GENERADORES BINARIOS DE SECUENCIAS EQUILIBRADAS

Amparo Fúster Sabater

Departamento de Tratamiento de la Información y Codificación (T.I.C.)
Instituto de Física Aplicada (C.S.I.C.)
Serrano 144, 28006 Madrid
amparo@iec.csic.es

Pedro García-Mochales Caro

Instituto de Microelectrónica de Madrid
IMM-CNM, C.S.I.C.
C/ Isaac Newton 8 (PTM)
28780 Tres Cantos, Madrid
pedrog@imm.cnm.csic.es

ABSTRACT

A method of computing the number of 0's and 1's in the sequence obtained from LFSR-based generators has been developed. The procedure in based on the concept of *global minterm* of the generating function and allows us to check the degree of balancedness of the generated sequence. The method is completely general and can be applied to combination (nonlinear filter) generators in a range of cryptographic interest.

1. INTRODUCCIÓN

Los generadores de secuencia basados en *Linear Feedback Shift Registers* (LFSRs) [1] son dispositivos muy conocidos para la generación de secuencias binarias pseudoaleatorias con aplicaciones en: simulaciones, testeo de circuitos, códigos correctores de errores o Criptografía. Una de las propiedades que deben exigirse a las secuencias obtenidas a partir de estos generadores es que sean *equilibradas*, es decir que su número de unos coincida con su número de ceros. En la práctica, la manera de analizar el grado de equilibrio de estas secuencias (dado que son secuencias de período muy largo) consiste en elegir aleatoriamente diferentes partes de la misma y contar el número de ceros y unos. Si el resultado del cómputo es satisfactorio en todas las porciones analizadas, entonces se considera que la secuencia verifica la condición de equilibrio.

En el presente trabajo se propone un método que, a partir de la expresión matemática del generador, permite calcular el número de ceros y unos de la secuencia generada. De esta manera se determina si la secuencia obtenida es o no *equilibrada* y en caso de no serlo su desviación con respecto al número ideal de ceros y unos. El procedimiento es completamente general y puede aplicarse a generadores de secuencia (filtros no lineales o combinadores) en un rango de interés criptográfico.

2. NOTACIÓN Y CONCEPTOS BÁSICOS

Un LFSR [1] es un dispositivo constituido por L celdas de memoria (etapas), desplazamiento cíclico y realimentación lineal. En términos matemáticos, un generador basado en N registros LFSRs es una función booleana no lineal F cuyas entradas son las diferentes etapas de los N LFSRs que integran dicho generador y cuya salida es un único bit. A cada golpe de reloj, las etapas de los LFSRs varían su contenido que constituye las nuevas variables de entrada a la función F. Así se van generando los sucesivos bits de la secuencia de salida o secuencia generada.

Sea A un LFSR arbitrario de longitud L_A cuyas etapas se denotan respectivamente por a_i $(i=1,\ldots,L_A)$ y cuya secuencia de salida tiene período $T_A = 2^{L_A} - 1$. Un minterm [2] de L_A variables puede escribirse como una función no lineal con un único término de orden j $(1 \le j \le L_A)$. Las j variables que aparecen en el término de menor orden se repiten en los restantes sumandos. Cada minterm consta de $2^{L_A - j}$ términos. Veamos un ejemplo.

Ejemplo 1: Para un LFSR de $L_A = 3$ etapas la forma particular de los minterms es:

$$A_{123} = a_{123} \qquad A_1 = a_{123} \oplus a_{12} \oplus a_{13} \oplus a_1$$
$$A_{23} = a_{123} \oplus a_{23} \qquad A_2 = a_{123} \oplus a_{23} \oplus a_{12} \oplus a_2$$
$$A_{13} = a_{123} \oplus a_{13} \qquad A_3 = a_{123} \oplus a_{23} \oplus a_{13} \oplus a_3$$
$$A_{12} = a_{123} \oplus a_{12}$$

donde a_{ij} representa el producto lógico (AND) de las etapas a_i y a_j, A_{ij} designa el minterm que incluye a_{ij} en todos los sumandos y el símbolo $\oplus$ representa la suma mod 2.

