REVISTA MATEMÁTICA COMPLUTENSE
(2000) vol. XIII, num. 1, 119-134
http://dx.doi.org/10.5209/rev_REMA.2000.v13.n1.17093
ISNN 1139-1138

SOBRE EL PARÁMETRO COMPLEJIDAD LINEAL Y LOS FILTROS NO LINEALES DE SEGUNDO ORDEN

A. FÚSTER SABATER and
L.J. GARCÍA VILLALBA

Abstract

A new method of analysing the linear complexity of $2nd-$order nonlinear filterings of m-sequences that is based on the concept of regular coset is presented. The procedure considers any value of the LFSR's length, L, (prime or composite number). Emphasis is on the geometric interpretation of the *regular cosets* which produce degeneracies in the linear complexity of the filtered sequence. Numerical expressions to compute the linear complexity of such sequences are given as well as practical rules to design $2nd-$order nonlinear filterings which preserve the maximal linear complexity are stated.

1 Introducción

El filtrado no lineal de m-secuencias [5] es un método ampliamente utilizado para la generación de secuencias pseudoaleatorias de aplicación en Criptografía, códigos correctores de errores, transmisiones con módem, teoría de números, etc. En términos generales, se considera que las secuencias obtenidas de esta forma cuentan con un período largo y un elevado valor de complejidad lineal, parámetro éste que da una medida de su impredecibilidad. Sin embargo, en la práctica, no se conoce un método eficaz para determinar ni la complejidad lineal ni el período de la secuencia generada por un filtro no lineal arbitrario aplicado a las L etapas de un Registro de Desplazamiento Realimentado Linealmente [5] (ó LFSR, del inglés Linear Feedback Shift-Register). En cualquier caso, sí se pueden reseñar unas cuantas referencias bibliográficas básicas que

1991 Mathematics Subject Classification: 11K45, 94A55.
Servicio de Publicaciones. Universidad Complutense. Madrid, 2000

consideran este problema: Groth [6] presentó la complejidad lineal como un parámetro controlable que se incrementaba con el orden de la función de filtrado. El autor aplicó funciones booleanas de segundo grado a las etapas de un LFSR con polinomio de conexión primitivo. El valor de la complejidad lineal de la secuencia resultante se incrementaba a medida que el procedimiento se repetía de forma iterativa. Sin embargo, en su trabajo no hay ninguna mención explícita a las degeneraciones (disminuciones) que puede haber en el valor de la complejidad lineal de la secuencia filtrada. Key [7] dio una cota superior al valor de la complejidad lineal de las secuencias obtenidas a partir de un filtro no lineal de orden k. Más aun, Key señaló que un producto de dos fases (etapas) distintas de la misma m-secuencia nunca degeneraba aunque, como más tarde puntualizó Rueppel [11], este resultado quedaba restringido a diferencias de fase menores que la longitud del LFSR. Haciendo uso de la transformada de Fourier discreta, Massey [10] demostró que el resultado de la no degeneración de productos de orden dos dado por Key se verificaba para cualquier elección arbitraria de la diferencia de fases, siempre que la longitud L del LFSR fuera un número primo.

En este trabajo, se desarrolla un nuevo método para calcular la complejidad lineal de las secuencias obtenidas a partir de un filtro no lineal de segundo orden aplicado a una m-secuencia. El procedimiento se basa en el concepto de *coset regular* y considera cualquier elección de L (ya sea número primo o compuesto). Si L es número primo, del procedimiento aquí desarrollado se deduce el mismo resultado probado por Massey. Si L es un número compuesto, se determinan las diferencias de fase que van a producir una disminución en la complejidad lineal de la secuencia filtrada; asimismo se señalan los *cosets* que van a degenerar y, en consecuencia, el valor de la complejidad lineal de la secuencia producto. Por último, se dan una serie de reglas prácticas para seleccionar las diferencias de fase que preservan la cota superior de complejidad lineal dada por Key.

El trabajo está organizado tal y como sigue: en la sección segunda se introducen algunos conceptos básicos y definiciones, en particular el concepto de *coset regular* que es el pilar sobre el que se sustenta este trabajo. La sección tercera describe en detalle la forma particular de los coeficientes asociados con los diferentes *cosets* de peso dos y uno. En la sección cuarta se da una interpretación geométrica de los *cosets*

regulares, que son los que originan la disminución cuantitativa de la complejidad lineal de la secuencia filtrada. Por último, en la sección 5 se presentan las conclusiones de este trabajo.

