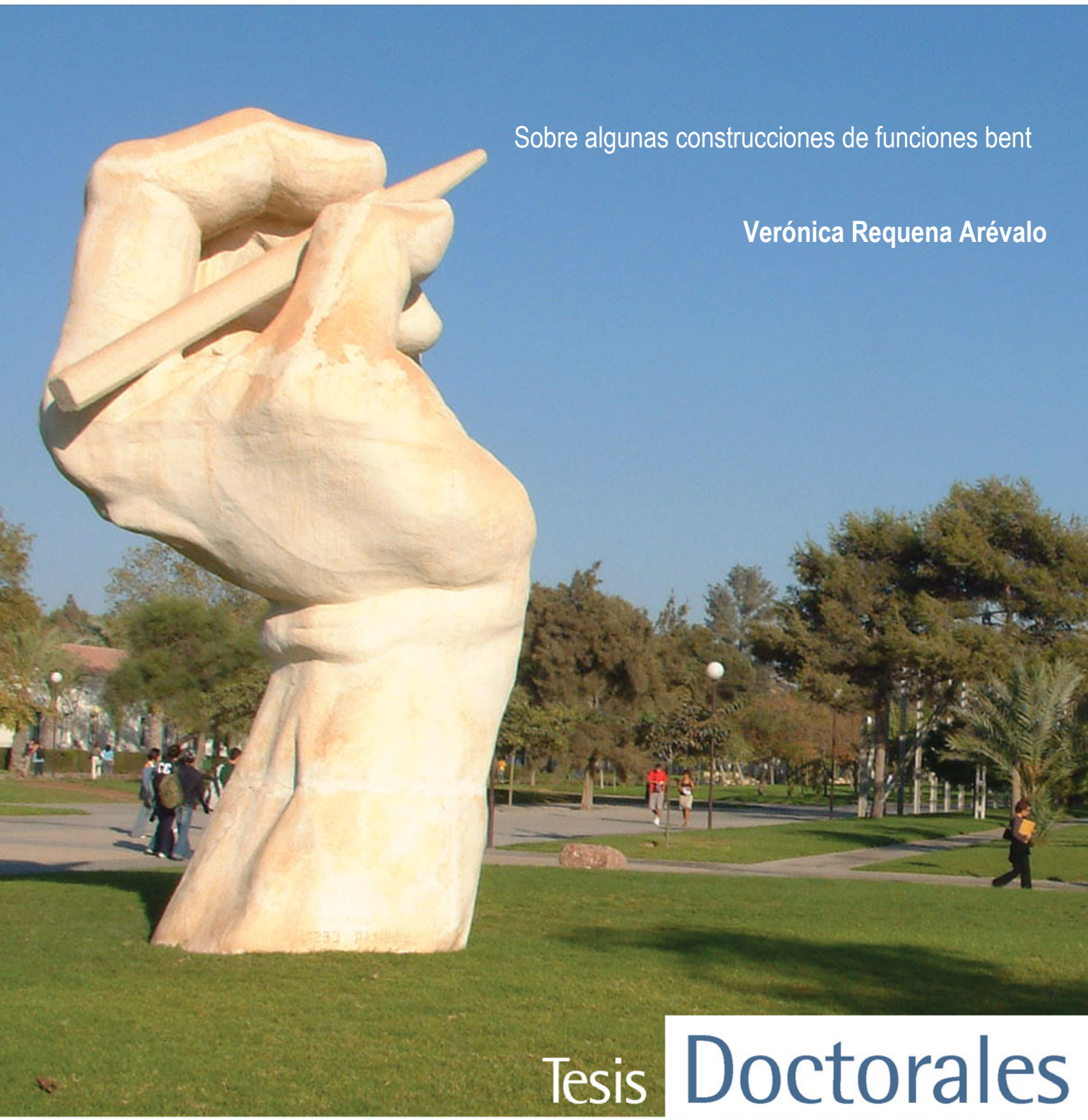
Universitat d'Alacant
Universidad de Alicante



Sobre algunas construcciones de funciones bent

Verónica Requena Arévalo

Tesis Doctorales

www.eltallerdigital.com

UNIVERSIDAD de ALICANTE

Universidad de Alicante

Departamento de Ciencia de la Computación e Inteligencia Artificial

Sobre algunas construcciones de funciones bent

TESIS DOCTORAL

Presentada por:
Verónica Requena Arévalo

Dirigida por:
Joan Josep Climent Coloma

Universidad de Alicante

Departamento de Ciencia de la Computación e Inteligencia Artificial

Sobre algunas construcciones de funciones bent

Memoria presentada para optar al grado de doctor por Verónica Requena Arévalo.

Alicante, octubre de 2010.

D. Joan Josep Climent Coloma, Catedrático de Universidad del Departamento de Estadística e Investigación Operativa de la Universidad de Alicante

CERTIFICA:

Que la presente memoria *Sobre algunas construcciones de funciones bent*, ha sido realizada bajo su dirección, en el Departamento de Ciencia de la Computación e Inteligencia Artificial de la Universidad de Alicante por la licenciada Dña. Verónica Requena Arévalo, y constituye su tesis para optar al grado de doctor.

Para que conste, en cumplimiento de la legislación vigente, autoriza la presentación de la referida tesis doctoral ante la comisión de Doctorado de la Universidad de Alicante, firmando el presente certificado.

Alicante, 7 de octubre de 2010

Joan Josep Climent Coloma

A mis padres,
por todos los caminos que me abrieron.

A Pedro,
por su gran paciencia y continuo apoyo.

La forma de llegar a la cima en cuanto a desarrollar una investigación original es ser un tonto, porque sólo los tontos siguen intentándolo. Tienes la idea número 1*, te entusiasmas y fracasa. Luego tienes la idea número* 2*, te entusiasmas y fracasa. Luego tienes la idea número* 99*, te entusiasmas y fracasa. Sólo un tonto se entusiasma con la idea número* 100*, pero puede que hagan falta* 100 *ideas antes de que una valga realmente la pena. A no ser que seas lo suficientemente tonto para entusiasmarte continuamente, no tendrás la motivación, no tendrás la energía para llegar hasta el final.*

Simon Singh. Los Códigos Secretos
Editoral Debate, Madrid 2000

Y, a veces, hasta la idea número 101 hemos llegado. Sin embargo, jamás lo habría conseguido sin la ayuda de muchísima gente, y a todos y cada uno de ellos me gustaría agradecérselo.

En primer lugar he de dar mi más sincero agradecimiento a mi director de tesis Joan Josep Climent quien ha dedicado tanto, o más, tiempo que yo a este trabajo. Gracias por contagiarnos siempre con tu energía y tu positividad, con tus ganas de trabajar y disfrutar de lo maravillosas que son las matemáticas. Con tu esfuerzo y tu apoyo todo ha sido mucho más fácil. Sin duda, he sido muy afortunada al encontrar al mejor investigador, al mejor compañero y a un gran amigo todo en una misma persona. Gracias por ser así.

Gracias a Paco García, mi compañero por sus grandes ideas, su generosa ayuda y su enorme bondad. Trabajar en equipo nunca había sido tan fácil con vosotros dos a mi lado. Sin ti, el camino de las funciones bent no habría sido el mismo.

Me gustaría agradecer a los profesores Joachim Rosenthal, Gary McGuire y Carmelo Interlando su infinita generosidad y su gran hospitalidad en mis visitas a Zurich, Dublín y San Diego, respectivamente. Gracias a ellos he aprendido de los mejores y me han enseñado lo importante que es ser un buen investigador.

Clara, Pedro, Virtu y Sara, os doy las gracias por todos los momentos que me

habéis ofrecido durante estos años; vuestras incansables palabras de ánimo en los momentos de tristeza, vuestra constante ayuda en la interminable burocracia, nuestras conversaciones indescifrables de matemáticos medio chalados ... Siempre estaréis cerca.

A mis amigas y a mis vecinas (incluidas mis princesitas), quienes siempre han creído en mí. Gracias a todas por hacerme comprender el significado de la amistad. Vosotras traspasáis toda frontera.

A Pedro, mi novio, mi compañero, mi mejor amigo, la persona que siempre ha estado a mi lado apoyándome y recordándome lo importante que son las matemáticas en nuestra vida. Gracias por tu increíble paciencia, por tu inacabable apoyo, por levantarme siempre que me caía, por acompañarme en todo momento y por comprenderme siempre. Te quiero hasta el infinito ....

Y como no, mi más sincero Gracias a mi familia, y a los que desde hace ya casi doce años también son lo son, pues sin ellos no habría conseguido nada de esto ni habría disfrutado de esta gran aventura. Mamá, Papá, gracias por brindarme esta gran oportunidad, por no haber dudado nunca de vuestra hija, por haberme ofrecido todo sin pedirme nunca nada a cambio. Os quiero mucho. David, Francis, gracias a vuestro enorme esfuerzo y sacrificio he conseguido muchas cosas. Vuestro amor es imprescindible en mi vida. Gracias por ayudarme siempre.

Gracias a todos los que directamente, o indirectamente, habéis hecho de mí alguien un poco mejor. A todos aquellos compañeros, amigos y profesores con los que he disfrutado durante la carrera y el doctorado. Con todos aquellos con quienes he disfrutado en los congresos, en los viajes y en mis estancias.

Gracias por hacer de mí lo que hoy soy, una matemática con muchas ganas de aprender.

Índice

Prólogo

Las funciones booleanas juegan un papel muy importante en la criptografía moderna y son la pieza fundamental de numerosos criptosistemas gracias a su habilidad para proporcionar seguridad en las comunicaciones. El estudio de las funciones booleanas, tanto desde una perspectiva teórica como práctica, es crucial en la provisión de seguridad en las aplicaciones criptográficas como los cifradores en bloque, los cifradores en flujo y las funciones hash. Las propiedades de no linealidad y equilibrio son dos criterios esenciales criptográficamente para las funciones booleanas. La no linealidad es la propiedad más importante en cualquier criptosistema de clave simétrica para alcanzar confusión. La definición más usada de no linealidad es la mínima distancia de una función booleana al conjunto de las funciones afines.

La familia de funciones bent son las funciones booleanas de un número par de variables con la máxima no linealidad, aunque no son equilibradas. A pesar de su definición simple y natural, las funciones bent poseen una estructura complicada en general.

La construcción de funciones criptográficamente completas es una tarea ardua. Actualmente existe una amplia gama de técnicas algebraicas y heurísticas para construir tales funciones, sin embargo estos métodos pueden ser complejos, computacionalmente difíciles para su implementación y no siempre producen una variedad suficiente de funciones.

Nuestro esfuerzo principal se ha centrado en el diseño de métodos de construcción para obtener el mayor número posible de nuevas funciones bent. Hay diferentes métodos para obtener funciones bent, muchos de ellos basados en la forma normal algebraica de una función booleana y en la transformada de Fourier (o Walsh). Sin embargo, nosotros utilizamos la representación clásica de las funciones booleanas a través de minterms para construir funciones bent de cualquier número par de

variables a partir de otras funciones booleanas de menor número de variables. Hemos adoptado esta técnica dada la imposibilidad de obtener, de forma aleatoria, funciones bent de más de 6 variables.

Tanto el uso de la forma normal algebraica (FNA) o de la tabla de verdad (equivalentemente, la expresión como suma de minterms), tienen sus ventajas y desventajas. Por ejemplo, la FNA de una función booleana $f(\boldsymbol{x})$ de n variables proporciona directamente su grado y, si éste es mayor que $n/2$ se puede asegurar que $f(\boldsymbol{x})$ no es una función bent; sin embargo, no conocemos la cardinalidad de su soporte (es decir, el número de minterms). Por otro lado, si conocemos la tabla de verdad de $f(\boldsymbol{x})$, sabemos si su soporte tiene el número necesario de minterms o no para ser una función bent, pero no conocemos su grado.

La presente memoria de investigación se divide en cuatro capítulos. En el capítulo 1 proporcionamos una extensa introducción sobre la importancia de las funciones booleanas en la criptografía y repasamos brevemente la historia de las funciones bent a lo largo de estas últimas cuatro décadas. Además presentamos, de manera breve, los conceptos principales relativos a las funciones booleanas y la notación que necesitaremos para la comprensión de los resultados mostrados en esta memoria. Por último, introducimos algunas de las construcciones clásicas de funciones bent más conocidas, lo que nos permitirá poder realizar una comparación exhaustiva con los métodos de construcción que presentamos en los capítulos siguientes.

En el capítulo 2 presentamos dos métodos de construcción de funciones bent de $n+2$ variables basados en la utilización de funciones bent de n de variables (con n par). Calculamos el número de funciones bent distintas que podemos obtener con cada una de dichas construcciones, proporcionando así una cota inferior del número de funciones bent de cualquier número de variables. Al final del capítulo, comparamos nuestras construcciones con algunos de los métodos de construcción de funciones bent más conocidos.

En el capítulo 3 definimos dos nuevas funciones bent de n variables, denominadas funciones de máximo y mínimo peso, construidas a partir de una función bent de n variables y algunas funciones lineales. Analizamos las propiedades principales de estas nuevas funciones y proporcionamos un nuevo método de construcción de funciones bent de $n+2$ variables basado en el uso de las funciones de máximo y mínimo peso de n variables y de los minterms de 2 variables. Introducimos algunos

resultados necesarios para contar el número de funciones bent proporcionado por la nueva construcción; y, por último, comparamos dicho método con las construcciones clásicas introducidas al final del capítulo 1, mostrando las diferencias entre éstos.

Y para finalizar, en el capítulo 4 introducimos el último método de construcción de funciones bent que presentamos en esta memoria. Esta construcción se basa en la utilización de funciones booleanas de n variables (ahora con n impar) y en el uso de los cuatro minterms de 2 variables para la obtención de funciones bent de $n+1$ variables. La diferencia con respecto a las construcciones presentadas anteriormente, es que la generación de estas nuevas funciones bent se basa en el empleo de funciones booleanas de n variables. Para la construcción explícita de estas funciones booleanas utilizamos funciones bent de $n-1$ variables. Analizamos algunas propiedades interesantes de las funciones booleanas implicadas en esta nueva construcción, lo que nos permitirá poder obtener la forma explícita de éstas y, por tanto, de la construcción. Finalmente, establecemos el número de funciones bent que podemos obtener a través del método introducido en este capítulo y lo comparamos con otros métodos de construcción de funciones bent conocidos.

La memoria termina con la relación de la bibliografía utilizada para su elaboración.

Finalmente, destacamos que la investigación plasmada en esta memoria ha sido subvencionada por los proyectos siguientes:

- Ayuda para becas y contratos destinada a la formación de doctores concedida por el Vicerrectorado de Investigación, Desarrollo e Innovación de la Universidad de Alicante (UA2006-48326906).
- Proyecto I+D: Construcción de códigos convolucionales. Algoritmos secuenciales y paralelos de decodificación (MTM2005-05759). Subvencionado por el Ministerio de Educación y Ciencia.
- Proyecto I+D: Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas (MTM2008-06674-C02-01). Subvencionado por el Ministerio de Ciencia e Innovación.
- Proyecto I+D: Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas (ACOMP/2009/142). Subvencionado por la Consellería de Educación.
- Proyecto I+D: Criptología y seguridad computacional (VIGROB-025). Sub-

vencionado por la Universidad de Alicante (2009, 2010).

Parte de los resultados plasmados en esta memoria han sido publicados en distintas revistas [22, 25, 26, 31], otros están en proceso de evaluación para su publicación [36, 37, 38] y otros han sido presentados en distintos congresos y publicados en las correspondientes actas y proceedings (véase [21, 27, 24, 23, 28, 30, 29, 33, 32, 34, 35]):

- XI Reunión Española sobre Criptología y Seguridad de la Información, Tarragona, España, 2010.
- V Congreso Iberoamericano de Seguridad Informática, Motevideo, Uruguay, 2009.
- XXI Congreso de Ecuaciones Diferenciales y Aplicaciones / XI Congreso de Matemática Aplicada, Ciudad Real, España, 2009.
- 5th Workshop on Coding and Systems, Dublín, Irlanda, 2009.
- Congreso de la Real Sociedad Matemática Española, Oviedo, España, 2009.
- 2008 International Symposium on Information Theory and its Applications (ISITA 2008), Auckland, Nueva Zelanda, 2008.
- Second Workshop on Mathematical Cryptology, Santader, España, 2008.
- X Reunión Española sobre Criptología y Seguridad de la Información (RECSI), Salamanca, España, 2008.
- 4th Workshop on Coding and Systems, Alicante–Elche, 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.

Capítulo 1

Preliminares

1.1 Introducción

Las funciones booleanas constituyen una fructífera herramienta para construir modelos de una gran cantidad de procesos de interés en la naturaleza, la lógica, la ingeniería o la ciencia. Particularmente, en *criptografía* se hace un uso intensivo de las mismas en la construcción y análisis de criptosistemas. Las funciones booleanas tiene un papel importante en los cifradores en bloque, cifradores en flujo y las funciones hash [7, 10, 18, 58]. Por ejemplo, la implementación de una caja de sustitución o S-box necesita funciones booleanas no lineales para resistir ataques tales como el criptoanálisis lineal y el diferencial [1, 45, 62]. En los modelos más comunes de cifradores en flujo, la clave se produce utilizando una función booleana. Una variedad de criterios para la selección de funciones booleanas determina sus habilidades para proporcionar seguridad.

Por tanto, la criptografía necesita formas para encontrar funciones booleanas que posean propiedades que reduzcan la efectividad de los avances de ataques criptoanalíticos. Como hemos dicho anteriormente, las funciones *bent* son un tipo especial de funciones booleanas que poseen máxima no linealidad. A pesar de sus buenas propiedades criptográficas, tales como la más alta no linealidad y la más baja autocorrelación [57, 70], las funciones bent pueden ser empleadas en cifradores simétricos para resistir los criptoanálisis anteriormente nombrados. Además, también son empleadas en comunicación, teoría de códigos, teoría combinatoria, entre otros muchos campos.

Por ejemplo, las funciones bent se utilizan en los códigos de Reed-Muller [53].

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 bent de n variables pueden ser caracterizadas como las funciones que poseen la máxima distancia posible a todas las palabras código del código de Reed-Muller de primer orden. Por otro lado, los códigos Kerdock son construidos utilizando funciones bent cuadráticas.

Este tipo de funciones booleanas ha sido objeto de estudio de muchos investigadores desde principios de los 70. A continuación explicaremos, brevemente, el paso por la historia de estas funciones, que hoy son el motivo de nuestro estudio principal.

El origen de las funciones bent se remonta a un artículo teórico de McFarland [56] sobre conjuntos de diferencias finitas en grupos finitos no cíclicos. Un año después, Dillon [40] en su tesis doctoral sistematizó y extendió las ideas de McFarland, proporcionando una gran cantidad de propiedades. El nombre *bent* con el que se conocen estas funciones se debe a Rothaus [72]. Desde entonces estas funciones han sido objeto de un intenso estudio en muchas áreas como se desprende de la abundante literatura al respecto (véase por ejemplo [2, 3, 4, 8, 12, 15, 43, 44, 50, 54, 61, 65] y las referencias en ellas incluidas).

Entre las propiedades mencionadas cabe citar que toda función bent de n variables, con $n > 2$, tiene grado máximo $n/2$ (véase [72]), que hay funciones bent con grado igual a $n/2$ y que las únicas funciones bent simétricas son las cuadráticas, existiendo exactamente cuatro de estas funciones para cada n. Estas funciones son denominadas *semibent* [19, 49].

A partir de las tablas de verdad de las funciones bent y las funciones lineales, es posible construir funciones bent con un número mayor de variables concatenando adecuadamente dichas tablas de verdad. Pero no todas las funciones bent de 6 variables se pueden obtener a partir de funciones bent y funciones lineales con un número menor de variables, como demostró Chang [16]. Esto no significa que no sea interesante construir funciones bent a partir de funciones bent 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 [8] conocemos dos familias infinitas de funciones bent de n variables que no se pueden obtener a partir de funciones bent con un número menor de variables. En dicho artículo, los autores también describen el método a través del cual se pueden construir, partiendo de una función bent de n variables, funciones booleanas de $n-1$ y $n-2$ variables con bastante alta no

linealidad.

Siguiendo una estrategia diferente, Hou y Langevin [48] describieron cómo a partir de una función bent conocida podíamos obtener, de modo efectivo, funciones bent nuevas con el mismo número de variables que la de partida.

Yarlagadda y Hershey [77] realizan también una aproximación secuencial al análisis y la construcción de funciones bent, utilizando para ello la secuencia formada por la tabla de verdad de las funciones booleanas. Esta es una de las cuatro vías de estudio de las funciones booleanas más utilizadas en la literatura. Otras dos centran su atención respectivamente en la representación polinómica y en la matricial de una función booleana.

Otra manera de analizar funciones bent consiste en explorar las propiedades de las estructuras algebraicas sobre GF(2^n). Tal es el caso, por ejemplo, de Carlet y Guillot [14] o de Hou [46, 47]. Los resultados obtenidos de este modo son teóricamente interesantes ya que permiten generar caracterizaciones o teoremas de existencia, pero en muchas ocasiones no proporcionan métodos efectivos de construcción de las funciones que postulan.

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 [71], caracterizando las funciones homogéneas de 6 variables y grado 3 que son *bent* 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 [17] encontraron algunas funciones bent homogéneas de grado 3 y con 8 o 10 variables.

Sabemos que las funciones con máxima no linealidad posible son las funciones bent, sin embargo éstas sólo existen cuando n es par. Las funciones con no linealidad casi perfecta [63] juegan un rol similar al de las funciones bent pero con n impar y no linealidad elevada, pero sin llegar a ser máxima. Dobbertin [42] ha resumido, aportando dos nuevos casos, el estado de la clasificación de las funciones casi perfectamente no lineales sobre $GF(2^n)$ cuando n es impar.

A mediados de esta década, Maity y Maitra [55] estudiaron la mínima distancia entre el conjunto de las funciones bent 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 este estudio han establecido un procedimiento para generar funciones 1-resilientes con alta no linealidad a partir de funciones bent de 8 variables.

En la misma línea, Borissov [5] ha estudiado la relación entre las funciones t-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 [66] ha generalizado un método, modificando la clase de funciones bent de Maiorana-McFarland, para construir *S-boxes* en las que cada una de las componentes —en definitiva una función booleana— sea t-resiliente y con elevado grado algebraico.

Una función bent se llama *normal* si es constante cuando se restringen sus n entradas a cierto subespacio de dimensión $n/2$ [41]. Hasta muy recientemente, todas las construcciones *concretas* conocidas proporcionaban funciones *bent normales*. Ahora se sabe ya que todas las funciones bent de 2, 4 y 6 variables son normales. Para dimensiones mayores, Carlet, Dobbertin y Leander [13] han demostrado que la suma de una función *bent normal* y una función *bent no normal* —de las que ahora se sabe su existencia— es siempre *no normal*.

Millan, Clark y Dawson [59, 60] 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 del 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 ampliamente en [70]. 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.

Cheon [20] ha conseguido establecer una cota inferior sobre la no linealidad de ciertos tipos de multifunciones booleanas.

La construcción de familias de funciones bent particulares es importante por las siguientes razones. Por un lado, existe la necesidad práctica de tener funciones de máxima no linealidad para implementar cifradores. Por otro lado, existen razones

teóricas para descubrir propiedades y contrastar conjeturas.

La literatura mencionada hasta ahora hace un uso intensivo de la representación de funciones booleanas en forma polinomial, en forma matricial y en forma secuencial. Sin embargo, el concepto clásico de minterm, el cual está directamente relacionado con la implementación de circuitos lógicos y su complejidad, no ha sido utilizado con frecuencia.

Esta memoria se centra, principalmente, en el estudio de la construcción de funciones bent de cualquier número de variables utilizando la representación de funciones booleanas como suma de minterms.

Un método general para generar todas las funciones bent aún no es conocido, excepto para algunos casos particulares. Cabe destacar que para $n = 2$ hay 8 funciones bent, para $n = 4$ hay 896 funciones bent (que se pueden obtener fácilmente mediante una búsqueda exhaustiva por ordenador), para $n = 6$ Preneel [69] (véase también [16]) probó que el número de funciones bent es de 5 425 430 528 y para $n = 8$, Langevin y Leander [52] provaron recientemente que el número de funciones bent 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 bent, continúa siendo un problema abierto.

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, es bien conocido que $\mathbb{F}_2^n$ 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 $\boldsymbol{b}$.

Para cada $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{F}_2^n$, consideramos 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

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

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 $\mathbb{F}_2^n$.

Una **función booleana** de n variables es una aplicación $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. El conjunto $\mathcal{B}_n$ de todas las funciones booleanas de n variables es un espacio vectorial sobre $\mathbb{F}_2$ con la adición $\oplus$ dada por

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

Si $f \in \mathcal{B}_n$, llamamos **tabla de verdad** de f (véase [64, 67]) a la secuencia binaria de longitud 2^n dada por

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

es decir, la i-ésima componente de $\boldsymbol{\xi}_f$, coincide con $f(\boldsymbol{i})$, para $\boldsymbol{i} = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{2^n - 1}$. La tabla de verdad de una función booleana queda perfectamente determinada a partir de sus minterms.

Definición 1.1: Llamamos **minterm** de n variables, definido por el vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_2^n$, a la función $m_{\boldsymbol{u}} \in \mathcal{B}_n$ dada por

$$m_{\boldsymbol{u}}(\boldsymbol{x}) = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_n \oplus x_n),$$

para todo $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$.

Por cuestiones prácticas, escribimos $m_{\boldsymbol{u}}(\boldsymbol{x})$ o $m_u(\boldsymbol{x})$, según convenga, donde, de acuerdo con lo dicho anteriormente, $\boldsymbol{u} \in \mathbb{F}_2^n$ es la expansión binaria de $u \in \mathbb{Z}_{2^n}$.

Para $i = 0, 1, 2, \ldots, 2^n - 1$, es evidente que $m_i(\boldsymbol{x}) = 1$ si y sólo si $\boldsymbol{x} = \boldsymbol{i}$. Por tanto, la tabla de verdad

$$(m_i(\mathbf{0}),\ m_i(\mathbf{1}),\ \ldots,\ m_i(\mathbf{2^n - 1}))$$

de $m_i(\boldsymbol{x})$ tiene un 1 en la i-ésima posición y 0 en las restantes. En consecuencia,

$$\bigoplus_{i=0}^{2^n-1} m_i(\boldsymbol{x}) = 1, \quad \text{para todo} \quad \boldsymbol{x} \in \mathbb{F}_2^n. \tag{1.1}$$

Además, como $m_i(\boldsymbol{x}) = m_j(\boldsymbol{x})$ si y sólo si $i = j$, podemos identificar el minterm $m_i(\boldsymbol{x})$ con el entero i (o con el vector $\boldsymbol{i}$ según convenga).

Ahora, para toda $f \in \mathcal{B}_n$ es fácil comprobar que

$$f(\boldsymbol{x}) = \bigoplus_{i=0}^{2^n-1} f(\boldsymbol{i})\ m_i(\boldsymbol{x}) \tag{1.2}$$

y como

$$\bigoplus_{i=0}^{2^n-1} a_i\ m_i(\boldsymbol{x}) = 0 \quad \text{implica que} \quad a_i = 0 \quad \text{para} \quad i = 0, 1, 2, \ldots, 2^n - 1,$$

podemos afirmar que el conjunto $\{m_0, m_1, \ldots, m_{2^n-1}\}$ es una base de $\mathcal{B}_n$. En consecuencia, $\dim \mathcal{B}_n = 2^n$ y, por tanto, $\operatorname{card}(\mathcal{B}_n) = 2^{2^n}$.

Definición 1.2: Llamamos **soporte** de f, y escribimos $\operatorname{Sop}(f)$, al conjunto de vectores de $\mathbb{F}_2^n$ cuya imagen por f es 1, es decir,

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

Por tanto, $\operatorname{Sop}(f)$ 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 $\mathbb{Z}_{2^n}$, en algunos casos escribimos

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

Así, de acuerdo con la expresión (1.2), podemos expresar $f(\boldsymbol{x})$ como

$$f(\boldsymbol{x}) = \bigoplus_{i \in \operatorname{Sop}(f)} m_i(\boldsymbol{x})$$

lo cual nos permite identificar $\operatorname{Sop}(f)$ con el conjunto de índices de los minterms de $f(\boldsymbol{x})$.

Definición 1.3: 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,

$$w(f) = \operatorname{card}(\operatorname{Sop}(f)).$$

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

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

Si $f \in \mathcal{B}_n$, podemos escribir $f(\boldsymbol{x})$ de forma única (véase, por ejemplo, [51, 64, 67, 70, 71]) como

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

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), en la que cada uno de los términos $\boldsymbol{x}^{\boldsymbol{u}}$ es un **monomio** cuyo grado es $w(\boldsymbol{u})$, se conoce con el nombre de **forma normal algebraica** (FNA) de $f(\boldsymbol{x})$.

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

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

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

A continuación, introducimos algunos resultados importantes de los minterms que serán útiles para la construcción de nuevas funciones bent en capítulos posteriores.

En primer lugar destacamos la siguiente propiedad de los minterms que los hace operativos desde el punto de vista algebraico.

Lema 1.1: *$m_{\boldsymbol{u}}(\boldsymbol{x} \oplus \boldsymbol{v}) = m_{\boldsymbol{u}\oplus\boldsymbol{v}}(\boldsymbol{x})$ para todo $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$.*

DEMOSTRACIÓN: Supongamos que

$$\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \qquad \text{y} \qquad \boldsymbol{v} = (v_1, v_2, \ldots, v_n);$$

entonces

$$m_{\boldsymbol{u}}(\boldsymbol{x} \oplus \boldsymbol{v}) = (1 \oplus u_1 \oplus x_1 \oplus v_1)(1 \oplus u_2 \oplus x_2 \oplus v_2) \cdots (1 \oplus u_n \oplus x_n \oplus v_n)$$
$$= m_{\boldsymbol{u} \oplus \boldsymbol{v}}(\boldsymbol{x}). \qquad \square$$

Además, como consecuencia de este resultado, tenemos las siguientes propiedades del soporte de una función booleana.

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

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

(b) $\mathrm{Sop}\,(f)\,\Delta(\boldsymbol{a} \oplus \mathrm{Sop}\,(f))$ *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) Supongamos que $f(\boldsymbol{x}) = \bigoplus_{\boldsymbol{b} \in \mathrm{Sop}(f)} m_{\boldsymbol{b}}(\boldsymbol{x})$, entonces, de acuerdo con el lema 1.1,

$$f(\boldsymbol{a} \oplus \boldsymbol{x}) = \bigoplus_{\boldsymbol{b} \in \mathrm{Sop}(f)} m_{\boldsymbol{b}}(\boldsymbol{a} \oplus \boldsymbol{x}) = \bigoplus_{\boldsymbol{b} \in \mathrm{Sop}(f)} m_{\boldsymbol{a} \oplus \boldsymbol{b}}(\boldsymbol{x}) = \bigoplus_{\boldsymbol{c} \in \boldsymbol{a} \oplus \mathrm{Sop}(f)} m_{\boldsymbol{c}}(\boldsymbol{x})$$

ya que la aplicación $\varphi : \mathrm{Sop}\,(f) \longrightarrow \boldsymbol{a} \oplus \mathrm{Sop}\,(f)$ dada por $\varphi(\boldsymbol{b}) = \boldsymbol{a} \oplus \boldsymbol{b}$ es biyectiva.

(b) Supongamos que $\boldsymbol{b} \in \mathbb{F}_2^n$. Tenemos que

$$f(\boldsymbol{b}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{b}) = 1 \quad \text{si y sólo si} \quad f(\boldsymbol{b}) = 1 \quad \text{o} \quad f(\boldsymbol{a} \oplus \boldsymbol{b}) = 1;$$

pero $f(\boldsymbol{b}) \neq f(\boldsymbol{a} \oplus \boldsymbol{b})$, por tanto, de acuerdo con el apartado (a), tenemos que

$$\boldsymbol{b} \in \mathrm{Sop}\,(f) \quad \text{o} \quad \boldsymbol{b} \in \boldsymbol{a} \oplus \mathrm{Sop}\,(f)\,.$$

Sin embargo, $\boldsymbol{b} \notin \mathrm{Sop}\,(f) \cap (\boldsymbol{a} \oplus \mathrm{Sop}\,(f))$, por lo que $\boldsymbol{b} \in \mathrm{Sop}\,(f)\,\Delta(\boldsymbol{a} \oplus \mathrm{Sop}\,(f))$. $\square$

El siguiente resultado nos permite obtener minterms de $n + k$ variables a partir del producto de dos minterms de k y n variables, respectivamente; concretamente, establece que por cada minterm de n variables podemos obtener 2^k minterms de $n + k$ variables.

