Saber, Universidad de Oriente, Venezuela.Vol. 27 Nº 4: 565 - 572. (2015)
ISSN: 2343-6468 Digital / Depósito Legal ppi 198702SU4231 ISSN: 1315-0162 Impreso / Depósito Legal pp 198702SU187

NO LINEALIDAD DISTINTA DE CERO EN FUNCIONES BOOLEANAS BALANCEADAS

NONZERO NONLINEARITY IN BALANCED BOOLEAN FUNCTIONS

OSCAR CASTRO PÉREZ, FELICIA VILLARROEL VILLARROEL, DANIEL BRITO QUIJADA

Universidad de Oriente, Núcleo de Sucre, Escuela de Ciencias, Departamento de Matemáticas, Cumaná, Venezuela. E-mail: ocastro@udo.edu.ve / feliciavillarroel@gmail.com / danieljosb@gmail.com

RESUMEN

No todas las funciones booleanas son apropiadas para construir buenas cajas *S* (en el sentido que posean buenas propiedades criptográficas que incluyen: alta no linealidad, balance, alto grado algebraico, resistencia, entre otras). El número de funciones booleanas elegibles de *n* bits de entrada está dado por 2^{2^n} (Rodríguez 2007). Aún para valores moderados de *n*, el espacio de búsqueda es desmesurado. Así, en el presente trabajo, se usan los basamentos que describen al anillo $\mathbb{Z}$ para lograr detallar los conceptos criptográficos de forma tal que originen la construcción de métodos algorítmicos determinísticos para desarrollar patrones que permitan, eficientemente, localizar y descartar algunas funciones booleanas con la propiedad de Balance y con No Linealidad distinta de cero.

PALABRAS CLAVES: anillo de los números enteros, cadena binaria, cajas S, propiedades criptográficas.

ABSTRACT

Not all boolean functions are appropriate for construct good boxes *S* (in the sense having good cryptographic properties including: high nonlinearity, balance, high algebraic degree, resistance, etc). The boolean functions eligible number, with *n* input bits, is 2^{2^n} (Rodríguez 2007). Even for moderate values of *n*, the search space is immense. Thus, in the present work, the bases that describe the ring $\mathbb{Z}$ are used itemize to achieve cryptographic concepts so that originating deterministic algorithmic methods to develop models that allow, efficiently, locate and discard some boolean functions with balance and nonzero nonlinearity.

KEY WORDS: integers ring, binary chain, boxes S, cryptographic properties.

INTRODUCCIÓN

En la Figura 1 se muestra un esquema del proceso de la comunicación; este modelo está basado en el modelo propuesto por Umberto Eco en 1977 y que, a su vez, está íntimamente ligado al modelo propuesto por Claude E. Shannon en 1948 (Rodrigo 2005). En este modelo se plantea la existencia de una multiplicidad de códigos (subcódigos) compartidos entre emisor y receptor para emitir y/o recibir por algún medio, una información en un contexto determinado.

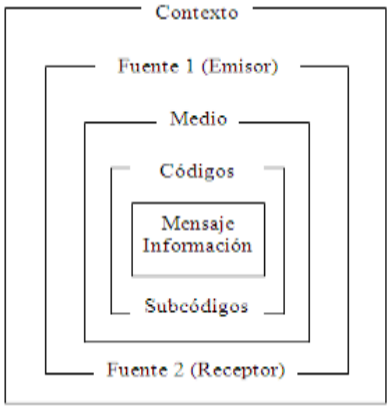

Figura 1. Esquema de la comunicación.

Recibido: noviembre 2014. Aprobado: julio 2015.
Versión final: agosto 2015.

El código es la forma que toma la información que se intercambia entre las fuentes (véase la Figura 1) de un lazo informático. Por ejemplo, el código binario, código fundamental en el que se basan los computadores que sólo consta de combinaciones de *bits* (en particular, 0 ó 1) como impulsos eléctricos y forman la base en la informática para la edición y la lectura de datos (Arredondo 2007).

Usando el esquema de la Figura 1, la *criptología* es la ciencia para el desarrollo y tratamiento de códigos (subcódigos) distintos e inherentes al código común que se maneja en el proceso de la comunicación entre dos fuentes en un contexto determinado. Esto es, el primer objetivo de la criptología es *cifrar*, de modo que ésta sólo sea inteligible únicamente, por el emisor y el receptor, aunque la comunicación entre ambos se dé a en algún contexto y con cualquier medio. El segundo objetivo de la criptología es *descifrar*, hacer inteligible (decodificar), a través del análisis de códigos, cualquier información que se transmita y/o se capte por un medio en un contexto determinado y sea de interés para alguna de las fuentes.

Finalmente, la criptología está dividida en dos grandes ramas: La *criptografía* (diseño del subcódigo, del cifrado del código común y de la clave) el *criptoanálisis* que trata sobre el descifrado del subcódigo, independientemente de si se posee o no la clave (Fernández 2004)

De manera general, en la criptografía, los métodos de cifrado/descifrado están íntimamente ligados, gracias al diseño o tenencia de la clave y pueden clasificarse en dos categorías: criptografía de llave simétrica (el emisor como el receptor usan la misma clave) y criptografía de llave pública (se utilizan más de una clave). En modernos métodos de llave simétrica se emplean, en el proceso de cifrado/descifrado con el uso de la clave, varias *cajas de sustitución S* (una función *s*: $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$, con *n*, $m \in \mathbb{N}$). El presente trabajo se centró en el estudio de dichas cajas, específicamente en un tipo de caja: las *funciones booleanas* (*f*: $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, con $n \in \mathbb{N}$), ya que una caja *S* es una combinación de funciones booleanas f_i: $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, con $i = 1, 2, \ldots, m$ (Rodríguez 2007).

Una forma de representar una función booleana es mediante su *tabla de verdad* o *cadena f*. Resulta suficiente analizar las cadenas para realizar el estudio de las cajas *S*, aunque no todas son apropiadas para construir buenas cajas *S* (en el sentido que posean buenas propiedades criptográficas que incluyen: el Alto Grado Algebraico, Efecto Avalancha, Resistencia, Autocorrelación, entre otras) (Rodríguez 2007), por lo que en el presente trabajo, se demostró que $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$; $\mathbb{Z}_{\prod_{i=1}^{n} m_i}$, un resultado suficiente para exhibir métodos algorítmicos determinísticos que permitieron desarrollar patrones que a su vez, inducen a la localización y exclusión de algunas funciones booleanas con la propiedad de Balance y con No Linealidad distinta de cero; propiciándose una mayor seguridad en la escogencia de las cadenas binarias con Alta no Linealidad, siendo estas bastante útiles en la creación de cajas *S* en los algoritmos cifradores (métodos de cifrado/descifrado).

