Universidad de Cantabria

FACULTAD DE CIENCIAS

REGISTRO DE DESPLAZAMIENTO CON RETROALIMENTACIÓN LINEAL

(LINEAR FEEDBACK SHIFT REGISTER)

Trabajo de fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autora: Sara Roig Zurita

Director: Daniel Sadornil Renedo

Junio-2025

Resumen

La criptografía se basa en el desarrollo y uso de algoritmos codificados para proteger información que se quiere transmitir. El objetivo es la ocultación de información importante o delicada, para garantizar la privacidad, integridad y autentificación de la misma. Idealmente, nos gustaría poder utilizar un código indescifrable para que, si un intruso intercepta esta comunicación, no pueda obtener la información cifrada.

El único código impenetrable conocido es el cifrado de Vernam. Este código perfecto utiliza como palabra clave para cifrar el texto deseado una secuencia de bits que sea lo suficientemente larga y aleatoria. Además, cada vez que se cifra un texto, se utiliza una nueva clave con estas propiedades, lo cual, para claves con las características anteriores, es bastante costoso.

Este trabajo se centra en el estudio de una herramienta para generar este tipo de claves, los registros de desplazamiento con retroalimentación. Estos son dispositivos que generan sucesiones pseudoaleatorias de manera rápida y eficiente. A pesar de necesitar sucesiones aleatorias, se buscarán sucesiones periódicas con periodo largo y con propiedades aleatorias específicas, ya que, como se verá, simulan aleatoriedad.

Abstract

Cryptography is based on the development and usage of encoded algorithms to protect information for its transmission. The goal of hiding important and sensitive information is to ensure its privacy, integrity, and authentication. The perfect idea is to choose an unbreakable code so, if an intruder intercepts this communication, they cannot obtain the encrypted information.

The only known impenetrable code is the Vernam cipher. This perfect cipher uses a sufficiently long and random keyword to encrypt the desired text. Furthermore, each time a text is encrypted, a new key with these properties is used.

Since continuous generation of this key is expensive, this work will focus on simplifying key production. The keyword is a sequence of bits, and this document will show that feedback shift registers are devices that quickly and efficiently generate pseudo-random sequences. Although random sequences are required, periodic sequences with a long period and specific random properties will be sought, since they simulate randomness.

Agradecimientos

Este trabajo no sería posible sin la ayuda de mi tutor Daniel Sadornil, a quien le agradezco inmensamente su trabajo y esfuerzo. Ha estado siempre pendiente y resolutivo cuando se me han presentado problemas y dudas. No cualquiera te responde a un correo un domingo por la tarde con una nueva idea para una demostración. Ha sido un tutor muy atento y le estaré siempre agradecida, ya que seguramente yo haya sido algo cansina en algunos momentos.

También me gustaría agradecer a mis familiares y amigos, que han estado aguantándome durante este largo proceso de carrera. Sin ellos no hubiese tenido la fuerza de aguantar en los momentos más difíciles en los que he estado baja de ánimos. También me han enseñado a desconectar y descansar cuando es necesario, para después poder volver a concentrarme y ser más productiva. Como siempre me han dicho, la carrera de matemáticas es una carrera de fondo y no de velocidad.

Índice general

Capítulo 1

Introducción

Los registros de desplazamiento con retroalimentación son una tecnología basada en circuitos electrónicos que ha sido utilizada durante décadas en una amplia variedad de aplicaciones. En la década de 1940, los registros de desplazamiento comenzaron a utilizarse en dispositivos electrónicos como calculadoras y computadoras, principalmente para almacenar y manipular datos binarios. En el siglo XX, el desarrollo de la electrónica digital facilitó la aplicación de los registros de desplazamiento en una amplia gama de dispositivos, incluyendo circuitos integrados, microcontroladores y sistemas de comunicación. En la actualidad, siguen siendo un componente esencial en la electrónica digital, con aplicaciones en el control de señales, la generación de códigos y la comunicación de datos. Las aplicaciones más comunes de los registros de desplazamiento con retroalimentación son el almacenamiento y movimiento de datos, el control de señales digitales, la generación de códigos y el control de dispositivos, ver [4].

En este trabajo nos centraremos en su capacidad de generar sucesiones pseudoaleatorias de forma rápida y eficaz, ya que dichas sucesiones son muy utilizadas en la criptografía por sus numerosas propiedades.

En criptografía, los sistemas de cifrado se pueden diferenciar en varios tipos; en particular, se distinguen los cifrados en bloque y los cifrados en flujo. Como su nombre indica, los cifrados en bloque trabajan cifrando bloques de texto de tamaño fijo. Es decir, dado un texto a cifrar, se toman grupos de bits de longitud fija y se cifran. En cambio, los cifrados en flujo toman contenido de tamaño arbitrario y lo cifran bit a bit. Estos son útiles cuando no se conoce el tamaño del texto que se desea cifrar o cuando el texto llega de forma continua bit a bit, como un flujo de información. Un ejemplo de cifrado en flujo es el cifrado de Vernam.

Gilbert Sandford Vernam fue un ingeniero de los laboratorios Bell y de AT&T, quien, en 1917, inventó el cifrado de Vernam. En 1949, Claude Shannon, también de Bell Labs, demostró que este código es indescifrable. Es el primer y único método de cifrado que se ha demostrado que es perfecto. Este cifrado irrompible se basa en el cifrado de Vigenère, el cual se puede entender como una combinación de cifrados de César.

El cifrado de César, ver [7], consiste en sustituir cada letra del mensaje por la que se encuentra r posiciones más adelante en el alfabeto. Es decir, si se toma un alfabeto con 27 letras y estas se numeran, cada letra x del texto se cifra como $f(x) = x + r \mod 27$. Este cifrado se puede romper fácilmente si el texto es largo y se posee una tabla de frecuencias de las letras más usadas del idioma utilizado.

Se podría decir que una evolución de este código es el cifrado de Vigenère [7], en el cual se fija una palabra clave $k = k_1k_2...k_s$ de longitud s, en vez de un solo valor r como en César. Sea $x = x_0x_1x_2...x_n$ el texto que se quiere cifrar, se divide en bloques de longitud s. Cada bit de cada bloque se cifra con el cifrado de César con el valor k_i que corresponda. Es decir, si nos encontramos en el bloque número t, el carácter i de ese bloque se cifra como $f(x_{st+i}) = x_{st+i} + k_i$. A pesar de ser una versión mejorada del cifrado de César, el cifrado de Vigenère no es perfecto. De forma similar, aunque un poco más compleja, se puede descifrar con una tabla de frecuencias si el texto es lo suficientemente largo.

En 1863, Friedrich Wilhelm Kasiski fue el primero en publicar un método (*La escritura secreta y el arte del desciframiento* o *Die Geheimschriften und die Dechiffrir-Kunst*) para descifrar el cifrado de Vigenère sin conocer la palabra clave. Conocido como el método de Kasiski [7], este consiste en calcular la longitud de la clave, a base de buscar palabras repetidas en el texto cifrado. Al encontrar tales palabras, se tiene que, muy probablemente, en esos bits coinciden tanto las letras que se quieren cifrar como el bit de la clave que se utiliza. De esto, la distancia entre las repeticiones será un múltiplo de la longitud de la clave, y si se repiten varias palabras, la longitud de la clave es muy probablemente el máximo común divisor de las distancias entre dichas palabras. Una vez hemos determinado esta longitud, para determinar la clave y poder descifrar el texto, se divide el texto en bloques de tamaño la longitud de la clave y se descifra como en César. Por otro lado, Friedman inventó un método basado en el índice de coincidencia [14], el cual mide la variación de frecuencia de letras para aproximar la longitud de la clave. Sea $x = x_1x_2...x_n$ un texto y sea N el número de letras del alfabeto utilizado, se define el índice de coincidencia de x ($IC(x)$) como la probabilidad de que dos elementos al azar x_i y x_j coincidan. Si f_i, con $i = 1, 2, ..., N$, es la frecuencia de la letra i-ésima del alfabeto en el texto x, entonces:

$$IC(x) = \frac{\sum_{i=1}^{N} f_i(f_i - 1)}{n(n-1)}$$

Finalmente, Vernam perfeccionó el cifrado de Vigenère, ver [7] y [14]. La solución para este código está en qué tipo de clave utilizar. Vernam propuso utilizar claves de longitud mayor o igual que la longitud del texto que se quiere cifrar. Además, planteó utilizar como clave una sucesión aleatoria que se utilice una única vez. Siguiendo la misma notación utilizada en el código anterior, el cifrado de Vernam del bit i sería $f(x_i) = x_i + k_i$. Como ya se ha señalado, Shannon demostró que este cifrado es perfecto, pero tiene una serie de problemas prácticos, ya que no es fácil encontrar claves aleatorias suficientemente largas. Frente a la necesidad de generar sucesiones pseudoaleatorias de gran tamaño, se utilizan los registros de desplazamiento con retroalimentación.

En este trabajo se va a profundizar en las propiedades de las sucesiones generadas por estos registros, buscando sucesiones con periodo grande y que cumplan una serie de propiedades relacionadas con la aleatoriedad. En primer lugar, en el capítulo 2 se introducen resultados preliminares del estudio de sucesiones, de estructuras algebraicas, teoría de Galois y teoría de cuerpos finitos necesarios para poder desarrollar el trabajo.

En el capítulo 3, se definen los registros de desplazamiento con retroalimentación lineal y las sucesiones de recurrencia lineal. Se demuestra que las sucesiones se pueden asociar a polinomios, y además, se dan resultados en relación a la periodicidad de estas sucesiones. Al final del capítulo se estudian las sucesiones impulso respuesta, esenciales para entender cómo obtener las sucesiones con periodo grande.

El capítulo 4 profundiza en propiedades que van a depender de la irreducibilidad de los polinomios asociados a las sucesiones de recurrencia lineal, y define el polinomio mínimo asociado a estas. La finalidad de este capítulo es determinar exactamente el periodo de las sucesiones, y para ello se deberá trabajar previamente en resultados relacionados con el polinomio mínimo y con las familias de sucesiones de recurrencia lineal.

