Sobre el número de funciones bent obtenidas a partir de funciones de máximo peso*

Joan-Josep Climent[1], Francisco J. García[2] y Verónica Requena[1,**]

[1] Departament de Ciència de la Computació i Intel·ligència Artificial.
Universitat d'Alacant.
Ap. correus 99, E-03080 Alacant, España.
jcliment@ua.es, vrequena@ua.es

[2] Departament de Fonaments de l'Anàlisi Econòmica.
Universitat d'Alacant.
Ap. correus 99, E-03080 Alacant, España.
francisco.garcia@ua.es

Resumen Dada una función bent $f(\boldsymbol{x})$ de n variables definimos sus funciones de máximo y mínimo peso como las funciones booleanas $f^+(\boldsymbol{x})$ y $f^-(\boldsymbol{x})$ cuyos soportes son los conjuntos $M^+ = \{\boldsymbol{a} \in \mathbb{Z}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} + 2^{\frac{n}{2}-1}\}$ y $M^- = \{\boldsymbol{a} \in \mathbb{Z}_2^n \mid w(f \oplus l_{\boldsymbol{a}}) = 2^{n-1} - 2^{\frac{n}{2}-1}\}$ respectivamente, donde $w(f \oplus l_{\boldsymbol{a}})$ denota el peso de Hamming de la función booleana $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ y $l_{\boldsymbol{a}}(\boldsymbol{x})$ es la función lineal definida por $\boldsymbol{a} \in \mathbb{Z}_2^n$. Combinando los 4 minterms de 2 variables con las funciones de máximo o mínimo peso de 4 funciones bent de n variables obtenemos una función bent de $n+2$ variables. Dado que no resulta fácil contar el número de funciones bent obtenidas con dicha construcción, proporcionamos una cota inferior de dicho número.

Palabras clave: Función booleana, función lineal, no linealidad, función bent, minterm, soporte, función de máximo peso, base de Gauss-Jordan

1 Introducción

Las funciones booleanas se utilizan en diferentes aplicaciones criptográficas tales como cifradores en bloque, cifradores en flujo, funciones hash [7,10,25], en teoría de códigos [5,22], entre otras. Con objeto de reducir al máximo las posibilidades de éxito del criptoanálisis, tanto diferencial como lineal, necesitamos funciones booleanas que posean buenas propiedades criptográficas. Para un número par de variables, las funciones bent son funciones booleanas que poseen la máxima no linealidad posible así como la menor autocorrelación posible [30,32],

* Este trabajo ha sido parcialmente subvencionado por el proyecto MTM2008-06674-C02-01 del Ministerio de Ciencia e Innovación del Gobierno de España.

** La investigación de esta autora ha sido financiada con una ayuda del Vicerrectorado de Investigación, Desarrollo e Innovación de la Universitat d'Alacant destinada a la formación de doctores.

lo cual las hace especialmente apropiadas para resistir los criptoanálisis anteriores. Por ejemplo, la implementación de una S-box necesita funciones booleanas no lineales para resistir ataques tales como el criptoanálisis diferencial [1,20,27].

El origen de las funciones bent se remonta a un artículo teórico de McFarland [24] sobre conjuntos de diferencias en grupos finitos no cíclicos. Posteriormente Dillon [17] 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 [29]; desde entonces estas funciones han sido objeto de estudio en muchas áreas como se desprende de la abundante literatura al respecto (véase por ejemplo [2,3,4,8,11,12,18,19,21,23,26,28] y las referencias en ellas incluidas).

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) (véase, por ejemplo, [2,11,32]). Sin embargo, para un entero par n, nosotros [14,15] usamos la representación clásica de las funciones booleanas a través de minterms para construir funciones bent de $n+2$ variables a partir de algunas funciones bent de n variables.

Tanto el uso de la forma normal algebraica como el de la tabla de verdad (equivalentemente, la expresión como suma de minterms), tienen sus ventajas y desventajas. Por ejemplo, la forma normal algebraica de una función booleana $f(\boldsymbol{x})$ de n variables proporciona directamente su grado y, si es mayor que $n/2$ se puede asegurar que $f(\boldsymbol{x})$ no es una función bent (véase [29]); 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.

Cabe destacar que no existe un método que permita generar todas las funciones bent, excepto para algunos casos particulares. Por ejemplo, para $n = 2$ solamente hay 8 funciones bent; para $n = 4$ sólo existen 896 funciones bent y para $n = 6$, Chang [13] probó que el número de funciones bent es $5\,425\,430\,528$. Sin embargo, su clasificación o determinación para $n \geq 8$ continúa siendo un problema abierto. Como comentamos al final de la sección 2, nosotros estamos intereados en la obtención del número de funciones bent distintas que podemos construir y no en el número de clases de funciones afínmente equivalentes.

El resto del artículo está organizado como sigue. En la sección 2 introducimos algunos conceptos básicos, la notación que utilizaremos a lo largo del artículo y algunos resultados de [14] necesarios para el seguimiento de este artículo, que puede ser considerado como la segunda parte de aquel. En la sección 3 introducimos los resultados que nos proporcionarán una cota inferior del número de funciones bent construidas de acuerdo con la construcción general introducida en [14]. Finalmente en la sección 4 presentamos algunas conclusiones.

