguiente lema técnico.

Lema 2.1: *Supongamos que* $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ *y consideremos el vector*

$$\boldsymbol{u} = \bigoplus_{j=1}^{k} \mathbf{2}^{\boldsymbol{n-i_j}} \in \mathbb{F}_2^n$$

Si $f \in \mathcal{B}_n$ *es el monomio definido por* $\boldsymbol{u}$*; esto es,* $f(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{u}}$ *y* $1 \leq k \leq n-2$*, entonces*

$$\bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(f)} \boldsymbol{a} = \mathbf{0}.$$

Demostración: Consideremos, como en el teorema 2.2, el vector

$$\boldsymbol{v} = \bigoplus_{\substack{l=1 \\ l \notin \{i_1, i_2, \ldots, i_k\}}}^{n} \mathbf{2}^{\boldsymbol{n-l}} \in \mathbb{F}_2^n.$$

Entonces, por el teorema 2.2, tenemos que

$$\bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(f)} \boldsymbol{a} = \bigoplus_{\boldsymbol{a}\in \boldsymbol{u}\oplus S(\boldsymbol{v})} \boldsymbol{a} = \bigoplus_{\boldsymbol{b}\in S(\boldsymbol{v})} \boldsymbol{u}\oplus \bigoplus_{\boldsymbol{b}\in S(\boldsymbol{v})} \boldsymbol{b}.$$

El resultado se sigue ahora puesto que, para $\dim S(\boldsymbol{v}) = n-k \geq 2$, tenemos que $\mathrm{Card}\,(S(\boldsymbol{v})) = 2^{n-k} \geq 4$ y consecuentemente

- $\displaystyle\bigoplus_{\boldsymbol{b}\in S(\boldsymbol{v})} \boldsymbol{u} = \boldsymbol{0}$, porque cada componente es la suma de un número par de 1,
- $\displaystyle\bigoplus_{\boldsymbol{b}\in S(\boldsymbol{v})} \boldsymbol{b} = \boldsymbol{0}$, porque $S(\boldsymbol{v})$ es un 2-grupo abeliano. □

Notemos que la condición $1 \leq k \leq n-2$ del corolario anterior es necesaria. Si $k = n$, entonces $f(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{u}}$ donde $\boldsymbol{u} = \displaystyle\bigoplus_{i=1}^{n} \boldsymbol{2^{n-i}}$. Así, $\mathrm{Sop}\,(f) = \{\boldsymbol{u}\} \subseteq \mathbb{F}_2^n$ y claramente $\boldsymbol{u} \neq \boldsymbol{0}$. Por otra parte, si $k = n-1$ y $f(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{u}_j}$, para algún j con $1 \leq j \leq n$, donde $\boldsymbol{u}_j = \boldsymbol{u} \oplus \boldsymbol{2^{n-j}}$, entonces $\mathrm{Sop}\,(f) = \{\boldsymbol{u}, \boldsymbol{u}_j\}$ y, claramente,

$$\boldsymbol{u} \oplus \boldsymbol{u}_j = \boldsymbol{2^{n-j}} \neq \boldsymbol{0}.$$

Teorema 2.3: *Sea $f \in \mathcal{B}_n$. Si $\mathrm{gr}\,(f) \leq n-2$, entonces* $\displaystyle\bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(f)} \boldsymbol{a} = \boldsymbol{0}$.

Demostración: Supongamos que $f(\boldsymbol{x}) = \bigoplus_{j=1}^{m} f_j(\boldsymbol{x})$ siendo $f_j(\boldsymbol{x})$ un monomio de grado menor o igual que $n-2$, para $j = 1, 2, \ldots, m$.

Procedemos ahora por inducción sobre m. Para $m = 1$ el resultado es cierto por el lema 2.1.

Supongamos que el resultado es verdadero para $m-1$, probaremos que también es verdadero para m. En primer lugar, observemos que de la expresión (1.1) tenemos que

$$\mathrm{Sop}\,(f) = \bigtriangleup_{j=1}^{m} \mathrm{Sop}\,(f_j) = \left(\bigtriangleup_{j=1}^{m-1} \mathrm{Sop}\,(f_j)\right) \Delta\, \mathrm{Sop}\,(f_m)\,.$$

Para simplificar la notación, denotamos por

$$A = \mathrm{Sop}\,(f)\,, \quad B = \bigtriangleup_{j=1}^{m-1} \mathrm{Sop}\,(f_j) \quad \text{y} \quad C = \mathrm{Sop}\,(f_m)\,.$$

De las propiedades de la unión, intersección y diferencia simétrica de conjuntos, de la hipótesis de inducción y del lema 2.1, se deduce que

$$\mathbf{0} = \bigoplus_{\boldsymbol{b}\in B} \boldsymbol{b} = \bigoplus_{\boldsymbol{b}\in A\cap B} \boldsymbol{b} \oplus \bigoplus_{\boldsymbol{d}\in B\cap C} \boldsymbol{d} \qquad \text{y} \qquad \mathbf{0} = \bigoplus_{\boldsymbol{c}\in C} \boldsymbol{c} = \bigoplus_{\boldsymbol{c}\in A\cap C} \boldsymbol{c} \oplus \bigoplus_{\boldsymbol{e}\in B\cap C} \boldsymbol{e}.$$

Ahora, sumando las dos expresiones anteriores, obtenemos

$$\mathbf{0} = \bigoplus_{\boldsymbol{b}\in A\cap B} \boldsymbol{b} \oplus \bigoplus_{\boldsymbol{c}\in A\cap C} \boldsymbol{c} = \bigoplus_{\boldsymbol{a}\in A} \boldsymbol{a}$$

porque $\displaystyle\bigoplus_{\boldsymbol{d}\in B\cap C} \boldsymbol{d} \oplus \bigoplus_{\boldsymbol{e}\in B\cap C} \boldsymbol{e} = \mathbf{0}$ y $(A\cap B)\,\Delta(A\cap C) = A$. □

El recíproco del teorema anterior no es cierto, como podemos ver en el siguiente ejemplo.

Ejemplo 2.3: Si $f \in \mathcal{B}_3$ y $\mathrm{Sop}\,(f) = \{\mathbf{3}, \mathbf{5}, \mathbf{6}\}$. Tenemos que $\mathbf{3} \oplus \mathbf{5} \oplus \mathbf{6} = \mathbf{0}$, pero del corolario 2.2, $\mathrm{gr}\,(f) = 3$. Así que, el recíproco del teorema 2.3 no es verdadero.■

El siguiente resultado muestra que la situación descrita en el ejemplo anterior sólo puede darse cuando $\mathrm{Card}\,(\mathrm{Sop}\,(f))$ es impar, es decir, cuando $\mathrm{gr}\,(f) = n$.

Teorema 2.4: *Supongamos que* $f \in \mathcal{B}_n$ *con* $\mathrm{Card}\,(\mathrm{Sop}\,(f))$ *un número par. Si* $\displaystyle\bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(f)} \boldsymbol{a} = \mathbf{0}$, *entonces* $\mathrm{gr}\,(f) \leq n-2$.

DEMOSTRACIÓN: Como $\mathrm{Card}\,(\mathrm{Sop}\,(f))$ es par, por el corolario 2.2, tenemos que $\mathrm{gr}\,(f) \leq n-1$.

Si $\mathrm{gr}\,(f) = n-1$, entonces f tiene por lo menos un monomio de grado $n-1$. Supongamos que

$$f(\boldsymbol{x}) = \bigoplus_{j=1}^{m} g_j(\boldsymbol{x}) \oplus h(\boldsymbol{x})$$

con $g_j(\boldsymbol{x})$, para $j = 1, 2, \ldots, m$, un monomio de grado $n-1$ que no contiene a la variable x_{i_j} y $\mathrm{gr}\,(h) \leq n-2$.

Procedemos ahora como en la demostración del teorema 2.3, teniendo en cuenta que $\bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(h)} \boldsymbol{a} = \mathbf{0}$. Si $\boldsymbol{u} = \bigoplus_{i=1}^{n} \mathbf{2^{n-i}}$, entonces

$$\mathbf{0} = \bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(f)} \boldsymbol{a} = \bigoplus_{j=1}^{m} \bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(g_j)} \boldsymbol{a} \oplus \bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(h)} \boldsymbol{a} = \begin{cases} \bigoplus_{j=1}^{m} \mathbf{2^{n-i_j}}, & \text{si } m \text{ es par,} \\ \boldsymbol{u} \oplus \bigoplus_{j=1}^{m} \mathbf{2^{n-i_j}}, & \text{si } m \text{ es impar,} \end{cases}$$

lo cual es una contradicción. Por tanto, $\mathrm{gr}\,(f) \leq n-2$. □

Así, como consecuencia de los teoremas 2.3 y 2.4 tenemos el siguiente resultado.

Corolario 2.3: *Sea* $f \in \mathcal{B}_n$ *tal que* $\mathrm{Card}\,(\mathrm{Sop}\,(f))$ *es un número par. Entonces* $\mathrm{gr}\,(f) \leq n-2$ *si y sólo si* $\bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(f)} \boldsymbol{a} = \mathbf{0}$.

Notemos que si $f \in \mathcal{B}_n$ y $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = 2$, necesariamente $\bigoplus_{\boldsymbol{a}\in \mathrm{Sop}(f)} \boldsymbol{a} \neq \mathbf{0}$ y, por el corolario 2.3, $\mathrm{gr}\,(f) = n-1$. Así pues, todas las funciones booleanas de n variables cuyo soporte tenga 2 elementos, tienen grado $n-1$.

Por otro lado, si $f \in \mathcal{B}_n$ y tenemos que $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = 2^n - 2$, entonces $\mathrm{Card}\,(\mathrm{Sop}\,(1 \oplus f)) = 2$ y por tanto $\mathrm{gr}\,(1 \oplus f) = n-1$ y también $\mathrm{gr}\,(f) = n-1$. Así, todas las funciones booleanas de n variables cuyo soporte tenga $2^n - 2$ elementos, tienen también grado $n-1$. Obtendremos estos resultados también como una consecuencia del teorema 2.6 enunciado más adelante en la sección 2.4 (véase la observación 2.1 en la página 38).

El número de estas funciones es

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

Antes de continuar, veremos cómo podemos usar los resultados obtenidos hasta ahora para determinar el grado de una función booleana a partir de su soporte.

Ejemplo 2.4: Consideremos de nuevo la función booleana $f \in \mathcal{B}_4$ del ejemplo 2.1. Como $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = 10$, es decir es un número par y puesto que

$$\mathbf{2} \oplus \mathbf{4} \oplus \mathbf{5} \oplus \mathbf{7} \oplus \mathbf{8} \oplus \mathbf{9} \oplus \mathbf{11} \oplus \mathbf{12} \oplus \mathbf{13} \oplus \mathbf{15} = \mathbf{0}$$

del corolario 2.3 se deduce que $\operatorname{gr}(f) \leq 4 - 2 = 2$.

Por otra parte, como $w(f) = \operatorname{Card}(\operatorname{Sop}(f)) \neq 8$, tenemos que $f(\boldsymbol{x})$ no es equilibrada y, por tanto, $f(\boldsymbol{x})$ no es ni lineal ni afín. Además, puesto que f no es una función constante, necesariamente, $\operatorname{gr}(f) > 1$.

Consecuentemente, $\operatorname{gr}(f) = 2$. ■

2.3 Resultados principales

En esta sección, suponemos que $1 \leq k < n$. Mediante un argumento similar al seguido para obtener la expresión (2.1), podemos separar las n variables en dos conjuntos de k y $n-k$ variables, respectivamente, como describimos en el siguiente resultado.

Teorema 2.5: *Supongamos que $f \in \mathcal{B}_n$. Si $1 \leq k < n$, entonces*

$$f(\boldsymbol{y}, \boldsymbol{x}) = \bigoplus_{\boldsymbol{b} \in \mathbb{F}_2^k} \left(\bigoplus_{\boldsymbol{a} \in S(\boldsymbol{b})} f_{\boldsymbol{a}}(\boldsymbol{x}) \right) \boldsymbol{y}^{\boldsymbol{b}} \tag{2.4}$$

donde $f_{\boldsymbol{a}} \in \mathcal{B}_k$, para $\boldsymbol{a} \in \mathbb{F}_2^k$, cumple $f_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{a}, \boldsymbol{x})$. Además,

(a) $\operatorname{Sop}(f_{\boldsymbol{a}}) = \{\boldsymbol{v} \in \mathbb{F}_2^{n-k} \mid (\boldsymbol{a}, \boldsymbol{v}) \in \operatorname{Sop}(f)\}$,

(b) $\operatorname{Sop}\left(\bigoplus_{\boldsymbol{a} \in S(\boldsymbol{b})} f_{\boldsymbol{a}} \right) = \bigtriangleup_{\boldsymbol{a} \in S(\boldsymbol{b})} \operatorname{Sop}(f_{\boldsymbol{a}})$, *para todo* $\boldsymbol{b} \in \mathbb{F}_2^k$,

(c) $\operatorname{gr}(f) = \max_{\boldsymbol{b} \in \mathbb{F}_2^k} \left\{ \operatorname{gr}\left(\bigoplus_{\boldsymbol{a} \in S(\boldsymbol{b})} f_{\boldsymbol{a}} \right) + w(\boldsymbol{b}) \right\}$.

DEMOSTRACIÓN: Procederemos por inducción sobre k. Para $k = 1$ tenemos que

$$f(y_1, \boldsymbol{x}) = (1 \oplus y_1) f(0, \boldsymbol{x}) \oplus y_1 f(1, \boldsymbol{x}) = f_0(\boldsymbol{x}) y_1^0 \oplus (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x})) y_1^1$$

Ahora, como $S(0) = \{0\}$ y $S(1) = \{0, 1\}$, tenemos que la expresión (2.4) se cumple para $k = 1$.

Supongamos ahora que la expresión (2.4) se cumple para $k-1$. Sea $\boldsymbol{b} \in \mathbb{F}_2^{k-1}$ y $b_k \in \mathbb{F}_2$. Como

$$S(\boldsymbol{b},0) = \{(\boldsymbol{a},0) \mid \boldsymbol{a} \in S(b)\} \quad \text{y} \quad S(\boldsymbol{b},1) = \{(\boldsymbol{a},0),(\boldsymbol{a},1) \mid \boldsymbol{a} \in S(b)\}$$

tenemos que

$$\begin{aligned}
f(\boldsymbol{y},y_k,\boldsymbol{x}) &= \bigoplus_{\boldsymbol{b}\in\mathbb{F}_2^{k-1}} \left(\bigoplus_{\boldsymbol{a}\in S(\boldsymbol{b})} f(\boldsymbol{a},y_k,\boldsymbol{x}) \right) \boldsymbol{y}^{\boldsymbol{b}} \\
&= \bigoplus_{\boldsymbol{b}\in\mathbb{F}_2^{k-1}} \left(\bigoplus_{\boldsymbol{a}\in S(\boldsymbol{b})} \Big(f(\boldsymbol{a},0,\boldsymbol{x}) \oplus \big(f(\boldsymbol{a},0,\boldsymbol{x}) \oplus f(\boldsymbol{a},1,\boldsymbol{x}) \big) y_k \Big) \right) \boldsymbol{y}^{\boldsymbol{b}} \\
&= \bigoplus_{\boldsymbol{b}\in\mathbb{F}_2^{k-1}} \left(\bigoplus_{\boldsymbol{a}\in S(\boldsymbol{b})} f(\boldsymbol{a},0,\boldsymbol{x}) \right) \boldsymbol{y}^{\boldsymbol{b}} \\
&\quad \oplus \bigoplus_{\boldsymbol{b}\in\mathbb{F}_2^{k-1}} \left(\bigoplus_{\boldsymbol{a}\in S(\boldsymbol{b})} \Big(f(\boldsymbol{a},0,\boldsymbol{x}) \oplus f(\boldsymbol{a},1,\boldsymbol{x}) \Big) y_k \right) \boldsymbol{y}^{\boldsymbol{b}} \\
&= \bigoplus_{(\boldsymbol{b},0)\in\mathbb{F}_2^{k}} \left(\bigoplus_{(\boldsymbol{a},0)\in S(\boldsymbol{b},0)} f(\boldsymbol{a},0,\boldsymbol{x}) \right) \boldsymbol{y}^{\boldsymbol{b}} y_k^0 \\
&\quad \oplus \bigoplus_{(\boldsymbol{b},1)\in\mathbb{F}_2^{k}} \left(\bigoplus_{(\boldsymbol{a},a_k)\in S(\boldsymbol{b},1)} f(\boldsymbol{a},a_k,\boldsymbol{x}) \right) \boldsymbol{y}^{\boldsymbol{b}} y_k^1 \\
&= \bigoplus_{(\boldsymbol{b},b_k)\in\mathbb{F}_2^{k}} \left(\bigoplus_{(\boldsymbol{a},a_k)\in S(\boldsymbol{b},b_k)} f(\boldsymbol{a},a_k,\boldsymbol{x}) \right) \boldsymbol{y}^{\boldsymbol{b}} y_k^{b_k}.
\end{aligned}$$

Así pues, la expresión(2.4) se cumple para k.

Ahora, la propiedad (a) es evidente y las propiedades (b) y (c) son consecuencia de las expresiones (1.1) y (2.4), respectivamente. □

Sea $f \in \mathcal{B}_n$ y supongamos que $1 \le k < n$. Supongamos también que $\boldsymbol{a} \in \mathbb{F}_2^k$ y sea $f_{\boldsymbol{a}} \in \mathcal{B}_k$ tal que $f_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{a},\boldsymbol{x})$ para todo $\boldsymbol{x} \in \mathbb{F}_2^{n-k}$. Si $\boldsymbol{v} \in \mathbb{F}_2^{n-k}$, entonces de acuerdo con el teorema 2.5(a) tenemos que

$$\boldsymbol{v} \in \operatorname{Sop}(f_{\boldsymbol{a}}) \quad \text{si y sólo si} \quad (\boldsymbol{a},\boldsymbol{v}) \in \operatorname{Sop}(f).$$

De esta forma, si a y v son números enteros cuya expansión binaria de k y $n-k$ dígitos son los vectores $\boldsymbol{a}$ y $\boldsymbol{v}$, respectivamente, entonces la expansión binaria de n dígitos del vector $(\boldsymbol{a}, \boldsymbol{v})$ es el número entero $a \cdot 2^{n-k} + v$. Consecuentemente, la representación con números enteros de los vectores de $\mathrm{Sop}\,(f_{\boldsymbol{a}})$ son los restos de la división de la representación de números enteros de los vectores de $\mathrm{Sop}\,(f)$ cuyo cociente es a. Más adelante, usaremos este hecho para calcular los soportes de las funciones booleanas en el paso (1) de los algoritmos 2.2 y 2.3.

A partir de los resultados obtenidos hasta este momento, estamos en condiciones de introducir un algoritmo para determinar el grado de una función booleana. Previamente mostraremos un ejemplo que nos ayudará a entender el proceso de obtención del grado.

Ejemplo 2.5: Sea $f \in \mathcal{B}_5$ tal que

$$\mathrm{Sop}\,(f) = \{\mathbf{2}, \mathbf{3}, \mathbf{8}, \mathbf{9}, \mathbf{16}, \mathbf{20}, \mathbf{22}, \mathbf{23}, \mathbf{25}, \mathbf{26}, \mathbf{27}, \mathbf{28}, \mathbf{30}, \mathbf{31}\}.$$

Como $\mathrm{Card}\,(\mathrm{Sop}\,(f))$ es par y

$$\mathbf{2} \oplus \mathbf{3} \oplus \mathbf{8} \oplus \mathbf{9} \oplus \mathbf{16} \oplus \mathbf{20} \oplus \mathbf{22} \oplus \mathbf{23} \oplus \mathbf{25} \oplus \mathbf{26} \oplus \mathbf{27} \oplus \mathbf{28} \oplus \mathbf{30} \oplus \mathbf{31} = \mathbf{0}$$

del teorema 2.4, tenemos que $\mathrm{gr}\,(f) \leq 5 - 2 = 3$.

Ahora, de acuerdo con el apartado (c) del teorema 2.5, tenemos que

$$\mathrm{gr}\,(f) = \max\{\mathrm{gr}\,(f_0)\,, 1 + \mathrm{gr}\,(f_0 \oplus f_1)\}$$

con $f_0, f_1 \in \mathcal{B}_4$ tales que

$$f_0(x_2, x_3, x_4, x_5) = f(0, x_2, x_3, x_4, x_5),$$
$$f_1(x_2, x_3, x_4, x_5) = f(1, x_2, x_3, x_4, x_5)$$

y, del apartado (a) del teorema 2.5 tenemos que

$$\mathrm{Sop}\,(f_0) = \{\mathbf{2}, \mathbf{3}, \mathbf{8}, \mathbf{9}\} \quad \text{y} \quad \mathrm{Sop}\,(f_1) = \{\mathbf{0}, \mathbf{4}, \mathbf{6}, \mathbf{7}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{14}, \mathbf{15}\}. \tag{2.5}$$

Por otro lado,

$$\mathrm{Sop}\,(f_0 \oplus f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(f_1) = \{\mathbf{0}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{6}, \mathbf{7}, \mathbf{8}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{14}, \mathbf{15}\}. \tag{2.6}$$

Además, como $\mathbf{2} \oplus \mathbf{3} \oplus \mathbf{8} \oplus \mathbf{9} = \mathbf{0}$, y

$$\mathbf{0} \oplus \mathbf{2} \oplus \mathbf{3} \oplus \mathbf{4} \oplus \mathbf{6} \oplus \mathbf{7} \oplus \mathbf{8} \oplus \mathbf{10} \oplus \mathbf{11} \oplus \mathbf{12} \oplus \mathbf{14} \oplus \mathbf{15} = \mathbf{0},$$

del teorema 2.4, tenemos que

$$\operatorname{gr}(f_0) \leq 4 - 2 = 2 \quad \text{y} \quad \operatorname{gr}(f_0 \oplus f_1) \leq 4 - 2 = 2$$

y, por tanto $\operatorname{gr}(f) \leq \max\{2, 2+1\} = 3$.

Ahora, de nuevo por el apartado (c) del teorema 2.5, tenemos que

$$\operatorname{gr}(f) = \max\{\operatorname{gr}(f_{\mathbf{0}}), 1 + \operatorname{gr}(f_{\mathbf{0}} \oplus f_{\mathbf{1}}), 1 + \operatorname{gr}(f_{\mathbf{0}} \oplus f_{\mathbf{2}}), 2 + \operatorname{gr}(f_{\mathbf{0}} \oplus f_{\mathbf{1}} \oplus f_{\mathbf{2}} \oplus f_{\mathbf{3}})\}$$

con $f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{2}}, f_{\mathbf{3}} \in \mathcal{B}_3$ tales que

$$f_{\mathbf{0}}(x_3, x_4, x_5) = f(0, 0, x_3, x_4, x_5), \quad f_{\mathbf{1}}(x_3, x_4, x_5) = f(0, 1, x_3, x_4, x_5),$$
$$f_{\mathbf{2}}(x_3, x_4, x_5) = f(1, 0, x_3, x_4, x_5), \quad f_{\mathbf{3}}(x_3, x_4, x_5) = f(1, 1, x_3, x_4, x_5),$$

y del apartado (a) del teorema 2.5

$$\operatorname{Sop}(f_{\mathbf{0}}) = \{\mathbf{2}, \mathbf{3}\}, \quad \operatorname{Sop}(f_{\mathbf{1}}) = \{\mathbf{0}, \mathbf{1}\},$$
$$\operatorname{Sop}(f_{\mathbf{2}}) = \{\mathbf{0}, \mathbf{4}, \mathbf{6}, \mathbf{7}\} \quad \text{y} \quad \operatorname{Sop}(f_{\mathbf{3}}) = \{\mathbf{01}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{6}, \mathbf{7}\}$$

en cuyo caso

$$\operatorname{Sop}(f_{\mathbf{0}} \oplus f_{\mathbf{1}}) = \operatorname{Sop}(f_{\mathbf{0}}) \,\Delta\, \operatorname{Sop}(f_{\mathbf{1}}) = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\},$$
$$\operatorname{Sop}(f_{\mathbf{0}} \oplus f_{\mathbf{2}}) = \operatorname{Sop}(f_{\mathbf{0}}) \,\Delta\, \operatorname{Sop}(f_{\mathbf{2}}) = \{\mathbf{0}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{6}, \mathbf{7}\},$$
$$\operatorname{Sop}(f_{\mathbf{0}} \oplus f_{\mathbf{1}} \oplus f_{\mathbf{2}} \oplus f_{\mathbf{3}}) = \operatorname{Sop}(f_{\mathbf{0}}) \,\Delta\, \operatorname{Sop}(f_{\mathbf{1}}) \,\Delta\, \operatorname{Sop}(f_{\mathbf{2}}) \,\Delta\, \operatorname{Sop}(f_{\mathbf{3}}) = \emptyset.$$

Además, como $f_{\mathbf{0}} \in \mathcal{B}_3$ y $\operatorname{Card}(\operatorname{Sop}(f_{\mathbf{0}})) = 2$, por el comentario que sigue al corolario 2.3,

$$\operatorname{gr}(f_{\mathbf{0}}) = 3 - 1 = 2.$$

Además, puesto que

$$\mathbf{0} \oplus \mathbf{1} \oplus \mathbf{2} \oplus \mathbf{3} = \mathbf{0} \qquad \text{y} \qquad \mathbf{0} \oplus \mathbf{2} \oplus \mathbf{3} \oplus \mathbf{4} \oplus \mathbf{6} \oplus \mathbf{7} = \mathbf{4} \neq \mathbf{0}$$

del corollario 2.3, tenemos que

$$\mathrm{gr}\,(f_{\mathbf{0}} \oplus f_{\mathbf{1}}) \leq 3-2=1 \qquad \text{y} \qquad \mathrm{gr}\,(f_{\mathbf{0}} \oplus f_{\mathbf{2}}) = 3-1=2.$$

Finalmente $f_{\mathbf{0}} \oplus f_{\mathbf{1}} \oplus f_{\mathbf{2}} \oplus f_{\mathbf{3}} = 0$; esto es $\mathrm{gr}\,(f_{\mathbf{0}} \oplus f_{\mathbf{1}} \oplus f_{\mathbf{2}} \oplus f_{\mathbf{3}}) = -\infty$.