El último capítulo se dedica a las sucesiones máximas, sucesiones con periodos máximos para su orden. Además, se estudiarán las características aleatorias de estas sucesiones y sus propiedades particulares. La finalidad es evaluar si estas sucesiones son buenas candidatas para ser utilizadas como clave en el cifrado de Vernam.

Capítulo 2

Preliminares algebraicos

En este capítulo se introducirán los resultados previos necesarios para entender y demostrar el trabajo. En particular, nos centraremos en la construcción de cuerpos finitos. Se toman como referencia [2], [8], [10] y [11].

2.1. Sucesiones

Debido a que en este trabajo se estudiarán las sucesiones de recurrencia lineal, es fundamental introducir primero algunos resultados básicos sobre sucesiones.

Definición 2.1. *Sea $s = (s_i)_{i=0}^{\infty}$ una sucesión y sea $\tau \geq 0$ un entero no negativo, se define la sucesión desplazada s^τ de s como $s_n^\tau = s_{n+\tau}$ para todo $n \geq 0$, y τ recibe el nombre de desplazamiento. Es decir, s^τ consiste en la sucesión s a partir del elemento s_τ.*

Definición 2.2. *Sea s una sucesión, se dice que*

- *es periódica si existe un número positivo t tal que existe n_0 cumpliendo que $s_{n+t} = s_n$ para todo $n \geq n_0$. Se denomina periodo al menor número que lo cumple.*
- *es preperiódica si es periódica a partir de un término distinto del inicial, es decir, sea t el periodo de la sucesión, existe $n_0 \geq 1$ cumpliendo que $s_{n+t} = s_n$ para todo $n \geq n_0$. Se denomina preperiodo a los valores iniciales previos al periodo.*

Si consideramos las sucesiones $s = 0010110110110...$ y $\bar{s} = 110110110...$ sobre $\mathbb{F}_2$, se observa que ambas son sucesiones periódicas de periodo 3, que s es preperiódica de preperido 4 y $\bar{s}$ no es preperiódica, es más, se tiene que $\bar{s} = s^4$.

Definición 2.3. *La función generatriz $G(x)$ asociada a una sucesión $(s_i)_{i\in\mathbb{N}}$ es la serie de potencias $G(x) = \sum_{i=0}^{\infty} s_i x^i$.*

Además, en el siguiente capítulo se verá que una sucesión de recurrencia lineal tiene asociada una matriz, y se trabajará con el orden de la misma para poder desarrollar ciertos resultados importantes. Es por ello que se define lo siguiente.

Definición 2.4. *Sea A una matriz, se llama orden de A al entero positivo más pequeño n tal que $A^n = Id$, y se escribe $O(A) = n$. Si no existe dicho entero decimos que el orden de A es infinito y se escribe $O(A) = \infty$.*

Aunque usualmente el orden de una matriz representa el número de filas y columnas de la matriz, la definición anterior hace referencia al concepto de orden de la matriz cuando se la considera como elemento de un grupo, que en este trabajo será $GL_n(\mathbb{F}_q)$, el grupo de matrices invertibles cuadradas de tamaño $n \times n$ con coeficientes en un cuerpo finito.

2.2. Estructuras algebraicas y teoría de Galois

Una vez que ya hemos introducido los conceptos clave para este trabajo, para poder enunciar y demostrar el Teorema de Lagrange, se deben conocer previamente las siguientes nociones básicas.

Definición 2.5. *Sea G un grupo, se llama orden de G, denotado por $\#G$, al número de sus elementos. Si tiene infinitos elementos escribimos $\#G = \infty$.*

Considerando el grupo G y un subgrupo $S \subseteq G$, así como la relación R_i de congruencia a la izquierda módulo S (aR_ib si $b^{-1}a \in S$ con $a, b \in G$) y la relación R_d de congruencia a la derecha módulo S (aR_db si $ab^{-1} \in S$ con $a, b \in G$), se pueden definir las clases laterales de la siguiente forma. La clase a la izquierda módulo S es la clase de equivalencia de $a \in G$ para R_i $[a]_{R_i} = aS := \{ax : x \in S\}$, y la clase a la derecha módulo S es la clase de equivalencia de $a \in G$ para R_d $[a]_{R_d} = Sa := \{xa : x \in S\}$. Se puede definir además el conjunto de las clases a la izquierda módulo S como $\mathcal{I} = \{aS : a \in G\}$ y el conjunto de las clases a la derecha módulo S como $\mathcal{D} = \{Sa : a \in G\}$. De esto, se llama índice de S en G al cardinal de $\mathcal{D}$ (o de $\mathcal{I}$, pues son iguales) y se denota por $\#(G : S)$.

Teorema 2.6. ***Teorema de Lagrange.*** *Dado G un grupo finito y sea $S \subseteq G$ un subgrupo, se cumple que $\#G = \#(G : S)\#S$. Como consecuencia, se tiene además que el orden de cada subgrupo de G divide al orden de G.*

Demostración: Como G es finito, se tiene que $\#(G : S) = n \in \mathbb{N}$ es finito. Elegimos $a_i \in G$ para $i \in \{1, ..., n\}$ un representante de cada una de las clases a la izquierda módulo S tal que tenemos $\mathcal{I} = \{a_1S, a_2S, ..., a_nS\}$ y $a_iS \cap a_jS = \emptyset$ con $i \neq j$. Como $G = \bigcup_{a \in G} aS$ se tiene $\#G = \sum_{i=1}^{n} \#(a_iS) = \sum_{i=1}^{n} \#S = n\#S = \#(G : S)\#S$. □

Visto este teorema, podemos entrar en propiedades algebraicas que nos servirán de ayuda para la construcción de cuerpos finitos.

Definición 2.7. *Un grupo G es cíclico si está generado por un solo elemento, es decir, G es cíclico si y solo si existe $a \in G$ tal que $G =< a >$.*

Teorema 2.8. *Se cumple lo siguiente:*

(i) Todo subgrupo de un grupo cíclico es cíclico.

(ii) En un grupo cíclico finito $< a >$ de orden m, el elemento a^k genera un subgrupo de orden m/mcd(k,m).

(iii) Si d es un divisor positivo del orden m de un grupo finito $< a >$, entonces $< a >$ contiene exactamente un subgrupo de índice d. Para cualquier divisor positivo c de m, $< a >$ contiene un subgrupo de orden c.

(iv) Sea c un divisor positivo del orden m del grupo cíclico finito $< a >$, entonces $< a >$ contiene $\varphi(c)$ elementos de orden c, con φ la función de Euler que indica el número de números enteros n, $1 \leq n \leq c$, que son coprimos con c.

(v) Un grupo cíclico finito $< a >$ de orden m contiene $\varphi(m)$ generadores, esto es, elementos a^r tal que $< a^r >=< a >$. Los generadores son las potencias a^r con mcd(r,m)=1.

Demostración: Se tiene que

(i) Sea H un subgrupo del grupo cíclico $< a >$ tal que $H \neq \{e\}$, con $e \in H$ el elemento neutro. Si $a^n \in H$, con $n \in \mathbb{Z}$, se tiene que $a^{-n} \in H$, por lo tanto H contiene al menos una potencia de a con exponente positivo. Sea d el exponente positivo más pequeño tal que $a^d \in H$ y sea $a^s \in H$. Si dividimos s entre d tenemos $s = qd + r$ con $0 \leq r < d$ y $q, r \in \mathbb{Z}$, luego $a^s(a^{-d})^q = a^r \in H$. Si $r \neq 0$ se contradeciría que d fuera el exponente positivo más pequeño tal que $a^d \in H$, luego $r = 0$. Por lo tanto, todos los exponentes de todas las potencias de a que pertenecen a H son divisibles por d, y se tiene entonces que $H =< a^d >$, es decir, H es cíclico.

(ii) Sea $d = mcd(k, m)$. El orden de $< a^k >$ es el número entero positivo n más pequeño tal que $a^{kn} = e$. Esto ocurre si y solo si m divide a kn, o equivalentemente, si y solo si m/d divide a n. El número positivo más pequeño que lo cumple es $n = m/d$.

(iii) Como d es un divisor de m entonces por (ii) se tiene que $< a^d >$ es un subgrupo de orden m/d, y por el Teorema de Lagrange se tiene que es de índice d. Si $< a^k >$ es otro subgrupo de índice d, entonces su orden es m/d y $d = mcd(k, m)$ por (ii). Además, como d divide a k, entonces $a^k \in < a^d >$ y $< a^k >$ es subgrupo de $< a^d >$. Pero como ambos grupos tienen mismo orden, coinciden. Como los subgrupos de orden c son precisamente los subgrupos de índice m/c (por el Teorema de Lagrange) se tiene la segunda parte del resultado.

(iv) Sea $m = dc$, por (ii) un elemento a^k es de orden c si y solo si $mcd(k, m) = d$. Por tanto, el número de elementos de orden c es igual al número de enteros k con $1 \leq k \leq m$ y $mcd(k, m) = d$. Si escribimos $k = dh$ con $1 \leq h \leq c$, la condición $mcd(k, m) = d$ es equivamente a $mcd(h, c) = 1$. El número de estos enteros es precisamente $\varphi(c)$.

(v) Los generadores de $< a >$ son los elementos de orden m, entonces la primera parte se tiene por (iv) y la segunda parte se tiene por (ii). □

Sean K y F cuerpos, se dice que F es una extensión de K si K es un subcuerpo de F y se denota como $K \hookrightarrow F$. El cuerpo F se puede considerar un K-espacio vectorial. La dimensión del espacio vectorial F es igual al grado de la extensión, y se denota por $[F : K] = dim_K F$. Si la dimensión es finita, entonces se dice que F es la extensión finita de K.

