XXI Congreso de Ecuaciones Diferenciales y Aplicaciones
XI Congreso de Matemática Aplicada
Ciudad Real, 21-25 septiembre 2009
(pp. 1–8)

Construcción de funciones bent a partir de una función bent y de sus traslaciones cíclicas basadas en bases de Gauss-Jordan de cardinalidad 2

J.-J. Climent[1], F. J. García[2] y V. Requena[1]

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

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

Palabras clave: función booleana, función bent, base de Gauss-Jordan, minterm

Resumen

En este artículo presentamos un método iterativo de construcción de funciones bent de $n+2$ variables a partir de una función bent de n variables y de una base de Gauss-Jordan de cardinalidad 2 de $\mathbb{F}_2^n$ utilizando minterms de n y 2 variables. Además, proporcionamos el número de funciones bent de $n+2$ variables que podemos obtener a través del método aquí introducido.

1. Introducción

Las funciones booleanas se utilizan en diferentes aplicaciones criptográficas tales como cifradores en bloque, cifradores en flujo y funciones hash [4, 12], en teoría de códigos [2, 9], entre otros. La implementación de una S-box necesita funciones no lineales que garanticen su efectividad criptográfica con el fin de resistir tanto el criptoanálisis lineal como el criptoanálisis diferencial [1, 8, 10, 13].

Para un número par de variables, las funciones booleanas que alcanzan la máxima no linealidad posible son las que mejor resisten los ataques basados en el criptoanálisis lineal y se conocen con el nombre de funciones *bent* [15, 17]. Las funciones bent constituyen un tópico fascinante en criptografía (como pone de manifiesto la abundante bibliografía existente sobre las mismas), pero lamentablemente existe un gran desconocimiento sobre sus propiedades, su clasificación y su número. En estos momentos, se desconoce la existencia de un método que permita obtener todas las funciones bent y solamente se conoce

su número para algunos casos particulares ($n = 2, 4, 6$ con n el número de variables); la clasificación para $n \geq 8$ continúa siendo un problema abierto.

El origen de las funciones bent se remonta a un artículo teórico de McFarland [11] sobre conjuntos diferencia en grupos finitos no cíclicos. Un año después, Dillon [7], sistematizó y recopiló las ideas de McFarland proporcionando un gran número de propiedades; la tesis de Dillon ha sido una excelente fuente en el estudio de las funciones bent desde mediados de los años 70 del pasado siglo. El nombre bent con el que se conocen estas funciones se debe a Rothaus [14].

El resto del artículo está organizado de la siguiente manera: En la sección 2, presentamos algunas definiciones básicas y la notación utilizada. En la sección 3, introducimos un método general para la construcción de funciones bent de $n + 2$ variables utilizando una función bent de n variables y algunas de sus traslaciones cíclicas. Finalmente, en la sección 4, presentamos los resultados necesarios para contar el número de funciones bent que podemos construir utilizando el método introducido en la sección 3, poniendo de manifiesto que para garantizar la unicidad de las funciones obtenidas necesitamos que los vectores utilizados para definir las traslaciones cíclicas constituyan una base de Gauss-Jordan de cardinalidad 2 de $\mathbb{F}_2^n$.

2. Preliminares

Consideremos el cuerpo binario $\mathbb{F}_2$ con la adición denotada por $\oplus$ y la multiplicación denotada por yuxtaposición. Para cualquier entero positivo n, sabemos que $\mathbb{F}_2^n$ es un espacio vectorial sobre $\mathbb{F}_2$ con la adición componente a componente y denotada también por $\oplus$. Decimos que el 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 $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ está en su forma escalonada reducida (véase también [3, 6]).

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 de dimensión 2^n sobre $\mathbb{F}_2$ con la adición usual de funciones (que denotamos también por $\oplus$).

Si $f \in \mathcal{B}_n$, llamamos **tabla de verdad** de f a la $(0, 1)$-secuencia de longitud 2^n dada por

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

donde $\mathbb{F}_2^n = \{\boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{2^n-1}\}$ y $\boldsymbol{e}_i$ es la expansión binaria del entero i. 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

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

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 $\boldsymbol{e}_i$). Además, para cualquier $f \in \mathcal{B}_n$ es fácil comprobar que

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

y el conjunto $M = \{\boldsymbol{e}_i \in \mathbb{F}_2^n \mid f(\boldsymbol{e}_i) = 1\}$ recibe el nombre de **soporte** de f.