PREVIOS

De ahora en adelante, considere el orden en el dominio entero $\mathbb{Z}$ y las operaciones en los anillos con identidad $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots, \mathbb{Z}_{m_n}$, (Herstein 2008).

Teorema 2.1. Sea $\{S_n\}_{n \in Z^+}$ en $\mathbb{Z}^+ - \{1\}$, entonces para todo $a \in \mathbb{Z}^+ \cup \{0\}$ y algún $k \in \mathbb{Z}^+$: $a = \sum_{j=1}^{k} r_j q_{j-1}$, con $r_j \in \mathbb{Z}^+ \cup \{0\}$ único, $r_j < s_j$, $q_j = \prod_{i=1}^{j} s_i$ y $q_0 = 1 \; \forall j = 1,2,..,k$.

Demostración. Si $a = 0$ ($a = 1$) entonces para $k = 1$ y $r_1 = 0$ ($k = 1$ y $r_1 = 1$) el teorema es cierto ($\{S_n\}_{n \in Z^+} \subset \mathbb{Z}^+ - \{1\}$, $\mathbb{Z}$ es un dominio entero).

Asimismo, sea $a \in \mathbb{Z}^+$ supóngase cierto el teorema para cualquier *b* en $\mathbb{Z}$, de modo que $1 < b < a$ y considérese el conjunto $A = \{ j \in \mathbb{Z}^+ \cup \{0\} / \; q_j \leq a\}$, el cual es distinto de vacío ($0 \in A$ e hipótesis inductiva). Además, *A* está acotado, superiormente, por *a*, ya que $\forall n \in \mathbb{Z}^+$, $q_n < q_{n+1}$, $n < q_n$ y $1 < s_n \Leftrightarrow 2 \leq s_n$ ($\{S_n\}_{n \in Z^+} \subset \mathbb{Z}^+ - \{1\}$).

Ahora bien, existe $d = maxA$ (consecuencia del *lema de Zorn* y el orden usual en $\mathbb{Z}$), así, $q_d \leq a < q_{d+1}$. Luego, como $q_d \in \mathbb{Z}^+$ ($1 < s_n$, $\forall n \in \mathbb{Z}^+$) existen *h* en $\mathbb{Z}^+$ y $t \in \mathbb{Z}^+ \cup \{0\}$, únicos, tal que $a = q_d h + t$ y $t < q_d$ ($1 < a$ y divisibilidad en $\mathbb{Z}^+$). Además, por hipótesis inductiva, $t < a$ ($q_d \leq a$) y con $m = d$ entonces existe r_j en $\mathbb{Z}$ único, de

modo que $\forall j=1,2,...,d$, $0 \le r_j < s_j$ y $t=\sum_{j=1}^{d} r_j q_{j-1}$, con $q_j = \prod_{i=1}^{j} s_i$ y $q_0 = 1$. Finalmente, considerándose que $q_d h \le a = q_d h + t < q_{d+1}$, $0 < 1 < s_d$ y $q_{d+1} = q_d s_{d+1}$ implica que $h < s_{d+1}$ y con $r_{d+1} = h$, se obtiene $\forall j=1,2,..,d,d+1$: $0 \le r_j < s_j$ y $a = r_{d+1}q_d + \sum_{j=1}^{d} r_j q_{j-1} = \sum_{j=1}^{d+1} r_j q_{j-1}$, con $q_j = \prod_{i=1}^{j} s_i$ y $q_0 = 1$. Así, el teorema queda demostrado para $a \in \mathbb{Z}^+$, con $k = d + 1$.•

El Teorema 2.1 hace referencia a las *bases generalizadas* (Cilleruelo *et al.* 2010). También, garantiza la existencia de una biyección entre a y sus dígitos, lo cual brinda la ventaja de representar al entero a mediante los dígitos $(r_j \in \mathbb{Z}^+ \cup \{0\} \quad \forall j=1,2,..,k)$. Esto es, se puede utilizar la notación de vector, $(r_1, r_2,\ldots, r_k)$, para a. Además, obsérvese que si $1 < b = s_n$, $\forall n \in \mathbb{Z}^+$ entonces se deduce la escritura usual de a en la base b.

Teorema 2.2. $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ es un grupo conmutativo, con $2 < n$,

$\sigma: (\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n})^2 \rightarrow \mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$,

tal que $(x_1, x_2,\ldots, x_n)\ \sigma\ (y_1, y_2,\ldots, y_n) = (z_1, z_2, \ldots, z_n)$, con $x_i, y_i \in \mathbb{Z}_{m_i}$, para todo $i = 1, 2, \ldots, n$, donde $z_i = x_i + y_i + r_i$ $(mod.\ m_i)$ y

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + y_{i+1} + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le x_{i+1} + y_{i+1} + r_{i+1} \end{cases}$$

Demostración. Considérese las hipótesis del teorema $\sigma: (\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n})^2 \rightarrow \mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$ es un operador. También, considerándose que $(x_1, x_2,\ldots, x_n)\ \sigma\ (0, 0,\ldots, 0) = (z_1, z_2,\ldots, z_n)$, con $x_i, 0 \in \mathbb{Z}_{m_i}$, donde $z_i = x_i + 0 + r_i$ $(mod.\ m_i)$ para todo $i=1, 2, \ldots, n$, y

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + 0 + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le x_{i+1} + 0 + r_{i+1} \end{cases}.$$

Esto es, $r_i = 0$ y $z_i = x_i$ $(mod.\ m_i)$ para todo $i = 1, 2,\ldots, n$ y $(x_1, x_2,\ldots, x_n)\ \sigma\ (0,0,\ldots,0) = (x_1, x_2,\ldots, x_n)$. Así, $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ posee neutro $(0, 0,\ldots, 0)$.