Consecuentemente, $\mathrm{gr}\,(f) = 3$. ■

Los resultados anteriores nos permiten introducir el siguiente algoritmo para determinar el grado de cualquier $f \in \mathcal{B}_n$ a partir de $\mathrm{Sop}\,(f)$.

Algoritmo 2.2: Supongamos que conocemos $\mathrm{Sop}\,(f)$ para una $f \in \mathcal{B}_n$ dada.

Este algoritmo proporciona $\mathrm{gr}\,(f)$.

(a) Si $\mathrm{Card}\,(\mathrm{Sop}\,(f))$ is impar, entonces $\mathrm{gr}\,(f) = n$. Ir al paso (f).

(b) Si $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = 2$ o $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = 2^n - 2$, entonces $\mathrm{gr}\,(f) = n-1$. Ir al paso (f).

(c) Sea $\boldsymbol{s} = \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(f)} \boldsymbol{a}$.

(d) Si $\boldsymbol{s} \neq \mathbf{0}$, entonces $\mathrm{gr}\,(f) = n-1$. Ir al paso (f).

(e) Sea $\mathrm{maxgr}\,(f) = n-2$ el valor máximo que $\mathrm{gr}\,(f)$ puede tomar y supongamos que $k = 1$.

(1) Para $\boldsymbol{b} \in \mathbb{F}_2^k$ hágase lo siguiente:

(i) Sea $g_{\boldsymbol{b}} = \bigoplus_{\boldsymbol{a} \in S(\boldsymbol{b})} f_{\boldsymbol{a}}$ y obténgase $\mathrm{Sop}\,(g_{\boldsymbol{b}})$ de acuerdo a los apartados (a) y (b) del teorema 2.5.

(ii) Si $\mathrm{Card}\,(\mathrm{Sop}\,(g_{\boldsymbol{b}}))$ es impar, entonces $\mathrm{gr}\,(g_{\boldsymbol{b}}) = n-k$. Ir al paso (vii).

(iii) Si $\mathrm{Card}\,(\mathrm{Sop}\,(g_{\boldsymbol{b}})) = 2$ o $\mathrm{Card}\,(\mathrm{Sop}\,(g_{\boldsymbol{b}})) = 2^{n-k} - 2$, entonces $\mathrm{gr}\,(g_{\boldsymbol{b}}) = n-k-1$. Ir al paso (vii).

(iv) Sea $\boldsymbol{s}_{\boldsymbol{b}} = \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(g_{\boldsymbol{b}})} \boldsymbol{a}$.

(v) Si $\boldsymbol{s}_{\boldsymbol{b}} \neq \mathbf{0}$, entonces $\mathrm{gr}\,(g_{\boldsymbol{b}}) = n-k-1$. Ir al paso (vii).

(vi) En otro caso, sea $\mathrm{maxgr}\,(g_{\boldsymbol{b}}) = n-k-2$ el valor máximo que $\mathrm{gr}\,(g_{\boldsymbol{b}})$ puede tener.

(vii) Fin del bucle

(2) Si $\mathrm{maxgr}\,(f) = \max_{\boldsymbol{b} \in \mathbb{F}_2^k} \{\mathrm{gr}\,(g_{\boldsymbol{b}}) + w(\boldsymbol{b})\}$, entonces $\mathrm{gr}\,(f) = \mathrm{maxgr}\,(f)$.

Ir al paso (f).

(3) En otro caso, hágase

$$\operatorname{maxgr}(f) = \max_{\boldsymbol{b}\in\mathbb{F}_2^k}\{\operatorname{gr}(g_{\boldsymbol{b}}) + w(\boldsymbol{b}), \operatorname{maxgr}(g_{\boldsymbol{b}}) + w(\boldsymbol{b})\},$$

incrementar k en una unidad e ir al paso (1).

(f) Fin.

A continuación comentamos algunos aspectos del algoritmo anterior.

Como mencionamos anteriormente (véase página 22), exactamente la mitad de las funciones booleanas de n variables tienen grado n y, para estas funciones, determinar su grado a partir de su soporte es inmediato.

Por otra parte (véase página 29) las funciones booleanas de n variables cuyo soporte tenga 2 o $2^n - 2$ elementos tienen grado $n-1$; el número de estas funciones es $2^n(2^n - 1)$.

Consecuentemente, si $f \in \mathcal{B}_n$ y $\operatorname{Card}(\operatorname{Sop}(f))$ es impar tenempos que, o bien $\operatorname{Card}(\operatorname{Sop}(f)) = 2$, o, si $\operatorname{Card}(\operatorname{Sop}(f)) = 2^n - 2$, podemos obtener $\operatorname{gr}(f)$ sin hacer ningún cálculo.

Para el resto de los valores de $\operatorname{Card}(\operatorname{Sop}(f))$, el número de operaciones que necesitamos para calcular $\operatorname{gr}(f)$ depende del número de veces que debamos repetir el paso (1) del algoritmo 2.2. El número de sumas binarias requeridas en esta etapa es alrededor de $\mathcal{O}(2^k n)$.

2.4 Algunas propiedades de álgebra lineal

En esta sección introducimos algunos resultados que nos permiten simplificar el proceso descrito en la sección anterior.

El resultado siguiente establece que cualquier subespacio vectorial de dimensión k de $\mathbb{F}_2^n$ (o el complementario de cualquier subespacio vectorial de dimensión k de $\mathbb{F}_2^n$) es el soporte de una función booleana de n variables con grado $n-k$.

Teorema 2.6: *Supongamos que* $1 \le k \le n$. *Si* F *o* $\mathbb{F}_2^n \setminus F$ *es un subespacio vectorial*

de dimensión k de $\mathbb{F}_2^n$, entonces existe $f \in \mathcal{B}_n$ tal que $\operatorname{gr}(f) = n-k$ *y* $F = \operatorname{Sop}(f)$.

DEMOSTRACIÓN: En primer lugar, supongamos que F es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$. Claramente, la aplicación $f : \mathbb{F}_2^n \to \mathbb{F}_2$ dada por

$$f(\boldsymbol{x}) = \begin{cases} 1, & \text{si } \boldsymbol{x} \in F, \\ 0, & \text{si } \boldsymbol{x} \notin F, \end{cases}$$

es una función booleana de n variables cuyo soporte es F.

Supongamos que $n-k+1 \leq l \leq n$ y que la ANF de $f(\boldsymbol{x})$ contiene el monomio $x_{i_1}x_{i_2}\cdots x_{i_l}$. Entonces, por el corolario 2.1(a), tenemos que

$$\operatorname{Card}\left(F \cap \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_l}}\right\}\right) \equiv 1 \pmod 2.$$

Sin embargo, como

$$\begin{aligned} &\dim\left(F \cap \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_l}}\right\}\right) \\ &\quad = \dim F + \dim \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_l}}\right\} \\ &\qquad\qquad - \dim\left(F + \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_l}}\right\}\right) \\ &\quad \geq k + l - n \geq 1, \end{aligned}$$

necesariamente

$$\begin{aligned} &\operatorname{Card}\left(F \cap \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_l}}\right\}\right) \\ &\qquad = 2^{\dim\left(F \cap \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_l}}\right\}\right)} \equiv 0 \pmod 2 \end{aligned}$$

lo que es una contradicción con la hipótesis. Entonces, la ANF de $f(\boldsymbol{x})$ no contiene ningún monomio de grado l y consecuentemente, $\operatorname{gr}(f) \leq n-k$.

Supongamos ahora que $\{\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots, \boldsymbol{b_k}\}$ es una base de F y completemos esta base con vectores de la base canónica para obtener una nueva base.

$$\left\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k, \boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_{n-k}}}\right\}$$

de $\mathbb{F}_2^n$. Claramente $F \cap \operatorname{Env}\left\{\boldsymbol{2^{n-i_1}}, \boldsymbol{2^{n-i_2}}, \ldots, \boldsymbol{2^{n-i_{n-k}}}\right\} = \{\boldsymbol{0}\}$ y, por el corolario 2.1(a), la ANF de $f(\boldsymbol{x})$ contiene al monomio $x_{i_1}x_{i_2}\cdots x_{i_{n-k}}$. Consecuentemente $\operatorname{gr}(f) \geq n-k$.

Ahora, a partir de esta desigualdad y la anterior, tenemos que $\mathrm{gr}\,(f) = n - k$.

Supongamos ahora que $G = \mathbb{F}_2^n \setminus F$ es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$. Entonces, por el apartado anterior, existe $g \in \mathcal{B}_n$ tal que $\mathrm{gr}\,(g) = n - k$ y $G = \mathrm{Sop}\,(g)$. Sea $f \in \mathcal{B}_n$ tal que $f = 1 \oplus g$. Claramente, $\mathrm{gr}\,(f) = \mathrm{gr}\,(g)$ y $\mathrm{Sop}\,(f) = \mathbb{F}_2^n \setminus \mathrm{Sop}\,(g)$; esto es, $\mathrm{gr}\,(f) = n - k$ y $F = \mathrm{Sop}\,(f)$. □

Observemos que, como consecuencia de este teorema, cualquier código binario $[n, k]$ es el soporte de una función booleana de n variables de grado $n - k$ (ver, por ejemplo, [45, 62, 69] donde los autores construyen funciones booleanas con determinadas propiedades usando códigos lineales).

El siguiente ejemplo muestra la ANF de una función booleana cuyo soporte es el código binario de Hamming $[7, 4]$.

Ejemplo 2.6: El código binario $[7, 4]$ de Hamming es el subespacio vectorial de $\mathbb{F}_2^7$, que denominaremos $\mathcal{C}$, de dimensión 4 constituido por los vectores

$$\begin{aligned}\mathcal{C} = \{&0000000, 0001110, 0010101, 0011011, 0100011,\\ &0101101, 0110110, 0111000, 1000111, 1001001,\\ &1010010, 1011100, 1100100, 1101010, 1110001, 1111111\}\\ = \{&\mathbf{0}, \mathbf{14}, \mathbf{21}, \mathbf{27}, \mathbf{35}, \mathbf{45}, \mathbf{54}, \mathbf{56}, \mathbf{71}, \mathbf{73}, \mathbf{82}, \mathbf{92}, \mathbf{100}, \mathbf{106}, \mathbf{113}, \mathbf{127}\}.\end{aligned}$$

Según el teorema 2.6, $\mathcal{C} = \mathrm{Sop}\,(f)$ para alguna $f \in \mathcal{B}_7$ tal que $\mathrm{gr}\,(f) = 3$. Usando, por ejemplo, el corolario 2.1, no es difícil obtener que

$$\begin{aligned}f(\boldsymbol{x}) = {}&\boldsymbol{x^0} \oplus \boldsymbol{x^1} \oplus \boldsymbol{x^2} \oplus \boldsymbol{x^3} \oplus \boldsymbol{x^4} \oplus \boldsymbol{x^5} \oplus \boldsymbol{x^6} \oplus \boldsymbol{x^7} \oplus \boldsymbol{x^8} \oplus \boldsymbol{x^9} \oplus \boldsymbol{x^{10}}\\ &\oplus \boldsymbol{x^{11}} \oplus \boldsymbol{x^{12}} \oplus \boldsymbol{x^{13}} \oplus \boldsymbol{x^{16}} \oplus \boldsymbol{x^{17}} \oplus \boldsymbol{x^{18}} \oplus \boldsymbol{x^{19}} \oplus \boldsymbol{x^{20}} \oplus \boldsymbol{x^{22}} \oplus \boldsymbol{x^{24}}\\ &\oplus \boldsymbol{x^{25}} \oplus \boldsymbol{x^{26}} \oplus \boldsymbol{x^{28}} \oplus \boldsymbol{x^{32}} \oplus \boldsymbol{x^{33}} \oplus \boldsymbol{x^{34}} \oplus \boldsymbol{x^{36}} \oplus \boldsymbol{x^{37}} \oplus \boldsymbol{x^{38}} \oplus \boldsymbol{x^{40}}\\ &\oplus \boldsymbol{x^{41}} \oplus \boldsymbol{x^{42}} \oplus \boldsymbol{x^{44}} \oplus \boldsymbol{x^{48}} \oplus \boldsymbol{x^{49}} \oplus \boldsymbol{x^{50}} \oplus \boldsymbol{x^{52}} \oplus \boldsymbol{x^{64}} \oplus \boldsymbol{x^{65}} \oplus \boldsymbol{x^{66}}\\ &\oplus \boldsymbol{x^{67}} \oplus \boldsymbol{x^{68}} \oplus \boldsymbol{x^{69}} \oplus \boldsymbol{x^{70}} \oplus \boldsymbol{x^{72}} \oplus \boldsymbol{x^{74}} \oplus \boldsymbol{x^{76}} \oplus \boldsymbol{x^{80}} \oplus \boldsymbol{x^{81}} \oplus \boldsymbol{x^{84}}\\ &\oplus \boldsymbol{x^{88}} \oplus \boldsymbol{x^{96}} \oplus \boldsymbol{x^{97}} \oplus \boldsymbol{x^{98}} \oplus \boldsymbol{x^{104}} \oplus \boldsymbol{x^{112}}\\ = {}&1 \oplus x_7 \oplus x_6 \oplus x_6x_7 \oplus x_5 \oplus x_5x_7 \oplus x_5x_6 \oplus x_5x_6x_7 \oplus x_4 \oplus x_4x_7\end{aligned}$$

$$\oplus\, x_4x_6 \oplus x_4x_6x_7 \oplus x_4x_5 \oplus x_4x_5x_7 \oplus x_3 \oplus x_3x_7 \oplus x_3x_6 \oplus x_3x_6x_7$$

$$\oplus\, x_3x_5 \oplus x_3x_4 \oplus x_3x_4x_7 \oplus x_3x_4x_6 \oplus x_3x_4x_5 \oplus x_2 \oplus x_2x_7$$

$$\oplus\, x_2x_6 \oplus x_2x_5 \oplus x_2x_5x_7 \oplus x_2x_5x_6 \oplus x_2x_4 \oplus x_2x_4x_7 \oplus x_2x_4x_6$$

$$\oplus\, x_2x_4x_5 \oplus x_2x_3 \oplus x_2x_3x_7 \oplus x_2x_3x_6 \oplus x_2x_3x_5 \oplus x_1 \oplus x_1x_7$$

$$\oplus\, x_1x_6 \oplus x_1x_6x_7 \oplus x_1x_5 \oplus x_1x_5x_7 \oplus x_1x_5x_6 \oplus x_1x_4$$

$$\oplus\, x_1x_4x_6 \oplus x_1x_4x_5 \oplus x_1x_3 \oplus x_1x_3x_7 \oplus x_1x_3x_5$$

$$\oplus\, x_1x_3x_4 \oplus x_1x_2 \oplus x_1x_2x_7 \oplus x_1x_2x_6 \oplus x_1x_2x_4 \oplus x_1x_2x_3. \qquad \blacksquare$$

El siguiente resultado establece que el teorema 2.6 también se verifica si en él sustituimos *subespacio vectorial* por *subespacio afín*.

Corolario 2.4: *Supongamos que* $1 \leq k \leq n$. *Si* F *o* $\mathbb{F}_2^n \setminus F$ *es un subespacio afín de dimensión* k *de* $\mathbb{F}_2^n$, *entonces existe* $f \in \mathcal{B}_n$ *tal que* $\operatorname{gr}(f) = n - k$ *y* $F = \operatorname{Sop}(f)$.

Demostración: En primer lugar, supongamos que F es un subespacio afín de dimensión k de $\mathbb{F}_2^n$. Entonces $F = \boldsymbol{a} \oplus G$, donde G es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$ y $\boldsymbol{a} \in \mathbb{F}_2^n \setminus G$. Luego, por el teorema 2.6, existe $g \in \mathcal{B}_n$ tal que $\operatorname{gr}(g) = n - k$ y $G = \operatorname{Sop}(g)$.

Ahora, sea $f \in \mathcal{B}_n$ tal que $f(\boldsymbol{x}) = g(\boldsymbol{x} \oplus \boldsymbol{a})$ para todo $\boldsymbol{x} \in \mathbb{F}_2^n$. Es evidente que $\operatorname{gr}(f) = n - k$ y $\operatorname{Sop}(f) = \boldsymbol{a} \oplus \operatorname{Sop}(g) = \boldsymbol{a} \oplus G = F$.

Supongamos ahora que $G = \mathbb{F}_2^n \setminus F$ es un subespacio afín de dimensión k de $\mathbb{F}_2^n$. Entonces, según el apartado anterior, existe $g \in \mathcal{B}_n$ tal que $\operatorname{gr}(g) = n - k$ y $G = \operatorname{Sop}(g)$. Sea $f \in \mathcal{B}_n$ tal que $f = 1 \oplus g$. Claramente $\operatorname{gr}(f) = \operatorname{gr}(g)$ y $\operatorname{Sop}(f) = \mathbb{F}_2^n \setminus \operatorname{Sop}(g)$; es decir, $\operatorname{gr}(f) = n - k$ y $F = \operatorname{Sop}(f)$. $\square$

Como consecuencia inmediata del teorema 2.6 y el corolario 2.4 tenemos la observación siguiente.

Observación 2.1: Supongamos que $f \in \mathcal{B}_n$.

(a) Si $\operatorname{Card}(\operatorname{Sop}(f)) = 2$ y $\mathbf{0} \in \operatorname{Sop}(f)$ (respectivamente, $\mathbf{0} \notin \operatorname{Sop}(f)$), entonces $\operatorname{Sop}(f)$ es un subespacio vectorial (respectivamente, subespacio afín) de dimensión 1 de $\mathbb{F}_2^n$ y, consecuentemente, $\operatorname{gr}(f) = n - 1$.

(b) Si $\mathrm{Card}\,(\mathrm{Sop}\,(f)) = 2^n - 2$ y $\mathbf{0} \notin \mathrm{Sop}\,(f)$ (respectivamente, $\mathbf{0} \in \mathrm{Sop}\,(f)$), entonces $\mathbb{F}_2^n \setminus \mathrm{Sop}\,(f)$ es un subespacio vectorial (respectivamente, subespacio afín) de dimensión 1 de $\mathbb{F}_2^n$ y consecuentemente $\mathrm{gr}\,(f) = n - 1$. ■

Recordemos que obtuvimos estos resultados en la sección 2.3 como consecuencia del corolario 2.3.

El recíproco del teorema 2.6 no es cierto en general, tal y como podemos ver más adelante en el ejemplo 2.7. Sin embargo, si $k = n$, entonces $F = \mathbb{F}_2^n$ es el soporte de la función constante $f(\boldsymbol{x}) = 1$ cuyo grado es 0. Además, si $k = n - 1$, entonces el recíproco del teorema 2.6 también se verifica, como podemos ver en el siguiente resultado.

Teorema 2.7: *Supongamos que $F \subseteq \mathbb{F}_2^n$. Entonces F o $\mathbb{F}_2^n \setminus F$ es un subespacio vectorial de dimensión $n-1$ de $\mathbb{F}_2^n$ si y sólo si existe $f \in \mathcal{B}_n$ tal que $\mathrm{gr}\,(f) = 1$ y $F = \mathrm{Sop}\,(f)$.*

Demostración: Si F o $\mathbb{F}_2^n \setminus F$ es un subespacio vectotial de dimensión $n-1$ de $\mathbb{F}_2^n$, por el teorema 2.6, existe $f \in \mathcal{B}_n$ tal que $\mathrm{gr}\,(f) = 1$ y $F = \mathrm{Sop}\,(f)$.

A la inversa, sea $f \in \mathcal{B}_n$ tal que $\mathrm{gr}\,(f) = 1$ y $F = \mathrm{Sop}\,(f)$. Por un lado

$$f(\boldsymbol{x}) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$$

para algunos $a_0 \in \mathbb{F}_2$ y $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ y claramente

$$S = \{(u_1, u_2, \ldots, u_n) \in \mathbb{F}_2^n \mid a_1 u_1 \oplus a_2 u_2 \oplus \cdots \oplus a_n u_n = 0\}$$

es un subespacio vectorial de dimensión $(n-1)$ de $\mathbb{F}_2^n$. Por otro lado, resulta fácil ver que $S = F$, si $a_0 = 1$, y $S = \mathbb{F}_2^n \setminus F$, si $a_0 = 0$. □

También es posible obtener un resultado similar al del teorema 2.7 considerando subespacios afines. Sin embargo, en este caso la demostración se deduce del hecho de que si F es un subespacio vectorial de dimensión $n-1$ de $\mathbb{F}_2^n$, entonces

$$\mathbb{F}_2^n \setminus F = \boldsymbol{a} \oplus F \quad \text{para todo } \boldsymbol{a} \in \mathbb{F}_2^n \setminus F$$

es un subespacio afín de dimensión $n-1$ de $\mathbb{F}_2^n$.

Corolario 2.5: *Supongamos que* $F \subseteq \mathbb{F}_2^n$. *Entonces* F *o* $\mathbb{F}_2^n \setminus F$ *es un subespacio afín de dimensión* $n-1$ *de* $\mathbb{F}_2^n$ *si y sólo si existe* $f \in \mathcal{B}_n$ *tal que* $\operatorname{gr}(f) = 1$ *y* $F = \operatorname{Sop}(f)$.

Como en general $2^n - 2^k = 2^k(2^{n-k} - 1)$ no es una potencia de 2, este resultado puede no ser cierto si $\dim F = k \neq n-1$.

El siguiente ejemplo muestra cómo podemos usar los resultados anteriores para mejorar el proceso descrito en la sección previa.

Ejemplo 2.7: Supongamos que $f \in \mathcal{B}_5$ la función booleana del ejemplo 2.5. Notemos que $\operatorname{Card}(\operatorname{Sop}(f)) = 14$ y $\operatorname{Card}(\mathbb{F}_2^5 \setminus \operatorname{Sop}(f)) = 18$, así que ni $\operatorname{Sop}(f)$ ni $\mathbb{F}_2^5 \setminus \operatorname{Sop}(f)$ pueden ser ni un subespacio vectorial ni un subespacio afín de $\mathbb{F}_2^5$.

Tras algunos cálculos, obtuvimos en el ejemplo 2.5 que

$$\operatorname{gr}(f) = \max\{\operatorname{gr}(f_0), 1 + \operatorname{gr}(f_0 \oplus f_1)\}$$

con $f_0, f_1 \in \mathcal{B}_4$ dadas por

$$f_0(x_2, x_3, x_4, x_5) = f(0, x_2, x_3, x_4, x_5),$$
$$f_1(x_2, x_3, x_4, x_5) = f(1, x_2, x_3, x_4, x_5)$$

Es fácil comprobar (véase la expresión (2.5)) que ninguno de los conjuntos $\operatorname{Sop}(f_0)$, $\mathbb{F}_2^4 \setminus \operatorname{Sop}(f_0)$, $\operatorname{Sop}(f_0 \oplus f_1)$ y $\mathbb{F}_2^4 \setminus \operatorname{Sop}(f_0 \oplus f_1)$ pueden ser subespacios vectoriales de $\mathbb{F}_2^4$. Sin embargo

$$\operatorname{Sop}(f_0) = \mathbf{2} \oplus \{\mathbf{0}, \mathbf{1}, \mathbf{10}, \mathbf{11}\} = \mathbf{2} \oplus \operatorname{Env}\{\mathbf{1}, \mathbf{10}\},$$
$$\mathbb{F}_2^4 \setminus \operatorname{Sop}(f_0 \oplus f_1) = \{\mathbf{1}, \mathbf{5}, \mathbf{9}, \mathbf{13}\} = \mathbf{1} \oplus \{\mathbf{0}, \mathbf{4}, \mathbf{8}, \mathbf{12}\} = \mathbf{1} \oplus \operatorname{Env}\{\mathbf{4}, \mathbf{8}\}$$

son subespacios afines de dimensión 2. Así que, por el corolario 2.4,

$$\operatorname{gr}(f_0) = 4 - 2 = 2 \quad \text{y} \quad \operatorname{gr}(f_0 \oplus f_1) = 4 - 2 = 2$$

y, por tanto $\operatorname{gr}(f) = \max\{2, 2+1\} = 3$. Recordemos que en el ejemplo 2.5 obtuvimos que

$$\operatorname{gr}(f_0 \oplus f_1) \leq 4 - 2 = 2$$

y, por tanto $\operatorname{gr}(f) \leq \max\{2, 2+1\} = 3$. ■

Una forma de comprobar si un subconjunto S con 2^k elementos es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$ consiste en escribir la matriz $M_{2^k \times n}$ cuyas filas son los vectores de S y calcular su forma escalonada reducida (de hecho, es suficiente calcular una matriz escalonada que sea equivalente a M). Si el rango de esta matriz es k, entonces S es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$. No obstante, este método no es muy eficiente, así que necesitamos un método rápido para comprobar si un conjunto dado S, cuyo número de elementos sea una potencia de 2, es un subespacio vectorial o afín de $\mathbb{F}_2^n$. El siguiente resultado proporciona las bases para un procedimiento que realice de modo eficiente tal verificación.