2 Preliminares

Consideremos el cuerpo binario $\mathbb{Z}_2$ con la adición módulo 2 (denotada por $\oplus$) y la multiplicación módulo 2 (denotada por yuxtaposición). Para cualquier entero positivo n, sabemos que $\mathbb{Z}_2^n$ es un espacio vectorial sobre $\mathbb{Z}_2$ con la adición $\oplus$ 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 $\mathbb{Z}_2^n$. En $\mathbb{Z}_2^n$ 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 $\boldsymbol{b}$. Denotamos por $\boldsymbol{e}_i = (e_1^{(i)}, e_2^{(i)}, \ldots, e_{n-1}^{(i)}, e_n^{(i)}) \in \mathbb{Z}_2^n$ la expansión binaria de n dígitos de i, es decir

$$e_1^{(i)} 2^{n-1} + e_2^{(i)} 2^{n-2} + \cdots + e_{n-1}^{(i)} 2^1 + e_n^{(i)} 2^0 = i.$$

Con esta representación, podemos identificar el vector $\boldsymbol{e}_i$ con el entero i y, en consecuencia, podemos identificar $\mathbb{Z}_2^n$ con $\mathbb{Z}_{2^n}$.

Decimos que el conjunto $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\} \subseteq \mathbb{Z}_2^n$ es una **base de Gauss-Jordan** de cardinalidad k si la matriz cuyas filas son $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ está en forma escalonada reducida (vease [9,16]).

Una función booleana de n variables es una aplicación $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$. El conjunto $\mathcal{B}_n$ de todas las funciones booleanas de n variables es un espacio vectorial sobre $\mathbb{Z}_2$ con la adición usual de funciones $\oplus$ 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 a la $(0,1)$-secuencia de longitud 2^n dada por

$$\boldsymbol{\xi}_f = (f(\boldsymbol{e}_0),\ f(\boldsymbol{e}_1),\ \ldots,\ f(\boldsymbol{e}_{2^n-1})).$$

La tabla de verdad de una función booleana queda perfectamente determinada a partir de sus minterms. Un **minterm** en las variables $x_1, x_2, \ldots, x_n$ es la función booleana dada por

$$m_{(u_1,u_2,\ldots,u_n)}(x_1, x_2, \ldots, x_n) = (1 \oplus u_1 \oplus x_1)(1 \oplus u_2 \oplus x_2) \cdots (1 \oplus u_n \oplus x_n).$$

Para $i = 0, 1, 2, \ldots, 2^n - 1$, es evidente que $m_{\boldsymbol{e}_i}(\boldsymbol{x}) = 1$ si y sólo si $\boldsymbol{x} = \boldsymbol{e}_i$. Cuando no haya lugar a confusión, escribiremos $m_i(\boldsymbol{x})$ en lugar de $m_{\boldsymbol{e}_i}(\boldsymbol{x})$. Por tanto, la tabla de verdad

$$(m_i(\boldsymbol{e}_0),\ m_i(\boldsymbol{e}_1),\ \ldots,\ m_i(\boldsymbol{e}_{2^n-1}))$$

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

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

También, 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 $\boldsymbol{e}_i$ según convenga).

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

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

y como la igualdad

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

implica $a_i = 0$ para $i = 0, 1, 2, \ldots, 2^n - 1$, podemos afirmar que el conjunto $\{m_0, m_1, m_2, \ldots, m_{2^n-1}\}$ es una base de $\mathcal{B}_n$.

Llamamos **soporte** de f al conjunto

$$M = \{\boldsymbol{a} \in \mathbb{Z}_2^n \mid f(\boldsymbol{a}) = 1\} \quad \text{o} \quad M = \{i \in \mathbb{Z}_{2^n} \mid f(\boldsymbol{e}_i) = 1\}$$

de acuerdo con la expresión (2) y la identificación de $\mathbb{Z}_2^n$ con $\mathbb{Z}_{2^n}$. Así, M es el conjunto de minterms de $f(\boldsymbol{x})$. De esta forma, podemos escribir la expresión (2) como

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

donde M es un subconjunto de $\mathbb{Z}_2^n$ o de $\mathbb{Z}_{2^n}$, según convenga.

El **peso de Hamming**, o simplemente **peso** de una $(0,1)$-secuencia $\boldsymbol{\alpha}$, que denotamos por $w(\boldsymbol{\alpha})$, es el número de 1 de $\boldsymbol{\alpha}$. El peso de Hamming de una función booleana $f(\boldsymbol{x})$, que denotamos por $w(f)$, es el peso de Hamming de su tabla de verdad $\boldsymbol{\xi}_f$; es decir, $w(f) = w(\boldsymbol{\xi}_f)$ y, en consecuencia, $w(f)$ es el número de minterms en la expresión de $f(\boldsymbol{x})$ como suma de minterms, o equivalentemente, el cardinal del soporte de $f(\boldsymbol{x})$.