Asimismo, para $i = 1,2,\ldots, n$, si $x_i \in \mathbb{Z}_{m_i}$ y $x_i \neq 0$ entonces en $\mathbb{Z}_{m_i}$, existe su opuesto $m_i - x_i$, tal que $x_i + m_i - x_i = 0$ $(mod.\ m_i)$ pero, si $x_i = 0$ entonces es opuesto de sí mismo. Además, $2 < n$ (hipótesis), considere $m_t - x_t \in \mathbb{Z}_{m_j}$ y $m_j - x_j - 1 \in \mathbb{Z}_{m_j}$ para todo $j=1, 2,\ldots, t-1$, con $t = max\{i / x_i \neq 0\}$ (*lema de Zorn*). Luego, $(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_1,\ldots, x_{t-1}, x_t,\ldots, x_n) = (x_1, \ldots, x_{t-1}, x_t, 0, \ldots, 0)$. En consecuencia, $(x_1,\ldots, x_{t-1}, x_t, 0,\ldots,0)\ \sigma\ (m_1 - x_1 - 1,\ldots, m_{t-1} - x_{t-1} - 1, m_t - x_t, 0,\ldots,0) = (z_1,\ldots, z_{t-1}, z_t, 0,\ldots,0)$,
donde $z_j = m_j - 1 + r_j$ $(mod.\ m_j)$ y

$$r_j = \begin{cases} 0, \text{ si } m_{j+1} - 1 + r_{j+1} < m_{j+1} \\ 1, \text{ si } m_{j+1} \le m_{j+1} - 1 + r_{j+1} \end{cases}$$

para todo $j = 1, 2, \ldots, t-2$. Considerándose que en $\mathbb{Z}$, $r_t = 0$ y $z_t = x_t + m_t - x_t + r_t = m_t$, por lo que $r_{t-1} = 1$ y $z_{t-1} = x_{t-1} + m_{t-1} - x_{t-1} - 1 + r_{t-1} = m_{t-1}$, en consecuencia, $r_{t-2} = 1$ y asimismo, $r_j = 1$ para todo $j=1, 2, \ldots, t-1$, ya que recurrentemente, $z_j = m_j$. Esto es, $z_j = 0$ $(mod.\ m_j)$ para todo $j = 1, 2, \ldots, t$ ó $(z_1,\ldots, z_{t-1}, z_t, 0,\ldots,0) = (0,\ldots,0,0,\ldots,0)$. Es decir, existe el opuesto para cada $(x_1, x_2,\ldots, x_{n-1}, x_n)$ en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$.

Finalmente, sean $(x_1, x_2,\ldots,x_n)$, $(y_1,y_2,\ldots,y_n)$, $(z_1,z_2,\ldots,z_n)$ en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$, considérese $[(x_1, x_2,\ldots, x_n)\ \sigma\ (y_1, y_2,\ldots, y_n)]\ \sigma\ (z_1, z_2,\ldots, z_n) = (v_1, v_2,\ldots, v_n)$, donde para cada $i = 1, 2, \ldots, n$: $v_i = (x_i + y_i + r_i) + z_i + s_i = x_i + y_i + z_i + r_i + s_i$ $(mod.\ m_i)$,

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + y_{i+1} + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le x_{i+1} + y_{i+1} + r_{i+1} \end{cases},$$

$$s_i = \begin{cases} 0, \text{ si } (x_{i+1} + y_{i+1} + r_{i+1}) + z_{i+1} + s_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le (x_{i+1} + y_{i+1} + r_{i+1}) + z_{i+1} + s_{i+1} \end{cases}.$$

También, $(x_1, x_2,\ldots, x_n)\ \sigma\ [(y_1, y_2,\ldots, y_n)\ \sigma\ (z_1, z_2,\ldots, z_n)] = (w_1, w_2,\ldots, w_n)$, donde para cada $i = 1, 2, \ldots, n$: $w_i = x_i + (y_i + z_i + t_i) + u_i = x_i + y_i + z_i + t_i + u_i$ $(mod.\ m_i)$, con

$$t_i = \begin{cases} 0, \text{ si } y_{i+1} + z_{i+1} + t_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le y_{i+1} + z_{i+1} + t_{i+1} \end{cases},$$

$$u_i = \begin{cases} 0, \text{ si } x_{i+1} + (y_{i+1} + z_{i+1} + t_{i+1}) + u_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le x_{i+1} + (y_{i+1} + z_{i+1} + t_{i+1}) + u_{i+1} \end{cases}.$$

Además, dada la asociatividad en $\mathbb{Z}_{m_i}$ para cada $i = 1, 2, \ldots, n$: $r_i + s_i = t_i + u_i =$

$$= \begin{cases} 0, \text{ si } (x_{i+1} + y_{i+1} + z_{i+1} + t_{i+1} + u_{i+1} < m_{i+1}) \text{ ó } (i = n) \\ 1, \text{ si } (m_{i+1} \le x_{i+1} + y_{i+1}) \text{ y } (x_{i+1} + y_{i+1} + z_{i+1} + t_{i+1} + u_{i+1} < 2m_{i+1}) \\ 2, \text{ si } 2m_{i+1} \le x_{i+1} + y_{i+1} + z_{i+1} + t_{i+1} + u_{i+1} \end{cases}$$

Note que en para cada $i = 1, 2,\ldots,n$, $x_i + y_i + z_i + t_i + u_i < 3m_i - 3 + 2 = 3m_i - 1$. Así, $v_i = w_i$ para todo $i = 1,2,\ldots,n$. Esto es, en $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ se cumple la propiedad asociativa y hereda la propiedad conmutativa de

cada $\mathbb{Z}_{m_i}$. Por tanto, $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ es un grupo abeliano. •

Teorema 2.3. $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$; $\mathbb{Z}_{\prod_{i=1}^{n} m_i}$.

Siempre y cuando se considere estrictamente a $\mathbb{Z}_{m_i} = \{[a]_{m_i} \subset \mathbb{Z} / a \in \mathbb{Z}, 0 \le a < m_i\} := \{0, 1, 2, \ldots, m_i - 1\}$ para todo $i = 1, 2, \ldots, n$.