Lema 1.2: *Supongamos que $a \in \mathbb{Z}_{2^n}$ y $b \in \mathbb{Z}_{2^k}$. Si $m_a(\boldsymbol{x})$ es un minterm de n variables y $m_b(\boldsymbol{y})$ es un minterm de k variables, entonces*

$$m_c(\boldsymbol{y}, \boldsymbol{x}) = m_b(\boldsymbol{y}) m_a(\boldsymbol{x})$$

es un minterm de $n+k$ variables donde

$$c = b_1 2^{n+k-1} + b_2 2^{n+k-2} + \cdots + b_k 2^n + a \qquad y \qquad b = b_1 2^{k-1} + b_2 2^{k-1} + \cdots + b_k.$$

DEMOSTRACIÓN: Supongamos que

$$a = a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_{n-1} 2 + a_n$$

y que $\boldsymbol{a}, \boldsymbol{b}$ son las expansiones binarias de los enteros a y b, respectivamente. Entonces

$$\begin{aligned} & m_{\boldsymbol{b}}(\boldsymbol{y})\ m_{\boldsymbol{a}}(\boldsymbol{x}) = m_{(b_1,b_2,\ldots,b_k)}(\boldsymbol{y})\ m_{(a_1,a_2,\ldots,a_n)}(\boldsymbol{x}) \\ & = (1 \oplus b_1 \oplus y_1)(1 \oplus b_2 \oplus y_2) \cdots (1 \oplus b_k \oplus y_k)(1 \oplus a_1 \oplus x_1) \cdots (1 \oplus a_n \oplus x_n) \\ & = m_{(b_1,b_2,\ldots,b_k,a_1,a_2,\ldots,a_n)}(\boldsymbol{y}, \boldsymbol{x}) = m_{\boldsymbol{c}}(\boldsymbol{y}, \boldsymbol{x}), \end{aligned}$$

donde

$$c = b_1 2^{n+k-1} + b_2 2^{n+k-2} + \cdots + b_k 2^n + a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_n 1$$

es el entero correspondiente a la expansión binaria del vector $\boldsymbol{c}$. □

Como caso particular del lema anterior, tomando $k = 1$, tenemos el siguiente corolario que nos proporciona dos minterms de $n+1$ variables a partir de un minterm de n variables.

Corolario 1.1: *Supongamos que $a \in \mathbb{Z}_{2^n}$ y $b \in \mathbb{Z}_2$. Si $m_a(\boldsymbol{x})$ es un minterm de n variables y $m_b(y)$ es un minterm de 1 variable, entonces $m_c(y, \boldsymbol{x}) = m_b(y) m_a(\boldsymbol{x})$ es un minterm de $n+1$ variables donde $c = b2^n + a \in \mathbb{Z}_{2^{n+1}}$.*

Por tanto, el corolario anterior nos permite obtener los minterms

$$m_{0+a}(y, \boldsymbol{x}) \quad \text{y} \quad m_{2^n+a}(y, \boldsymbol{x}).$$

de $n+1$ variables.

Si en lugar de utilizar enteros para denotar los subíndices de los minterms, utilizamos vectores, entonces a partir del minterm $m_{\boldsymbol{a}}(\boldsymbol{x})$ de n variables, podemos obtener los minterms

$$m_{(0,\boldsymbol{a})}(\boldsymbol{x}) \qquad \text{y} \qquad m_{(1,\boldsymbol{a})}(\boldsymbol{x})$$

de $n+1$ variables.

Otro caso particular del lema 1.2 sería tomar $k=2$, obteniendo el siguiente corolario que nos proporciona cuatro minterms de $n+2$ variables a partir de un minterm de n variables.

Corolario 1.2: *Supongamos que $a \in \mathbb{Z}_{2^n}$ y $b \in \mathbb{Z}_{2^2}$. Si $m_a(\boldsymbol{x})$ es un minterm de n variables y $m_b(\boldsymbol{y})$ es un minterm de 2 variables, entonces $m_c(\boldsymbol{y},\boldsymbol{x}) = m_b(\boldsymbol{y})m_a(\boldsymbol{x})$ es un minterm de $n+2$ variables donde*

$$c = b_1 2^{n+1} + b_2 2^n + a \qquad y \qquad b = b_1 2 + b_2.$$

En este caso, el corolario anterior permite obtener los minterms

$$m_{0+a}(\boldsymbol{y},\boldsymbol{x}), \quad m_{2^n+a}(\boldsymbol{y},\boldsymbol{x}), \quad m_{2^{n+1}+a}(\boldsymbol{y},\boldsymbol{x}) \quad \text{y} \quad m_{2^n+2^{n+1}+a}(\boldsymbol{y},\boldsymbol{x}).$$

de $n+2$ variables.

Observemos que, si utilizamos vectores para los subíndices de los minterms en lugar de enteros, entonces a partir del minterm $m_{\boldsymbol{a}}(\boldsymbol{x})$ de n variables, podemos obtener los minterms

$$m_{(\boldsymbol{0},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}), \quad m_{(\boldsymbol{1},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}), \quad m_{(\boldsymbol{2},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}), \quad \text{y} \quad m_{(\boldsymbol{3},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}).$$

de $n+2$ variables.

El ejemplo siguiente nos ayudará a entender estos resultados y la notación utilizada.

Ejemplo 1.1: Supongamos que $n=2$. A partir del minterm $m_3(\boldsymbol{x})$ de 2 variables, podemos obtener los minterms

$$m_3(\boldsymbol{y},\boldsymbol{x}), \quad m_7(\boldsymbol{y},\boldsymbol{x}), \quad m_{11}(\boldsymbol{y},\boldsymbol{x}) \quad \text{y} \quad m_{15}(\boldsymbol{y},\boldsymbol{x}),$$

de 4 variables, ya que

$$7 = 3 + 2^2,\ 11 = 3 + 2^3 \quad \text{y} \quad 15 = 3 + 2^2 + 2^3.$$

Ahora, como $\mathbf{3} = (1,1) \in \mathbb{F}_2^2$, tenemos que

$$(\mathbf{0},\mathbf{3}) = (0,0;1,1) = \mathbf{3}, \qquad (\mathbf{1},\mathbf{3}) = (0,1;1,1) = \mathbf{7},$$
$$(\mathbf{2},\mathbf{3}) = (1,0;1,1) = \mathbf{11}, \qquad (\mathbf{3},\mathbf{3}) = (1,1;1,1) = \mathbf{15},$$

por tanto, a partir del minterm $m_{\mathbf{3}}(\boldsymbol{x})$ de 2 variables, obtenemos los minterms

$$m_{\mathbf{3}}(\boldsymbol{y},\boldsymbol{x}), \quad m_{\mathbf{7}}(\boldsymbol{y},\boldsymbol{x}), \quad m_{\mathbf{11}}(\boldsymbol{y},\boldsymbol{x}) \quad \text{y} \quad m_{\mathbf{15}}(\boldsymbol{y},\boldsymbol{x}),$$

de 4 variables. ■

Definición 1.4: 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 $w(f) = 2^{n-1}$.

Definición 1.5: Decimos que $f \in \mathcal{B}_n$ es una **función afín** si

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

donde $\boldsymbol{a} \in \mathbb{F}_2^n$ 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.

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 [68].

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 [75]) por

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

Las funciones bent son las funciones booleanas que alcanzan la máxima no linealidad (véase [75]). Más formalmente,

Definición 1.8: Sea $f \in \mathcal{B}_n$. Decimos que f es una **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 [74, 75]), 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 $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$.*

(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 $\boldsymbol{a} = \boldsymbol{0}$ en el apartado (c), tenemos que el número de 1 de su tabla de verdad, es decir, $w(f)$, 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 [62].

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 [73]), 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 [73]), $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ 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 $f(\boldsymbol{x})$, tal como ponemos de manifiesto en el siguiente ejemplo.

Ejemplo 1.2: Sea

$$f(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x})$$

una función bent de 4 variables; claramente $w(f) = 6 = 2^{4-1} - 2^{2-1}$. Es fácil comprobar que tomando la función lineal

$$l_{\mathbf{1}}(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x})$$

tenemos que

$$f(\boldsymbol{x}) \oplus l_{\mathbf{1}}(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}),$$

con lo que $w(f \oplus l_{\mathbf{1}}) = 10 = 2^{4-1} + 2^{2-1} \neq 6 = w(f)$. Sin embargo, si tomamos la función lineal

$$l_{\mathbf{7}}(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x})$$

tenemos que

$$f(\boldsymbol{x}) \oplus l_{\mathbf{7}}(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}),$$

con lo que $w(f \oplus l_{\mathbf{7}}) = 6 = w(f)$. ■

Antes de pasar a la sección siguiente, recordemos que dos funciones booleanas $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son **afínmente equivalentes** si existen $A \in GL_2(n)$, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ y $c \in \mathcal{F}_2$ tales que

$$g(\boldsymbol{x}) = f(\boldsymbol{x}A \oplus \boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}) \oplus c.$$

Es bien conocido, (véase por ejemplo [6]) que dos funciones afínmente equivalentes son ambas bent o ambas no lo son. Así que, son muchos los autores que trabajan en el problema de *encontrar el número y los representantes de las clases afínmente equivalentes de las funciones bent*. Sin embargo, nuestro interés se centra en el problema de *encontrar cuántas funciones bent diferentes existen o podemos construir*, ya que no todas las funciones bent afínmente equivalentes son diferentes como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 1.3: Consideremos la función bent

$$f(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x})$$

de 4 variables, la matriz invertible

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

los vectores $\boldsymbol{a} = (0,0,0,1)$ y $\boldsymbol{b} = (0,0,0,0)$ y el escalar $c = 0$.

Es fácil comprobar que ambas funciones $f(\boldsymbol{x}A \oplus \boldsymbol{a})$ y $f(\boldsymbol{x})$ tienen la misma tabla de verdad y, por tanto, son iguales. ■

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 tres de tales construcciones: la construcción de Rothaus, la de Maiorana-McFarland y la de Carlet, que podemos considerar como construcciones clásicas y que nos servirán para compararlas con las construcciones introducidas en los diferentes capítulos de esta memoria.

Rothaus [72, pág. 303] presenta dos construcciones de funciones bent que recogemos en el teorema siguiente para futuras referencias.

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 a la construcción (b) como la construcción de Rothaus. La mayor dificultad de dicha construcción estriba en la imposibilidad de determinar 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, habiendo podido establecer solamente algunos casos particulares (véase [72]); por tanto, es imposible averiguar, para los distintos valores de n, cuántas funciones bent de esta clase existen.

Notemos que en la construcción de Rothaus aparece el monomio $x_{n+1}x_{n+2}$, es decir, el producto de las dos variables que hemos añadido a las n variables que teníamos inicialmente. Por tanto, sabremos que aquellas funciones booleanas que no contengan dicho monomio no serán de la clase Rothaus. Esto nos servirá para la comparación de nuestros métodos con el de Rothaus.

El resultado siguiente (que puede encontrarse, por ejemplo en [40, 50]) 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 cual-*

quiera 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 [11]) 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,

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

como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 1.4: Consideremos la cuaterna de funciones bent de 2 variables dada por

$$(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), g_0(\boldsymbol{y}), g_1(\boldsymbol{y})) = (m_0(\boldsymbol{x}), m_3(\boldsymbol{x}), m_0(\boldsymbol{y}), m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y}))\,.$$

Aplicando el teorema 1.5 a la cuaterna anterior, obtenemos la función bent de 4 variables dada por

$$C(\boldsymbol{y},\boldsymbol{x}) = m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}).$$

Consideremos ahora la cuaterna de funciones bent de 2 variables, definida por

$$(f_0'(\boldsymbol{x}), f_1'(\boldsymbol{x}), g_0'(\boldsymbol{y}), g_1'(\boldsymbol{y})) = (m_1(\boldsymbol{x}), m_3(\boldsymbol{x}), m_0(\boldsymbol{y}), m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y}))\,.$$

Aplicando el teorema 1.5 a esta cuaterna, obtenemos la función bent de 4 variables

$$C(\boldsymbol{y},\boldsymbol{x}) = m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}).$$

Por tanto, tenemos que partiendo de dos cuaternas de funciones bent distintas, podemos obtener la misma función bent de la clase Carlet. ■

Capítulo 2

Construcciones de funciones bent de $n+2$ variables a partir de funciones bent de n variables

2.1 Construcción basada en dos funciones bent

En este capítulo presentamos dos construcciones de funciones bent de $n+2$ variables a partir de algunas funciones bent de n variables y los cuatro minterms de dos variables. Además, comparamos las construcciones obtenidas en este capítulo con las construcciones clásicas introducidas en el capítulo 1.

En el resto del capítulo consideramos que $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ es un vector de $\mathbb{F}_2^n$ y que $\boldsymbol{y} = (y_1, y_2)$ es un vector de $\mathbb{F}_2^2$.

La primera construcción de funciones bent se basa en la utilización de dos funciones bent de n variables y los cuatro minterms de 2 variables para obtener funciones bent de $n+2$ variables.

Teorema 2.1: *Sean $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ funciones bent de n variables y supongamos que σ es una permutación de $\{0,1,2,3\}$. Entonces*

$$F(\boldsymbol{y},\boldsymbol{x}) = \big(m_{\sigma(0)}(\boldsymbol{y}) \oplus m_{\sigma(1)}(\boldsymbol{y})\big)\, f_0(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})(1 \oplus f_1(\boldsymbol{x}))$$

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

y_1	y_2	$\boldsymbol{x}$	$m_0(\boldsymbol{y})$	$m_1(\boldsymbol{y})$	$m_2(\boldsymbol{y})$	$m_3(\boldsymbol{y})$	$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$
$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{I}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{0}$	$\mathbf{I}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{I}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi}_0 \oplus b_2\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{I}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{I}$	$\mathbf{0}$	$\boldsymbol{\xi}_1 \oplus b_1\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{I}$	$\mathbf{I}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{I}$	$\mathbf{I} \oplus \boldsymbol{\xi}_1 \oplus b_1\mathbf{I} \oplus b_2\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Tabla 2.1: *Tabla de verdad de* $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$

DEMOSTRACIÓN: De acuerdo con el teorema 1.2, basta con probar que el número de 1 de la tabla de verdad (esto es, el número de minterms) de la función booleana

$$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = F(\boldsymbol{y},\boldsymbol{x}) \oplus l_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$$

es $2^{n+1} \pm 2^{\frac{n}{2}}$ para todo $(\boldsymbol{b},\boldsymbol{a}) \in \mathbb{F}_2^2 \times \mathbb{F}_2^n$.

Supongamos en primer lugar que σ es la permutación identidad. Si $\boldsymbol{b} = (b_1, b_2)$, entonces

$$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = (m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}))\, f_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})(1 \oplus f_1(\boldsymbol{x})) \oplus b_1 y_1 \oplus b_2 y_2 \oplus l_{\boldsymbol{a}}(\boldsymbol{x}).$$

Por tanto, si $\mathbf{0}$ e $\mathbf{I}$ son las columnas de longitud 2^n con todos los elementos iguales a 0 y 1, respectivamente; $\boldsymbol{\tau}$ es la matriz de tamaño $2^n \times n$ cuya i-ésima fila es $\boldsymbol{i}$, para $i = 0, 1, \ldots, 2^n - 1$; $\boldsymbol{\xi}_0$ y $\boldsymbol{\xi}_1$ son las tablas de verdad de $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$, respectivamente; y $\boldsymbol{\Lambda}_{\boldsymbol{a}}$ es la tabla de verdad de la función lineal $l_{\boldsymbol{a}}(\boldsymbol{x})$, entonces la última columna de la tabla 2.1 muestra la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$. Ahora, cada columna de la tabla 2.2 representa los cuatro bloques de la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ para los distintos valores de $\boldsymbol{b}$.

Como $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ son funciones bent, por el teorema 1.2, tenemos que, para $j = 0, 1$, el número de 1 de $\boldsymbol{\xi}_j \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ es $2^{n-1} \pm 2^{\frac{n}{2}-1}$, y por tanto, el número de 1 de $\boldsymbol{\xi}_j \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ es $2^{n-1} \mp 2^{\frac{n}{2}-1}$. Así que, en cualquier caso, tenemos tres bloques en los que el número de 1 es $2^{n-1} + 2^{\frac{n}{2}-1}$ y un bloque en el que el número de 1 es $2^{n-1} - 2^{\frac{n}{2}-1}$, o tres bloques en los que el número de 1 es $2^{n-1} - 2^{\frac{n}{2}-1}$ y un bloque en

$b_1=0 \quad b_2=0$	$b_1=0 \quad b_2=1$	$b_1=1 \quad b_2=0$	$b_1=1 \quad b_2=1$
$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{I} \oplus \boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\mathbf{I} \oplus \boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Tabla 2.2: *Tabla de verdad de* $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ *para los distintos valores de* $\boldsymbol{b} = (b_1, b_2)$.

el que el número de 1 es $2^{n-1} + 2^{\frac{n}{2}-1}$. En consecuencia, el número de 1 de la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ es siempre $2^{n+1} + 2^{\frac{n}{2}}$ o $2^{n+1} - 2^{\frac{n}{2}}$.

Finalmente, si σ es una permutación cualquiera de $\{0,1,2,3\}$ distinta de la permutación identidad, entonces los cuatro bloques de la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ dados en la tabla 2.2 se permutan de acuerdo con σ y por tanto, obtenemos el mismo resultado que en el caso anterior. □

Notemos que, como consecuencia del corolario 1.2, si utilizamos enteros para los subíndices de los minterms, podemos identificar la permutación σ con una permutación

$$\begin{pmatrix} 0 & 2^n & 2^{n+1} & 2^{n+1}+2^n \\ a_0 & a_1 & a_2 & a_3 \end{pmatrix}$$

del conjunto $\{0, 2^n, 2^{n+1}, 2^{n+1}+2^n\}$; por tanto, de acuerdo con el teorema 2.1, tenemos que

$$\begin{aligned} \mathrm{Sop}\,(F) = &\{a_0 + a, a_1 + a \mid a \in \mathrm{Sop}\,(f_0)\} \cup \{a_2 + a \mid a \in \mathrm{Sop}\,(f_1)\} \\ &\cup \left\{a_3 + a \mid a \in \overline{\mathrm{Sop}\,(f_1)}\right\} \end{aligned} \tag{2.1}$$

donde $\overline{\mathrm{Sop}\,(f_1)} = \mathbb{Z}_{2^n} \setminus \mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(1 \oplus f_1)$.

En cambio, si para los subíndices de los minterms utilizamos vectores, entonces

$$\begin{aligned} \mathrm{Sop}\,(F) = &\{(\boldsymbol{a}_0, \boldsymbol{a}), (\boldsymbol{a}_1, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_0)\} \cup \{(\boldsymbol{a}_2, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_1)\} \\ &\cup \left\{(\boldsymbol{a}_3, \boldsymbol{a}) \mid \boldsymbol{a} \in \overline{\mathrm{Sop}\,(f_1)}\right\} \end{aligned} \tag{2.2}$$

donde

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \boldsymbol{a}_0 & \boldsymbol{a}_1 & \boldsymbol{a}_2 & \boldsymbol{a}_3 \end{pmatrix}$$

es una permutación de $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$ y, como antes, $\overline{\mathrm{Sop}\,(f_1)} = \mathrm{Sop}\,(1 \oplus f_1)$.

Notemos que los conjuntos que aparecen en el segundo miembro de las expresiones (2.1) y (2.2) son, por el corolario 1.2, disjuntos dos a dos.

Nuestro objetivo ahora es conocer el número de funciones bent de $n+2$ variables distintas que podemos obtener a partir de la construcción dada en el teorema 2.1.

Para facilitar el cómputo de las funciones bent obtenidas mediante esta construcción, consideramos los dos casos particulares (véanse los corolarios 2.1 y 2.2 más abajo) que obtenemos directamente del teorema 2.1. El primero corresponde al caso en que

$$f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \quad \text{o} \quad f_1(\boldsymbol{x}) = 1 \oplus f_0(\boldsymbol{x}),$$

y se basa en el hecho de que (véase la expresión (1.1)),

$$m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}) \oplus m_3(\boldsymbol{y}) = 1 \quad \text{para todo} \quad \boldsymbol{y} \in \mathbb{F}_2^2.$$

El segundo, corresponde al caso en que

$$f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x}) \quad \text{y} \quad f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x}).$$

Corolario 2.1: *Si $f_0(\boldsymbol{x})$ es una función bent de n variables y σ es una permutación de $\{0,1,2,3\}$, entonces*

$$A_{f_0}(\boldsymbol{y}, \boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})$$

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

Corolario 2.2: *Sean $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ funciones bent de n variables tales que*

$$f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x}) \qquad y \qquad f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x}).$$

Si σ es una permutación cualquiera del conjunto $\{0,1,2,3\}$, entonces

$$B_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) = \left(m_{\sigma(0)}(\boldsymbol{y}) \oplus m_{\sigma(1)}(\boldsymbol{y})\right) f_0(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\,(1 \oplus f_1(\boldsymbol{x}))$$

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

A continuación probamos que las funciones bent construidas de acuerdo con el corolario 2.1 son todas distintas.

Lema 2.1: *Sean $f_0(\boldsymbol{x})$ y $g_0(\boldsymbol{x})$ funciones bent de n variables tales que $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$. Supongamos también que σ y τ son permutaciones de $\{0,1,2,3\}$. Si $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $A_{g_0}(\boldsymbol{y},\boldsymbol{x})$ son las funciones bent construidas de acuerdo con el corolario 2.1 utilizando $f_0(\boldsymbol{x})$ y $g_0(\boldsymbol{x})$ y las permutaciones σ y τ respectivamente, entonces*

$$A_{f_0}(\boldsymbol{y},\boldsymbol{x}) \neq A_{g_0}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}_0$ y $\boldsymbol{\eta}_0$ son las tablas de verdad de $f_0(\boldsymbol{x})$ y $g_0(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $A_{g_0}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$\begin{array}{lcccc} A_{f_0}: & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_0 & \boldsymbol{\xi}_0 & \mathbf{I}\oplus\boldsymbol{\xi}_0 \\ A_{g_0}: & \boldsymbol{\eta}_0 & \boldsymbol{\eta}_0 & \boldsymbol{\eta}_0 & \mathbf{I}\oplus\boldsymbol{\eta}_0 \end{array}$$

Como $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, sabemos que $\boldsymbol{\xi}_0 \neq \boldsymbol{\eta}_0$. Por tanto, si $A_{f_0}(\boldsymbol{y},\boldsymbol{x}) = A_{g_0}(\boldsymbol{y},\boldsymbol{x})$, necesariamente $\boldsymbol{\xi}_0 = \mathbf{I}\oplus\boldsymbol{\eta}_0$ y $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_0$, lo cual es una contradicción. Con lo que, $A_{f_0}(\boldsymbol{y},\boldsymbol{x}) \neq A_{g_0}(\boldsymbol{y},\boldsymbol{x})$. □

De igual forma, probamos que las funciones bent construidas de acuerdo con el corolario 2.2 son todas distintas.

Lema 2.2: *Sean $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $g_0(\boldsymbol{x})$ y $g_1(\boldsymbol{x})$ funciones bent de n variables tales que*

- $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$,
- $f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x})$,
- $g_1(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, $g_1(\boldsymbol{x}) \neq 1 \oplus g_0(\boldsymbol{x})$.

Supongamos también que σ y τ son permutaciones de $\{0,1,2,3\}$. Si $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ y $B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$ son las funciones bent construidas de acuerdo con el corolario 2.2 utilizando las funciones $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$, y la permutación σ, y las funciones $g_0(\boldsymbol{x})$ y $g_1(\boldsymbol{x})$, y la permutación τ, respectivamente, entonces

$$B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) \neq B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}_0$, $\boldsymbol{\xi}_1$, $\boldsymbol{\eta}_0$ y $\boldsymbol{\eta}_1$ son las tablas de verdad de $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $g_0(\boldsymbol{x})$ y $g_1(\boldsymbol{x})$, respectivamente, entonces las tablas de verdad de $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ y $B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$B_{f_0,f_1}: \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_1 \quad \mathbf{I} \oplus \boldsymbol{\xi}_1$$

$$B_{g_0,g_1}: \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_1 \quad \mathbf{I} \oplus \boldsymbol{\eta}_1$$

Como $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, sabemos que $\boldsymbol{\xi}_0 \neq \boldsymbol{\eta}_0$. Por tanto, si suponemos que $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) = B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$, entonces tenemos uno de los siguientes casos:

- $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1$, $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1 \oplus \mathbf{I}$, $\boldsymbol{\xi}_1 = \boldsymbol{\eta}_0$ y $\boldsymbol{\xi}_1 \oplus \mathbf{I} = \boldsymbol{\eta}_0$.
- $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1 \oplus \mathbf{I}$, $\boldsymbol{\xi}_0 = \boldsymbol{\eta}_1$, $\boldsymbol{\xi}_1 = \boldsymbol{\eta}_0$ y $\boldsymbol{\xi}_1 \oplus \mathbf{I} = \boldsymbol{\eta}_0$.

Pero, entonces $f_i(\boldsymbol{x}) = f_i(\boldsymbol{x}) \oplus 1$ y $g_i(\boldsymbol{x}) = g_i(\boldsymbol{x}) \oplus 1$, para $i = 0, 1$, lo que es una contradicción. Por tanto, $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) \neq B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$. □

Una pregunta que nos surge llegados a este punto es la siguiente: partiendo de la misma función bent $f_0(\boldsymbol{x})$ de n variables, ¿pueden coincidir las funciones bent $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ de $n+2$ variables (para cualquier función bent $f_1(\boldsymbol{x})$ de n variables), construidas de acuerdo con los corolarios 2.1 y 2.2? La respuesta es negativa como ponemos de manifiesto en el resultado siguiente.

Lema 2.3: *Sean $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ dos funciones bent de n variables tales que*

$$f_1(\boldsymbol{x}) \neq f_0(\boldsymbol{x}) \quad y \quad f_1(\boldsymbol{x}) \neq 1 \oplus f_0(\boldsymbol{x}),$$

y sean σ y τ permutaciones de $\{0,1,2,3\}$. Supongamos que $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ son las funciones bent construidas de acuerdo con los corolarios 2.1 y 2.2 utilizando la función $f_0(\boldsymbol{x})$ y la permutación σ, y las funciones $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ y la permutación τ, respectivamente. Entonces

$$A_{f_0}(\boldsymbol{y},\boldsymbol{x}) \neq B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: De acuerdo con los corolarios 2.1 y 2.2, tenemos que

$$A_{f_0}(\boldsymbol{y},\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y}),$$

$$B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) = \left(m_{\tau(0)}(\boldsymbol{y}) \oplus m_{\tau(1)}(\boldsymbol{y})\right) f_0(\boldsymbol{x}) \oplus m_{\tau(2)}(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_{\tau(3)}(\boldsymbol{y}) \left(1 \oplus f_1(\boldsymbol{x})\right).$$

Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}_0$ y $\boldsymbol{\xi}_1$ son las tablas de verdad de $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$, respectivamente, entonces las tablas de verdad de $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$A_{f_0}: \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \mathbf{I} \oplus \boldsymbol{\xi}_0$$

$$B_{f_0,f_1}: \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_1 \quad \mathbf{I} \oplus \boldsymbol{\xi}_1$$

Ahora, como $\boldsymbol{\xi}_1 \neq \boldsymbol{\xi}_0$, es evidente que $A_{f_0}(\boldsymbol{y},\boldsymbol{x}) \neq B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$, ya que $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ tiene tres bloques $\boldsymbol{\xi}_0$ y $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ sólo tiene dos bloques $\boldsymbol{\xi}_0$. □

Otra pregunta que nos aparece en este punto es la siguiente: Sean $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$ las funciones bent de $n+2$ variables construidas de acuerdo con los corolarios 2.1 y 2.2, partiendo ahora de las funciones bent de n variables $f_0(\boldsymbol{x})$ y $g_0(\boldsymbol{x})$, respectivamente; ¿si $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$, es posible que $A_{f_0}(\boldsymbol{y},\boldsymbol{x}) = B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$? El resultado siguiente muestra que esta situación no puede ocurrir.

Lema 2.4: *Sean $f_0(\boldsymbol{x})$, $g_0(\boldsymbol{x})$ y $g_1(\boldsymbol{x})$ funciones bent de n variables tales que*

$$f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x}), \quad g_1(\boldsymbol{x}) \neq g_0(\boldsymbol{x}) \quad y \quad g_1(\boldsymbol{x}) \neq 1 \oplus g_0(\boldsymbol{x}).$$

Supongamos que σ y τ son permutaciones de $\{0,1,2,3\}$. Si $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ y $B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x})$ son las funciones bent construidas de acuerdo con los corolarios 2.1 y 2.2 utilizando la función bent $f_0(\boldsymbol{x})$ y la permutación σ, y las funciones bent $g_0(\boldsymbol{x})$ y $g_1(\boldsymbol{x})$ y la permutación τ, respectivamente. Entonces

$$A_{f_0}(\boldsymbol{y},\boldsymbol{x}) \neq B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x}).$$

Demostración: De acuerdo con los corolarios 2.1 y 2.2, tenemos que

$$A_{f_0}(\boldsymbol{y},\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y}),$$

$$B_{g_0,g_1}(\boldsymbol{y},\boldsymbol{x}) = \left(m_{\tau(0)}(\boldsymbol{y}) \oplus m_{\tau(1)}(\boldsymbol{y})\right) g_0(\boldsymbol{x}) \oplus m_{\tau(2)}(\boldsymbol{y}) g_1(\boldsymbol{x}) \oplus m_{\tau(3)}(\boldsymbol{y}) \left(1 \oplus g_1(\boldsymbol{x})\right).$$

Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}_0$, $\boldsymbol{\eta}_0$ y $\boldsymbol{\eta}_1$ son las tablas de verdad de $f_0(\boldsymbol{x})$, $g_0(\boldsymbol{x})$ y $g_1(\boldsymbol{x})$, respectivamente, entonces las tablas

de verdad de $A_{f_0}(\boldsymbol{y}, \boldsymbol{x})$ y $B_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$A_{f_0}: \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \boldsymbol{\xi}_0 \quad \mathbf{I} \oplus \boldsymbol{\xi}_0 \tag{2.3}$$

$$B_{g_0,g_1}: \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_1 \quad \mathbf{I} \oplus \boldsymbol{\eta}_1 \tag{2.4}$$

Como $f_0(\boldsymbol{x}) \neq g_0(\boldsymbol{x})$ tenemos, sin pérdida de generalidad, que

$$f_0(\boldsymbol{x}) = m_i(\boldsymbol{x}) \oplus g_0(\boldsymbol{x})$$

donde $m_i(\boldsymbol{x})$ es un minterm que no está en la expresión de $g_0(\boldsymbol{x})$ como suma de minterms.

Así que, de acuerdo con la expresión (2.3), en la i-ésima posición de cada uno de los cuatro bloques de la tabla de verdad de $A_{f_0}(\boldsymbol{y}, \boldsymbol{x})$, tenemos

$$1 \quad 1 \quad 1 \quad 0$$

pero, de acuerdo con la expresión (2.4), en la i-ésima posición de cada uno de los cuatro bloques de la tabla de verdad de $B_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$, tenemos

$$0 \quad 0 \quad ? \quad ?$$

dependiendo de $g_1(\boldsymbol{x})$. En cada caso, es evidente que ambas tablas de verdad son diferentes. Por tanto, $A_{f_0}(\boldsymbol{y}, \boldsymbol{x}) \neq B_{g_0,g_1}(\boldsymbol{y}, \boldsymbol{x})$. □

Ahora, como consecuencia de los lemas anteriores, podemos obtener el número de funciones bent de $n+2$ variables distintas que podemos obtener de acuerdo con los corolarios 2.1 y 2.2 (o equivalentemente, de acuerdo con el teorema 2.1).

Teorema 2.2: *Si ν_n es el número de funciones bent de n variables, entonces el número de funciones bent de $n+2$ variables que podemos construir utilizando los corolarios 2.1 y 2.2 es*

$$6\nu_n^2 - 8\nu_n. \tag{2.5}$$

DEMOSTRACIÓN: Podemos elegir $f_0(\boldsymbol{x})$ de ν_n formas distintas.

Elegida $f_0(\boldsymbol{x})$, el corolario 2.1 proporciona, de acuerdo con el lema 2.1, cuatro funciones bent de $n+2$ variables. Por tanto, el corolario 2.1 proporciona $4\nu_n$ funciones bent de $n+2$ variables.

Fijada $f_0(\boldsymbol{x})$, si tomamos $f_1(\boldsymbol{x})$ como $f_0(\boldsymbol{x})$ o como $1 \oplus f_0(\boldsymbol{x})$, obtenemos las 4 funciones bent del caso anterior; por tanto, podemos elegir $f_1(\boldsymbol{x})$ entre $\nu_n - 2$ funciones bent y como las elecciones $f_1(\boldsymbol{x}) = g(\boldsymbol{x})$ y $f_1(\boldsymbol{x}) = 1 \oplus g(\boldsymbol{x})$ proporcionan la misma función bent de $n+2$ variables, solamente tenemos $\frac{\nu_n - 2}{2}$ funciones bent posibles. Además, puesto que, de acuerdo con la notación introducida en el corolario 2.2, cualquier permutación de $\{\sigma(0), \sigma(1)\}$ proporciona la misma función bent, tenemos que el corolario 2.2 proporciona, de acuerdo con el lema 2.2,

$$\frac{4!}{2!}\nu_n\frac{\nu_n - 2}{2} \tag{2.6}$$

funciones bent de $n+2$ variables.

Ahora, como los lemas 2.3 y 2.4 garantizan que ninguna función bent construida de acuerdo con el corolario 2.1 coincide con ninguna de las funciones bent construidas de acuerdo con el corolario 2.2, tenemos que

$$4\nu_n + \frac{4!}{2!}\nu_n\frac{\nu_n - 2}{2} = 6\nu_n^2 - 8\nu_n$$

es el número de funciones bent distintas de $n+2$ variables que podemos obtener utilizando los corolarios 2.1 y 2.2 (o equivalentemente, el teorema 2.1). □

En particular, como $\nu_2 = 8$, podemos construir

$$6 \cdot 8^2 - 8 \cdot 8 = 320$$

funciones bent de 4 variables. Notemos que $\nu_4 = 896$, por tanto, la construcción introducida en esta sección no permite obtener todas las funciones bent de 4 variables a partir de las funciones bent de 2 variables.