2 Conceptos Básicos y Notación Utilizada

En esta sección se introduce cierta notación específica y diferentes conceptos básicos que se utilizarán a lo largo de todo el trabajo:

$\{a_n\}$ es la secuencia binaria de salida de un LFSR de L etapas con polinomio de conexión primitivo [5], por tanto $\{a_n\}$ es una $m-$secuencia de período $2^L - 1$. α es una raíz del polinomio característico del LFSR a la vez que un elemento primitivo de $GF(2^L)$. En lo sucesivo y sin pérdida de generalidad, se asumirá que $\{a_n\}$ está en su fase característica, es decir, el elemento genérico a_n puede escribirse como [7]

$$a_n = \sum_{i=0}^{L-1} \alpha^{2^i n} \tag{2.1}$$

F denota un filtro no lineal de segundo orden aplicado a las L etapas del LFSR, es decir, F es el producto de dos fases distintas de la secuencia $\{a_n\}$, $a_{n+t_0} \cdot a_{n+t_1}$, donde t_0, t_1 son números enteros que verifican $0 \leq t_0 < t_1 < 2^L - 1$.

$\{z_n\}$ es la secuencia obtenida a la salida del filtro no lineal F.

El elemento genérico de esta secuencia, notado z_n, puede escribirse $z_n = a_{n+t_0} \cdot a_{n+t_1}$.

Definición 1. *Sea Z_{2^L-1} el conjunto de números enteros $[1, \ldots, 2^L - 1]$, se considera la siguiente relación de equivalencia, denotada por R_e, definida sobre sus elementos: e_1 R_e e_2 con e_1, $e_2 \in Z_{2^L-1}$ si existe un entero j, $0 \leq j < L$, tal que*

$$2^j \cdot e_1 = e_2 \bmod (2^L - 1) \tag{2.2}$$

R_e divide al conjunto Z_{2^L-1} en clases de equivalencia que denominaremos[1] *cosets ciclotómicos* mod $(2^L - 1)$.

[1] A lo largo de este trabajo utilizaremos el término *coset* en lugar de clase de equivalencia por seguir la notación habitual encontrada en la literatura.

El elemento líder del *coset ciclotómico* E, notado e, es el menor entero dentro de dicha clase de equivalencia. Un *coset ciclotómico* E queda unívocamente caracterizado por su elemento líder. El cardinal de cada *coset ciclotómico* E es L o un divisor propio de L (excepto el *coset* 0 cuyo cardinal es 1). Todos los elementos de un *coset ciclotómico* tienen el mismo peso binario, es decir, el mismo número de unos en su representación binaria.

A continuación se introduce un tipo particular de *cosets ciclotómicos,* los denominados *cosets regulares.* Dichos *cosets* fueron estudiados primeramente por Caballero [1] y se defininen de la siguiente manera:

Definición 2. *Un* **coset ciclotómico** $\bmod (2^L-1)$ *se denomina* **coset regular** *si su cardinal* m *es un divisor propio de* L. *En efecto, un* **coset regular** R*-es un conjunto de enteros de la forma* $\{r, r\cdot 2, r\cdot 2^2, ..., r\cdot 2^{m-1}\} \bmod (2^L-1)$, *donde el menor entero positivo* m *que satisface*

$$r\cdot 2^m \equiv r \bmod (2^L-1) \tag{2.3}$$

es un divisor propio de L.

En términos binarios, un *coset regular* R-de peso binario k se representa unívocamente por una cadena binaria de L bits y k unos, que sería la representación binaria de su elemento líder r. Sean p_i $(i = 1, ..., n)$ los divisores propios de L, entonces la cadena binaria representativa de un *coset regular* R asociado con p_i se compone de $c_i = L/p_i$ repeticiones de grupos de p_i bits con k/c_i unos en cada grupo. El cardinal del *coset regular* R será p_i. El nombre de *cosets regulares* se debe a la distribución 'regular' de los k unos a lo largo de la cadena binaria de L bits. Obviamente, si L es un número primo, entonces no existen *cosets regulares.* Con el fin de ilustrar este concepto fundamental, presentamos un ejemplo sencillo de *cosets regulares.*