Demostración. Considérese la relación f: $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n} \to \mathbb{Z}_{\varphi_1}$, tal que

$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i \varphi_{i+1} \ (mod.\ \varphi_1)$, con $x_i \in \mathbb{Z}_{m_i}$, $\varphi_i = \prod_{j=i}^{n} m_j \ \forall i = 1,2,..,n$ y $\varphi_{n+1} = 1$; f es una función biyectiva (Teorema 2.1); además, observe que

$$f((x_1, x_2, \ldots, x_n)\sigma(y_1, y_2, \ldots, y_n)) =$$

$$= f(z_1, z_2, \ldots, z_n) = \sum_{i=1}^{n} z_i \varphi_{i+1} \ (mod.\ \varphi_1),$$

donde $z_i = x_i + y_i + r_i \ (mod.\ m_i)$ para $i = 1, 2, \ldots, n$, con

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + y_{i+1} + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \le x_{i+1} + y_{i+1} + r_{i+1} \end{cases}$$

Por otro lado, $f(x_1, x_2, \ldots, x_n) + f(y_1, y_2, \ldots, y_n) = \sum_{i=1}^{n} x_i \varphi_{i+1} + \sum_{i=1}^{n} y_i \varphi_{i+1} \ (mod.\ \varphi_1)$. Además, si para todo $i = 1, 2, \ldots, n$ se considera, por hipótesis que estrictamente, $\mathbb{Z}_{m_i} = \{[a]_{m_i} \subset \mathbb{Z} / a \in \mathbb{Z}, 0 \le a < m_i\} := \{0, 1, 2, \ldots, m_i - 1\}$, se obtiene que $x_i + y_i < x_i + y_i + r_i < 2m_i$, $x_i + y_i = \gamma_i^1 m_i + k_i^1$, $x_i + y_i + r_i = \gamma_i^1 m_i + k_i^1 + r_i$, con $0 \le k_i^1 < m_i$, y

$$\sum_{i=1}^{n} x_i \varphi_{i+1} + \sum_{i=1}^{n} y_i \varphi_{i+1} = \sum_{i=1}^{n} (x_i + y_i) \varphi_{i+1} =$$

$$= \sum_{i=1}^{n} \left(\gamma_i^1 m_i + k_i^1\right) \varphi_{i+1} = \gamma_1^1 m_1 \varphi_2 + \sum_{i=1}^{n} \left(k_i^1 + \gamma_{i+1}^1\right) \varphi_{i+1}, \text{ con}$$

$$\gamma_i^1 = \begin{cases} 0, \text{ si } x_i + y_i < m_i \text{ ó } i = n+1 \\ 1, \text{ si } m_i \le x_i + y_i \end{cases}.$$

Analogamente, para $i = 1, 2, \ldots, n$

$$\gamma_1^1 \varphi_1 + \sum_{i=1}^{n} \left(k_i^1 + \gamma_{i+1}^1\right) \varphi_{i+1} = \gamma_1^1 \varphi_1 + \sum_{i=1}^{n} \left(\gamma_i^2 m_i + k_i^2\right) \varphi_{i+1} =$$

$$= \gamma_1^1 \varphi_1 + \gamma_1^2 m_1 \varphi_2 + \sum_{i=1}^{n} \left(k_i^2 + \gamma_{i+1}^2\right) \varphi_{i+1},$$

con $0 \le k_i^1, k_i^2 < m_i$, tal que $k_n^2 = k_n^1$ y

$$\gamma_i^2 = \begin{cases} 0, \text{ si } k_i^1 + \gamma_{i+1}^1 < m_i \text{ ó } i = n, n+1 \\ 1, \text{ si } m_i = k_i^1 + \gamma_{i+1}^1 \end{cases}.$$

Así,

$$\gamma_1^1 \varphi_1 + \gamma_1^2 \varphi_1 + \sum_{i=1}^{n} (k_i^2 + \gamma_{i+1}^2) \varphi_{i+1} = \ldots$$

$$= \sum_{j=1}^{n} \gamma_1^j \varphi_1 + \sum_{i=1}^{n} (k_i^n + \gamma_{i+1}^n) \varphi_{i+1},$$

con $0 \le k_i^j < m_i$, tal que $k_i^j = k_i^{n-i+1}$, si $n - i + 1 < j$ ó $n - j + 1 < i$ para $i, j = 1, 2, \ldots, n$, ya que

$$\gamma_i^j = \begin{cases} 0, \text{ si } k_i^{j-1} + \gamma_{i+1}^{j-1} < m_i \text{ ó } n - j + 1 < i \\ 1, \text{ si } m_i = k_i^{j-1} + \gamma_{i+1}^{j-1} \end{cases}.$$

Es decir, $0 \le k_i^n = k_i^{n-i+1} < m_i$ para $1 < i$ de modo que

$$\sum_{i=1}^{n} (x_i + y_i) \varphi_{i+1} = \sum_{j=1}^{n} \gamma_1^j \varphi_1 + \sum_{i=1}^{n} (k_i^{n-i+1}) \varphi_{i+1}.$$

De forma semejante,

$$\sum_{i=1}^{n} (x_i + y_i + r_i) \varphi_{i+1} = \sum_{j=1}^{n} \gamma_1^j \varphi_1 + \sum_{i=1}^{n} k_i^{n-i+1} \varphi_{i+1} + \sum_{i=1}^{n} r_i \varphi_{i+1}.$$

Esto es,

$$\sum_{j=1}^{n} \gamma_1^j \varphi_1 + \sum_{i=1}^{n} k_i^{n-i+1} \varphi_{i+1} + \sum_{i=1}^{n} r_i \varphi_{i+1} =$$

$$\sum_{j=1}^{n-1} \gamma_1^j \varphi_1 + \sum_{i=1}^{n} \left(k_i^{n-i+1}\right) \varphi_{i+1} + \gamma_1^n m_1 \varphi_2 + \sum_{i=1}^{n-1} r_i m_{i+1} \varphi_{i+2} + r_n$$

como $r_n = 0$ se obtiene

$$\sum_{i=1}^{n} (x_i + y_i + r_i) \varphi_{i+1} = \sum_{j=1}^{n-1} \gamma_1^j \varphi_1 + \left(k_1^n + \gamma_1^n m_1\right) \varphi_2 +$$

$$+ \sum_{i=2}^{n} \left(k_i^{n-i+1} + r_{i-1} m_i\right) \varphi_{i+1}.$$

Luego, por la unicidad de los coeficientes de cada término de la serie finita en $\mathbb{Z}_{\varphi_1}$ (hipótesis y Teorema 2.1), se tiene

$$\sum_{i=1}^{n} (x_i + y_i) \varphi_{i+1} = \sum_{i=1}^{n} \left(k_i^{n-i+1}\right) \varphi_{i+1} \ (mod.\ \varphi_1)$$

$$= \sum_{i=1}^{n} \left(k_i^{n-i+1} \ (mod.\ m_i)\right) \varphi_{i+1} \ (mod.\ \varphi_1).$$