Teorema 2.9. *Sea K un cuerpo y F una extensión de K. Dado $f(x) \in K[x]$, $\alpha \in F$ es una raíz múltiple de $f(x)$ si y solo si α es raíz de $f(x)$ y de su derivada $f'(x)$.*

Demostración: Supongamos que $\alpha \in F$ es raíz múltiple de $f(x)$, entonces $f(x) = (x - \alpha)^r g(x)$ para algún $g(x) \in F[x]$ y con $r \geq 2$. Por tanto, $f'(x) = (x-\alpha)^{r-1} g(x) + (x-\alpha)^r g'(x)$ y se tiene $f'(\alpha) = 0$. Supongamos ahora que α es raíz de $f(x)$ y de $f'(x)$. Por tanto, se tiene que $f(x) = (x - \alpha)g(x)$ para algún $g(x) \in F[x]$, luego $f'(x) = g(x) + (x - \alpha)g'(x)$. De esto, $f'(\alpha) = g(\alpha) = 0$, y se tiene $f(x) = (x-\alpha)^2 h(x)$ para algún $h(x) \in F[x]$, es decir, α es raíz múltiple de $f(x)$. □

Sea $K \hookrightarrow F$ una extensión y $u \in F$, se dice que u es algebraico sobre K si existe un polinomio no nulo de $K[x]$ tal que u es raíz. Las extensiones son algebraicas si lo son todos sus elementos. En este trabajo utilizaremos extensiones finitas, y por tanto, algebraicas.

Definición 2.10. *Sea $K \hookrightarrow F$ una extensión y $\alpha \in F$ algebraico sobre K. Se denomina polinomio mínimo de α sobre K al polinomio mónico de menor grado que anula al elemento α.*

Es fácil comprobar que se cumple el siguiente resultado.

Proposición 2.11. *Sea $K \hookrightarrow F$ una extensión y $\alpha \in F$ algebraico sobre K, entonces el polinomio mínimo $g(x)$ de α sobre K cumple las siguientes propiedades:*

(i) $g(x)$ es irreducible en $K[x]$.

(ii) Para un polinomio $f(x) \in K[x]$ se tiene que $f(\alpha) = 0$ si y solo si $g(x)$ divide a $f(x)$.

Teorema 2.12. *Sea L una extensión finita de K y M una extensión finita de L, entonces M es una extensión finita de K tal que $[M : K] = [M : L][L : K]$.*

Demostración: Sea $[L : K] = n$ y $\{\alpha_i\}_{i=1}^n$ base de L como K-espacio vectorial con $\alpha_i \in L$, y sea $[M : L] = m$ y $\{\beta_j\}_{j=1}^m$ base de M como L-espacio vectorial con $\beta_j \in M$. Vamos a ver que $\{\alpha_i\beta_j\}_{\substack{i=1,...,n \\ j=1,...,m}}$, con $\alpha_i\beta_j \in M$, es base de M como K-espacio vectorial. Sea $\gamma \in M$, existen $\lambda_1, ..., \lambda_m \in L$ tal que $\gamma = \sum_{j=1}^m \lambda_j \beta_j$. Además, como $\lambda_j \in L$, se tiene $\lambda_j = \sum_{i=1}^n \mu_{ij}\alpha_i$ con $\mu_{ij} \in K$, luego $\gamma = \sum_{j=1}^m \sum_{i=1}^n \mu_{ij}\alpha_i\beta_j = \sum_{i,j} \mu_{ij}(\alpha_i\beta_j)$. Por lo tanto, $\{\alpha_i\beta_j\}_{i,j}$ es sistema generador.

Sea $\sum_{i,j} \nu_{ij}(\alpha_i\beta_j) = 0$ con $\nu_{ij} \in K$, como $\sum_{i,j} \nu_{ij}(\alpha_i\beta_j) = \sum_{j=1}^m (\sum_{i=1}^n \nu_{ij}\alpha_i)\beta_j$ con $\sum_{i=1}^n \nu_{ij}\alpha_i \in L$, y como $\{\beta_j\}_{j=1}^m$ es base de M como L-espacio vectorial, entonces $\sum_{i=1}^n \nu_{ij}\alpha_i = 0$. Al ser $\{\alpha_i\}_{i=1}^n$ base de L como K-espacio vectorial, entonces $\nu_{ij} = 0$, luego $\{\alpha_i\beta_j\}_{i,j}$ es linealmente independiente. Por lo tanto $\{\alpha_i\beta_j\}_{\substack{i=1,...,n \\ j=1,...,m}}$ es base de M como K-espacio vectorial. □

Siendo R un anillo y considerando el conjunto $C = \{n \in \mathbb{N} : nx = 0 \text{ para todo } x \in R\}$, si C es vacío se dice que la característica de R es 0, es decir, $car(R) = 0$, y si C es no vacío se dice que la característica de R es el mínimo del conjunto C, es decir, $car(R) = min(C)$. Además, la característica de un dominio D es o bien 0 o bien un número primo.

Definición 2.13. *Sea F un cuerpo, se llama subcuerpo primo de F a la intersección de todos los subcuerpos de F, y se representa por $\pi(F)$.*

Se prueba fácilmente el siguiente resultado.

Teorema 2.14. *Sea F un cuerpo, entonces se cumple que $\pi(F) \approx \mathbb{Q}$ o $\pi(F) \approx \mathbb{F}_p$, para algún p primo. Es decir, el subcuerpo primo de un cuerpo F es isomorfo o bien a $\mathbb{F}_p$ si su característica es un número primo p, o bien a $\mathbb{Q}$ si su característica es 0.*

Sea K un cuerpo y $f(x) \in K[x]$ un polinomio. Se dice que $f(x)$ factoriza completamente o escinde en K si es posible escribir $f(x) = a_n(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$ con $\alpha_i \in K$. Además, sea $f(x) \in K[x]$ un polinomio, un cuerpo F, extensión de K, se dice cuerpo de escisión de $f(x)$ sobre K si se cumplen las dos condiciones siguientes

- $f(x)$ escinde en F
- $F = K(\alpha_1, \alpha_2, ..., \alpha_n)$ con $\alpha_1, \alpha_2, ..., \alpha_n$ todas las raices de $f(x)$ en F.

Teorema 2.15. ***Existencia y unicidad de cuerpos de escisión.*** *Si K es un cuerpo y $f(x)$ en $K[x]$ un polinomio de grado positivo $n > 0$, entonces existe un cuerpo de escisión F de $f(x)$ sobre K tal que $[F : K] \leq n!$. Además, cualesquiera dos cuerpos de escisión de $f(x)$ sobre K son isomorfos.*

Demostración: Aplicamos inducción en el grado n del polinomio $f(x) \in K[x]$ para probar la existencia de cuerpos de escisión. Si $n = 1$, tenemos $f(x) = ax + b \in K[x]$ con $a \neq 0$, luego $x = -b/a \in K$. Por lo tanto $F = K$ es el cuerpo de escisión y se tiene $[F : K] = [K : K] = 1 \leq 1!$. Suponemos que es cierto el resultado si el grado de $f(x)$ es $n - 1$. Si el grado del polinomio es n y $f(x)$ escinde en K, entonces el cuerpo de escisión de $f(x)$ es K y se tiene $[F : K] = [K : K] = 1 \leq n!$. Si en cambio, el grado del polinomio es n y $f(x)$ no escinde en K, entonces existe $g(x) \in K[x]$ de grado $d \leq n$ irreducible sobre $K[x]$ tal que $g(x)$ divide a $f(x)$. Existe un cuerpo raíz $K(\alpha)$ de $g(x)$ sobre K para α raíz de $g(x)$ y de $f(x)$, y se tiene $[K(\alpha) : K] = d \leq n$ por ser $g(x)$ irreducible en $K[x]$. Sobre $K(\alpha)$ se tiene que $f(x) = (x - \alpha)h(x)$, siendo el grado de $h(x)$ igual a $n - 1$. Si aplicamos la hipótesis inductiva, tenemos que existe F cuerpo de escisión de $h(x)$ sobre $K(\alpha)$ tal que $[F : K(\alpha)] \leq (n-1)!$. Por lo tanto tenemos $[F : K] = [F : K(\alpha)][K(\alpha) : K] \leq (n-1)!n = n!$ y además $f(x)$ escinde en F. Queda así demostrada la existencia de cuerpos de escisión.

Para probar la unicidad de cuerpos de escisión aplicamos inducción sobre el grado de la extensión $K \hookrightarrow F$. Si $[F : K] = 1$, entonces es claro que el cuerpo de escisión de $f(x)$ sobre K es el propio K. Suponemos cierto el resultado para $[F : K] \leq n - 1$. Si tenemos $[F : K] = n$ y $f(x)$ escinde en K, entonces el cuerpo de escisión de $f(x)$ es K. Si $[F : K] = n$ y $f(x)$ no escinde en K, entonces existe $g(x) \in K[x]$ de grado $d < n$ irreducible sobre $K[x]$ tal que $g(x)$ divide a $f(x)$. Sea α una raíz de $g(x)$, y por tanto raíz de $f(x)$, tal que $\alpha \notin K$, existe entonces un cuerpo raíz $K(\alpha)$ de $g(x)$ sobre K. Por ser $g(x)$ irreducible

en $K[x]$, $K(\alpha)$ es único salvo isomorfismo y se tiene $[K(\alpha) : K] = d < n$. Además, como $[F : K] = [F : K(\alpha)][K(\alpha) : K]$ con $[F : K(\alpha)] \leq n - 1$, por la hipótesis inductiva se tiene que F es único salvo isomorfismo. □

2.3. Cuerpos finitos

Sabemos que $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo si y solo si $n = p$ es un número primo, y lo denotamos como $\mathbb{F}_p$. Por el Teorema 2.14, todo cuerpo F de característica p contiene un subcuerpo isomorfo a $\mathbb{F}_p$. Además, el cuerpo F es una extensión de $\mathbb{F}_p$.