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

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

donde $\boldsymbol{a} \in \mathbb{Z}_2^n$, $b \in \mathbb{Z}_2$ y $l_{\boldsymbol{a}}(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle$. Si $b = 0$, decimos que f es una **función lineal**.

Definimos la **no linealidad** de una función $f \in \mathcal{B}_n$ como

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

donde $\mathcal{A}_n \subseteq \mathcal{B}_n$ es el conjunto de todas las funciones afines y la distancia $d(f, g)$, para $f, g \in \mathcal{B}_n$, está definida como $d(f, g) = w(f \oplus g)$. La no linealidad de f está acotada superiormente (véase [32]) por

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

Llamamos **funciones bent** a las funciones booleanas que alcanzan la máxima no linealidad (véase [32]). Por tanto, las funciones bent solamente existen para n par.

El resultado siguiente (véase [31,32]), que enunciamos para futuras referencias, proporciona una caracterización de las funciones bent.

Teorema 1. *Sea $f(\boldsymbol{x})$ una función booleana de n variables. $f(\boldsymbol{x})$ es una función bent si y sólo si el número de 1 de la tabla de verdad de la función booleana $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ es $2^{n-1} \pm 2^{\frac{n}{2}-1}$ para todo $\boldsymbol{a} \in \mathbb{Z}_2^n$.*

Como consecuencia del teorema anterior, si $f(\boldsymbol{x})$ es una función bent, entonces el número de 1 de su tabla de verdad es $2^{n-1} \pm 2^{\frac{n}{2}-1}$, o equivalentemente, $w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Además, $1 \oplus f(\boldsymbol{x})$ y $f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ son funciones bent para todo $\boldsymbol{a} \in \mathbb{Z}_2^n$.

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

Definición 1. Sea $f(\boldsymbol{x})$ una función bent de n variables. Llamamos **función de máximo peso** de $f(\boldsymbol{x})$ a la función

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

donde

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

es el **conjunto de máximo peso** de $f(\boldsymbol{x})$.

Análogamente, llamamos **función de mínimo peso** de $f(\boldsymbol{x})$ a la función

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

donde

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

es el **conjunto de mínimo peso** de $f(\boldsymbol{x})$.

Notemos que al ser $f(\boldsymbol{x})$ una función bent, por el teorema 1 y la expresión (1) tenemos que

$$f^-(\boldsymbol{x}) = 1 \oplus f^+(\boldsymbol{x}), \tag{3}$$

es decir, la función de mínimo peso de $f(\boldsymbol{x})$ es la función complementaria de la función de máximo peso de $f(\boldsymbol{x})$.

Notemos también que, en general, $f^+ \neq f \neq f^-$,

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

como ponemos de manifiesto en la tabla 1 que muestra la relación entre f, f^+ y f^- cuando f recorre el conjunto formado por las ocho funciones bent de 2 variables.

Para una función bent $f(\boldsymbol{x})$ de n variables, en [14] introdujimos la función $f^+(\boldsymbol{x})$ como $f^\star(\boldsymbol{x})$, la llamamos función dual de $f(\boldsymbol{x})$ y probamos que también era una función bent. Los resultados siguientes recogen, para futuras referencias, los resultados más importantes de dicho artículo.

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 1. Funciones de máximo y mínimo peso de las ocho funciones bent de 2 variables

Teorema 2 (Teorema 2 de [14]). *Si $f(\boldsymbol{x})$ es una función bent de n variables, entonces su función de máximo peso $f^+(\boldsymbol{x})$ también es una función bent de n variables.*

Teorema 3.

1. **(Corolario 1 de [14]).** *Sea $f(\boldsymbol{x})$ una función bent de n variables. Si $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$, entonces $g^+(\boldsymbol{x}) = 1 \oplus f^+(\boldsymbol{x})$.*
2. **(Corolario 2 de [14]).** *Si $f(\boldsymbol{x})$ es una función bent de n variables, entonces $f^{+^+}(\boldsymbol{x}) = f(\boldsymbol{x})$.*
3. **(Corolario 3 de [14]).** *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces $f^+(\boldsymbol{x}) \neq g^+(\boldsymbol{x})$.*

Teorema 4 (Teorema 3 de [14]). *Sean $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $f_2(\boldsymbol{x})$ y $f_3(\boldsymbol{x})$ cuatro funciones bent de n variables (no necesariamente distintas) tales que*

$$f_0(\boldsymbol{x}) \oplus f_1(\boldsymbol{x}) \oplus f_2(\boldsymbol{x}) \oplus f_3(\boldsymbol{x}) = 1. \tag{4}$$

Si (i_0, i_1, i_2, i_3) es una permutación de $(0, 1, 2, 3)$ e $\boldsymbol{y} = (y_1, y_2)$ es un vector de dos variables, entonces

$$F(\boldsymbol{y}, \boldsymbol{x}) = m_{i_0}(\boldsymbol{y})\, f_0^+(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y})\, f_1^+(\boldsymbol{x}) \oplus m_{i_2}(\boldsymbol{y})\, f_2^+(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y})\, f_3^+(\boldsymbol{x})$$

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

Notemos que como consecuencia de la expresión (3), los resultados anteriores son también válidos si cambiamos las funciones de peso máximo por las correspondientes funciones de peso mínimo.