El **peso de Hamming** de una función booleana $f(\boldsymbol{x})$, que denotamos por $w(f)$, es el número de 1 de su tabla de verdad y, en consecuencia, $w(f)$ es el número de minterms en la expresión de $f(\boldsymbol{x})$ como suma de minterms. Decimos que $f \in \mathcal{B}_n$ es **equilibrada** si su peso es 2^{n-1}.

Decimos que $f \in \mathcal{B}_n$ es una **función afín** si $f(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle \oplus b$, donde $\boldsymbol{a} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$ y $\langle \boldsymbol{a}, \boldsymbol{x} \rangle$ es el producto escalar usual de los vectores $\vec{a}$ y $\vec{x}$. Si $b = 0$, decimos que f es una **función lineal**. Definimos la **no linealidad** de una función $f \in \mathcal{B}_n$ como

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

donde $\mathcal{A}_n$ es el conjunto de todas las funciones afines y la distancia $d(f, g)$ entre dos funciones booleanas $f, g \in \mathcal{B}_n$ se define como $d(f, g) = w(f \oplus g)$. La no linealidad de f está acotada superiormente (véase [17]) 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 [17]). Por tanto, las funciones bent solamente existen para n par.

El resultado siguiente (véase [16, 17]), que enunciamos para futuras referencias, nos proporciona una caracterización de las funciones bent.

Teorema 1 *Sea $f(\boldsymbol{x})$ una función de n variables. Las afirmaciones siguientes son equivalentes.*

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

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, $f(\boldsymbol{x})$ se expresa como suma de $2^{n-1} \pm 2^{\frac{n}{2}-1}$ minterms y, en consecuencia, $f(\boldsymbol{x})$ no es equilibrada. Además, $1 \oplus f(\boldsymbol{x})$ y $f(\boldsymbol{x} \oplus \boldsymbol{u})$ son funciones bent para todo $\boldsymbol{u} \in \mathbb{F}_2^n$.

3. Resultados principales

En el resto del artículo consideraremos 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 $\mathbb{F}_2^2$. Primero introducimos la siguiente propiedad de los minterms que nos permitirá construir funciones booleanas de $n + 2$ variables a partir de funciones booleanas de n variables.

Lema 1 (Lema 1 de [5]) *Supongamos que $a \in \mathbb{F}_{2^n}$ y $b \in \mathbb{F}_{2^2}$. 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*

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

El lema anterior nos dice que los cuatro minterms de $n+2$ variables, que podemos obtener a partir del minterm $m_a(\boldsymbol{x})$ de n variables, son

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

Además, los minterms tiene la siguiente propiedad, cuya demostración es evidente y que por tanto omitimos, que los hace operativos desde el punto de vista algebraico.

Lema 2 *$m_{\boldsymbol{u}}(\boldsymbol{x} \oplus \boldsymbol{v}) = m_{\boldsymbol{u} \oplus \boldsymbol{v}}(\boldsymbol{x})$ para todo $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$.*

En el siguiente teorema, que es el resultado principal de este artículo, introducimos una nueva construcción de funciones bent de $n+2$ variables a partir de una función bent $f(\boldsymbol{x})$ de n variables y algunas de las traslaciones cíclicas de $f(\boldsymbol{x})$ mediante algunos vectores de $\mathbb{F}_2^n$.

Teorema 2 *Sea $f(\boldsymbol{x})$ una función bent de n variables y consideremos $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$. Si (i_0, i_1, i_2, i_3) es cualquier permutación de $(0, 1, 2, 3)$, entonces*

$$B(\boldsymbol{y}, \boldsymbol{x}) = m_{i_0}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_{i_2}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{v}) \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})\right)$$

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

Demostración: De acuerdo con el teorema 1 debemos probar que la función booleana

$$B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}) = B(\boldsymbol{y}, \boldsymbol{x}) \oplus B((\boldsymbol{y}, \boldsymbol{x}) \oplus (\boldsymbol{b}, \boldsymbol{a}))$$

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

$$\begin{aligned} B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y}, \boldsymbol{x}) &= B(\boldsymbol{y}, \boldsymbol{x}) \oplus B(\boldsymbol{y} \oplus \boldsymbol{b}, \boldsymbol{x} \oplus \boldsymbol{b}) \\ &= m_{i_0}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_{i_2}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{v}) \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})\right) \\ &\quad \oplus m_{i_0 \oplus b}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus m_{i_1 \oplus b}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{a}) \oplus m_{i_2 \oplus b}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{v} \oplus \boldsymbol{a}) \\ &\quad \oplus m_{i_3 \oplus b}(\boldsymbol{y}) \left(1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v} \oplus \boldsymbol{a})\right) \end{aligned} \tag{2}$$

y consideramos los diferentes casos dependiendo de los valores de $(\boldsymbol{b}, \boldsymbol{a})$.