Tampoco permite obtener todas las funciones bent de 6 variables ya que

$$6\nu_4^2 - 8\nu_4 \quad = \quad 6 \cdot 896^2 - 8 \cdot 896 = 4\,809\,728 \leq 5\,425\,430\,528 = \nu_6.$$

Análogamente, tenemos

$$6\nu_6^2 - 8\nu_6 \quad = \quad 6 \cdot 5\,425\,430\,528^2 - 8 \cdot 5\,425\,430\,528 \approx 2^{67}$$

$$\leq \quad 99\,270\,589\,265\,934\,370\,305\,785\,861\,242\,880 = \nu_8 \approx 2^{106}.$$

Así pues, el teorema 2.2, proporciona una cota inferior del número de funciones bent de $n+2$ variables, en función del número de funciones bent de n variables.

2.2 Construcción basada en una función bent y traslaciones cíclicas

La segunda construcción de funciones bent, que introducimos en este capítulo, se basa en la utilización de una función bent $f(\boldsymbol{x})$ de n variables, algunas permutaciones cíclicas $f(\boldsymbol{x} \oplus \boldsymbol{u})$ de $f(\boldsymbol{x})$ para algunos vectores $\boldsymbol{u} \in \mathbb{F}_2^n$ y los cuatro minterms de dos variables.

Teorema 2.3: *Sea $f(\boldsymbol{x})$ una función bent de n variables y consideremos $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$. Si σ es una permutación cualquiera de $\{0,1,2,3\}$, entonces*

$$G(\boldsymbol{y},\boldsymbol{x}) = m_{\sigma(0)}(\boldsymbol{y})f(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})f(\boldsymbol{x}\oplus\boldsymbol{u}) \oplus m_{\sigma(2)}(\boldsymbol{y})f(\boldsymbol{x}\oplus\boldsymbol{v}) \oplus m_{\sigma(3)}(\boldsymbol{y})\left(1 \oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})\right)$$

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

Demostración: De acuerdo con el teorema 1.2, basta probar que la función booleana

$$G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = G(\boldsymbol{y},\boldsymbol{x}) \oplus G((\boldsymbol{y},\boldsymbol{x}) \oplus (\boldsymbol{b},\boldsymbol{a}))$$

es equilibrada para todo $(\boldsymbol{b},\boldsymbol{a}) \in \mathbb{F}_2^2 \times \mathbb{F}_2^n$ con $(\boldsymbol{b},\boldsymbol{a}) \neq (\mathbf{0}_2,\mathbf{0}_n)$. A continuación, utilizamos el vector $\boldsymbol{b} = (b_1,b_2) \in \mathbb{F}_2^2$ como argumento de las funciones y su representación entera $b = b_1 2 + b_2 \in \mathbb{Z}_{2^2}$ como subíndice de un minterm. Así, por el lema 1.1,

$$\begin{aligned} G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) &= G(\boldsymbol{y},\boldsymbol{x}) \oplus G(\boldsymbol{y}\oplus\boldsymbol{b},\boldsymbol{x}\oplus\boldsymbol{b}) \\ &= m_{\sigma(0)}(\boldsymbol{y})f(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})f(\boldsymbol{x}\oplus\boldsymbol{u}) \oplus m_{\sigma(2)}(\boldsymbol{y})f(\boldsymbol{x}\oplus\boldsymbol{v}) \\ &\quad \oplus m_{\sigma(3)}(\boldsymbol{y})\left(1 \oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})\right) \oplus m_{\sigma(0)\oplus b}(\boldsymbol{y})f(\boldsymbol{x}\oplus\boldsymbol{a}) \oplus m_{\sigma(1)\oplus b}(\boldsymbol{y})f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{a}) \end{aligned}$$

$$\oplus\, m_{\sigma(2)\oplus b}(\boldsymbol{y}) f(\boldsymbol{x}\oplus\boldsymbol{v}\oplus\boldsymbol{a}) \oplus m_{\sigma(3)\oplus b}(\boldsymbol{y})\,(1\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}\oplus\boldsymbol{a}))\,. \tag{2.7}$$

Ahora, para cada $b\in\mathbb{Z}_{2^2}$, si consideramos μ_b la permutación de $\{0,1,2,3\}$ dada por

$$\mu_b(i)=\sigma(i)\oplus b \quad \text{para} \quad i=0,1,2,3,$$

entonces, no es díficil probar que los $4!\cdot 4$ casos correspondientes a los diferentes valores de $\sigma(i)$ y b, se reducen a uno de los siguientes cuatro casos para alguna permutación η de $\{0,1,2,3\}$.

1. $$\begin{aligned} G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) &= m_{\eta(0)}(\boldsymbol{y})\,(f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(1)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(2)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{v}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(3)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}\oplus\boldsymbol{a})) \end{aligned}$$
2. $$\begin{aligned} G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) &= m_{\eta(0)}(\boldsymbol{y})\,(f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(1)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(2)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}\oplus\boldsymbol{a})\oplus 1)\\ &\quad\oplus m_{\eta(3)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{v}\oplus\boldsymbol{a})\oplus 1) \end{aligned}$$
3. $$\begin{aligned} G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) &= m_{\eta(0)}(\boldsymbol{y})\,(f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{v}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(1)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}\oplus\boldsymbol{a})\oplus 1)\\ &\quad\oplus m_{\eta(2)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(3)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{a})\oplus 1) \end{aligned}$$
4. $$\begin{aligned} G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) &= m_{\eta(0)}(\boldsymbol{y})\,(f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}\oplus\boldsymbol{a})\oplus 1)\\ &\quad\oplus m_{\eta(1)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u})\oplus f(\boldsymbol{x}\oplus\boldsymbol{v}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(2)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{a}))\\ &\quad\oplus m_{\eta(3)}(\boldsymbol{y})\,(f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a})\oplus 1)\,. \end{aligned}$$

Notemos que podemos escribir cada uno de los factores que multiplican a $m_{\eta(i)}(\boldsymbol{y})$ para $i=0,1,2,3$, como

$$f(\boldsymbol{z})\oplus f(\boldsymbol{z}\oplus\boldsymbol{a}) \quad \text{o} \quad f(\boldsymbol{z})\oplus f(\boldsymbol{z}\oplus\boldsymbol{a})\oplus 1$$

para $\boldsymbol{z}\in\{\boldsymbol{x},\boldsymbol{x}\oplus\boldsymbol{u},\boldsymbol{x}\oplus\boldsymbol{v},\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}\}$.

Ahora, por el teorema 1.2, como $f(\boldsymbol{z})\oplus f(\boldsymbol{z}\oplus\boldsymbol{a})$ es equilibrada para todo $\boldsymbol{a}\neq\boldsymbol{0}$, tenemos que $G_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ es equilibrada, a menos que $\boldsymbol{a}=\boldsymbol{b}=\boldsymbol{0}$. □

Supongamos que $f(\boldsymbol{x})$ es una función bent de n variables. Para cada $\boldsymbol{w} \in \mathbb{F}_2^n$ sabemos que la función $f_{\boldsymbol{w}}(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{w})$ es también una función bent de n variables y por el teorema 1.1(a) tenemos que

$$\mathrm{Sop}\,(f_{\boldsymbol{w}}) = \{\boldsymbol{a} \oplus \boldsymbol{w} \mid \boldsymbol{a} \in \mathrm{Sop}\,(f)\} = \boldsymbol{w} \oplus \mathrm{Sop}\,(f)\,.$$

Además, como consecuencia del lema 1.2, si utilizamos enteros para los subíndices de los minterms, podemos identificar la permutación σ con una permutación

$$\begin{pmatrix} 0 & 2^n & 2^{n+1} & 2^{n+1}+2^n \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$$

del conjunto $\{0, 2^n, 2^{n+1}, 2^{n+1}+2^n\}$; por tanto, de acuerdo con el teorema 2.3, tenemos que

$$\begin{aligned} \mathrm{Sop}\,(G) = &\{b_0 + a \mid a \in \mathrm{Sop}\,(f)\} \cup \{b_1 + a \mid a \in \mathrm{Sop}\,(f_{\boldsymbol{u}})\} \\ &\cup \{b_2 + a \mid a \in \mathrm{Sop}\,(f_{\boldsymbol{v}})\} \cup \{b_3 + a \mid a \in \mathrm{Sop}\,(f_{\boldsymbol{u} \oplus \boldsymbol{v}})\}\,. \end{aligned} \tag{2.8}$$

En cambio, si para los subíndices de los minterms utilizamos vectores, entonces

$$\begin{aligned} \mathrm{Sop}\,(G) = &\{(\boldsymbol{b}_0, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f)\} \cup \{(\boldsymbol{b}_1, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_{\boldsymbol{u}})\} \\ &\cup \{(\boldsymbol{b}_2, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_{\boldsymbol{v}})\} \cup \{(\boldsymbol{b}_3, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_{\boldsymbol{u} \oplus \boldsymbol{v}})\} \end{aligned} \tag{2.9}$$

donde

$$\begin{pmatrix} \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{2} & \boldsymbol{3} \\ \boldsymbol{b}_0 & \boldsymbol{b}_1 & \boldsymbol{b}_2 & \boldsymbol{b}_3 \end{pmatrix}$$

es una permutación de $\{\boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, \boldsymbol{3}\}$. Notemos que los conjuntos que aparecen en el segundo miembro de las expresiones (2.8) y (2.9) son disjuntos dos a dos por el corolario 1.2.

A continuación, introducimos algunos resultados necesarios para contar el número de funciones bent distintas que podemos construir utilizando el teorema 2.3. Para facilitar dicho cómputo consideramos los tres casos particulares (véanse los corolarios 2.3, 2.4 y 2.5 siguientes) que obtenemos directamente del teorema 2.3. El primero corresponde al caso $\boldsymbol{u} = \boldsymbol{v} = \boldsymbol{0}$; el segundo, al caso $\boldsymbol{u} = \boldsymbol{v} \neq \boldsymbol{0}$ y el tercero, al caso $\boldsymbol{0} \neq \boldsymbol{u} \neq \boldsymbol{v} \neq \boldsymbol{0}$.

Corolario 2.3: *Si $f(\boldsymbol{x})$ es una función bent de n variables y σ es una permutación cualquiera de $\{0,1,2,3\}$, entonces*

$$A'_f(\boldsymbol{y},\boldsymbol{x}) = \left(m_{\sigma(0)}(\boldsymbol{y}) \oplus m_{\sigma(1)}(\boldsymbol{y}) \oplus m_{\sigma(2)}(\boldsymbol{y})\right) f(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}))$$

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

Corolario 2.4: *Si $f(\boldsymbol{x})$ es una función bent de n variables, $\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y σ es una permutación cualquiera de $\{0,1,2,3\}$, entonces*

$$C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}) = m_{\sigma(0)}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus \left(m_{\sigma(1)}(\boldsymbol{y}) \oplus m_{\sigma(2)}(\boldsymbol{y})\right) f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_{\sigma(3)}(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}))$$

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

Corolario 2.5: *Si $f(\boldsymbol{x})$ es una función bent de n variables, $\boldsymbol{u},\boldsymbol{v} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$, con $\boldsymbol{u} \neq \boldsymbol{v}$ y σ es una permutación cualquiera de $\{0,1,2,3\}$, entonces*

$$D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}) = m_{\sigma(0)}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_{\sigma(2)}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{v}) \oplus m_{\sigma(3)}(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v}))$$

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

A continuación introducimos algunos resultados que nos pemitirán probar bajo qué condiciones los corolarios anteriores producen funciones bent distintas.

El resultado siguiente establece que las funciones bent de $n+2$ variables obtenidas utilizando el corolario 2.3 son todas distintas entre sí (la demostración es análoga a la del lema 2.1 y por tanto la omitimos). De hecho, como se comprobará más adelante, ambas construcciones son idénticas.

Lema 2.5: *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $A'_f(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.3 utilizando $f(\boldsymbol{x})$ y la permutación σ de $\{0,1,2,3\}$. Supongamos también que $A'_g(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.3 utilizando $g(\boldsymbol{x})$ y la permutación*

τ de $\{0,1,2,3\}$. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces

$$A'_f(\boldsymbol{y},\boldsymbol{x}) \neq A'_g(\boldsymbol{y},\boldsymbol{x}).$$

Igual que en el caso anterior, el resultado siguiente establece que las funciones bent obtenidas utilizando el corolario 2.4 son todas distintas entre sí.

Lema 2.6: *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.4 utilizando $f(\boldsymbol{x})$, el vector $\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y la permutación σ de $\{0,1,2,3\}$. Supongamos también que $C_{g,\boldsymbol{a}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.4 utilizando $g(\boldsymbol{x})$, el vector $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y la permutación τ de $\{0,1,2,3\}$. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces*

$$C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}) \neq C_{g,\boldsymbol{a}}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}$ y $\boldsymbol{\eta}$ son las tablas de verdad de $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$ y $C_{g,\boldsymbol{a}}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$C_{f,\boldsymbol{u}}: \quad \boldsymbol{\xi} \quad \boldsymbol{\xi}_{\boldsymbol{u}} \quad \boldsymbol{\xi}_{\boldsymbol{u}} \quad \mathbf{I} \oplus \boldsymbol{\xi}$$

$$C_{g,\boldsymbol{a}}: \quad \boldsymbol{\eta} \quad \boldsymbol{\eta}_{\boldsymbol{a}} \quad \boldsymbol{\eta}_{\boldsymbol{a}} \quad \mathbf{I} \oplus \boldsymbol{\eta}$$

donde $\boldsymbol{\xi}_{\boldsymbol{u}}$ y $\boldsymbol{\eta}_{\boldsymbol{a}}$ son las tablas de verdad de $f(\boldsymbol{x} \oplus \boldsymbol{u})$ y $g(\boldsymbol{x} \oplus \boldsymbol{a})$, respectivamente.

Si $C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}) = C_{g,\boldsymbol{a}}(\boldsymbol{y},\boldsymbol{x})$, entonces los cuatro bloques de la segunda fila son una permutación de los cuatro bloques de la primera fila. Pero si consideramos los 4! casos correspondientes a esas permutaciones, obtenemos que $f(\boldsymbol{x}) = g(\boldsymbol{x})$, o que $\boldsymbol{a} = \boldsymbol{0}$, o que $\boldsymbol{u} = \boldsymbol{0}$, o bien que $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ ambas tienen el mismo número de minterms y el número complementario de minterms. Así que, en cualquiera de los casos obtenemos una contradicción y, por tanto, $C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}) \neq C_{g,\boldsymbol{a}}(\boldsymbol{y},\boldsymbol{x})$. □

Sin embargo, en contra de lo que podíamos pensar a la vista de los dos resultados anteriores, no todas las funciones bent construidas de acuerdo con el corolario 2.5 son distintas entre sí como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 2.1: Supongamos que $n = 2$ y consideremos los vectores

$$\boldsymbol{u} = \mathbf{1} = (0,1) \quad \text{y} \quad \boldsymbol{v} = \mathbf{2} = (1,0)$$

y la función bent de 2 variables $f(\boldsymbol{x}) = m_0(\boldsymbol{x})$. Entonces, de acuerdo con el corolario 2.5, la expresión (1.1), el lema 1.1 y el corolario 1.2, tenemos que

$$\begin{aligned}
&D_{f,\mathbf{1},\mathbf{2}}(\boldsymbol{y},\boldsymbol{x}) \\
&= m_0(\boldsymbol{y})f(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})f(\boldsymbol{x}\oplus\mathbf{1}) \oplus m_2(\boldsymbol{y})f(\boldsymbol{x}\oplus\mathbf{2}) \oplus m_3(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}\oplus\mathbf{3})) \\
&= m_0(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})\,(1 \oplus m_3(\boldsymbol{x})) \\
&= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{13}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x})
\end{aligned}$$

es una función bent de $n+2 = 4$ variables.

Por otro lado, si consideramos los vectores

$$\boldsymbol{a} = \mathbf{1} = (0,1) \quad \text{y} \quad \boldsymbol{b} = \mathbf{3} = (1,1)$$

y la función bent de 2 variables $g(\boldsymbol{x}) = m_1(\boldsymbol{x})$, de nuevo, por la expresión (1.1), el lema 1.1 y los corolarios 1.2 y 2.5, tenemos que

$$\begin{aligned}
&D_{g,\mathbf{1},\mathbf{3}}(\boldsymbol{y},\boldsymbol{x}) \\
&= m_1(\boldsymbol{y})g(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})g(\boldsymbol{x}\oplus\mathbf{1}) \oplus m_2(\boldsymbol{y})g(\boldsymbol{x}\oplus\mathbf{3}) \oplus m_3(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}\oplus\mathbf{2})) \\
&= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{13}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x})
\end{aligned}$$

es una función bent de $n+2 = 4$ variables.

Claramente, $D_{g,\mathbf{1},\mathbf{3}}(\boldsymbol{y},\boldsymbol{x}) = D_{f,\mathbf{1},\mathbf{2}}(\boldsymbol{y},\boldsymbol{x})$ ya que ambas funciones tienen la misma expresión como suma de minterms. ■

Si analizamos un poco el ejemplo anterior, para poder estudiar bajo qué condiciones podemos obtener funciones bent distintas basadas en la construcción del corolario 2.5, observamos que $g(\boldsymbol{x}) = f(\boldsymbol{x}\oplus\mathbf{1})$ y que $\{\mathbf{1},\mathbf{2}\}$ y $\{\mathbf{1},\mathbf{3}\}$ son bases del mismo subespacio vectorial $\{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}$ de $\mathbb{F}_2^2$.

Con el objetivo de evitar estas situaciones que proporcionan funciones bent idénticas, consideramos sólo vectores $\boldsymbol{u},\boldsymbol{v} \in \mathbb{F}_2^n$ tales que $\{\boldsymbol{u},\boldsymbol{v}\}$ sea una base de Gauss-Jordan de cardinalidad 2. Recordemos que un conjunto $\{\boldsymbol{u}_1,\boldsymbol{u}_2,\ldots,\boldsymbol{u}_k\} \subseteq \mathbb{F}_2^n$ es una

base de Gauss-Jordan de cardinalidad k si la matriz, cuyas filas son los vectores $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$, es escalonada reducida (véase, por ejemplo [9, 39]).

Así, nuestro próximo resultado establece que las funciones bent construidas de acuerdo con el corolario 2.5 son distintas dos a dos, si $\{\boldsymbol{u}, \boldsymbol{v}\}$ es una base de Gauss-Jordan de cardinalidad 2 de $\mathbb{F}_2^n$.

Lema 2.7: *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.5 utilizando $f(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{u}, \boldsymbol{v}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$ y la permutación σ de $\{0, 1, 2, 3\}$. Supongamos también que $D_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.5 utilizando $g(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a}, \boldsymbol{b}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$ y la permutación τ de $\{0, 1, 2, 3\}$. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces*

$$D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}) \neq D_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}$ y $\boldsymbol{\eta}$ son las tablas de verdad de $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ y $D_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$\begin{array}{lcccc} D_{f,\boldsymbol{u},\boldsymbol{v}}: & \boldsymbol{\xi} & \boldsymbol{\xi}_{\boldsymbol{u}} & \boldsymbol{\xi}_{\boldsymbol{v}} & \mathbf{I} \oplus \boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}} \\ D_{g,\boldsymbol{a},\boldsymbol{b}}: & \boldsymbol{\eta} & \boldsymbol{\eta}_{\boldsymbol{a}} & \boldsymbol{\eta}_{\boldsymbol{b}} & \mathbf{I} \oplus \boldsymbol{\eta}_{\boldsymbol{a}\oplus\boldsymbol{b}} \end{array}$$

donde $\boldsymbol{\xi}_{\boldsymbol{u}}$, $\boldsymbol{\xi}_{\boldsymbol{v}}$, $\boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}}$, $\boldsymbol{\eta}_{\boldsymbol{a}}$, $\boldsymbol{\eta}_{\boldsymbol{b}}$ y $\boldsymbol{\eta}_{\boldsymbol{a}\oplus\boldsymbol{b}}$ son las tablas de verdad de $f(\boldsymbol{x} \oplus \boldsymbol{u})$, $f(\boldsymbol{x} \oplus \boldsymbol{v})$, $f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})$, $g(\boldsymbol{x} \oplus \boldsymbol{a})$, $g(\boldsymbol{x} \oplus \boldsymbol{b})$ y $g(\boldsymbol{x} \oplus \boldsymbol{a} \oplus \boldsymbol{b})$, respectivamente.

Si $D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}) = D_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$, entonces los cuatro bloques de la segunda fila son una permutación de los cuatro bloques de la primera fila. Pero si consideramos los 4! casos correspondientes a esas permutaciones, obtenemos que $f(\boldsymbol{x}) = g(\boldsymbol{x})$ o que $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ tienen ambas el mismo número de minterms y el número complementario de minterms, o que

$$(\boldsymbol{a}, \boldsymbol{b}) \in \{(\boldsymbol{u}, \boldsymbol{u} \oplus \boldsymbol{v}), (\boldsymbol{v}, \boldsymbol{u} \oplus \boldsymbol{v}), (\boldsymbol{u} \oplus \boldsymbol{v}, \boldsymbol{u}), (\boldsymbol{u} \oplus \boldsymbol{v}, \boldsymbol{v})\};$$

para este último caso, notemos que si $\{\boldsymbol{u}, \boldsymbol{v}\}$ es una base de Gauss-Jordan de cardinalidad 2, entonces $\{\boldsymbol{a}, \boldsymbol{b}\}$ no puede ser una base de Gauss-Jordan de car-

dinalidad 2. Así que, en cualquier caso obtenemos una contradicción y, por tanto, $D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}) \neq D_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$. □

Nuestro próximo resultado establece que ninguna de las funciones bent obtenidas por alguno de los corolarios 2.3, 2.4 y 2.5, puede obtenerse por alguno de los otros dos corolarios implicados.

Lema 2.8: *Sean $f(\boldsymbol{x})$, $g(\boldsymbol{x})$ y $h(\boldsymbol{x})$ tres funciones bent de n variables (no necesariamente distintas). Supongamos que $A'_f(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.3 utilizando $f(\boldsymbol{x})$ y la permutación σ de $\{0,1,2,3\}$. Supongamos que $C_{g,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.4 utilizando $g(\boldsymbol{x})$, el vector $\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y la permutación τ de $\{0,1,2,3\}$. Finalmente, supongamos que $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 2.5 utilizando $h(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a},\boldsymbol{b}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$ y la permutación ω de $\{0,1,2,3\}$. Entonces*

$$A'_f(\boldsymbol{y},\boldsymbol{x}) \neq C_{g,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}), \quad A'_f(\boldsymbol{y},\boldsymbol{x}) \neq D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \quad y \quad C_{g,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}) \neq D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}$, $\boldsymbol{\eta}$ y $\boldsymbol{\zeta}$ son las tablas de verdad de $f(\boldsymbol{x})$, $g(\boldsymbol{x})$ y $h(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $A'_f(\boldsymbol{y},\boldsymbol{x})$, $C_{g,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$ y $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$\begin{array}{rcccc} A'_f: & \boldsymbol{\xi} & \boldsymbol{\xi} & \boldsymbol{\xi} & \mathbf{I} \oplus \boldsymbol{\xi} \\ C_{g,\boldsymbol{u}}: & \boldsymbol{\eta} & \boldsymbol{\eta}_{\boldsymbol{u}} & \boldsymbol{\eta}_{\boldsymbol{u}} & \mathbf{I} \oplus \boldsymbol{\eta} \\ D_{h,\boldsymbol{a},\boldsymbol{b}}: & \boldsymbol{\zeta} & \boldsymbol{\zeta}_{\boldsymbol{a}} & \boldsymbol{\zeta}_{\boldsymbol{b}} & \mathbf{I} \oplus \boldsymbol{\zeta}_{\boldsymbol{a}\oplus\boldsymbol{b}} \end{array}$$

donde $\boldsymbol{\eta}_{\boldsymbol{u}}$, $\boldsymbol{\zeta}_{\boldsymbol{a}}$, $\boldsymbol{\zeta}_{\boldsymbol{b}}$ y $\boldsymbol{\zeta}_{\boldsymbol{a}\oplus\boldsymbol{b}}$ son las tablas de verdad de $g(\boldsymbol{x}\oplus\boldsymbol{u})$, $h(\boldsymbol{x}\oplus\boldsymbol{a})$, $h(\boldsymbol{x}\oplus\boldsymbol{b})$ y $h(\boldsymbol{x}\oplus\boldsymbol{a}\oplus\boldsymbol{b})$, respectivamente.

El resultado es ahora evidente ya que $A'_f(\boldsymbol{y},\boldsymbol{x})$ tiene tres bloques iguales, $C_{g,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$ tiene sólo dos bloques iguales, y todos los bloques de $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ son distintos. □

Ahora, como consecuencia de los lemas anteriores, podemos obtener el número de funciones bent de $n+2$ variables que podemos construir de acuerdo con los corolarios 2.3, 2.4 y 2.5.

Teorema 2.4: *Si ν_n es el número de funciones bent de n variables, entonces utilizando los corolarios 2.3, 2.4 y 2.5 podemos construir*

$$2^{2n+2}\nu_n$$

funciones bent de $n+2$ variables distintas.

DEMOSTRACIÓN: De acuerdo con el lema 2.5, el corolario 2.3 proporciona

$$\frac{4!}{3!}\nu_n \tag{2.10}$$

funciones bent de $n+2$ variables.

Análogamente, de acuerdo con el lema 2.6, el corolario 2.4 proporciona

$$\frac{4!}{2!}\nu_n(2^n-1) \tag{2.11}$$

funciones bent de $n+2$ variables.

Finalmente, de acuerdo con el lema 2.7, el corolario 2.5 proporciona

$$4!\nu_n N(n,2) \tag{2.12}$$

funciones bent de $n+2$ variables, donde $N(n,2)$ es el número de bases de Gauss-Jordan de cardinalidad 2 en $\mathbb{F}_2^n$; ahora, teniendo en cuenta que cada subespacio vectorial de dimensión 2 tiene una única base de Gauss-Jordan de cardinalidad 2, tenemos que $N(n,2)$ es el número de subespacios vectoriales de dimensión 2 en $\mathbb{F}_2^n$; por tanto (véase [76, pág 46])

$$N(n,2) = \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} = \frac{(2^n-1)(2^{n-1}-1)}{3}. \tag{2.13}$$

Puesto que el lema 2.8 garantiza que las funciones construidas de acuerdo con los corolarios 2.3, 2.4 y 2.5 son todas distintas, sustituyendo la expresión (2.13) en la expresión (2.12) y sumando las expresiones (2.10), (2.11) y (2.12), tenemos que

$$\begin{aligned}&\frac{4!}{3!}\nu_n + \frac{4!}{2!}\nu_n(2^n-1) + 4!\nu_n\frac{(2^n-1)(2^{n-1}-1)}{3}\\ &= \frac{4!}{3!}\nu_n\left(1+3(2^n-1)+2(2^n-1)(2^{n-1}-1)\right)\end{aligned}$$

$$
\begin{aligned}
&= 4\nu_n \left(1 + (2^n - 1)\left(3 + 2(2^{n-1} - 1)\right)\right) \\
&= 4\nu_n \left(1 + (2^n - 1)(2^n + 1)\right) \\
&= 2^{2n+2}\nu_n. \qquad \square
\end{aligned}
$$

Puesto que $\nu_2 = 8$, $\nu_4 = 896$ y $\nu_6 = 5\,425\,430\,528$ tenemos que los corolarios 2.3, 2.4 y 2.5 (o equivalentemente, el teorema 2.3), proporcionan

$$2^{2\cdot 2+2}\nu_2 = 512 < 896, \quad 2^{2\cdot 4+2}\nu_4 = 917\,504 < 5\,425\,430\,528$$

y

$$2^{2\cdot 6+2}\nu_6 \approx 2^{45} < 99\,270\,589\,265\,934\,370\,305\,785\,861\,242\,880 \approx 2^{106}$$

funciones bent de 4, 6 y 8 variables, respectivamente.

2.3 Comparación con otros métodos

En esta sección comparamos las construcciones introducidas en este capítulo, primero entre ellas (para ver si las funciones bent que proporcionan ambas construcciones son distintas entre sí) y también con las construcciones clásicas introducidas en la sección 1.3.

2.3.1 Construcción basada en dos funciones bent y construcción basada en una función bent

En primer lugar comparamos las construcciones de funciones bent introducidas en las secciones 2.1 y 2.2.

Es fácil comprobar, utilizando la expresión (1.1), que cada una de las funciones $A'_f(\boldsymbol{y}, \boldsymbol{x})$ construidas de acuerdo con el corolario 2.3, coincide con alguna de las funciones $A_f(\boldsymbol{y}, \boldsymbol{x})$ construida de acuerdo con el corolario 2.1; por tanto, al variar $f(\boldsymbol{x})$ en el conjunto de todas las funciones bent de n variables, tenemos que ambos corolarios proporcionan las mismas funciones bent de $n+2$ variables. Así, si llamamos **construcción** A a la proporcionada por el corolario 2.1 (o equivalentemente, por el corolario 2.3), el teorema 2.2 (o equivalentemente, el teorema 2.4) afirma que el

número de funciones bent de $n+2$ variables que proporciona esta construcción es $4\nu_n$.

Notemos que, de acuerdo con los lemas 2.4 y 2.8, ninguna de las funciones bent construidas de acuerdo con la construcción A puede coincidir con ninguna de las funciones bent obtenidas de acuerdo con los corolarios 2.2, 2.4 y 2.5.

También es evidente que podemos obtener las funciones bent $C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$, construidas de acuerdo con el corolario 2.4, a partir del corolario 2.2 si tomamos

$$(f_0(\boldsymbol{x}),f_1(\boldsymbol{x}))=(f(\boldsymbol{x}\oplus\boldsymbol{u}),f(\boldsymbol{x}))\quad\text{o}\quad(f_0(\boldsymbol{x}),f_1(\boldsymbol{x}))=(f(\boldsymbol{x}\oplus\boldsymbol{u}),1\oplus f(\boldsymbol{x})).$$

De hecho, para $n=2$, las construcciones de los corolarios 2.2 y 2.4 proporcionan las mismas funciones bent de $n+2=4$ variables. Sin embargo, el siguiente resultado establece que éste es el único caso donde ambas construcciones proporcionan la misma función bent.

Teorema 2.5: *Sean $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$ y $f(\boldsymbol{x})$ funciones bent de n variables (con $n\geq 4$) y consideremos $\boldsymbol{u}\in\mathbb{F}_2^n\setminus\{\boldsymbol{0}\}$. Si*

$$(f_0(\boldsymbol{x}),f_1(\boldsymbol{x}))\neq(f(\boldsymbol{x}\oplus\boldsymbol{u}),f(\boldsymbol{x}))\quad y\quad(f_0(\boldsymbol{x}),f_1(\boldsymbol{x}))\neq(f(\boldsymbol{x}\oplus\boldsymbol{u}),1\oplus f(\boldsymbol{x})),$$

entonces

$$B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})\neq C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\eta}_0$, $\boldsymbol{\eta}_1$, $\boldsymbol{\xi}$ y $\boldsymbol{\xi}_{\boldsymbol{u}}$ son las tablas de verdad de las funciones $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $f(\boldsymbol{x})$ y $f(\boldsymbol{x}\oplus\boldsymbol{u})$ respectivamente, entonces, de acuerdo con los corolarios 2.2 y 2.4, las tablas de verdad de las funciones $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})$ y $C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$B_{f_0,f_1}:\quad \boldsymbol{\eta}_0\quad \boldsymbol{\eta}_0\quad \boldsymbol{\eta}_1\quad \mathbf{I}\oplus\boldsymbol{\eta}_1$$

$$C_{f,\boldsymbol{u}}:\quad \boldsymbol{\xi}\quad \boldsymbol{\xi}_{\boldsymbol{u}}\quad \boldsymbol{\xi}_{\boldsymbol{u}}\quad \mathbf{I}\oplus\boldsymbol{\xi}$$

Si $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x})=C_{f,\boldsymbol{u}}(\boldsymbol{y},\boldsymbol{x})$, entonces los cuatro bloques de la segunda fila son una permutación de los cuatro bloques de la primera fila. Pero si consideramos los 4! casos correspondientes a esas permutaciones, obtenemos alguna de las cinco condiciones siguientes:

- $\boldsymbol{u} = \mathbf{0}$,
- $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x})) = (f(\boldsymbol{x} \oplus \boldsymbol{u}), f(\boldsymbol{x}))$,
- $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x})) = (f(\boldsymbol{x} \oplus \boldsymbol{u}), 1 \oplus f(\boldsymbol{x}))$,
- $f(\boldsymbol{x} \oplus \boldsymbol{u}) = 1 \oplus f(\boldsymbol{x})$,
- $f(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$.

Por tanto, cualquiera de los casos anteriores produce una contradicción y, en consecuencia, $B_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) \neq C_{f,\boldsymbol{u}}(\boldsymbol{y}, \boldsymbol{x})$. □

A partir de ahora, llamamos **construcción** B **y** C a las construcciones proporcionadas por los corolarios 2.2 y 2.4, respectivamente. Así, de acuerdo con lo dicho anteriormente, para $n = 2$ las construcciones B y C proporcionan las mismas funciones bent de 4 variables. Sin embargo, para $n \geq 4$, los teoremas 2.4 y 2.5 garantizan que la construcción B proporciona, de acuerdo con las expresiones (2.6) y (2.11)

$$\frac{4!}{2!}\nu_n \frac{\nu_n - 2}{2} - \frac{4!}{2}\nu_n \left(2^n - 1\right) = 6\nu_n \left(\nu_n - 2^{n+1}\right)$$

funciones bent de $n+2$ variables que no se pueden obtener mediante la construcción C.