Teorema 2.8: *Supongamos que E_k es un subespacio vectorial de dimensión k de $\mathbb{F}_2^n$ y que $\boldsymbol{a}_{k+1} \in \mathbb{F}_2^n \setminus E_k$, entonces $E_{k+1} = E_k \cup (\boldsymbol{a}_{k+1} \oplus E_k)$ es un subespacio vectorial de dimensión $k+1$ de $\mathbb{F}_2^n$.*

DEMOSTRACIÓN: Como E_k es un subespacio vectorial, tenemos que $\mathbf{0} \in E_k \subseteq E_{k+1}$.

Ahora, supongamos que $\boldsymbol{x}, \boldsymbol{y} \in E_{k+1}$ y consideremos los siguientes casos:

- $\boldsymbol{x}, \boldsymbol{y} \in E_k$. Entonces $\boldsymbol{x} \oplus \boldsymbol{y} \in E_k \subseteq E_{k+1}$ por ser E_k un subespacio vectorial.
- $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{a}_{k+1} \oplus E_k$. Entonces, $\boldsymbol{x} = \boldsymbol{a}_{k+1} \oplus \boldsymbol{u}$ e $\boldsymbol{y} = \boldsymbol{a}_{k+1} \oplus \boldsymbol{v}$ con $\boldsymbol{u}, \boldsymbol{v} \in E_k$. Ahora, $\boldsymbol{x} \oplus \boldsymbol{y} = \boldsymbol{u} \oplus \boldsymbol{v} \in E_k \subseteq E_{k+1}$.
- $\boldsymbol{x} \in E_k$ e $\boldsymbol{y} \in \boldsymbol{a}_{k+1} \oplus E_k$. Entonces, $\boldsymbol{y} = \boldsymbol{a}_{k+1} \oplus \boldsymbol{v}$ con $\boldsymbol{v} \in E_k$ y por tanto $\boldsymbol{x} \oplus \boldsymbol{y} = \boldsymbol{a}_{k+1} \oplus \boldsymbol{x} \oplus \boldsymbol{v} \in \boldsymbol{a}_{k+1} \oplus E_k \subseteq E_{k+1}$.
- $\boldsymbol{x} \in \boldsymbol{a}_{k+1} \oplus E_k$ y $\boldsymbol{y} \in E_k$. Este caso es análogo al anterior.

Así, en cualquier caso, tenemos que $\boldsymbol{x} \oplus \boldsymbol{y} \in E_{k+1}$.

Por consiguiente, E_{k+1} es un subespacio vectorial de $\mathbb{F}_2^n$.

Además, si $\boldsymbol{x} \in E_k \cap (\boldsymbol{a}_{k+1} \oplus E_k)$, entonces $\boldsymbol{x} = \boldsymbol{a}_{k+1} \oplus \boldsymbol{u}$ con $\boldsymbol{u} \in E_k$ y por tanto $\boldsymbol{a}_{k+1} = \boldsymbol{x} \oplus \boldsymbol{u} \in E_k$ lo cual es una contradicción. Así que, $E_k \cap (\boldsymbol{a}_{k+1} \oplus E_k) = \emptyset$.

Por último, como $\operatorname{Card}(E_k) = 2^k$ tenemos que $\operatorname{Card}(E_{k+1}) = 2 \operatorname{Card}(E_k) = 2^{k+1}$ y por consiguiente $\dim E_{k+1} = 2^{k+1}$. □

Como consecuencia inmediata de este resultado tenemos el siguiente corolario.

Corolario 2.6: *Supongamos que $1 < k \leq n$ y sea E_k un subconjunto de $\mathbb{F}_2^n$ tal que $\operatorname{Card}(E_k) = 2^k$. Supongamos también que para $i = k-1, k-2, \ldots, 2, 1$, existe un*

conjunto E_i de $\mathbb{F}_2^n$ y un elemento $\boldsymbol{a}_{i+1} \in \mathbb{F}_2^n \setminus E_i$ tal que

$$E_{i+1} = E_i \cup (\boldsymbol{a}_{i+1} \oplus E_i) \quad y \quad E_i \cap (\boldsymbol{a}_{i+1} \oplus E_i) = \emptyset.$$

Si $E_1 = \{\mathbf{0}, \boldsymbol{a}_1\}$ con $\boldsymbol{a}_1 \neq \mathbf{0}$, entonces E_i, para $i = 1, 2, \ldots, k$, es un subespacio vectorial de dimensión i de $\mathbb{F}_2^n$ y $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i\}$ es una base de E_i.

DEMOSTRACIÓN: El resultado se sigue del teorema 2.8 y del hecho de que E_1 es un subespacio vectorial de dimensión 1 de $\mathbb{F}_2^n$.

Consideremos ahora que

$$\alpha_1\boldsymbol{a}_1 + \alpha_2\boldsymbol{a}_2 + \cdots + \alpha_{i-1}\boldsymbol{a}_{i-1} + \alpha_i\boldsymbol{a}_i = \mathbf{0}$$

para algún $\alpha_1, \alpha_2, \ldots, \alpha_i \in \mathbb{F}_2$. Si $\alpha_i \neq 0$, entonces

$$\boldsymbol{a}_i = \alpha_1\boldsymbol{a}_1 + \alpha_2\boldsymbol{a}_2 + \cdots + \alpha_{i-1}\boldsymbol{a}_{i-1},$$

Por tanto

$$\boldsymbol{a}_i \in E_{i-1} \cap E_i = E_{i-1} \cap (E_{i-1} \cup (\boldsymbol{a}_i \oplus E_{i-1})) = \emptyset$$

lo cual es una contradicción. Así que $\alpha_i = 0$.

Siguiendo un argumento similar, obtenemos que $\alpha_{i-1} = \cdots = \alpha_2 = \alpha_1 = 0$.

Así que, los vectores $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_i$ son linealmente independientes y, consecuentemente, constituyen una base de E_i. □

La siguiente observación será útil para introducir nuestro próximo algoritmo. Si $\boldsymbol{u} \in \mathbb{F}_2^n$, denotamos la i-ésima componente de $\boldsymbol{u}$ por $\boldsymbol{u}(i)$.

Observación 2.2: Sea $1 < l \leq n$ y supongamos que los vectores del conjunto

$$S = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2^{l-1}}, \boldsymbol{u}_{2^{l-1}+1}, \boldsymbol{u}_{2^{l-1}+2}, \ldots, \boldsymbol{u}_{2^l}\}$$

de $\mathbb{F}_2^n$ se encuentran en orden lexicográfico descendente con $\boldsymbol{u}_{2^l} = \mathbf{0}$.

Para $j = 1, 2, \ldots, 2^l$, sea $1 \leq p \leq n$ tal que $\boldsymbol{u}_j(i) = 0$ para $i = 1, 2, \ldots, p-1$.

(a) Supongamos que existe un número entero positivo r tal que

$$\boldsymbol{u}_j(p) = \begin{cases} 1, & \text{para } j = 1, 2, \ldots, 2^{l-1}, 2^{l-1}+1, 2^{l-1}+2, \ldots, 2^{l-1}+r, \\ 0, & \text{para } j = 2^{l-1}+r+1, 2^{l-1}+r+2, \ldots, 2^l. \end{cases}$$

Ahora, para $j = 1, 2, \ldots, 2^{l-1}, 2^{l-1}+1, 2^{l-1}+2, \ldots, 2^{l-1}+r$, consideramos el vector $\boldsymbol{v}_j = \boldsymbol{u}_1 + \boldsymbol{u}_j$. Como $\boldsymbol{v}_j(p) = 0$, al menos uno de estos vectores no está en S. Por consiguiente, S no es un subespacio vectorial de $\mathbb{F}_2^n$.

(b) Supongamos que existe un número entero positivo s tal que

$$\boldsymbol{u}_j(p) = \begin{cases} 1, & \text{para } j = 1, 2, \ldots, 2^{l-1} - s, \\ 0, & \text{para } j = 2^{l-1} - s + 1, 2^{l-1} - s + 2, \ldots, 2^{l-1}, \ldots, 2^l \end{cases}$$

y consideremos, para $j = 1, 2, \ldots, 2^{l-1} - s$, el vector $\boldsymbol{w}_j = \boldsymbol{u}_1 + \boldsymbol{u}_j$. Puesto que $\boldsymbol{w}_j(p) = 1$, al menos uno de estos vectores no está en S. Por consiguiente, S no es un subespacio vectorial de $\mathbb{F}_2^n$.

(c) Supongamos que

$$\boldsymbol{u}_j(p) = \begin{cases} 1, & \text{para } j = 1, 2, \ldots, 2^{l-1}, \\ 0, & \text{para } j = 2^{l-1} + 1, 2^{l-1} + 2, \ldots, 2^l. \end{cases}$$

Ahora, para $j = 1, 2, \ldots, 2^{l-1}$, consideremos el vector $\boldsymbol{z}_j = \boldsymbol{u}_j + \boldsymbol{u}_{2^{l-1}}$. Puesto que $\boldsymbol{z}_j(p) = 0$, si

$$\boldsymbol{z}_j \notin \{\boldsymbol{u}_{2^{l-1}+1}, \boldsymbol{u}_{2^{l-1}+2}, \ldots, \boldsymbol{u}_{2^l}\}$$

entonces S no es un subespacio vectorial de $\mathbb{F}_2^n$. ■

Como consecuencia del corolario 2.6 y de la observación 2.2 tenemos el siguiente algoritmo que nos permite determinar si un subconjunto dado S de $\mathbb{F}_2^n$, tal que Card (S) es una potencia de 2 y $\mathbf{0} \in S$, es un subespacio vectorial. Antes de proceder, necesitamos la siguiente notación para una matriz M:

- $M(r, c)$ denota el elemento que está en la fila r y en la columna c,
- $M(r, :)$ denota la r-ésima fila de M,
- $M(:, c)$ denota la columna c-ésima de M,
- $M(r_1 : r_2, c)$, con $r_1 < r_2$, denota la submatriz de M formada por los elementos en las filas $r_1, r_1 + 1, \ldots, r_2$ y columna c,
- $M(r_1 : r_2, :)$, con $r_1 < r_2$, denota la submatriz de M formada por los elementos en las filas $r_1, r_1 + 1, \ldots, r_2$ y todas las columnas.

Algoritmo 2.3: Supongamos que S es un subconjunto de $\mathbb{F}_2^n$ tal que $\text{Card}\,(S) = 2^k$, con $1 < k < n$; supongamos también que $\mathbf{0} \in S$ y consideremos la matriz $M_{2^k \times n}$ cuyas filas son los vectores de S en orden lexicográfico descendente (esto quiere decir que la última fila de M tiene todos sus elementos iguales a cero). Supongamos que $l = k$.

(a) Sea c_l el primer índice de la columna de la primera fila de M con $M(1, c_l) = 1$.
(b) Si $w(M(:, c_l)) \neq 2^{l-1}$, entonces S (véase la observación 2.2(a)) no es un subespacio vectorial. Ir al paso (h).
(c) En otro caso, eso significa que $M(1 : 2^{l-1}, c_l)$ y $M(2^{l-1} + 1 : 2^l, c_l)$ son las columnas con todos sus elementos iguales a 1 y 0 respectivamente. Sea N la matriz que obtenemos cuando sumamos la fila $M(2^{l-1}, :)$ a cada una de las filas de $M(1 : 2^{l-1}, :)$.
(d) Si $N \neq M(2^{l-1} + 1 : 2^l, :)$, entonces S no es un subespacio vectorial (véase observación 2.2(c)). Ir al paso (h).
(e) En otro caso, disminuir, l en una unidad.
(f) Si $l = 1$, entonces S es un subespacio vectorial de dimensión k (véase corolario 2.6). Ir al paso (h).
(g) En otro caso, hacer $M = N$ e ir al paso (a).
(h) Fin.

Notemos que si el algoritmo anterior acaba mostrando que S es un subespacio vectorial, entonces de acuerdo con el corolario 2.6, los vectores correspondientes a las filas

$$1, 2^k + 1, 2^k + 2^{k-1} + 1, \ldots, 2^k + 2^{k-1} + \cdots + 2 + 1$$

constituyen una base de S.

Supongamos ahora que S es un subconjunto de $\mathbb{F}_2^n$ tal que $\text{Card}\,(S) = 2^k$, con $1 < k < n$. Si $\mathbf{0} \notin S$, entonces $\mathbf{0} \in \boldsymbol{a} \oplus S$ para todo $\boldsymbol{a} \in S$. Por tanto, podemos aplicar el algoritmo 2.3 a $\boldsymbol{a} \oplus S$ para algún $\boldsymbol{a} \in S$, para comprobar si S es un subespacio afín de dimensión k de $\mathbb{F}_2^n$.

Los siguientes ejemplos nos ayudarán a comprender este algoritmo.

Ejemplo 2.8: Consideremos el subconjunto

$$S = \{\mathbf{9}, \mathbf{10}, \mathbf{16}, \mathbf{19}, \mathbf{45}, \mathbf{46}, \mathbf{52}, \mathbf{55}, \mathbf{141}, \mathbf{142}, \mathbf{148}, \mathbf{151}, \mathbf{169}, \mathbf{170}, \mathbf{176}, \mathbf{179}\}$$

de $\mathbb{F}_2^8$, con $\mathrm{Card}\,(S) = 2^4$.

Dado que $\mathbf{0} \notin S$, tenemos que S no es un subespacio vectorial de $\mathbb{F}_2^8$. No es difícil comprobar que

$$\mathbf{9} \oplus S = \{\mathbf{0}, \mathbf{3}, \mathbf{25}, \mathbf{26}, \mathbf{36}, \mathbf{39}, \mathbf{61}, \mathbf{62}, \mathbf{132}, \mathbf{135}, \mathbf{157}, \mathbf{158}, \mathbf{160}, \mathbf{163}, \mathbf{185}, \mathbf{186}\}.$$

Sea M la matriz $2^4 \times 8$ cuyas filas son los vectores de S en orden lexicográfico descendente; esto es,

$$M = \begin{bmatrix} \mathbf{186} \\ \mathbf{185} \\ \mathbf{163} \\ \mathbf{160} \\ \mathbf{158} \\ \mathbf{157} \\ \mathbf{135} \\ \mathbf{132} \\ \mathbf{62} \\ \mathbf{61} \\ \mathbf{39} \\ \mathbf{36} \\ \mathbf{26} \\ \mathbf{25} \\ \mathbf{3} \\ \mathbf{0} \end{bmatrix} = \left[\begin{array}{cccccccc} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Sea $l = 4$. Como $M(1,1) = 1$, tenemos que $c_4 = 1$. También, tenemos que $w(M(:,1)) = 2^3$.

Sea N la matriz que obtenemos cuando sumamos la fila $M(2^3,:)$ a cada una de

las filas de $M(1:2^3,:)$; entonces

$$N = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Claramente $N = M(2^3+1:2^4,:)$.

Ahora, disminuimos l en una unidad (esto es $l=3$) y tomamos $M=N$; es decir,

$$M = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Como $M(1,3)=1$, tenemos que $c_3 = 3$. También, tenemos que $w(M(:,3)) = 2^2$.

Sea N la matriz que obtenemos cuando sumamos la fila $M(2^2,:)$ a cada una de las filas de $M(1:2^2,:)$; entonces

$$N = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Claramente $N = M(2^2+1:2^3,:)$.

Ahora, disminuimos l en una unidad (es decir $l = 2$) y tomamos $M = N$; es decir,

$$M = \left[\begin{array}{cccccccc} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Como $M(1,4) = 1$, tenemos que $c_2 = 4$. También, tenemos que $w(M(:,4)) = 2^1$.

Sea N la matriz que obtenemos cuando sumamos la fila $M(2^1,:)$ a cada una de las columnas de $M(1:2^1,:)$; entonces

$$N = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Claramente $N = M(2^1+1:2^2,:)$.

Ahora, disminuimos l en una unidad (con lo que $l = 1$). Al ser $l = 1$, concluimos que $\mathbf{9} \oplus S$ es un subespacio vectorial de dimensión 4 de $\mathbb{F}_2^8$ y, por consiguiente S es un subespacio afín de dimensión 4 de $\mathbb{F}_2^8$. ■

Ejemplo 2.9: Consideremos el subconjunto

$$S = \{\mathbf{0}, \mathbf{31}, \mathbf{92}, \mathbf{126}, \mathbf{141}, \mathbf{175}, \mathbf{209}, \mathbf{243}\}$$

de $\mathbb{F}_2^8$. Claramente $\mathrm{Card}\,(S) = 2^3$.

Sea M la matriz $2^3 \times 8$ cuyas columnas son los vectores de S en orden lexicográfico descendente; esto es,

$$M = \begin{bmatrix} \mathbf{243} \\ \mathbf{209} \\ \mathbf{175} \\ \mathbf{141} \\ \mathbf{126} \\ \mathbf{92} \\ \mathbf{31} \\ \mathbf{0} \end{bmatrix} = \left[\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Si procedemos como en el ejemplo anterior, obtenemos que

$$N = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Como $N \neq M(2^2+1:2^3,:)$, concluimos que S no es un subespacio vectorial de $\mathbb{F}_2^8$. ■

Por último, modificamos el algoritmo 2.2 para comprobar si el soporte (con cardinal una potencia de 2) de la función que estamos considerando es un subespacio vectorial o un subespacio afín.

Algoritmo 2.4: Supongamos que conocemos $\mathrm{Sop}(f)$ para una $f \in \mathcal{B}_n$ dada.

Este algoritmo proporciona $\mathrm{gr}(f)$.

(a) Si $\mathrm{Card}(\mathrm{Sop}(f))$ es impar, entonces $\mathrm{gr}(f) = n$. Ir al paso (g).

(b) Si $\mathrm{Card}(\mathrm{Sop}(f)) = 2$ o $\mathrm{Card}(\mathrm{Sop}(f)) = 2^n - 2$, entonces $\mathrm{gr}(f) = n-1$. Ir al paso (g).

(c) Si $\mathrm{Card}(\mathrm{Sop}(f))$ es una potencia de 2, por ejemplo 2^r (con $r \geq 2$), aplicar el algoritmo 2.3 para comprobar si $\mathrm{Sop}(f)$ es un subespacio vectorial o afín. Si es éste el caso, entonces $\mathrm{gr}(f) = n - r$. Ir al paso (g).

(d) Sea $\boldsymbol{s} = \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(f)} \boldsymbol{a}$.

(e) Si $\boldsymbol{s} \neq \mathbf{0}$, entonces $\mathrm{gr}(f) = n-1$. Ir al paso (g).

(f) Sea $\mathrm{maxgr}(f) = n-2$ el valor máximo que $\mathrm{gr}(f)$ puede tomar y supongamos que $k = 1$.

(1) Para $\boldsymbol{b} \in \mathbb{F}_2^k$ hacer lo siguiente:

(i) Sea $g_{\boldsymbol{b}} = \bigoplus_{\boldsymbol{a} \in S(\boldsymbol{b})} f_{\boldsymbol{a}}$ y obtener $\mathrm{Sop}(g_{\boldsymbol{b}})$ de acuerdo a los apartados (a) y (b) del Teorema 2.5.

(ii) Si $\mathrm{Card}(\mathrm{Sop}(g_{\boldsymbol{b}}))$ es impar, entonces $\mathrm{gr}(g_{\boldsymbol{b}}) = n-k$. Ir al paso (viii).

(iii) Si $\mathrm{Card}(\mathrm{Sop}(g_{\boldsymbol{b}})) = 2$ o $\mathrm{Card}(\mathrm{Sop}(g_{\boldsymbol{b}})) = 2^{n-k}-2$, entonces $\mathrm{gr}(f) = n-k-1$. Ir al paso (viii).

(iv) Si $\mathrm{Card}\,(\mathrm{Sop}\,(g_{\boldsymbol{b}}))$ es una potencia de 2, por ejemplo 2^r (con $r \geq 2$), aplicar el algoritmo 2.3 para comprobar si $\mathrm{Sop}\,(g_{\boldsymbol{b}})$ es un subespacio vectorial o afín. Si es éste el caso, entonces $\mathrm{gr}\,(g_{\boldsymbol{b}}) = n - k - r$. Ir al paso (viii).

(v) Sea $\boldsymbol{s_b} = \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(g_{\boldsymbol{b}})} \boldsymbol{a}$.

(vi) Si $\boldsymbol{s_b} \neq \boldsymbol{0}$, entonces $\mathrm{gr}\,(g_{\boldsymbol{b}}) = n - k - 1$. Ir al paso (viii).

(vii) Por otra parte, sea $\mathrm{maxgr}\,(g_{\boldsymbol{b}}) = n - k - 2$ el valor máximo que $\mathrm{gr}\,(g_{\boldsymbol{b}})$ puede tomar.

(viii) Fin del paso.

(2) Si $\mathrm{maxgr}\,(f) = \max_{\boldsymbol{b} \in \mathbb{F}_2^k} \{\mathrm{gr}\,(g_{\boldsymbol{b}}) + w(\boldsymbol{b})\}$, entonces $\mathrm{gr}\,(f) = \mathrm{maxgr}\,(f)$. Ir al paso (g).

(3) En otro caso, hacer

$$\mathrm{maxgr}\,(f) = \max_{\boldsymbol{b} \in \mathbb{F}_2^k} \{\mathrm{gr}\,(g_{\boldsymbol{b}}) + w(\boldsymbol{b}), \mathrm{maxgr}\,(g_{\boldsymbol{b}}) + w(\boldsymbol{b})\},$$

Incrementar k en una unidad e ir al paso (1).

(g) Fin.

2.5 Resultados numéricos

Para un n dado, el número de funciones booleanas de n variables es 2^{2^n}. Para valores diferentes de n (con $8 \leq n \leq 14$) en un ordenador personal estándar obtuvimos, aleatoriamente, 1000 subconjuntos de $\mathbb{F}_2^n$; es decir, 1000 soportes de funciones booleanas de n variables. Para estos soportes determinamos el grado de la función booleana correspondiente calculando la ANF utilizando la expresión (2.1) y empleando los algoritmos 2.1, 2.2 y 2.4. Las columnas 2, 3, 4 y 5 de la tabla 2.1 muestran el tiempo medio (en segundos) que obtuvimos en cada caso.

Para $n = 13, 14$ no tenemos suficiente memoria en nuestro ordenador. En general, el algoritmo 2.2 resulta más rápido que el algoritmo 2.4. No obstante, si los soportes considerados son subespacios vectoriales, entonces el algoritmo 2.4 resulta mucho más rápido que el algoritmo 2.2. La tabla 2.2 muestra el tiempo medio (en segundos)

n	ANF	Algoritmo 2.1	Algoritmo 2.2	Algoritmo 2.4
8	0,0075	0,0748	0,0033	0,0038
9	0,0229	0,1489	0,0059	0,0069
10	0,0696	0,3564	0,0132	0,0159
11	0,2151	0,8105	0,0278	0,0348
12	0,7766	1,7892	0,0527	0,0767
13	− − −	5,0492	0,1172	0,2177
14	− − −	9,4359	0,2360	0,5370

Tabla 2.1: *Tiempos obtenidos en el cálculo del grado de una función booleana de n variables desde su soporte*

n	Algoritmo 2.2	Algoritmo 2.4
8	0,0036	0,0004
9	0,0069	0,0007
10	0,0151	0,0015
11	0,0324	0,0036
12	0,0714	0,0087
13	0,1761	0,0196
14	0,4998	0,0542

Tabla 2.2: *Tiempos obtenidos en el cálculo del grado de una función booleana de n variables cuyo soporte es un subespacio vectorial*

necesario para calcular el grado de las funciones booleanas correspondientes a 1000 subespacios vectoriales de $\mathbb{F}_2^n$ para diferentes valores de n.

2.6 Conclusiones

En este capítulo hemos presentado algunas propiedades del soporte de una función booleana que nos permiten obtener los diferentes términos de su forma normal algebraica. En particular, cuando conocemos el soporte de una función booleana, podemos obtener su grado sin necesidad de calcular su forma normal algebraica.

Por ejemplo, si $f(\boldsymbol{x})$ es una función booleana de n variables, demostramos que el grado de f es n si y sólo si el soporte de f tiene un número par de elementos; observamos que es muy fácil comprobar esta propiedad; de hecho, la mitad de las funciones booleanas tienen grado n. Además, si el soporte de una función booleana de n variables es un subespacio vectorial o afín de $\mathbb{F}_2^n$, entonces obtenemos que su grado es $n - k$.

Como consecuencia de estas propiedades, también obtenemos diferentes algoritmos para calcular el grado de una función booleana a partir de su soporte, sin necesidad de calcular su ANF.

Capítulo 3

Construcción de funciones bent de $2k$ variables a partir de una base de $\mathbb{F}_2^{2k}$

3.1 Introducción

En este capítulo, a partir de una base de $\mathbb{F}_2^{2k}$, definimos algunos conjuntos en $\mathbb{F}_2^{2k}$ que tienen la propiedad de ser los soportes de *funciones de no linealidad perfecta* o *funciones bent* de $2k$ variables. En la sección 3.2 detallamos un procedimiento para obtener iterativamente dichos conjuntos de modo efectivo. En la sección 3.3 obtenemos algunos resultados con el propósito de contar cuántas *funciones de no linealidad perfecta* podemos construir usando el método introducido en la sección 3.2 y, finalmente, en la sección 3.5 presentamos algunas conclusiones y problemas abiertos.