También, para $i = 1, 2, \ldots, n$, $z_i = x_i + y_i + r_i \ (mod.\ m_i)$ se tiene

$$\sum_{i=1}^{n}(z_i)\varphi_{i+1} = \sum_{i=1}^{n}\left(k_i^{n-i+1}\ (mod.\ m_i)\right)\varphi_{i+1}\ (mod.\ \varphi_1).$$

Por tanto, $f((x_1, x_2,\ldots, x_n)\ \sigma\ (y_1,y_2,\ldots, y_n)) = f(x_1, x_2, \ldots, x_n) + f(y_1, y_2, \ldots, y_n)$. Esto es f es un homomorfismo y $(\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}, \alpha)$; $\mathbb{Z}_{\prod_{i=1}^{n} m_i}$.•

Notación. De ahora en adelante, para $j = 1, 2,\ldots, n$, se representará a $x^k \in \mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}$, como $x^k = \left(x_1^k, x_2^k,\ldots,x_n^k\right) := x_1^k x_2^k \ldots x_n^k$, con $n \in \mathbb{Z}^+$, $k := (x^k)_{10} = (x_1, x_2, \ldots, x_n)_{10} \in \mathbb{Z}_{\prod_{j=1}^{n} m_j}$ y $x_j^k \in \mathbb{Z}_{m_j}$ y a $x_1^k x_2^k \ldots x_n^k$ se le denominará la *cadena* de k ó x^k, indistintamente y a los elementos x_j^k de la cadena k se les denominará *componentes*.

Definición 2.1. Sea $n \in \mathbb{Z}^+$, la *tabla de vedad* o *cadena binaria* de una función booleana $f:\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ es una cadena f^k para algún $k \in \mathbb{Z}_{2^{2^n}}$, tal que: $f^k = f(x^1)\ f(x^2)\ldots f(x^{2^n})$ siempre y cuando $(f^k)_{10} = k$ y $(x^1)_{10} < (x^2)_{10} <\ldots < (x^{2^n})_{10}$, considerando que $x^i \in \mathbb{Z}_2^n$, $x^i = \left(x_0^i, x_1^i,\ldots,x_{n-1}^i\right)$, con $x_j^i \in \mathbb{Z}_2$, $i = 1, 2,\ldots, 2^n$ y $j = 0, 1,\ldots, n-1$.

Así, una caja S, g: $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$, con $n, m \in \mathbb{Z}^+$ es la matriz o el arreglo $G = \left(g_{i,j}\right)_{2^n \times m}$, tal que para $i = 1, 2,\ldots, 2^n$, $x^i \in \mathbb{Z}_2^n$ y $g(x^i) = \left(x_1^i, x_2^i,\ldots,x_m^i\right)$, con $x_j^i \in \mathbb{Z}_2$ y $j = 1, 2, \ldots, m$ de modo que $g_{i,j} := f_j(x^i) := x_j^i$, siempre y cuando $(x^1)_{10} < (x^2)_{10} < \ldots <(x^{2^n})_{10}$ dado que $(x^j)_{10} := x_0^j 2^{n-1} + x_1^j 2^{n-2} + \ldots + x_{n-1}^j 2^0$

Teorema 2.4. (Rodríguez 2007). El número de cajas S, g: $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$, con $n, m \in \mathbb{Z}^+$, es 2^{m2^n} .

Definición 2.2. (González 2002). Sean $n \in \mathbb{Z}^+$, $k_1, k_2 \in \mathbb{Z}_{\prod_{j=1}^{n} m_j}$ x^{k_1}, x^{k_2} en $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}$, con $x^{k_1} = x_1^{k_1} x_2^{k_1} \ldots x_n^{k_1}$, $x^{k_2} = x_1^{k_2} x_2^{k_2} \ldots x_n^{k_2}$ y $x_j^{k_1}$, $x_j^{k_2}$ en $\mathbb{Z}_{m_j}$ para j=1,2, …, n, la *distancia Hamming* entre las dos cadenas x^{k_1} y x^{k_2} es

$$d(x^{k_1}, x^{k_2}) := d(k_1, k_2) := \left|\{ j \in \mathbb{Z}^+ / x_j^{k_1} \neq x_j^{k_2} \}\right|.$$

Definición 2.3. (González 2002). Sean $n \in \mathbb{Z}^+$ y $k \in \mathbb{Z}_{\prod_{j=1}^{n} m_j}$, x^k en $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}$, el *peso Hamming* de la cadena x^k es $P(x^k) := P(k) := d(x^k, x^0)$.

Definición 2.4. Sean $n \in \mathbb{Z}^+$, $\varphi_1 = \prod_{j=1}^{n} m_j$ y $k_1, k_2 \in \mathbb{Z}_{\varphi_1}$ para dos cadenas x^{k_1}, x^{k_2} en $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}$, x^{k_1} es *complemento* de x^{k_2} *sii* $x^{k_1}\ \sigma\ x^{k_2} = x^{\varphi_1 - 1}$.

Teorema 2.5. Sean $n \in \mathbb{Z}^+$, $k_1, k_2 \in \mathbb{Z}_{\prod_{j=1}^{n} m_j}$ y respectivamente, las cadenas x^{k_1}, x^{k_2} en $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}$, entonces la distancia Hamming entre $x^{k_1} = x_1^{k_1} x_2^{k_1} \ldots x_n^{k_1}$, $x^{k_2} = x_1^{k_2} x_2^{k_2} \ldots x_n^{k_2}$ es

$$d(x^{k_1}, x^{k_2}) = \sum_{j=1}^{n} p\left(x_j^{k_1} - x_j^{k_2}\right), \text{ tal que}$$

$$p\left(x_j^{k_1} - x_j^{k_2}\right) = \begin{cases} 0, \text{ si } x_j^{k_1} - x_j^{k_2} = 0 \\ 1, \text{ si } x_j^{k_1} - x_j^{k_2} \neq 0 \end{cases}$$

donde $x_j^{k_1} - x_j^{k_2}$ es la diferencia usual en $\mathbb{Z}$ de las componentes de cada cadena para todo $j = 1, 2, \ldots, n$.