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 (4) no es fácil. Sin embargo, si $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son funciones bent de n variables, entonces las cuaternas

$$(f(\boldsymbol{x}), f(\boldsymbol{x}), f(\boldsymbol{x}), 1 \oplus f(\boldsymbol{x})) \tag{5}$$

$$(f(\boldsymbol{x}), f(\boldsymbol{x}), g(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x})) \tag{6}$$

satisfacen, evidentemente, la expresión (4) con lo que tenemos el resultado siguiente.

Teorema 5.

1. **(Corolario 4 de [14]).** *Si $f(\boldsymbol{x})$ es una función bent n variables e $i \in \{0,1,2,3\}$, entonces*

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

   es una función bent de $n+2$ variables.
2. **(Corolario 5 de [14]).** *Si $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son funciones bent de n variables e (i_0,i_1,i_2,i_3) es una permutación de $(0,1,2,3)$, entonces*

$$B_{f,g}(\boldsymbol{y},\boldsymbol{x}) = (m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y}))\, f^+(\boldsymbol{x}) \oplus m_{i_2}(\boldsymbol{y}) g^+(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus g^+(\boldsymbol{x})\right)$$

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

Ahora, si en el teorema 5.2 exigimos que $g(\boldsymbol{x}) \neq f(\boldsymbol{x})$ y $g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x})$, entonces todas las funciones bent construidas de acuerdo con el teorema 5 son distintas entre sí. Por tanto, si denotamos por ν_n el número de funciones bent de n variables, tenemos que

$$6\nu_n^2 - 8\nu_n \tag{7}$$

es el número de funciones bent de $n+2$ variables que podemos construir de acuerdo con el teorema 5 (vease [14, página 15]).

Fuera de los casos particulares proporcionados por el teorema 5 resulta difícil contar cuántas cuaternas $(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), f_3(\boldsymbol{x}))$ de funciones bent de n variables satisfacen la expresión (4), excluidas las correspondientes a las expresiones (5) y (6) y, por tanto, resulta difícil contar cuántas funciones bent de $n+2$ variables distintas proporciona el teorema 4. En la sección siguiente estableceremos una cota inferior de dicho número que, a partir de ahora, denotaremos por ω_n.

Antes de pasar a la sección siguiente, recordemos que dos funciones booleanas $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son **afínmente equivalentes** si existe una matriz invertible A de tamaño $n \times n$ y un vector $\boldsymbol{a} \in \mathbb{Z}_2^n$ tales que $g(\boldsymbol{x}) = f(\boldsymbol{x}A \oplus \boldsymbol{a})$ y en tal caso (váse por ejemplo [6]) $g(\boldsymbol{x})$ es bent si y sólo si $f(\boldsymbol{x})$ lo es. En consecuencia, muchos autores trabajan en el problema de *encontrar el número de clases de funciones afínmente equivalentes y sus representantes*. Sin embargo, nosotros estamos interesados en el problema de *obtener el número de funciones bent distintas que existen o que podemos construir*, ya que el hecho de que dos funciones bent sean afínmente equivalentes no implica que sean distintas como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 1. 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

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

y el vector $\boldsymbol{a} = (0,0,0,1)$. Es fácil comprobar que las funciones $f(\boldsymbol{x}A \oplus \boldsymbol{a})$ y $f(\boldsymbol{x})$ tienen la misma tabla de verdad y, en consecuencia, que son iguales.

3 Resultados principales

Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables, supongamos que $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_2^n$ y consideremos las cuaternas de funciones bent

$$(f(\boldsymbol{x}), f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x}), g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x}), 1 \oplus g(\boldsymbol{x}) \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}}(\boldsymbol{x}))\,. \tag{8}$$

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 expresión (4). Antes de continuar, notemos que si tomamos $\boldsymbol{a} = \boldsymbol{b} = \boldsymbol{0}$, entonces las cuaternas (5) y (6) son un caso particular de la cuaterna anterior cuando $g(\boldsymbol{x}) = f(\boldsymbol{x})$ y $g(\boldsymbol{x}) \neq f(\boldsymbol{x})$ respectivamente. Por tanto, sólo necesitamos considerar los dos casos siguientes (justificaremos esta afirmación más adelante).