Teorema 2.16. *Sea F un cuerpo finito y K un subcuerpo de F con q elementos, entonces F tiene q^m elementos donde $m = [F : K]$.*

Demostración: F es un K-espacio vectorial, y como F es finito, tiene dimensión finita como espacio vectorial sobre K. Si $[F : K] = m$, entonces F tiene una base sobre K de m elementos, digamos que son $b_1, b_2, ..., b_m$. Luego todo elemento de F se puede representar de manera única de la forma $a_1b_1+a_2b_2+...+a_mb_m$, donde $a_1, a_2, ..., a_m \in K$. Como K contiene q elementos, cada a_i puede tener q valores, luego F tiene exactamente q^m elementos. □

A partir del teorema anterior y del Teorema 2.14, se obtiene entonces el siguiente resultado.

Corolario 2.17. *Sea F un cuerpo finito, entonces F tiene p^n elementos donde p es primo y es la característica de F y n es el grado de F sobre su subcuerpo primo.*

La siguiente propiedad es básica para el trabajo sobre cuerpos finitos. Su demostración es trivial, y se basa en que, si F es un cuerpo finito de q elementos, las unidades de F son un grupo de $q - 1$ elementos y $F = F^* \cup \{0\}$. El resultado se sigue de que el orden de un elemento en un grupo divide al orden del grupo.

Lema 2.18. *Si F es un cuerpo finito con q elementos, entonces todo elemento $a \in F$ cumple $a^q = a$.*

Lema 2.19. *Si F es un cuerpo finito de q elementos y K es un subcuerpo de F, entonces el polinomio $x^q - x \in K[x]$ factoriza en $F[x]$ como $x^q - x = \prod_{a \in F}(x - a)$ y F es cuerpo de escisión de $x^q - x$ sobre K.*

Demostración: El polinomio $x^q - x$ tiene como mucho q raíces en F. Por el Lema 2.18 sabemos que todos los elementos de F son raíces del polinomio, luego $x^q - x$ escinde en F y no escinde en otro cuerpo menor que F. □

Así como se vio la existencia y unicidad de cuerpos de escisión, gracias al lema anterior se puede demostrar el teorema principal para caracterizar cuerpos finitos.

Teorema 2.20. ***Existencia y unicidad de cuerpos finitos.*** *Para todo p primo y todo entero positivo n existe un cuerpo finito con p^n elementos. Todo cuerpo finito de $q = p^n$ elementos es isomorfo al cuerpo de escisión de $x^q - x$ sobre $\mathbb{F}_p$.*

Demostración: Para $q = p^n$ consideramos el polinomio $x^q - x \in \mathbb{F}_p[x]$, y sea F su cuerpo de escisión sobre $\mathbb{F}_p$. Como su derivada $qx^{q-1} - 1 = -1$ en $\mathbb{F}_p[x]$, por el Teorema 2.9 se tiene que el polinomio tiene q raíces distintas en F. Sea $S = \{a \in F : a^q - a = 0\}$, se tiene que $0, 1 \in S$. Como q es la característica de F, entonces se tiene $(a-b)^q = a^q - b^q = a - b$ para todo $a, b \in S$, luego $a - b \in S$. Además, para todo $a, b \in S$ con $b \neq 0$ se tiene que $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, por lo tanto, S es un subcuerpo de F. Entonces, $x^q - x$ escinde en S ya que S contiene todas sus raíces, luego $F = S$, y como S tiene q elementos se tiene que F es un cuerpo finito con q elementos. Queda probada así la existencia y faltaría probar la unicidad. Sea F un cuerpo finito de $q = p^n$ elementos, entonces F tiene característica p por el Corolario 2.17, y entonces $\mathbb{F}_p$ es subcuerpo de F. Por el Lema 2.19 se tiene que F es el cuerpo de escisión de $x^q - x$ sobre $\mathbb{F}_p$, y el resultado buscado es consecuencia de la unicidad de cuerpos de escisión vista en el Teorema 2.15. □

Como consecuencia de lo anterior, se obtiene el siguiente resultado.

Teorema 2.21. *Sea $\mathbb{F}_q$ el cuerpo finito de $q = p^n$ elementos con p primo. Entonces todo subcuerpo de $\mathbb{F}_q$ tiene orden p^m, con m un divisor positivo de n. Si en cambio tenemos que m es un divisor positivo de n, entonces hay exactamente un subcuerpo de $\mathbb{F}_q$ con p^m elementos.*

Es claro que el conjunto de unidades de un cuerpo finito, $\mathbb{F}_q^*$, es un grupo. Además, este grupo es cíclico. A un generador del grupo cíclico $\mathbb{F}_q^*$ se le denomina elemento primitivo de $\mathbb{F}_q$, y por el Teorema 2.8 (v) tenemos que $\mathbb{F}_q$ contiene $\varphi(q-1)$ elementos primitivos.

A lo largo de este trabajo se verá la importancia de los polinomios en los registros de desplazamiento con retroalimentación lineal, donde las propiedades de irreducibilidad tendrán un papel importante. De la Proposición 2.11, se sigue el siguiente resultado.

Lema 2.22. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ y sea α una raíz de $f(x)$ en una extensión de $\mathbb{F}_q$. Dado un polinomio $h(x) \in \mathbb{F}_q[x]$, se tiene que $h(\alpha) = 0$ si y solo si f(x) divide a h(x).*

Lema 2.23. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado k irreducible sobre $\mathbb{F}_q$. Entonces f(x) divide a $x^{q^n} - x$ si y solo si k divide a n.*

Demostración: Supongamos que $f(x)$ divide a $x^{q^n} - x$. Sea α raíz de $f(x)$ en el cuerpo de escisión de $f(x)$ sobre $\mathbb{F}_q$, entonces tenemos $\alpha^{q^n} = \alpha$. Luego $\alpha \in \mathbb{F}_{q^n}$ y $\mathbb{F}_q(\alpha)$ es subcuerpo de $\mathbb{F}_{q^n}$. Como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = k$ y $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, entonces por el Teorema 2.12 se tiene que k divide a n.
Supongamos que k divide a n, entonces por el Teorema 2.21, $\mathbb{F}_{q^k}$ es subcuerpo de $\mathbb{F}_{q^n}$. Sea α raíz de $f(x)$ en el cuerpo de escisión de $f(x)$ sobre $\mathbb{F}_q$, entonces tenemos $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = k$ y $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$. Por lo tanto, como $\alpha \in \mathbb{F}_{q^k}$ y $\mathbb{F}_{q^k}$ es subcuerpo de $\mathbb{F}_{q^n}$, se tiene que $\alpha \in \mathbb{F}_{q^n}$. Por tanto, $\alpha^{q^n} = \alpha$, luego α es raíz de $x^{q^n} = x \in \mathbb{F}_q[x]$. Por el Lema 2.22 tenemos entonces que $f(x)$ divide a $x^{q^n} - x$. □

Teorema 2.24. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado k irreducible sobre $\mathbb{F}_q$, entonces $f(x)$ tiene una raíz α en $\mathbb{F}_{q^k}[x]$. Además, todas las raíces de $f(x)$ son simples, siendo estas $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{k-1}} \in \mathbb{F}_{q^k}[x]$.*

Demostración: Sea α una raíz de $f(x)$ en el cuerpo de escisión de $\mathbb{F}_q$. Entonces el grado de la extensión es $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = k$ y por tanto $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$ y $\alpha \in \mathbb{F}_{q^k}$. Veamos que si $\beta \in \mathbb{F}_{q^k}$ es una raíz de $f(x)$ entonces β^q también es raíz de $f(x)$. Sea $f(x) = a_k x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0$ con $a_i \in \mathbb{F}_q$ para $0 \leq i \leq k$, entonces tenemos $f(\beta^q) = a_k\beta^{qk} + ... + a_1\beta^q + a_0$, y por el Lema 2.18, $f(\beta^q) = a_k\beta^{qk} + ... + a_1\beta^q + a_0 = a_k^q\beta^{qk} + ... + a_1^q\beta^q + a_0^q$. Como el cuerpo finito $\mathbb{F}_q = \mathbb{F}_{p^n}$ tiene característica p, tenemos que $(a+b)^q = (a+b)^{p^n} = a^{p^n} + b^{p^n} = a^q + b^q$ para todo $a, b \in \mathbb{F}_q$, y por lo tanto, $f(\beta^q) = a_k^q\beta^{qk} + ... + a_1^q\beta^q + a_0^q = (a_k\beta^k + ... + a_1\beta + a_0)^q = f(\beta)^q = 0$. Tenemos entonces que $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{k-1}}$ son raíces de $f(x)$. Para ver que son raíces distintas supongamos por reducción al absurdo que $\alpha^{q^i} = \alpha^{q^j}$ para $0 \leq i < j \leq k-1$. Si elevamos esta identidad a q^{k-j} tenemos $\alpha^{q^{k-j+i}} = \alpha^{q^k} = \alpha$. Por el Lema 2.22, se tiene que $f(x)$ divide a $x^{q^{k-j+i}} - x$, y por el Lema 2.23, esto se tiene si y solo si k divide a $k-j+i$, en contra con $0 < k - j + i < k$. Luego las raíces $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{k-1}}$ son simples. □

Se ha probado entonces que $f(x)$ escinde en $\mathbb{F}_{q^k}$ y además $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{k-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$ para una raíz α de $f(x)$ en $\mathbb{F}_{q^k}$. Se tiene entonces el siguiente resultado.