Ejemplo 1. Para $L = 12$, $k = 6$ los diferentes *cosets regulares* $R_i (i = 1, \ldots, 5)$ en términos de sus correspondientes cadenas binarias de L bits

o de sus elementos líderes, r_i, pueden escribirse tal y como sigue[2]

$$\begin{aligned}
000111\ 000111 &\iff r_1 = 2^0 + 2^1 + 2^2 + 2^6 + 2^7 + 2^8 \\
001011\ 001011 &\iff r_2 = 2^0 + 2^1 + 2^3 + 2^6 + 2^7 + 2^9 \\
010011\ 010011 &\iff r_3 = 2^0 + 2^1 + 2^4 + 2^6 + 2^7 + 2^{10} \\
0011\ 0011\ 0011 &\iff r_4 = 2^0 + 2^1 + 2^4 + 2^5 + 2^8 + 2^9 \\
01\ 01\ 01\ 01\ 01\ 01 &\iff r_5 = 2^0 + 2^2 + 2^4 + 2^6 + 2^8 + 2^{10}
\end{aligned}$$

Los cosets R_1, R_2, R_3 están asociados con el divisor propio 6, el coset R_4 con 4 y el coset R_5 con 2. Por tanto, sus correspondientes cardinales p_i son 6, 4 y 2 respectivamente.

En términos geométricos un *coset regular* puede interpretarse como una cadena binaria de L bits tal que cuando se rota circularmente p_i posiciones permanece invariable.

3 Complejidad Lineal de Filtros No Lineales de Segundo Orden de $m-$Secuencias

Se define la complejidad lineal de una secuencia como la longitud del menor LFSR que puede generarla. En efecto, existen algoritmos conocidos [11] que permiten determinar la recursión lineal de una secuencia de complejidad lineal l con sólo observar $2l$ bits consecutivos.

Una función no lineal de orden k aplicada a las etapas de un LFSR puede considerarse 'bien elegida' para fines criptográficos si -entre otros requisitos- la complejidad lineal LC de su secuencia filtrada alcanza (o se aproxima a) la cota superior dada por Key [7] cuyo valor numérico es:

$$LC_{\max} = \sum_{i=1}^{k} \binom{L}{i} \tag{3.1}$$

La complejidad lineal de una secuencia filtrada [7] coincide con el número de potencias de α que aparecen en la expresión del elemento genérico z_n de la secuencia filtrada obtenida a partir de la ecuación (2.1). En efecto

[2]En lo sucesivo, un coset ciclotómico quedará representado ya sea por su elemento líder o por la cadena binaria de L bits que corresponde a la representación binaria de su elemento líder.

$$
\begin{aligned}
z_n = F(a_n, a_{n+1}, ..., a_{n+L-1}) = \\
C_1\alpha^{E_1 n} + (C_1\alpha^{E_1 n})^2 + ... + (C_1\alpha^{E_1 n})^{2^{(r_1-1)}} + \\
C_2\alpha^{E_2 n} + (C_2\alpha^{E_2 n})^2 + ... + (C_2\alpha^{E_2 n})^{2^{(r_2-1)}} + \\
\vdots \\
C_i\alpha^{E_i n} + (C_i\alpha^{E_i n})^2 + ... + (C_i\alpha^{E_i n})^{2^{(r_i-1)}} + \\
\vdots \\
C_N\alpha^{E_N\, n} + (C_N\alpha^{E_N\, n})^2 + ... + (C_N\alpha^{E_N\, n})^{2^{(r_N-1)}}
\end{aligned}
\tag{3.2}
$$

donde $C_i \in GF(2^{r_i})$ es el coeficiente correspondiente al *coset* E_i de cardinal r_i. El subíndice i se extiende a los N *cosets ciclotómicos* de peso $\leq k$. Si $C_i = 0$, entonces el correspondiente *coset* E_i es *degenerado* y no contribuye a la complejidad lineal de la secuencia filtrada.

Por tanto para filtros no lineales de segundo orden, la complejidad lineal de la secuencia producto se obtiene del estudio de los coeficientes C_i asociados con los *cosets ciclotómicos* de peso binario menor o igual que dos. A continuación, damos sus correspondientes expresiones.