Primero, supongamos que $\boldsymbol{a} = \boldsymbol{0}_n$ y $\boldsymbol{b} \neq \boldsymbol{0}_2$. Entonces, la expresión (2) se convierte en

$$\begin{aligned} B_{(\boldsymbol{b},\boldsymbol{0})}(\boldsymbol{y}, \boldsymbol{x}) &= \left(m_{i_0}(\boldsymbol{y}) \oplus m_{i_0 \oplus b}(\boldsymbol{y})\right) f(\boldsymbol{x}) \oplus \left(m_{i_1}(\boldsymbol{y}) \oplus m_{i_1 \oplus b}(\boldsymbol{y})\right) f(\boldsymbol{x} \oplus \boldsymbol{u}) \\ &\quad \oplus \left(m_{i_2}(\boldsymbol{y}) \oplus m_{i_2 \oplus b}(\boldsymbol{y})\right) f(\boldsymbol{x} \oplus \boldsymbol{v}) \oplus \left(m_{i_3}(\boldsymbol{y}) \oplus m_{i_3 \oplus b}(\boldsymbol{y})\right) \left(1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v})\right) \end{aligned}$$

y ahora, analizamos dicha expresión para los diferentes valores de b.

y_1	y_2	$\boldsymbol{x}$	$m_0(\boldsymbol{y})$	$m_1(\boldsymbol{y})$	$m_2(\boldsymbol{y})$	$m_3(\boldsymbol{y})$	$B_{(\mathbf{1},\mathbf{0})}(\boldsymbol{y},\boldsymbol{x})$
$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi} \oplus \boldsymbol{\xi}_{\boldsymbol{u}}$
$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi} \oplus \boldsymbol{\xi}_{\boldsymbol{u}}$
$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\xi}_{\boldsymbol{v}} \oplus \mathbf{1} \oplus \boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}}$
$\mathbf{1}$	$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\xi}_{\boldsymbol{v}} \oplus \mathbf{1} \oplus \boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}}$

Tabla 1: Tabla de verdad de $B_{(\mathbf{1},\mathbf{0})}(\boldsymbol{y},\boldsymbol{x})$

Si $b = 1$, entonces la expresión anterior se convierte en

$$\begin{aligned} B_{(\mathbf{1},\mathbf{0})}(\boldsymbol{y},\boldsymbol{x}) = {} & (m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y}))\,(f(\boldsymbol{x}) \oplus f(\boldsymbol{x}\oplus\boldsymbol{u})) \\ & \oplus (m_{i_2}(\boldsymbol{y}) \oplus m_{i_3}(\boldsymbol{y}))\,(f(\boldsymbol{x}\oplus\boldsymbol{v}) \oplus 1 \oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v}))\,. \end{aligned} \tag{3}$$

Por tanto, si $\mathbf{0}$ y $\mathbf{1}$ son las matrices $2^n \times 1$ con todas las entradas iguales a 0 y 1 respectivamente; $\boldsymbol{\tau}$ es la matriz $2^n \times n$ cuya i-ésima fila es $\boldsymbol{e}_i$; $\boldsymbol{\xi}$, $\boldsymbol{\xi}_{\boldsymbol{u}}$, $\boldsymbol{\xi}_{\boldsymbol{v}}$ y $\boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}}$ son las tablas de verdad de $f(\boldsymbol{x})$, $f(\boldsymbol{x}\oplus\boldsymbol{u})$, $f(\boldsymbol{x}\oplus\boldsymbol{v})$ y $f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})$, respectivamente, entonces, de acuerdo con la expresión (3), la última columna de la tabla 1 corresponde a la tabla de verdad de $B_{(\mathbf{1},\mathbf{0})}(\boldsymbol{y},\boldsymbol{x})$ para $(i_0, i_1, i_2, i_3) = (0, 1, 2, 3)$. Por tanto, la tabla de verdad de $B_{(\mathbf{1},\mathbf{0})}(\boldsymbol{y},\boldsymbol{x})$ tiene cuatro bloques (no necesariamente en ese orden):