Ahora, si llamamos **construcción** D a la construcción proporcionada por el corolario 2.5, el siguiente resultado establece que ninguna de las funciones bent de la construcción B se puede obtener a partir de la construcción D y viceversa.

Teorema 2.6: *Sean $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$ y $f(\boldsymbol{x})$ funciones bent de n variables y supongamos que $\{\boldsymbol{u}, \boldsymbol{v}\}$ es una base de Gauss-Jordan de cardinalidad 2 de $\mathbb{F}_2^n$, entonces*

$$B_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x}) \neq D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\eta}_0$, $\boldsymbol{\eta}_1$, $\boldsymbol{\xi}$, $\boldsymbol{\xi}_{\boldsymbol{u}}$, $\boldsymbol{\xi}_{\boldsymbol{v}}$ y $\boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}}$ son las tablas de verdad de las funciones $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $f(\boldsymbol{x})$, $f(\boldsymbol{x}\oplus\boldsymbol{u})$, $f(\boldsymbol{x}\oplus\boldsymbol{v})$ y $f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})$, respectivamente, entonces, de acuerdo con los corolarios 2.2 y 2.5, las tablas de verdad de las funciones $B_{f_0,f_1}(\boldsymbol{y}, \boldsymbol{x})$ y $D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$B_{f_0,f_1}: \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_0 \quad \boldsymbol{\eta}_1 \quad \mathbf{1} \oplus \boldsymbol{\eta}_1$$

$$D_{f,\boldsymbol{u},\boldsymbol{v}}: \quad \boldsymbol{\xi} \quad \boldsymbol{\xi}_{\boldsymbol{u}} \quad \boldsymbol{\xi}_{\boldsymbol{v}} \quad \mathbf{1} \oplus \boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}}$$

Si $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) = D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$, entonces los cuatro bloques de la segunda fila son una permutación de los cuatro bloques de la primera fila. Pero si consideramos los 4! casos correspondientes a estas permutaciones, obtenemos alguna de las cinco condiciones siguientes:

- $\boldsymbol{u} = \boldsymbol{0}$,
- $\boldsymbol{v} = \boldsymbol{0}$,
- $\boldsymbol{u} = \boldsymbol{v}$,
- $f(\boldsymbol{x} \oplus \boldsymbol{u}) = 1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})$,
- $f(\boldsymbol{x} \oplus \boldsymbol{v}) = 1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})$.

Por tanto, cualquiera de los casos anteriores produce una contradicción y, en consecuencia, $B_{f_0,f_1}(\boldsymbol{y},\boldsymbol{x}) \neq D_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$. □

Así pues, el teorema 2.6 y las expresiones (2.12) y (2.13) aseguran que el número de funciones bent distintas de $n+2$ variables que proporciona la construcción D es

$$4!\nu_n \frac{(2^n-1)\,(2^{n-1}-1)}{3} = 8\nu_n(2^n-1)(2^{n-1}-1). \tag{2.14}$$

Finalmente, como consecuencia de los teoremas 2.2 y 2.4, y los comentarios anteriores, obtenemos el resultado siguiente que establece el número de funciones bent de $n+2$ variables que proporcionan las construcciones A, B, C y D.

Teorema 2.7: *Si ν_n es el número de funciones bent de n variables, entonces el número de funciones bent de $n+2$ variables que podemos construir de acuerdo con las teoremas 2.1 y 2.3 (es decir, las construcciones A, B, C y D) es*

$$6\nu_n^2 + 2^{n+2}\,(2^n-3)\,\nu_n.$$

DEMOSTRACIÓN: De acuerdo con lo dicho anteriormente, la construcción A proporciona $4\nu_n$ funciones bent de $n+2$ variables.

Análogamente, la construcción B proporciona $6\nu_n\,(\nu_n - 2^{n+1})$ funciones bent de $n+2$ variables que no se pueden obtener a partir de la construcción C.

La construcción C proporciona $12\nu_n(2^n-1)$ funciones bent de $n+2$ variables.

Finalmente, la construcción D proporciona $8\nu_n(2^n-1)(2^{n-1}-1)$ funciones bent de $n+2$ variables.

Ahora, como todas estas funciones son distintas, tenemos que las construcciones A, B, C y D proporcionan

$$\begin{aligned}
&4\nu_n + 6\nu_n\left(\nu_n - 2^{n+1}\right) + 12\nu_n(2^n-1) + 8\nu_n\left(2^n-1\right)\left(2^{n-1}-1\right)\\
&= \nu_n\left(4 + 6\nu_n - 12\cdot 2^n + 12\cdot 2^n + 12 + 8\left(2^{2n-1} - 3\cdot 2^{n-1} + 1\right)\right)\\
&= \nu_n\left(6\nu_n + 2^{2n+2} - 3\cdot 2^{n+2}\right)\\
&= 6\nu_n^2 + 2^{n+2}(2^n-3)\nu_n
\end{aligned}$$

funciones bent de $n+2$ variables. □

2.3.2 Clase Rothaus

A continuación mostramos algunos ejemplos de funciones bent obtenidas a través de las construcciones dadas en este capítulo que no son funciones bent de clase Rothaus.

Para el caso $n = 2$ hemos comprobado que las funciones bent de 4 variables correspondientes a las contrucciones A y B son todas de la clase Rothaus, construyendo todas las funciones bent de esta clase computacionalmente.

Para el caso $n = 4$ hemos obtenido, de forma aleatoria, funciones bent de 6 variables pertenecientes a las contrucciones A y B pero no hemos conseguido determinar si eran o no de la clase Rothaus, pues para su comprobación nos hemos basado en la aparición o no del monomio y_1y_2 de las nuevas variables, lo cual es una condición necesaria pero no suficiente. En todas las funciones bent obtenidas aparecía dicho monomio, lo cual no significa que sean de la clase Rothaus, pero comprobarlo resulta una tarea muy ardua pues se han de expresar estas funciones a través de tres funciones bent de 4 variables satisfaciendo las condiciones del teorema 1.3(b). Nos bastaría con encontrar un ejemplo donde no apareciese el término y_1y_2, de las nuevas variables, para probar que dicha función no es de la clase Rothaus. Aún no lo hemos conseguido.

Ejemplo 2.2: Supongamos que $n = 2$ y consideremos la función bent de 2 variables

$$f(\boldsymbol{x}) = m_1(\boldsymbol{x}),$$

los vectores $\boldsymbol{u} = \mathbf{2} = (1,0)$, $\boldsymbol{v} = \mathbf{1} = (0,1)$ y la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & 2 \end{pmatrix}.$$

Entonces, a partir del corolario 2.5, la expresión (1.1), el lema 1.1 y el corolario1.2, obtenemos la función bent de 4 variables

$$\begin{aligned}
&D(\boldsymbol{y},\boldsymbol{x}) \\
&= m_0(\boldsymbol{y})f(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})f(\boldsymbol{x}\oplus\mathbf{2}) \oplus m_1(\boldsymbol{y})f(\boldsymbol{x}\oplus\mathbf{1}) \oplus m_2(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}\oplus\mathbf{1}\oplus\mathbf{2})) \\
&= m_0(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})m_3(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})\,(1 \oplus m_2(\boldsymbol{x})) \\
&= m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_8(\boldsymbol{y},\boldsymbol{x}) \oplus m_9(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}) \\
&= (1\oplus y_1)(1\oplus y_2)(1\oplus x_1)(1\oplus 1\oplus x_2) \oplus (1\oplus y_1)(1\oplus 1\oplus y_2)(1\oplus x_1)(1\oplus x_2) \\
&\oplus (1\oplus 1\oplus y_1)(1\oplus y_2)(1\oplus x_1)(1\oplus x_2) \oplus (1\oplus 1\oplus y_1)(1\oplus y_2)(1\oplus x_1)(1\oplus 1\oplus x_2) \\
&\oplus (1\oplus 1\oplus y_1)(1\oplus y_2)(1\oplus 1\oplus x_1)(1\oplus 1\oplus x_2) \\
&\oplus (1\oplus 1\oplus y_1)(1\oplus 1\oplus y_2)(1\oplus 1\oplus x_1)(1\oplus 1\oplus x_2) \\
&= (1\oplus y_1\oplus y_2\oplus y_1y_2)(x_2\oplus x_1x_2) \oplus (y_2\oplus y_1y_2)(1\oplus x_1\oplus x_2\oplus x_1x_2) \\
&\oplus (y_1\oplus y_1y_2)(1\oplus x_1\oplus x_2\oplus x_1x_2) \oplus (y_1\oplus y_1y_2)(x_2\oplus x_1x_2) \oplus (y_1\oplus y_1y_2)x_1x_2 \\
&\oplus y_1y_2x_1x_2 \\
&= x_2 \oplus x_1x_2 \oplus y_1x_2 \oplus y_1x_1x_2 \oplus y_2x_2 \oplus y_2x_1x_2 \oplus y_1y_2x_2 \oplus y_1y_2x_1x_2 \oplus y_2 \oplus y_2x_1 \\
&\oplus y_2x_2 \oplus y_2x_1x_2 \oplus y_1y_2 \oplus y_1y_2x_1 \oplus y_1y_2x_2 \oplus y_1y_2x_1x_2 \oplus y_1 \oplus y_1x_1 \oplus y_1x_2 \oplus y_1x_1x_2 \\
&\oplus y_1y_2 \oplus y_1y_2x_1 \oplus y_1y_2x_2 \oplus y_1y_2x_1x_2 \oplus y_1x_2 \oplus y_1x_1x_2 \oplus y_1y_2x_2 \oplus y_1y_2x_1x_2 \\
&\oplus y_1x_1x_2 \oplus y_1y_2x_1x_2 \oplus y_1y_2x_1x_2 \\
&= x_2 \oplus y_1 \oplus y_2 \oplus x_1x_2 \oplus x_1y_1 \oplus x_1y_2 \oplus x_2y_1.
\end{aligned}$$

Si observamos su FNA tenemos que no contiene el monomio y_1y_2 (que correspondería al término $x_{n+1}x_{n+2}$ de las nuevas variables) y por el comentario que aparece después del teorema 1.3, podemos asegurar que dicha función no es de la clase Rothaus. ■

2.3.3 Clase Maiorana-McFarland

Ahora mostramos algunos ejemplos de funciones bent obtenidas a través de las dos construcciones presentadas en este capítulo, que no son funciones de la clase Maiorana-McFarland.

Ejemplo 2.3: Supongamos que $n = 2$ y consideremos las funciones bent de 2 variables

$$f_0(\boldsymbol{x}) = m_0(\boldsymbol{x}) \quad \text{y} \quad f_1(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}).$$

De acuerdo con el teorema 2.1, el corolario 1.2 y la expresión (1.1), la función booleana $F(\boldsymbol{y}, \boldsymbol{x})$ de 4 variables dada por

$$\begin{aligned}
&F(\boldsymbol{y}, \boldsymbol{x}) \\
&= (m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}))f_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})f_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})(1 \oplus f_1(\boldsymbol{x})) \\
&= (m_0(\boldsymbol{y}) \oplus m_1(\boldsymbol{y}))m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})\,(m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})) \oplus m_3(\boldsymbol{y})(m_2(\boldsymbol{x})) \\
&= m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_4(\boldsymbol{y}, \boldsymbol{x}) \oplus m_8(\boldsymbol{y}, \boldsymbol{x}) \oplus m_9(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{11}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{14}(\boldsymbol{y}, \boldsymbol{x}) \\
&= (1 \oplus y_1)(1 \oplus y_2)(1 \oplus x_1)(1 \oplus x_2) \oplus (1 \oplus y_1)(1 \oplus 1 \oplus y_2)(1 \oplus x_1)(1 \oplus x_2) \\
&\oplus (1 \oplus 1 \oplus y_1)(1 \oplus y_2)(1 \oplus x_1)(1 \oplus x_2) \oplus (1 \oplus 1 \oplus y_1)(1 \oplus y_2)(1 \oplus x_1)(1 \oplus 1 \oplus x_2) \\
&\oplus (1 \oplus 1 \oplus y_1)(1 \oplus y_2)(1 \oplus 1 \oplus x_1)(1 \oplus 1 \oplus x_2) \\
&\oplus (1 \oplus 1 \oplus y_1)(1 \oplus 1 \oplus y_2)(1 \oplus 1 \oplus x_1)(1 \oplus x_2) \\
&= 1 \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus y_1x_2 \oplus y_1y_2
\end{aligned}$$

es una función bent. Sin embargo, no pertenece a la clase Maiorana-McFarland ya que no existe ninguna permutación π de $\mathbb{F}_2^{\frac{n+2}{2}}$ tal que dicha función pueda expresarse como una de las funciones bent definidas a partir del teorema 1.4. Esto se puede comprobar fácilmente a través de su FNA, ya que el término x_1x_2 no se ajusta con la expresión $\langle \boldsymbol{x}, \pi(\boldsymbol{y}) \rangle \oplus f(\boldsymbol{y})$ de una función bent de la clase Maiorana-McFarland. ■

Ejemplo 2.4: Supongamos que $n = 2$ y consideremos la función bent de 2 variables

$$f(\boldsymbol{x}) = m_0(\boldsymbol{x}),$$

los vectores $\boldsymbol{u} = \mathbf{2} = (1,0)$, $\boldsymbol{v} = \mathbf{1} = (0,1)$ y la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & 2 \end{pmatrix}.$$

Entonces, a partir de la expresión (1.1), el lema 1.1, el corolario 1.2 y el teorema 2.3, obtenemos la función bent de 4 variables

$$\begin{aligned}
&G(\boldsymbol{y},\boldsymbol{x}) \\
&= m_0(\boldsymbol{y})f(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})f(\boldsymbol{x}\oplus\mathbf{2}) \oplus m_1(\boldsymbol{y})f(\boldsymbol{x}\oplus\mathbf{1}) \oplus m_2(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}\oplus\mathbf{1}\oplus\mathbf{2})) \\
&= m_0(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})m_2(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})\,(1 \oplus m_3(\boldsymbol{x})) \\
&= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \\
&= (1\oplus y_1)(1\oplus y_2)(1\oplus x_1)(1\oplus 1\oplus x_2) \\
&\quad \oplus (1\oplus 1\oplus y_1)(1\oplus 1\oplus y_2)(1\oplus 1\oplus x_1)(1\oplus x_2) \\
&\quad \oplus (1\oplus y_1)(1\oplus 1\oplus y_2)(1\oplus x_1)(1\oplus 1\oplus x_2) \\
&\quad \oplus (1\oplus 1\oplus y_1)(1\oplus y_2)(1\oplus 1\oplus x_1)(1\oplus x_2) \\
&\quad \oplus (1\oplus 1\oplus y_1)(1\oplus y_2)(1\oplus 1\oplus x_1)(1\oplus 1\oplus x_2) \\
&\quad \oplus (1\oplus 1\oplus y_1)(1\oplus 1\oplus y_2)(1\oplus x_1)(1\oplus x_2) \\
&= 1 \oplus x_2 \oplus x_1 \oplus x_1x_2 \oplus y_2 \oplus y_2x_1 \oplus y_1 \oplus y_1x_2 \oplus y_1x_1x_2 \oplus y_1y_2x_2.
\end{aligned}$$

Sin embargo, no pertenece a la clase Maiorana-McFarland ya que el término x_1x_2 de su FNA no se ajusta con la expresión $\langle \boldsymbol{x}, \pi(\boldsymbol{y})\rangle \oplus f(\boldsymbol{y})$ de las funciones bent de la clase Maiorana-McFarland. ■

2.3.4 Clase Carlet

Si comparamos la construcción de Carlet definida en el teorema 1.5 con la construcción de funciones bent definida en el teorema 2.1 , tenemos que tomando $m = 2$ y considerando

$$f_0(\boldsymbol{x}) = f_1(\boldsymbol{x}) = f(\boldsymbol{x}) \quad \text{y} \quad g_0(\boldsymbol{y}) = g_1(\boldsymbol{y}) = m_{\sigma(3)}(\boldsymbol{y})$$

obtenemos la construcción dada en el corolario 2.1, es decir, la construcción A. Mientras que, si consideramos

$$g_0(\boldsymbol{y}) = m_{\sigma(3)}(\boldsymbol{y}) \quad \text{y} \quad g_1(\boldsymbol{y}) = m_{\sigma(2)}(\boldsymbol{y}),$$

después de algunas manipulaciones algebraicas, obtenemos la construcción dada en el corolario 2.2, es decir, la construcción B. Por tanto, la construcción dada en el teorema 2.1 coincide con la construcción de Carlet.

Podemos decir que, la novedad de nuestra construcción, a diferencia de la construcción de Carlet, es que nosotros podemos calcular el número de funciones bent diferentes que podemos construir y que no utilizamos la transformada de Walsh ni la función dual de las funciones bent utilizadas.

Hemos comprobado computacionalmente, para el caso $n = 2$ y $m = 2$, que todas las funciones bent de 4 variables obtendias a partir de la construcción de Carlet se pueden obtener a partir de la construcción dada en el teorema 2.3; sin embargo, existen funciones bent de 4 variables obtenidas a partir del teorema 2.3 (en concreto, correspondientes a la construcción D) que no pertenecen a la clase de Carlet, como ponemos de manifiesto en el siguiente ejemplo.

Ejemplo 2.5: Supongamos que $n = 2$ y consideremos la función bent de 2 variables

$$f(\boldsymbol{x}) = m_0(\boldsymbol{x}),$$

los vectores $\boldsymbol{u} = \mathbf{2} = (1, 0)$, $\boldsymbol{v} = \mathbf{1} = (0, 1)$ y la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 2 & 0 \end{pmatrix}.$$

A partir del teorema 2.3, la expresión (1.1), el lema 1.1 y el corolario 1.2, obtenemos la función bent de 4 variables

$$\begin{aligned} &G(\boldsymbol{y}, \boldsymbol{x}) \\ &= m_1(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_2(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{v}) \oplus m_0(\boldsymbol{y})(1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})) \\ &= m_1(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) m_2(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) m_1(\boldsymbol{x}) \\ &\quad \oplus m_0(\boldsymbol{y}) \left(m_0(\boldsymbol{x} \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x})\right) \end{aligned}$$

$$= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_9(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}).$$

Esta función no es de la clase Carlet, ya que no existen funciones bent de 2 variables $f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), g_0(\boldsymbol{y})$ y $g_1(\boldsymbol{y})$ tales que la función $G(\boldsymbol{y},\boldsymbol{x})$ pueda expresarse como una de las funciones bent definidas a partir del teorema 1.5. Dicha comprobación se ha verificado computacionalmente calculando todas las funciones bent de 4 variables de la clase Carlet y comprobando que la función obtenida a través de este ejemplo no coincidía con ninguna de ellas. ■

Capítulo 3

Construcción de funciones bent a partir de funciones de máximo y mínimo peso

3.1 Construcción de funciones de máximo y mínimo peso

En este capítulo proporcionamos una nueva construcción de funciones bent basada, en lo que definimos como funciones de máximo y mínimo peso provenientes de funciones bent. Al igual que en las construcciones obtenidas en el capítulo 2, partimos de funciones bent de n variables y obtenemos funciones bent de $n+2$ variables; además, comprobamos que las construcciones anteriores son casos particulares de la nueva construcción. Por último, mostramos ejemplos de funciones bent obtenidas a partir de la construcción dada en este capítulo que no coinciden con ninguna de las funciones obtenidas a partir de las construcciones clásicas definidas en el capítulo 1.

Supongamos que $f(\boldsymbol{x})$ es una función bent de n variables. De acuerdo con el teorema 1.2(c), podemos afirmar que el peso de la función $f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ es $2^{n-1}\pm 2^{\frac{n}{2}-1}$ para todo $\boldsymbol{a}\in\mathbb{F}_2^n$, lo que motiva la siguiente definición.

Definición 3.1: Sea $f(\boldsymbol{x})$ una función bent de n variables y consideremos los conjuntos

$$M^+ = \{\boldsymbol{a}\in\mathbb{F}_2^n \mid w(f\oplus l_{\boldsymbol{a}}) = 2^{n-1}+2^{\frac{n}{2}-1}\},$$

$$M^- = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\}.$$

Llamamos **función de máximo peso** asociada a $f(\boldsymbol{x})$ a la función booleana de n variables $f^+(\boldsymbol{x})$ cuyo soporte es el conjunto M^+, es decir,

$$f^+(\boldsymbol{x}) = \bigoplus_{\boldsymbol{a} \in M^+} m_{\boldsymbol{a}}(\boldsymbol{x}).$$

Análogamente, llamamos **función de mínimo peso** asociada a $f(\boldsymbol{x})$ a la función booleana de n variables $f^-(\boldsymbol{x})$ cuyo soporte es el conjunto M^-, es decir,

$$f^-(\boldsymbol{x}) = \bigoplus_{\boldsymbol{a} \in M^-} m_{\boldsymbol{a}}(\boldsymbol{x}).$$

Notemos que, de acuerdo con esta definición,

$$\mathrm{Sop}\left(f^+\right) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\},$$
$$\mathrm{Sop}\left(f^-\right) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\}.$$

Además, por el teorema 1.2, tenemos que

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

y de la expresión (1.1),

$$\begin{aligned} 1 \oplus f^+(\boldsymbol{x}) &= \bigoplus_{\boldsymbol{a} \in \mathbb{F}_2^n} m_{\boldsymbol{a}}(\boldsymbol{x}) \oplus \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(f^+)} m_{\boldsymbol{a}}(\boldsymbol{x}) \\ &= \bigoplus_{\boldsymbol{a} \in \mathrm{Sop}(f^-)} m_{\boldsymbol{a}}(\boldsymbol{x}) \\ &= f^-(\boldsymbol{x}). \end{aligned} \tag{3.1}$$

Nuestro primer objetivo es probar que las funciones de máximo y mínimo peso asociadas a una función bent, son también funciones bent. Ahora bien, como consecuencia de la expresión (3.1), basta con probar que $f^+(\boldsymbol{x})$ es una función bent. Sin embargo, antes introducimos algunos lemas técnicos que nos facilitarán la demostración de dicho resultado.

Lema 3.1: *Sea $f(\boldsymbol{x})$ una función bent de n variables y consideremos su función asociada de máximo peso $f^+(\boldsymbol{x})$. Para $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ consideramos la función booleana de n variables definida por*

$$g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}). \tag{3.2}$$

Entonces $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$ si y sólo si $w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$.

DEMOSTRACIÓN: Supongamos en primer lugar que $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$, entonces

$$f^+(\boldsymbol{a}) = 1 \quad \text{y} \quad l_{\boldsymbol{a}}(\boldsymbol{b}) = 0 \quad \text{o bien} \quad f^+(\boldsymbol{a}) = 0 \quad \text{y} \quad l_{\boldsymbol{a}}(\boldsymbol{b}) = 1.$$

En el primer caso, $\boldsymbol{a} \in \mathrm{Sop}\,(f^+)$ y de la expresión (3.2) tenemos que

$$w(g_{\boldsymbol{a},\boldsymbol{b}}) = w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

En el segundo caso, $\boldsymbol{a} \notin \mathrm{Sop}\,(f^+)$ y, de nuevo por la expresión (3.2), tenemos que

$$w(g_{\boldsymbol{a},\boldsymbol{b}}) = w(f \oplus l_{\boldsymbol{a}} \oplus 1) = 2^n - w(f \oplus l_{\boldsymbol{a}}) = 2^n - (2^{n-1} - 2^{\frac{n}{2}-1}) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

Recíprocamente, supongamos ahora que $w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$.

Si $l_{\boldsymbol{a}}(\boldsymbol{b}) = 0$, de la expresión (3.2), tenemos que

$$g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}),$$

con lo que $w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}$ y, en consecuencia, $\boldsymbol{a} \in \mathrm{Sop}\,(f^+)$, es decir, $f^+(\boldsymbol{a}) = 1$.

Si $l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$, de la expresión (3.2), tenemos que

$$g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus 1,$$

y así $w(f \oplus l_{\boldsymbol{a}}) = 2^n - w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$; por tanto, $\boldsymbol{a} \notin \mathrm{Sop}\,(f^+)$, es decir, $f^+(\boldsymbol{a}) = 0$.

En cualquier caso, $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1$. □

Notemos que, con la notación del lema anterior, también tenemos que

$$f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 0 \quad \text{si y sólo si} \quad w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Por tanto, podemos afirmar que $w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Pero esto no garantiza que $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ sea una función bent; únicamente garantiza que tiene el número de minterms necesario para poder serlo.

Ahora, como consecuencia inmediata del lema anterior tenemos el siguiente resultado que relaciona el peso de la función $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ con el valor de $f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b})$.

Lema 3.2: *Sea $f(\boldsymbol{x})$ una función bent de n variables y consideremos su función asociada de máximo peso $f^+(\boldsymbol{x})$. Para $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ consideramos la función booleana $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ definida por la expresión (3.2). Entonces*

$$f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}}.$$

DEMOSTRACIÓN: El resultado es evidente aplicando las relaciones obtenidas en la demostración del lema anterior

$$f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 0 \quad \text{si y sólo si} \quad w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$$

y

$$f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{a}}(\boldsymbol{b}) = 1 \quad \text{si y sólo si} \quad w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

□

A continuación, daremos el último lema ténico necesario para probar que la función de máximo peso asociada a una función bent, es también una función bent.

Lema 3.3: *Sea $f(\boldsymbol{x})$ una función bent de n variables. Entonces*

$$\sum_{\boldsymbol{a} \in \mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{2n-1} \pm 2^{n-1} \quad \textit{para todo } \boldsymbol{b} \in \mathbb{F}_2^n$$

donde $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ es la función booleana de la expresión (3.2).

DEMOSTRACIÓN: De la expresión (3.2) tenemos que

$$\begin{aligned}\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n}\left(\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{b}))\right)\\ &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n}\left(f(\boldsymbol{b})+\sum_{\substack{\boldsymbol{x}\in\mathbb{F}_2^n\\ \boldsymbol{x}\neq\boldsymbol{b}}}(f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x}\oplus\boldsymbol{b}))\right)\\ &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} f(\boldsymbol{b})+\sum_{\substack{\boldsymbol{x}\in\mathbb{F}_2^n\\ \boldsymbol{x}\neq\boldsymbol{b}}}\left(\sum_{\boldsymbol{a}\in\mathbb{F}_2^n}(f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x}\oplus\boldsymbol{b}))\right) \qquad (3.3)\end{aligned}$$

ya que

$$l_{\boldsymbol{a}}(\boldsymbol{b})\oplus l_{\boldsymbol{b}}(\boldsymbol{a})=0 \qquad \text{y} \qquad l_{\boldsymbol{a}}(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{b})=l_{\boldsymbol{a}}(\boldsymbol{x}\oplus\boldsymbol{b}).$$

Además, considerada como una función en la variable $\boldsymbol{a}$, si $\boldsymbol{x}\neq\boldsymbol{b}$, entonces

$$f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x}\oplus\boldsymbol{b})=f(\boldsymbol{x})\oplus l_{\boldsymbol{x}\oplus\boldsymbol{b}}(\boldsymbol{a})$$

es una función afín, por tanto

$$\sum_{\boldsymbol{a}\in\mathbb{F}_2^n}(f(\boldsymbol{x})\oplus l_{\boldsymbol{x}\oplus\boldsymbol{b}}(\boldsymbol{a}))=2^{n-1}$$

y sustituyendo en la expresión (3.3) tenemos que

$$\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}})=2^n f(\boldsymbol{b})+(2^n-1)2^{n-1}=\begin{cases}2^{2n-1}+2^{n-1}, & \text{si } f(\boldsymbol{b})=1,\\ 2^{2n-1}-2^{n-1}, & \text{si } f(\boldsymbol{b})=0.\end{cases}$$ □

Ahora estamos ya en condiciones de probar que la función de máximo peso asociada a una función bent es también una función bent.

Teorema 3.1: *Si $f(\boldsymbol{x})$ es una función bent de n variables, entonces su función asociada de máximo peso $f^+(\boldsymbol{x})$ también es una función bent de n variables.*

DEMOSTRACIÓN: Si $\boldsymbol{b}\in\mathbb{F}_2^n$, de los lemas 3.2 y 3.3 y de la igualdad $l_{\boldsymbol{b}}(\boldsymbol{a})=l_{\boldsymbol{a}}(\boldsymbol{b})$, tenemos que

$$w(f^+\oplus l_{\boldsymbol{b}})=\sum_{\boldsymbol{a}\in\mathbb{F}_2^n}\left(f^+(\boldsymbol{a})\oplus l_{\boldsymbol{b}}(\boldsymbol{a})\right)$$

$$= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}}$$

$$= \frac{2^{2n-1} \pm 2^{n-1} - 2^n(2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}}$$

$$= 2^{n-1} \pm 2^{\frac{n}{2}-1}$$

y, por el teorema 1.2(c), concluimos que $f^+(\boldsymbol{x})$ es una función bent. □

Ahora, como consecuencia inmediata del teorema anterior tenemos los resultados siguientes que establecen algunas propiedades de las funciones de máximo y mínimo peso asociadas a una función bent.

El siguiente corolario establece que la función de máximo peso asociada a la función complementaria de una función bent es la función complementaria de la función de máximo peso asociada a dicha función bent.

Corolario 3.1: *Sea $f(\boldsymbol{x})$ una función bent de n variables. Si $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$, entonces*

$$g^+(\boldsymbol{x}) = 1 \oplus f^+(\boldsymbol{x}).$$

DEMOSTRACIÓN: De acuerdo con la definición 3.1 y del comentario que le sigue, tenemos que

$$\mathrm{Sop}\left(f^-\right) = \left\{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\right\},$$

$$\mathrm{Sop}\left(g^+\right) = \left\{\boldsymbol{a} \in \mathbb{F}_2^n \mid w(g \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\right\}.$$

Si $\boldsymbol{a} \in \mathrm{Sop}\,(g^+)$, entonces

$$2^{n-1} + 2^{\frac{n}{2}-1} = w(g \oplus l_{\boldsymbol{a}}) = w(1 \oplus f \oplus l_{\boldsymbol{a}}) = 2^n - w(f \oplus l_{\boldsymbol{a}})$$

con lo que $w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$, es decir, $\boldsymbol{a} \in \mathrm{Sop}\,(f^-)$ y así $\mathrm{Sop}\,(g^+) \subseteq \mathrm{Sop}\,(f^-)$.

Supongamos ahora que $\boldsymbol{a} \in \mathrm{Sop}\,(f^-)$, entonces

$$w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}$$

con lo que

$$w(g \oplus l_{\boldsymbol{a}}) = w(1 \oplus f \oplus l_{\boldsymbol{a}}) = 2^n - w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1},$$

es decir, $\boldsymbol{a} \in \mathrm{Sop}\,(g^+)$ y así $\mathrm{Sop}\,(f^-) \subseteq \mathrm{Sop}\,(g^+)$.

Ahora, de esta inclusión y de la anterior, tenemos que $\mathrm{Sop}\,(g^+) = \mathrm{Sop}\,(f^-)$ y, por tanto, $g^+(\boldsymbol{x}) = f^-(\boldsymbol{x})$. Finalmente, de la expresión (3.1), tenemos que

$$g^+(\boldsymbol{x}) = 1 \oplus f^+(\boldsymbol{x}).$$

□

El siguiente corolario establece que la función de máximo peso asociada a la función de máximo peso asociada a una función bent es la propia función bent.

Corolario 3.2: *Si $f(\boldsymbol{x})$ es una función bent de n variables, entonces*

$$f^{+^+}(\boldsymbol{x}) = f(\boldsymbol{x}).$$

DEMOSTRACIÓN: Probaremos que $\mathrm{Sop}\left(f^{+^+}\right) = \mathrm{Sop}\,(f)$.

Supongamos en primer lugar que $\boldsymbol{b} \in \mathrm{Sop}\left(f^{+^+}\right)$; entonces, de acuerdo con la definición 3.1,

$$w(f^+ \oplus l_{\boldsymbol{b}}) = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

Ahora bien, por el lema 3.2,

$$\begin{aligned} w(f^+ \oplus l_{\boldsymbol{b}}) &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \left(f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{a})\right) \\ &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} \\ &= \frac{\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) - 2^n(2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} \end{aligned}$$

donde $g_{\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{x})$ es la función definida por la expresión (3.2). Por tanto

$$\begin{aligned} \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) &= 2^{\frac{n}{2}}(2^{n-1} + 2^{\frac{n}{2}-1}) + 2^n(2^{n-1} - 2^{\frac{n}{2}-1}) \\ &= 2^{2n-1} + 2^{n-1}, \end{aligned}$$

pero entonces, de acuerdo con la demostración del lema 3.3, $f(\boldsymbol{b}) = 1$, es decir, $\boldsymbol{b} \in \mathrm{Sop}\,(f)$. Así pues, $\mathrm{Sop}\left(f^{+^+}\right) \subseteq \mathrm{Sop}\,(f)$.