3.1 Coset Ciclotómico de Peso Binario 1

Según (2.1) los elementos genéricos a_{n+t_0} y a_{n+t_1} de la m-secuencia $\{a_n\}$ pueden escribirse como:

$$a_{n+t_0} = \sum_{i=0}^{L-1} \alpha^{2^i t_0} \cdot \alpha^{2^i n} \tag{3.3}$$

$$a_{n+t_1} = \sum_{i=0}^{L-1} \alpha^{2^i t_1} \cdot \alpha^{2^i n} \tag{3.4}$$

Luego, el elemento genérico z_n de la secuencia filtrada $\{z_n\}$ es

$$
\begin{aligned}
z_n = \alpha^{2^{(l-1)}t_0} \cdot \alpha^{2^{(L-1)}t_1} \cdot \alpha^n + \alpha^{t_0} \cdot \alpha^{t_1} \cdot \alpha^{2n} + \alpha^{2t_0} \cdot \alpha^{2t_1} \cdot \alpha^{4n} \cdots = \\
C_1 \cdot \alpha^n + (C_1)^2 \cdot \alpha^{2n} + (C_1)^4 \cdot \alpha^{4n} \cdots
\end{aligned}
\tag{3.5}
$$

siendo C_1 el coeficiente asociado al *coset 1*. Identificando coeficientes en ambos términos, tenemos

$$C_1 = \alpha^{2^{(L-1)}t_0} \cdot \alpha^{2^{(L-1)}t_1} \tag{3.6}$$

Ya que C_1 es distinto de cero, el *coset 1* siempre será no degenerado y contribuirá a la complejidad lineal de la secuencia filtrada. El valor de tal contribución será su cardinal L. De la ecuación anterior, se deduce un resultado relativo al período T de la secuencia producto.

Lema 1. *El período T de la secuencia producto de dos fases arbitrarias de una m-secuencia $\{a_n\}$, $a_{n+t_0} \cdot a_{n+t_1}$, es $2^L - 1$.*

Demostración. Según [4], el período de la secuencia producto es el mínimo común múltiplo de los períodos de las secuencias características asociadas con los *cosets* no *degenerados* de peso binario dos y uno. Como la secuencia característica asociada al *coset 1* es la m-secuencia $\{a_n\}$ de período $2^L - 1$, entonces el período de la secuencia producto será también $2^L - 1$.

■

3.2 Cosets Ciclotómicos de Peso Binario 2

Sea e el líder de un *coset ciclotómico* E genérico de peso dos, es decir e puede escribirse:

$$e = 2^{e_0} + 2^{e_1} \qquad 0 = e_0 < e_1 \leq \lfloor \frac{L}{2} \rfloor \tag{3.7}$$

Entonces C_E, el coeficiente asociado al *coset* E, puede calcularse a partir del test de presencia de raíces de Rueppel [11] tal y como sigue:

$$C_E = \begin{vmatrix} \alpha^{t_0 \cdot 2^{e_0}} & \alpha^{t_1 \cdot 2^{e_0}} \\ \alpha^{t_0 \cdot 2^{e_1}} & \alpha^{t_1 \cdot 2^{e_1}} \end{vmatrix} \tag{3.8}$$

Para simplificar el estudio de estos coeficientes C_E, vamos a agrupar todos los filtros no lineales de orden dos que producen la secuencia filtrada

$$\{z_n\} = \{a_{n+t_0} \cdot a_{n+t_1}\} \tag{3.9}$$

o una versión desplazada de la misma

$$\{z_n\}^* = \{a_{n+t_0+k} \cdot a_{n+t_1+k}\} \qquad k = 1, 2, \ldots, 2^L - 2 \tag{3.10}$$

(la suma en los subíndices se toma mod $(2^L - 1)$). De acuerdo con [4], todos estos filtros no lineales pertenecen a una misma clase de equivalencia denotada por $[z_{t_0 t_1}]$. Por tanto, el estudio de todos los filtros no lineales de orden dos dados por F puede reducirse al estudio de un elemento representativo de cada una de dichas clases. En particular, consideraremos

$$[z_{0d}] = [a_n \cdot a_{n+d}] \qquad d = t_1 - t_0 = 1, 2, \ldots, 2^{L-1} - 1 \tag{3.11}$$

como el elemento representativo de la clase de equivalencia correspondiente. Después de este inciso, podemos tomar sin pérdida de generalidad $t_0 = 0$ y $t_1 = d$ en (3.8). Por tanto

$$C_E = \begin{vmatrix} 1 & \alpha^d \\ & \\ 1 & \alpha^{d \cdot 2^{e_1}} \end{vmatrix} \tag{3.12}$$