$$\boldsymbol{\xi} \oplus \boldsymbol{\xi}_{\boldsymbol{u}} \qquad \boldsymbol{\xi} \oplus \boldsymbol{\xi}_{\boldsymbol{u}} \qquad \boldsymbol{\xi}_{\boldsymbol{v}} \oplus \mathbf{1} \oplus \boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}} \qquad \boldsymbol{\xi}_{\boldsymbol{v}} \oplus \mathbf{1} \oplus \boldsymbol{\xi}_{\boldsymbol{u}\oplus\boldsymbol{v}} \tag{4}$$

que corresponde, para $\boldsymbol{u} \neq \mathbf{0}$, a la tabla de verdad de una función equilibrada, ya que las funciones

$$f(\boldsymbol{x}) \oplus f(\boldsymbol{x}\oplus\boldsymbol{u}) \quad \text{y} \quad f(\boldsymbol{x}\oplus\boldsymbol{v}) \oplus f(\boldsymbol{x}\oplus\boldsymbol{u}\oplus\boldsymbol{v})$$

son, por el teorema 1, equilibradas. Además, para $\boldsymbol{u} = \mathbf{0}$, la expresión (4) se convierte en

$$\mathbf{0} \qquad \mathbf{0} \qquad \mathbf{1} \qquad \mathbf{1}$$

que corresponde a la tabla de verdad de una función equilibrada ya que la longitud de cada bloque es 2^n. Así pues, la función $B_{(\mathbf{1},\mathbf{0})}(\boldsymbol{y},\boldsymbol{x})$ es equilibrada. Lo mismo ocurre para $b = 2$ y $b = 3$.

También, mediante razonamientos análogos, obtenemos que la función $B_{(\boldsymbol{b},\boldsymbol{a})}(\boldsymbol{y},\boldsymbol{x})$ es equilibrada cuando $\boldsymbol{a} \neq \mathbf{0}_n$ y $\boldsymbol{b} = \mathbf{0}_2$ y cuando $\boldsymbol{a} \neq \mathbf{0}_n$ y $\boldsymbol{b} \neq \mathbf{0}_2$. □

4. Contando funciones bent

En esta sección introducimos algunos resultados necesarios para contar el número de funciones bent que podemos construir utilizando el teorema 2. Sin embargo, primero, consideramos tres casos particulares (véase los corolarios 1, 2 y 3 siguientes) que pueden derivarse directamente del teorema 2. El primero de ellos corresponde al caso $\boldsymbol{u} = \boldsymbol{v} = \mathbf{0}$; el segundo, al caso $\boldsymbol{u} = \boldsymbol{v} \neq \mathbf{0}$ y el tercero, al caso $\mathbf{0} \neq \boldsymbol{u} \neq \boldsymbol{v} \neq \mathbf{0}$.

Corolario 1 *Si $f(\boldsymbol{x})$ es una función bent de n variables e (i_0, i_1, i_2, i_3) es cualquier permutación de $(0, 1, 2, 3)$, entonces*

$$F_f(\boldsymbol{y},\boldsymbol{x}) = (m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y}) \oplus m_{i_2}(\boldsymbol{y}))\, f(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y})\,(1 \oplus f(\boldsymbol{x}))$$

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

Corolario 2 *Si $f(\boldsymbol{x})$ es una función bent de n variables, $\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ e (i_0, i_1, i_2, i_3) es cualquier permutación de $(0, 1, 2, 3)$, entonces*

$$G_{f,\boldsymbol{u}}(\boldsymbol{y}, \boldsymbol{x}) = m_{i_0}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus (m_{i_1}(\boldsymbol{y}) \oplus m_{i_2}(\boldsymbol{y}))\, f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_{i_3}(\boldsymbol{y})\, (1 \oplus f(\boldsymbol{x}))$$

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

Corolario 3 *Si $f(\boldsymbol{x})$ es una función bent de n variables, $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$, con $\boldsymbol{u} \neq \boldsymbol{v}$ e (i_0, i_1, i_2, i_3) es una permutación de $(0, 1, 2, 3)$, entonces*

$$H_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}) = m_{i_0}(\boldsymbol{y}) f(\boldsymbol{x}) \oplus m_{i_1}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{u}) \oplus m_{i_2}(\boldsymbol{y}) f(\boldsymbol{x} \oplus \boldsymbol{v}) \oplus m_{i_3}(\boldsymbol{y})\, (1 \oplus f(\boldsymbol{x} \oplus \boldsymbol{u} \oplus \boldsymbol{v}))$$

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

El resultado siguiente establece que las funciones bent obtenidas utilizando el corolario 1 son todas distintas entre sí. La demostración se basa en considerar los 4! casos correspondientes a las distintas permutaciones de $(0, 1, 2, 3)$ y la omitimos por falta de espacio.