Supongamos ahora que $\boldsymbol{b} \in \mathrm{Sop}\,(f)$. Entonces $f(\boldsymbol{b}) = 1$ y, de acuerdo con la demostración del lema 3.3,

$$\sum_{\boldsymbol{a}\in\mathbb{F}_2^n} w(g_{\boldsymbol{a},\boldsymbol{b}}) = 2^{2n-1} + 2^{n-1},$$

pero entonces, procediendo como en la demostración del teorema 3.1, tenemos que

$$\begin{aligned} w(f^+ \oplus l_{\boldsymbol{b}}) &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \left(f^+(\boldsymbol{a}) \oplus l_{\boldsymbol{b}}(\boldsymbol{a})\right) \\ &= \sum_{\boldsymbol{a}\in\mathbb{F}_2^n} \frac{w(g_{\boldsymbol{a},\boldsymbol{b}}) - (2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} \\ &= \frac{2^{2n-1} + 2^{n-1} - 2^n(2^{n-1} - 2^{\frac{n}{2}-1})}{2^{\frac{n}{2}}} \\ &= 2^{n-1} + 2^{\frac{n}{2}-1} \end{aligned}$$

y, de acuerdo con la definición 3.1, $\boldsymbol{b} \in \mathrm{Sop}\left(f^{+^+}\right)$. Por tanto, $\mathrm{Sop}\,(f) \subseteq \mathrm{Sop}\left(f^{+^+}\right)$.

De esta inclusión y de la anterior tenemos que $\mathrm{Sop}\left(f^{+^+}\right) = \mathrm{Sop}\,(f)$. □

El siguiente resultado establece que las funciones de máximo peso asociadas a funciones bent distintas son también distintas.

Corolario 3.3: *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces*

$$f^+(\boldsymbol{x}) \neq g^+(\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $f^+(\boldsymbol{x}) = g^+(\boldsymbol{x})$, entonces por el corolario 3.2 tenemos que

$$f(\boldsymbol{x}) = f^{+^+}(\boldsymbol{x}) = g^{+^+}(\boldsymbol{x}) = g(\boldsymbol{x}),$$

en contra de la hipótesis. Por tanto, $f^+(\boldsymbol{x}) \neq g^+(\boldsymbol{x})$. □

Notemos que, como consecuencia de la expresión (3.1) tenemos que el teorema 3.1 y los corolarios 3.1, 3.2 y 3.3 son también válidos si cambiamos $f^+(\boldsymbol{x})$ por $f^-(\boldsymbol{x})$.

Notemos también que, en general,

- $f^+ \neq f \neq f^-$,

f	f^+	f^-
m_0	$m_1 \oplus m_2 \oplus m_3$	m_0
m_1	m_2	$m_0 \oplus m_1 \oplus m_2$
m_2	m_1	$m_0 \oplus m_2 \oplus m_3$
m_3	m_3	$m_0 \oplus m_1 \oplus m_3$
$m_0 \oplus m_1 \oplus m_2$	$m_0 \oplus m_1 \oplus m_2$	m_3
$m_0 \oplus m_1 \oplus m_3$	$m_0 \oplus m_2 \oplus m_3$	m_1
$m_0 \oplus m_2 \oplus m_3$	$m_0 \oplus m_1 \oplus m_3$	m_2
$m_1 \oplus m_2 \oplus m_3$	m_0	$m_1 \oplus m_2 \oplus m_3$

Tabla 3.1: *Funciones de máximo y mínimo peso asociadas a las funciones bent de 2 variables.*

- $w(f^+) \neq 2^{n-1} + 2^{\frac{n}{2}-1}$,
- $w(f^-) \neq 2^{n-1} - 2^{\frac{n}{2}-1}$,

como podemos comprobar en la tabla 3.1 que muestra la relación entre f, f^+ y f^- cuando f recorre las ocho funciones bent de 2 variables.

Ahora estamos ya en condiciones de establecer el resultado principal de este capítulo que nos permite construir una función bent de $n+2$ variables a partir de las funciones de máximo peso asociadas a cuatro funciones bent de n variables.

Teorema 3.2: *Sean $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $f_2(\boldsymbol{x})$ y $f_3(\boldsymbol{x})$ funciones bent de n variables tales que*

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1. \tag{3.4}$$

Si σ es una permutación de $\{0,1,2,3\}$ e $\boldsymbol{y} = (y_1, y_2)$ es un vector de dos variables, entonces

$$F(\boldsymbol{y}, \boldsymbol{x}) = m_{\sigma(0)}(\boldsymbol{y})\, f_0^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})\, f_1^+(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})\, f_2^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})\, f_3^+(\boldsymbol{x})$$

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

y_1	y_2	$\boldsymbol{x}$	$m_0(\boldsymbol{y})$	$m_1(\boldsymbol{y})$	$m_2(\boldsymbol{y})$	$m_3(\boldsymbol{y})$	$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$
0	**0**	$\boldsymbol{\tau}$	**I**	**0**	**0**	**0**	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
0	**I**	$\boldsymbol{\tau}$	**0**	**I**	**0**	**0**	$\boldsymbol{\xi}_1^+ \oplus b_2\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
I	**0**	$\boldsymbol{\tau}$	**0**	**0**	**I**	**0**	$\boldsymbol{\xi}_2^+ \oplus b_1\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
I	**I**	$\boldsymbol{\tau}$	**0**	**0**	**0**	**I**	$\boldsymbol{\xi}_3^+ \oplus b_1\mathbf{I} \oplus b_2\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Tabla 3.2: *Tabla de verdad de* $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$

DEMOSTRACIÓN: Basta probar, de acuerdo con el teorema 1.2(c), que el número de 1 de la tabla de verdad (es decir, el número de minterms) de la función booleana

$$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = F(\boldsymbol{y},\boldsymbol{x}) \oplus l_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$$

es $2^{n+1} \pm 2^{\frac{n}{2}}$ para todo $(\boldsymbol{b},\boldsymbol{a}) \in \mathbb{F}_2^2 \times \mathbb{F}_2^n$.

Supongamos en primer lugar que σ es la permutación identidad. Entonces

$$F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x}) = m_0(\boldsymbol{y})\, f_0^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})\, f_1^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})\, f_2^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})\, f_3^+(\boldsymbol{x})$$
$$\oplus\, b_1 y_1 \oplus b_2 y_2 \oplus l_{\boldsymbol{a}}(\boldsymbol{x}),$$

con $\boldsymbol{b} = (b_1, b_2)$.

Si **0** e **I** son las columnas de longitud 2^n con todos los elementos iguales a 0 y 1 respectivamente; $\boldsymbol{\tau}$ es la matriz de tamaño $2^n \times n$ cuya i-ésima fila es $\boldsymbol{i}$, para $i = 0, 1, \ldots, 2^n - 1$; $\boldsymbol{\xi}_j^+$ es la tabla de verdad de $f_j^+(\boldsymbol{x})$, para $j = 0, 1, 2, 3$; y $\boldsymbol{\Lambda}_{\boldsymbol{a}}$ es la tabla de verdad de la función lineal $l_{\boldsymbol{a}}(\boldsymbol{x})$, entonces la última columna de la tabla 3.2 es la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$, donde $b_t\mathbf{I}$, con $t = 1, 2$, es la columna de longitud 2^n con todos los elementos iguales a b_t. Por tanto, cada columna de la tabla 3.3 representa los cuatro bloques de la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ para los diferentes valores de $\boldsymbol{b}$.

Ahora, si para algún $j \in \{0, 1, 2, 3\}$ es $f_j(\boldsymbol{a}) = 1$, entonces, por el corolario 3.2, también $f_j^{+^+}(\boldsymbol{a}) = 1$ y, de acuerdo con la definición 3.1,

$$w(f_j^+ \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1},$$

es decir, el número de 1 en el bloque $\boldsymbol{\xi}_j^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ es $2^{n-1} + 2^{\frac{n}{2}-1}$. En cambio, si $f_j(\boldsymbol{a}) = 0$, mediante el mismo razonamiento, tenemos que el número de 1 en el bloque $\boldsymbol{\xi}_j^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

$b_1=0 \quad b_2=0$	$b_1=0 \quad b_2=1$	$b_1=1 \quad b_2=0$	$b_1=1 \quad b_2=1$
$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_1^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1^+ \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1^+ \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_2^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_2^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_2^+ \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_2^+ \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_3^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_3^+ \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_3^+ \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_3^+ \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Tabla 3.3: *Tabla de verdad de* $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ *para los diferentes valores de* $\boldsymbol{b}=(b_1,b_2)$.

es $2^{n-1}-2^{\frac{n}{2}-1}$. A partir de la expresión (3.4), podemos afirmar que en la cuaterna $(f_0(\boldsymbol{a}),f_1(\boldsymbol{a}),f_2(\boldsymbol{a}),f_3(\boldsymbol{a}))$ hay un 1 y tres 0 o bien un 0 y tres 1; por tanto, concluimos que el número de 1 de cada una de las columnas de la tabla 3.3 es

$$2^{n-1}+2^{\frac{n}{2}-1}+3(2^{n-1}-2^{\frac{n}{2}-1})=2^{n+1}-2^{\frac{n}{2}}$$

o bien

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

Finalmente, si σ es una permutación de $\{0,1,2,3\}$ distinta de la identidad, entonces los cuatro bloques de la tabla de verdad de $F_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ dados en la tabla 3.3 están permutados de acuerdo con σ y, por tanto, obtenemos el mismo resultado que en el caso anterior. □

Al igual que ocurrió en el capítulo 2, como consecuencia del corolario 1.2, podemos identificar la permutación σ con una permutación

$$\begin{pmatrix} 0 & 2^n & 2^{n+1} & 2^{n+1}+2^n \\ a_0 & a_1 & a_2 & a_3 \end{pmatrix}$$

del conjunto $\{0,2^n,2^{n+1},2^{n+1}+2^n\}$; por tanto, de acuerdo con el teorema 3.2, tenemos que

$$\begin{aligned}\mathrm{Sop}\,(F)=&\{a_0+a \mid a\in \mathrm{Sop}\left(f_0^+\right)\}\cup\{a_1+a \mid a\in \mathrm{Sop}\left(f_1^+\right)\}\\ &\cup\{a_2+a \mid a\in \mathrm{Sop}\left(f_2^+\right)\}\cup\{a_3+a \mid a\in \mathrm{Sop}\left(f_3^+\right)\}.\end{aligned} \tag{3.5}$$

Sin embargo, si para los subíndices de los minterms utilizamos vectores, entonces

$$\begin{aligned}\mathrm{Sop}\,(F) = &\{(\boldsymbol{a}_0, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\left(f_0^+\right)\} \cup \{(\boldsymbol{a}_1, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\left(f_1^+\right)\} \\ &\cup \{(\boldsymbol{a}_2, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\left(f_2^+\right)\} \cup \{(\boldsymbol{a}_3, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\left(f_3^+\right)\}. \qquad (3.6)\end{aligned}$$

donde

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \boldsymbol{a}_0 & \boldsymbol{a}_1 & \boldsymbol{a}_2 & \boldsymbol{a}_3 \end{pmatrix}$$

es una permutación de $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$.

Los ejemplos siguientes ponen de manifiesto que todas las hipótesis del teorema 3.2 son necesarias.

Así, si en el teorema 3.2 utilizamos las funciones $f_j(\boldsymbol{x})$ en lugar de las funciones $f_j^+(\boldsymbol{x})$ para $j = 0, 1, 2, 3$, entonces la función $F(\boldsymbol{y}, \boldsymbol{x})$ no es necesariamente bent, como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 3.1: Consideremos las funciones bent de 4 variables

$$\begin{aligned} f_0(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}), \\ f_1(\boldsymbol{x}) &= m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}), \\ f_2(\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}), \\ f_3(\boldsymbol{x}) &= m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}). \end{aligned}$$

Claramente, de la expresión (1.1), tenemos que

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1.$$

Sin embargo, la función

$$F(\boldsymbol{y}, \boldsymbol{x}) = m_0(\boldsymbol{y}) f_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) f_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f_3(\boldsymbol{x})$$

no es bent ya que, si desarrollamos la expresión anterior tenemos que

$$\begin{aligned} &F(\boldsymbol{y}, \boldsymbol{x}) \\ &= m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_1(\boldsymbol{y}, \boldsymbol{x}) \oplus m_2(\boldsymbol{y}, \boldsymbol{x}) \oplus m_5(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{11}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{13}(\boldsymbol{y}, \boldsymbol{x}) \\ &\quad \oplus m_{18}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{20}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{21}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{23}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{24}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{28}(\boldsymbol{y}, \boldsymbol{x}) \end{aligned}$$

$$\oplus\, m_{33}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{37}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{38}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{39}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{42}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{47}(\boldsymbol{y},\boldsymbol{x})$$

$$\oplus\, m_{49}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{50}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{51}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{55}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{57}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{62}(\boldsymbol{y},\boldsymbol{x})$$

solamente tiene 24 minterms y, de acuerdo con los comentarios posteriores al teorema 1.2, las funciones bent de 6 variables han de tener 28 o 36 minterms. ■

Por otro lado, la condición expresada por la ecuación (3.4) sobre las funciones $f_j(\boldsymbol{x})$, para $j = 0, 1, 2, 3$, también es necesaria como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 3.2: Supongamos que $n = 2$ y consideremos las funciones booleanas de 2 variables

$$f_0(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})$$

$$f_1(\boldsymbol{x}) = m_1(\boldsymbol{x}), \quad f_2(\boldsymbol{x}) = m_2(\boldsymbol{x}) \quad \text{y} \quad f_3(\boldsymbol{x}) = m_3(\boldsymbol{x}).$$

Claramente

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 0$$

con lo que no se satisface la ecuación (3.4). Ahora, de acuerdo con la tabla 3.1, tenemos que

$$f_0^+(\boldsymbol{x}) = m_0(\boldsymbol{x}), \quad f_1^+(\boldsymbol{x}) = m_2(\boldsymbol{x}), \quad f_2^+(\boldsymbol{x}) = m_1(\boldsymbol{x}) \quad \text{y} \quad f_3^+(\boldsymbol{x}) = m_3(\boldsymbol{x})$$

y sin embargo

$$\begin{aligned} F(\boldsymbol{y},\boldsymbol{x}) &= m_0(\boldsymbol{y}) f_0^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) f_1^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_2^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f_3^+(\boldsymbol{x}) \\ &= m_0(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) m_2(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) m_3(\boldsymbol{x}) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_6(\boldsymbol{y},\boldsymbol{x}) \oplus m_9(\boldsymbol{y},\boldsymbol{x}) \oplus m_{15}(\boldsymbol{y},\boldsymbol{x}) \end{aligned}$$

no es una función bent ya que solamente tiene 4 minterms y las funciones bent de cuatro variables tienen 6 o 10 minterms. ■

Finalmente, notemos que como consecuencia de la expresión (3.1), los resultados anteriores son también válidos si cambiamos las funciones de máximo peso por las correspondientes funciones de mínimo peso.

3.2 Número de funciones bent

Determinar todas las cuaternas $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x}))$ de funciones bent de n variables que satisfacen la expresión (3.4) no es fácil. Sin embargo, si $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son funciones bent de n variables, entonces las cuaternas

$$(f(\boldsymbol{x}), f(\boldsymbol{x}), f(\boldsymbol{x}), 1 \oplus f(\boldsymbol{x})) \tag{3.7}$$

$$(f(\boldsymbol{x}), f(\boldsymbol{x}), g(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x})) \tag{3.8}$$

satisfacen, evidentemente, la expresión (3.4) con lo que tenemos los resultados siguientes.

Corolario 3.4: *Si $f(\boldsymbol{x})$ es una función bent de n variables y σ es una permutación de $\{0,1,2,3\}$, entonces*

$$A_f(\boldsymbol{y}, \boldsymbol{x}) = f^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y})$$

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

Corolario 3.5: *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ dos funciones bent de n variables tales que*

$$g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \quad y \quad g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x}).$$

Si σ es una permutación de $\{0,1,2,3\}$, entonces

$$B_{f,g}(\boldsymbol{y}, \boldsymbol{x}) = \left(m_{\sigma(0)}(\boldsymbol{y}) \oplus m_{\sigma(1)}(\boldsymbol{y})\right) f^+(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y}) g^+(\boldsymbol{x}) \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus g^+(\boldsymbol{x})\right)$$

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

Notemos que los dos casos particulares anteriores coinciden con las construcciones de funciones bent introducidas en los corolarios 2.1 y 2.2, las denominadas construcciones A y B, con la particularidad de que ahora utilizamos funciones bent de máximo peso.

Notemos también que partiendo de una misma función bent $f(\boldsymbol{x})$ de n variables, el corolario 3.4 proporciona una función bent diferente que la proporcionada por el corolario 2.1, ya que, en general, $f^+(\boldsymbol{x}) \neq f(\boldsymbol{x})$; sin embargo, el número total

de funciones bent proporcionadas por ambos corolarios es el mismo y las funciones obtenidas son las mismas aunque en distinto orden. El mismo argumento es válido para las funciones bent construidas a partir del corolario 2.2 y del corolario 3.5.

Por tanto, la construcción de funciones bent proporcionada por el teorema 2.1 (las llamadas construcciones A y B) es un caso particular de la construcción introducida en el teorema 3.2.

De acuerdo con los comentarios anteriores, el siguiente teorema (véase el teorema 2.2) establece el número de funciones bent de $n+2$ variables que podemos construir utilizando los corolarios 3.4 y 3.5.

Teorema 3.3: *Si ν_n es el número de funciones bent de n variables, entonces el número de funciones bent de $n+2$ variables que podemos construir utilizando los corolarios 3.4 y 3.5 es*

$$6\nu_n^2 - 8\nu_n. \tag{3.9}$$

Fuera de los dos casos proporcionados por los corolarios 3.4 y 3.5, es difícil contar cuántas cuaternas $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x}))$ diferentes de funciones bent de n variables satisfacen la ecuación (3.4); por lo tanto, si denotamos por ω_n el número de cuaternas de funciones bent que satisfacen dicha ecuación, excluyendo las correspondientes a las cuaternas (3.7) y (3.8), ya analizadas anteriormente, podemos construir $4!\omega_n$ funciones bent de $n+2$ variables. Como consecuencia, tenemos el siguiente resultado.

Teorema 3.4: *Si ν_n es el número de funciones bent de n variables y ω_n es el número de cuaternas de funciones bent de n variables que satisfacen la ecuación (3.4), excluyendo las correspondientes a las cuaternas (3.7) y (3.8), entonces el número de funciones bent de $n+2$ variables que podemos construir utilizando el teorema 3.2 es*

$$6\nu_n^2 - 8\nu_n + 24\omega_n.$$

A continuación introducimos una familia de cuaternas de funciones bent de n variables que satisface la expresión (3.4) y que nos permitirá establecer una cota inferior para ω_n.

Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ y

consideremos la cuaterna

$$(f(\boldsymbol{x}), f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}), g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x}) \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x}))\,. \tag{3.10}$$

Como $l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x}) = l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x})$, es evidente que dicha cuaterna satisface la ecuación (3.4). Antes de continuar, notemos que si tomamos $\boldsymbol{a} = \boldsymbol{b} = \boldsymbol{0}$, entonces las cuaternas (3.7) y (3.8) son un caso particular de la cuaterna (3.10) cuando tomamos $g(\boldsymbol{x}) = f(\boldsymbol{x})$ y $g(\boldsymbol{x}) \neq f(\boldsymbol{x})$, respectivamente. Por tanto, sólo necesitamos considerar los dos casos siguientes (justificaremos esta afirmación más adelante).

La demostración de ambos resultados es consecuencia inmediata del corolario 3.1 y del teorema 3.1, ya que la cuaterna (3.10) satisface la ecuación (3.4).

Corolario 3.6: *Sean $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ con $\boldsymbol{a} \neq \boldsymbol{b}$ y supongamos que $f(\boldsymbol{x})$ es una función bent de n variables. Si σ es una permutación de $\{0,1,2,3\}$, entonces*

$$\begin{aligned} D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) =& m_{\sigma(0)}(\boldsymbol{y}) f^{+}(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^{+}(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{b}})^{+}(\boldsymbol{x}) \\ & \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus (f \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^{+}(\boldsymbol{x})\right) \end{aligned}$$

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

Corolario 3.7: *Sean $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ con $\boldsymbol{a} \neq \boldsymbol{b}$ y supongamos que $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son funciones bent de n variables tales que $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$. Si σ es una permutación de $\{0,1,2,3\}$, entonces*

$$\begin{aligned} E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) =& m_{\sigma(0)}(\boldsymbol{y}) f^{+}(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^{+}(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})(g \oplus l_{\boldsymbol{b}})^{+}(\boldsymbol{x}) \\ & \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus (g \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^{+}(\boldsymbol{x})\right) \end{aligned}$$

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

Notemos que no todas las funciones bent proporcionadas por el corolario 3.6 son distintas entre sí como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 3.3: Supongamos que $n = 2$ y consideremos los vectores $\boldsymbol{a} = \boldsymbol{1} = (0,1)$, $\boldsymbol{b} = \boldsymbol{2} = (1,0)$ y la función bent de 2 variables

$$f(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}).$$

Es fácil comprobar que,

$$l_{\mathbf{1}}(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}),\ l_{\mathbf{2}}(\boldsymbol{x}) = m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \text{ y } l_{\mathbf{1}\oplus\mathbf{2}}(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}).$$

Si consideramos la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix},$$

entonces, de acuerdo con el corolario 3.6 y la tabla 3.1, tenemos que

$$\begin{aligned} &D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \\ &= m_0(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(f \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})(f \oplus l_{\mathbf{2}})^+(\boldsymbol{x}) \\ &\quad \oplus m_3(\boldsymbol{y}) \left(1 \oplus (f \oplus l_{\mathbf{3}})^+(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) m_2(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) \left(1 \oplus m_3(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{13}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

Por otro lado, si considereamos los vectores $\boldsymbol{u} = \mathbf{1} = (0,1)$, $\boldsymbol{v} = \mathbf{3} = (1,1)$, la función bent de 2 variables $g(\boldsymbol{x}) = m_2(\boldsymbol{x})$ y la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix},$$

entonces, procediendo como en el caso anterior, tenemos que

$$\begin{aligned} &D_{g,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}) \\ &= m_1(\boldsymbol{y}) g^+(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})(g \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(g \oplus l_{\mathbf{3}})^+(\boldsymbol{x}) \\ &\quad \oplus m_3(\boldsymbol{y}) \left(1 \oplus (g \oplus l_{\mathbf{2}})^+(\boldsymbol{x})\right) \\ &= m_1(\boldsymbol{y}) m_1(\boldsymbol{x}) \oplus m_0(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) \left(1 \oplus m_3(\boldsymbol{x})\right) \\ &= m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_5(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{13}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x}), \end{aligned}$$

que, evidentemente, coincide con $D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$. ■

Notemos que en el ejemplo anterior $\{\mathbf{1},\mathbf{2}\}$ y $\{\mathbf{1},\mathbf{3}\}$ son bases del mismo subespacio vectorial $\{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3}\}$ de $\mathbb{F}_2^n$. Con el fin de evitar esta situación, consideramos

solamente vectores $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}^n$ tales que $\{\boldsymbol{a}, \boldsymbol{b}\}$ es una base de Gauss-Jordan de $\mathbb{F}_2^n$ de cardinalidad 2 (véase la página 34 para recordar dicho concepto).

El resultado siguiente establece que las funciones bent construidas de acuerdo con el corolario 3.6 son distintas, si $\{\boldsymbol{a}, \boldsymbol{b}\}$ es una base de Gauss-Jordan de $\mathbb{F}_2^n$ de cardinalidad 2.

Lema 3.4: *Sean $f(\boldsymbol{x})$ y $p(\boldsymbol{x})$ dos funciones bent distintas de n variables. Supongamos que $D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent de $n+2$ variables construida de acuerdo con el corolario 3.6 utilizando $f(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a}, \boldsymbol{b}\}$ de $\mathbb{F}_2^n$ de cardinalidad 2 y la permutación σ de $\{0, 1, 2, 3\}$. Supongamos también que $D_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent de $n+2$ variables construida de acuerdo con el corolario 3.6 utilizando $p(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{u}, \boldsymbol{v}\}$ de $\mathbb{F}_2^n$ de cardinalidad 2 y la permutación τ de $\{0, 1, 2, 3\}$. Entonces*

$$D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x}) \neq D_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi}$ y $\boldsymbol{\eta}$ son las tablas de verdad de $f(\boldsymbol{x})$ y $p(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ y $D_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$\begin{array}{lcccc} D_{f,\boldsymbol{a},\boldsymbol{b}}: & \boldsymbol{\xi}^+ & (\boldsymbol{\xi} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}})^+ & (\boldsymbol{\xi} \oplus \boldsymbol{\Lambda}_{\boldsymbol{b}})^+ & \mathbf{I} \oplus (\boldsymbol{\xi} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}\oplus\boldsymbol{b}})^+ \\ D_{p,\boldsymbol{u},\boldsymbol{v}}: & \boldsymbol{\eta}^+ & (\boldsymbol{\eta} \oplus \boldsymbol{\Lambda}_{\boldsymbol{u}})^+ & (\boldsymbol{\eta} \oplus \boldsymbol{\Lambda}_{\boldsymbol{v}})^+ & \mathbf{I} \oplus (\boldsymbol{\eta} \oplus \boldsymbol{\Lambda}_{\boldsymbol{u}\oplus\boldsymbol{v}})^+ \end{array}$$

donde $\boldsymbol{\Lambda}_{\boldsymbol{a}}$, $\boldsymbol{\Lambda}_{\boldsymbol{b}}$, $\boldsymbol{\Lambda}_{\boldsymbol{a}\oplus\boldsymbol{b}}$, $\boldsymbol{\Lambda}_{\boldsymbol{u}}$, $\boldsymbol{\Lambda}_{\boldsymbol{v}}$ y $\boldsymbol{\Lambda}_{\boldsymbol{u}\oplus\boldsymbol{v}}$ son las tablas de verdad de las funciones lineales $l_{\boldsymbol{a}}(\boldsymbol{x})$, $l_{\boldsymbol{b}}(\boldsymbol{x})$, $l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x})$, $l_{\boldsymbol{u}}(\boldsymbol{x})$, $l_{\boldsymbol{v}}(\boldsymbol{x})$ y $l_{\boldsymbol{u}\oplus\boldsymbol{v}}(\boldsymbol{x})$ respectivamente.

Si $D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x}) = D_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$, entonces los cuatro bloques de la segunda fila son una permutación de los cuatro bloques de la primera fila. Ahora bien, si consideramos los 4! casos correspondientes a dichas permutaciones, utilizando los corolarios 3.2 y 3.3, obtenemos que $f(\boldsymbol{x}) = p(\boldsymbol{x})$, o que $l_{\boldsymbol{c}}(\boldsymbol{x}) = 1$ para algún $\boldsymbol{c} \in \mathbb{F}_2^n$ que depende de los vectores $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{u}$ y $\boldsymbol{v}$, o que

$$(\boldsymbol{u}, \boldsymbol{v}) \in \{(\boldsymbol{a}, \boldsymbol{a} \oplus \boldsymbol{b}), (\boldsymbol{b}, \boldsymbol{a} \oplus \boldsymbol{b}), (\boldsymbol{a} \oplus \boldsymbol{b}, \boldsymbol{a}), (\boldsymbol{a} \oplus \boldsymbol{b}, \boldsymbol{b})\}. \tag{3.11}$$

En cualquier caso tenemos una contradicción ya que $f(\boldsymbol{x}) \neq p(\boldsymbol{x})$ por hipótesis, $l_{\boldsymbol{c}}(\boldsymbol{x}) \neq 1$ para todo $\boldsymbol{c} \in \mathbb{Z}_2^n$ y si se satisface la relación (3.11), entonces $\{\boldsymbol{a}, \boldsymbol{b}\}$ y

$\{\boldsymbol{u}, \boldsymbol{v}\}$ no pueden ser simultáneamente bases de Gauss-Jordan de cardinalidad 2. En consecuencia, $D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x}) \neq D_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$. □

Como ya hemos mencionado anteriormente (véanse los corolarios 3.4 y 3.5), la construcción de funciones bent introducida en la sección 2.1 (véanse los corolarios 2.1 y 2.1; es decir, lo que llamamos construcciones A y B en las páginas 37 y 39, respectivamente), es un caso particular de la construcción dada en este capítulo. Ahora, probamos que la construcción introducida en el corolario 2.5 (es decir, lo que llamamos construcción D en la página 39) coincide con la construcción introducida en el corolario 3.6, cambiando las funciones bent de n variables por las funciones asociadas de máximo peso. Para ello, antes necesitamos el siguiente resultado.

Teorema 3.5: *Si $f(\boldsymbol{x})$ es una función bent de n variables y $\boldsymbol{a} \in \mathbb{F}_2^n$, entonces*

$$(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}) = f^+(\boldsymbol{x} \oplus \boldsymbol{a}). \tag{3.12}$$

Demostración: Recordemos que

$$\mathrm{Sop}\left((f \oplus l_{\boldsymbol{a}})^+\right) = \left\{\boldsymbol{u} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{a}} \oplus l_{\boldsymbol{u}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\right\},$$

$$\mathrm{Sop}\left(f^+\right) = \left\{\boldsymbol{v} \in \mathbb{F}_2^n \mid w(f \oplus l_{\boldsymbol{v}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\right\}.$$

Entonces, como consecuencia del teorema 1.1(a), tenemos que el conjunto

$$\boldsymbol{a} \oplus \mathrm{Sop}\left(f^+\right) = \left\{\boldsymbol{a} \oplus \boldsymbol{v} \mid \boldsymbol{v} \in \mathrm{Sop}\left(f^+\right)\right\}$$

es el soporte de $f^+(\boldsymbol{x} \oplus \boldsymbol{a})$.

Si $\boldsymbol{u} \in \mathrm{Sop}\left((f \oplus l_{\boldsymbol{a}})^+\right)$, entonces

$$2^{n-1} + 2^{\frac{n}{2}-1} = w(f \oplus l_{\boldsymbol{a}} \oplus l_{\boldsymbol{u}}) = w(f \oplus l_{\boldsymbol{a} \oplus \boldsymbol{u}})$$

y, como consecuencia, $\boldsymbol{a} \oplus \boldsymbol{u} \in \mathrm{Sop}\left(f^+\right)$; es decir, $\boldsymbol{u} \in \boldsymbol{a} \oplus \mathrm{Sop}\left(f^+\right)$. Por tanto,

$$\mathrm{Sop}\left((f \oplus l_{\boldsymbol{a}})^+\right) \subseteq \boldsymbol{a} \oplus \mathrm{Sop}\left(f^+\right).$$

Mediante un argumento similar, $\boldsymbol{a} \oplus \mathrm{Sop}\left(f^+\right) \subseteq \mathrm{Sop}\left((f \oplus l_{\boldsymbol{a}})^+\right)$ y por lo tanto,

$$\mathrm{Sop}\left((f \oplus l_{\boldsymbol{a}})^+\right) = \boldsymbol{a} \oplus \mathrm{Sop}\left(f^+\right).$$

Puesto que las funciones $(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x})$ y $f^+(\boldsymbol{x} \oplus \boldsymbol{a})$ tienen el mismo soporte, podemos afirmar que son iguales. □

Ahora, como consecuencia de este resultado, podemos escribir el corolario 3.6 de la siguiente manera (véase el corolario 2.5).

Corolario 3.8: *Sean* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ *con* $\boldsymbol{a} \neq \boldsymbol{b}$ *y supongamos que* $f(\boldsymbol{x})$ *es una función bent de* n *variables. Si* σ *es una permutación de* $\{0,1,2,3\}$*, entonces*

$$\begin{aligned} D_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) =& m_{\sigma(0)}(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y}) f^+(\boldsymbol{x} \oplus \boldsymbol{a}) m_{\sigma(2)}(\boldsymbol{y}) f^+(\boldsymbol{x} \oplus \boldsymbol{b}) \\ & \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus f^+(\boldsymbol{x} \oplus \boldsymbol{a} \oplus \boldsymbol{b})\right) \end{aligned}$$

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

Observemos que tomando una función bent de n variables $f(\boldsymbol{x})$, el corolario anterior, generalmente, proporciona una función bent diferente a la proporcionada por el corolario 2.5 (lo que llamamos construcción D en la página 39); sin embargo, al variar $f(\boldsymbol{x})$ en el conjunto de todas las funciones bent de n variables y las bases de Gauss-Jordan $\{\boldsymbol{a}, \boldsymbol{b}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$, ambos corolarios proporcionan las mismas funciones bent de $n+2$ variables. Por tanto, tenemos el siguiente resultado (véase el teorema 2.4) que proporciona el número de funciones bent diferentes que podemos construir a partir del corolario 3.6 (o equivalentemente, del corolario 3.8).