Corolario 2.25. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado k, entonces el cuerpo de escisión de $f(x)$ sobre $\mathbb{F}_q[x]$ es $\mathbb{F}_{q^k}[x]$.*

Definición 2.26. *Sea $\mathbb{F}_{q^k}$ una extensión de $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^k}$, entonces los elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{k-1}}$ se denominan conjugados de α respecto a $\mathbb{F}_q$.*

Teorema 2.27. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado k y $\alpha \in \mathbb{F}_{q^k}$ una raíz de $f(x)$. Entonces, los conjugados de $\alpha \in \mathbb{F}_{q^k}$ tienen el mismo orden en el grupo $\mathbb{F}_{q^k}^*$.*

Demostración: Sabemos que $\mathbb{F}_{q^k}^*$ es un grupo cíclico de orden $q^k - 1$, y como $\alpha \in \mathbb{F}_{q^k}^*$, por el Teorema 2.8 (ii) se tiene que α^{q^m}, con $1 \leq m \leq k-1$, genera un subgrupo de orden $d/mcd(q^m, d)$, con d un divisor de $q^k - 1$. Como $mcd(q^m, d) = 1$ para $1 \leq m \leq k-1$, se tiene que α^{q^m} genera un subgrupo de orden d, es decir, tiene el mismo orden que α. □

Además de la irreducibilidad, que el polinomio con el que trabajemos sea primitivo será esencial para poder encontrar las sucesiones aleatorias buscadas. Para poder definir un polinomio primitivo antes se tiene que hablar del orden de un polinomio.

Proposición 2.28. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado $k \geq 1$ y $f(0) \neq 0$. Entonces, existe un entero positivo e menor o igual que $q^k - 1$ tal que $f(x)$ divide a $x^e - 1$.*

Demostración: Como $f(x)$ es de grado k, entonces el anillo $\mathbb{F}_q[x]/(f)$ contiene q^k clases $b_0 + b_1x + b_2x^2 + ... + b_{k-1}x^{k-1} + (f(x))$ con $b_i \in \mathbb{F}_q$, y una de ellas cumple $b_i = 0$ para todo $0 \leq i \leq k-1$, que es la clase del cero. Por otra parte, se consideran las q^k clases $x^j + (f(x))$ con $j = 0, 1, ..., q^k - 1$. Todas ellas son distintas de la clase $0 + (f(x))$, luego por el Principio del Palomar debe haber dos iguales. Es decir, existen r y s enteros con $0 \leq r \lneq s \leq q^k - 1$ tal que $x^s \equiv x^r \mod (f(x))$. Como $f(0) \neq 0$, se tiene que $\text{mcd}(x, f(x)) = 1$ luego $x^{s-r} \equiv 1 \mod (f(x))$. Por tanto, $f(x)$ divide a $x^{s-r} - 1$, y tomando $e = s - r \leq q^k - 1$ se tiene el resultado. □

Definición 2.29. *Sea $f(x) \neq 0 \in \mathbb{F}_q[x]$ un polinomio con $f(0) \neq 0$, se denomina orden de $f(x)$ al menor entero e tal que $f(x)$ divide a $x^e - 1$, y se denota por ord(f). Si $f(0) = 0$, entonces se tiene $f(x) = x^h g(x)$, donde $h \in \mathbb{N}$ y $g(x) \in \mathbb{F}_q[x]$ con $g(0) \neq 0$, y en este caso el orden de $f(x)$ es definido como ord(g).*

Como cualquier polinomio constante divide a $x - 1$ en $\mathbb{F}_q[x]$, los polinomios constantes se incluyen en la definición anterior y tienen orden igual a 1.

Del Corolario 2.25, el Teorema 2.27, el Lema 2.22 y las definiciones de orden de un polinomio y orden de un elemento en el grupo $\mathbb{F}^*_{q^k}$, se sigue el siguiente resultado directamente.

Teorema 2.30. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado k irreducible sobre $\mathbb{F}_q$ cumpliendo $f(0) \neq 0$, entonces el orden de $f(x)$ coincide con el orden de cualquier raíz de $f(x)$ en el grupo multiplicativo $\mathbb{F}^*_{q^k}$.*

Y a partir del teorema anterior se tiene la siguiente propiedad para polinomios irreducibles.

Corolario 2.31. *Sea $f(x) \neq 0 \in \mathbb{F}_q[x]$ un polinomio de grado k irreducible, entonces el orden del polinomio divide a $q^k - 1$.*

Los siguientes resultados serán de ayuda a la hora de determinar todos los posibles periodos de la sucesión con la que trabajaremos, en función del polinomio asociado que tenga.

Lema 2.32. *Sea c un entero positivo y $f(x) \in \mathbb{F}_q[x]$ un polinomio tal que $f(0) \neq 0$, entonces $f(x)$ divide a $x^c - 1$ si y solo si $ord(f)$ divide a c.*

Demostración: Si $e = ord(f)$ divide a c, entonces $x^e - 1$ divide a $x^c - 1$, y como $f(x)$ divide a $x^e - 1$, se tiene que $f(x)$ divide a $x^c - 1$. Por otro lado, si $f(x)$ divide a $x^c - 1$, tenemos que $c \geq e$ y podemos escribir $c = me + r$, con $m \in \mathbb{N}$ y $0 \leq r < e$. Como $x^c - 1 = (x^{me} - 1)x^r + (x^r - 1)$, se tiene que $f(x)$ divide a $x^r - 1$, que solo es posible si $r = 0$, luego tenemos que e divide a c. □

Teorema 2.33. *Sea $g(x) \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ con $g(0) \neq 0$ y $ord(g) = e$, y sea $f(x) = g(x)^b$ con b un entero positivo. Si t es el menor entero que cumple $p^t \geq b$, con p la característica de $\mathbb{F}_q$, entonces $ord(f) = ep^t$.*

Demostración: Sea $c = ord(f)$, nótese que como $f(x)$ divide a $x^c - 1$, $g(x)$ también divide a $x^c - 1$, luego por el Lema 2.32 e divide a c. Además, como $g(x)$ divide a $x^e - 1$, $f(x)$ divide a $(x^e - 1)^b$, que a su vez divide a $(x^e - 1)^{p^t} = x^{ep^t} - 1$. Luego $f(x)$ divide a $x^{ep^t} - 1$, y por el Lema 2.32, c divide a ep^t. Como e divide a c y c divide a ep^t, se tiene que $c = ep^u$, con $0 \leq u \leq t$. Veamos que $u = t$.

Por el Corolario 2.31, e divide a $q^k - 1$, con k el grado de $g(x)$. Como p es la característica de $\mathbb{F}_q$, es claro que p no divide a $q^k - 1$, luego e no es múltiplo de p. La derivada de $x^e - 1$ es ex^{e-1}. Si $e = 1$, es claro que $x^e - 1$ no tiene raíces múltiples. Si $e > 2$, como la única raíz de ex^{e-1} es 0 y 0 no es raíz de $x^e - 1$, por el Teorema 2.9, $x^e - 1$ no tiene raíces múltiples. Por tanto, $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ tiene e raíces distintas y todas tienen multiplicidad

p^u. Además, $g(x)$ es irreducible, luego por el Teorema 2.24 no tiene raíces múltiples. Por tanto, $f(x) = g(x)^b$ tiene las mismas raíces de $g(x)$ con multiplicidad b. Como $g(x)^b$ divide a $x^{ep^u} - 1$, comparando multiplicidades se tiene que $p^u \geq b$, luego $u \geq t$, ya que t es el menor entero que cumple $p^t \geq b$. Por tanto, se tiene que $u = t$. □

Teorema 2.34. *Sean $g_1(x), ..., g_h(x)$ polinomios no nulos y primos entre sí sobre $\mathbb{F}_q[x]$, y sea $f(x) = g_1(x) \cdot ... \cdot g_h(x)$, entonces $ord(f) = mcm(ord(g_1), ..., ord(g_h))$.*

Demostración: Es fácil ver que para demostrar el resultado basta considerar el caso $g(0) \neq 0$ para $1 \leq i \leq h$. Sea $e = ord(f)$ y $e_i = ord(g_i)$, para $1 \leq i \leq h$, y sea $c = mcm(e_1, ..., e_h)$. Entonces, como cada $g_i(x)$ divide a $x^{e_i} - 1$, se tiene que todo $g_i(x)$ divide a $x^c - 1$. Como $g_1(x), ..., g_h(x)$ son primos entre sí, $f(x)$ divide $x^c - 1$, y por el Lema 2.32, e divide a c. Como $f(x)$ divide a $x^e - 1$, cada $g_i(x)$ divide a $x^e - 1$, y por el Lema 2.32, cada e_i divide a e. Por tanto, c divide a e y se tiene entonces que $e = c$. □

Usando el mismo razonamiento de los teoremas anteriores, se puede ver que el orden del mínimo común múltiplo de un número finito de polinomios no nulos es igual al mínimo común múltiplo de los órdenes de los polinomios.

Ejemplo 2.35. *Sea $f(x) = x^8+x^7+x^6+x^4+x^3+x+1 = (x^3+x+1)^2(x^2+x+1) \in \mathbb{F}_2[x]$. Como $ord(x^3+x+1) = 7$, se tiene por el Teorema 2.33 que $ord((x^3+x+1)^2) = 14$. Además, como $ord(x^2 + x + 1) = 3$, por el Teorema 2.34, $ord(f) = mcm(14, 3) = 42$. Nótese que $ord(f)$ no divide a $2^8 - 1$, ya que el Corolario 2.31 no se cumple necesariamente para polinomios reducibles.*

Por tanto, de los teoremas 2.33 y 2.34 se sigue la siguiente fórmula general para el orden de un polinomio.