3.2 Resultados principales

De aquí en adelante, asumimos que $n = 2k$ y que $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ es una base de $\mathbb{F}_2^n$. Para $i = 1, 2, \ldots, k$, consideremos los subespacios vectoriales de $\mathbb{F}_2^n$ dados por

$$G_i = \operatorname{Env}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\} \quad \text{y} \quad H_i = \operatorname{Env}\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}.$$

Obviamente, $\dim G_i = 2i$ y $\dim H_i = 2$. Además, si consideramos $G_0 = \{\mathbf{0}\}$,

entonces

$$G_i = G_{i-1} \oplus H_i \quad \text{y} \quad G_{i-1} \cap H_i = \{\mathbf{0}\}, \tag{3.1}$$

y por tanto, G_i es la suma directa de G_{i-1} y H_i. En particular, $G_1 = H_1$.

Para mayor claridad en la notación, haremos referencia a los elementos de H_i, para $i = 1, 2, \ldots, k$, como

$$\boldsymbol{a}_0^{(i)} = \mathbf{0}, \quad \boldsymbol{a}_1^{(i)} = \boldsymbol{u}_{2i-1}, \quad \boldsymbol{a}_2^{(i)} = \boldsymbol{u}_{2i} \quad \text{y} \quad \boldsymbol{a}_3^{(i)} = \boldsymbol{u}_{2i-1} \oplus \boldsymbol{u}_{2i}.$$

Usando los conjuntos G_{i-1} y los elementos de H_i, para $i = 1, 2, \ldots, k$, definimos una serie de subconjuntos de G_i con algunas propiedades que permiten que los subconjuntos de G_k obtenidos sean, al final del proceso iterativo, los soportes de funciones bent de $2k$ variables.

Para $p \in \{0, 1, 2, 3\}$ consideremos los conjuntos

$$B(p) = \left\{\boldsymbol{a}_p^{(1)}\right\} \quad \text{y} \quad \widehat{B}(p) = \bigcup_{\substack{q=0 \\ q \neq p}}^{3} \left\{\boldsymbol{a}_q^{(1)}\right\}.$$

Es evidente que

$$G_1 = B(p) \cup \widehat{B}(p) \quad \text{y} \quad B(p) \cap \widehat{B}(p) = \emptyset. \tag{3.2}$$

Además, si $r, s \in \{0, 1, 2, 3\}$ con $r \neq s$, entonces $B(r) \neq B(s)$.

Ahora, sea $(p_1, p_2, \ldots, p_{i-1}, p_i) \in \{0, 1, 2, 3\}^i$ y supongamos que hemos definido los conjuntos $B(p_1, p_2, \ldots, p_{i-1})$ y $\widehat{B}(p_1, p_2, \ldots, p_{i-1})$. Entonces, definimos

$$\begin{aligned} &B(p_1, p_2, \ldots, p_{i-1}, p_i) \\ &= \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right), \end{aligned} \tag{3.3}$$

$$\begin{aligned} &\widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i) \\ &= \left(\boldsymbol{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right). \end{aligned} \tag{3.4}$$

Nuestro objetivo es probar que para todo $(p_1, p_2, \ldots, p_k) \in \{0, 1, 2, 3\}^k$, los conjuntos

$$B(p_1, p_2, \ldots, p_k) \quad \text{y} \quad \widehat{B}(p_1, p_2, \ldots, p_k)$$

son los soportes de dos funciones bent de $2k$ variables, de forma que una es la función complementaria de la otra. Sin embargo, conviene demostrar primero algunos lemas técnicos que simplificarán el desarrollo de la demostración del resultado mencionado.

El primer resultado establece que los conjuntos de las expresiones (3.3) y (3.4) son conjuntos complementarios en G_i.

Lema 3.1: *Para $i = 1, 2, \ldots, k$, y para todo $(p_1, p_2, \ldots, p_i) \in \{0, 1, 2, 3\}^i$, tenemos que*

(a) $G_i = B(p_1, p_2, \ldots, p_i) \cup \widehat{B}(p_1, p_2, \ldots, p_i)$
(b) $B(p_1, p_2, \ldots, p_i) \cap \widehat{B}(p_1, p_2, \ldots, p_i) = \emptyset$

DEMOSTRACIÓN: Procedemos por inducción sobre i. Para $i = 1$ el resultado viene dado por la expresión (3.2). Supongamos que el resultado es cierto para $i - 1 < k$, demostraremos que también es cierto para i.

Primero, por la hipótesis de inducción, tenemos que

$$B(p_1, p_2, \ldots, p_{i-1}) \cup \widehat{B}(p_1, p_2, \ldots, p_{i-1}) = G_{i-1}$$

y por tanto

$$\begin{aligned}
&B(p_1, p_2, \ldots, p_{i-1}, p_i) \cup \widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i) \\
&= \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \\
&\quad \cup \left(\boldsymbol{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \\
&= \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \left(B(p_1, p_2, \ldots, p_{i-1}) \cup \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right)\right) \\
&\quad \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \left(B(p_1, p_2, \ldots, p_{i-1}) \cup \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right)\right)
\end{aligned}$$

$$= \left(\boldsymbol{a}_{p_i}^{(i)} \oplus G_{i-1}\right) \cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus G_{i-1}\right) = \left\{\boldsymbol{a}_0^{(i)}, \boldsymbol{a}_1^{(i)}, \boldsymbol{a}_2^{(i)}, \boldsymbol{a}_3^{(i)}\right\} \oplus G_{i-1} = G_i$$

donde la última igualdad se deduce de la primera igualdad en la expresión (3.1).

Análogamente, tras algunas manipulaciones algebraicas, obtenemos que

$$\begin{aligned}
&B(p_1, p_2, \ldots, p_{i-1}, p_i) \cap \widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i) \\
&= \left(\left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \right) \\
&\quad \cap \left(\left(\boldsymbol{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \right) \\
&= \bigcup_{r=0}^{3} \left(\left(\boldsymbol{a}_r^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_r^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \right) && (3.5a) \\
&\quad \cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \right) && (3.5b) \\
&\quad \cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\left(\boldsymbol{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \right) && (3.5c) \\
&\quad \cup \bigcup_{\substack{q,r=0 \\ q,r\neq p_i \\ q\neq r}}^{3} \left(\left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_r^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \right) && (3.5d)
\end{aligned}$$

Con el fin de demostrar que $B(p_1, p_2, \ldots, p_{i-1}, p_i) \cap \widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i) = \emptyset$, es suficiente comprobar que todas las intersecciones que aparecen en las expresiones (3.5a), (3.5b), (3.5c) y (3.5d) son vacías.

Por la hipótesis de inducción tenemos que

$$\left(\boldsymbol{a}_r^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_r^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right)$$

$$= \boldsymbol{a}_r^{(i)} \oplus \left(B(p_1, p_2, \ldots, p_{i-1}) \cap \widehat{B}(p_1, p_2, \ldots, p_{i-1}) \right) = \emptyset,$$

por tanto, todas las intersecciones en la expresión (3.5a) son vacías.

Supongamos ahora que $q \in \{0,1,2,3\} \setminus \{p_i\}$. Si

$$\boldsymbol{x} \in \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1}) \right) \cap \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1}) \right),$$

entonces

$$\boldsymbol{x} = \boldsymbol{a}_{p_i}^{(i)} \oplus \boldsymbol{u} = \boldsymbol{a}_q^{(i)} \oplus \boldsymbol{v}$$

para algunos $\boldsymbol{u}, \boldsymbol{v} \in \widehat{B}(p_1, p_2, \ldots, p_{i-1}) \subseteq G_{i-1}$. Pero entonces, teniendo en cuenta que G_{i-1} y H_i son subespacios vectoriales, tenemos que

$$\boldsymbol{u} \oplus \boldsymbol{v} = \boldsymbol{a}_{p_i}^{(i)} \oplus \boldsymbol{a}_q^{(i)} \in G_{i-1} \cap H_i = \{\boldsymbol{0}\}$$

por la expresión (3.1), y entonces, $\boldsymbol{a}_{p_i}^{(i)} = \boldsymbol{a}_q^{(i)}$ lo cual es una contradicción. Por consiguiente, las intersecciones que aparecen en la expresión (3.5b) son vacías.

Por un argumento similar, obtenemos que todas las intersecciones de las expresiones (3.5c) y (3.5d) son también vacías. □

El siguiente resultado establece el número de elementos de los conjuntos definidos por las expresiones (3.3) y (3.4).

Lema 3.2: *Para $i = 1, 2, \ldots, k$, y para todo $(p_1, p_2, \ldots, p_i) \in \{0,1,2,3\}^i$, tenemos que*

(a) $\text{Card}\left(B(p_1, p_2, \ldots, p_i)\right) = 2^{2i-1} - 2^{i-1}$
(b) $\text{Card}\left(\widehat{B}(p_1, p_2, \ldots, p_i)\right) = 2^{2i-1} + 2^{i-1}$

DEMOSTRACIÓN: Procedemos por inducción sobre i.

Para $i = 1$ y para todo $p \in \{0,1,2,3\}$, tenemos que

$$\text{Card}\left(B(p)\right) = 1 = 2^{2\cdot 1-1} - 2^{1-1} \quad \text{y} \quad \text{Card}\left(\widehat{B}(p)\right) = 3 = 2^{2\cdot 1-1} + 2^{1-1}.$$

Supongamos ahora que el resultado es cierto para $i - 1 < k$, vamos a demostrar que también es cierto para i.

Sea $(p_1, p_2, \ldots, p_{i-1}, p_i) \in \{0,1,2,3\}^i$. Por un argumento similar al utilizado en la demostración del lema 3.1, si $q \in \{0,1,2,3\} \setminus \{p_i\}$, entonces

$$\left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) = \emptyset,$$

y si $q, r \in \{0,1,2,3\} \setminus \{p_i\}$ con $q \neq r$, entonces

$$\left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cap \left(\boldsymbol{a}_r^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) = \emptyset.$$

Por tanto, de la expresión (3.3) tenemos que

$$\begin{aligned}
&\operatorname{Card}\left(B(p_1, p_2, \ldots, p_i)\right) \\
&= \operatorname{Card}\left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) + \sum_{\substack{q=0 \\ q \neq p_i}}^{3} \operatorname{Card}\left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \\
&= 2^{2(i-1)-1} + 2^{i-1-1} + 3\left(2^{2(i-1)-1} - 2^{i-1-1}\right) = 2^{2i-1} - 2^{i-1}.
\end{aligned}$$

Ahora, como $\widehat{B}(p_1, p_2, \ldots, p_i) = G_i \setminus B(p_1, p_2, \ldots, p_i)$ tenemos que

$$\operatorname{Card}\left(\widehat{B}(p_1, p_2, \ldots, p_i)\right) = 2^{2i} - \operatorname{Card}\left(B(p_1, p_2, \ldots, p_i)\right) = 2^{2i-1} + 2^{i-1}. \qquad \square$$

Con argumentos similares a los de los lemas anteriores, podemos demostrar también los siguientes resultados.

Lema 3.3: *Para $i = 1, 2, \ldots, k$, si $(p_1, p_2, \ldots, p_i) \in \{0,1,2,3\}^i$ y $\boldsymbol{u} \in G_i \setminus \{\mathbf{0}\}$, entonces:*

(a) $\operatorname{Card}\left(B(p_1, p_2, \ldots, p_i) \cap \left(\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_i)\right)\right) = 2^{2i-2} - 2^{i-1}$,

(b) $\operatorname{Card}\left(\widehat{B}(p_1, p_2, \ldots, p_i) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p_1, p_2, \ldots, p_i)\right)\right) = 2^{2i-2} + 2^{i-1}$,

(c) $\operatorname{Card}\left(B(p_1, p_2, \ldots, p_i) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p_1, p_2, \ldots, p_i)\right)\right) = 2^{2i-2}$,

(d) $\operatorname{Card}\left(\widehat{B}(p_1, p_2, \ldots, p_i) \cap \left(\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_i)\right)\right) = 2^{2i-2}$.

DEMOSTRACIÓN: Procedemos, como en los lemas anteriores, por inducción sobre i. Para $i = 1$, tenemos que $G_1 = \left\{\boldsymbol{a}_p^{(1)}, \boldsymbol{a}_q^{(1)}, \boldsymbol{a}_r^{(1)}, \boldsymbol{a}_s^{(1)}\right\}$ donde $\{p, q, r, s\} = \{0,1,2,3\}$, así que

$$B(p) = \left\{\boldsymbol{a}_p^{(1)}\right\} \quad \text{y} \quad \widehat{B}(p) = \left\{\boldsymbol{a}_q^{(1)}, \boldsymbol{a}_r^{(1)}, \boldsymbol{a}_s^{(1)}\right\}.$$

Si $\boldsymbol{u} \in G_1 \setminus \{\mathbf{0}\}$, podemos suponer que

$$\boldsymbol{u} \oplus \boldsymbol{a}_p^{(1)} = \boldsymbol{a}_q^{(1)},$$

y se sigue el mismo argumento si $\boldsymbol{u} \oplus \boldsymbol{a}_p^{(1)} = \boldsymbol{a}_r^{(1)}$ o $\boldsymbol{u} \oplus \boldsymbol{a}_p^{(1)} = \boldsymbol{a}_s^{(1)}$.

Así que

$$B(p) \cap \left(\boldsymbol{u} \oplus B(p)\right) = \left\{\boldsymbol{a}_p^{(1)}\right\} \cap \left\{\boldsymbol{u} \oplus \boldsymbol{a}_p^{(1)}\right\} = \left\{\boldsymbol{a}_p^{(1)}\right\} \cap \left\{\boldsymbol{a}_q^{(1)}\right\} = \emptyset,$$

y por lo tanto

$$\text{Card}\left(B(p) \cap \left(\boldsymbol{u} \oplus B(p)\right)\right) = 0 = 2^{2\cdot 1-2} - 2^{1-1}.$$

Por otra parte, como G_1 es un subespacio vectorial, tenemos que

$$\begin{aligned}\widehat{B}(p) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p)\right) &= \left\{\boldsymbol{a}_q^{(1)}, \boldsymbol{a}_r^{(1)}, \boldsymbol{a}_s^{(1)}\right\} \cap \left\{\boldsymbol{u} \oplus \boldsymbol{a}_q^{(1)}, \boldsymbol{u} \oplus \boldsymbol{a}_r^{(1)}, \boldsymbol{u} \oplus \boldsymbol{a}_s^{(1)}\right\} \\ &= \left\{\boldsymbol{a}_q^{(1)}, \boldsymbol{a}_r^{(1)}, \boldsymbol{a}_s^{(1)}\right\} \cap \left\{\boldsymbol{a}_p^{(1)}, \boldsymbol{a}_s^{(1)}, \boldsymbol{a}_r^{(1)}\right\} \\ &= \left\{\boldsymbol{a}_r^{(1)}, \boldsymbol{a}_s^{(1)}\right\}\end{aligned}$$

y por lo tanto

$$\text{Card}\left(\widehat{B}(p) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p)\right)\right) = 2 = 2^{2\cdot 1-2} + 2^{1-1}.$$

Además

$$B(p) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p)\right) = \left\{\boldsymbol{a}_p^{(1)}\right\} \cap \left\{\boldsymbol{a}_p^{(1)}, \boldsymbol{a}_s^{(1)}, \boldsymbol{a}_r^{(1)}\right\} = \left\{\boldsymbol{a}_p^{(1)}\right\}$$

entonces

$$\text{Card}\left(B(p) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p)\right)\right) = 1 = 2^{2\cdot 1-2}.$$

Finalmente

$$\widehat{B}(p) \cap \left(\boldsymbol{u} \oplus B(p)\right) = \left\{\boldsymbol{a}_q^{(1)}, \boldsymbol{a}_r^{(1)}, \boldsymbol{a}_s^{(1)}\right\} \cap \left\{\boldsymbol{u} \oplus \boldsymbol{a}_p^{(1)}\right\} = \left\{\boldsymbol{a}_q^{(1)}\right\}$$

y entonces

$$\text{Card}\left(\widehat{B}(p) \cap \left(\boldsymbol{u} \oplus B(p)\right)\right) = 1 = 2^{2\cdot 1-2}.$$

Por tanto, las propiedades (a), (b), (c) y (d) se verifican para $i = 1$.

Supongamos ahora que las propiedades (a), (b), (c) y (d) se verifican para $i-1<k$. Demostraremos que estas propiedades también se verifican para i. Sea $(p_1,p_2,\ldots,p_{i-1},p_i)\in\{0,1,2,3\}^i$ y supongamos que $\boldsymbol{u}\in G_i\setminus\{\mathbf{0}\}$. De la expresión (3.3) tenemos que

$$
\begin{aligned}
&B(p_1,p_2,\ldots,p_{i-1},p_i)\cap(\boldsymbol{u}\oplus B(p_1,p_2,\ldots,p_{i-1},p_i))\\
&=\left(\left(\boldsymbol{a}_{p_i}^{(i)}\oplus\widehat{B}(p_1,p_2,\ldots,p_{i-1})\right)\cap\left(\boldsymbol{u}\oplus\boldsymbol{a}_{p_i}^{(i)}\oplus\widehat{B}(p_1,p_2,\ldots,p_{i-1})\right)\right) &\text{(3.6a)}\\
&\quad\cup\bigcup_{\substack{q=0\\q\neq p_i}}^{3}\left(\left(\boldsymbol{a}_{p_i}^{(i)}\oplus\widehat{B}(p_1,p_2,\ldots,p_{i-1})\right)\cap\left(\boldsymbol{u}\oplus\boldsymbol{a}_{q}^{(i)}\oplus B(p_1,p_2,\ldots,p_{i-1})\right)\right) &\text{(3.6b)}\\
&\quad\cup\bigcup_{\substack{q=0\\q\neq p_i}}^{3}\left(\left(\boldsymbol{a}_{q}^{(i)}\oplus B(p_1,p_2,\ldots,p_{i-1})\right)\cap\left(\boldsymbol{u}\oplus\boldsymbol{a}_{p_i}^{(i)}\oplus\widehat{B}(p_1,p_2,\ldots,p_{i-1})\right)\right) &\text{(3.6c)}\\
&\quad\cup\bigcup_{\substack{q,r=0\\q,r\neq p_i}}^{3}\left(\left(\boldsymbol{a}_{q}^{(i)}\oplus B(p_1,p_2,\ldots,p_{i-1})\right)\cap\left(\boldsymbol{u}\oplus\boldsymbol{a}_{r}^{(i)}\oplus B(p_1,p_2,\ldots,p_{i-1})\right)\right). &\text{(3.6d)}
\end{aligned}
$$

De la expresión (3.1) tenemos que $\boldsymbol{u}=\boldsymbol{v}\oplus\boldsymbol{a}_l^{(i)}$ con $\boldsymbol{v}\in G_{i-1}$ y $l\in\{0,1,2,3\}$.

Si $l=p_i$, entonces el conjunto en la expresión (3.6a) se convierte en

$$
\boldsymbol{a}_{p_i}^{(i)}\oplus\left(\widehat{B}(p_1,p_2,\ldots,p_{i-1})\cap\left(\boldsymbol{v}\oplus\widehat{B}(p_1,p_2,\ldots,p_{i-1})\right)\right), \tag{3.7}
$$

los conjuntos de las expresiones (3.6b) y (3.6c) se convierten en el conjunto vacío, y el conjunto de las expresiones (3.6d) se convierte en

$$
\bigcup_{\substack{q=0\\q\neq p_i}}^{3}\boldsymbol{a}_q^{(i)}\oplus\left(B(p_1,p_2,\ldots,p_{i-1})\cap(\boldsymbol{v}\oplus B(p_1,p_2,\ldots,p_{i-1}))\right). \tag{3.8}
$$

Además, no es dificil demostrar que el conjunto de la expresión (3.7) es disjunto con cada uno de los tres conjuntos que aparecen en la expresión (3.8). Es también fácil demostrar que estos tres conjuntos son mutuamente disjuntos. Por tanto, mediante la hipótesis de inducción,

$$
\begin{aligned}
&\operatorname{Card}\left(B(p_1,p_2,\ldots,p_{i-1},p_i)\cap(\boldsymbol{u}\oplus B(p_1,p_2,\ldots,p_{i-1},p_i))\right)\\
&=\operatorname{Card}\left(\widehat{B}(p_1,p_2,\ldots,p_{i-1})\cap\left(\boldsymbol{v}\oplus\widehat{B}(p_1,p_2,\ldots,p_{i-1})\right)\right)
\end{aligned}
$$

$$+ 3 \cdot \mathrm{Card}\left(B(p_1, p_2, \ldots, p_{i-1}) \cap (\boldsymbol{v} \oplus B(p_1, p_2, \ldots, p_{i-1}))\right)$$
$$= 2^{2(i-1)-2} + 2^{(i-1)-1} + 3\left(2^{2(i-1)-2} - 2^{(i-1)-1}\right) = 2^{2i-2} - 2^{i-1}.$$

Sin embargo, si $p_i \neq l$, entonces el conjunto en la expresión (3.6a) se convierte en el conjunto vacío, los conjuntos de las expresiones (3.6b) y (3.6c) se convierten en los conjuntos

$$\boldsymbol{a}_{p_i}^{(i)} \oplus \left(\widehat{B}(p_1, p_2, \ldots, p_{i-1}) \cap (\boldsymbol{v} \oplus B(p_1, p_2, \ldots, p_{i-1}))\right) \tag{3.9}$$

y

$$\boldsymbol{a}_{l}^{(i)} \oplus \left(B(p_1, p_2, \ldots, p_{i-1}) \cap \left(\boldsymbol{v} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right)\right) \tag{3.10}$$

respectivamente, y el conjunto de la expresión (3.6d) se convierte en el conjunto

$$\left(\boldsymbol{a}_{r}^{(i)} \oplus (B(p_1, p_2, \ldots, p_{i-1}) \cap (\boldsymbol{v} \oplus B(p_1, p_2, \ldots, p_{i-1})))\right) \tag{3.11a}$$
$$\cup \left(\boldsymbol{a}_{s}^{(i)} \oplus (B(p_1, p_2, \ldots, p_{i-1}) \cap (\boldsymbol{v} \oplus B(p_1, p_2, \ldots, p_{i-1})))\right) \tag{3.11b}$$

para cualquier $r, s \in \{0, 1, 2, 3\} \setminus \{p_i, l\}$.

Además, no es difícil demostrar que los conjuntos de las expresiones (3.9), (3.10), (3.11a) y (3.11b) son disjuntos dos a dos. Así que, por la hipótesis de inducción,

$$\mathrm{Card}\left(B(p_1, p_2, \ldots, p_{i-1}, p_i) \cap (\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_{i-1}, p_i))\right)$$
$$= \mathrm{Card}\left(\widehat{B}(p_1, p_2, \ldots, p_{i-1}) \cap (\boldsymbol{v} \oplus B(p_1, p_2, \ldots, p_{i-1}))\right)$$
$$+ \mathrm{Card}\left(B(p_1, p_2, \ldots, p_{i-1}) \cap \left(\boldsymbol{v} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right)\right)$$
$$+ 2 \cdot \mathrm{Card}\left(B(p_1, p_2, \ldots, p_{i-1}) \cap (\boldsymbol{v} \oplus B(p_1, p_2, \ldots, p_{i-1}))\right)$$
$$= 2^{2(i-1)-2} + 2^{2(i-1)-2} + 2\left(2^{2(i-1)-2} - 2^{(i-1)-1}\right) = 2^{2i-2} - 2^{i-1}.$$

Por consiguiente, la propiedad (a) se verifica para i.

Por un argumento similar, tenemos también que las propiedades (b), (c) y (d) se verifican para i. □

Ahora estamos en condiciones de demostrar que los conjuntos $B(p_1, p_2, \ldots, p_k)$ y $\widehat{B}(p_1, p_2, \ldots, p_k)$ son los soportes de una función bent de $2k$ variables y su complementaria, respectivamente.

Teorema 3.1: *Para todo* $(p_1, p_2, \ldots, p_k) \in \{0,1,2,3\}^k$ *los conjuntos*

$$B(p_1, p_2, \ldots, p_k) \quad y \quad \widehat{B}(p_1, p_2, \ldots, p_k)$$

son los soportes de dos funciones bent de $2k$ *variables de modo que una es la función complementaria de la otra.*

DEMOSTRACIÓN: Supongamos que $\boldsymbol{u} \in \mathbb{F}_2^{2k} \backslash \{\mathbf{0}\}$. Como $\mathbb{F}_2^{2k} = G_k$, por los lemas 3.1, 3.2 y 3.3 tenemos que

$$\begin{aligned}
&\operatorname{Card}\left(B(p_1, p_2, \ldots, p_k)\, \Delta\, (\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_k))\right) \\
&\quad = \operatorname{Card}\left(B(p_1, p_2, \ldots, p_k)\right) + \operatorname{Card}\left(\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_k)\right) \\
&\qquad - 2\operatorname{Card}\left(B(p_1, p_2, \ldots, p_k) \cap (\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_k))\right) \\
&\quad = 2^{2k-1} - 2^{k-1} + 2^{2k-1} - 2^{k-1} - 2\left(2^{2k-2} - 2^{k-1}\right) = 2^{2k-1}
\end{aligned}$$

y por lo tanto, $B(p_1, p_2, \ldots, p_k)\, \Delta (\boldsymbol{u} \oplus B(p_1, p_2, \ldots, p_k))$ es el soporte de una función equilibrada de $2k$ variables. Así, por el corolario 2.3, tenemos que $B(p_1, p_2, \ldots, p_k)$ es el soporte de una función bent $f(\boldsymbol{x})$ de $2k$ variables.