Teorema 6. *Sean $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_2^n \setminus \{\boldsymbol{0}\}$ con $\boldsymbol{a} \neq \boldsymbol{b}$. Si $f(\boldsymbol{x})$ es una función bent de n variables e (i_0, i_1, i_2, i_3) es una permutación de $(0,1,2,3)$, entonces*

$$\begin{aligned} C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) = {} & m_{i_0}(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}) \\ & \oplus m_{i_2}(\boldsymbol{y})(f \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus (f \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})\right) \end{aligned}$$

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

Teorema 7. *Sean $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_2^n \setminus \{\boldsymbol{0}\}$ con $\boldsymbol{a} \neq \boldsymbol{b}$. Si $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ son funciones bent de n variables tales que $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$ e (i_0, i_1, i_2, i_3) es una permutación de $(0,1,2,3)$, entonces*

$$\begin{aligned} D_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) = {} & m_{i_0}(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y})(f \oplus l_{\boldsymbol{a}})^+(\boldsymbol{x}) \\ & \oplus m_{i_2}(\boldsymbol{y})(g \oplus l_{\boldsymbol{b}})^+(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus (g \oplus l_{\boldsymbol{a}\oplus\boldsymbol{b}})^+(\boldsymbol{x})\right) \end{aligned}$$

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

Notemos que no todas las funciones bent proporcionadas por el teorema 6 son distintas entre sí como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 2. Supongamos que $n = 2$, consideremos los vectores $\boldsymbol{a} = \boldsymbol{1} = (0,1)$ y $\boldsymbol{b} = \boldsymbol{2} = (1,0)$, la función bent $f(\boldsymbol{x}) = m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})$ y la permutación $(0,2,1,3)$ de $(0,1,2,3)$. Entonces

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

y, de acuerdo con el teorema 6 y la tabla 1, tenemos que

$$\begin{aligned} C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) = {} & m_0(\boldsymbol{y}) f^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})(f \oplus l_{\boldsymbol{1}})^+(\boldsymbol{x}) \\ & \oplus m_1(\boldsymbol{y})(f \oplus l_{\boldsymbol{2}})^+(\boldsymbol{x}) \oplus m_3(\boldsymbol{y}) \left(1 \oplus (f \oplus l_{\boldsymbol{3}})^+(\boldsymbol{x})\right) \end{aligned}$$

$$= m_0(\boldsymbol{y})m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{y})m_2(\boldsymbol{x}) \oplus m_1(\boldsymbol{y})m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})\,(1 \oplus m_3(\boldsymbol{x}))\,.$$

Por otro lado, si considereamos los vectores $\boldsymbol{u} = \mathbf{1} = (0,1)$ y $\boldsymbol{v} = \mathbf{3} = (1,1)$, la función bent $g(\boldsymbol{x}) = m_2(\boldsymbol{x})$, y la permutación $(1,0,2,3)$ de $(0,1,2,3)$, entonces, procediendo como en el caso anterior tenemos que

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

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

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 $\mathbb{Z}_2^n$. Con el fin de evitar esta situación, consideraremos solamente vectores $\boldsymbol{a},\boldsymbol{b} \in \mathbb{Z}_2^n$ tales que $\{\boldsymbol{a},\boldsymbol{b}\}$ es una base de Gauss-Jordan de $\mathbb{Z}_2^n$ de cardinalidad 2. El resultado siguiente establece que las funciones bent construidas de acuerdo con el teorema 6 son distintas dos a dos si $\{\boldsymbol{a},\boldsymbol{b}\}$ es una base de Gauss-Jordan de $\mathbb{Z}_2^n$ de cardinalidad 2.

Lema 1. *Sean $f(\boldsymbol{x})$ y $p(\boldsymbol{x})$ dos funciones bent de n variables. Supongamos que $C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent de $n+2$ variables construida de acuerdo con el teorema 6 utilizando $f(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a},\boldsymbol{b}\}$ de $\mathbb{Z}_2^n$ de cardinalidad 2 y la permutación (i_0,i_1,i_2,i_3) de $(0,1,2,3)$. Supongamos también que $C_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent de $n+2$ variables construida de acuerdo con el teorema 6 utilizando $p(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{u},\boldsymbol{v}\}$ de $\mathbb{Z}_2^n$ de cardinalidad 2 y la permutación (j_0,j_1,j_2,j_3) de $(0,1,2,3)$. Si $f(\boldsymbol{x}) \neq p(\boldsymbol{x})$, entonces $C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \neq C_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$.*

Demostración. Si $\boldsymbol{\xi}$ y $\boldsymbol{\eta}$ son las tablas de verdad de $f(\boldsymbol{x})$ y $p(\boldsymbol{x})$ respectivamente, entonces las tablas de verdad de $C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ y $C_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ tienen cuatro bloques (no necesariamente en dicho orden y no necesariamente el mismo orden para las dos):

$$\begin{array}{lcccc} C_{f,\boldsymbol{a},\boldsymbol{b}}: & \boldsymbol{\xi}^+ & (\boldsymbol{\xi} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}})^+ & (\boldsymbol{\xi} \oplus \boldsymbol{\Lambda}_{\boldsymbol{b}})^+ & \mathbf{1} \oplus (\boldsymbol{\xi} \oplus \boldsymbol{\Lambda}_{\boldsymbol{a}\oplus\boldsymbol{b}})^+ \\ C_{p,\boldsymbol{u},\boldsymbol{v}}: & \boldsymbol{\eta}^+ & (\boldsymbol{\eta} \oplus \boldsymbol{\Lambda}_{\boldsymbol{u}})^+ & (\boldsymbol{\eta} \oplus \boldsymbol{\Lambda}_{\boldsymbol{v}})^+ & \mathbf{1} \oplus (\boldsymbol{\eta} \oplus \boldsymbol{\Lambda}_{\boldsymbol{u}\oplus\boldsymbol{v}})^+ \end{array}$$

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, y $\mathbf{1}$ es la tabla de verdad de la función constante 1.