Teorema 2.36. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado positivo tal que $f(0) \neq 0$. Sea $f(x) = af_1^{b_1}(x) \cdot ... \cdot f_k^{b_k}(x)$ con $a \in \mathbb{F}_q$, $b_1, ..., b_k \in \mathbb{N}$ y $f_1(x), ..., f_k(x)$ polinomios mónicos, irreducibles sobre $\mathbb{F}_q$ y distintos. Entonces, $ord(f) = p^t mcm(ord(f_1), ..., ord(f_k))$, con t el menor entero tal que $p^t \geq max(b_1, ..., b_k)$, y p la característica de $\mathbb{F}_q$.*

Definición 2.37. *Sea $f(x) \neq 0 \in \mathbb{F}_q[x]$ un polinomio de grado k, se dice que es primitivo sobre $\mathbb{F}_q$ si es mónico, irreducible y tiene orden $q^k - 1$.*

Si $f(x) \in \mathbb{F}_q[x]$ es un polinomio primitivo de grado k, entonces tiene orden $q^k - 1$ por definición. Además, por el Teorema 2.30, si $\alpha \in \mathbb{F}_{q^k}$ es una raíz de $f(x)$, α tiene orden $q^k - 1$, y por tanto, α es un elemento primitivo de $\mathbb{F}_{q^k}^*$, es decir, es un generador de este grupo cíclico y $f(x)$ es su polinomio mínimo.

Reciprocamente, si $\alpha \in \mathbb{F}_{q^k}$ es un generador del grupo $\mathbb{F}_{q^k}^*$, su orden es $q^k - 1$ y su polinomio mínimo es de grado k. Además, sea $f(x)$ el polinomio mínimo de α, por el Teorema 2.30, el orden de $f(x)$ es $q^k - 1$, y por tanto, $f(x)$ es primitivo.

Es decir, ser polinomio primitivo en $\mathbb{F}_{q^k}$ es equivalente a ser el polinomio mínimo de un elemento primitivo de $\mathbb{F}_{q^k}^*$.

Teorema 2.38. *Para cada grado k, en $\mathbb{F}_q[x]$ existen $\varphi(q^k - 1)/k$ polinomios primitivos de grado k.*

Demostración: En el grupo cíclico $\mathbb{F}_{q^k}^*$ existen $\varphi(q^k-1)$ elementos primitivos. Como cada polinomio irreducible de grado k tiene k raíces, y por el Teorema 2.27, todas las raíces tienen el mismo orden en $\mathbb{F}_{q^k}^*$, entonces todos los elementos primitivos se distribuyen en $\varphi(q^k-1)/k$ polinomios primitivos. □

Es necesario introducir unos conceptos clave en relación con la traza de un elemento en un cuerpo finito. Estas propiedades servirán de ayuda en ciertos resultados del trabajo, donde se tratará con la traza de raíces de polinomios.

Definición 2.39. *Sea $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ una extensión de cuerpos y sea α un elemento de $\mathbb{F}_{q^n}$. La traza de α se define como $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{n-1}}$. Si además, $q = p$ es primo, se dice que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ es la traza absoluta de α.*

Proposición 2.40. *Sea $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ una extensión de cuerpos, se cumplen las siguientes propiedades:*

(i) $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$ *para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$.

(ii) $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *para todo* $c \in \mathbb{F}_q$ *y todo* $\alpha \in \mathbb{F}_{q^n}$.

(iii) $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *es una transformación lineal de* $\mathbb{F}_{q^n}$ *en* $\mathbb{F}_q$, *con* $\mathbb{F}_{q^n}$ *y* $\mathbb{F}_q$ *considerados* $\mathbb{F}_q$*-espacios vectoriales.*

Demostración: Como los cuerpos $\mathbb{F}_q = \mathbb{F}_{p^m}$ y $\mathbb{F}_{q^n} = \mathbb{F}_{p^{mn}}$ son cuerpos finitos de característica p, se tiene que

(i) Al ser $\alpha+\beta$ un elemento de $\mathbb{F}_{q^n}$, entonces $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = \alpha+\beta+(\alpha+\beta)^q + ... + (\alpha+\beta)^{q^{n-1}} = \alpha+\beta+\alpha^q+\beta^q+...+\alpha^{q^{n-1}}+\beta^{q^{n-1}} = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$.

(ii) Al ser c un elemento de $\mathbb{F}_q$ se tiene que $c^{q^j} = c$ con $j \geq 0$, luego $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = c\alpha + c^q\alpha^q + ... + c^{q^{n-1}}\alpha^{q^{n-1}} = c\alpha + c\alpha^q + ... + c\alpha^{q^{n-1}} = cTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

(iii) Como $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$, de las propiedades (i) y (ii) se tiene que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ es una transformación lineal de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$. Falta probar que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ es sobreyectiva. Basta con ver que existe $\alpha \in \mathbb{F}_{q^n}$ tal que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$. Sea $\alpha \in \mathbb{F}_{q^n}$, se tiene $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ si y solo si α es raíz del polinomio $x^{q^{n-1}} + ... + x^q + x \in \mathbb{F}_q$ en $\mathbb{F}_{q^n}$. El polinomio tiene como mucho q^{n-1} raíces y $\mathbb{F}_{q^n}$ tiene q^n elementos, luego existe un elemento α de $\mathbb{F}_{q^n}$ tal que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$. □

Teorema 2.41. *Sea $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ una extensión finita, entonces las transformaciones lineales de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$ son exactamente las aplicaciones θ_β, con $\beta \in \mathbb{F}_{q^n}$ y donde $\theta_\beta(\alpha) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta\alpha)$ para todo $\alpha \in \mathbb{F}_{q^n}$. Además, si $\beta \neq \gamma$ son elementos distintos de $\mathbb{F}_{q^n}$, entonces se tiene $\theta_\beta \neq \theta_\gamma$.*

Demostración: Por la Proposición 2.40 (iii), cada aplicación θ_β es una transformación lineal de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$. Sean $\beta, \gamma \in \mathbb{F}_{q^n}$ con $\beta \neq \gamma$, se tiene que $\theta_\beta(\alpha) - \theta_\gamma(\alpha) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta\alpha) - Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma\alpha) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}((\beta-\gamma)\alpha) \neq 0$ para cierto $\alpha \in \mathbb{F}_{q^n}$, y se tiene que las aplicaciones θ_β

y θ_γ son distintas. Además, como toda transformación lineal de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$ puede obtenerse asignando elementos arbitrarios de $\mathbb{F}_q$ a los n elementos de una base dada de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, y como esto puede hacerse de q^n maneras diferentes, se tiene que las aplicaciones θ_β, con $\beta \in \mathbb{F}_{q^n}$, ocupan todas las posibles transformaciones lineales de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$. □

Teorema 2.42. ***Transitividad de la traza.*** *Sean $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ y $\mathbb{F}_{q^n} \hookrightarrow \mathbb{F}_{q^{nm}}$ extensiones de cuerpos, entonces $Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^n}}(\alpha))$ para todo $\alpha \in \mathbb{F}_{q^{nm}}$.*

Demostración: Sea $\alpha \in \mathbb{F}_{q^{nm}}$,

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^n}}(\alpha)) = \sum_{i=0}^{n-1} Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^n}}(\alpha)^{q^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} \alpha^{q^{nj}} \right)^{q^i} =$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha^{q^{nj+i}} = \sum_{k=0}^{nm-1} \alpha^{q^k} = Tr_{\mathbb{F}_{q^{nm}}/\mathbb{F}_q}(\alpha)$$

□

Definición 2.43. *Sea $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ una extensión de cuerpos. Las bases $\{\alpha_1, ..., \alpha_n\}$ y $\{\beta_1, ..., \beta_n\}$ de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se dicen que son duales o complementarias si para $1 \leq i, j \leq n$ se tiene*

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i \beta_j) = \begin{cases} 0 & si\ i \neq j, \\ 1 & si\ i = j \end{cases}$$

Teorema 2.44. *Sean $\{\alpha_1, ..., \alpha_n\}$ y $\{\beta_1, ..., \beta_n\}$ bases duales de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Si $x = x_1\alpha_1 + x_2\alpha_2 + ... + x_n\alpha_n \in \mathbb{F}_{q^n}$ con $x_j \in \mathbb{F}_q$, entonces $x_j = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j x)$ para $1 \leq j \leq n$.*

Demostración: Por la Proposición 2.40 y la definición de bases duales se tiene que

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j x) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j x_1 \alpha_1 + \beta_j x_2 \alpha_2 + ... + \beta_j x_n \alpha_n) =$$

$$= x_1 Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j \alpha_1) + x_2 Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j \alpha_2) + ... + x_j Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j \alpha_j) + ... + x_n Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta_j \alpha_n) = x_j$$

□

Capítulo 3

SLR y primeras propiedades

Como ya se ha indicado previamente, los registros de desplazamiento con retroalimentación, o más conocidos en inglés como FSR (Feedback Shift Register), son dispositivos utilizados para generar sucesiones de manera rápida y pseudoaleatoria. Las sucesiones que generan tienen buenas propiedades estadísticas, que son útiles en criptografía, en particular en el cifrado en flujo. Para este capítulo se tomarán como referencia [6], [9], [10], [11] y [12].

Los FSRs pueden entenderse como leyes de recurrencia que, junto con unos valores iniciales, generan las sucesiones buscadas. En este trabajo nos centraremos en los registros de desplazamiento con retroalimentación lineal o LFSRs (Linear Feedback Shift Registers) sobre cuerpos finitos, que son los asociados a recurrencias lineales.

Las sucesiones de recurrencia lineal (SLR) se pueden clasificar como homogéneas o no homogéneas.