Además, del lema 3.1, tenemos que $\widehat{B}(p_1, p_2, \ldots, p_k) = G_k \backslash B(p_1, p_2, \ldots, p_k)$ y, por consiguiente, el conjunto $\widehat{B}(p_1, p_2, \ldots, p_k)$ es el soporte de la función complementaria $1 \oplus f(\boldsymbol{x})$. □

3.3 Recuento de funciones bent

Con el fin de contar el número de funciones bent proporcionado por el teorema 3.1, necesitamos el siguiente resultado.

Teorema 3.2: *Para* $i = 1, 2, \ldots, k$, *sea* $(p_1, p_2, \ldots, p_i), (q_1, q_2, \ldots, q_i) \in \{0,1,2,3\}^i$. *Si* $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_l = q_l$, *pero* $p_{l+1} \neq q_{l+1}$ *para algún* $l \in \{1, 2, \ldots, i-1\}$, *entonces*

$$B(p_1, p_2, \ldots, p_l, p_{l+1}, p_{l+2}, \ldots p_{l+m}) \neq B(p_1, p_2, \ldots, p_l, q_{l+1}, q_{l+2}, \ldots q_{l+m}),$$

$$\widehat{B}(p_1, p_2, \ldots, p_l, p_{l+1}, p_{l+2}, \ldots p_{l+m}) \neq \widehat{B}(p_1, p_2, \ldots, p_l, q_{l+1}, q_{l+2}, \ldots q_{l+m})$$

para $m = 1, 2, \ldots, i - l$.

DEMOSTRACIÓN: Procedemos por inducción sobre m. Supongamos que $m = 1$. Como $p_{l+1} \neq q_{l+1}$, podemos suponer que $\{0, 1, 2, 3\} = \{p_{l+1}, q_{l+1}, r, s\}$ con $r \neq s$. Por lo tanto, si

$$B(p_1, p_2, \ldots, p_l, p_{l+1}) = B(p_1, p_2, \ldots, p_l, q_{l+1}),$$

de la expresión (3.3) tenemos que

$$\begin{aligned}&\left(\boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)\right) \cup \left(\boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \ldots, p_l)\right)\\ &= \left(\boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)\right) \cup \left(\boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \ldots, p_l)\right).\end{aligned}$$

Sea $\boldsymbol{x} \in \boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)$, entonces

$$\boldsymbol{x} \in \boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l) \quad \text{o} \quad \boldsymbol{x} \in \boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \ldots, p_l).$$

En el primer caso,

$$\boldsymbol{x} = \boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \boldsymbol{u} = \boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus \boldsymbol{v}$$

con $\boldsymbol{u}, \boldsymbol{v} \in \widehat{B}(p_1, p_2, \ldots, p_l) \subseteq G_l$; pero entonces

$$\boldsymbol{u} \oplus \boldsymbol{v} = \boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \boldsymbol{a}_{q_{l+1}}^{(l+1)} \in G_l \cap H_{l+1} = \{\boldsymbol{0}\}$$

por tanto $\boldsymbol{a}_{p_{l+1}}^{(l+1)} = \boldsymbol{a}_{q_{l+1}}^{(l+1)}$, lo cual es una contradicción.

En el segundo caso,

$$\boldsymbol{x} = \boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \boldsymbol{u} = \boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \boldsymbol{v}$$

con $\boldsymbol{u} \in \widehat{B}(p_1, p_2, \ldots, p_l)$ y $\boldsymbol{v} \in B(p_1, p_2, \ldots, p_l)$; pero entonces

$$\boldsymbol{u} = \boldsymbol{v} \in \widehat{B}(p_1, p_2, \ldots, p_l) \cap B(p_1, p_2, \ldots, p_l) = \emptyset$$

lo que también es una contradicción.

Así que, ninguno de los elementos de $\boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)$ pertenece al conjunto

$$\left(\boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)\right) \cup \left(\boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \ldots, p_l)\right).$$

Un argumento análogo muestra que ninguno de los elementos de

$$\boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)$$

pertenece al conjunto

$$\left(\boldsymbol{a}_{q_{l+1}}^{(l+1)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l)\right) \cup \left(\boldsymbol{a}_{p_{l+1}}^{(l+1)} \oplus B(p_1, p_2, \ldots, p_l)\right).$$

Por consiguiente, $B(p_1, p_2, \ldots, p_l, p_{l+1}) \neq B(p_1, p_2, \ldots, p_l, q_{l+1})$ y del lema 3.1, también tenemos que $\widehat{B}(p_1, p_2, \ldots, p_l, p_{l+1}) \neq \widehat{B}(p_1, p_2, \ldots, p_l, q_{l+1})$.

Supongamos ahora que el resultado es cierto para $m-1$, demostraremos que también es verdadero para m. Si

$$B(p_1, p_2, \ldots, p_l, p_{l+1}, p_{l+2}, \ldots p_{l+m}) = B(p_1, p_2, \ldots, p_l, q_{l+1}, q_{l+2}, \ldots q_{l+m})$$

de la expresión (3.3) tenemos que

$$\begin{aligned}
&\left(\boldsymbol{a}_{p_{l+m}}^{(l+m)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l, p_{l+1}, \ldots, p_{l+m-1})\right) \\
&\qquad \cup \bigcup_{\substack{r=0 \\ r \neq p_{l+m}}}^{3} \left(\boldsymbol{a}_r^{(l+m)} \oplus B(p_1, p_2, \ldots, p_l, p_{l+1}, \ldots, p_{l+m-1})\right) \\
&= \left(\boldsymbol{a}_{q_{l+m}}^{(l+m)} \oplus \widehat{B}(p_1, p_2, \ldots, p_l, q_{l+1}, \ldots, q_{l+m-1})\right) \\
&\qquad \cup \bigcup_{\substack{s=0 \\ s \neq q_{l+m}}}^{3} \left(\boldsymbol{a}_s^{(l+m)} \oplus B(p_1, p_2, \ldots, p_l, q_{l+1}, \ldots, q_{l+m-1})\right)
\end{aligned}$$

Ahora, mediante un argumento similar al anterior, pero considerando los casos $p_{l+m} = q_{l+m}$ y $p_{l+m} \neq q_{l+m}$, obtenemos que ninguno de los elementos del conjunto del primer miembro de la expresión anterior pertenece al conjunto del segundo miembro.

Así que,

$$B(p_1, p_2, \ldots, p_l, p_{l+1}, p_{l+2}, \ldots p_{l+m}) \neq B(p_1, p_2, \ldots, p_l, q_{l+1}, q_{l+2}, \ldots q_{l+m})$$

y del lema 3.1, concluimos que

$$\widehat{B}(p_1, p_2, \ldots, p_l, p_{l+1}, p_{l+2}, \ldots p_{l+m}) \neq \widehat{B}(p_1, p_2, \ldots, p_l, q_{l+1}, q_{l+2}, \ldots q_{l+m}). \qquad \square$$

Como consecuencia de este resultado, tenemos el siguiente corolario.

Corolario 3.1: *Para una base de $\mathbb{F}_2^{2k}$ el número de funciones bent de $2k$ variables que podemos construir usando el procedimiento descrito en la sección 3.2 es 2^{2k+1}.*

DEMOSTRACIÓN: Para una base fija $\mathcal{U}$, podemos construir tantos conjuntos del tipo $B(p_1, p_2, \ldots, p_k)$ como elementos haya en $\{0, 1, 2, 3\}^k$. Lo mismo es cierto para los conjuntos de tipo $\widehat{B}(p_1, p_2, \ldots, p_k)$. Por tanto, el número de funciones bent de $2k$ variables que podemos construir es

$$2\,\mathrm{Card}\left(\{0, 1, 2, 3\}^k\right) = 2^{2k+1}. \qquad \square$$

En este punto surge de modo natural la siguiente pregunta: ¿a partir de dos bases diferentes $\mathcal{U}$ y $\mathcal{V}$ de $\mathbb{F}_2^{2k}$, las 2^{2k+1} funciones bent obtenidas de la base $\mathcal{U}$ son diferentes de las 2^{2k+1} funciones bent obtenidas de la base $\mathcal{V}$?

El número de bases diferentes de $\mathbb{F}_2^{2k}$ (ver [96, página 46]) es $\prod_{i=0}^{2k-1}(2^{2k} - 2^i)$. En consecuencia, podemos aplicar el procedimiento iterativo de

$$2^{2k+1} \prod_{i=0}^{2k-1} (2^{2k} - 2^i)$$

formas distintas. Por ejemplo, para $k = 2$, construiremos, al aplicar cada una de esas posibilidades, 645 120 funciones bent. Sin embargo, es bien sabido que el número de funciones bent de 4 variables diferentes entre sí es 896. Así pues hay diferentes bases que proporcionan las mismas funciones bent, tal y como podemos ver en el siguiente ejemplo.

Ejemplo 3.1: Supongamos que $k = 2$ y consideremos la base $\mathcal{U} = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{8}\}$ de $\mathbb{F}_2^4$. Los soportes de las funciones bent que podemos construir usando el procedimiento descrito en la sección 3.2 se muestran en la tabla 3.1. Por otra parte, si consideramos la base $\mathcal{V} = \{\mathbf{6}, \mathbf{7}, \mathbf{9}, \mathbf{13}\}$, entonces los soportes de las funciones bent

(p_1, p_2)	$B(p_1, p_2)$	$\widehat{B}(p_1, p_2)$
$(0,0)$	$\mathbf{1,2,3,4,8,12}$	$\mathbf{0,5,6,7,9,10,11,13,14,15}$
$(0,1)$	$\mathbf{0,5,6,7,8,12}$	$\mathbf{1,2,3,4,9,10,11,13,14,15}$
$(0,2)$	$\mathbf{0,4,9,10,11,12}$	$\mathbf{1,2,3,5,6,7,8,13,14,15}$
$(0,3)$	$\mathbf{0,4,8,13,14,15}$	$\mathbf{1,2,3,5,6,7,9,10,11,12}$
$(1,0)$	$\mathbf{0,2,3,5,9,13}$	$\mathbf{1,4,6,7,8,10,11,12,14,15}$
$(1,1)$	$\mathbf{1,4,6,7,9,13}$	$\mathbf{0,2,3,5,8,10,11,12,14,15}$
$(1,2)$	$\mathbf{1,5,8,10,11,13}$	$\mathbf{0,2,3,4,6,7,9,12,14,15}$
$(1,3)$	$\mathbf{1,5,9,12,14,15}$	$\mathbf{0,2,3,4,6,7,8,10,11,13}$
$(2,0)$	$\mathbf{0,1,3,6,10,14}$	$\mathbf{2,4,5,7,8,9,11,12,13,15}$
$(2,1)$	$\mathbf{2,4,5,7,10,14}$	$\mathbf{0,1,3,6,8,9,11,12,13,15}$
$(2,2)$	$\mathbf{2,6,8,9,11,14}$	$\mathbf{0,1,3,4,5,7,10,12,13,15}$
$(2,3)$	$\mathbf{2,6,10,12,13,15}$	$\mathbf{0,1,3,4,5,7,8,9,11,14}$
$(3,0)$	$\mathbf{0,1,2,7,11,15}$	$\mathbf{3,4,5,6,8,9,10,12,13,14}$
$(3,1)$	$\mathbf{3,4,5,6,11,15}$	$\mathbf{0,1,2,7,8,9,10,12,13,14}$
$(3,2)$	$\mathbf{3,7,8,9,10,15}$	$\mathbf{0,1,2,4,5,6,11,12,13,14}$
$(3,3)$	$\mathbf{3,7,11,12,13,14}$	$\mathbf{0,1,2,4,5,6,8,9,10,15}$

Tabla 3.1: *Soportes de las funciones bent construídas con la base $\mathcal{U}$ del ejemplo 3.1*

que podemos construir usando el procedimiento descrito en la sección 3.2 se muestran en la tabla 3.2. Como podemos ver, obtenemos las mismas funciones bent en ambos casos, aunque para diferentes valores de $(p_1, p_2) \in \{0,1,2,3\}^2$. ■

De aquí en adelante para referirnos a los soportes de las funciones *bent* proporcionadas por el proceso iterativo descrito en la sección 3.2 mediante la base $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ escribiremos

$$B_{\mathcal{U}}(p_1, p_2, \ldots, p_k) \quad \text{y} \quad \widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_k).$$

Además, si observamos detenidamente las expresiones (3.3) y (3.4) vemos que los conjuntos anteriores dependen de los subespacios vectoriales $H_i = \text{Env}\,\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$,

(p_1, p_2)	$B(p_1, p_2)$	$\widehat{B}(p_1, p_2)$
$(0,0)$	$\mathbf{3,7,11,12,13,14}$	$\mathbf{0,1,2,4,5,6,8,9,10,15}$
$(0,1)$	$\mathbf{0,1,2,7,11,15}$	$\mathbf{3,4,5,6,8,9,10,12,13,14}$
$(0,2)$	$\mathbf{0,4,9,10,11,12}$	$\mathbf{1,2,3,5,6,7,8,13,14,15}$
$(0,3)$	$\mathbf{0,5,6,7,8,12}$	$\mathbf{1,2,3,4,9,10,11,13,14,15}$
$(1,0)$	$\mathbf{0,4,8,13,14,15}$	$\mathbf{1,2,3,5,6,7,9,10,11,12}$
$(1,1)$	$\mathbf{1,2,3,4,8,12}$	$\mathbf{0,5,6,7,9,10,11,13,14,15}$
$(1,2)$	$\mathbf{3,7,8,9,10,15}$	$\mathbf{0,1,2,4,5,6,11,12,13,14}$
$(1,3)$	$\mathbf{3,4,5,6,11,15}$	$\mathbf{0,1,2,7,8,9,10,12,13,14}$
$(2,0)$	$\mathbf{0,1,3,6,10,14}$	$\mathbf{2,4,5,7,8,9,11,12,13,15}$
$(2,1)$	$\mathbf{2,6,10,12,13,15}$	$\mathbf{0,1,3,4,5,7,8,9,11,14}$
$(2,2)$	$\mathbf{1,4,6,7,9,13}$	$\mathbf{0,2,3,5,8,10,11,12,14,15}$
$(2,3)$	$\mathbf{1,5,8,10,11,13}$	$\mathbf{0,2,3,4,6,7,9,12,14,15}$
$(3,0)$	$\mathbf{0,2,3,5,9,13}$	$\mathbf{1,4,6,7,8,10,11,12,14,15}$
$(3,1)$	$\mathbf{1,5,9,12,14,15}$	$\mathbf{0,2,3,4,6,7,8,10,11,13}$
$(3,2)$	$\mathbf{2,4,5,7,10,14}$	$\mathbf{0,1,3,6,8,9,11,12,13,15}$
$(3,3)$	$\mathbf{2,6,8,9,11,14}$	$\mathbf{0,1,3,4,5,7,10,12,13,15}$

Tabla 3.2: *Soportes de las funciones bent construídas con las bases $\mathcal{V}$ del ejemplo 3.1*

para $i = 1, 2, \ldots, k$, y no tanto de la la base $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$ considerada. Por tanto podemos establecer el siguiente resultado.

Lema 3.4: *Sean $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ y $\mathcal{V} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{2k-1}, \boldsymbol{v}_{2k}\}$ dos bases de $\mathbb{F}_2^{2k}$. Supongamos que existe $r \in \{1, 2, \ldots, k\}$ tal que*

- $(\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}) = (\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i})$ *para* $i \in \{1, 2, \ldots, k\} \setminus \{r\}$,
- $\mathrm{Env}\{\boldsymbol{v}_{2r-1}, \boldsymbol{v}_{2r}\} = \mathrm{Env}\{\boldsymbol{u}_{2r-1}, \boldsymbol{u}_{2r}\}$,

entonces

$$B_{\mathcal{U}}(p_1, p_2, \ldots, p_k) = B_{\mathcal{V}}(p_1, p_2, \ldots, p_k) \quad y \quad \widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_k) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \ldots, p_k)$$

para todo $(p_1, p_2, \ldots, p_k) \in \{0, 1, 2, 3\}^k$.

Además, el orden en que cada par de vectores aparece dentro de la base no es significativo, como podemos ver en el siguiente ejemplo.

Ejemplo 3.2: Supongamos que $k = 4$ y consideremos las bases

$$\mathcal{U} = \{\mathbf{1}, \mathbf{2}; \mathbf{4}, \mathbf{8}; \mathbf{16}, \mathbf{32}; \mathbf{64}, \mathbf{128}\} \quad \text{y} \quad \mathcal{V} = \{\mathbf{1}, \mathbf{2}; \mathbf{16}, \mathbf{32}; \mathbf{4}, \mathbf{8}; \mathbf{64}, \mathbf{128}\}$$

de $\mathbb{F}_2^8$. Entonces, siguiendo el proceso descrito en la sección 3.2 obtenemos a partir de la base $\mathcal{U}$ los siguientes conjuntos

$$\begin{aligned}
B_{\mathcal{U}}(0) &= \{\mathbf{0}\},\\
B_{\mathcal{U}}(0,2) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}\},\\
B_{\mathcal{U}}(0,2,1) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36},\\
&\quad \mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}\},\\
B_{\mathcal{U}}(0,2,1,3) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36},\\
&\quad \mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}, \mathbf{64}, \mathbf{68}, \mathbf{73}, \mathbf{74}, \mathbf{75}, \mathbf{76}, \mathbf{81},\\
&\quad \mathbf{82}, \mathbf{83}, \mathbf{85}, \mathbf{86}, \mathbf{87}, \mathbf{88}, \mathbf{93}, \mathbf{94}, \mathbf{95}, \mathbf{96}, \mathbf{100}, \mathbf{105}, \mathbf{106}, \mathbf{107}, \mathbf{108},\\
&\quad \mathbf{112}, \mathbf{116}, \mathbf{121}, \mathbf{122}, \mathbf{123}, \mathbf{124}, \mathbf{128}, \mathbf{132}, \mathbf{137}, \mathbf{138}, \mathbf{139}, \mathbf{140},\\
&\quad \mathbf{145}, \mathbf{146}, \mathbf{147}, \mathbf{149}, \mathbf{150}, \mathbf{151}, \mathbf{152}, \mathbf{157}, \mathbf{158}, \mathbf{159}, \mathbf{160}, \mathbf{164},\\
&\quad \mathbf{169}, \mathbf{170}, \mathbf{171}, \mathbf{172}, \mathbf{176}, \mathbf{180}, \mathbf{185}, \mathbf{186}, \mathbf{187}, \mathbf{188}, \mathbf{193}, \mathbf{194},\\
&\quad \mathbf{195}, \mathbf{197}, \mathbf{198}, \mathbf{199}, \mathbf{200}, \mathbf{205}, \mathbf{206}, \mathbf{207}, \mathbf{208}, \mathbf{212}, \mathbf{217}, \mathbf{218},\\
&\quad \mathbf{219}, \mathbf{220}, \mathbf{225}, \mathbf{226}, \mathbf{227}, \mathbf{229}, \mathbf{230}, \mathbf{231}, \mathbf{232}, \mathbf{237}, \mathbf{238}, \mathbf{239},\\
&\quad \mathbf{241}, \mathbf{242}, \mathbf{243}, \mathbf{245}, \mathbf{246}, \mathbf{247}, \mathbf{248}, \mathbf{253}, \mathbf{254}, \mathbf{255}\},
\end{aligned}$$

y los siguientes conjuntos a partir de la base $\mathcal{V}$

$$\begin{aligned}
B_{\mathcal{V}}(0) &= \{\mathbf{0}\},\\
B_{\mathcal{V}}(0,1) &= \{\mathbf{0}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{32}, \mathbf{48}\},\\
B_{\mathcal{V}}(0,1,2) &= \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36},\\
&\quad \mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}\},
\end{aligned}$$

$$B_{\mathcal{V}}(0,1,2,3) = \{\mathbf{0}, \mathbf{4}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{24}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{36},$$
$$\mathbf{41}, \mathbf{42}, \mathbf{43}, \mathbf{44}, \mathbf{48}, \mathbf{52}, \mathbf{57}, \mathbf{58}, \mathbf{59}, \mathbf{60}, \mathbf{64}, \mathbf{68}, \mathbf{73}, \mathbf{74}, \mathbf{75}, \mathbf{76}, \mathbf{81},$$
$$\mathbf{82}, \mathbf{83}, \mathbf{85}, \mathbf{86}, \mathbf{87}, \mathbf{88}, \mathbf{93}, \mathbf{94}, \mathbf{95}, \mathbf{96}, \mathbf{100}, \mathbf{105}, \mathbf{106}, \mathbf{107}, \mathbf{108},$$
$$\mathbf{112}, \mathbf{116}, \mathbf{121}, \mathbf{122}, \mathbf{123}, \mathbf{124}, \mathbf{128}, \mathbf{132}, \mathbf{137}, \mathbf{138}, \mathbf{139}, \mathbf{140},$$
$$\mathbf{145}, \mathbf{146}, \mathbf{147}, \mathbf{149}, \mathbf{150}, \mathbf{151}, \mathbf{152}, \mathbf{157}, \mathbf{158}, \mathbf{159}, \mathbf{160}, \mathbf{164},$$
$$\mathbf{169}, \mathbf{170}, \mathbf{171}, \mathbf{172}, \mathbf{176}, \mathbf{180}, \mathbf{185}, \mathbf{186}, \mathbf{187}, \mathbf{188}, \mathbf{193}, \mathbf{194},$$
$$\mathbf{195}, \mathbf{197}, \mathbf{198}, \mathbf{199}, \mathbf{200}, \mathbf{205}, \mathbf{206}, \mathbf{207}, \mathbf{208}, \mathbf{212}, \mathbf{217}, \mathbf{218},$$
$$\mathbf{219}, \mathbf{220}, \mathbf{225}, \mathbf{226}, \mathbf{227}, \mathbf{229}, \mathbf{230}, \mathbf{231}, \mathbf{232}, \mathbf{237}, \mathbf{238}, \mathbf{239},$$
$$\mathbf{241}, \mathbf{242}, \mathbf{243}, \mathbf{245}, \mathbf{246}, \mathbf{247}, \mathbf{248}, \mathbf{253}, \mathbf{254}, \mathbf{255}\}.$$

Observemos que $B_{\mathcal{U}}(0) = B_{\mathcal{V}}(0)$ y $B_{\mathcal{U}}(0,2) \neq B_{\mathcal{V}}(0,1)$, pero $B_{\mathcal{U}}(0,2,1) = B_{\mathcal{V}}(0,1,2)$ y por consiguiente $B_{\mathcal{U}}(0,2,1,3) = B_{\mathcal{V}}(0,1,2,3)$. Así que, ambas bases $\mathcal{U}$ y $\mathcal{V}$ proporcionan la misma función bent de 8 variables, aunque los conjuntos intermedios en el proceso no son necesariamente iguales. ■

El siguiente resultado establece la propiedad descrita en el ejemplo anterior.

Lema 3.5: *Sean* $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ *y* $\mathcal{V} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{2k-1}, \boldsymbol{v}_{2k}\}$ *dos bases de* $\mathbb{F}_2^{2k}$. *Supongamos que exisite* $r, s \in \{1, 2, \ldots, k\}$, *con* $r < s$, *tal que*

- $(\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}) = (\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i})$ *para* $i \in \{1, 2, \ldots, k\} \setminus \{r, s\}$,
- $(\boldsymbol{v}_{2r-1}, \boldsymbol{v}_{2r}) = (\boldsymbol{u}_{2s-1}, \boldsymbol{u}_{2s})$ *y* $(\boldsymbol{v}_{2s-1}, \boldsymbol{v}_{2s}) = (\boldsymbol{u}_{2r-1}, \boldsymbol{u}_{2r})$,

entonces

$$B_{\mathcal{U}}(p_1, p_2, \ldots, p_r, \ldots, p_s, \ldots, p_k) = B_{\mathcal{V}}(p_1, p_2, \ldots, p_s, \ldots, p_r, \ldots, p_k),$$
$$\widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_r, \ldots, p_s, \ldots, p_k) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \ldots, p_s, \ldots, p_r, \ldots, p_k),$$

para todo $(p_1, p_2, \ldots, p_k) \in \{0, 1, 2, 3\}^k$.

DEMOSTRACIÓN: Sin pérdida de generalidad podemos suponer que $s = r + 1$.

A partir de la elección de las bases $\mathcal{U}$ y $\mathcal{V}$, tenemos que

$$B_{\mathcal{U}}(p_1, p_2, \ldots, p_{r-1}) = B_{\mathcal{V}}(p_1, p_2, \ldots, p_{r-1})$$

$$\widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_{r-1}) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \ldots, p_{r-1}).$$

Siguiendo argumentos similares a los utilizados en las demostraciones de los resultados de la sección 3.2, no es difícil demostrar que

$$B_{\mathcal{U}}(p_1, p_2, \ldots, p_{r-1}, p_r, p_{r+1}) = B_{\mathcal{V}}(p_1, p_2, \ldots, p_{r-1}, p_{r+1}, p_r),$$
$$\widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_{r-1}, p_r, p_{r+1}) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \ldots, p_{r-1}, p_{r+1}, p_r).$$

Ahora, el resultado se sigue de la elección de las bases $\mathcal{U}$ y $\mathcal{V}$. □

Como consecuencia de los lemas 3.4 y 3.5 tenemos el siguiente resultado.