De la ecuación (3.12) se observa que el coeficiente C_E será cero si y sólo si se verifica

$$\alpha^{d \cdot 2^{e_1}} = \alpha^d \tag{3.13}$$

o equivalentemente

$$d \cdot 2^{e_1} \equiv d \mod (2^L - 1) \tag{3.14}$$

Luego, las ecuaciones (2.3) y (3.14) tienen las mismas soluciones y los valores de la diferencia de fase d que produce la degeneración de los cosets de peso binario dos son los elementos de los *cosets regulares.*

4 Una Interpretación Geométrica de la Complejidad Lineal para Filtros No Lineales de Segundo Orden

Ahora vamos a considerar los diferentes *cosets regulares* asociados con L y las correspondientes degeneraciones que ellos producen en la secuencia filtrada. Consideraremos dos casos diferentes:

4.1 L es un número primo

De las anteriores ecuaciones se deduce fácilmente el siguiente resultado:

Teorema 4.1. *Sea L el número de etapas de un LFSR con polinomio de conexión primitivo. Si L es un número primo, entonces la complejidad lineal de la secuencia producto de dos fases distintas de $\{a_n\}, a_{n+t_0} \cdot a_{n+t_1}$, alcanza siempre la cota superior dada por Key.*

Demostración. Este resultado se deriva inmediatamente del hecho de que si L es primo, entonces no hay *cosets regulares* o, equivalentemente, la ecuación (3.14) no tiene solución. En este caso todos los *cosets ciclotómicos* de peso binario dos y uno contribuyen a la complejidad lineal de la secuencia resultante. ■

El teorema anterior confirma el resultado de la no degeneración de productos de orden dos dado por Massey mediante la utilización de la transformada de Fourier discreta.

4.2 L es un número compuesto

Sean $p_1 > p_2 > \ldots > p_n$ los divisores propios de L. Para cada p_i tenemos diferentes[3] *cosets regulares* R cuyos elementos están unívocamente definidos por cadenas binarias de L bits compuestas por $c_i = L/p_i$ repeticiones de p_i grupos de bits con $k_i \in [1, 2, \ldots, p_i - 1]$ unos. Para cada uno de los valores posibles de k_i tendremos

$$\binom{p_i}{k_i} \tag{4.1}$$

de tales cadenas binarias (i.e. k_i unos colocados en p_i posiciones diferentes). Por tanto en total obtendremos

$$\sum_{j=1}^{p_i-1} \binom{p_i}{j} \tag{4.2}$$

cadenas binarias diferentes de L bits o, equivalentemente, valores de la diferencia de fase d asociados con p_i que van a producir degeneraciones

[3]Puede haber *coset regulares* asociados a más de un p_i (si la subcadena binaria asociada a p_i es también un coset regular), en este caso los *coset regulares* se considerarán asociados al menor p_i.

en la secuencia producto $\{a_n \cdot a_{n+d}\}$. Para calcular el valor cuantitativo de tales degeneraciones damos una interpretación geométrica de la degeneración de los *cosets ciclotómicos* de peso binario dos:

En efecto, sea d el valor numérico asociado a una de las anteriores cadenas binarias de L bits y sea $e = 2^0 + 2^{e_1} = 2^0 + 2^{\overset{\bullet}{p_i}}$ el líder de un *coset ciclotómico* de peso binario dos. Entonces de acuerdo con (3.14), el término $2^{\overset{\bullet}{p_i}}$ causará un desplazamiento circular de p_i (o múltiplo de p_i) posiciones en la cadena binaria asociada a d que permanecerá invariable. Consecuentemente, la ecuación (3.14) se verificará y el *coset ciclotómico* E será degenerado para la secuencia producto $\{a_n \cdot a_{n+d}\}$. El procedimiento puede repetirse para cada uno de los divisores propios p_i de L. A continuación se presenta un ejemplo ilustrativo.