Definición 3.1. *Sean $a, a_0, ..., a_{k-1}$ elementos del cuerpo finito $\mathbb{F}_q$ con $a_0 \neq 0$. Para $n = 0, 1, ...$, una sucesión $s = (s_i)_{i=0}^{\infty}$ se dice que es una*

- *SLR no homogénea de orden k con coeficientes constantes si satisface la ley de recurrencia*

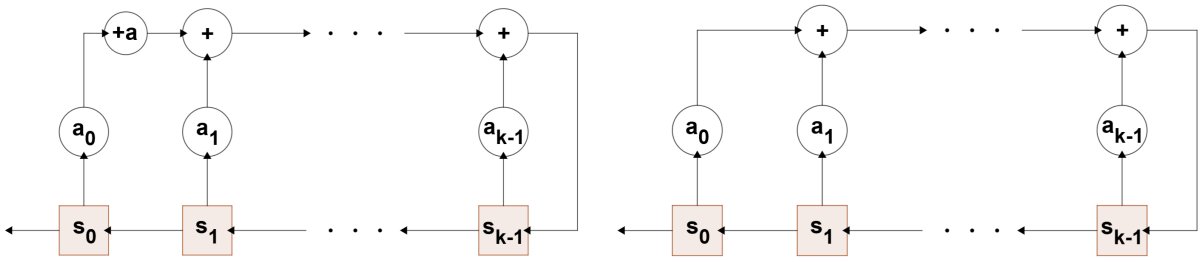
$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n + a \quad , n \geq 0 \tag{3.1}$$

- *SLR homogénea de orden k con coeficientes constantes si satisface la ley de recurrencia*

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n \quad , n \geq 0 \tag{3.2}$$

Se puede describir una SLR, homogénea o no, mediante un circuito de desplazamiento con retroalimentación. En la Figura 3.1 se muestra la noción de desplazamiento con retroalimentación; ambos dispositivos se basan en implementaciones que dependen de los términos precedentes, obteniendo así el siguiente término de la sucesión a partir de los ya existentes.

A pesar de haber definido SLRs homogéneas y no homogéneas, únicamente se trabajará con las homogéneas, ya que se puede obtener una homogénea partiendo de una que no lo



(a) LFSR no homogéneo que satisface (3.1). (b) LFSR homogéneo que satisface (3.2).

Figura 3.1

es. Sea s una SLR no homogénea de orden k que satisface (3.1). Se tiene que también satisface entonces

$$s_{n+k+1} = a_{k-1}s_{n+k} + a_{k-2}s_{n+k-1} + ... + a_0 s_{n+1} + a$$

Restando ambas se tiene

$$s_{n+k+1} - s_{n+k} = a_{k-1}s_{n+k} + (a_{k-2} - a_{k-1})s_{n+k-1} + (a_{k-3} - a_{k-2})s_{n+k-2} + ... + (a_0 - a_1)s_{n+1} - a_0 s_n + a - a$$

$$s_{n+k+1} = (a_{k-1} - 1)s_{n+k} + (a_{k-2} - a_{k-1})s_{n+k-1} + ... + (a_0 - a_1)s_{n+1} - a_0 s_n$$

obteniendo así una SLR homogénea de orden $k+1$.

Definimos las SLRs con $a_0 \neq 0$ ya que, en caso contrario, tendríamos una sucesión de orden menor; en el caso de la ecuación (3.2) si $a_0 = a_1 = ... = a_i = 0$ y $a_{i+1} \neq 0$, tendríamos que la SLR es de orden $k-i$. A partir de ahora, si no se especifica lo contrario, supondremos que toda sucesión de recurrencia lineal es homogénea de orden k.

Definición 3.2. *Dada una SLR de orden k, a los primeros k términos $s_0, s_1, ..., s_{k-2}, s_{k-1}$ se les conoce como estado inicial.*

Si se toma el estado inicial nulo entonces se tiene la sucesión nula para toda ley de recurrencia de orden k. Por ello, para el estudio de las SLRs solo se toman estados iniciales no nulos, por tanto, el conjunto de estos estados tiene cardinal $q^k - 1$.

Definición 3.3. *Dada una ecuación de recurrencia homogénea $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n$, existe un polinomio $f(x) \in \mathbb{F}_q[x]$ asociado a ella llamado polinomio característico o polinomio de retroalimentación*

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_1 x - a_0 \tag{3.3}$$

El LFSR es equivalente al polinomio característico, pues el coeficiente que multiplica a x^i del polinomio característico coincide con el opuesto de la constante que multiplica al término s_{n+i} de la recurrencia, con $0 \leq i \leq k-1$. Por tanto, un LFSR se puede dar mediante el circuito descrito en la Figura 3.1, la ley de recurrencia (3.2) o el polinomio (3.3). El polinomio característico junto al estado inicial determinan unívocamente la SLR, a partir

del polinomio asociado a la sucesión, $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_0$, y dado el estado inicial $s_0, s_1, ..., s_{k-2}, s_{k-1}$, el término s_{n+k} es $a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n$.

El polinomio idénticamente nulo $f(x) = 0 \in \mathbb{F}_q[x]$ está asociado a cualquier SLR, ya que por definición, el polinomio nulo está asociado a las SLRs que cumplan $0 = 0$, es decir, toda sucesión.

A pesar de buscar la aleatoriedad, las sucesiones generadas mediante LFSRs no son realmente aleatorias, sino que son periódicas, como se muestra a continuación.

Notación: Denotemos la *sucesión vectorial* asociada a la SLR s como $S_n = (s_n, s_{n+1}, ..., s_{n+k-1})$ para todo $n \geq 0$.

Lema 3.4. *Toda SLR de orden k sobre el cuerpo finito $\mathbb{F}_q$ es periódica, y su periodo es a lo sumo $q^k - 1$.*

Demostración: Partimos de una SLR de orden k y del estado inicial $(s_0, s_1, ..., s_{k-1}) \neq (0, ..., 0)$. Sea $S_r = (s_r, s_{r+1}, ..., s_{r+k-1})$ una lista de k elementos consecutivos de la sucesión. Tomamos las listas $S_0, S_1, ..., S_{q^k-1}$ y vamos a demostrar que existen $i, j \in \mathbb{Z}$ con $0 \leq i < j \leq q^k - 1$ tales que $S_i = S_j$. Cada una de estas listas es una lista de tamaño k de elementos de $\mathbb{F}_q$ y hemos tomado q^k listas. Por otro lado, todas las combinaciones posibles de elementos que puede haber en una lista son q^k. Si alguna $S_r = (0, 0, ..., 0)$ entonces $S_t = (0, 0, ..., 0)$ para todo $t \geq r$, es decir, la sucesión sería la sucesión constante igual a cero y su periodo es $1 < q^k - 1$. Considerando entonces las sucesiones no nulas tenemos $q^k - 1$ posibles listas. Como tenemos q^k listas y solo $q^k - 1$ posibles, por el Principio del Palomar se tiene que al menos dos se repiten. Es decir, existen $i, j \in \mathbb{N}$ con $0 \leq i < j \leq q^k - 1$ tales que $S_i = S_j$. Ahora, como el elemento s_{i+k} depende de S_i y el elemento s_{j+k} depende de S_j, al ser $S_i = S_j$, entonces $s_{i+m} = s_{j+m}$ para todo $m \geq 0$, es decir, la sucesión es periódica y el periodo es como mucho $j - i - 1$. Como teníamos que $0 \leq i < j \leq q^k - 1$, se tiene entonces que $0 \leq j - i - 1 \leq q^k - 1$, o lo que es lo mismo, el periodo es a lo sumo $q^k - 1$. □

Observación 3.5. *Si se partiera de una SLR no homogénea de orden k, se tendría en su lugar que su periodo estaría acotado superiormente por q^k en vez de por $q^k - 1$, ya que sí se admitiría el vector nulo.*

Además, tal como se muestra a continuación, toda SLR es periódica desde el primer término de la sucesión.

Proposición 3.6. *Toda SLR de orden k es no preperiódica.*

Demostración: Supongamos por reducción al absurdo que, siendo $a_0 \neq 0$, la sucesión s es preperiódica. Sea el preperiodo $n_0 \geq 1$ y el periodo r, se tiene que

$$s_{n+r} = s_n \qquad \forall n \geq n_0 \tag{3.4}$$

Tomemos $n = n_0 + r - 1$ en la ley de recurrencia (3.2), obteniendo así

$$s_{n_0+r+k-1} = a_{k-1}s_{n_0+r+k-2} + a_{k-2}s_{n_0+r+k-3} + ... + a_1 s_{n_0+r} + a_0 s_{n_0+r-1}$$

Como $a_0 \neq 0$, podemos despejar s_{n_0+r-1} de la siguiente manera

$$s_{n_0+r-1} = a_0^{-1}(s_{n_0+r+k-1} - a_{k-1}s_{n_0+r+k-2} - a_{k-2}s_{n_0+r+k-3} - ... - a_1 s_{n_0+r})$$

$$= a_0^{-1}(s_{n_0+k-1} - a_{k-1}s_{n_0+k-2} - a_{k-2}s_{n_0+k-3} - ... - a_1 s_{n_0})$$

por (3.4). Como $s_{n_0+k-1} = a_{k-1}s_{n_0+k-2} + a_{k-2}s_{n_0+k-3} + ... + a_1 s_{n_0} + a_0 s_{n_0-1}$ por (3.2), se tiene que

$$s_{n_0-1} = a_0^{-1}(s_{n_0+k-1} - a_{k-1}s_{n_0+k-2} - a_{k-2}s_{n_0+k-3} - ... - a_1 s_{n_0})$$

es decir, llegamos a $s_{n_0+r-1} = s_{n_0-1}$, lo cual es absurdo pues s_{n_0-1} es un elemento del preperiodo. □

Ejemplo 3.7. *Veamos un ejemplo de una sucesión de recurrencia lineal sobre* $\mathbb{F}_2$. *Sea el estado inicial* $(s_0, s_1, s_2, s_3, s_4) = (1, 1, 0, 1, 0)$ *y sea el polinomio* $f(x) = x^5 + x^2 + x + 1$. *Se tiene entonces la siguiente ley de recurrencia*

$$s_{n+5} = s_{n+2} + s_{n+1} + s_n$$

y los siguientes primeros valores son

$$n = 0 : s_5 = s_2 + s_1 + s_0 = 0 + 1 + 1 = 0$$
$$n = 1 : s_6 = s_3 + s_2 + s_1 = 1 + 0 + 1 = 0$$
$$n = 2 : s_7 = s_4 + s_3 + s_2 = 0 + 1 + 0 = 1$$
$$n = 3 : s_8 = s_5 + s_4 + s_3 = 0 + 0 + 1 = 1$$
$$n = 4 : s_9 = s_6 + s_5 + s_4 = 0 + 0 + 0 = 0$$
$$n = 5 : s_{10} = 1 + 0 + 0 = 1$$
$$n = 6 : s_{11} = 1 + 1 + 0 = 0$$
$$n = 7 : s_{12} = 0 + 1 + 1 = 0$$
$$n = 8 : s_{13} = 1 + 0 + 1 = 0$$
$$. \quad . \quad . \quad .$$

Luego obtenemos la sucesión 11010001101000... que tiene periodo 7. En la Figura 3.2 se puede ver el circuito que genera esta SLR.
Si en cambio, se parte del estado inicial $(s_0, s_1, s_2, s_3, s_4) = (0, 0, 1, 0, 1)$, *mediante el mismo procedimiento, se tiene la sucesión 00101110010111... también de periodo 7.*

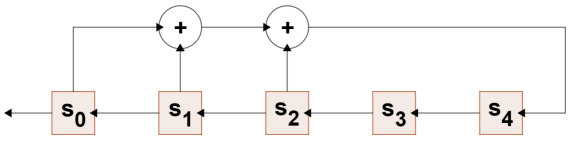


Figura 3.2: LFSR del ejemplo 3.7.