Teorema 3.3: *Sean* $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ *y* $\mathcal{V} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{2k-1}, \boldsymbol{v}_{2k}\}$ *bases de* $\mathbb{F}_2^{2k}$ *tales que* $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$ *y* $\{\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}\}$ *sean bases Gauss-Jordan de cardinalidad 2. Si* σ *es una permutación de* $\{1, 2, \ldots, k\}$*, tal que*

$$(\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}) = (\boldsymbol{u}_{2\sigma(i)-1}, \boldsymbol{u}_{2\sigma(i)}) \quad \textit{para} \quad i = 1, 2, \ldots, k,$$

entonces $\mathcal{U}$ *y* $\mathcal{V}$ *proporcionan las mismas funciones bent de* $2k$ *variables.*

De aquí en adelante, además de considerar que $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$ es una base de Gauss-Jordan de cardinalidad 2 consideraremos también que $\boldsymbol{u}_{2i-1} > \boldsymbol{u}_{2j-1}$ (orden lexicográfico) si $i < j$. Como cada subespacio vectorial de dimensión 2 tiene 6 bases diferentes, pero sólo una es base de Gauss-Jordan de cardinalidad 2, tenemos que el número de bases de $\mathbb{F}_2^{2k}$ que satisfacen estas condiciones es

$$\frac{\prod_{i=0}^{2k-1}(2^{2k} - 2^i)}{6^k \cdot k!}.$$

En particular, para $k = 2$ tenemos 280 bases que cumplen estas condiciones. Por consiguiente, de acuerdo con el corolario 3.1, podemos construir $2^5 \cdot 280 = 8960$ funciones bent de 4 variables. Recordemos que el número de funciones bent diferentes de 4 variables es 896 (448 con peso 6 y 448 con peso 10). Una búsqueda exhaustiva

por ordenador muestra que estas 896 funciones bent pueden obtenerse a partir de las siguientes 28 bases de $\mathbb{F}_2^4$:

$$\mathcal{U}_1 = \{\mathbf{8},\mathbf{7};\mathbf{5},\mathbf{3}\},\quad \mathcal{U}_2 = \{\mathbf{8},\mathbf{7};\mathbf{4},\mathbf{2}\},\quad \mathcal{U}_3 = \{\mathbf{8},\mathbf{7};\mathbf{4},\mathbf{1}\},\quad \mathcal{U}_4 = \{\mathbf{8},\mathbf{7};\mathbf{2},\mathbf{1}\},$$

$$\mathcal{U}_5 = \{\mathbf{8},\mathbf{6};\mathbf{5},\mathbf{2}\},\quad \mathcal{U}_6 = \{\mathbf{8},\mathbf{6};\mathbf{4},\mathbf{3}\},\quad \mathcal{U}_7 = \{\mathbf{8},\mathbf{6};\mathbf{4},\mathbf{1}\},\quad \mathcal{U}_8 = \{\mathbf{8},\mathbf{6};\mathbf{2},\mathbf{1}\},$$

$$\mathcal{U}_9 = \{\mathbf{8},\mathbf{5};\mathbf{6},\mathbf{1}\},\quad \mathcal{U}_{10} = \{\mathbf{8},\mathbf{5};\mathbf{4},\mathbf{3}\},\quad \mathcal{U}_{11} = \{\mathbf{8},\mathbf{5};\mathbf{4},\mathbf{2}\},\quad \mathcal{U}_{12} = \{\mathbf{8},\mathbf{5};\mathbf{2},\mathbf{1}\},$$

$$\mathcal{U}_{13} = \{\mathbf{8},\mathbf{4};\mathbf{6},\mathbf{1}\},\quad \mathcal{U}_{14} = \{\mathbf{8},\mathbf{4};\mathbf{5},\mathbf{3}\},\quad \mathcal{U}_{15} = \{\mathbf{8},\mathbf{4};\mathbf{5},\mathbf{2}\},\quad \mathcal{U}_{16} = \{\mathbf{8},\mathbf{4};\mathbf{2},\mathbf{1}\},$$

$$\mathcal{U}_{17} = \{\mathbf{8},\mathbf{3};\mathbf{6},\mathbf{1}\},\quad \mathcal{U}_{18} = \{\mathbf{8},\mathbf{3};\mathbf{5},\mathbf{2}\},\quad \mathcal{U}_{19} = \{\mathbf{8},\mathbf{3};\mathbf{4},\mathbf{2}\},\quad \mathcal{U}_{20} = \{\mathbf{8},\mathbf{3};\mathbf{4},\mathbf{1}\},$$

$$\mathcal{U}_{21} = \{\mathbf{8},\mathbf{2};\mathbf{6},\mathbf{1}\},\quad \mathcal{U}_{22} = \{\mathbf{8},\mathbf{2};\mathbf{5},\mathbf{3}\},\quad \mathcal{U}_{23} = \{\mathbf{8},\mathbf{2};\mathbf{4},\mathbf{3}\},\quad \mathcal{U}_{24} = \{\mathbf{8},\mathbf{2};\mathbf{4},\mathbf{1}\},$$

$$\mathcal{U}_{25} = \{\mathbf{8},\mathbf{1};\mathbf{5},\mathbf{3}\},\quad \mathcal{U}_{26} = \{\mathbf{8},\mathbf{1};\mathbf{5},\mathbf{2}\},\quad \mathcal{U}_{27} = \{\mathbf{8},\mathbf{1};\mathbf{4},\mathbf{3}\},\quad \mathcal{U}_{28} = \{\mathbf{8},\mathbf{1};\mathbf{4},\mathbf{2}\}.$$

Además, si consideramos las siguientes matrices binarias de tamaño 4×4

$$P_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},\quad P_2 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},\quad P_3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

$$P_4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},\quad P_5 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix},\quad P_6 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$P_7 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},\quad P_8 = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},\quad P_9 = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

$$P_{10} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

k	Segundos	Número de soportes
2	0,0276	2^5
3	0,2923	2^7
4	4,7412	2^9
5	74,5827	2^{11}
6	1215,0815	2^{13}
7	21347,9378	2^{15}

Tabla 3.3: *Para una base dada, tiempo (en segundos) para obtener todas las funciones bent de $2k$ variables para diferentes valores de k*

y si para $i = 1, 2, \ldots, 28$ y $j = 1, 2, \ldots, 10$, consideramos las nuevas bases

$$\mathcal{V}_{i,j} = \left\{ P_j \boldsymbol{u}_1^{(i)}, P_j \boldsymbol{u}_2^{(i)}; P_j \boldsymbol{u}_3^{(i)}, P_j \boldsymbol{u}_4^{(i)} \right\}$$

donde $\mathcal{U}_i = \{\boldsymbol{u}_1^{(i)}, \boldsymbol{u}_2^{(i)}; \boldsymbol{u}_3^{(i)}, \boldsymbol{u}_4^{(i)}\}$, entonces, las funciones bent proporcionadas por las bases $\mathcal{V}_{i,j}$ y $\mathcal{U}_i$, para $j = 1, 2, \ldots, 10$, son las mismas. Hay que tener en cuenta que no todas las bases $\mathcal{V}_{i,j}$ tienen las mismas propiedades que las bases $\mathcal{U}_i$ en el sentido de que $\left\{ P_j \boldsymbol{u}_1^{(i)}, P_j \boldsymbol{u}_2^{(i)} \right\}$ y $\left\{ P_j \boldsymbol{u}_3^{(i)}, P_j \boldsymbol{u}_4^{(i)} \right\}$ no son necesariamente bases de Gauss-Jordan de cardinalidad 2 y que no necesariamente $P_j \boldsymbol{u}_1^{(i)} > P_j \boldsymbol{u}_3^{(i)}$ (orden lexicográfico), pero tras algunas operaciones elementales, podemos obtener una base $\mathcal{V}'_{i,j}$ con tales propiedades.

Para $k = 3$ no es posible obtener una clasificación completa similar a la clasificación anterior para $k = 2$ porque el número de bases que satisfacen las condiciones necesarias es 15 554 560.

Finalmente, resumimos en la tabla 3.3, el tiempo requerido (en segundos) para obtener, en un ordenador personal estándar, los 2^{2k+1} soportes de funciones bent de $2k$ variables a partir de la misma base de $\mathbb{F}_2^n$ usando el procedimiento iterativo descrito en la sección 3.2. Vale la pena mencionar que el tiempo medio necesario para obtener aleatoriamente los soportes de 100 funciones bent de 4 variables (esto es, para $k = 2$) fue de 6,56 segundos; sin embargo, tras más de 250 horas de computación, no obtuvimos (aleatoriamente) ningún soporte correspondiente a una función bent de 6 variables (esto es, para $k = 3$).

3.4 Más resultados

En toda esta sección suponemos que k y l son dos enteros fijos tales que $3 \leq l < k$. Sea B_{2l} el conjunto de todas las funciones bent de $2l$ variables y denotemos por $\mathsf{B}_{2l}^{(1)}$ el conjunto de todas las funciones bent de $2l$ variables que podemos obtener mediante la construcción introducida en la sección 3.2. Claramente $\mathsf{B}_{2l}^{(1)} \subseteq \mathsf{B}_{2l}$ y, de acuerdo con lo dicho al final de dicha sección, la inclusión anterior es estricta, con lo que $\mathsf{B}_{2l}^{(2)} = \mathsf{B}_{2l} \setminus \mathsf{B}_{2l}^{(1)} \neq \emptyset$ es el conjunto de todas las funciones bent que no podemos obtener mediante dicha construcción. Sea $f \in \mathsf{B}_{2l}^{(2)}$ tal que $w(f) = 2^{2l-1} - 2^{l-1}$ y denotemos por A y $\widehat{A}$ los soportes de f y $1 \oplus f$ respectivamente.

Por otro lado, si identificamos el vector $\boldsymbol{v} \in \mathbb{F}_2^{2l}$ con el vector $(\mathbf{0}_{2(k-l)}, \boldsymbol{v}) \in \mathbb{F}_2^{2k}$, podemos suponer que $G_l = \mathbb{F}_2^{2l}$ es un subespacio vectorial de dimensión $2l$ de $\mathbb{F}_2^{2k}$. De esta forma, los subconjuntos A y $\widehat{A}$ de G_l satisfacen las propiedades:

- $G_l = A \cup \widehat{A}$ y $A \cap \widehat{A} = \emptyset$,
- $\mathrm{Card}\,(A) = 2^{2l-1} - 2^{l-1}$ y $\mathrm{Card}\left(\widehat{A}\right) = 2^{2l-1} + 2^{l-1}$.

Sea $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2l-1}, \boldsymbol{u}_{2l}\}$ una base de G_l y consideremos

$$\boldsymbol{u}_{2l+1}, \boldsymbol{u}_{2l+2}, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k} \in \mathbb{F}_2^{2k}$$

de manera que:

- $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2l-1}, \boldsymbol{u}_{2l}, \boldsymbol{u}_{2l+1}, \boldsymbol{u}_{2l+2}, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ es una base de $\mathbb{F}_2^{2k}$,
- $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$, para $i = l+1, l+2, \ldots, k$, es una base de Gauss-Jordan de cardinalidad 2,
- $\boldsymbol{u}_{2i-1} > \boldsymbol{u}_{2j-1}$ (en orden lexicográfico), si $l+1 \leq i < j \leq k$.

Para $i = l+1, l+2, \ldots, k$, consideramos los subespacios vectoriales

$$G_i = \mathrm{Env}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2l-1}, \boldsymbol{u}_{2l}, \ldots, \boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\},$$

$$H_i = \mathrm{Env}\,\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\},$$

de $\mathbb{F}_2^{2k}$. Claramente, $\dim G_i = 2i$ y $\dim H_i = 2$. Además,

$$G_i = G_{i-1} \oplus H_i \quad \text{y} \quad G_{i-1} \cap H_i = \{\mathbf{0}\},$$

con lo que G_i es la suma directa de G_{i-1} y H_i.

Igual que en la sección 3.2, por conveniencia en la notación, nos referiremos a los elementos de H_i, para $i = l+1, l+2, \ldots, k$, como

$$\boldsymbol{a}_0^{(i)} = \mathbf{0},\ \boldsymbol{a}_1^{(i)} = \boldsymbol{u}_{2i-1},\ \boldsymbol{a}_2^{(i)} = \boldsymbol{u}_{2i} \text{ y } \boldsymbol{a}_3^{(i)} = \boldsymbol{u}_{2i-1} \oplus \boldsymbol{u}_{2i}.$$

Para $p \in \{0,1,2,3\}$ consideramos los conjuntos

$$C(p) = \left(\boldsymbol{a}_p^{(l+1)} \oplus \widehat{A}\right) \cup \bigcup_{\substack{q=0 \\ q\neq p}}^{3} \left(\boldsymbol{a}_q^{(l+1)} \oplus A\right),$$

$$\widehat{C}(p) = \left(\boldsymbol{a}_p^{(l+1)} \oplus A\right) \cup \bigcup_{\substack{q=0 \\ q\neq p}}^{3} \left(\boldsymbol{a}_q^{(l+1)} \oplus \widehat{A}\right).$$

Ahora, si $(p_1, p_2, \ldots, p_{i-1}, p_i) \in \{0,1,2,3\}^i$ y suponemos que hemos definido los conjuntos $C(p_1, p_2, \ldots, p_{i-1})$ y $\widehat{C}(p_1, p_2, \ldots, p_{i-1})$, podemos definir

$$C(p_1, p_2, \ldots, p_{i-1}, p_i) = \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{C}(p_1, p_2, \ldots, p_{i-1})\right)$$

$$\cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus C(p_1, p_2, \ldots, p_{i-1})\right),$$

$$\widehat{C}(p_1, p_2, \ldots, p_{i-1}, p_i) = \left(\boldsymbol{a}_{p_i}^{(i)} \oplus C(p_1, p_2, \ldots, p_{i-1})\right)$$

$$\cup \bigcup_{\substack{q=0 \\ q\neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{C}(p_1, p_2, \ldots, p_{i-1})\right).$$

Así, mediante los mismos argumentos utilizados en la sección 3.2, es fácil comprobar que los lemas 3.1, 3.2 y 3.3 continúan siendo válidos si cambiamos los conjuntos $B(p_1, p_2, \ldots, p_{i-1}, p_i)$ y $\widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i)$ por los conjuntos $C(p_1, p_2, \ldots, p_{i-1}, p_i)$ y $\widehat{C}(p_1, p_2, \ldots, p_{i-1}, p_i)$ respectivamente. Además, el teorema 3.1 también es válido si cambiamos los conjuntos $B(p_1, p_2, \ldots, p_k)$ y $\widehat{B}(p_1, p_2, \ldots, p_k)$ por los conjuntos $C(p_1, p_2, \ldots, p_{k-l})$ y $\widehat{C}(p_1, p_2, \ldots, p_{k-l})$ respectivamente. Finalmente, el teorema 3.2 también permite afirmar que los soportes de las funciones bent de $2k$ variables obtenidas de esta forma son distintos de los soportes de las funciones bent de $2k$ variables obtenidos a partir de la construcción de la sección 3.2.

3.5 Conclusiones

En este capítulo hemos empleado una base de $\mathbb{F}_2^{2k}$ para construir 2^{2k+1} conjuntos en $\mathbb{F}_2^{2k}$ que son soportes de funciones bent de $2k$ variables. La mitad de las funciones bent obtenidas son funciones complementarias de la otra mitad.

Ponemos de manifiesto que dos bases distintas pueden proporcionar las mismas funciones bent y damos una clasificación completa para el caso $k = 2$; es decir, para las funciones bent de 4 variables. Sin embargo, no hemos podido establecer una clasificación análoga para $k > 2$, con lo que es necesario profundizar más en esta construcción para determinar bajo qué condiciones dos bases distintas proporcionan las mismas funciones bent.

Nuestra construcción permite obtener todas las funciones bent de 4 variables, pero no todas las funciones bent de más variables. Sin embargo, partiendo del soporte de una función bent de $2l$ variables, con $3 \leq l < k$, que no se pueda obtener con dicha construcción, podemos iniciar un proceso iterativo similar y otener más funciones bent. Estas nuevas funciones bent son distintas de las obtenidas con la construcción de la sección 3.2, pero no hemos podido establecer bajo qué condiciones se da la igualdad entre las funciones bent obtenidas. Esto será objeto de un trabajo posterior.

Capítulo 4

Construcción de funciones bent de clase $\mathcal{PS}$

4.1 Introducción

Utilizando una base de $\mathbb{F}_2^n$ (con n un número par) y la matriz asociada de un polinomio primitivo de grado $n/2$ y coeficientes en $\mathbb{F}_2$, construimos los soportes de algunas funciones bent de n variables que pertenecen a la clase $\mathcal{PS}$.

El capítulo está organizado de la siguiente manera. En la sección 4.2, introducimos algunas definiciones básicas y la notación utilizada. En la sección 4.3, presentamos un método general para caracterizar la construcción de funciones bent de n variables (con n un número par) de la clase $\mathcal{PS}$ utilizando una base de $\mathbb{F}_2^n$ y un polinomio primitivo de grado $n/2$ en $\mathbb{F}_2[\mathsf{X}]$. En la sección 4.4, introducimos un procedimiento práctico para la obtención del soporte de una función bent del tipo $\mathcal{PS}$, mostrando algunos ejemplos; además establecemos el número de dichos soportes que podemos construir con una base y un polinomio primitivo fijo; dicho número constituye, en definitiva, una cota inferior del número de funciones bent de n variables de la clase $\mathcal{PS}$. Finalmente, en la sección 4.5, presentamos algunos problemas abiertos relacionados con la construcción introducida en este capítulo.

4.2 Preliminares

Para una matriz cualquiera A de tamaño $n \times k$ con elementos en $\mathbb{F}_2$, denotamos por $\mathrm{Col}\,(A)$ el espacio vectorial generado por las columnas de A; por tanto, $\mathrm{Col}\,(A)$

es un subespacio vectorial de $\mathbb{F}_2^n$. En este capítulo, los vectores de $\mathbb{F}_2^n$ serán siempre vectores columna. Recordemos que la matriz de control de paridad H del $[2^k-1,k]$-código binario de Hamming es la matriz cuya i-ésima columna está formada por los k dígitos de la representación binaria del entero i para $1 \leq i \leq 2^k-1$ (véase [90]); por tanto, es evidente que los vectores de $\mathrm{Col}\,(A)$ son las columnas de la matriz AH.

Suponemos que $n = 2k$ y nos centramos en la obtención de funciones bent de la clase $\mathcal{PS}$. El teorema siguiente, al que haremos referencia en diversas ocasiones, introduce dicha clase de funciones bent (véase [46]).

Teorema 4.1: *Supongamos que $G_1, G_2, \ldots, G_t$ son subespacios vectoriales de $\mathbb{F}_2^n$ de dimensión k tales que $G_i \cap G_j = \{\mathbf{0}\}$ para $i, j = 1, 2, \ldots, t$ con $i \neq j$, y consideremos el conjunto*

$$B = \begin{cases} \bigcup_{i=1}^{t} G_i^*, & si \;\; t = 2^{k-1}, \\ \{\mathbf{0}\} \cup \bigcup_{i=1}^{t} G_i^*, & si \;\; t = 2^{k-1}+1, \end{cases}$$

con $G_i^* = G_i \setminus \{\mathbf{0}\}$. Entonces B es el soporte de una función bent de n variables.

Dillon [46] denotó por $\mathcal{PS}^-$ (respectivamente, $\mathcal{PS}^+$), la clase de funciones bent para la que $t = 2^{k-1}$ (respectivamente, $t = 2^{k-1}+1$).

Ahora, construimos funciones bent basadas en la clase $\mathcal{PS}$ utilizando los complementos ortogonales de los subespacios vectoriales en lugar de los propios subespacios. Pero primero recordemos que el **complemento ortogonal** de un subespacio vectorial G de $\mathbb{F}_2^n$, denotado por $G^\perp$, es el subespacio vectorial

$$G^\perp = \{\boldsymbol{y} \in \mathbb{F}_2^n \mid \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \text{ para todo } \boldsymbol{x} \in G\}.$$

El siguiente resultado, cuya demostración se puede encontrar en cualquier libro de álgebra lineal, será necesario para probar el corolario 4.1, que establece que los complementos ortogonales de los subespacios vectoriales satisfacen las condiciones necesarias para que los soportes que definen correspondan a funciones bent de la clase $\mathcal{PS}$.

Lema 4.1: *Si G y H son dos subespacios vectoriales de $\mathbb{F}_2^n$ tales que $G \cap H = \{\mathbf{0}\}$ y $\dim G = \dim H = k$, entonces*

$$G^\perp \cap H^\perp = \{\mathbf{0}\} \quad y \quad \dim G^\perp = \dim H^\perp = k.$$

Ahora, como consecuencia inmediata del lema anterior, tenemos el siguiente resultado.

Corolario 4.1: *Sean $G_1, G_2, \ldots, G_t$ subespacios vectoriales de $\mathbb{F}_2^n$ de dimensión k, tales que $G_i \cap G_j = \{\mathbf{0}\}$ para $i, j = 1, 2, \ldots, t$ con $i \neq j$. Si*

$$B^{(\perp)} = \begin{cases} \bigcup_{i=1}^{t} \left(G_i^\perp\right)^*, & \text{para } \ t = 2^{k-1}, \\ \{\mathbf{0}\} \cup \bigcup_{i=1}^{t} \left(G_i^\perp\right)^*, & \text{para } \ t = 2^{k-1} + 1, \end{cases}$$

con $\left(G_i^\perp\right)^* = G_i^\perp \backslash \{\mathbf{0}\}$, entonces $B^{(\perp)}$ es el soporte de una función bent de n variables.

Demostración: Para $i = 1, 2, \ldots, 2^{k-1} + 1$ tenemos que

$$\dim G_i^\perp = n - \dim G_i = k.$$

Además, si $\boldsymbol{x} \in G_i^\perp \cap G_j^\perp$, entonces

$$\langle \boldsymbol{x}, \boldsymbol{u} \rangle = \langle \boldsymbol{x}, \boldsymbol{v} \rangle = 0, \quad \text{para todo } \boldsymbol{u} \in G_i, \boldsymbol{v} \in G_j,$$

es decir,

$$\langle \boldsymbol{x}, \boldsymbol{u} \oplus \boldsymbol{v} \rangle = 0, \quad \text{para todo } \boldsymbol{u} \in G_i, \boldsymbol{v} \in G_j,$$

y por el lema 4.1,

$$\langle \boldsymbol{x}, \boldsymbol{w} \rangle = 0, \quad \text{para todo } \boldsymbol{w} \in \mathbb{F}_2^n.$$

Por tanto, $\boldsymbol{x} = \mathbf{0}$ y, en consecuencia $G_i^\perp \cap G_j^\perp = \{\mathbf{0}\}$.

Ahora, por el teorema 4.1 tenemos que $B^{(\perp)}$ es el soporte de una función bent de n variables. □

4.3 Resultados principales

Ya estamos en condiciones de construir, de forma explícita, los subespacios G_i del teorema 4.1. Para ello, primero consideraremos algunas bases del espacio columna de las matrices obtenidas a partir de dos matrices de tamaño $n \times k$ con coeficientes en $\mathbb{F}_2$ y cuyo rango es k y la matriz asociada a un polinomio primitivo de grado k en $\mathbb{F}_2[\mathsf{X}]$.

La demostración del siguiente lema es directa y por ello la omitimos.

Lema 4.2: *Supongamos que C es la matriz asociada al polinomio primitivo*

$$c_0 + c_1\mathsf{X} + c_2\mathsf{X}^2 + \cdots + c_{k-1}\mathsf{X}^{k-1} + \mathsf{X}^k \in \mathbb{F}_2[\mathsf{X}].$$

Supongamos también que la matriz $U = \begin{bmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_k \end{bmatrix}$ de tamaño $n \times k$ tiene rango k, y consideremos, para $j = 1, 2, \ldots, 2^k - 2$, el vector

$$\boldsymbol{u}_{j+k} = c_0\boldsymbol{u}_j \oplus c_1\boldsymbol{u}_{j+1} \oplus \cdots \oplus c_{k-1}\boldsymbol{u}_{j+k-1} \in \mathbb{F}_2^n.$$

Entonces, para $i = 1, 2, \ldots, 2^k - 1$,

$$UC^{i-1} = \begin{bmatrix} \boldsymbol{u}_i & \boldsymbol{u}_{i+1} & \cdots & \boldsymbol{u}_{i+k-1} \end{bmatrix} \quad y \quad \mathrm{Col}\,(U) = \mathrm{Col}\,\left(UC^{i-1}\right)$$

Notemos que como consecuencia de este resultado, tenemos que

$$\mathrm{rg}\left(UC^{i-1}\right) = k, \quad \text{para } i = 1, 2, \ldots, 2^k - 1$$

y, por tanto, las columnas de la matriz UC^{i-1} constituyen también una base de $\mathrm{Col}\,(U)$.

El teorema siguiente nos permite construir una familia de subespacios G_i que satisfacen las condiciones del teorema 4.1.