Si $C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) = C_{p,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$, 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 obtenemos, utilizando el teorema 3, que $f(\boldsymbol{x}) = p(\boldsymbol{x})$, o que $l_{\boldsymbol{c}}(\boldsymbol{x}) = 1$ para algún $\boldsymbol{c} \in \mathbb{Z}_2^n$ que depende de los vectores $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{u}$ y $\boldsymbol{v}$, o que

$$(\boldsymbol{u},\boldsymbol{v}) \in \{(\boldsymbol{a},\boldsymbol{a}\oplus\boldsymbol{b}),(\boldsymbol{b},\boldsymbol{a}\oplus\boldsymbol{b}),(\boldsymbol{a}\oplus\boldsymbol{b},\boldsymbol{a}),(\boldsymbol{a}\oplus\boldsymbol{b},\boldsymbol{b})\}\,. \tag{9}$$

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

Ahora, como consecuencia inmediata del lema anterior tenemos el resultado siguiente que establece el número de funciones bent de $n+2$ variables distintas que podemos construir de acuerdo con el teorema 6.

Teorema 8. *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 el teorema 6 es*

$$\frac{4!}{3}\binom{2^n-1}{2}\nu_n. \tag{10}$$

Demostración. De acuerdo con el lema 1, utilizando el teorema 6 podemos construir $4!\nu_n N(n,2)$ funciones bent de $n+2$ variables, donde $N(n,2)$ es el número de bases de Gauss-Jordan de $\mathbb{Z}_2^n$ de cardinalidad 2. Ahora bien, como cada subespacio vectorial de dimensión 2 de $\mathbb{Z}_2^n$ tiene una única base de Gauss-Jordan de cardinalidad 2, tenemos que $N(n,2)$ coincide con el número de subespacios vectoriales de $\mathbb{Z}_2^n$ de dimensión 2; por tanto (véase [33, página 46])

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

con lo que la expresión (10) representa el número de funciones bent de $n+2$ variables distintas que proporciona el teorema 6. □

Igual que ocurría con el teorema 6, tampoco todas las funciones bent construidas de acuerdo con el teorema 7 son distintas entre sí como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 3. Supongamos que $n = 2$, consideremos los vectores $\boldsymbol{a} = \mathbf{1} = (0,1)$ y $\boldsymbol{b} = \mathbf{2} = (1,0)$, las funciones bent $f(\boldsymbol{x}) = m_0(\boldsymbol{x})$ y $g(\boldsymbol{x}) = 1 \oplus m_3(\boldsymbol{x})$, y la permutación $(0,1,2,3)$ de $(0,1,2,3)$. De acuerdo con el teorema 7 y la tabla 1 (véase también el ejemplo 2 para las funciones $l_{\mathbf{1}}(\boldsymbol{x})$, $l_{\mathbf{2}}(\boldsymbol{x})$ y $l_{\mathbf{3}}(\boldsymbol{x})$), tenemos que

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

Por otro lado, si considereamos los vectores $\boldsymbol{u} = \mathbf{1} = (0,1)$ y $\boldsymbol{v} = \mathbf{3} = (1,1)$, las funciones bent $p(\boldsymbol{x}) = m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})$ y $q(\boldsymbol{x}) = m_3(\boldsymbol{x})$, y la permutación $(1,0,3,2)$ de $(0,1,2,3)$, entonces, procediendo como en el caso anterior, tenemos que

$$D_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}) = m_1(\boldsymbol{y}) p^+(\boldsymbol{x}) \oplus m_0(\boldsymbol{y})(p \oplus l_{\mathbf{1}})^+(\boldsymbol{x})$$

$$\begin{aligned}
&\oplus m_3(\boldsymbol{y})(q \oplus l_{\boldsymbol{3}})^+(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) \left(1 \oplus (q \oplus l_{\boldsymbol{2}})^+(\boldsymbol{x})\right) \\
&= m_0(\boldsymbol{y})\,(m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})) \\
&\quad \oplus (m_1(\boldsymbol{y}) \oplus m_2(\boldsymbol{y}))\,(m_0(\boldsymbol{x}) \oplus m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{x})) \oplus m_3(\boldsymbol{y}) m_0(\boldsymbol{x})
\end{aligned}$$

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

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, para evitar estas situaciones, en la construcción de las funciones $D_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ proporcionadas por el teorema 7 supondremos siempre que

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

El resultado siguiente, cuya demostración es similar a la del lema 1 y que por tanto omitimos, establece que las funciones bent construidas de acuerdo con el teorema 7 son distintas dos a dos cuando las funciones $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ satisfacen la desigualdad anterior.