Ejemplo 2. Para $L = 15$, sus divisores propios son $p_1 = 5$, $p_2 = 3$.

- Las cadenas binarias de 15 bits correspondientes a los *cosets regulares* R_j asociados con p_1 son:

$$\begin{aligned}
&00001\ 00001\ 00001 \iff \textit{coset } R_1,\ k_1 = 1\\
&\\
&00011\ 00011\ 00011 \iff \textit{coset } R_2,\ k_1 = 2\\
&00101\ 00101\ 00101 \iff \textit{coset } R_3,\ k_1 = 2\\
&\\
&00111\ 00111\ 00111 \iff \textit{coset } R_4,\ k_1 = 3\\
&01011\ 01011\ 01011 \iff \textit{coset } R_5,\ k_1 = 3\\
&\\
&01111\ 01111\ 01111 \iff \textit{coset } R_6,\ k_1 = 4
\end{aligned}$$

- Las cadenas binarias de 15 bits correspondientes a los *cosets regulares* R_j asociados con p_2 son:

$$\begin{aligned}
&001\ 001\ 001\ 001\ 001 \iff \textit{coset } R_7,\ k_2 = 1\\
&011\ 011\ 011\ 011\ 011 \iff \textit{coset } R_8,\ k_2 = 2
\end{aligned}$$

Ahora, podemos escribir los *cosets ciclotómicos* $\mathrm{mod}(2^{15} - 1)$ de peso

binario dos.

$$\begin{aligned}
&00000\ 00000\ 00011 \iff \textit{coset } E_1\\
&00000\ 00000\ 00101 \iff \textit{coset } E_2\\
&00000\ 00000\ 01001 \iff \textit{coset } E_3\\
&00000\ 00000\ 10001 \iff \textit{coset } E_4\\
&00000\ 00001\ 00001 \iff \textit{coset } E_5\\
&00000\ 00010\ 00001 \iff \textit{coset } E_6\\
&00000\ 00100\ 00001 \iff \textit{coset } E_7
\end{aligned}$$

Según la anterior interpretación geométrica tenemos:

- Para $p_1 = 5$, el *coset ciclotómico* E_5 será degenerado para las diferencias de fases d que tomen valores en los elementos de los *cosets regulares* $R_1, R_2, \ldots, R_6$.
- Para $p_2 = 3$, los *cosets ciclotómicos* E_3 y E_6 serán degenerados para diferencias de fases d que tomen valores en los elementos de los *cosets regulares* R_7, R_8.

De la anterior interpretación geométrica se derivan los siguientes resultados:

Teorema 4.2. *Sea p_i un divisor propio de L y sea $[R_i]$ el conjunto de cosets regulares asociados con p_i. Si d es un elemento de alguno de estos cosets regulares $[R_i]$, entonces el número de cosets ciclotómicos degenerados de peso binario dos viene dado por:*

$$N_{p_i} = \lfloor \frac{\lfloor L/2 \rfloor}{p_i} \rfloor \tag{4.3}$$

Demostración. Según la interpretación geométrica de la degeneración de un *coset ciclotómico* de peso binario dos, es fácil ver que N_{p_i} coincide con el número de veces que una estructura de p_i bits está contenida en la distancia máxima entre unos en los *cosets ciclotómicos* mod $(2^L - 1)$ de peso binario dos. El hecho de que, por construcción, la distancia máxima sea $\lfloor L/2 \rfloor$ para el *coset* $2^0 + 2^{\lfloor L/2 \rfloor}$ completa la demostración.

■

Como una consecuencia del teorema anterior, se obtienen los siguientes corolarios:

Corolario 1. *Para una diferencia de fases d bajo las condiciones del teorema 4.2, el valor de la complejidad lineal de la secuencia filtrada verifica*

$$\frac{L^2+L}{2} - (N_{p_i} \cdot L) \geq LC \geq \frac{L^2+L}{2} - (N_{p_i} - 1)\, L - L/2 \qquad (4.4)$$

siendo $\frac{L^2+L}{2}$ *la cota superior de Key para un filtro no lineal de segundo orden y* N_{p_i} *el valor definido en el teorema 4.2. En efecto, LC alcanza la cota inferior si L es par y* $p_i = L/2$ *(o divisor). En caso contrario, LC es igual a la cota superior.*