Teorema 4.2: *Sean U y V matrices de tamaño $n \times k$ tales que $\begin{bmatrix} U & V \end{bmatrix}$ es invertible y supongamos que C es la matriz asociada a un polinomio primitivo de grado k en*

$\mathbb{F}_2[\mathsf{X}]$. *Si* $G_0 = \mathrm{Col}\,(V)$, $G_{2^k} = \mathrm{Col}\,(U)$ *y*

$$G_i = \mathrm{Col}\left(UC^{i-1} \oplus V\right), \quad \textit{para } i = 1, 2, \ldots, 2^k - 1,$$

entonces $\dim G_r = k$, *y* $G_r \cap G_s = \{\mathbf{0}\}$ *para* $r, s = 0, 1, 2, \ldots, 2^k$ *con* $r \neq s$.

DEMOSTRACIÓN: Claramente $\dim U = \dim V = k$. Así, $\dim G_0 = \dim G_{2^k} = k$.

Si $\dim G_i < k$ para algún $i \in \{1, 2, \ldots, 2^k - 1\}$, entonces, existe $\boldsymbol{a} \in \mathbb{F}_2^k \setminus \{\mathbf{0}\}$ tal que

$$\left(UC^{i-1} \oplus V\right)\boldsymbol{a} = UC^{i-1}\boldsymbol{a} \oplus V\boldsymbol{a} = \begin{bmatrix} UC^{i-1} & V \end{bmatrix} \begin{bmatrix} \boldsymbol{a} \\ \boldsymbol{a} \end{bmatrix} = \mathbf{0}$$

pero esto es una contradicción ya que las columnas de la matriz $\begin{bmatrix} UC^{i-1} & V \end{bmatrix}$ forman una base de $\mathbb{F}_2^n$ de acuerdo con la elección de las matrices U y V y el lema 4.2. En consecuencia, $\dim G_i = k$ para $i = 1, 2, \ldots, 2^k - 1$.

Evidentemente, $G_0 \cap G_{2^k} = \{\mathbf{0}\}$.

Supongamos primero que $\boldsymbol{w} \in G_0 \cap G_i$ para algún $i \in \{1, 2, 3, \ldots, 2^{k-1} - 1\}$. Entonces, de acuerdo con el lema 4.2

$$\boldsymbol{w} = \left(UC^{i-1} \oplus V\right)\boldsymbol{a} \quad \text{y} \quad \boldsymbol{w} = V\boldsymbol{b}$$

para algunos $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^k$. Por tanto,

$$UC^{i-1}\boldsymbol{a} \oplus V\left(\boldsymbol{a} \oplus \boldsymbol{b}\right) = \begin{bmatrix} UC^{i-1} & V \end{bmatrix} \begin{bmatrix} \boldsymbol{a} \\ \boldsymbol{a} \oplus \boldsymbol{b} \end{bmatrix} = \mathbf{0} \tag{4.1}$$

y otra vez, como las columnas de la matriz $\begin{bmatrix} UC^{i-1} & V \end{bmatrix}$ forman una base de $\mathbb{F}_2^n$, de la expresión (4.1) podemos decir que

$$\boldsymbol{a} = \mathbf{0} \quad \text{y} \quad \boldsymbol{a} \oplus \boldsymbol{b} = \mathbf{0};$$

así que, $\boldsymbol{b} = \mathbf{0}$ con lo que $\boldsymbol{w} = \mathbf{0}$.

Por tanto, $G_0 \cap G_i = \{\mathbf{0}\}$ para $i \in \{1, 2, 3, \ldots, 2^k - 1\}$.

Supongamos ahora que $\boldsymbol{w} \in G_i \cap G_j$ para algunos i, j tales que $1 \leq i < j \leq 2^k - 1$. Procediendo como en el caso anterior, tenemos que

$$\boldsymbol{w} = \left(UC^{i-1} \oplus V\right)\boldsymbol{a} = \left(UC^{j-1} \oplus V\right)\boldsymbol{b}, \tag{4.2}$$

por tanto, de acuerdo con el lema 4.2, tenemos que

$$\mathbf{0} = \left(UC^{i-1} \oplus V\right) \boldsymbol{a} \oplus \left(UC^{j-1} \oplus V\right) \boldsymbol{b} = U\boldsymbol{d} \oplus V\left(\boldsymbol{a} \oplus \boldsymbol{b}\right) = \begin{bmatrix} U & V \end{bmatrix} \begin{bmatrix} \boldsymbol{d} \\ \boldsymbol{a} \oplus \boldsymbol{b} \end{bmatrix}$$

para algún $\boldsymbol{d} \in \mathbb{F}_2^k$. Sin embargo, como las columnas de la matriz $\begin{bmatrix} U & V \end{bmatrix}$ forman una base de $\mathbb{F}_2^n$, necesariamente

$$\boldsymbol{d} = \boldsymbol{a} \oplus \boldsymbol{b} = \mathbf{0}.$$

En particular, $\boldsymbol{a} = \boldsymbol{b}$ y, sustituyendo en la expresión (4.2), obtenemos que

$$UC^{i-1}\boldsymbol{a} = UC^{j-1}\boldsymbol{a}$$

y, por tanto, $\left(C^{j-i} \oplus I\right) \boldsymbol{a} = \mathbf{0}$ ya que $i < j$ y $\operatorname{rg}(U) = k$. Ahora, como C es la matriz asociada a un polinomio primitivo de grado k y $\mathbb{F}_{2^k}$ es isomorfo a $\mathbb{F}_2[C]$ (véase [66]), podemos afirmar que la matriz $C^{j-i} \oplus I$ es invertible y, en consecuencia, $\boldsymbol{a} = \mathbf{0}$. Por tanto, sustituyendo dicho valor en la expresión (4.2), tenemos que $\boldsymbol{w} = \mathbf{0}$ y así, $G_i \cap G_j = \{\mathbf{0}\}$.

Finalmente, supongamos que $\boldsymbol{w} \in G_{2^k} \cap G_i$ para algún $i \in \{1, 2, 3, \ldots, 2^k - 1\}$. Entonces, procediendo como en el caso anterior, tenemos que

$$\boldsymbol{w} = U\boldsymbol{b} \quad \text{y} \quad \boldsymbol{w} = \left(UC^{i-1} \oplus V\right) \boldsymbol{a}, \tag{4.3}$$

para algunos $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^k$. Por tanto, de acuerdo con el lema 4.2, tenemos que

$$\mathbf{0} = \left(UC^{i-1} \oplus V\right) \boldsymbol{a} \oplus U\boldsymbol{b} = U\boldsymbol{d} \oplus V\boldsymbol{a} = \begin{bmatrix} U & V \end{bmatrix} \begin{bmatrix} \boldsymbol{d} \\ \boldsymbol{a} \end{bmatrix}$$

para algún $\boldsymbol{d} \in \mathbb{F}_2^k$. Otra vez, como las columnas de la matriz $\begin{bmatrix} U & V \end{bmatrix}$ forman una base de $\mathbb{F}_2^n$, necesariamente $\boldsymbol{d} = \boldsymbol{a} = \mathbf{0}$, y, sustituyendo en la expresión (4.3), obtenemos que $\boldsymbol{w} = \mathbf{0}$. Por tanto, $G_{2^k} \cap G_i = \{\mathbf{0}\}$ para $i = 1, 2, \ldots, 2^k - 1$. □

En el teorema 4.2, podríamos haber considerado también los subespacios vectoriales

$$F_j = \operatorname{Col}\left(U \oplus VC^{j-1}\right) \quad \text{para } j = 1, 2, \ldots, 2^k - 1,$$

ya que satisfacen todas las condiciones necesarias siempre que $i + j \neq 2^k + 1$. Sin embargo, esto no es posible ya que cada uno de estos subespacios coincide con alguno de los subespacios G_i definidos en dicho teorema, como ponemos de manifiesto en el siguiente resultado.

Teorema 4.3: *Sean U y V matrices de tamaño $n \times k$ tales que $\begin{bmatrix} U & V \end{bmatrix}$ es invertible, supongamos que C es la matriz asociada a un polinomio primitivo de grado k en $\mathbb{F}_2[\mathsf{X}]$ y consideremos, para $i, j \in \{1, 2, \ldots, 2^k - 1\}$, los subespacios vectoriales*

$$G_i = \mathrm{Col}\left(UC^{i-1} \oplus V\right) \quad y \quad F_j = \mathrm{Col}\left(U \oplus VC^{j-1}\right).$$

Entonces para todo $i \in \{1, 2, \ldots, 2^k - 1\}$ existe un único $j \in \{1, 2, \ldots, 2^k - 1\}$ tal que $G_i = F_j$.

DEMOSTRACIÓN: Claramente $F_1 = G_1$.

Supongamos que $\boldsymbol{w} \in G_i$, para algún $i \in \{2, 3, \ldots, 2^k - 1\}$. Por el lema 4.2, tenemos que

$$\boldsymbol{w} = \left(UC^{i-1} \oplus V\right) \boldsymbol{a} \tag{4.4}$$

para algún $\boldsymbol{a} \in \mathbb{F}_2^k$. Sea $\boldsymbol{b} = C^{i-1}\boldsymbol{a}$, entonces, por ser C la matriz asociada a un polinomio primitivo de grado k, tenemos que

$$\boldsymbol{a} = C^{2^k-1}\boldsymbol{a} = C^{2^k-i}C^{i-1}\boldsymbol{a} = C^{2^k-i}\boldsymbol{b}.$$

Sustituyendo el valor de $\boldsymbol{a}$, obtenido anteriormente, en la expresión (4.4) tenemos que

$$\boldsymbol{w} = \left(UC^{i-1} \oplus V\right) C^{2^k-i}\boldsymbol{b} = \left(U \oplus VC^{2^k-i}\right) \boldsymbol{b}$$

con lo que $\boldsymbol{w} \in F_j$, con $j = 2^k + 1 - i$ y así $G_i \subseteq F_j$. Ahora, como $\dim G_i = \dim F_j$, necesariamente $G_i = F_j$.

Evidentemente $j \in \{2, 3, \ldots, 2^k - 1\}$. Además, si existe $l \in \{2, 3, \ldots, 2^k - 1\}$ tal que $G_i = F_l$, entonces, necesariamente $l = j$. □

Finalmente, como consecuencia de los teoremas 4.1 y 4.2 tenemos el siguiente resultado que nos permite construir el soporte de una función bent a partir de una base de $\mathbb{F}_2^n$ y la matriz asociada a un polinomio primitivo de grado k en $\mathbb{F}_2[\mathsf{X}]$.

Corolario 4.2: *Supongamos que*

$$\mathcal{A} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$$

es una base de $\mathbb{F}_2^n$ *y consideremos las matrices*

$$U = \begin{bmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_k \end{bmatrix} \quad y \quad V = \begin{bmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \cdots & \boldsymbol{v}_k \end{bmatrix}.$$

Supongamos también que C *es una matriz asociada a un polinomio primitivo de grado* k *en* $\mathbb{F}_2[\mathsf{X}]$*, y definamos los subespacios vectoriales* G_i*, para* $i = 0, 1, 2, \ldots, 2^k$*, como en el teorema 4.2. Si* $I \subseteq \{0, 1, 2, \ldots, 2^k\}$ *con* $\mathrm{Card}\,(I) = 2^{k-1}$ *(respectivamente,* $\mathrm{Card}\,(I) = 2^{k-1} + 1$*), entonces*

$$B = \bigcup_{i \in I} G_i^* \quad \left(\textit{respectivamente, } B = \{\mathbf{0}\} \cup \bigcup_{i \in I} G_i^* \right)$$

es el soporte de una función bent de n *variables.*

Ahora, con la notación del corolario 4.2, si $\mathrm{Card}\,(I) = 2^{k-1}$, consideramos el soporte y $J = \{0, 1, 2, \ldots, 2^k\} \setminus I$, y denotamos por $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ las funciones bent cuyos soportes son los conjuntos

$$B_I = \bigcup_{i \in I} G_i^* \quad \text{y} \quad B_J = \{\mathbf{0}\} \cup \bigcup_{j \in J} G_j^*,$$

respectivamente, entonces $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$.

4.4 Procedimiento práctico

A continuación, describimos un procedimiento práctico que nos permitirá construir los subespacios G_i del teorema 4.2 a partir de una base $\mathcal{A}$ de $\mathbb{F}_2^n$ y la matriz C asociada a un polinomio primitivo de grado k en $\mathbb{F}_2[\mathsf{X}]$. Supongamos pues, como en el corolario 4.2, que agrupamos los vectores de $\mathcal{A}$ en dos matrices U y V de dimensión $n \times k$. Así, de acuerdo con lo dicho en la sección 4.2, los vectores no nulos de G_0, G_i para $i = 1, 2, 3, \ldots, 2^k - 1$ y G_{2^k} son, respectivamente, las columnas de

las matrices

$$V_0 = VH, \quad V_i = (UC^{i-1} \oplus V)H \quad \text{y} \quad V_{2^k} = UH$$

donde H es la matriz de control de paridad del $[2^k-1, k]$-código binario de Hamming. Por tanto, si consideramos, por ejemplo, el conjunto $I = \{0, 1, 2, 3, \ldots, 2^{k-1} - 1\}$, entonces, de acuerdo con los teoremas 4.1 y 4.2 y lo dicho anteriormente, tenemos que las columnas de la matriz B

$$\begin{aligned} B &= \begin{bmatrix} V_0 & V_1 & V_2 & V_3 & \cdots & V_{2^{k-1}-1} \end{bmatrix} \\ &= \begin{bmatrix} VH & (U \oplus V)H & (UC \oplus V)H & (UC^2 \oplus V)H & \cdots & (UC^{2^{k-1}-2} \oplus V)H \end{bmatrix} \end{aligned}$$

constituyen el soporte de una función bent de n variables.

El siguiente ejemplo nos ayudará a entender el proceso anterior.

Ejemplo 4.1: Supongamos que $n = 6$ (y, por tanto, $k = 3$) y consideremos la base $\mathcal{A} = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{8}, \mathbf{16}, \mathbf{32}\}$ y las matrices

$$U = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{4} \end{bmatrix} \quad \text{y} \quad V = \begin{bmatrix} \mathbf{8} & \mathbf{16} & \mathbf{32} \end{bmatrix}.$$

Aquí

$$\mathbf{1} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad \mathbf{2} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{3} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \quad \ldots$$

y así sucesivamente; es decir, denotamos por $\boldsymbol{i}$ el vector columna correspondiente a la expansión binaria de 6 bits del entero i, para $i = 0, 1, 2, \ldots, 2^6 - 1$.

Consideremos el polinomio primitivo $p(\mathsf{X}) = 1 + \mathsf{X} + \mathsf{X}^3 \in \mathbb{F}_2[\mathsf{X}]$ y su matriz asociada

$$C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Finalmente, consideremos la matriz de control de paridad

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

del $[7, 3]$-código binario de Hamming.

De acuerdo con el proceso anteriormente descrito, tenemos que

$$\begin{aligned} V_0 = VH &= \begin{bmatrix} \mathbf{8} & \mathbf{16} & \mathbf{32} \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{32} & \mathbf{16} & \mathbf{48} & \mathbf{8} & \mathbf{40} & \mathbf{24} & \mathbf{56} \end{bmatrix}, \\ V_1 = (U \oplus V)H &= \begin{bmatrix} \mathbf{9} & \mathbf{18} & \mathbf{36} \end{bmatrix} H \\ &= \begin{bmatrix} \mathbf{36} & \mathbf{18} & \mathbf{54} & \mathbf{9} & \mathbf{45} & \mathbf{27} & \mathbf{63} \end{bmatrix}, \\ V_2 = (UC \oplus V)H &= \begin{bmatrix} \mathbf{10} & \mathbf{20} & \mathbf{35} \end{bmatrix} H \\ &= \begin{bmatrix} \mathbf{35} & \mathbf{20} & \mathbf{55} & \mathbf{10} & \mathbf{41} & \mathbf{30} & \mathbf{61} \end{bmatrix}, \\ V_3 = (UC^2 \oplus V)H &= \begin{bmatrix} \mathbf{12} & \mathbf{19} & \mathbf{38} \end{bmatrix} H \\ &= \begin{bmatrix} \mathbf{38} & \mathbf{19} & \mathbf{53} & \mathbf{12} & \mathbf{42} & \mathbf{31} & \mathbf{57} \end{bmatrix}. \end{aligned}$$

Por tanto, las columnas de la matriz

$$B = \begin{bmatrix} V_0 & V_1 & V_2 & V_3 \end{bmatrix}$$

son los elementos del soporte de una función bent de 6 variables.

Si obtenemos las $2^3 + 1 = 9$ matrices V_i, podemos construir $\binom{2^3+1}{2^{3-1}} = 126$ funciones bent pertenecientes a la clase $\mathcal{PS}^-$ y 126 funciones bent pertenecientes a la clase $\mathcal{PS}^+$, siendo todas ellas distintas. ■

Fijada una base $\mathcal{A}$ de $\mathbb{F}_2^n$ y un polinomio primitivo de grado k y coeficientes en $\mathbb{F}_2$, podemos considerar $\binom{2^k+1}{2^{k-1}}$ subconjuntos I de $\{0, 1, 2, \ldots, 2^k\}$ de 2^{k-1} elementos

y la misma cantidad de subconjuntos de $2^{k-1}+1$ elementos. Por tanto, de acuerdo con el teorema 4.2, podemos construir $2\binom{2^k+1}{2^{k-1}}$ soportes de funciones bent, que serán distintos dos a dos ya que si $i, j \in \{0, 1, 2, \ldots, 2^k\}$ con $i \neq j$, entonces $V_i \neq V_j$.

4.5 Problemas abiertos

Ya hemos comentado al final de la sección anterior que fijada una base de $\mathbb{F}_2^n$ y un polinomio primitivo de grado k y coeficientes en $\mathbb{F}_2$, de acuerdo con el teorema 4.2, podemos construir $2\binom{2^k+1}{2^{k-1}}$ soportes de funciones bent que son distintos dos a dos. Surge ahora, de modo natural, la pregunta siguiente: si fijamos una base distinta, ¿son distintos de los anteriores los $2\binom{2^k+1}{2^{k-1}}$ soportes de funciones bent construidos de acuerdo con el corolario 4.1? El ejemplo siguiente pone de manifiesto que la respuesta no es necesariamente afirmativa.

Ejemplo 4.2: Supongamos que $n = 4$ (y, por tanto, $k = 2$) y consideremos la base $\mathcal{A} = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{8}\}$ y las matrices $U = \begin{bmatrix} \mathbf{1} & \mathbf{2} \end{bmatrix}$ y $V = \begin{bmatrix} \mathbf{4} & \mathbf{8} \end{bmatrix}$. Consideremos el polinomio primitivo $p(\mathsf{X}) = 1 + \mathsf{X} + \mathsf{X}^2 \in \mathbb{F}_2[\mathsf{X}]$, su matriz asociada C, y la matriz de control de paridad H del $[3, 2]$-código binario de Hamming.

De acuerdo con lo dicho al inicio de la sección 4.4, tenemos que

$$V_0 = VH = \begin{bmatrix} \mathbf{4} & \mathbf{8} \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{8} & \mathbf{4} & \mathbf{12} \end{bmatrix},$$

$$V_1 = (U \oplus V)H = \begin{bmatrix} \mathbf{10} & \mathbf{5} & \mathbf{15} \end{bmatrix},$$

$$V_2 = (UC \oplus V)H = \begin{bmatrix} \mathbf{11} & \mathbf{6} & \mathbf{13} \end{bmatrix},$$

$$V_3 = (UC^2 \oplus V)H = \begin{bmatrix} \mathbf{9} & \mathbf{7} & \mathbf{14} \end{bmatrix},$$

$$V_4 = UH = \begin{bmatrix} \mathbf{2} & \mathbf{1} & \mathbf{3} \end{bmatrix}.$$

Por tanto, al aplicar el corolario 4.2 a cada uno de los subconjuntos I de $\{0, 1, 2, 3, 4\}$ de 2 elementos (análogamente para los de 3 elementos), obtenemos que cada uno de los conjuntos

$$B_1 = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{8}, \mathbf{12}\}, \quad B_2 = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{10}, \mathbf{15}\},$$

$$B_3 = \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{6},\mathbf{11},\mathbf{13}\}, \quad B_4 = \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{7},\mathbf{9},\mathbf{14}\},$$
$$B_5 = \{\mathbf{4},\mathbf{5},\mathbf{8},\mathbf{10},\mathbf{12},\mathbf{15}\}, \quad B_6 = \{\mathbf{4},\mathbf{6},\mathbf{8},\mathbf{11},\mathbf{12},\mathbf{13}\},$$
$$B_7 = \{\mathbf{4},\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{12},\mathbf{14}\}, \quad B_8 = \{\mathbf{5},\mathbf{6},\mathbf{10},\mathbf{11},\mathbf{13},\mathbf{15}\},$$
$$B_9 = \{\mathbf{5},\mathbf{7},\mathbf{9},\mathbf{10},\mathbf{14},\mathbf{15}\}, \quad B_{10} = \{\mathbf{6},\mathbf{7},\mathbf{9},\mathbf{11},\mathbf{13},\mathbf{14}\},$$

es el soporte de una función bent de la clase $\mathcal{PS}^-$ de 4 variables.

Si calculamos los complementos ortogonales de los subespacios vectoriales cuyos vectores no nulos son las columnas de las matrices V_i, es decir, de los subespacios G_i del teorema 4.2, obtenemos los subespacios ortogonales

$$G_0^\perp = \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}, \quad G_1^\perp = \{\mathbf{0},\mathbf{5},\mathbf{10},\mathbf{15}\},$$
$$G_2^\perp = \{\mathbf{0},\mathbf{7},\mathbf{9},\mathbf{14}\}, \quad G_3^\perp = \{\mathbf{0},\mathbf{6},\mathbf{11},\mathbf{13}\},$$
$$G_4^\perp = \{\mathbf{0},\mathbf{4},\mathbf{8},\mathbf{12}\}.$$

Puesto que

$$G_0^\perp = G_4, \quad G_1^\perp = G_1, \quad G_2^\perp = G_3,$$
$$G_3^\perp = G_2 \text{ y } G_4^\perp = G_0,$$

es evidente que cada uno de los soportes construidos de acuerdo con el corolario 4.1 coincide con alguno de los soportes construidos de acuerdo con el teorema 4.1.

Consideremos ahora la base $\mathcal{A}' = \{\mathbf{9},\mathbf{11},\mathbf{12},\mathbf{4}\}$ y las matrices $U' = \begin{bmatrix}\mathbf{9} & \mathbf{11}\end{bmatrix}$ y $V' = \begin{bmatrix}\mathbf{12} & \mathbf{4}\end{bmatrix}$.

Procediendo como en el caso anterior, tenemos que

$$V_0' = \begin{bmatrix}\mathbf{4} & \mathbf{12} & \mathbf{8}\end{bmatrix}, \quad V_1' = \begin{bmatrix}\mathbf{15} & \mathbf{5} & \mathbf{10}\end{bmatrix},$$
$$V_2' = \begin{bmatrix}\mathbf{6} & \mathbf{7} & \mathbf{1}\end{bmatrix}, \quad V_3' = \begin{bmatrix}\mathbf{13} & \mathbf{14} & \mathbf{3}\end{bmatrix},$$
$$V_4' = \begin{bmatrix}\mathbf{11} & \mathbf{9} & \mathbf{2}\end{bmatrix}$$

y, por tanto, cada uno de los conjuntos

$$B_1' = \{\mathbf{1},\mathbf{2},\mathbf{6},\mathbf{7},\mathbf{9},\mathbf{11}\}, \quad B_2' = \{\mathbf{1},\mathbf{3},\mathbf{6},\mathbf{7},\mathbf{13},\mathbf{14}\},$$

$$B'_3 = \{\mathbf{1},\mathbf{4},\mathbf{6},\mathbf{7},\mathbf{8},\mathbf{12}\}, \quad B'_4 = \{\mathbf{1},\mathbf{5},\mathbf{6},\mathbf{7},\mathbf{10},\mathbf{15}\},$$
$$B'_5 = \{\mathbf{2},\mathbf{3},\mathbf{9},\mathbf{11},\mathbf{13},\mathbf{14}\}, \quad B'_6 = \{\mathbf{2},\mathbf{4},\mathbf{8},\mathbf{9},\mathbf{11},\mathbf{12}\},$$
$$B'_7 = \{\mathbf{2},\mathbf{5},\mathbf{9},\mathbf{10},\mathbf{11},\mathbf{15}\}, \quad B'_8 = \{\mathbf{3},\mathbf{4},\mathbf{8},\mathbf{12},\mathbf{13},\mathbf{14}\},$$
$$B'_9 = \{\mathbf{3},\mathbf{5},\mathbf{10},\mathbf{13},\mathbf{14},\mathbf{15}\}, \quad B'_{10} = \{\mathbf{4},\mathbf{5},\mathbf{8},\mathbf{10},\mathbf{12},\mathbf{15}\},$$

es el soporte de una función bent de la clase $\mathcal{PS}^-$ de 4 variables.