Teorema 3.6: *Si* ν_n *es el número de funciones bent de* n *variables, entonces el número de funciones bent de* $n+2$ *variables que podemos construir utilizando el corolario 3.6 (o equivalentemente, el corolario 3.8) es*

$$8\binom{2^n-1}{2}\nu_n.$$

Demostración: De la última parte de la demostración del teorema 2.4, tenemos que el corolario 2.5 (o equivalentemente, el corolario 3.6) proporciona

$$4!\nu_n \frac{(2^n-1)(2^{n-1}-1)}{3} = 8\binom{2^n-1}{2}\nu_n. \qquad \square$$

Igual que ocurría con el corolario 3.6, no todas las funciones bent construidas de acuerdo con el corolario 3.7 son distintas entre sí, como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 3.4: Supongamos que $n = 2$, consideremos los vectores $\boldsymbol{a} = \mathbf{1} = (0,1)$, $\boldsymbol{b} = \mathbf{2} = (1,0)$ y las funciones bent de 2 variables

$$f(\boldsymbol{x}) = m_0(\boldsymbol{x}) \quad \text{y} \quad g(\boldsymbol{x}) = 1 \oplus m_3(\boldsymbol{x}).$$

Si consideramos la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix},$$

entonces, de acuerdo con el corolario 3.7 y la tabla 3.1 (véase también el ejemplo 3.3 para la expresión de las funciones $l_{\mathbf{1}}(\boldsymbol{x})$, $l_{\mathbf{2}}(\boldsymbol{x})$ y $l_{\mathbf{3}}(\boldsymbol{x})$), tenemos que

$$\begin{aligned}
&E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \\
&= m_0(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(f \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})(g \oplus l_{\mathbf{2}})^+(\boldsymbol{x}) \\
&\quad \oplus m_3(\boldsymbol{y}) \left(1 \oplus (g \oplus l_{\mathbf{3}})^+(\boldsymbol{x})\right) \\
&= m_0(\boldsymbol{y}) \left(m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \oplus \left(m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y})\right) \left(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\
&\quad \oplus m_3(\boldsymbol{y}) m_0(\boldsymbol{x}) \\
&= m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_3(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_6(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \\
&\quad \oplus m_8(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x}).
\end{aligned}$$

Consideremos ahora los vectores $\boldsymbol{u} = \mathbf{1} = (0,1)$, $\boldsymbol{v} = \mathbf{3} = (1,1)$ y las funciones bent de 2 variables

$$p(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \quad \text{y} \quad q(\boldsymbol{x}) = m_3(\boldsymbol{x}).$$

Si consideramos la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix},$$

entonces, procediendo como en el caso anterior, tenemos que

$$\begin{aligned}
&E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}) \\
&= m_1(\boldsymbol{y}) p^+(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})(p \oplus l_{\mathbf{1}})^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})(q \oplus l_{\mathbf{3}})^+(\boldsymbol{x})
\end{aligned}$$

$$
\begin{aligned}
&\oplus m_2(\boldsymbol{y})\left(1 \oplus (q \oplus l_{\boldsymbol{2}})^{+}(\boldsymbol{x})\right) \\
&= m_0(\boldsymbol{y})\left(m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \oplus m_3(\boldsymbol{y}) m_0(\boldsymbol{x}) \\
&\oplus \left(m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y})\right)\left(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right) \\
&= m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_3(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_6(\boldsymbol{y},\boldsymbol{x}) \oplus m_7(\boldsymbol{y},\boldsymbol{x}) \\
&\oplus m_8(\boldsymbol{y},\boldsymbol{x}) \oplus m_{10}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{11}(\boldsymbol{y},\boldsymbol{x}) \oplus m_{12}(\boldsymbol{y},\boldsymbol{x})
\end{aligned}
$$

que, evidentemente, coincide con $E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$. ■

Notemos que en el ejemplo anterior se satisfacen las igualdades

$$g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{3}}(\boldsymbol{x}) \qquad \text{y} \qquad q(\boldsymbol{x}) = p(\boldsymbol{x}) \oplus l_{\boldsymbol{2}}(\boldsymbol{x}) \oplus 1.$$

Por tanto, con el fin de evitar estas situaciones en la construcción de las funciones $E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ introducida en el corolario 3.7, supondremos siempre que

$$g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \oplus c, \quad \text{para todo } (\boldsymbol{c}, c) \in \mathbb{F}_2^n \times \mathbb{F}_2.$$

El siguiente resultado establece que, bajo ciertas condiciones, las funciones bent obtenidas a partir del corolario 3.7 son todas diferentes entre sí.

Lema 3.5: *Sean $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ tales que $\boldsymbol{a} \neq \boldsymbol{b}$ y $\boldsymbol{u} \neq \boldsymbol{v}$ y consideremos cuatro funciones bent $f(\boldsymbol{x})$, $g(\boldsymbol{x})$, $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$ de n variables tales que*

(a) $f(\boldsymbol{x}) \neq p(\boldsymbol{x})$,
(b) $f(\boldsymbol{x}) \neq p(\boldsymbol{x}) \oplus l_{\boldsymbol{u}}(\boldsymbol{x})$,
(c) $f(\boldsymbol{x}) \neq q(\boldsymbol{x}) \oplus l_{\boldsymbol{v}}(\boldsymbol{x})$,
(d) $f(\boldsymbol{x}) \neq 1 \oplus q(\boldsymbol{x}) \oplus l_{\boldsymbol{u}}(\boldsymbol{x}) \oplus l_{\boldsymbol{v}}(\boldsymbol{x})$.

Supongamos que $E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 3.9 utilizando las funciones bent $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$, los vectores $\boldsymbol{a}$ y $\boldsymbol{b}$ y la permutación σ de $\{0,1,2,3\}$. Supongamos también que $E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el corolario 3.9 utilizando las funciones bent $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$, los vectores $\boldsymbol{u}$ y $\boldsymbol{v}$ y la permutación τ de $\{0,1,2,3\}$. Entonces

$$E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \neq E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y

$$\boldsymbol{\xi}_f, \quad \boldsymbol{\xi}_{f,\boldsymbol{a}}, \quad \boldsymbol{\xi}_{g,\boldsymbol{b}}, \quad \boldsymbol{\xi}_{g,\boldsymbol{a}\oplus\boldsymbol{b}}, \quad \boldsymbol{\xi}_p, \quad \boldsymbol{\xi}_{p,\boldsymbol{u}}, \quad \boldsymbol{\xi}_{q,\boldsymbol{v}}, \quad \boldsymbol{\xi}_{q,\boldsymbol{u}\oplus\boldsymbol{v}}$$

son las tablas de verdad de $f^+(\boldsymbol{x})$, $(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x})$, $(g \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x})$, $(g \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})$, $p^+(\boldsymbol{x})$, $(p \oplus l_{\boldsymbol{u}})^+(\boldsymbol{x})$, $(q \oplus l_{\boldsymbol{v}})^+(\boldsymbol{x})$ y $(q \oplus l_{\boldsymbol{u}\oplus\boldsymbol{v}})^+(\boldsymbol{x})$ respectivamente; entonces las tablas de verdad de $E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ y $E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$\begin{aligned} E_{f,g,\boldsymbol{a},\boldsymbol{b}} &: \boldsymbol{\xi}_f \quad \boldsymbol{\xi}_{f,\boldsymbol{a}} \quad \boldsymbol{\xi}_{g,\boldsymbol{b}} \quad \mathbf{I} \oplus \boldsymbol{\xi}_{g,\boldsymbol{a}\oplus\boldsymbol{b}} \\ E_{p,q,\boldsymbol{u},\boldsymbol{v}} &: \boldsymbol{\xi}_p \quad \boldsymbol{\xi}_{p,\boldsymbol{u}} \quad \boldsymbol{\xi}_{q,\boldsymbol{v}} \quad \mathbf{I} \oplus \boldsymbol{\xi}_{q,\boldsymbol{u}\oplus\boldsymbol{v}} \end{aligned}$$

Si $E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) = E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$, entonces los cuatro bloques de la segunda fila son una permutación de los cuatro bloques de la primera fila. Por tanto, si consideramos los 4! casos correspondientes a esas permutaciones, por los corolarios 3.2 y 3.3 obtenemos siempre uno de los siguientes casos:

- $f(\boldsymbol{x}) = p(\boldsymbol{x})$,
- $f(\boldsymbol{x}) = p(\boldsymbol{x}) \oplus l_{\boldsymbol{u}}(\boldsymbol{x})$,
- $f(\boldsymbol{x}) = q(\boldsymbol{x}) \oplus l_{\boldsymbol{v}}(\boldsymbol{x})$,
- $f(\boldsymbol{x}) = 1 \oplus q(\boldsymbol{x}) \oplus l_{\boldsymbol{v}}(\boldsymbol{x})$.

Así que, en todos los casos obtenemos una contradicción y, por tanto,

$$E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \neq E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}). \qquad \square$$

Así que, añadiendo a la construcción introducida en el corolario 3.7 las condiciones del lema anterior, tenemos el siguiente resultado.

Corolario 3.9: *Sean $\boldsymbol{a},\boldsymbol{b} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ con $\boldsymbol{a} \neq \boldsymbol{b}$ y supongamos que $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son funciones bent de n variables tales que*

(a) $g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x})$,
(b) $g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x})$,

donde $\boldsymbol{c} \in \{\mathbf{0}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a}\oplus\boldsymbol{b}\}$. Si σ es una permutación de $\{0,1,2,3\}$, entonces

$$\begin{aligned} E_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) =& m_{\sigma(0)}(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_{\sigma(1)}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}) \oplus m_{\sigma(2)}(\boldsymbol{y})(g \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x}) \\ & \oplus m_{\sigma(3)}(\boldsymbol{y}) \left(1 \oplus (g \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})\right) \end{aligned}$$

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

Ahora, si llamamos **construcción** E a la construcción proporcionada por el corolario 3.9, el siguiente resultado establece, como consecuencia del lema 3.5, el número de funciones bent de $n+2$ variables que proporciona la construcción E.

Teorema 3.7: *Si ν_n es el número de funciones bent de n variables, entonces el número de funciones bent de $n+2$ variables que podemos construir a partir del corolario 3.9 es*

$$4!\binom{2^n-1}{2}\frac{\nu_n}{2^n}\left(\frac{\nu_n}{2^{n+1}}-1\right). \tag{3.13}$$

DEMOSTRACIÓN: Como consecuencia del lema 3.5, podemos elegir $f(\boldsymbol{x})$ de $\nu_n/2^n$ formas distintas y, fijada $f(\boldsymbol{x})$, podemos escoger $g(\boldsymbol{x})$ de $\nu_n/2^{n+1}-1$ formas distintas. Por otro lado, podemos elegir los vectores $\boldsymbol{a}$ y $\boldsymbol{b}$ de $\binom{2^n-1}{2}$ formas distintas y como hay 4! permutaciones diferentes de $\{0,1,2,3\}$, con esto obtendríamos el resultado.□

Notemos que para $n=2$ la expresión (3.13) es igual a 0, es decir, no obtenemos ninguna función bent de 4 variables. Esto es debido a que no existen funciones bent de 2 variables cumpliendo las condiciones del corolario 3.9.

Como ya hemos comentado en este capítulo, los corolarios 3.4, 3.5 y 3.6 son un caso particular de los corolarios 2.1, 2.2 y 2.5. Por tanto, sabemos que las funciones bent obtenidas a través de estas construcciones son distintas entre sí (son las funciones correspondientes a las llamadas construcciones A, B y D). Sin embargo, aún nos queda por probar que las funciones bent obtenidas a partir del corolario 3.9 (es decir, las correspondientes a la construcción E) son todas distintas a las funciones bent obtenidas a partir de los corolarios 3.4, 3.5 y 3.6 (es decir, las correspondientes a la construcciones A, B y D).

Lema 3.6: *Sean $f_0(\boldsymbol{x})$,$f(\boldsymbol{x})$, $g(\boldsymbol{x})$, $h(\boldsymbol{x})$, $p(\boldsymbol{x})$, $q(\boldsymbol{x})$ funciones bent de n variables (no necesariamente distintas). Supongamos que $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida en el corolario 3.4 utilizando $f_0(\boldsymbol{x})$. Supongamos que $B_{f,g}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida en el corolario 3.5 utilizando $f(\boldsymbol{x})$, $g(\boldsymbol{x})$ y la permutación σ de $\{0,1,2,3\}$. Supongamos que $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida en el corolario 3.6 utilizando $h(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a},\boldsymbol{b}\}$ de $\mathbb{F}_2^n$ de cardinalidad 2 y la permutación τ de $\{0,1,2,3\}$. Finalmente, supongamos que $E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida en el corolario 3.9 utilizando $p(\boldsymbol{x})$, $q(\boldsymbol{x})$, los vectores*

$\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, con $\boldsymbol{u} \neq \boldsymbol{v}$ y la permutación α de $\{0,1,2,3\}$. Entonces

$$A_{f_0}(\boldsymbol{y},\boldsymbol{x}) \neq E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}),\ B_{f,g}(\boldsymbol{y},\boldsymbol{x}) \neq E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}) \text{ y } D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \neq E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x}).$$

DEMOSTRACIÓN: Si $\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a 1 y $\boldsymbol{\xi_0}$, $\boldsymbol{\xi}$, $\boldsymbol{\eta}$, $\boldsymbol{\zeta}$, $\boldsymbol{\lambda}$ y $\boldsymbol{\gamma}$ son las tablas de verdad de $f_0(\boldsymbol{x})$, $f(\boldsymbol{x})$, $g(\boldsymbol{x})$, $h(\boldsymbol{x})$, $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$, $B_{f,g}(\boldsymbol{y},\boldsymbol{x})$, $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ y $E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en ese orden ni el mismo orden para todos):

$$\begin{array}{rcccc}
A_{f_0}: & \boldsymbol{\xi_0} & \boldsymbol{\xi_0} & \boldsymbol{\xi_0} & \mathbf{I} \oplus \boldsymbol{\xi_0} \\
B_{f,g}: & \boldsymbol{\xi} & \boldsymbol{\xi} & \boldsymbol{\eta} & \mathbf{I} \oplus \boldsymbol{\eta} \\
D_{h,\boldsymbol{a},\boldsymbol{b}}: & \boldsymbol{\zeta} & \boldsymbol{\zeta_a} & \boldsymbol{\zeta_b} & \mathbf{I} \oplus \boldsymbol{\zeta_{a\oplus b}} \\
E_{p,q,\boldsymbol{u},\boldsymbol{v}}: & \boldsymbol{\lambda} & \boldsymbol{\lambda_u} & \boldsymbol{\gamma_v} & \mathbf{I} \oplus \boldsymbol{\gamma_{u\oplus v}}
\end{array}$$

donde $\boldsymbol{\zeta_a}$, $\boldsymbol{\zeta_b}$, $\boldsymbol{\zeta_{a\oplus b}}$, $\boldsymbol{\lambda_u}$, $\boldsymbol{\gamma_v}$ y $\boldsymbol{\gamma_{u\oplus v}}$ son las tablas de verdad de $(h \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x})$, $(h \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x})$, $(h \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})$, $(p \oplus l_{\boldsymbol{u}})^+(\boldsymbol{x})$, $(q \oplus l_{\boldsymbol{v}})^+(\boldsymbol{x})$ y $(q \oplus l_{\boldsymbol{u}\oplus\boldsymbol{v}})^+(\boldsymbol{x})$, respectivamente.

El resultado es ahora evidente ya que $A_{f_0}(\boldsymbol{y},\boldsymbol{x})$ tiene tres bloques idénticos, $B_{f,g}(\boldsymbol{y},\boldsymbol{x})$ tiene sólo dos bloques idénticos y todos los bloques de $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ y $E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ son diferentes. Además, si suponemos que $D_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) = E_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$, entonces las funciones $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$ no cumplirían las condiciones exigidas en el corolario 3.9. □

Ahora, como consecuencia del lema 3.6 y de los teoremas 3.6 y 3.7 podemos enunciar el resultado siguiente que establece el número de funciones bent de $n+2$ variables distintas que podemos construir de acuerdo con los corolarios 3.6 y 3.9.

Corolario 3.10: *Si ν_n es el número de funciones bent de n variables, entonces el número de funciones bent de $n+2$ variables distintas que podemos construir utilizando los corolarios 3.6 y 3.9 es*

$$4!\binom{2^n-1}{2}\nu_n\left(\frac{1}{3}+\frac{1}{2^n}\left(\frac{\nu_n}{2^{n+1}}-1\right)\right). \tag{3.14}$$

DEMOSTRACIÓN: De acuerdo con los teoremas 3.6 y 3.7, el número de funciones bent de $n+2$ variables que proporcionan los corolarios 3.6 y 3.9 es

$$8\binom{2^n-1}{2}\nu_n + 4!\binom{2^n-1}{2}\frac{\nu_n}{2^n}\left(\frac{\nu_n}{2^{n+1}}-1\right) = 4!\binom{2^n-1}{2}\nu_n\left(\frac{1}{3}+\frac{1}{2^n}\left(\frac{\nu_n}{2^{n+1}}-1\right)\right)$$

ya que, por el lema 3.6, las funciones bent proporcionadas por los corolarios 3.6 y 3.9 son distintas entre sí. □

Finalmente, tal como habíamos anunciado al inicio de la sección, cualquier otra posibilidad de elección de los vectores $\boldsymbol{a}$ y $\boldsymbol{b}$, o de las funciones $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$, puede ser reducida a uno de los casos considerados en los corolarios 3.4, 3.5, 3.6 y 3.9. Por ejemplo:

- Si $\boldsymbol{a}=\boldsymbol{0}$ y $\boldsymbol{b}\neq\boldsymbol{0}$, entonces la cuaterna (3.10) se convierte en

  $$(f(\boldsymbol{x}), f(\boldsymbol{x}), g(\boldsymbol{x})\oplus l_{\boldsymbol{b}}(\boldsymbol{x}), 1\oplus g(\boldsymbol{x})\oplus l_{\boldsymbol{b}}(\boldsymbol{x}))$$

  que corresponde al corolario 3.4 cuando $f(\boldsymbol{x})=g(\boldsymbol{x})\oplus l_{\boldsymbol{b}}(\boldsymbol{x})$, o al corolario 3.5 si $f(\boldsymbol{x})\neq g(\boldsymbol{x})\oplus l_{\boldsymbol{b}}(\boldsymbol{x})$.
- Si $\boldsymbol{a}\neq\boldsymbol{0}$ y $\boldsymbol{b}=\boldsymbol{0}$, entonces la cuaterna (3.10) se convierte en

  $$(f(\boldsymbol{x}), f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x}), g(\boldsymbol{x}), 1\oplus g(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x}))$$

  que corresponde al corolario 3.5 en los casos en los que
  - $g(\boldsymbol{x})=f(\boldsymbol{x})$,
  - $g(\boldsymbol{x})=1\oplus f(\boldsymbol{x})$,
  - $g(\boldsymbol{x})=f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x})$,
  - $g(\boldsymbol{x})=1\oplus f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x})$;

  o al corolario 3.9 cuando
  - $g(\boldsymbol{x})\neq f(\boldsymbol{x})$,
  - $g(\boldsymbol{x})\neq 1\oplus f(\boldsymbol{x})$,
  - $g(\boldsymbol{x})\neq f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x})$,
  - $g(\boldsymbol{x})\neq 1\oplus f(\boldsymbol{x})\oplus l_{\boldsymbol{a}}(\boldsymbol{x})$.

Así que, como consecuencia del teorema 3.4, el lema 3.6 y el corolario 3.10, tenemos los resultados siguientes que establecen una cota inferior para ω_n y el número de funciones bent diferentes que podemos obtener a partir de los corolarios 3.4, 3.5, 3.6 y 3.9.

Corolario 3.11: *Si ν_n es el número de funciones bent de n variables y ω_n es el número de cuaternas de funciones bent que satisfacen la ecuación (3.4), excluyendo las correspondientes a los corolarios 3.4 y 3.5, entonces*

$$\omega_n \geq \binom{2^n-1}{2}\nu_n\left(\frac{1}{3}+\frac{1}{2^n}\left(\frac{\nu_n}{2^{n+1}}-1\right)\right).$$

Corolario 3.12: *Si ν_n es el número de funciones bent de n variables, entonces el número de funciones bent de $n+2$ variables diferentes que podemos construir utilizando los corolarios 3.4, 3.5, 3.6 y 3.9 es*

$$6\nu_n^2+\left(-8+24\binom{2^n-1}{2}\left(\frac{1}{3}+\frac{1}{2^n}\left(\frac{\nu_n}{2^{n+1}}-1\right)\right)\right)\nu_n. \tag{3.15}$$

DEMOSTRACIÓN: Por el teorema 3.3, el número de funciones bent de $n+2$ variables que proporcionan los corolarios 3.4 y 3.5 viene dado por la expresión (3.9).

Análogamente, por el corolario 3.10, el número de funciones bent de $n+2$ variables que proporcionan los corolarios 3.6 y 3.9 viene dado por la expresión (3.14).

Ahora, como consecuencia del lema 3.6, podemos afirmar que al sumar las expresiones (3.9) y (3.14) obtenemos el número de funciones bent de $n+2$ variables que proporcionan los corolarios 3.4, 3.5, 3.6 y 3.9. Dicha suma coincide con la expresión (3.15) como podemos comprobar sin ninguna dificultad. □

Observemos que para $n=2$, la expresión (3.15) se convierte en

$$6\cdot 8^2-8\cdot 8+24\cdot 3\cdot 8\left(8-2^3+\frac{1}{3}\right)=512,$$

es decir, partiendo de las ocho funciones bent de 2 variables, podemos asegurar que nuestra construcción proporciona 512 funciones bent de 4 variables de las 896 que existen.

Análogamente, para $n=4$, la expresión (3.15) se convierte en

$$6\cdot 896^2-8\cdot 896+24\cdot 105\cdot 896\left(896-2^5+\frac{1}{3}\right)=1\,956\,405\,248\leq 5\,425\,430\,528=\nu_6.$$

Y, finalmente, para $n = 6$, la expresión (3.15) se convierte en

$$\begin{aligned}
&6 \cdot 5\,425\,430\,528^2 - 8 \cdot 5\,425\,430\,528 \\
&+ 24 \cdot 1953 \cdot 5\,425\,430\,528 \left(5\,425\,430\,528 - 2^7 + \frac{1}{3}\right) \\
&= 1\,379\,867\,792\,836\,951\,751\,574\,352 \\
&< 99\,270\,589\,265\,934\,370\,305\,785\,861\,242\,880.
\end{aligned}$$

3.3 Comparación con otros métodos

En esta sección comparamos las construcciones introducidas en este capítulo con los métodos de construcción clásicos introducidos en el capítulo 1. En la sección 3.2, ya comprobamos que las construcciones definidas en el capítulo 2 son casos particulares de la construcción definida en este capítulo, por lo tanto, no es necesaria su comparación en esta sección.

3.3.1 Clase Rothaus

El ejemplo siguiente muestra que existen funciones bent construidas a partir del teorema 3.2 que no son funciones bent de la clase Rothaus, es decir, que no se pueden obtener a partir del teorema 1.3.

Ejemplo 3.5: Supongamos que $n = 4$ y consideremos las funciones booleanas de 4 variables

$$\begin{aligned}
f_0(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_8(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}), \\
f_1(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_9(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}), \\
f_2(\boldsymbol{x}) &= m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}), \\
f_3(\boldsymbol{x}) &= m_3(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}),
\end{aligned}$$

donde sus funciones asociadas de mínimo peso son

$$f_0^-(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}),$$

$$f_1^-(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{14}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x}),$$
$$f_2^-(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}) \oplus m_{13}(\boldsymbol{x}) \oplus m_{15}(\boldsymbol{x})$$
$$f_3^-(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x})$$
$$\oplus m_9(\boldsymbol{x}) \oplus m_{10}(\boldsymbol{x}) \oplus m_{11}(\boldsymbol{x}) \oplus m_{12}(\boldsymbol{x}).$$

Si consideramos la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 2 & 3 \end{pmatrix},$$

entonces, a partir del teorema 3.2, aplicándolo para las funciones de mínimo peso, y por el corolario 1.2, obtenemos la función bent de 6 variables dada por

$$\begin{aligned}
&F(\boldsymbol{y}, \boldsymbol{x}) \\
&= m_1(\boldsymbol{y}) f_0^-(\boldsymbol{x}) \oplus m_0(\boldsymbol{y}) f_1^-(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_2^-(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f_3^-(\boldsymbol{x}) \\
&= m_{16}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{23}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{27}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{29}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{30}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{31}(\boldsymbol{y}, \boldsymbol{x}) \\
&\quad \oplus m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_3(\boldsymbol{y}, \boldsymbol{x}) \oplus m_5(\boldsymbol{y}, \boldsymbol{x}) \oplus m_7(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{14}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{15}(\boldsymbol{y}, \boldsymbol{x}) \\
&\quad \oplus m_{32}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{35}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{38}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{39}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{45}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{47}(\boldsymbol{y}, \boldsymbol{x}) \\
&\quad \oplus m_{48}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{49}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{50}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{52}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{53}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{54}(\boldsymbol{y}, \boldsymbol{x}) \\
&\quad \oplus m_{57}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{58}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{59}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{60}(\boldsymbol{y}, \boldsymbol{x}) \\
=&m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_3(\boldsymbol{y}, \boldsymbol{x}) \oplus m_5(\boldsymbol{y}, \boldsymbol{x}) \oplus m_7(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{14}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{15}(\boldsymbol{y}, \boldsymbol{x}) \\
&\oplus m_{16}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{23}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{27}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{29}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{30}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{31}(\boldsymbol{y}, \boldsymbol{x}) \\
&\oplus m_{32}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{35}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{38}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{39}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{45}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{47}(\boldsymbol{y}, \boldsymbol{x}) \\
&\oplus m_{48}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{49}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{50}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{52}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{53}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{54}(\boldsymbol{y}, \boldsymbol{x}) \\
&\oplus m_{57}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{58}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{59}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{60}(\boldsymbol{y}, \boldsymbol{x}).
\end{aligned}$$

Si calculamos su forma normal algebraica a través de la definición de minterm, tenemos que

$$F(\boldsymbol{y}, \boldsymbol{x}) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus y_1y_2x_2$$

$$\oplus\, y_1y_2x_3 \oplus y_1y_2x_4 \oplus y_1x_2x_3 \oplus y_1x_2x_4 \oplus y_2x_2x_4 \oplus y_2x_3x_4,$$

en cuya expresión no aparece el término y_1y_2 (que correspondería al término $x_{n+1}x_{n+2}$ de las nuevas variables); por el comentario que aparece después del teorema 1.3, podemos asegurar que no es de la clase Rothaus. ■

3.3.2 Clase Maiorana-McFarland

Ahora mostramos un ejemplo de función bent construida a través del teorema 3.2, que no se puede obtener a partir de la construcción de Maiorana-McFarland introducida en el teorema 1.4.

Ejemplo 3.6: Supongamos que $n = 2$ y consideremos las funciones boolenas de 2 variables

$$\begin{aligned} f_0(\boldsymbol{x}) =& f_1(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}),\\ f_2(\boldsymbol{x}) =& m_2(\boldsymbol{x}),\\ f_3(\boldsymbol{x}) =& m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}), \end{aligned}$$

entonces, sus funciones asociadas de máximo peso son

$$\begin{aligned} f_0^+(\boldsymbol{x}) =& f_1^+(\boldsymbol{x}) = m_0(\boldsymbol{x}),\\ f_2^+(\boldsymbol{x}) =& m_1(\boldsymbol{x}),\\ f_3^+(\boldsymbol{x}) =& m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}). \end{aligned}$$

Si consideramos σ como la permutación identidad, entonces aplicando el teorema 3.2 y el corolario 1.2, obtenemos la función bent de 4 variables dada por

$$\begin{aligned} & F(\boldsymbol{y}, \boldsymbol{x})\\ =& m_0(\boldsymbol{y}) f_0^+(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) f_1^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) f_2^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) f_3^+(\boldsymbol{x})\\ =& m_0(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) \left(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})\right)\\ =& m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_4(\boldsymbol{y}, \boldsymbol{x}) \oplus m_9(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{12}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{14}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{15}(\boldsymbol{y}, \boldsymbol{x}). \end{aligned}$$

Sin embargo, no es de la clase Maiorana-McFarland ya que no existe ninguna permutación π de $\mathbb{F}_2^2$ tal que la función se pueda expresar como en el teorema 1.4.

Además, si calculamos su forma normal algebraica a través de la definición de minterm, obtenemos que

$$F(\boldsymbol{y}, \boldsymbol{x}) = 1 \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus y_1 \oplus y_1x_1 \oplus y_1y_2$$

donde la aparición del término x_1x_2 no se ajustaría a la fórmula $\langle \boldsymbol{x}, \pi(\boldsymbol{y}) \rangle \oplus f(\boldsymbol{y})$ de una función de clase Maiorana-McFarland. ■

3.3.3 Clase Carlet

Ahora mostramos un ejemplo de función bent construida a través del teorema 3.2, que no se puede obtener a partir de la construcción de Carlet introducida en el teorema 1.5.

Ejemplo 3.7: Supongamos que $n = 2$ y consideremos las funciones boolenas de 2 variables

$$\begin{aligned} f_0(\boldsymbol{x}) =& m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x}), \\ f_1(\boldsymbol{x}) =& m_2(\boldsymbol{x}), \\ f_2(\boldsymbol{x}) =& m_1(\boldsymbol{x}), \\ f_3(\boldsymbol{x}) =& m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}), \end{aligned}$$

entonces, las funciones asociadas de máximo peso son

$$\begin{aligned} f_0^+(\boldsymbol{x}) =& m_0(\boldsymbol{x}), \\ f_1^+(\boldsymbol{x}) =& m_1(\boldsymbol{x}), \\ f_2^+(\boldsymbol{x}) =& m_2(\boldsymbol{x}), \\ f_3^+(\boldsymbol{x}) =& m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}). \end{aligned}$$

Si consideramos la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix},$$

Variables	4	6	8	10
Bent	896	5 425 430 528	2^{106}	?
Rothaus	512	?	?	?
Maiorana-McFarland	384	10 321 920	2^{60}	2^{150}
Carlet	320	?	?	?
Construcción A	32	3 584	$2^{34,3}$	$2^{108,3}$
Construcción B	288	4 806 144	$2^{67,25}$	$2^{215,17}$
Construcción C	288	161 280	2^{42}	$2^{117,87}$
Construcción D	192	752 640	$2^{46,26}$	$2^{124,27}$
Construcción E	0	68 040	$2^{40,85}$	$2^{116,85}$

Tabla 3.4: *Número de funciones bent construidas con diferentes métodos*

entonces, por el teorema 3.2 y por el corolario 1.2, obtenemos la función bent de 4 variables dada por

$$\begin{aligned}
&F(\boldsymbol{y},\boldsymbol{x})\\
=&m_1(\boldsymbol{y})f_0^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})f_1^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})f_2^+(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})f_3^+(\boldsymbol{x}) \oplus\\
=&m_1(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})m_2(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})\left(m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x})\right)\\
=&m_0(\boldsymbol{y},\boldsymbol{x}) \oplus m_1(\boldsymbol{y},\boldsymbol{x}) \oplus m_2(\boldsymbol{y},\boldsymbol{x}) \oplus m_4(\boldsymbol{y},\boldsymbol{x}) \oplus m_9(\boldsymbol{y},\boldsymbol{x}) \oplus m_{14}(\boldsymbol{y},\boldsymbol{x})
\end{aligned}$$

Sin embargo, esta función no es de la clase Carlet ya que no existen funciones bent de 2 variables $f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), g_0(\boldsymbol{y})$ y $g_1(\boldsymbol{y})$ tales que pueda expresarse como la función definida por el teorema 1.5. Dicha comprobación se ha verificado computacionalmente calculando todas las funciones de la clase Carlet de 4 variables y comprobando que la función obtenida a través de este ejemplo no era ninguna de ellas. ■

La tabla 3.4 recopila el número de funciones bent que podemos obtener a partir de las construcciones A, B, C, D y E definidas en los capítulos 2 y 3, comparándolo con el número de funciones bent de las clases Rothaus, Maiorana-McFarland y Carlet (para $m = 2$). El número de funciones bent para $n > 8$ variables, el número de funciones de la clase Rothaus de 6 y 8 variables y el número de funciones bent de la clase Carlet (para $n > 2$) son aún desconocidos. Observamos que para 4 variables el

número de funciones bent proporcionado por las construcciones A y B es el mismo que el número de funciones bent propocionado por la construcción de Rothaus; sin embargo, la construcción B (dada en el teorema 2.3) proporciona funciones bent distintas a las de la clase Rothaus como hemos comprobado en la subsección 2.3.2.

Capítulo 4

Caracterización y construcción de funciones bent de $n+1$ variables a partir de funciones booleanas de n variables

4.1 Construcción basada en dos funciones booleanas

Las construcciones definidas en los capítulos 2 y 3 se basan en la obtención de funciones bent de $n+2$ variables a partir de funciones bent de n variables, con n un entero positivo par. Sin embargo, en este capítulo definimos un método de construcción a partir del cual generamos funciones bent de $n+1$ variables partiendo de funciones booleanas de n variables (siendo n un entero positivo impar) que no pueden ser funciones bent. Además, también propocionamos la forma explícita de las funciones booleanas implicadas en la construcción, con lo que observamos que estas provienen a su vez de funciones bent de $n-1$ variables.