Demostración. Sean $n \in \mathbb{Z}^+$, $k_1, k_2 \in \mathbb{Z}_{\varphi_1}$, con $\varphi_1 = \prod_{j=1}^{n} m_j$, tal que $0 < k_1 < k_2$, $k_1, k_2 \in \mathbb{Z}_{\varphi_1}$, y las cadenas x^{k_1}, x^{k_2} en $(\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots,\mathbb{Z}_{m_n}, \sigma)$, de modo que $x^{k_1} = x_1^{k_1} x_2^{k_1} \ldots x_n^{k_1}$, $x^{k_2} = x_1^{k_2} x_2^{k_2} \ldots x_n^{k_2}$ y $x_j^{k_1}$, $x_j^{k_2} \in \mathbb{Z}_{m_j}$ para $j = 1, 2, \ldots, n$ la distancia Hamming entre x^{k_1}, x^{k_2} es $d(x^{k_1}, x^{k_2}) = d(k_1, k_2) = \left|\{ j \in \mathbb{Z}^+ / x_j^{k_1} \neq x_j^{k_2} \}\right|$ (Definición 2.2). También considérese la diferencia usual en $\mathbb{Z}$ de las componentes de cada cadena para toda $j = 1, 2, \ldots, n$, específicamente:

$$\left|\{ j \in \mathbb{Z}^+ / x_j^{k_1} \neq x_j^{k_2} \}\right| = \left|\{ j \in \mathbb{Z}^+ / x_j^{k_1} - x_j^{k_2} \neq 0\}\right|.$$

Luego, sea $A_0 = \{j \in \mathbb{Z}^+ / x_j^{k_1} - x_j^{k_2} \neq 0\}$ entonces la función de conjunto $|A_0|$, cuenta sólo los elementos j, tal que a

$x_j^{k_1} - x_j^{k_2} \neq 0$ pero $j \in \{1, 2, \ldots, n\} = A_0 \cup A_0^c$, con $A_0^c = \{ j \in \mathbb{Z}^+ / x_j^{k_1} - x_j^{k_2} = 0\}$. Entonces asígnesele uno (1) a todos los elementos de A_0 y cero (0) al resto de los elementos que no están A_0 (que están A_0^c). Esto es, defínase $d(x^{k_1}, x^{k_2}) = \sum_{j=1}^{n} p\left(x_j^{k_1} - x_j^{k_2}\right)$, tal que

$$p\left(x_j^{k_1} - x_j^{k_2}\right) = \begin{cases} 0, \text{ si } x_j^{k_1} - x_j^{k_2} = 0 \\ 1, \text{ si } x_j^{k_1} - x_j^{k_2} \neq 0 \end{cases}. \bullet$$

En particular, considerándose la Definición 2.1, la Definición 2.2 y el Teorema 2.5, la distancia Hamming y el peso Hamming se reducen, en $\mathbb{Z}$, a

$$d(x^k, x^{k_1}) = \sum_{j=1}^{n} \left| x_j^k - x_j^{k_1} \right| \text{ y } P(x^k) = \sum_{j=1}^{n} x_j^k .$$

Así, dichas expresiones se pueden usar para determinar el peso Hamming y la distancia Hamming en el grupo de las cadenas binarias de las funciones booleanas.

Definición 2.5. (Rodríguez 2007). Se dice que una función booleana de *n* variables está balanceada, si su cadena binaria f^k, con $k \in \mathbb{Z}_{2^{2^n}}$, contiene un número igual de ceros y unos.

Teorema 2.6. Sean *n*, $m \in \mathbb{Z}^+$ y $k \in \mathbb{Z}_{2^n}$, x^k en $\mathbb{Z}_2^n$, la cadena x^k es *balanceada sii* $P(x^k) = k$ y $n = 2m$.

Teorema 2.7. (Rodríguez, 2007). El número de funciones booleanas balanceadas de *n* variables es $\binom{2^n}{2^{n-1}}$.

Definición 2.6. (Rodríguez 2007) Sean $x^k \in \mathbb{Z}_2^n$, con $n \in \mathbb{Z}^+$ y $k \in \mathbb{Z}_{2^n}$, la suma *xor* de productos *and* entre la cadena x^k fija y cualquier cadena $x^i \in \mathbb{Z}_{2^n}$ se expresa, para todo $i \in \mathbb{Z}_{2^n}$, como $L_{x^k}^n\left(x^i\right) = L_k^n(i) := \sum_{j=1}^{n}\left(x_j^k x_j^i\right) mod.\, 2$, tal que $x^k = x_1^k x_2^k \ldots x_n^k$, $x^i = x_1^i x_2^i \ldots x_n^i$, y $x_j^k, x_j^i \in \mathbb{Z}_2$ para $j = 1,2, \ldots, n$.

Definición 2.7. (Rodríguez 2007). La función booleana que tiene la misma cadena binaria que alguna $L_k^n(i)$ se denomina función booleana *lineal*. El conjunto de las funciones booleanas *lineales* se denota por L_B^n.

Definición 2.8. (Rodríguez 2007). El conjunto de complementos de las funciones booleanas lineales se denota por $L_{B^c}^n$. Así, el conjunto de las funciones booleanas *afines* es $A_B^n := L_B^n \cup L_{B^c}^n$.

Definición 2.9. (Rodríguez 2007). Sean *k*, $k_1 \in \mathbb{Z}_{2^{2^n}}$, la *no linealidad* de una función booleana f^k está expresada como $N_L(f^k) = N_L(k) := min\{d(f^k, f^{k_1}) / f^{k_1} \in A_B^n\}$.

RESULTADOS

Algoritmos de búsquedas de funciones booleanas balanceadas y lineales:

A. Algoritmo que construye todas las cadenas del grupo $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ *a partir de los elementos de* $\mathbb{Z}_{\prod_{i=1}^{n} m_i}$.

Sean $n, m_1, m_2, \ldots, m_n \in \mathbb{Z}^+ - \{1\}$

1) [Inicio] Para $r = 1, 2, \ldots, n + 1$, Calcúlese $\varphi_r = \prod_{j=r}^{n} m_j$, $\varphi_{n+1} = 1$.