Demostración. El resultado es una consecuencia directa del teorema 4.2. La complejidad lineal tomará el valor máximo dado por la cota superior de Key salvo la contribución a la complejidad lineal de los *cosets ciclotómicos* mod $(2^L - 1)$ de peso binario dos que sean degenerados. El valor cuantitativo de esta disminución será el número de cosets degenerados N_{p_i} multiplicado por sus correspondientes cardinales. Por construcción, todos los *cosets ciclotómicos* mod $(2^L - 1)$ de peso binario dos tienen cardinal L salvo el *coset* E de líder $e = 2^0 + 2^{L/2}$, para L par, cuyo cardinal es $L/2$. La cota inferior se debe al hecho de que si L es par y $p_i = L/2$ (o divisor), entonces el *coset ciclotómico* E de líder $e = 2^0 + 2^{L/2}$ es degenerado . En cualquier otro caso, como todos los *cosets ciclotómicos* de peso binario dos tienen cardinal L, la complejidad lineal tomará el valor dado por la cota superior.

■

Corolario 2. *Para una diferencia de fases d bajo las condiciones del teorema 4.2, los* **cosets ciclotómicos** *de peso binario dos que van a degenerar obedecen a las siguientes expresiones binarias y decimales de*

sus líderes:

$$
\begin{array}{ll}
1\ \underbrace{000\ldots1}_{p_i} & \Longleftrightarrow\ e_1 = 2^0 + 2^{p_i} \\
1\ \underbrace{000\ldots0}_{p_i}\ \underbrace{000\ldots1}_{p_i} & \Longleftrightarrow\ e_2 = 2^0 + 2^{2\,p_i} \\
\quad\vdots & \quad\vdots \\
\underbrace{1\ \underbrace{000\ldots0}_{p_i}\ \underbrace{000\ldots0}_{p_i}\ \ldots\ldots\ \underbrace{000\ldots1}_{p_i}}_{N_{p_i}\ veces} & \Longleftrightarrow\ e_{N_{p_i}} = 2^0 + 2^{N_{p_i}\ p_i}
\end{array}
$$

Demostración. El resultado es consecuencia inmediata de la interpretación geométrica de la degeneración de un *coset ciclotómico* de peso binario dos.

■

Corolario 3. *Si $L = p^n$ siendo p un número primo, entonces los cosets regulares asociados con p producirán las mayores degeneraciones en la secuencia filtrada, ya que dichos cosets incluirán las degeneraciones de los cosets regulares asociados con los restantes divisores propios de L.*

Demostración. Como $p \mid p_i \ \ \forall i$, entonces una estructura de p bits siempre estará contenida en una estructura de p_i bits. Por tanto, los *cosets regulares* asociados con p incluyen las degeneraciones de los *cosets regulares* asociados con $p_i\ \forall i$. A las degeneraciones previas tenemos que añadirle las degeneraciones debidas exclusivamente a los *cosets regulares* asociados con p.

■

Como una aplicación de este corolario, damos una tabla con valores representativos:

L	p	N_p	LC_{max}	$LC_{\min}$
$121 = 11^2$	11	5	7381	6776
$125 = 5^3$	5	12	7875	6375
$128 = 2^7$	2	32	8256	4224
$243 = 3^5$	3	40	29646	19926
$256 = 2^8$	2	64	32896	16640
$343 = 7^3$	7	24	58996	50764
$512 = 2^9$	2	128	131328	66048
$625 = 5^4$	5	62	195625	156875
$729 = 3^6$	3	121	266085	177876

donde LC_{max} es la cota superior de Key y $LC_{\min}$ es el valor de la complejidad lineal cuando d toma valores en el conjunto de los *cosets regulares* asociados con p.

4.3 Reglas Prácticas para elegir la diferencia de fases

Según las secciones precedentes, sabemos que cuando la diferencia de fases d toma valores en M, el conjunto de los *cosets regulares* de L, se producirán degeneraciones en la secuencia filtrada. Por tanto, una regla práctica para evitar tales degeneraciones consiste en elegir $d \notin M$. Otras elecciones más específicas se definen de la siguiente manera:

1 Si p_1 es el mayor divisor propio de L, entonces el menor líder de los *cosets regulares asociados a* L será:

$$e_{\min} = 2^0 + 2^{p_1} + 2^{2\,p_1} + \ldots + 2^{(c_1-1)\,p_1} \tag{4.5}$$

con $c_1 = L/p_1$. Por tanto, tomando d en el intervalo

$$0 < d < e_{\min} \tag{4.6}$$

queda garantizada la máxima complejidad lineal de la secuencia filtrada.