En todo este capítulo, suponemos que $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ son dos funciones booleanas de n variables y consideramos la función booleana de $n+1$ variables dada por

$$f(y, \boldsymbol{x}) = m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) f_1(\boldsymbol{x}). \tag{4.1}$$

Puesto que

$$m_i(y) = \begin{cases} 1, & \text{si } y = i, \\ 0, & \text{si } y \neq i, \end{cases}$$

tenemos que

$$f(0, \boldsymbol{x}) = f_0(\boldsymbol{x}) \qquad \text{y} \qquad f(1, \boldsymbol{x}) = f_1(\boldsymbol{x}). \tag{4.2}$$

Además, como consecuencia del corolario 1.1,

$$\mathrm{Sop}\,(f) = \mathrm{Sop}\,(f_0) \cup \{2^n + a \mid a \in \mathrm{Sop}\,(f_1)\}$$

y, como

$$\mathrm{Sop}\,(f_0) \cap \{2^n + a \mid a \in \mathrm{Sop}\,(f_1)\} = \emptyset,$$

tenemos que

$$w(f) = w(f_0) + w(f_1).$$

En cambio, si utilizamos vectores como subíndices de los minterms, entonces

$$\mathrm{Sop}\,(f) = \{(0, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_0)\} \cup \{(1, \boldsymbol{a}) \mid \boldsymbol{a} \in \mathrm{Sop}\,(f_1)\}. \tag{4.3}$$

El resultado siguiente, necesario para la demostración de uno de los teoremas principales de este capítulo (véase el teorema 4.1 más adelante), nos propociona el peso de la función $f(\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(\boldsymbol{x})$ a partir de los pesos de las funciones

$$f_0(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \quad \text{y} \quad f_1(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}).$$

Lema 4.1: *Sean $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ dos funciones booleanas de n variables y consideremos la función booleana $f(y, \boldsymbol{x})$ de $n+1$ variables definida por la expresión (4.1). Si $\boldsymbol{a} \in \mathbb{F}_2^n$ y $b \in \mathbb{F}_2$, entonces*

$$w(f \oplus l_{(b,\boldsymbol{a})}) = \begin{cases} w(f_0 \oplus l_{\boldsymbol{a}}) + w(f_1 \oplus l_{\boldsymbol{a}}), & \text{si } b = 0, \\ w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n - w(f_1 \oplus l_{\boldsymbol{a}}), & \text{si } b = 1. \end{cases}$$

Demostración: De la expresión (4.1) y de la definición de $l_{(b,\boldsymbol{a})}(y, \boldsymbol{x})$, tenemos que

$$f(y, \boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y, \boldsymbol{x}) = m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) f_1(\boldsymbol{x}) \oplus by \oplus l_{\boldsymbol{a}}(\boldsymbol{x}).$$

y	$\boldsymbol{x}$	$m_0(y)$	$m_1(y)$	$f_0(\boldsymbol{x})$	$f_1(\boldsymbol{x})$	by	$\lambda_{\boldsymbol{a}}(\boldsymbol{x})$	$f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$
$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{I}$	$\mathbf{0}$	$\boldsymbol{\xi}_0$	$\boldsymbol{\xi}_1$	$\mathbf{0}$	$\boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\mathbf{I}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{I}$	$\boldsymbol{\xi}_0$	$\boldsymbol{\xi}_1$	$b\mathbf{I}$	$\boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus b\mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Tabla 4.1: *Tabla de verdad de* $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$

$b=0$	$b=1$
$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_0 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$
$\boldsymbol{\xi}_1 \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$	$\boldsymbol{\xi}_1 \oplus \mathbf{I} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$

Tabla 4.2: *Tabla de verdad de* $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$ *para los distintos valores de* b.

Si $\mathbf{0}$ e $\mathbf{I}$ son las columnas de longitud 2^n con todos los elementos iguales a 0 y 1 respectivamente; $\boldsymbol{\tau}$ es la matriz de tamaño $2^n \times n$ cuya i-ésima fila es $\boldsymbol{i}$, para $i = 0, 1, \ldots, 2^n - 1$; $\boldsymbol{\xi}_0$ y $\boldsymbol{\xi}_1$ son las tablas de verdad de $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ respectivamente; y $\boldsymbol{\Lambda}_{\boldsymbol{a}}$ es la tabla de verdad de la función lineal $l_{\boldsymbol{a}}(\boldsymbol{x})$, entonces la última columna de la tabla 4.1 muestra la tabla de verdad de la función booleana $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$, donde $b\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a b.

Ahora, de la tabla 4.2, que representa los dos bloques de la tabla de verdad de la función booleana $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{a})}(y,\boldsymbol{x})$ para los diferentes valores de b, obtenemos el resultado, ya que $w(f_j \oplus l_{\boldsymbol{a}})$ coincide con el número de 1 del bloque $\boldsymbol{\xi}_j \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}}$ para $j = 0, 1$. □

A partir de ahora y hasta el final del capítulo, suponemos que n es impar y, por tanto, que $n+1$ es par. El siguiente resultado introduce una condición necesaria y suficiente para que la función $f(y,\boldsymbol{x})$ definida por la expresión (4.1) sea bent.

Teorema 4.1: *Sean* $f_0(\boldsymbol{x})$ *y* $f_1(\boldsymbol{x})$ *dos funciones booleanas de* n *variables. La función booleana* $f(y,\boldsymbol{x})$ *de* $n+1$ *variables definida por la expresión (4.1) es bent si y sólo si para todo* $\boldsymbol{a} \in \mathbb{F}_2^n$ *se satisface una de las dos condiciones siguientes:*

(a) $w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1} \pm 2^{\frac{n-1}{2}}$ y $w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1}$,
(b) $w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1}$ y $w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1} \pm 2^{\frac{n-1}{2}}$.

DEMOSTRACIÓN: Supongamos que $f(y, \boldsymbol{x})$ es una función bent. Entonces, de acuerdo con el teorema 1.2 tenemos que

$$w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n \pm 2^{\frac{n-1}{2}}$$

para todo $(b, \boldsymbol{a}) \in \mathbb{F}_2^{1+n}$.

Supongamos en primer lugar que $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n + 2^{\frac{n-1}{2}}$ cuando $b = 0, 1$. Entonces, por el lema 4.1,

$$2^n + 2^{\frac{n-1}{2}} = w(f_0 \oplus l_{\boldsymbol{a}}) + w(f_1 \oplus l_{\boldsymbol{a}}), \tag{4.4}$$

$$2^n + 2^{\frac{n-1}{2}} = w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n - w(f_1 \oplus l_{\boldsymbol{a}}). \tag{4.5}$$

Si sumamos miembro a miembro las igualdades (4.4) y (4.5) obtenemos que

$$2\left(2^n + 2^{\frac{n-1}{2}}\right) = 2w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n$$

y por tanto,

$$w(f_0 \oplus l_{\boldsymbol{a}}) = 2^n + 2^{\frac{n-1}{2}} - 2^{n-1} = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

Si en lugar de sumar las igualdades (4.4) y (4.5) las restamos, entonces obtenemos que

$$0 = 2w(f_1 \oplus l_{\boldsymbol{a}}) - 2^n,$$

con lo que

$$w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1}.$$

Supongamos ahora que $w(f \oplus l_{(b,\boldsymbol{a})}) = 2^n - 2^{\frac{n-1}{2}}$ cuando $b = 0, 1$. Entonces, mediante un razonamiento análogo al anterior, obtenemos que

$$w(f_0 \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n-1}{2}} \quad \text{y} \quad w(f_1 \oplus l_{\boldsymbol{a}}) = 2^{n-1}.$$

Finalmente, si suponemos que

$$w(f \oplus l_{b,\boldsymbol{a}}) = \begin{cases} 2^n + 2^{\frac{n-1}{2}}, & \text{si } b = 0, \\ 2^n - 2^{\frac{n-1}{2}}, & \text{si } b = 1, \end{cases}$$

o que

$$w(f \oplus l_{b,\boldsymbol{a}}) = \begin{cases} 2^n - 2^{\frac{n-1}{2}}, & \text{si } b = 0, \\ 2^n + 2^{\frac{n-1}{2}}, & \text{si } b = 1, \end{cases}$$

entonces, razonando de forma análoga, obtenemos las igualdades del apartado (b).

Para probar el recíproco, supongamos primero que se satisface la condición (a).

Si $b = 0$, entonces por el lema 4.1,

$$\begin{aligned} w(f \oplus l_{(b,\boldsymbol{a})}) &= w(f_0 \oplus l_{\boldsymbol{a}}) + w(f_1 \oplus l_{\boldsymbol{a}}) \\ &= 2^{n-1} \pm 2^{\frac{n-1}{2}} + 2^{n-1} \\ &= 2^n \pm 2^{\frac{n-1}{2}}. \end{aligned}$$

En cambio si $b = 1$, entonces, de nuevo por el lema 4.1,

$$\begin{aligned} w(f \oplus l_{(b,\boldsymbol{a})}) &= w(f_0 \oplus l_{\boldsymbol{a}}) + 2^n - w(f_1 \oplus l_{\boldsymbol{a}}) \\ &= 2^{n-1} \pm 2^{\frac{n-1}{2}} + 2^n - 2^{n-1} \\ &= 2^n \pm 2^{\frac{n-1}{2}}. \end{aligned}$$

Por tanto, por el teorema 1.2, $f(y, \boldsymbol{x})$ es una función bent de $n+1$ variables.

Finalmente, si se satisface la condición (b), mediante un razonamiento completamente análogo al anterior, también obtenemos que $f(y, \boldsymbol{x})$ es una función bent de $n+1$ variables. □

Como consecuencia inmediata del teorema anterior tenemos los siguientes dos corolarios que nos proporcionan algunas propiedades interesantes de las funciones booleanas de n variables $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ de la expresión (4.1).

Corolario 4.1: *Sean $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ dos funciones booleanas de n variables. Si la función booleana $f(y, \boldsymbol{x})$ de $n+1$ variables definida por la expresión (4.1) es bent, entonces sólo una de las dos funciones $f_0(\boldsymbol{x})$ o $f_1(\boldsymbol{x})$ es equilibrada.*

Demostración: Como $f(y, \boldsymbol{x})$ es una función bent, tomando $\boldsymbol{a} = \boldsymbol{0}$ en el teorema 4.1 sabemos que se satisface una de las dos condiciones siguientes:

- $w(f_0) = 2^{n-1} \pm 2^{\frac{n-1}{2}}$ y $w(f_1) = 2^{n-1}$,
- $w(f_0) = 2^{n-1}$ y $w(f_1) = 2^{n-1} \pm 2^{\frac{n-1}{2}}$.

Por tanto, es evidente que sólo una de las dos funciones $f_0(\boldsymbol{x})$ o $f_1(\boldsymbol{x})$ es equilibrada. □

Corolario 4.2: *Sean $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ dos funciones booleanas de n variables. Si la función booleana $f(y, \boldsymbol{x})$ de $n+1$ variables definida por la expresión (4.1) es bent, entonces*

$$f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \quad y \quad f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x})$$

son funciones equilibradas para todo $\boldsymbol{a} \in \mathbb{F}_2^n$.

DEMOSTRACIÓN: Por el teorema 1.2 tenemos que la función booleana

$$\begin{aligned} &f(y, \boldsymbol{x}) \oplus f((b, \boldsymbol{a}) \oplus (y, \boldsymbol{x})) = f(y, \boldsymbol{x}) \oplus f(b \oplus y, \boldsymbol{a} \oplus \boldsymbol{x}) \\ &= m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) f_1(\boldsymbol{x}) \oplus m_0(b \oplus y) f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus m_1(b \oplus y) f_1(\boldsymbol{a} \oplus \boldsymbol{x}) \end{aligned}$$

es equilibrada para todo $(b, \boldsymbol{a}) \in \mathbb{F}_2 \times \mathbb{F}_2^n$ con $(b, \boldsymbol{a}) \neq (0, \boldsymbol{0})$. Ahora, como por el lema 1.1

$$m_0(1 \oplus y) = m_1(y) \quad y \quad m_1(1 \oplus y) = m_0(y)$$

tenemos que

$$\begin{aligned} &f(y, \boldsymbol{x}) \oplus f((1, \boldsymbol{a}) \oplus (y, \boldsymbol{x})) \\ &= m_0(y) \left(f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x})\right) \oplus m_1(y) \left(f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x})\right) \end{aligned}$$

y, por tanto, utilizando la expresión (4.2),

$$\begin{aligned} 2^n &= \sum_{(y,\boldsymbol{x}) \in \mathbb{F}_2 \times \mathbb{F}_2^n} f(y, \boldsymbol{x}) \oplus f((1, \boldsymbol{a}) \oplus (y, \boldsymbol{x})) \\ &= \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} f(0, \boldsymbol{x}) \oplus f((1, \boldsymbol{a}) \oplus (0, \boldsymbol{x})) + \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} f(1, \boldsymbol{x}) \oplus f((1, \boldsymbol{a}) \oplus (1, \boldsymbol{x})) \\ &= \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} \left(f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x})\right) + \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} \left(f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x})\right). \end{aligned} \tag{4.6}$$

Ahora, como la aplicación $\sigma_{\boldsymbol{a}} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ dada por $\sigma_{\boldsymbol{a}}(\boldsymbol{x}) = \boldsymbol{a} \oplus \boldsymbol{x}$ es biyectiva, tenemos que

$$\sum_{\boldsymbol{x}\in\mathbb{F}_2^n} (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x})) = \sum_{\boldsymbol{x}\in\mathbb{F}_2^n} (f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x}))\,,$$

y de la expresión (4.6), concluimos que

$$2^{n-1} = \sum_{\boldsymbol{x}\in\mathbb{F}_2^n} (f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x})) \quad \text{y} \quad 2^{n-1} = \sum_{\boldsymbol{x}\in\mathbb{F}_2^n} (f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x}))\,;$$

por tanto, las funciones

$$f_0(\boldsymbol{a} \oplus \boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \quad \text{y} \quad f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{a} \oplus \boldsymbol{x})$$

son equilibradas. □

Notemos que si $f(y, \boldsymbol{x})$ es una función bent de $n+1$ variables, por el corolario 4.2 tenemos que la función booleana de n variables $f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x})$ es equilibrada (basta tomar $\boldsymbol{a} = \boldsymbol{0}$). Sin embargo, del hecho de que dicha función sea equilibrada no podemos asegurar que la función $f(y, \boldsymbol{x})$ sea bent, como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 4.1: Supongamos que $n = 3$ y consideremos las funciones booleanas de 3 variables

$$f_0(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \quad \text{y} \quad f_1(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_7(\boldsymbol{x}).$$

Claramente, la función booleana de 3 variables

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) = m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x})$$

es equilibrada y, por el corolario 1.1,

$$\begin{aligned} f(y, \boldsymbol{x}) &= m_0(y)\,(m_0(\boldsymbol{x}) \oplus m_6(\boldsymbol{x})) \oplus m_1(y)\,(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_7(\boldsymbol{x})) \\ &= m_0(y, \boldsymbol{x}) \oplus m_6(y, \boldsymbol{x}) \oplus m_8(y, \boldsymbol{x}) \oplus m_{10}(y, \boldsymbol{x}) \oplus m_{12}(y, \boldsymbol{x}) \oplus m_{15}(y, \boldsymbol{x}). \end{aligned}$$

Notemos que, por el comentario que sigue al teorema 1.2, tenemos que la función $f(y, \boldsymbol{x})$ tiene el número de minterms necesario para ser una función bent, sin embargo no lo es, como vemos a continuación.

Para $\boldsymbol{a} = (1,0,0) \in \mathbb{F}_2^3$ tenemos que

$$l_{\boldsymbol{a}}(\boldsymbol{x}) = m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}) \oplus m_7(\boldsymbol{x})$$

con lo que

$$f_0(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_4(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_7(\boldsymbol{x})$$

y

$$f_1(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_5(\boldsymbol{x}) \oplus m_6(\boldsymbol{x}).$$

Por tanto,

$$w(f_0 \oplus l_{\boldsymbol{a}}) = 4 \quad \text{y} \quad w(f_1 \oplus l_{\boldsymbol{a}}) = 4.$$

Así, por el teorema 4.1, $f(y, \boldsymbol{x})$ no puede ser una función bent. ■

A continuación, obtenemos una construcción explícita de las funciones $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ de n variables para que la función bent $f(y, \boldsymbol{x})$ de $n+1$ variables definida por la expresión (4.1) sea bent.

Con el objetivo de simplificar la notación y las distintas demostraciones introducimos la notación siguiente. Si $\boldsymbol{x} = (x_1, x_2, \ldots, x_{n-1}, x_n) \in \mathbb{F}_2^n$, denotamos por $\hat{\boldsymbol{x}}$ el vector de $\mathbb{F}_2^{n-1}$ formado por las $n-1$ primeras componentes de $\boldsymbol{x}$, es decir, $\hat{\boldsymbol{x}} = (x_1, x_2, \ldots, x_{n-1})$, con lo que $\boldsymbol{x} = (\hat{\boldsymbol{x}}, x_n)$.

Supongamos en primer lugar que $\hat{\boldsymbol{a}} = (a_1, a_2, \ldots, a_{n-1}) \in \mathbb{F}_2^{n-1}$ y consideremos

- el vector $\boldsymbol{a} = (\hat{\boldsymbol{a}}, 1) \in \mathbb{F}_2^n$,
- el conjunto

$$L_{\boldsymbol{a}} = \{\boldsymbol{x} \in \mathbb{F}_2^n \mid l_{\boldsymbol{a}}(\boldsymbol{x}) = 0\} = \big\{(\hat{\boldsymbol{x}}, x_n) \in \mathbb{F}_2^n \mid x_n = l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})\big\},$$

  que es un subespacio vectorial de $\mathbb{F}_2^n$ de dimensión $n-1$,
- la aplicación $\Phi_{\boldsymbol{a}} : \mathbb{F}_2^{n-1} \longrightarrow L_{\boldsymbol{a}}$ dada por

$$\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{x}}) = (\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) \tag{4.7}$$

  que, evidentemente, es un isomorfismo de espacios vectoriales,
- la aplicación $\bar{\Phi}_{\boldsymbol{a}} : \mathbb{F}_2^{n-1} \longrightarrow \mathbb{F}_2^n \setminus L_{\boldsymbol{a}}$ dada por

$$\bar{\Phi}_{\boldsymbol{a}}(\hat{\boldsymbol{x}}) = (\hat{\boldsymbol{x}}, 1 \oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) = \Phi_{\boldsymbol{a}}(\hat{\boldsymbol{x}}) \oplus (\hat{\boldsymbol{0}}, 1) \tag{4.8}$$

  que, claramente es biyectiva, aunque ahora no se trate de una aplicación lineal.

Ahora podemos establecer el resultado principal de este capítulo (véase el teorema 4.2 más adelante). Sin embargo, veamos primero un lema que facilitará la demostración de dicho teorema.

Lema 4.2: *Supongamos que $\hat{\boldsymbol{u}}, \hat{\boldsymbol{x}} \in \mathbb{F}_2^{n-1}$. Si $\Phi_{\boldsymbol{a}}$ y $\bar{\Phi}_{\boldsymbol{a}}$ son las aplicaciones definidas por las expresiones (4.7) y (4.8) respectivamente, entonces*

$$m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) = m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{x}}) = m_{\bar{\Phi}_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{x}}, 1 \oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})).$$

DEMOSTRACIÓN: De la expresión (4.7) y de la definición de minterm, tenemos que

$$\begin{aligned} & m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) = m_{(\hat{\boldsymbol{u}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{u}}))}(\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) \\ & = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_{n-1} \oplus x_{n-1})(1 \oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{u}}) \oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) \\ & = m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{x}})(1 \oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{u}}) \oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})). \end{aligned}$$

Ahora, si $\hat{\boldsymbol{x}} = \hat{\boldsymbol{u}}$, entonces $l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}}) = l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{u}})$ y $m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{x}}) = 1$ con lo que

$$m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) = 1.$$

En cambio, si $\hat{\boldsymbol{x}} \neq \hat{\boldsymbol{u}}$, entonces $m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{x}}) = 0$ y, por tanto,

$$m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) = 0.$$

En cualquier caso, $m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{x}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) = m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{x}})$.

La otra igualdad se obtiene a partir de la expresión (4.8) y de la definición de minterm mediante un razonamiento completamente análogo. □

El teorema siguiente, que es uno de los resultados principales de este capítulo, proporciona un método para construir las funciones booleanas $f_0(\boldsymbol{x})$ y $f_1(\boldsymbol{x})$ de forma explícita para que la función $f(y, \boldsymbol{x})$, definida por la expresión (4.1), sea bent.

Teorema 4.2: *Sean $b_0(\hat{\boldsymbol{x}})$ y $b_1(\hat{\boldsymbol{x}})$ dos funciones bent de $n-1$ variables y consideremos la función booleana de n variables*

$$f_0(\boldsymbol{x}) = \begin{cases} \displaystyle\bigoplus_{\hat{\boldsymbol{u}} \in \mathrm{Sop}(b_0)} m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in L_{\boldsymbol{a}} \\ \displaystyle\bigoplus_{\hat{\boldsymbol{v}} \in \mathrm{Sop}(b_1)} m_{\bar{\Phi}_{\boldsymbol{a}}(\hat{\boldsymbol{v}})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \mathbb{F}_2^n \setminus L_{\boldsymbol{a}} \end{cases} \tag{4.9}$$

con $\Phi_{\boldsymbol{a}}$ y $\bar{\Phi}_{\boldsymbol{a}}$ las aplicaciones definidas por las expresiones (4.7) y (4.8) respectivamente. Si

$$f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \quad o \quad f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus 1 \tag{4.10}$$

entonces la función $f(y, \boldsymbol{x})$ de $n+1$ variables definida por la expresión (4.1) es bent.

DEMOSTRACIÓN: Supongamos que $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$. Sustituyendo en la expresión (4.1) y teniendo en cuenta la expresión (1.1) y la defínción de minterm, obtenemos que

$$\begin{aligned} f(y, \boldsymbol{x}) &= m_0(y) f_0(\boldsymbol{x}) \oplus m_1(y) \left(f_0(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})\right) \\ &= \left(m_0(y) \oplus m_1(y)\right) f_0(\boldsymbol{x}) \oplus m_1(y) l_{\boldsymbol{a}}(\boldsymbol{x}) \\ &= f_0(\boldsymbol{x}) \oplus y l_{\boldsymbol{a}}(\boldsymbol{x}). \end{aligned} \tag{4.11}$$

Ahora, para que esta función sea bent debemos probar, de acuerdo con el teorema 1.2, que el número de 1 de la tabla de verdad de $f(y, \boldsymbol{x}) \oplus l_{(b,\boldsymbol{c})}(y, \boldsymbol{x})$ es $2^n \pm 2^{\frac{n-1}{2}}$ para todo $(b, \boldsymbol{c}) \in \mathbb{F}_2 \times \mathbb{F}_2^n$, con $\boldsymbol{c} = (\hat{\boldsymbol{c}}, c_n)$.

Supongamos que $\boldsymbol{x} = (\hat{\boldsymbol{x}}, x_n) \in \mathbb{F}_2^n$. Si $\boldsymbol{x} \in L_{\boldsymbol{a}}$, entonces $x_n = l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})$ y por el lema 4.2 y la expresión (4.9) tenemos que

$$\begin{aligned} f_0(\boldsymbol{x}) &= \bigoplus_{\hat{\boldsymbol{u}} \in \mathrm{Sop}(b_0)} m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\boldsymbol{x}) \\ &= \bigoplus_{\hat{\boldsymbol{u}} \in \mathrm{Sop}(b_0)} m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{x}}) \\ &= b_0(\hat{\boldsymbol{x}}), \end{aligned}$$

y ahora, de la expresión (4.11), tenemos que

$$\begin{aligned} f(y, \boldsymbol{x}) \oplus l_{(b,\boldsymbol{c})}(y, \boldsymbol{x}) &= b_0(\hat{\boldsymbol{x}}) \oplus y l_{\boldsymbol{a}}(\boldsymbol{x}) \oplus by \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \\ &= b_0(\hat{\boldsymbol{x}}) \oplus by \oplus l_{\hat{\boldsymbol{c}}}(\hat{\boldsymbol{x}}) \oplus c_n l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}}) \end{aligned}$$

ya que $l_{\boldsymbol{a}}(\boldsymbol{x}) = 0$ (pues $\boldsymbol{x} \in L_{\boldsymbol{a}}$).

Si $\mathbf{0}$ e $\mathbf{I}$ son las columnas de longitud 2^{n-1} con todos los elementos iguales a 0 y 1 respectivamente; $\hat{\boldsymbol{\tau}}$ es la matriz de tamaño $2^{n-1} \times (n-1)$ cuya i-ésima fila es $\hat{\boldsymbol{i}}$

					$l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})=0$	$l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})=1$
y	$\hat{\boldsymbol{x}}$	$b_0(\hat{\boldsymbol{x}})$	by	$l_{\hat{\boldsymbol{c}}}(\hat{\boldsymbol{x}})$	$f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$	$f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$
$\mathbf{0}$	$\hat{\boldsymbol{\tau}}$	$\hat{\boldsymbol{\xi}}_0$	$\mathbf{0}$	$\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}\oplus c_n\mathbf{I}$
$\mathbf{I}$	$\hat{\boldsymbol{\tau}}$	$\hat{\boldsymbol{\xi}}_0$	$b\mathbf{I}$	$\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}\oplus b\mathbf{I}$	$\hat{\boldsymbol{\xi}}_0\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}\oplus(b\oplus c_n)\mathbf{I}$

(a) $\boldsymbol{x}\in L_{\boldsymbol{a}}$

					$l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})=0$	$l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})=1$
y	$\hat{\boldsymbol{x}}$	$b_1(\hat{\boldsymbol{x}})$	$(1\oplus b)y$	$l_{\hat{\boldsymbol{c}}}(\hat{\boldsymbol{x}})$	$f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$	$f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$
$\mathbf{0}$	$\hat{\boldsymbol{\tau}}$	$\hat{\boldsymbol{\xi}}_1$	$\mathbf{0}$	$\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}\oplus c_n\mathbf{I}$	$\hat{\boldsymbol{\xi}}_1\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$
$\mathbf{I}$	$\hat{\boldsymbol{\tau}}$	$\hat{\boldsymbol{\xi}}_1$	$(1\oplus b)\mathbf{I}$	$\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}\oplus(1\oplus b\oplus c_n)\mathbf{I}$	$\hat{\boldsymbol{\xi}}_1\oplus\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}\oplus(1\oplus b)\mathbf{I}$

(b) $\boldsymbol{x}\in\mathbb{F}_2^n\setminus L_a$

Tabla 4.3: *Tabla de verdad de* $f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$

para $i=0,1,2,\ldots,2^{n-1}-1$; $\hat{\boldsymbol{\xi}}_j$ es la tabla de verdad de $b_j(\hat{\boldsymbol{x}})$, para $j=0,1$; $\boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$ es la tabla de verdad de la función lineal $l_{\hat{\boldsymbol{c}}}(\hat{\boldsymbol{x}})$; y $b\mathbf{I}$ es la columna de longitud 2^n con todos los elementos iguales a b; entonces las dos últimas columnas de la tabla 4.3(a) representan la tabla de verdad de la función $f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$ para $\boldsymbol{x}\in L_{\boldsymbol{a}}$ cuando $l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})=0$ y $l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})=1$, respectivamente.

En cambio, si $\boldsymbol{x}\in\mathbb{F}_2^n\setminus L_{\boldsymbol{a}}$, entonces $x_n=1\oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})$ y por el lema 4.2 y la expresión (4.9), tenemos que

$$\begin{aligned} f_0(\boldsymbol{x}) &= \bigoplus_{\hat{\boldsymbol{v}}\in\mathrm{Sop}(b_1)} m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{v}})}(\boldsymbol{x}) \\ &= \bigoplus_{\hat{\boldsymbol{v}}\in\mathrm{Sop}(b_1)} m_{\hat{\boldsymbol{v}}}(\hat{\boldsymbol{x}}) \\ &= b_1(\hat{\boldsymbol{x}}), \end{aligned}$$

y ahora, de la expresión (4.11), tenemos que

$$\begin{aligned} f(y,\boldsymbol{x})\oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x}) &= b_1(\hat{\boldsymbol{x}})\oplus y l_{\boldsymbol{a}}(\boldsymbol{x})\oplus by\oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \\ &= b_1(\hat{\boldsymbol{x}})\oplus(1\oplus b)y\oplus l_{\hat{\boldsymbol{c}}}(\hat{\boldsymbol{x}})\oplus c_n(1\oplus l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}})) \end{aligned}$$

$f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$	
$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus c_n\mathbf{I}$
$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus b\mathbf{I}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus (b \oplus c_n)\mathbf{I}$
$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus c_n\mathbf{I}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$
$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus (1 \oplus b \oplus c_n)\mathbf{I}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus (1 \oplus b)\mathbf{I}$

Tabla 4.4: *Tabla de verdad de* $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$.

ya que $l_{\boldsymbol{a}}(\boldsymbol{x}) = 1$ (pues $\boldsymbol{x} \in \mathbb{F}_2^n \setminus L_{\boldsymbol{a}}$).

Ahora, procediendo como en el caso anterior, las dos últimas columnas de la tabla 4.3(b) representan la tabla de verdad de la función $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$ para $\boldsymbol{x} \in \mathbb{F}_2^n \setminus L_{\boldsymbol{a}}$ cuando $l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}}) = 0$ y $l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}}) = 1$, respectivamente.

En consecuencia, los cuatro bloques que constituyen la tabla de verdad de la función $f(y,\boldsymbol{x}) \oplus l_{(b,\boldsymbol{c})}(y,\boldsymbol{x})$ son los bloques de la primera o de la segunda columna de la tabla 4.4.

Ahora, la tabla 4.5(a) representa los cuatro bloques de la primera columna de la tabla 4.4 según los distintos valores de b y c_n, mientras que la tabla 4.5(b) representa los cuatro bloques de la segunda columna de la tabla 4.4, también según los distintos valores de b y c_n.

Puesto que $b_j(\hat{\boldsymbol{x}})$, para $j = 0, 1$, es una función bent de $n-1$ variables, por el teorema 1.2, tenemos que

$$w(b_j \oplus l_{\hat{\boldsymbol{c}}}) = 2^{n-2} \pm 2^{\frac{n-3}{2}}.$$

Por tanto, en la primera columna de la tabla 4.5(a) hay tres bloques cuyo número de 1 es $2^{n-2} + 2^{\frac{n-3}{2}}$ y un bloque cuyo número de 1 es $2^{n-2} - 2^{\frac{n-3}{2}}$, o bien un bloque cuyo número de 1 es $2^{n-2} + 2^{\frac{n-3}{2}}$ y tres bloques cuyo número de 1 es $2^{n-2} - 2^{\frac{n-3}{2}}$. En cualquier caso, podemos afirmar que el número de 1 de dicha columna es $2^n \pm 2^{\frac{n-1}{2}}$.

Lo mismo ocurre con cada una de las restantes columnas de la tabla 4.5(a) y con todas las columnas de la tabla 4.5(b).

En consecuencia, $f(y,\boldsymbol{x})$ es una función bent de $n+1$ variables. □

El ejemplo siguiente nos muestra cómo podemos construir funciones bent a partir

b c_n	b c_n	b c_n	b c_n
0 0	0 1	1 0	1 1
$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$
$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$
$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$
$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$

(a) Bloques de la primera columna de la tabla 4.4

b c_n	b c_n	b c_n	b c_n
0 0	0 1	1 0	1 1
$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$
$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_0 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$
$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$
$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}} \oplus \mathbf{I}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$	$\hat{\boldsymbol{\xi}}_1 \oplus \boldsymbol{\Lambda}_{\hat{\boldsymbol{c}}}$

(b) Bloques de la segunda columna de la tabla 4.4

Tabla 4.5: *Bloques de las columnas de la tabla 4.4 según los distintos valores de b y c_n.*

del teorema 4.2.

Ejemplo 4.2: Supongamos que $n = 3$ y consideremos el vector $\boldsymbol{a} = \mathbf{1} = (0, 0, 1)$. Entonces

$$\begin{aligned} L_{\mathbf{1}} &= \{(x_1, x_2, x_3) \in \mathbb{F}_2^3 \mid x_3 = 0\} \\ &= \{(0,0,0), (0,1,0), (1,0,0), (1,1,0)\} = \{\mathbf{0}, \mathbf{2}, \mathbf{4}, \mathbf{6}\} \end{aligned}$$

y

$$\mathbb{F}_2^3 \setminus L_{\mathbf{1}} = \{(0,0,1), (0,1,1), (1,0,1), (1,1,1)\} = \{\mathbf{1}, \mathbf{3}, \mathbf{5}, \mathbf{7}\}.$$

Además

$$\Phi_{\mathbf{1}} : \mathbb{F}_2^2 \longrightarrow L_{\mathbf{1}} \qquad \text{y} \qquad \bar{\Phi}_{\mathbf{1}} : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^3 \setminus L_{\mathbf{1}}$$

satisfacen

$$\Phi_{\mathbf{1}}(x_1, x_2) = (x_1, x_2, 0) \quad \text{y} \quad \bar{\Phi}_{\mathbf{1}}(x_1, x_2) = (x_1, x_2, 1).$$

Supongamos que

$$\mathrm{Sop}\,(b_0) = \{\mathbf{2}\} = \{(1,0)\} \quad \text{y} \quad \mathrm{Sop}\,(b_1) = \{\mathbf{3}\} = \{(1,1)\},$$

entonces, de acuerdo con la expresión (4.9), tenemos que

$$f_0(\boldsymbol{x}) = \begin{cases} m_{\Phi_{\mathbf{1}}(\mathbf{2})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in L_{\mathbf{1}}, \\ m_{\bar{\Phi}_{\mathbf{1}}(\mathbf{3})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \mathbb{F}_2^3 \setminus L_{\mathbf{1}}, \end{cases}$$

$$= \begin{cases} m_{\mathbf{4}}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \{\mathbf{0}, \mathbf{2}, \mathbf{4}, \mathbf{6}\}, \\ m_{\mathbf{7}}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \{\mathbf{1}, \mathbf{3}, \mathbf{5}, \mathbf{7}\}, \end{cases}$$

ya que

$$\Phi_{\mathbf{1}}(\mathbf{2}) = \Phi_{\mathbf{1}}(1,0) = (1,0,0) = \mathbf{4},$$
$$\bar{\Phi}_{\mathbf{1}}(\mathbf{3}) = \bar{\Phi}_{\mathbf{1}}(1,1) = (1,1,1) = \mathbf{7},$$

por tanto,

$$\mathrm{Sop}\,(f_0) = \{\mathbf{4}, \mathbf{7}\}.$$

Ahora, si tomamos $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\mathbf{1}}(\boldsymbol{x})$, como $\mathrm{Sop}\,(l_{\mathbf{1}}) = \mathbb{F}_2^3 \setminus L_{\mathbf{1}}$, tenemos que

$$\mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(l_{\mathbf{1}}) = \{\mathbf{4}, \mathbf{7}\}\Delta\{\mathbf{1}, \mathbf{3}, \mathbf{5}, \mathbf{7}\} = \{\mathbf{1}, \mathbf{3}, \mathbf{4}, \mathbf{5}\},$$

por la expresión (4.3,)

$$\mathrm{Sop}\,(f) = \{(0,\mathbf{4}), (0,\mathbf{7}), (1,\mathbf{1}), (1,\mathbf{3})(1,\mathbf{4}), (1,\mathbf{5})\} = \{\mathbf{4}, \mathbf{7}, \mathbf{9}, \mathbf{11}, \mathbf{12}, \mathbf{13}\},$$

con lo que

$$f(y, \boldsymbol{x}) = m_4(y, \boldsymbol{x}) \oplus m_7(y, \boldsymbol{x}) \oplus m_9(y, \boldsymbol{x}) \oplus m_{11}(y, \boldsymbol{x}) \oplus m_{12}(y, \boldsymbol{x}) \oplus m_{13}(y, \boldsymbol{x}).$$

En cambio, si tomamos $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\mathbf{1}}(\boldsymbol{x}) \oplus 1$, como $\mathrm{Sop}\,(1 \oplus l_{\mathbf{1}}) = L_{\mathbf{1}}$, tenemos que

$$\mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(l_{\mathbf{1}} \oplus 1) = \{\mathbf{4}, \mathbf{7}\}\Delta\{\mathbf{0}, \mathbf{2}, \mathbf{4}, \mathbf{6}\} = \{\mathbf{0}, \mathbf{2}, \mathbf{6}, \mathbf{7}\}$$

y, por la expresión (4.3),

$$\mathrm{Sop}\,(f) = \{(0,\mathbf{4}),(0,\mathbf{7}),(1,\mathbf{0}),(1,\mathbf{2}),(1,\mathbf{6}),(1,\mathbf{7})\} = \{\mathbf{4},\mathbf{7},\mathbf{8},\mathbf{10},\mathbf{14},\mathbf{15}\},$$

con lo que

$$f(y,\boldsymbol{x}) = m_4(y,\boldsymbol{x}) \oplus m_7(y,\boldsymbol{x}) \oplus m_8(y,\boldsymbol{x}) \oplus m_{10}(y,\boldsymbol{x}) \oplus m_{14}(y,\boldsymbol{x}) \oplus m_{15}(y,\boldsymbol{x}). \blacksquare$$

Seguidamente, introducimos los resultados que nos permitirán contabilizar el número de funciones bent distintas que podemos construir de acuerdo con el teorema 4.2.