2) Se inicializa $k := 0$.

3) Para $r = 1, 2, \ldots, n + 1$, se calcula c_r de modo que $k = c_r\varphi_r + s$, con $0 \leq s < \varphi_r$.

4) Para $j = 1, 2, \ldots, n$, cada componente, $x_j^k \in \mathbb{Z}_{m_j}$, de la cadena x^k en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$ se obtiene: $x_j^k := c_{j+1} - m_j c_j$.

5) Se repiten los pasos tres (3) y cuatro (4) para $k = 1, 2, \ldots, \varphi_1 - 1$.

6) [Fin] $x^k = x_1^k x_2^k \ldots x_n^k$ para $k \in \mathbb{Z}_{\prod_{i=1}^{n} m_i}$ son todas las cadenas en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ \ldots \ x \mathbb{Z}_{m_n}$.

B. Algoritmo que haya todas cadenas balanceadas del grupo $(\mathbb{Z}_2^n, \sigma)$*, con "n" un entero par, a partir de los elementos de* $\mathbb{Z}_{2^n}$.

Sea $n = 2m$, con $m \in \mathbb{Z}^+$.

1) [Inicio] Para cada $k \in \mathbb{Z}_{2^n}$, se construye la cadena binaria $x^k = x_1^k x_2^k ... x_n^k$ en $\mathbb{Z}_2^n$ con el Algoritmo A.
2) Por cada $k \in \mathbb{Z}_{2^n}$, calcúlese el peso Hamming de cada cadena binaria $x^k = x_1^k x_2^k ... x_n^k$ de modo que

$$P(x^k) = \sum_{j=1}^{n} x_j^k .$$

3) Constrúyase el conjunto $B = \{ x^k \in \mathbb{Z}_2^n \ / \ k \in \mathbb{Z}_{2^n}$ y $P(x^k) = 2^{n-1}\}$.
4) [Fin] Cada elemento de B son las cadenas binarias balanceadas de $\mathbb{Z}_2^n$.

C. Algoritmo que haya todas las cadenas binarias de las funciones booleanas afines de $\mathbb{Z}_2^n$ en $\mathbb{Z}_2$ del grupo $(\mathbb{Z}_2^{2^n}, \sigma)$, a partir de los elementos de $\mathbb{Z}_{2^{2^n}}$.

Sea $m = 2^n$, con $n \in \mathbb{Z}^+$.
1) [Inicio] Para cada $k \in \mathbb{Z}_{2^m}$, se construye la cadena binaria $x^k = x_1^k x_2^k ... x_m^k$ en $\mathbb{Z}_2^m$ con el Algoritmo A.
2) Para cada $i \in \mathbb{Z}_m$, se construye la cadena binaria $y^i = y_1^i y_2^i ... y_n^i$ en $\mathbb{Z}_2^n$ con el Algoritmo A.
3) Se inicializa $A = \emptyset$.
4) Se inicializa $i = 0$.
5) Se calcula para cada $s \in \mathbb{Z}_m$,

$$L_{y^i}^n(y^s) = \sum_{j=1}^{n} (y_j^s y_j^i) \ mod. \ 2 .$$

6) Se localiza la cadena binaria $x^{k_i} = L_{y^i}^n(y^0) L_{y^i}^n(y^1) ... L_{y^i}^n(y^m)$ en $\mathbb{Z}_2^m$, tal que $k_i = (x^{k_i})_{10}$.
7) Se localiza la cadena binaria $x^{2^m - k_i - 1}$ en $\mathbb{Z}_2^m$.
8) Se construye el conjunto $A := A \cup \{ x^{k_i}, x^{2^m - k_i - 1} \}$
9) Se repiten los pasos cinco (5), seis (6), siete (7) y ocho (8) para $i = 1, 2, \ldots, 2^n - 1$.
10) [Fin] $A_B^n := A$.

Análisis de los conjuntos obtenidos en los algoritmos A, B y C. (aseveraciones y conjeturas):

Teorema 3.1. (Aseveración 1). Si una cadena Binaria es balanceada su complemento también lo es.

Demostración. Sean las cadenas binarias x^k, $x^{k_1} \in \mathbb{Z}_2^n$, con $n = 2m$, $m \in \mathbb{Z}^+$ y $k, k_1 \in \mathbb{Z}_{2^n}$, tal que $x^k = x_1^k x_2^k ... x_n^k$, $x^{k_1} = x_1^{k_1} x_2^{k_1} ... x_n^{k_1}$, y $x_j^k, x_j^{k_1} \in \mathbb{Z}_2$ para $j = 1, 2, \ldots, n$.
Primeramente, considere que $1 - x_j^k \in \mathbb{Z}_2$ para todo $j = 1, 2, \ldots, t-1$, con $t = max\{ j \ / \ x_j^k = 1\}$ (*lema de Zorn*). Luego, $x^k = x_1^k x_2^k ... x_n^k = x_1^k x_2^k ... x_{t-1}^k 10...0$, y su opuesto es $x^{2^n - k} = (1 - x_1^k, ..., 1 - x_{t-1}^k, 1, 0, ..., 0)$ (Teorema 2.2). Y por Teorema 2.3 y la Definición 2.4 se tiene: $x^k \sigma x^{k_1} = x^{2^n - 1}$ <=> $x^{k_1} = x^{2^n - 1} \sigma x^{2^n - k} = x^{2^n - 1 - k \ (mod. \ 2^n)}$.

Por otro lado, $x^{2^n - 1} = 11\ldots1$. Así, similarmente por el Teorema 2.2 y el Teorema 2.3 se tiene: $x^{2^n - 1} \sigma x^{2^n - k} = (1 - x_1^k, 1 - x_2^k, ..., 1 - x_{t-1}^k, 0, 1, ..., 1)$. Esto es, al contar las componentes en la cadena $x^{2^n - 1 - k}$, $n - t$ componentes no son ceros y como $P(x^k) = m$ entonces $| \{ j / 1 - x_j^k = 1 \} | = m - (n - t)$, por lo que $P(x^{k_1}) = P(x^{2^n - 1 - k}) = m$ (Teorema 2.5 y Teorema 2.6). •

Conjetura 1. Las funciones booleanas afines para cualquier $n \in \mathbb{Z}^+$, distintas a $L_{x^0}^n(x^i)$ y su complemento, son funciones booleanas balanceadas. Así, las funciones booleanas balanceadas, con no linealidad distinta de cero, se obtienen extrayendo las funciones lineales distintas a $L_{x^0}^n(x^i)$ del conjunto de las funciones booleanas balanceadas.