Todo minterm considerado como una función no lineal aplicada a las etapas del LFSR A genera una secuencia binaria con un único 1 y período $T_A = 2^{L_A} - 1$. Ahora, denotamos por *A, B, ..., Z* los N LFSRs que intervienen en el generador considerado cuyas longitudes son respectivamente L_A, L_B, ..., L_Z. Llamamos a_i $(i=1,\ldots,L_A)$, b_j $(j=1,\ldots,L_B)$, ..., z_k $(k=1,\ldots,L_Z)$ a sus correspondientes etapas. Los minterms globales asociados con el generador tendrán ahora $L_A + L_B + \ldots + L_Z$ variables y son de la forma $A_{ij}\, B_{pqr} \ldots Z_s$ es decir el producto lógico de los minterms de cada uno de los LFSRs. Todo minterm global considerado como una función no lineal aplicada a las etapas de los LFSRs genera una secuencia binaria con un único 1 y con período $T = m.c.m.((2^{L_A} - 1), (2^{L_B} - 1), \ldots, (2^{L_Z} - 1))$.

Los minterms globales constituyen una base para representar cualquier función no lineal F. Las secuencias asociadas a cada minterm global son secuencias canónicas con un único 1. Luego, la secuencia generada por F puede descomponerse como suma de las secuencias canónicas asociadas a los minterms globales de F.

Por tanto la idea básica de este trabajo puede resumirse en: Dada una función booleana no lineal F se trata de escribirla en términos de sus minterms globales. El número de minterms que aparezcan en la representación de F coincide con el número de unos en la secuencia generada.

3. MÉTODO DE CÁLCULO

Para un generador con 2 LFSRs de longitudes $L_A = 3$, $L_B = 2$ y función no lineal $F = a_1 b_1$ se procede tal y como sigue:

1) Se sustituye cada término de F por su correspondiente minterm global dando lugar a la función dual ϕ
$$\phi = A_1 B_1.$$
2) Se sustituye cada término de ϕ por su correspondiente expresión
$$\phi = A_1 B_1 = (a_{123} \oplus a_{12} \oplus a_{13} \oplus a_1)(b_{12} \oplus b_1) =$$
$$a_{123}b_{12} \oplus a_{123}b_1 \oplus a_{12}b_{12} \oplus a_{12}b_1 \oplus$$
$$a_{13}b_{12} \oplus a_{13}b_1 \oplus a_1 b_{12} \oplus a_1 b_1.$$
3) Se reescribe F en términos de los minterms globales
$$F = A_{123}B_{12} \oplus A_{123}B_1 \oplus A_{12}B_{12} \oplus A_{12}B_1 \oplus$$
$$A_{13}B_{12} \oplus A_{13}B_1 \oplus A_1 B_{12} \oplus A_1 B_1.$$

El número de minterms globales en 3) coincide con el número de unos de la secuencia generada, que en este caso es 8.

Para calcular el número de minterms globales en F se hace uso de las siguientes expresiones. Para un LFSR, por ejemplo A, la suma de todos sus minterms es

$$A_{12\ldots L_A} \oplus A_{12\ldots L_A - 1} \oplus \cdots \oplus A_{2\ldots L_A} \oplus \cdots \oplus A_{L_A} \oplus \cdots \oplus A_1 = 1$$

que de forma compacta puede reescribirse como

$$A_1^{'} \oplus A_1 = 1$$

donde el número de términos en $A_1^{'}$ es $2^{L_A - 1} - 1$ mientras que en A_1 el número de términos es $2^{L_A - 1}$.