Lema 2. *Supongamos que $f(\boldsymbol{x})$, $g(\boldsymbol{x})$, $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$ son funciones bent de n variables tales que*

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

Supongamos que $D_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el teorema 7 utilizando las funciones bent $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$, los vectores $\boldsymbol{a}$ y $\boldsymbol{b}$ de $\mathbb{Z}_2^n$ (con $\boldsymbol{a} \neq \boldsymbol{b}$) y la permutación (i_0, i_1, i_2, i_3) de $(0,1,2,3)$. Supongamos también que $D_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$ es la función bent construida de acuerdo con el teorema 7 utilizando las funciones bent $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$, los vectores $\boldsymbol{u}$ y $\boldsymbol{v}$ de $\mathbb{Z}_2^n$ (con $\boldsymbol{u} \neq \boldsymbol{v}$) y la permutación (j_0, j_1, j_2, j_3) de $(0,1,2,3)$. Si $f(\boldsymbol{x}) \neq p(\boldsymbol{x})$ y $f(\boldsymbol{x}) \neq p(\boldsymbol{x}) \oplus l_{\boldsymbol{u}}(\boldsymbol{x})$, entonces $D_{f,g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y},\boldsymbol{x}) \neq D_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y},\boldsymbol{x})$.

Ahora, como consecuencia inmediata del lema anterior tenemos el resultado siguiente que establece el número de funciones bent de $n+2$ variables distintas que podemos construir de acuerdo con el teorema 7.

Teorema 9. *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 el teorema 7 es*

$$4! \binom{2^n - 1}{2} \frac{\nu_n}{2^n} \left(\frac{\nu_n}{2^{n+1}} - 1 \right). \tag{11}$$

Demostración. Como consecuencia del lema 2 podemos elegir $f(\boldsymbol{x})$ de $\nu_n/2^n$ formas distintas y, una vez fijada $f(\boldsymbol{x})$, podemos elegir $g(\boldsymbol{x})$ de $\nu_n/2^{n+1} - 1$ formas distintas. Por otro lado, puesto que podemos elegir los vectores $\boldsymbol{a}$ y $\boldsymbol{b}$ de $\binom{2^n-1}{2}$ formas distintas y dado que hay 4! permutaciones distintas de $(0,1,2,3)$, tenemos que la expresión (11) representa el número de funciones bent de $n+2$ variables distintas que proporciona el teorema 7. □

El resultado siguiente, cuya demostración es análoga a la de los lemas 1 y 2 y que por tanto omitimos, establece que ninguna de las funciones bent construidas de acuerdo con el teorema 6 coincide con ninguna de las funciones bent proporcionadas por el teorema 7 y viceversa.

Lema 3. *Supongamos que $f(\boldsymbol{x})$, $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$ son funciones bent de n variables tales que*

$$q(\boldsymbol{x}) \neq p(\boldsymbol{x}) \oplus l_{\boldsymbol{c}}(\boldsymbol{x}) \oplus c \quad \textit{para todo } (\boldsymbol{c}, c) \in \mathbb{Z}_2^n \times \mathbb{Z}_2.$$

Supongamos que $C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida de acuerdo con el teorema 6 utilizando la función bent $f(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a}, \boldsymbol{b}\}$ de $\mathbb{Z}_2^n$ de cardinalidad 2 y la permutación (i_0, i_1, i_2, i_3) de $(0, 1, 2, 3)$. Supongamos también que $D_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida de acuerdo con el teorema 7 utilizando las funciones bent $p(\boldsymbol{x})$ y $q(\boldsymbol{x})$, los vectores $\boldsymbol{u}$ y $\boldsymbol{v}$ de $\mathbb{Z}_2^n$ (con $\boldsymbol{u} \neq \boldsymbol{v}$) y la permutación (j_0, j_1, j_2, j_3) de $(0, 1, 2, 3)$. Entonces $C_{f,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x}) \neq D_{p,q,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$.

Ahora, como consecuencia del lema 3 y de los teoremas 8 y 9 podemos enunciar el resultado siguiente que establece el número de funciones bent de $n+2$ variables distintas que podemos construir de acuerdo con los teoremas 6 y 7.

Corolario 1. *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 teoremas 6 y 7 es*

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

Demostración. Basta sumar las expresiones (10) y (11) para obtener el resultado ya que, por el lema 3, las funciones bent construidas de acuerdo con los teoremas 6 y 7 son distintas entre sí. □

Finalmente, tal como habíamos anunciado al inicio de la sección, cualquier otra posible 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 teoremas 5, 6 y 7 (junto con las condiciones adicionales del lema 2). Por ejemplo:

- Si $\boldsymbol{a} = \boldsymbol{0}$ y $\boldsymbol{b} \neq \boldsymbol{0}$, entonces la 4-tupla de la expresión (8) 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 teorema 5.1 si $f(\boldsymbol{x}) = g(\boldsymbol{x}) \oplus l_{\boldsymbol{b}}(\boldsymbol{x})$, o al teorema 5.2 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 4-tupla de la expresión (8) 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 teorema 5.1 si $g(\boldsymbol{x}) = f(\boldsymbol{x})$, $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x})$, $g(\boldsymbol{x}) = f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ o $g(\boldsymbol{x}) = 1 \oplus f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$; o al teorema 7 (junto con las condiciones adicionales del lema 2) si $g(\boldsymbol{x}) \neq f(\boldsymbol{x})$, $g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x})$, $g(\boldsymbol{x}) \neq f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$ o $g(\boldsymbol{x}) \neq 1 \oplus f(\boldsymbol{x}) \oplus l_{\boldsymbol{a}}(\boldsymbol{x})$.