Ahora, si calculamos, como antes, los complementos ortogonales de los subespacios vectoriales cuyos vectores no nulos son las columnas de las matrices V'_i, es decir, de los subespacios G'_i del teorema 4.2, obtenemos los subespacios ortogonales

$$(G'_0)^\perp = \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}, \quad (G'_1)^\perp = \{\mathbf{0},\mathbf{5},\mathbf{10},\mathbf{15}\},$$
$$(G'_2)^\perp = \{\mathbf{0},\mathbf{6},\mathbf{8},\mathbf{14}\}, \quad (G'_3)^\perp = \{\mathbf{0},\mathbf{7},\mathbf{11},\mathbf{12}\},$$
$$(G'_4)^\perp = \{\mathbf{0},\mathbf{4},\mathbf{9},\mathbf{13}\},$$

que proporcionan los siguientes soportes de funciones bent de la clase $\mathcal{PS}^-$ de 4 variables:

$$(B'_1)^\perp = \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{9},\mathbf{13}\},$$
$$(B'_2)^\perp = \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{5},\mathbf{10},\mathbf{15}\},$$
$$(B'_3)^\perp = \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{6},\mathbf{8},\mathbf{14}\},$$
$$(B'_4)^\perp = \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{7},\mathbf{11},\mathbf{12}\},$$
$$(B'_5)^\perp = \{\mathbf{4},\mathbf{5},\mathbf{9},\mathbf{10},\mathbf{13},\mathbf{15}\},$$
$$(B'_6)^\perp = \{\mathbf{4},\mathbf{6},\mathbf{8},\mathbf{9},\mathbf{13},\mathbf{14}\},$$
$$(B'_7)^\perp = \{\mathbf{4},\mathbf{7},\mathbf{9},\mathbf{11},\mathbf{12},\mathbf{13}\},$$
$$(B'_8)^\perp = \{\mathbf{5},\mathbf{7},\mathbf{10},\mathbf{11},\mathbf{12},\mathbf{15}\},$$
$$(B'_9)^\perp = \{\mathbf{5},\mathbf{6},\mathbf{8},\mathbf{10},\mathbf{14},\mathbf{15}\},$$
$$(B'_{10})^\perp = \{\mathbf{6},\mathbf{7},\mathbf{8},\mathbf{11},\mathbf{12},\mathbf{14}\}.$$

Notemos que en este caso, a diferencia de lo que ocurría en el caso anterior, ninguno de los conjuntos $(B'_j)^\perp$ coincide con ninguno de los conjuntos B'_i. ■

Tal como se desprende del ejemplo anterior, y en todos los ejemplos que hemos comprobado, existen bases para las que cada uno de los soportes B coincide con alguno de los soportes $B^{(\perp)}$ y existen bases para las que ninguno de los soportes B coincide con ninguno de los soportes $B^{(\perp)}$. Este hecho sugiere los problemas siguientes: ¿Fijada una base cualquiera, son éstas las dos únicas situaciones posibles? En caso afirmativo, ¿bajo qué condiciones se da cada una de dichas situaciones?

Además, si observamos de nuevo el ejemplo 4.2, vemos que $B_5 = B'_{10}$, es decir, solamente uno de los soportes obtenidos con la base $\mathcal{A}$ coincide con uno de los soportes obtenidos con la base $\mathcal{A}'$. No ocurre lo mismo si consideramos las bases $\mathcal{A}$ y $\mathcal{A}'' = \{\mathbf{1}, \mathbf{2}, \mathbf{5}, \mathbf{10}\}$, ya que en este caso, todos los soportes obtenidos con la base $\mathcal{A}$ coinciden con los soportes obtenidos con la base $\mathcal{A}''$. De nuevo, en todos los ejemplos que hemos comprobado se da alguna de estas dos situaciones, lo cual sugiere los problemas siguientes: ¿Dadas dos bases cualquieras, son estas las dos únicas situaciones posibles? En caso afirmativo, ¿bajo qué condiciones se da cada una de dichas situaciones?

Otro problema que aparece en esta construcción es si influye o no el polinomio primitivo considerado. Es decir, ¿para una misma base y polinomios primitivos diferentes, podemos obtener idénticas funciones bent? ¿y si consideramos bases y polinomios diferentes?

Estos y otros problemas que puedan surgir de esta construcción se abordarán en futuros trabajos.

Bibliografía

[1] C. M. Adams. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes and Cryptography*, **12**: 283–316 (1997). 1

[2] C. M. Adams y S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, **35(6)**: 1170–1173 (1990). 3

[3] C. M. Adams y S. E. Tavares. Generating bent sequences. *Discrete Applied Mathematics*, **39**: 155–159 (1992). 3

[4] D. A. M. Barrington, R. Beigel y S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Computational Complexity*, **4(4)**: 367–382 (1998). 2

[5] T. P. Berger, A. Canteaut, P. Charpin y Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, **52(9)**: 4160–4170 (2006). 3

[6] Y. Borissov, A. Braeken, S. Nikova y B. Preneel. On the covering radius of second order binary Reed-Muller code in the set of resilient Boolean functions. En K. G. Paterson (editor), *Cryptography and Coding*, volumen 2898 de *Lecture Notes in Computer Science*, páginas 82–92. Springer-Verlag, Berlin, 2003. 5

[7] Y. Borissov, A. Braeken, S. Nikova y B. Preneel. On the covering radii of binary Reed-Muller codes in the set of resilient Boolean functions. *IEEE Transactions on Information Theory*, **51(3)**: 1182–1189 (2005). 1

[8] A. Braeken, V. Nikov, S. Nikova y B. Preneel. On Boolean functions with generalized cryptographic properties. En A. Canteaut y K. Viswanathan (editores), *Progress in Cryptology – INDOCRYPT 2004*, volumen 3348 de *Lecture Notes in Computer Science*, páginas 120–135. Springer-

Verlag, Berlin, 2004. 1

[9] A. Canteaut y P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, **49(8)**: 2004–2019 (2003). 3, 4

[10] A. Canteaut, M. Daum, H. Dobbertin y G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, **154**: 202–218 (2006). 8

[11] C. Carlet y Y. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, **25**: 263–279 (2002). 1

[12] C. Carlet. On the secondary constructions of resilient and bent functions. *Progress in Computer Science and Applied Logic*, **23**: 3–28 (2004). 16

[13] C. Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. En M. Fossorier, H. Imai, S. Lin y A. Poli (editores), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-16)*, volumen 3857 de *Lecture Notes in Computer Science*, páginas 1–28. Springer-Verlag, Berlin, 2006. 3

[14] C. Carlet. Boolean functions for cryptography and error-correcting codes. En Y. Crama y P. Hammer (editores), *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, capítulo 8, páginas 257–397. Cambridge University Press, 2010. 13

[15] C. Carlet, H. Dobbertin y G. Leander. Normal extensions of bent functions. *IEEE Transactions on Information Theory*, **50(11)**: 2880–2885 (2004). 6

[16] C. Carlet y P. Guillot. A characterization of binary bent functions. *Journal of Combinatorial Theory (Series A)*, **76**: 328–335 (1996). 4

[17] C. Carlet y P. Guillot. An alternate characterization of the bentness of binary functions, with uniqueness. *Designs, Codes and Cryptography*, **14**: 133–140 (1998). 3

[18] D. K. Chang. Binary bent sequences of order 64. *Utilitas Mathematica*, **52**: 141–151 (1997). 4, 6

[19] C. Charnes, M. Rötteler y T. Beth. On homogeneous bent functions. En S. Boztaş y I. E. Shparlinski (editores), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-14)*, volumen 2227 de *Lecture Notes in Computer Science*, páginas 249–259. Springer-Verlag, Berlin, 2001. 5

[20] C. Charnes, M. Rötteler y T. Beth. Homogeneous bent functions, in-

variants, and designs. *Designs, Codes and Cryptography*, **26**: 139–154 (2002). 1, 5

[21] P. Charpin, E. Pasalic y C. Tavernier. On bent and semi-bent quadratic Boolean functions. *IEEE Transactions on Information Theory*, **51(12)**: 4286–4298 (2005). 4

[22] J.-J. Climent, F. J. García y V. Requena. Construcción de funciones bent de $n+2$ variables a partir de las funciones duales de funciones bent de n variables. En A. Castro, J. Liporace y J. Ramió (editores), *Anales del IV Congreso Iberoamericano de Seguridad Informática (CIBSI 2007)*, páginas 3–17. Universidad Católica de Salta, Argentina, 2007. xiv, 6

[23] J.-J. Climent, F. J. García y V. Requena. Some constructions of bent functions of $n+2$ variables from bent functions of n variables. En J.-F. Michon, P. Valarcher y J.-B. Yunès (editores), *Proceedings of the 3rd International Conference on Boolean Functions: Cryptography and Applications*, páginas 57–72. Université Denis Diderot (París 7), Paris, France, 2007. xiv, 6

[24] J.-J. Climent, F. J. García y V. Requena. Caracterización y construcción de funciones bent de $n+1$ variables a partir de funciones booleanas de n variables. En L. Hernández Encinas y A. Martín del Rey (editores), *Actas X Reunión Española sobre Criptología y Seguridad de la Información*, páginas 133–140. Salamanca, España, 2008. xiv, 6

[25] J.-J. Climent, F. J. García y V. Requena. New bent functions from positive and negative functions of old bent functions. En U. Speidel y H. Yokoo (editores), *Proceedings of the 2008 International Symposium on Information Theory and its Applications (ISITA2008)*, páginas 1344–1349. IEEE Press, 2008. xiv

[26] J.-J. Climent, F. J. García y V. Requena. On the characterization and construction of bent functions of $n+1$ variables from Boolean functions of n variables. En A. Ibeas y J. Gutiérrez (editores), *Extended Abstracts of the Second Workshop on Mathematical Cryptology (WMC2008)*, páginas 11–14. Santander, España, 2008. xiv, 6

[27] J.-J. Climent, F. J. García y V. Requena. On the construction of bent functions of $n+2$ variables from bent functions of n variables. *Advances in Mathematics of Communications*, **2(4)**: 421–431 (2008). xiv, 6

[28] J.-J. Climent, F. J. García y V. Requena. Construcción de funciones

bent a partir de una función bent y de sus traslaciones cíclicas basadas en bases de Gauss-Jordan de cardinalidad 2. En *Actas del XXI Congreso de Ecuaciones Diferenciales y Aplicaciones / XI Congreso de Matemática Aplicada*, páginas 1–8. Ediciones de la Universidad de Castilla-La Mancha, Ciudad Real, España, 2009. xiv

[29] J.-J. Climent, F. J. García y V. Requena. Sobre algunas construcciones de funciones bent. En P. Abascal, J. M. Miret, D. Sadornil y J. G. Tena (editores), *Nuevos Avances en Criptografía y Codificación de la Información*, páginas 43–52. Ediciones y Publicaciones de la UdL, Lleida, 2009. xiv, 6

[30] J.-J. Climent, F. J. García y V. Requena. Sobre el número de funciones bent obtenidas a partir de funciones de máximo peso. En G. Betarte, J. Ramió y A. Ribagorda (editores), *Actas del V Congreso Iberoamericano de Seguridad Informática (CIBSI 2009)*, páginas 133–147. Universidad de la República, Uruguay, Montevideo, Uruguay, 2009. xiv

[31] J.-J. Climent, F. J. García y V. Requena. Cálculo del grado de una función booleana a partir de su soporte. En J. Domingo Ferrer, A. Martínez Ballesté, J. Castellà Roca y A. Solanas Gómez (editores), *Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI2010)*, páginas 7–12. Publicacions URV, Tarragona, 2010. xiv

[32] J.-J. Climent, F. J. García y V. Requena. Computing the degree of a Boolean function from its support. En C.-C. Chao y R. Kohno (editores), *Proceedings of the 2010 International Symposium on Information Theory and its Applications (ISITA2010)*, páginas 123–128. IEEE Press, 2010. xiv, 20

[33] J.-J. Climent, F. J. García y V. Requena. Construcción de funciones bent de n variables a partir de una base de $\mathbb{F}_2^n$. En J. Domingo Ferrer, A. Martínez Ballesté, J. Castellà Roca y A. Solanas Gómez (editores), *Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI2010)*, páginas 13–18. Publicacions URV, Tarragona, 2010. xiv

[34] J.-J. Climent, F. J. García y V. Requena. On the characterization and construction of bent functions of $n+1$ variables from Boolean functions of n variables. Submitted. xiv, 6

[35] J.-J. Climent, F. J. García y V. Requena. On the construction of new

bent functions from the max-weight functions of old bent functions. Submitted. xiv, 6

[36] J.-J. Climent, F. J. García y V. Requena. Some algebraic properties related to the degree of a Boolean function. En J. Vigo Aguiar (editor), *Proceedings of the 10th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2010)*, páginas 373–384. 2010. xiv, 20

[37] J.-J. Climent, F. J. García y V. Requena. Construction of bent functions of n variables from a basis of $\mathbb{F}_2^n$. En J. Vigo Aguiar (editor), *Proceedings of the 11th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2011)*, páginas 350–356. 2011. xiv

[38] J.-J. Climent, F. J. García y V. Requena. Construction of bent functions of $2k$ variables from a basis of $\mathbb{F}_2^{2k}$. *International Journal of Computer Mathematics*, **89(7)**: 863–880 (2012). xiv

[39] J.-J. Climent, F. J. García y V. Requena. Some algebraic properties of the support of a Boolean function related to its degree. Submitted. xiv

[40] J.-J. Climent, F. J. García y V. Requena. Una nueva construcción de funciones bent de $2k$ variables a partir de una base de $\mathbb{F}_2^{2k}$. En U. Zurutuza, R. Uribeetxeberria y I. Arenaza-Nuño (editores), *Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI2012)*, páginas 93–98. Servicio Editorial de Mondragon Unibertsitatea, Arrasate - Mondragon, 2012. xiv

[41] J.-J. Climent, F. J. García y V. Requena. The degree of a Boolean function and some algebraic properties of its support. *WIT Transactions on Information and Communication Technologies*, **45**: 25–36 (2013). xiv

[42] J.-J. Climent, F. J. García y V. Requena. A construction of bent functions of $n+2$ variables from a bent function of n variables and its cyclic shifts. *Algebra*, **2014(Article ID 701298)**: 11 pages. (2014). xiv, 6

[43] T. W. Cusick y P. Stănică. *Cryptographic Boolean Functions and Applications*. Academic Press, San Diego, CA, 2009. 13

[44] M. Daum, H. Dobbertin y G. Leander. An algorithm for checking normality of Boolean functions. En *Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003)*, páginas 133–142. marzo 2003. 8

[45] E. Dawson y C.-K. Wu. Construction of correlation immune Boolean func-

tions. En Y. Han, T. Okamoto y S. Qing (editores), *Information and Communications Security – ICIS '97*, volumen 1334 de *Lecture Notes in Computer Science*, páginas 170–180. Springer-Verlag, Berlin, 1997. 1, 37

[46] J. F. Dillon. *Elementary Hadamard Difference Sets*. Tesis Doctoral, University of Maryland, 1974. 3, 16, 17, 78

[47] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. En B. Preneel (editor), *Fast Sofware Encription*, volumen 1008 de *Lecture Notes in Computer Science*, páginas 61–74. Springer-Verlag, Berlin, 1995. 5

[48] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case. *IEEE Transactions on Information Theory*, **45(4)**: 1271–1275 (1999). 4

[49] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke y P. Gaborit. Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory (Series A)*, **113(5)**: 779–798 (2004). 3

[50] J. Fuller, E. Dawson y W. Millan. Evolutionary generation of bent functions for cryptography. En *Proceedings of the 2003 Congress on Evolutionary Computation*, volumen 2, páginas 1655–1661. IEEE, 2003. 3

[51] J. Gonda. Transformation of the canonical disjunctive normal form of a Boolean function to its Zhegalkin-polynomial and back. *Annals of Discrete Mathematics*, **19**: 147–164 (2001). 2

[52] K. C. Gupta y P. Sarkar. Improved construction of nonlinear resilient S-boxes. *IEEE Transactions on Information Theory*, **51(1)**: 339–348 (2005). 1

[53] M. K. Habib. Boolean matrix representation for the conversion of minterms to Reed-Muller coefficients and the minimization of Exclusiove-OR switching functions. *Internationa Journal of Electronics*, **68(4)**: 493–506 (1990). 2

[54] X.-D. Hou. $GL(m, 2)$ acting on $R(r, m)/R(r-1, m)$. *Discrete Mathematics*, **149**: 99–122 (1996). 4

[55] X.-D. Hou. Cubic bent functions. *Discrete Mathematics*, **189**: 149–161 (1998). 5

[56] X.-D. Hou. On the coefficients of binary bent functions. *Proceedings of the American Mathematical Society*, **128(4)**: 987–996 (1999). 4

[57] X.-D. Hou y P. Langevin. Results on bent functions. *Journal of Combinatorial Theory (Series A)*, **80**: 232–246 (1997). 4

[58] K. Khoo, G. Gong y D. R. Stinson. A new characterization of semi-bent and bent functions on finite fields. *Designs, Codes and Cryptography*, **38**: 279–295 (2006). 4

[59] P. V. Kumar, R. A. Scholtz y L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory (Series A)*, **40**: 90–107 (1985). 3, 16

[60] K. Kurosawa, T. Iwata y T. Yoshiwara. New covering radius of Reed-Muller codes for t-resilient functions. *IEEE Transactions on Information Theory*, **50(3)**: 468–475 (2004). 1, 12

[61] K. Kurosawa y R. Matsumoto. Almost security of cryptographic Boolean functions. *IEEE Transactions on Information Theory*, **50(11)**: 2752–2761 (2004). 1

[62] K. Kurosawa y T. Satoh. Design of $SAC/PC(l)$ of order k Boolean functions and three other cryptographic criteria. En W. Fumy (editor), *Advances in Cryptology – EUROCRYPT '97*, volumen 1233 de *Lecture Notes in Computer Science*, páginas 434–449. Springer-Verlag, Berlin, 1997. 1, 37

[63] P. Langevin y G. Leander. Counting all bent functions in dimension eight. Submitted (Presented at the 2009 International Workshop on Coding and Cryptography. May 10–15, 2009. Ullensvang (Norway)). 6

[64] N. G. Leander. *Normality of Bent Functions Monomial- and Binomial-Bent Functions*. Tesis Doctoral, Ruhr Universität Bochum, noviembre 2004. 3

[65] A. Lempel y M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, **28(6)**: 865–868 (1982). 3

[66] R. Lidl. On cryptosystems based on polynomials and finite fields. En T. Beth, N. Cot y I. Ingemarsson (editores), *Advances in Cryptography – EUROCRYPT'84*, volumen 209 de *Lecture Notes in Computer Science*, páginas 10–15. Springer-Verlag, Berlin, 1985. 82

[67] F. J. MacWilliams y N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 6ª edición, 1988. 20

[68] S. Maity y S. Maitra. Minimum distance between bent and 1-resilient Boolean functions. En B. Roy y W. Meier (editores), *Fast Software Encryption – FSE 2004*, volumen 3017 de *Lecture Notes in Computer Science*, páginas 143–160. Springer-Verlag, Berlin, 2004. 5

[69] R. Matsumoto, K. Kurosawa, T. Itoh, T. Konno y T. Uyematsu.

Primal-dual distance bounds of linear codes with application to cryptography. *IEEE Transactions on Information Theory*, **52(9)**: 4251–4256 (2006). 1, 37

[70] R. L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, **15**: 1–10 (1973). xiii, 3

[71] W. Meier, E. Pasalic y C. Carlet. Algebraic attacks and decomposition of Boolean functions. En C. Cachin y J. Camenisch (editores), *Advances in Cryptology – EUROCRYPT 2004*, volumen 3027 de *Lecture Notes in Computer Science*, páginas 474–491. Springer-Verlag, Berlin, 2004. 2

[72] W. Meier y O. Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, **1(3)**: 159–176 (1989). 3

[73] W. Meier y O. Staffelbach. Nonlinearity criteria for cryptographic functions. En J. J. Quisquater y J. Vandewalle (editores), *Advances in Cryptology – EUROCRYPT'89*, volumen 434 de *Lecture Notes in Computer Science*, páginas 549–562. Springer-Verlag, Berlin, 1990. 1, 13, 14

[74] W. Millan. How to improve the nonlinearity of bijective S-boxes. En C. Boyd y E. Dawson (editores), *Proceedings of the Australasian Conference on Information Security and Privacy – ACISP'98*, volumen 1438 de *Lecture Notes in Computer Science*, páginas 181–192. Springer-Verlag, Berlin, 1998. 6

[75] W. Millan, A. Clark y E. Dawson. Heuristic design of cryptographically strong balanced Boolean functions. En K. Nyberg (editor), *Advances in Cryptology – EUROCRYP'98*, volumen 1403 de *Lecture Notes in Computer Science*, páginas 489–499. Springer-Verlag, Berlin, 1998. 6

[76] N. Nisan y M. Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, **4(4)**: 301–313 (1998). 2

[77] K. Nyberg. Constructions of bent functions and difference sets. En I. B. Damgård (editor), *Advances in Cryptology – EUROCRYPT'90*, volumen 473 de *Lecture Notes in Computer Science*, páginas 151–160. Springer-Verlag, Berlin, 1991. 3

[78] K. Nyberg. Perfect nonlinear S-boxes. En D. W. Davies (editor), *Advances in Cryptology – EUROCRYPT'91*, volumen 547 de *Lecture Notes in Computer Science*, páginas 378–386. Springer-Verlag, Berlin, 1991. 1, 14

[79] K. Nyberg. Differentially uniform mappings for cryptography. En T. Helleseth (editor), *Advances in Cryptology – EUROCRYPT'93*, volumen 765 de *Lecture Notes in Computer Science*, páginas 55–64. Springer-Verlag, Berlin,

1994. 4

[80] D. Olejár y M. Stanek. On cryptographic properties of random Boolean functions. *Journal of Universal Computer Science*, **4(8)**: 705–717 (1998). 9, 12

[81] J. D. Olsen, R. A. Scholtz y L. R. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, **28(6)**: 858–864 (1982). 3

[82] R. Ozols, R. Freivalds, J. Ivanovs, E. Kalniņa, L. Lāce, M. Miyakawa, T. Hisayuki y D. Taimiņa. Boolean functions with a low polynomial degree and quantum query algorithms. En P. Vojtáš, M. Bieliková, B. Charron-Bost y O. Sýkora (editores), *SOFSEM 2005: Theory and Practice of Computer Science*, volumen 3381 de *Lecture Notes in Computer Science*, páginas 408–412. Springer-Verlag, Berlin, 2005. 2

[83] E. Pasalic. Degree optimized resilient Boolean functions from Maiorana-McFarland class. En K. G. Paterson (editor), *Cryptography and Coding*, volumen 2898 de *Lecture Notes in Computer Science*, páginas 93–114. Springer-Verlag, Berlin, 2003. 5

[84] E. Pasalic y T. Johansson. Further results on the relation between nonlinearity and resiliency for Boolean functions. En M. Walker (editor), *Crytography and Coding*, volumen 1746 de *Lecture Notes in Computer Science*, páginas 35–44. Springer-Verlag, Berlin, 1999. 9, 12

[85] J. Pieprzyk y G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEEE Proceedings*, **135(6)**: 325–335 (1988). 13

[86] B. Preneel. *Analysis and Design of Cryptographic Hash Functions.* Tesis Doctoral, Katholieke University Leuven, enero 1993. 6

[87] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts y J. Vandewalle. Propagation characteristics of Boolean functions. En I. B. Damgard (editor), *Advances in Cryptology – EUROCRYPT'90*, volumen 473 de *Lecture Notes in Computer Science*, páginas 161–173. Springer-Verlag, Berlin, 1991. 3, 6, 12, 13

[88] C. Qu, J. Seberry y J. Pieprzyk. On the symmetric property of homogeneous Boolean functions. En J. Pieprzyk, R. Safavi-Naini y J. Seberry (editores), *Proceedings of the Australasian Conference on Information Security and Privacy – ACISP'99*, volumen 1587 de *Lecture Notes in Computer Science*, páginas 26–35. Springer-Verlag, Berlin, 1999. 5, 12

[89] V. Requena. *Sobre algunas construcciones de funciones bent.* Tesis Doctoral,

Departamento de Ciencia de la Computación e Inteligencia Artificial, Universidad de Alicante, Alicante, España, noviembre 2010. 2, 6, 17

[90] S. Roman. *Introduction to Coding and Information Theory*. Springer, New York, NY, 1997. 78

[91] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, **20**: 300–305 (1976). 3, 15, 16

[92] J. Seberry y X.-M. Zhang. Highly nonlinear 0-1 balanced Boolean functions satisfying strict avalanche criterion (extended abstract). En J. Seberry y Y. Zheng (editores), *Advances in Cryptology – ASIACRYPT '92*, volumen 718 de *Lecture Notes in Computer Science*, páginas 145–155. Springer-Verlag, Berlin, 1992. 14

[93] J. Seberry y X.-M. Zhang. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, **9**: 21–35 (1994). 14

[94] J. Seberry, X.-M. Zhang y Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, **119**: 1–13 (1995). 13, 14

[95] I. Strazdins. Universal affine classification of Booelan functions. *Acta Applicandae Mathematicae*, **46**: 147–167 (1997). 2

[96] S. A. Vanstone y P. C. van Oorschot. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 1989. 23, 65

[97] R. Yarlagadda y J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings*, **136(2)**: 112–123 (1989). 4

[98] W. Zhang y G. Xiao. Constructions of almost optimal resilient Boolean functions on large even number of variables. *IEEE Transactions on Information Theory*, **55(12)**: 5822–5831 (2009). 2

[99] X.-M. Zhang, Y. Zheng y H. Imai. Duality of boolean functions and its cryptographic significance. En Y. Han, T. Okamoto y S. Quing (editores), *Information and Communications Security*, volumen 1334 de *Lecture Notes in Computer Science*, páginas 159–169. Springer-Verlag, Berlin, 1997. 21, 22