2 Si la expresión binaria de d contiene k unos pero $(L, k) = 1$, entonces d no será nunca un elemento de un *coset regular,* por lo tanto queda garantizada la máxima complejidad lineal de la secuencia filtrada.

3 Si $(L, k) \neq 1$ pero los k unos en la expresión binaria de d no están regularmente repetidos a lo largo de los grupos de p_i bits, entonces la máxima complejidad lineal de la secuencia filtrada queda también garantizada.

En resumen, el número y distribución de los unos en la representación binaria de d es el parámetro que podemos manipular para preservar la cota superior dada por Key sobre el valor de la complejidad lineal de la secuencia filtrada.

5 Conclusiones

En este artículo se ha desarrollado un nuevo procedimiento para analizar la complejidad lineal de secuencias filtradas en términos de los *cosets regulares*. El método, que está basado en una interpretación geométrica del concepto de *coset regular*, permite determinar fácilmente los *cosets* degenerados en la secuencia filtrada. También se han dado expresiones generales para calcular la complejidad lineal de las secuencias así generadas. El trabajo finaliza con una serie de reglas prácticas para diseñar filtros no lineales de segundo orden cuyas secuencias resultantes alcancen la cota superior de complejidad lineal dada por Key.

6 Agradecimientos

Este trabajo ha sido financiado por la Fundación Ramón Areces, por la Comisión Interministerial de Ciencia y Tecnología (CICYT) Proyecto TEL98-1020 y por la Comunidad Autónoma de Madrid Proyecto 07T/0044/1998.

References

[1] P. Caballero-Gil, *Regular Cosets and Upper Bounds on the Linear Complexity of Certain Sequences*, First International Conference on Sequences and Their Applications - SETA'98, December 14-17 1998, National University of Singapore.

[2] P. Caballero Gil y A. Fúster Sabater, *Equivalente Lineal Descompuesto del Filtrado no Lineal y Resultados sobre Complejidad Lineal*, Revista de la Academia Canaria de Ciencias. Vol. VI, No. 1, 1994.

[3] A. Fúster-Sabater and P. Caballero-Gil, *On the Linear Complexity of Nonlinearly Filtered PN-Sequences*, Advances in Cryptology-ASIACRYPT'94. Lecture Notes in Computer Science Vol. 917, Springer-Verlag.

[4] A. Fúster-Sabater and L. J. García-Villalba, *On the Structural Properties of Nonlinear Filterings of m-Sequences*, Proceedings of 1998 IEEE International Symposium on Information Theory. Massachusetts Institute of Technology (M.I.T.), Cambridge, MA, U.S.A, 16-21 August 1998, pp. 104.

[5] S.W. Golomb, *Shift Register-Sequences*, Holden-Day, San Francisco, 1967.

[6] E.J. Groth, *Generation of Binary Sequences with Controllable Complexity*, IEEE Trans. on Information Theory, Vol. IT-17, pp. 288-296, May 1971.

[7] E.L. Key, *An Analysis of the Structure and Complexity of Non-Linear Binary Sequence Generators*, IEEE Trans. on Information Theory, Vol. IT-22, No. 6, pp. 732-736, Nov. 1976.

[8] P.V. Kumar and R.A. Scholtz, *Bounds on the Linear Span of Bent Sequences*, IEEE Trans. on Information Theory, Vol. IT-29, pp. 854-862, Nov. 1983.

[9] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications. Cambridge University Press, 1986.

[10] J.L. Massey and S. Serconek, *A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences*, Advances in Cryptology-CRYPTO'94. Lecture Notes in Computer Science Vol. 839, pp. 332-340, Springer-Verlag, 1994.

[11] R.A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, New York, 1986.

Departamento de tratamiento de la información y codificación
Instituto de Física Aplicada (C.S.I.C.)
Serrano 144
28006 Madrid
(Spain)
E-mail address: {amparo, luisj}@iec.csic.es

Recibido: 18 de Enero de 1999
Revisado: 1 de Julio de 1999