Teorema 3.2. (Aseveración 3). Sean $k, l \in \mathbb{Z}_m$, con $m = 2^n$ y $n \in \mathbb{Z}^+$ entonces x^k, $x^l \in \mathbb{Z}_2^m$ son la primera y última cadena binaria (respetando el orden usual de los enteros en $\mathbb{Z}_{2^m}$) en el conjunto de las cadenas de las funciones booleanas balanceadas *sii* $k = 2^{2^{n-1}} - 1$ y $l = 2^{2^n} - 2^{2^{n-1}}$.
Demostración. Sean $k, l \in \mathbb{Z}_m$, con $m = 2^n$ y $n \in \mathbb{Z}^+$ entonces x^k, $x^l \in \mathbb{Z}_2^m$, tal que $x^k = x_1^k x_2^k ... x_{2^n}^k$, $x^l = x_1^l x_2^l ... x_{2^n}^l$, y $x_j^k, x_j^l \in \mathbb{Z}_2$ para $j = 1, 2, \ldots, 2^n$. Considérese el Teorema 2.3 entonces

$$x_j^k = \begin{cases} 0, \text{ si } j \le 2^{n-1} \\ 1, \text{ si } 2^{n-1} < j \end{cases}$$

forma una cadena binaria balanceada *sii* $k = 2^{2^{n-1}} - 1$. Por la Definición 2.4, el Teorema 2.4 y el Teorema 3.1, x^k, x^l, con $l = 2^{2^n} - 2^{2^{n-1}}$ son la primera y última cadena binaria (respetando el orden usual de los enteros en $\mathbb{Z}_{2^n}$) en el conjunto de las cadenas de las funciones booleanas balanceada.•

Conjetura 2. Sea $n \in \mathbb{Z}^+ - \{1\}$ entonces las primeras $2^{n-2}\left(2^{n-1}+3\right)+1$ funciones balanceadas son $k_0 = 2^{2^{n-1}} - 1$ y $k_l = k_{l-1} + d_l$, con $l = 1, 2, \ldots, r_{2^{n-1}}+1$, donde $d_{r_i+j_i} = 2^{2^{n-1}-(i+j_i)}$, $d_{r_{i+1}-1} = d_{r_i} + d_{r_{i+1}-2}$, $d_{r_{2^{n-1}}} = 1$ y $d_{r_{2^{n-1}}+1} = 2$, tal que $r_i = (i-1)\left(2^{n-1}+1\right) + \frac{i}{2}(3-i)$ y $r_{2^{n-1}} = 2^{n-2}\left(2^{n-1}+3\right) - 1$ para $i = 1, 2, \ldots, 2^{n-1} - 1$ y $j_i = 0, 1, \ldots, r_{i+1} - r_i - 2$.

CONCLUSIONES

Se demostró sin usar el Algoritmo de Euclides para la División Entera, la generalización de la escritura única de un entero cómo la suma de productos de elementos de una sucesión en $\mathbb{Z}^+ - \{1\}$ no necesariamente geométrica (base generalizada, véase el Teorema 2.1); lo cual fue necesario para introducir una nueva operación en el producto cartesiano entre conjuntos de clases de equivalencia de $\mathbb{Z}$ (dada la partición generada por la relación de equivalencia congruencia modulo en $\mathbb{Z}$, véase el Teorema 2.2), obteniéndose, así el isomorfismo del Teorema 2.3. Además, se hizo énfasis en el uso de cadenas binarias y el isomorfismo $\mathbb{Z}_{2^k}$; $(\mathbb{Z}_2^k, \sigma)$, con $k \in \mathbb{Z}^+$, para organizar a las funciones booleanas y estudiar el balanceo y la no linealidad como buenas propiedades criptográficas (véase las definiciones establecidas en la sección 2), desarrollándose tres algoritmos determinísticos, que al ser empleados se generaron tres aseveraciones y tres conjeturas, las cuales, a su vez sustentan la teoría de que el conjunto de las funciones booleanas balanceadas con no linealidad distinta de cero es el conjunto diferencia entre las funciones booleanas balanceadas y el conjunto de las funciones booleanas lineales, al respecto se propicia la caracterización de las funciones booleanas balanceadas, lo cual manifiesta una probable debilidad del uso de este tipo de funciones para construir cajas *S* (véase la Conjetura 1, el Teorema 3.2 y la Conjetura 2).

REFERENCIAS

ARREDONDO T. 2007. ELO211: Sistemas Digitales, 1er Semestre – 2000. Chile. Disponible en línea: http://profesores.elo.utfsm.cl/~tarredondo/info/digital-systems/2Funciones%20Booleanas.pdf (Acceso 08.07.2010).

CILLERUELO J. KISS S. RUZSA I. VINUESA C. 2010. Generalization of a theorem of Erdos and Renyi on Sidon sets. Rand. Struct. and Alg.37(4): 455-464.

FERNÁNDEZ S. 2004. La Criptografía Clásica. España. Disponible en línea: http://www.hezkuntza.ejgv.euskadi.net/r43573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografi_clasica.pdf (Acceso: 13/12/2010).

GONZÁLEZ M. 2002. Códigos Reed-Muller sobre Ciertos Subconjuntos del Espacio Proyectivo. Ciudad de México, D.F: Universidad Autónoma Metropolitana Iztapalapa, División de Ciencias Básicas e Ingeniería. [Disertación Doctorado en Ciencias Especialidad en Matemáticas], pp 42.

HERSTEIN I. 2008. Álgebra Moderna. Trillas. México D.F., México, pp. 384.

RODRIGO M. 2005. Modelos de la Comunicación. España. Disponible en línea: http://www.portalcomunicacion.com/esp/pdf/aab_lec/20.pdf (Acceso: 01/12/2010).

RODRÍGUEZ F. 2007. De la Búsqueda de Funciones Booleanas con Buenas Propiedades Criptográficas. México. Disponible en línea: http://delta.cs.cinvestav.mx/~francisco/cajass.pdf (Acceso: 28/05/2010).