4. APLICACIONES

El procedimiento descrito puede aplicarse a generadores standard de uso criptográfico. Para el generador de Geffe [3] con tres LFSRs A, B y C de longitudes L_A, L_B, L_C y función no lineal

$$F = a_1 b_1 \oplus b_1 c_1 \oplus c_1$$

procedemos a escribir su función dual ϕ

$$\phi = A_1 B_1 \oplus B_1 C_1 \oplus C_1$$
$$= A_1 B_1 (C_1^{'} + C_1) \oplus (A_1^{'} + A_1) B_1 C_1 \oplus (A_1^{'} + A_1)(B_1^{'} + B_1) C_1$$
$$= A_1 B_1 (C_1^{'} + C_1) \oplus (A_1^{'} + A_1) B_1^{'} C_1.$$

Luego, el número de términos en ϕ o equivalentemente el número de unos en la secuencia generada es

$$No.1s = 2^{L_A - 1} 2^{L_B - 1} (2^{L_C} - 1) + (2^{L_A} - 1)(2^{L_B - 1} - 1) 2^{L_C - 1}$$

que es la expresión general del número de unos de la secuencia obtenida a partir de un generador de Geffe.

El procedimiento desarrollado nos permite también deducir reglas prácticas de diseño de generadores de secuencia. Consideremos las siguientes funciones no lineales para generadores con 3 LFSRs.

$$F_0 = a_1 b_1 \oplus b_1 c_1 \oplus a_1 c_1 \oplus a_1 b_1 \oplus a_1 \oplus b_1 \oplus c_1$$
$$F_1 = a_1 b_1 \oplus b_1 c_1 \oplus a_1 \oplus b_1 \oplus c_1$$
$$F_2 = a_1 b_1 \oplus b_1 c_1 \oplus b_1$$
$$F_3 = a_1 b_1 \oplus b_1 c_1 \oplus a_1$$
$$F_4 = a_1 b_1 \oplus c_1$$

La Tabla 1 muestra el número de unos de las secuencias producidas por estos generadores para una elección arbitraria de $L_A = 2$, $L_B = 3$, $L_C = 5$ y período $T = m.c.m.(3, 7, 31)$.

	No. 1's (ideal)	No. 1's (real)	Orden de magnitud
F_0	326	478	$\approx T/2 + T/4$
F_1	326	510	$\approx T/2 + T/4$
F_2	326	188	$\approx T/4$
F_3	326	378	$\approx T/2$ *(sec. equilibrada)*
F_4	326	328	$\approx T/2$ *(sec. equilibrada)*

Tabla 1. *Resultados numéricos para diferentes generadores.*

Las funciones no lineales F_0, F_1 incluyen todos los términos de primer orden a_1, b_1, c_1 lo que conlleva un gran número de términos en ϕ, por consiguiente el número de unos en la secuencia generada será mayor que $T/2$. F_2 incluye b_1 en todos los sumandos lo que supone un gran número de términos cancelados en ϕ, por tanto el número de unos de la secuencia de salida será menor que $T/2$. Estas funciones no lineales nunca producirán secuencias equilibradas. Por el contrario F_3 y F_4 debido a la forma particular de sus términos dan lugar a secuencias con un número de unos en el rango de $\approx T/2$.

En resumen, de acuerdo con este procedimiento un simple estudio de la función generatriz permite al diseñador de generadores de secuencia saber si la secuencia de salida tendrá un número de unos en el rango deseado.

5. CONCLUSIONES

En este trabajo se ha presentado un método sencillo y eficaz de cómputo del número de unos (ceros) de la secuencia obtenida a partir de un generador basado en registros LFSRs. El procedimiento puede aplicarse a generadores prácticos de interés criptográfico pudiéndose deducir fácilmente reglas de diseño.

6. REFERENCIAS

[1] Golomb, S.W., *Shift Register Sequences,* Aegean Park Press, Laguna Hill, 1982.

[2] Mange, D., *Analysis and Synthesis of Logic Systems,* Artech House Inc., Boston, 1986.

[3] Massey, J., *Cryptography: Fundamentals and Applications* Advanced Technology Seminars, Zurich, 1994.