Lema 3 *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $F_f(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 1 utilizando $f(\boldsymbol{x})$ y la permutación (i_0, i_1, i_2, i_3) de $(0, 1, 2, 3)$. Supongamos también que $F_g(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 1 utilizando $g(\boldsymbol{x})$ y la permutación (j_0, j_1, j_2, j_3) de $(0, 1, 2, 3)$. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces $F_f(\boldsymbol{y}, \boldsymbol{x}) \neq F_g(\boldsymbol{y}, \boldsymbol{x})$.*

Igual que en el caso anterior, el resultado siguiente establece que las funciones bent obtenidas utilizando el corolario 2 son todas distintas entre sí.

Lema 4 *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $G_{f,\boldsymbol{u}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 2 utilizando $f(\boldsymbol{x})$, el vector $\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y la permutación (i_0, i_1, i_2, i_3) de $(0, 1, 2, 3)$. Supongamos también que $G_{g,\boldsymbol{a}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 2 utilizando $g(\boldsymbol{x})$, el vector $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y la permutación (j_0, j_1, j_2, j_3) de $(0, 1, 2, 3)$. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces $G_f(\boldsymbol{y}, \boldsymbol{x}) \neq G_g(\boldsymbol{y}, \boldsymbol{x})$.*

Sin embargo, no todas las funciones bent construidas de acuerdo con el corolario 3 son distintas entre sí como ponemos de manifiesto en el ejemplo siguiente.

Ejemplo 1 *Supongamos que $n = 2$ y consideremos los vectores $\boldsymbol{u} = (0, 1)$, $\boldsymbol{v} = (1, 0)$ y la función bent $f(\boldsymbol{x}) = m_0(\boldsymbol{x})$. Entonces, de acuerdo con el corolario 3, la expresión (1) y los lemas 1 y 2 tenemos que*

$$\begin{aligned} H_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}) &= m_0(\boldsymbol{y}) m_0(\boldsymbol{x}) \oplus m_1(\boldsymbol{y}) m_1(\boldsymbol{x}) \oplus m_2(\boldsymbol{y}) m_2(\boldsymbol{x}) \oplus m_3(\boldsymbol{y})\, (1 \oplus m_3(\boldsymbol{x})) \\ &= m_0(\boldsymbol{y}, \boldsymbol{x}) \oplus m_5(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{10}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{12}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{13}(\boldsymbol{y}, \boldsymbol{x}) \oplus m_{14}(\boldsymbol{y}, \boldsymbol{x}). \end{aligned}$$

Si ahora consideremos los vectores $\boldsymbol{a} = (0, 1)$ y $\boldsymbol{b} = (1, 1)$ y la función bent $g(\boldsymbol{x}) = m_1(\boldsymbol{x})$, es fácil comprobar que $H_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x}) = H_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$.

Notemos que en el ejemplo anterior $g(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{1})$ y que $\{\boldsymbol{1}, \boldsymbol{2}\}$ y $\{\boldsymbol{1}, \boldsymbol{3}\}$ son bases del mismo subespacio vectorial $\{\boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, \boldsymbol{3}\}$ de $\mathbb{F}_2^n$. Con el objetivo de evitar esta situación, consideraremos sólo vectores $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$ tales que $\{\boldsymbol{u}, \boldsymbol{v}\}$ es una base de Gauss-Jordan de cardinalidad 2. Así, nuestro próximo resultado establece que las funciones bent construidas de acuerdo con el corolario 3 son todas distintas dos a dos si $\{\boldsymbol{u}, \boldsymbol{v}\}$ es una base de Gauss-Jordan de cardinalidad 2 de $\mathbb{F}_2^n$.

Lema 5 *Sean $f(\boldsymbol{x})$ y $g(\boldsymbol{x})$ funciones bent de n variables. Supongamos que $H_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 3 utilizando $f(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{u}, \boldsymbol{v}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$ y la permutación (i_0, i_1, i_2, i_3) de $(0, 1, 2, 3)$. Supongamos también que $H_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 3 utilizando $g(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a}, \boldsymbol{b}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$ y la permutación (j_0, j_1, j_2, j_3) de $(0, 1, 2, 3)$. Si $f(\boldsymbol{x}) \neq g(\boldsymbol{x})$, entonces $H_{f,\boldsymbol{u},\boldsymbol{v}}(\boldsymbol{y}, \boldsymbol{x}) \neq H_{g,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$.*

Nuestro próximo resultado establece que ninguna de las funciones bent obtenidas por alguno de los corolarios 1, 2 y 3, puede ser obtenida por alguno de los otros corolarios implicados.