Teorema 4.3: *Supongamos que $\boldsymbol{a} = (\hat{\boldsymbol{a}},1) \in \mathbb{F}_2^n$ y que $f_0(\boldsymbol{x})$ y $f_0'(\boldsymbol{x})$ son las funciones de la expresión (4.9) definidas por los pares de funciones bent de $n-1$ variables $(b_0(\hat{\boldsymbol{x}}),b_1(\hat{\boldsymbol{x}}))$ y $(b_0'(\hat{\boldsymbol{x}}),b_1'(\hat{\boldsymbol{x}}))$, respectivamente. Supongamos que $f_1(\boldsymbol{x})$ y $f_1'(\boldsymbol{x})$ son las funciones de la expresión (4.10) definidas a partir de las funciones $f_0(\boldsymbol{x})$ y $f_0'(\boldsymbol{x})$, respectivamente. Finalmente, supongamos que $f(y,\boldsymbol{x})$ y $f'(y,\boldsymbol{x})$ son las funciones construidas de acuerdo con el teorema 4.2 a partir de los pares de funciones $(f_0(\boldsymbol{x}),f_1(\boldsymbol{x}))$ y $(f_0'(\boldsymbol{x}),f_1'(\boldsymbol{x}))$, respectivamente. Si $(b_0(\hat{\boldsymbol{x}}),b_1(\hat{\boldsymbol{x}})) \neq (b_0'(\hat{\boldsymbol{x}}),b_1'(\hat{\boldsymbol{x}}))$, entonces $f(y,\boldsymbol{x}) \neq f'(y,\boldsymbol{x})$.*

Demostración: Por la expresión (4.3), tenemos que

$$\mathrm{Sop}\,(f) = \{(0,\boldsymbol{b}) \mid \boldsymbol{b} \in \mathrm{Sop}\,(f_0)\} \cup \{(1,\boldsymbol{b}) \mid \boldsymbol{b} \in \mathrm{Sop}\,(f_1)\}$$

y

$$\mathrm{Sop}\,(f') = \{(0,\boldsymbol{b'}) \mid \boldsymbol{b'} \in \mathrm{Sop}\,(f_0')\} \cup \{(1,\boldsymbol{b'} \mid \boldsymbol{b'} \in \mathrm{Sop}\,(f_1')\}.$$

Supongamos que $f(y,\boldsymbol{x}) = f'(y,\boldsymbol{x})$. Entonces $\mathrm{Sop}\,(f) = \mathrm{Sop}\,(f')$ y, de las expresiones anteriores, necesariamente

$$\mathrm{Sop}\,(f_0) = \mathrm{Sop}\,(f_0') \qquad \text{y} \qquad \mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_1')\,. \tag{4.12}$$

Supongamos que $\hat{\boldsymbol{e}} \in \mathrm{Sop}\,(b_0) \subseteq \mathbb{F}_2^{n-1}$; entonces $\boldsymbol{e} = (\hat{\boldsymbol{e}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{e}})) \in L_{\boldsymbol{a}}$. Ahora, por el lema 4.2, tenemos que

$$m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\hat{\boldsymbol{e}}, l_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{e}}) = m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{e}}) = \begin{cases} 1, & \text{si } \hat{\boldsymbol{u}} = \hat{\boldsymbol{e}} \\ 0, & \text{si } \hat{\boldsymbol{u}} \neq \hat{\boldsymbol{e}}, \end{cases}$$

y por la expresión (4.9), tenemos que

$$\begin{aligned} f_0(\boldsymbol{e}) &= \bigoplus_{\hat{\boldsymbol{u}}\in \mathrm{Sop}(b_0)} m_{\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{u}})}(\boldsymbol{e}) \\ &= \bigoplus_{\hat{\boldsymbol{u}}\in \mathrm{Sop}(b_0)} m_{\hat{\boldsymbol{u}}}(\hat{\boldsymbol{e}}) \\ &= 1 \end{aligned}$$

con lo que $\boldsymbol{e} \in \mathrm{Sop}\,(f_0)$ y, de la expresión (4.12), $f_0'(\boldsymbol{e}) = 1$. De nuevo, por el lema 4.2 y la expresión (4.9), tenemos que $\hat{\boldsymbol{e}} \in \mathrm{Sop}\,(b_0')$. Por tanto,

$$\mathrm{Sop}\,(b_0) \subseteq \mathrm{Sop}\,(b_0')\,.$$

Mediante un razonamiento análogo obtenemos que $\mathrm{Sop}\,(b_0') \subseteq \mathrm{Sop}\,(b_0)$.

En consecuencia, $\mathrm{Sop}\,(b_0) = \mathrm{Sop}\,(b_0')$.

Ahora, procediendo como en el caso anterior, obtenemos también que

$$\mathrm{Sop}\,(b_1) = \mathrm{Sop}\,(b_1')\,.$$

Por tanto, $(b_0(\hat{\boldsymbol{x}}), b_1(\hat{\boldsymbol{x}})) = (b_0'(\hat{\boldsymbol{x}}), b_1'(\hat{\boldsymbol{x}}))$, que es una contradicción. En consecuencia, $f(y, \boldsymbol{x}) \neq f'(y, \boldsymbol{x})$. □

¿Qué ocurre si en los teoremas 4.2 y 4.3 consideramos un vector $\boldsymbol{a}$ cuya última componente es 0? El ejemplo siguiente nos ayudará a entender los cambios que debemos hacer para que dichos teoremas continúen siendo válidos.

Ejemplo 4.3: Supongamos, como en el ejemplo 4.2, que $n = 3$ y consideremos el vector $\boldsymbol{a} = \mathbf{2} = (0, 1, 0)$. Entonces

$$\begin{aligned} L_{\mathbf{2}} &= \{(x_1, x_2, x_3) \in \mathbb{F}_2^3 \mid x_2 = 0\} \\ &= \{(0,0,0), (0,0,1), (1,0,0), (1,0,1)\} = \{\mathbf{0}, \mathbf{1}, \mathbf{4}, \mathbf{5}\} \end{aligned}$$

y

$$\mathbb{F}_2^3 \setminus L_{\mathbf{2}} = \{(0,1,0), (0,1,1), (1,1,0), (1,1,1)\} = \{\mathbf{2}, \mathbf{3}, \mathbf{6}, \mathbf{7}\}.$$

Consideremos ahora las aplicaciones

$$\Phi_{\mathbf{2}} : \mathbb{F}_2^2 \longrightarrow L_{\mathbf{2}} \qquad \text{y} \qquad \bar{\Phi}_{\mathbf{2}} : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^3 \setminus L_{\mathbf{2}}$$

tales que

$$\Phi_{\mathbf{2}}(x_1, x_2) = (x_1, 0, x_2) \quad \text{y} \quad \bar{\Phi}_{\mathbf{2}}(x_1, x_2) = (x_1, 1, x_2).$$

Si suponemos, como en el ejemplo 4.2, que

$$\mathrm{Sop}\,(b_0) = \{\mathbf{2}\} = \{(1,0)\} \quad \text{y} \quad \mathrm{Sop}\,(b_1) = \{\mathbf{3}\} = \{(1,1)\},$$

entonces, de acuerdo con la expresión (4.9), tenemos que

$$f_0(\boldsymbol{x}) = \begin{cases} m_{\Phi_{\mathbf{2}}(\mathbf{2})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in L_{\mathbf{2}}, \\ m_{\bar{\Phi}_{\mathbf{2}}(\mathbf{3})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \mathbb{F}_2^3 \setminus L_{\mathbf{2}}, \end{cases}$$

$$= \begin{cases} m_{\mathbf{4}}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \{\mathbf{0}, \mathbf{1}, \mathbf{4}, \mathbf{5}\}, \\ m_{\mathbf{7}}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \{\mathbf{2}, \mathbf{3}, \mathbf{6}, \mathbf{7}\}, \end{cases}$$

ya que

$$\Phi_{\mathbf{2}}(\mathbf{2}) = \Phi_{\mathbf{2}}(1,0) = (1,0,0) = \mathbf{4},$$
$$\bar{\Phi}_{\mathbf{2}}(\mathbf{3}) = \bar{\Phi}_{\mathbf{2}}(1,1) = (1,1,1) = \mathbf{7},$$

por tanto,

$$\mathrm{Sop}\,(f_0) = \{\mathbf{4}, \mathbf{7}\}.$$

Ahora, si tomamos $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\mathbf{2}}(\boldsymbol{x})$, como $\mathrm{Sop}\,(l_{\mathbf{2}}) = \mathbb{F}_2^3 \setminus L_{\mathbf{2}}$, tenemos que

$$\mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(l_{\mathbf{2}}) = \{\mathbf{4}, \mathbf{7}\}\Delta\{\mathbf{2}, \mathbf{3}, \mathbf{6}, \mathbf{7}\} = \{\mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{6}\}$$

y, por la expresión (4.3),

$$\mathrm{Sop}\,(f) = \{(0,\mathbf{4}), (0,\mathbf{7}), (1,\mathbf{2}), (1,\mathbf{3}), (1,\mathbf{4}), (1,\mathbf{6})\} = \{\mathbf{4}, \mathbf{7}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{14}\},$$

por tanto,

$$f(y, \boldsymbol{x}) = m_4(y, \boldsymbol{x}) \oplus m_7(y, \boldsymbol{x}) \oplus m_{10}(y, \boldsymbol{x}) \oplus m_{11}(y, \boldsymbol{x}) \oplus m_{12}(y, \boldsymbol{x}) \oplus m_{14}(y, \boldsymbol{x}).$$

En cambio, si tomamos $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\mathbf{2}}(\boldsymbol{x}) \oplus 1$, como $\mathrm{Sop}\,(1 \oplus l_{\mathbf{2}}) = L_{\mathbf{2}}$, tenemos que

$$\mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(l_{\mathbf{2}} \oplus 1) = \{\mathbf{4}, \mathbf{7}\}\Delta\{\mathbf{0}, \mathbf{1}, \mathbf{4}, \mathbf{5}\} = \{\mathbf{0}, \mathbf{1}, \mathbf{5}, \mathbf{7}\}$$

y, por la expresión (4.3),

$$\mathrm{Sop}\,(f) = \{(0,\mathbf{4}),(0,\mathbf{7}),(1,\mathbf{0}),(1,\mathbf{1}),(1,\mathbf{5}),(1,\mathbf{7})\} = \{\mathbf{4},\mathbf{7},\mathbf{8},\mathbf{9},\mathbf{13},\mathbf{15}\}.$$

Por tanto

$$f(y,\boldsymbol{x}) = m_4(y,\boldsymbol{x}) \oplus m_7(y,\boldsymbol{x}) \oplus m_8(y,\boldsymbol{x}) \oplus m_9(y,\boldsymbol{x}) \oplus m_{13}(y,\boldsymbol{x}) \oplus m_{15}(y,\boldsymbol{x}). \blacksquare$$

Así pues, tal y como se desprende del ejemplo anterior, si $\boldsymbol{a} = (\tilde{\boldsymbol{a}}, 0) \in \mathbb{F}_2^n$ con $\tilde{\boldsymbol{a}} \neq \mathbf{0}$, entonces $\pi(\boldsymbol{a}) = (\hat{\boldsymbol{a}}, 1)$ para alguna permutación π del conjunto $\{1, 2, \ldots, n\}$. Por tanto, si aplicamos los teoremas 4.2 y 4.3 con $\pi(\boldsymbol{a})$ y $\pi(\boldsymbol{x})$, podemos afirmar que dichos teoremas siguen siendo válidos para cualquier $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ y, como consecuencia inmediata del teorema 4.3, tenemos el resultado siguiente.

Corolario 4.3: *Si ν_{n-1} es el número de funciones bent de $n-1$ variables, entonces el número de funciones bent de $n+1$ variables que podemos construir de acuerdo con el teorema 4.2 es*

$$2(2^n - 1)\nu_{n-1}^2.$$

DEMOSTRACIÓN: Podemos elegir el par (b_0, b_1) de ν_{n-1}^2 formas distintas y el vector $\boldsymbol{a}$ de $2^n - 1$ formas distintas. Ahora, de acuerdo con la expresión (4.10), podemos elegir $f_1(\boldsymbol{x})$ de 2 formas distintas. En consecuencia, el número de funciones bent de $n+1$ variables que podemos construir de acuerdo con el teorema 4.2 es

$$2(2^n - 1)\nu_{n-1}^2. \qquad \square$$

Así, como $\nu_2 = 8$, el teorema 4.2 proporciona $2(2^3 - 1)8^2 = 896$ funciones bent de 4 variables y como $\nu_4 = 896$, tenemos que con este método obtenemos todas las funciones bent de 4 variables. En cambio, el número de funciones bent de 6 y 8 variables que podemos construir utilizando el teorema 4.2 es

$$2(2^5 - 1)\nu_4^2 = 49\,774\,592 \quad \text{y} \quad 2(2^7 - 1)\nu_6^2 \approx 2^{73}$$

que está bastante lejos de $\nu_6 = 5\,425\,430\,528$ y $\nu_8 \approx 2^{106}$.

En la construcción introducida en el teorema 4.2 hemos considerado, para cada $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, un par de aplicaciones concretas $\Phi_{\boldsymbol{a}}$ y $\bar{\Phi}_{\boldsymbol{a}}$. Ahora bien, si tenemos en

cuenta el comentario que precede al corolario 4.3 y consideramos un isomorfismo de espacios vectoriales $\phi_i : \mathbb{F}_2^{n-1} \longrightarrow \mathbb{F}_2^{n-1}$, para $i = 0, 1$, y definimos

$$\Phi_{\boldsymbol{a}} : \mathbb{F}_2^{n-1} \longrightarrow L_{\boldsymbol{a}} \qquad \text{y} \qquad \bar{\Phi}_{\boldsymbol{a}} : \mathbb{F}_2^{n-1} \longrightarrow \mathbb{F}_2^n \setminus L_{\boldsymbol{a}}$$

como

$$\Phi_{\boldsymbol{a}}(\hat{\boldsymbol{x}}) = (\phi_0(\hat{\boldsymbol{x}}), l_{\hat{\boldsymbol{a}}}(\phi_0(\hat{\boldsymbol{x}}))) \quad \text{y} \quad \bar{\Phi}_{\boldsymbol{a}}(\hat{\boldsymbol{x}}) = (\phi_1(\hat{\boldsymbol{x}}), l_{\hat{\boldsymbol{a}}}(\phi_1(\hat{\boldsymbol{x}})) \oplus 1)$$

respectivamente, entonces podemos afirmar que los teoremas 4.2 y 4.3 siguen siendo válidos para todo $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$. Sin embargo, no podemos asegurar que las funciones bent sean todas distintas como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 4.4: Supongamos, como en el ejemplo 4.2, que $n = 3$ y que $\boldsymbol{a} = \mathbf{1} = (0, 0, 1)$. Consideremos los isomorfismos de espacios vectoriales $\phi_i : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$, para $i = 0, 1$, dados por

$$\phi_{\mathbf{0}}(x_1, x_2) = (x_1 \oplus x_2, x_1) \quad \text{y} \quad \bar{\phi}_{\mathbf{1}}(x_1, x_2) = (x_1, x_1 \oplus x_2).$$

y consideramos ahora las aplicaciones

$$\Phi_{\mathbf{1}} : \mathbb{F}_2^2 \longrightarrow L_{\mathbf{1}} \qquad \text{y} \qquad \bar{\Phi}_{\mathbf{1}} : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^3 \setminus L_{\mathbf{1}}$$

dadas por

$$\Phi_{\mathbf{1}}(x_1, x_2) = (\phi_0(x_1, x_2), l_{\hat{\mathbf{1}}}(\phi_0(x_1, x_2))) = (x_1 \oplus x_2, x_1, 0),$$
$$\bar{\Phi}_{\mathbf{1}}(x_1, x_2) = (\phi_1(x_1, x_2), l_{\hat{\mathbf{1}}}(\phi_1(x_1, x_2)) \oplus 1) = (x_1, x_1 \oplus x_2, 1),$$

ya que

$$l_{\hat{\mathbf{1}}}(\phi_0(x_1, x_2)) = l_{(0,0)}(x_1 \oplus x_2, x_1) = 0$$

y

$$l_{\hat{\mathbf{1}}}(\phi_1(x_1, x_2)) = l_{(0,0)}(x_1, x_1 \oplus x_2) = 0.$$

Supongamos también que

$$\text{Sop}(b_0) = \{\mathbf{1}\} = \{(0, 1)\} \quad \text{y} \quad \text{Sop}(b_1) = \{\mathbf{2}\} = \{(1, 0)\},$$

entonces, de acuerdo con la expresión (4.9), tenemos que

$$f_0(\boldsymbol{x}) = \begin{cases} m_{\Phi_{\mathbf{1}}(\mathbf{1})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in L_{\mathbf{1}}, \\ m_{\bar{\Phi}_{\mathbf{1}}(\mathbf{2})}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \mathbb{F}_2^3 \setminus L_{\mathbf{1}}, \end{cases}$$

$$= \begin{cases} m_{\mathbf{4}}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \{\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6}\}, \\ m_{\mathbf{7}}(\boldsymbol{x}), & \text{si } \boldsymbol{x} \in \{\mathbf{1},\mathbf{3},\mathbf{5},\mathbf{7}\}, \end{cases}$$

ya que

$$\Phi_{\mathbf{1}}(\mathbf{1}) = \Phi_{\mathbf{1}}(0,1) = (1,0,0) = \mathbf{4},$$

$$\bar{\Phi}_{\mathbf{1}}(\mathbf{2}) = \bar{\Phi}_{\mathbf{1}}(1,0) = (1,1,1) = \mathbf{7},$$

por tanto,

$$\mathrm{Sop}\,(f_0) = \{\mathbf{4},\mathbf{7}\}.$$

Ahora, si tomamos $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\mathbf{1}}(\boldsymbol{x})$, como $\mathrm{Sop}\,(l_{\mathbf{1}}) = \mathbb{F}_2^3 \setminus L_{\mathbf{1}}$, tenemos que

$$\mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(l_{\mathbf{1}}) = \{\mathbf{4},\mathbf{7}\}\Delta\{\mathbf{1},\mathbf{3},\mathbf{5},\mathbf{7}\} = \{\mathbf{1},\mathbf{3},\mathbf{4},\mathbf{5}\}$$

y, por la expresión (4.3),

$$\mathrm{Sop}\,(f) = \{(0,\mathbf{4}),(0,\mathbf{7}),(1,\mathbf{1}),(1,\mathbf{3}),(1,\mathbf{4}),(1,\mathbf{5})\} = \{\mathbf{4},\mathbf{7},\mathbf{9},\mathbf{11},\mathbf{12},\mathbf{13}\},$$

por tanto,

$$f(y,\boldsymbol{x}) = m_4(y,\boldsymbol{x}) \oplus m_7(y,\boldsymbol{x}) \oplus m_9(y,\boldsymbol{x}) \oplus m_{11}(y,\boldsymbol{x}) \oplus m_{12}(y,\boldsymbol{x}) \oplus m_{13}(y,\boldsymbol{x}).$$

En cambio, si tomamos $f_1(\boldsymbol{x}) = f_0(\boldsymbol{x}) \oplus l_{\mathbf{1}}(\boldsymbol{x}) \oplus 1$, como $\mathrm{Sop}\,(l_{\mathbf{1}} \oplus 1) = L_{\mathbf{1}}\}$, tenemos que

$$\mathrm{Sop}\,(f_1) = \mathrm{Sop}\,(f_0)\,\Delta\,\mathrm{Sop}\,(l_{\mathbf{1}} \oplus 1) = \{\mathbf{4},\mathbf{7}\}\Delta\{\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6}\} = \{\mathbf{0},\mathbf{2},\mathbf{6},\mathbf{7}\}$$

y, por la expresión (4.3),

$$\mathrm{Sop}\,(f) = \{(0,\mathbf{4}),(0,\mathbf{7}),(1,\mathbf{0}),(1,\mathbf{2}),(1,\mathbf{6}),(1,\mathbf{7})\} = \{\mathbf{4},\mathbf{7},\mathbf{8},\mathbf{10},\mathbf{14},\mathbf{15}\}.$$

Por tanto,

$$f(y,\boldsymbol{x}) = m_4(y,\boldsymbol{x}) \oplus m_7(y,\boldsymbol{x}) \oplus m_8(y,\boldsymbol{x}) \oplus m_{10}(y,\boldsymbol{x}) \oplus m_{14}(y,\boldsymbol{x}) \oplus m_{15}(y,\boldsymbol{x}).$$

Notemos que hemos obtenido la misma función bent $f(y,\boldsymbol{x})$ que en el ejemplo 4.2. ■

Los ejemplos 4.2 y 4.4 ponen de manifiesto, en el caso $n = 3$, que las funciones bent construidas a partir del teorema 4.2 utilizando un vector $\boldsymbol{a} \neq \mathbf{0}$ y el par de aplicaciones $(\Phi_{\boldsymbol{a}}, \bar{\Phi}_{\boldsymbol{a}})$ puede coincidir con la función bent construida utilizando otro vector $\boldsymbol{b} \neq \mathbf{0}$ y otro par de aplicaciones $(\Psi_{\boldsymbol{b}}, \bar{\Psi}_{\boldsymbol{b}})$. Esto es así porque para $n = 3$ el conjunto $\{(\Phi_{\boldsymbol{a}}, \bar{\Phi}_{\boldsymbol{a}}) \mid \boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}\}$ determina todas las funciones bent de 4 variables. Sin embargo, para $n = 5$ no estamos en condiciones de afirmar o negar dicha propiedad ya que, en este caso, el conjunto anterior no determina todas las funciones bent de 6 variables.

4.2 Comparación con otros métodos

Tal como hemos dicho en la sección anterior, la construcción de funciones bent introducida en este capítulo, permite obtener todas las funciones bent de 4 variables. Sin embargo, tal como hemos visto en los capítulos 2 y 3 ninguna de las construcciones A, B, C, D y E permite obtener todas las funciones bent de 4 variables; tampoco todas juntas. Por tanto, podemos afirmar que para $n = 4$ la construcción introducida en el teorema 4.2 es distinta de las construcciones introducidas en los capítulos anteriores, incluso distintas de las construcciones clásicas de Rothaus, Maiorana-McFarland y Carlet. De hecho, podemos afirmar que para $n = 4$ todas estas construcciones constituyen casos particulares de esta nueva construcción.

Sin embargo, no estamos en condiciones de afirmar lo mismo para $n = 6$, ya que tal como hemos visto también en la sección anterior, no obtenemos todas las funciones bent de 6 variables. Esto se debe a la imposibilidad de determinar de forma explícita todas las funciones bent de 6 variables obtenidas mediante las distintas construcciones consideradas y comprobar si hay coincidencias entre ellas.

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). 2

[3] C. M. Adams y S. E. Tavares. Generating bent sequences. *Discrete Applied Mathematics*, **39**: 155–159 (1992). 2

[4] 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). 2

[5] 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 2003*, volumen 2898 de *Lecture Notes in Computer Science*, páginas 82–92. Springer-Verlag, Berlin, 2003. 4

[6] A. Braeken, Y. Borissov, S. Nikova y B. Preneel. Classification of Boolean functions of 6 variables or less with respect to some cryptographic properties. En L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi y M. Yung (editores), *Automata, Languages and Programming*, volumen 3580 de *Lecture Notes in Computer Science*, páginas 324–334. Springer-Verlag, Berlin, 2005. 15

[7] 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

[8] A. Canteaut y P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, **49(8)**: 2004–2019 (2003). 2

[9] A. Canteaut, M. Daum, H. Dobbertin y G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, **154**: 202–218 (2006). 34

[10] C. Carlet y Y. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, **25**: 263–279 (2002). 1

[11] C. Carlet. On the secondary constructions of resilient and bent functions. *Progress in Computer Science and Applied Logic*, **23**: 3–28 (2004). 17

[12] 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. 2

[13] C. Carlet, H. Dobbertin y G. Leander. Normal extensions of bent functions. *IEEE Transactions on Information Theory*, **50(11)**: 2880–2885 (2004). 4

[14] C. Carlet y P. Guillot. A characterization of binary bent functions. *Journal of Combinatorial Theory (Series A)*, **76**: 328–335 (1996). 3

[15] C. Carlet y P. Guillot. An alternate characterization of the bentness of binary functions, with uniqueness. *Designs, Codes and Cryptography*, **14**: 133–140 (1998). 2

[16] D. K. Chang. Binary bent sequences of order 64. *Utilitas Mathematica*, **52**: 141–151 (1997). 2, 5

[17] 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. 3

[18] C. Charnes, M. Rötteler y T. Beth. Homogeneous bent functions, invariants, and designs. *Designs, Codes and Cryptography*, **26**: 139–154 (2002). 1

[19] 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). 2

[20] J. H. Cheon, S. Chee y C. Park. S-boxes with controllable nonlinearity. En J. Stern (editor), *EUROCRYPT'99*, volumen 1592 de *Lecture Notes in Computer Science*, páginas 286–294. Springer-Verlag, Berlin, 1999. 4

[21] J.-J. Climent, F. J. García y V. Requena. A new iterative method to construct bent functions. En *Proceedings of the 5th International Conference on Information Security and Privacy*, páginas 19–22. WSEAS, WSEAS Press, 2006. xvi

[22] J.-J. Climent, F. J. García y V. Requena. On the iterative construction of bent functions. En *Proceedings of the 5th International Conference on Information Security and Privacy*, páginas 15–18. WSEAS, WSEAS Press, 2006. xvi

[23] J.-J. Climent, F. J. García y V. Requena. A characterization of bent functions of $n+1$ variables. En M. Katehakis, A. Zamora y R. Álvarez (editores), *Proceedings of the 6th International Conference on Information Security and Privacy*, páginas 44–47. WSEAS, WSEAS Press, 2007. xvi

[24] 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. xvi

[25] J.-J. Climent, F. J. García y V. Requena. An iterative method to construct new bent funcions from old bent functions. *Transactions on Information Science and Applications*, **4(2)**: 245–250 (2007). xvi

[26] J.-J. Climent, F. J. García y V. Requena. Iterative methods to construct boolean bent funcions. *Transactions on Information Science and Applications*, **4(2)**: 251–256 (2007). xvi

[27] 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. xvi

[28] 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 varia-

bles. 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. xvi

[29] 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. xvi

[30] 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. xvi

[31] 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). xvi

[32] 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. xvi

[33] 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. xvi

[34] 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. xvi

[35] 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. xvi

[36] 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. Submitted. xvi

[37] J.-J. Climent, F. J. García y V. Requena. On the characterizarion and construction of bent functions of $n+1$ variables from Boolean functions of n variables. Submitted. xvi

[38] 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. xvi

[39] 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. 34

[40] J. F. Dillon. *Elementary Hadamard Difference Sets*. Tesis Doctoral, University of Maryland, 1974. 2, 16

[41] 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. 4

[42] H. Dobbertin. Almost perfect nonlinear power functions on $gf(2^n)$: The Welch case. *IEEE Transactions on Information Theory*, **45(4)**: 1271–1275 (1999). 3

[43] 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). 2

[44] 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. 2

[45] K. C. Gupta y P. Sarkar. Improved construction of nonlinear resilient S-boxes. *IEEE Transactions on Information Theory*, **51(1)**: 339–348 (2005). 1

[46] X.-D. Hou. $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$. *Discrete Mathematics*, **149**: 99–122 (1996). 3

[47] X.-D. Hou. On the coefficients of binary bent functions. *Proceedings of the*

American Mathematical Society, **128(4)**: 987–996 (1999). 3

[48] X.-D. Hou y P. Langevin. Results on bent functions. *Journal of Combinatorial Theory (Series A)*, **80**: 232–246 (1997). 3

[49] 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). 2

[50] 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). 2, 16

[51] 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). 8

[52] 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)). 5

[53] N. G. Leander. *Normality of Bent Functions Monomial- and Binomial-Bent Functions*. Tesis Doctoral, Ruhr Universität Bochum, noviembre 2004. 1

[54] A. Lempel y M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, **28(6)**: 865–868 (1982). 2

[55] 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. 3

[56] R. L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, **15**: 1–10 (1973). 2

[57] W. Meier y O. Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, **1(3)**: 159–176 (1989). 1

[58] W. Meier y O. Staffelbach. Nonlinearity criteria for cryptographic functions. En 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

[59] 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. 4

[60] W. Millan, A. Clark y E. Dawson. Heuristic design of cryptographically strong balanced Boolean functions. En K.Ñyberg (editor), *Advances in Cryptology – EUROCRYP'98*, volumen 1403 de *Lecture Notes in Computer Science*, páginas 489–499. Springer-Verlag, Berlin, 1998. 4

[61] K.Ñyberg. 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. 2

[62] K.Ñyberg. 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

[63] K.Ñyberg. 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. 3

[64] D. Olejár y M. Stanek. On cryptographic properties of random Boolean functions. *Journal of Universal Computer Science*, **4(8)**: 705–717 (1998). 6, 8

[65] J. D. Olsen, R. A. Scholtz y L. R. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, **28(6)**: 858–864 (1982). 2

[66] E. Pasalic. Degree optimized resilient Boolean functions from Maiorana-McFarland class. En K. G. Paterson (editor), *Cryptography and Coding 2003*, volumen 2898 de *Lecture Notes in Computer Science*, páginas 93–114. Springer-Verlag, Berlin, 2003. 4

[67] 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. 6, 8

[68] J. Pieprzyk y G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEEE Proceedings*, **135(6)**: 325–335 (1988). 12

[69] B. Preneel. *Analysis and Design of Cryptographic Hash Functions*. Tesis Doctoral, Katholieke University Leuven, enero 1993. 5

[70] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts y J. Vandewalle. Propagation characteristics of Boolean functions. En I. B. Dam-

GARD (editor), *Advances in Cryptology – EUROCRYPT'90*, volumen 473 de *Lecture Notes in Computer Science*, páginas 161–173. Springer-Verlag, Berlin, 1991. 1, 4, 8

[71] 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. 3, 8

[72] O. S. ROTHAUS. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, **20**: 300–305 (1976). 2, 16

[73] 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

[74] J. SEBERRY y X.-M. ZHANG. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, **9**: 21–35 (1994). 13

[75] J. SEBERRY, X.-M. ZHANG y Y. ZHENG. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, **119**: 1–13 (1995). 13

[76] S. A. VANSTONE y P. C. VAN OORSCHOT. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 2000. 36

[77] R. YARLAGADDA y J. E. HERSHEY. Analysis and synthesis of bent sequences. *IEE Proceedings*, **136(2)**: 112–123 (1989). 3

Reunido el Tribunal que suscribe en el día de la fecha acordó otorgar, por ..... a la Tesis Doctoral de Dª Verónica Requena Arévalo la calificación de .....

Alicante, ... de .... de .....

El Secretario El Presidente

Universidad de Alicante
cedip

La presente Tesis de Dª Verónica Requena Arévalo ha sido registrada con el nº ..... del registro de entrada correspondiente.

Alicante, ... de .... de .....

El Encargado del Registro