Mediante un razonamiento análogo al utilizado en los lemas 1, 2 y 3, podemos probar que ninguna de las funciones bent construida de acuerdo con el teorema 5 puede ser obtenida por los teoremas 6 y 7 y viceversa. Por tanto, como consecuencia del corolario 1 tenemos el resultado siguiente.

Corolario 2. *Si ν_n es el número de funciones bent de n variables y ω_n es el número de 4-tuplas de funciones bent que satisfacen la ecuación (4), excluyendo las correspondientes a los casos contemplados en el teorema 5, entonces*

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

Finalmente, de la expresión (7) y el corolario anterior tenemos que el teorema 4 proporciona, al menos,

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

funciones bent de $n+2$ variables distintas. Así, nuestra construcción proporciona 512 funciones bent de 4 variables, 9 372 608 funciones bent de 6 variables y 345 031 196 824 408 177 152 funciones bent de 8 variables. Como no conocemos el valor de ν_8, no podemos determinar el número de funciones bent que podemos construir.

4 Conclusiones

En [14] presentamos un método general para obtener funciones bent de $n+2$ variables a partir de 4 funciones bent $f_0(\boldsymbol{x})$, $f_1(\boldsymbol{x})$, $f_2(\boldsymbol{x})$ y $f_3(\boldsymbol{x})$ de n variables que satisfacen la condición expresada por la ecuación (4). En este artículo hemos introducido una familia de cuaternas de funciones bent de n variables que satisfacen dicha condición y establecido el número de funciones bent de $n+2$ variables que podemos construir a partir de dichas cuaternas, obteniendo, en consecuencia, una cota inferior del número de funciones bent que se pueden obtener a partir del método general introducido en [14].

Referencias

1. C. M. Adams. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes and Cryptography*, **12**: 283–316 (1997).
2. C. M. Adams y S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, **35(6)**: 1170–1173 (1990).
3. C. M. Adams y S. E. Tavares. Generating bent sequences. *Discrete Applied Mathematics*, **39**: 155–159 (1992).
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).

5. Y. Borissov, A. Braeken, S. Nikova y B. Preneel. On the covering radii of binary Reed-Muller codes in the set of resilient Boolean functions. *IEEE Transactions on Information Theory*, **51(3)**: 1182–1189 (2005).
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.
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.
8. A. Canteaut y P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, **49(8)**: 2004–2019 (2003).
9. A. Canteaut, M. Daum, H. Dobbertin y G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, **154**: 202–218 (2006).
10. C. Carlet y Y. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, **25**: 263–279 (2002).
11. 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.
12. C. Carlet y P. Guillot. An alternate characterization of the bentness of binary functions, with uniqueness. *Designs, Codes and Cryptography*, **14**: 133–140 (1998).
13. D. K. Chang. Binary bent sequences of order 64. *Utilitas Mathematica*, **52**: 141–151 (1997).
14. 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, 2007.
15. 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).
16. 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.
17. J. F. Dillon. *Elementary Hadamard Difference Sets*. Tesis Doctoral, University of Maryland, 1974.
18. 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).
19. 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.
20. K. C. Gupta y P. Sarkar. Improved construction of nonlinear resilient S-boxes. *IEEE Transactions on Information Theory*, **51(1)**: 339–348 (2005).
21. 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).

22. 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).
23. A. Lempel y M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, **28(6)**: 865–868 (1982).
24. R. L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, **15**: 1–10 (1973).
25. 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.
26. K. Nyberg. Constructions of bent functions and difference sets. En I. B. Damgård (editor), *Advances in Cryptology – EUROCRYPT '90*, volumen 473 de *Lecture Notes in Computer Science*, páginas 151–160. Springer-Verlag, Berlin, 1991.
27. K. Nyberg. Perfect nonlinear S-boxes. En D. W. Davies (editor), *Advances in Cryptology – EUROCRYPT '91*, volumen 547 de *Lecture Notes in Computer Science*, páginas 378–386. Springer-Verlag, Berlin, 1991.
28. J. D. Olsen, R. A. Scholtz y L. R. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, **28(6)**: 858–864 (1982).
29. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, **20**: 300–305 (1976).
30. P. Sarkar y S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. En B. Preneel (editor), *Advances in Cryptology – EUROCRYPT 2000*, volumen 1807 de *Lecture Notes in Computer Science*, páginas 485–506. Springer-Verlag, Berlin, 2000.
31. J. Seberry y X.-M. Zhang. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, **9**: 21–35 (1994).
32. J. Seberry, X.-M. Zhang y Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, **119**: 1–13 (1995).
33. S. A. Vanstone y P. C. van Oorschot. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 2000.