Lema 6 *Sean $f(\boldsymbol{x})$, $g(\boldsymbol{x})$ y $h(\boldsymbol{x})$ tres funciones bent de n variables (no necesariamente distintas). Supongamos que $F_f(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 1 utilizando $f(\boldsymbol{x})$ y la permutación (i_0, i_1, i_2, i_3) de $(0, 1, 2, 3)$. Supongamos que $G_{g,\boldsymbol{u}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 2 utilizando $g(\boldsymbol{x})$, el vector $\boldsymbol{u} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$ y la permutación (j_0, j_1, j_2, j_3) de $(0, 1, 2, 3)$. Finalmente, supongamos que $H_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ es la función bent construida en el corolario 3 utilizando $h(\boldsymbol{x})$, la base de Gauss-Jordan $\{\boldsymbol{a}, \boldsymbol{b}\}$ de cardinalidad 2 de $\mathbb{F}_2^n$ y la permutación (k_0, k_1, k_2, k_3) de $(0, 1, 2, 3)$. Entonces $F_f(\boldsymbol{y}, \boldsymbol{x}) \neq G_{g,\boldsymbol{u}}(\boldsymbol{y}, \boldsymbol{x})$, $F_f(\boldsymbol{y}, \boldsymbol{x}) \neq H_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$ y $G_{g,\boldsymbol{u}}(\boldsymbol{y}, \boldsymbol{x}) \neq H_{h,\boldsymbol{a},\boldsymbol{b}}(\boldsymbol{y}, \boldsymbol{x})$.*

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 1, 2 y 3.

Teorema 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 1, 2 y 3 es $2^{2n+2}\nu_n$.*

Demostración: De acuerdo con el lema 3, el corolario 1, proporciona $4\nu_n$ funciones bent de $n + 2$ variables. Análogamente, de acuerdo con el lema 4, el corolario 2 proporciona $12\nu_n(2^n - 1)$ funciones bent de $n + 2$ variables. Finalmente, de acuerdo con el lema 5, el corolario 3 proporciona $24\,\nu_n\,N(n, 2)$ 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 [18, pág 46])

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

El resultado se sigue ahora por el lema 6 que garantiza que las funciones bent construidas de acuerdo con los corolarios 1, 2 y 3 son todas distintas entre sí. □

Agradecimientos

Este trabajo ha sido parcialmente subvencionado por el proyecto MTM2008-06674-C02-01 del Ministerio de Ciencia e Innovación del Gobierno de España. Además, la investigación de Verónica Requena ha sido financiada con una ayuda del Vicerrectorado de Investigación, Desarrollo e Innovación de la Universitat d'Alacant destinada a la formación de doctores.

Referencias

[1] C. M. Adams. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes and Cryptography*, **12**: 283–316 (1997).

[2] 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).

[3] A. Canteaut, M. Daum, H. Dobbertin y G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, **154**: 202–218 (2006).

[4] C. Carlet y Y. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, **25**: 263–279 (2002).

[5] 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).

[6] 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.

[7] J. F. Dillon. *Elementary Hadamard Difference Sets*. Tesis Doctoral, University of Maryland, 1974.

[8] K. C. Gupta y P. Sarkar. Improved construction of nonlinear resilient S-boxes. *IEEE Transactions on Information Theory*, **51(1)**: 339–348 (2005).

[9] 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).

[10] M. Matsui. Linear cryptanalysis method for DES cipher. En T. Helleseth (editor), *Advances in Cryptology – EUROCRYPT '93*, volumen 765 de *Lecture Notes in Computer Science*, páginas 386–397. Springer-Verlag, Berlin, 1994.

[11] R. L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, **15**: 1–10 (1973).

[12] 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.

[13] 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.

[14] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, **20**: 300–305 (1976).

[15] 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.

[16] J. Seberry y X.-M. Zhang. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, **9**: 21–35 (1994).

[17] J. Seberry, X.-M. Zhang y Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, **119**: 1–13 (1995).

[18] S. A. Vanstone y P. C. van Oorschot. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 2000.