3.1. Descripción algebraica

Las SLRs se pueden definir también por su forma matricial, ya que a cada ecuación de recurrencia lineal $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n$ se le puede asociar una matriz de tamaño $k \times k$

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & ... & 0 \\ 0 & 0 & 1 & 0 & ... & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & ... & 1 \\ a_0 & a_1 & a_2 & a_3 & ... & a_{k-1} \end{pmatrix} \tag{3.5}$$

tal que se tiene

$$\begin{pmatrix} s_{n+1} \\ s_{n+2} \\ . \\ . \\ s_{n+k} \end{pmatrix} = A \begin{pmatrix} s_n \\ s_{n+1} \\ . \\ . \\ s_{n+k-1} \end{pmatrix}$$

Proposición 3.8. *Sea A la matriz asociada a una SLR, se cumple que* $S_n = A^n S_0$.

Demostración: De la definición de la matriz es inmediato comprobar que $S_n = AS_{n-1} = A^2 S_{n-2} = ... = A^n S_0$. □

Ejemplo 3.9. *Continuando con el ejemplo 3.7, la matriz asociada a esa SLR sería*

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

Se puede obtener s_{14} *gracias a la propiedad dada. Sabemos que* $S_9 = (s_9, s_{10}, s_{11}, s_{12}, s_{13})^T = (0, 1, 0, 0, 0)^T$, *luego* $AS_9 = S_{10} = (s_{10}, s_{11}, s_{12}, s_{13}, s_{14})^T = (1, 0, 0, 0, 1)^T$ *y* $s_{14} = 1$.

Proposición 3.10. *El polinomio característico asociado a la SLR coincide con el polinomio característico de la matriz A.*

Demostración: A partir de la matriz asociada a la SLR, definamos las matrices A_i de tamaño $k - i \times k - i$ para $0 \leq i \leq k - 1$ de la siguiente forma

$$A_0 = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & ... & 1 \\ a_0 & a_1 & a_2 & ... & a_{k-1} \end{pmatrix} \quad ... \quad A_i = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & ... & 1 \\ a_i & a_{i+1} & a_{i+2} & ... & a_{k-1} \end{pmatrix} \quad ... \quad A_{k-1} = a_{k-1}$$

Para calcular $|xId - A| = |xId - A_0|$, podemos obtener una fórmula recurrente calculando el polinomio característico de A_i, con $0 \leq i < k-1$, desarrollando por la primera columna.

$$P_i = |xId - A_i| = \begin{vmatrix} x & -1 & 0 & ... & 0 & 0 \\ 0 & x & -1 & ... & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & ... & x & -1 \\ -a_i & -a_{i+1} & -a_{i+2} & ... & -a_{k-2} & x - a_{k-1} \end{vmatrix} =$$

$$= x \begin{vmatrix} x & -1 & 0 & ... & 0 \\ 0 & x & -1 & ... & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & ... & -1 \\ -a_{i+1} & -a_{i+2} & -a_{i+3} & ... & x - a_{k-1} \end{vmatrix} + (-1)^{k-i+1}(-a_i) \begin{vmatrix} -1 & 0 & ... & 0 & 0 \\ x & -1 & ... & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & ... & x & -1 \end{vmatrix} =$$

$$= xP_{i+1} + (-1)^{k-i+1}(-a_i)(-1)^{k-i-1} = xP_{i+1} - a_i$$

Por tanto, tenemos la recurrencia $P_i = xP_{i+1} - a_i$ para $0 \leq i < k-1$. Por otro lado, se tiene $P_{k-1} = |x - a_{k-1}| = x - a_{k-1}$, luego calculamos el polinomio caracteístico de la matriz $|xId - A_0| = P_0 = xP_1 - a_0 = x(xP_2 - a_1) - a_0 = x^2P_2 - a_1x - a_0 = ... = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_0$, que coincide con el polinomio de retroalimentación. □

Proposición 3.11. *El polinomio característico asociado a la SLR coincide con el polinomio mínimo de la matriz A.*

Demostración: El polinomio característico asociado a la SLR es mónico por definición, $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_0$. Además, como $AS_n = S_{n+1}$ para todo $n \geq 0$, se tiene $f(A)S_0 = A^kS_0 - a_{k-1}A^{k-1}S_0 - ... - a_1AS_0 - a_0S_0 = S_k - a_{k-1}S_{k-1} - ... - a_1S_1 - a_0S_0$ y $f(x)$ genera s, entonces $f(A)S_0 = S_k - S_k = 0$. Al ser S_0 un vector arbitrario se tiene que $f(A) = 0$.
Falta ver que es el polinomio mónico de menor grado que anula a A. Si partimos del estado inicial $S_0 = (0, 0, ..., 0, 1)^T$, se tiene que los k primeros términos de la sucesión vectorial son de la forma

$$S_0 = (0, ..., 0, 1)^T \ ... \quad S_i = (0, ..., 0, 1, s_k, ..., s_{k+i-1})^T \ ... \quad S_{k-1} = (1, s_k, s_{k+1}, ..., s_{2k-1})^T$$

que claramente son linealmente independientes. Sea $g(x) = x^r + b_{r-1}x^{r-1} + ... + b_1x + b_0 \in \mathbb{F}_q[x]$ un polinomio mónico de grado $r < k$. Si $g(A) = 0$, entonces $g(A)S_0 = 0$, luego

$$0 = g(A)S_0 = S_r + b_{r-1}S_{r-1} + ... + b_1S_1 + b_0S_0$$

contradiciendo que los S_i con $0 \leq i \leq k-1$ sean linealmente independientes, pues $r \leq k-1$. □

Proposición 3.12. *La matriz asociada a la SLR es invertible, es decir, $A \in GL_k(\mathbb{F}_q)$.*

Demostración: Sea A la matriz asociada a una SLR de orden k, entonces $a_0 \neq 0$, y como $| A | = (-1)^{k-1}a_0$, se tiene el resultado. □

A partir de la matriz asociada a una SLR es fácil obtener la siguiente propiedad relativa al periodo de la sucesión.

Proposición 3.13. *Dada una SLR de orden k, el periodo de la sucesión divide al orden de su matriz asociada A en $GL_k(\mathbb{F}_q)$.*

Demostración: Sea m el orden de la matriz A asociada a la SLR. Se tiene que para todo $n \geq 0$, $S_{n+m} = A^{n+m}S_0 = A^nA^mS_0 = A^nIS_0 = A^nS_0 = S_n$. Por tanto, como la sucesión se repite tras m términos, el periodo de la SLR divide a m. □

Corolario 3.14. *El periodo de una SLR sobre $\mathbb{F}_q$ de orden k divide a $(q^k-1)(q^k-q)(q^k-q^2)...(q^k-q^{k-1})$.*

Demostración: Es inmediato a partir del resultado anterior, pues el grupo $GL_k(\mathbb{F}_q)$ tiene orden $\prod_{i=0}^{k-1}(q^k-q^i)$ y el orden de una matriz divide al orden del grupo. □

3.2. Sucesión impulso respuesta

Un LFSR puede generar distintas sucesiones si tomamos estados iniciales diferentes. A su vez, estas sucesiones pueden tener periodos distintos entre sí. Como buscamos sucesiones pseudoaleatorias, es claro que nos interesa que el periodo sea lo más grande posible, por ello vamos a estudiar algunas propiedades de las sucesiones de recurrencia lineal relacionadas con su periodo.

Ejemplo 3.15. *Sea $f(x) = x^5 + x^3 + x^2 + 1$ el polinomio del LFSR sobre $\mathbb{F}_2$, por el Lema 3.4 el periodo es menor que 31, por la Proposición 3.13 divide a 12 (el orden de la matriz asociada A), y por el Corolario 3.14 divide al orden del grupo $GL_5(\mathbb{F}_2)$, que es 9999360. Si tomamos como estado inicial $S_0 = (1,0,0,1,0)^T$, se genera la sucesión 100100100... de periodo 3. En cambio, si partimos del mismo LFSR pero en su lugar tomamos el estado inicial $S_0 = (0,0,1,1,0)^T$, la sucesión generada es 001100110011... de periodo 4, y si tomamos $S_0 = (0,0,0,1,1)^T$ se genera la sucesión 000111000111... de periodo 6.*

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

Definición 3.16. *Se denomina periodo máximo de un LFSR al máximo de los periodos de las sucesiones que genera.*

De entre todos los valores iniciales que podemos tomar de un LFSR dado, existe uno especial que determina los periodos de este LFSR para cualesquiera valores iniciales, como veremos a continuación.

Definición 3.17. *Dado un LFSR, tomando el estado inicial $S_0 = (0,0,...,0,1)^T$, a la sucesión obtenida se la conoce como sucesión impulso respuesta.*

Esta sucesión es muy importante en nuestro estudio, ya que tiene unas propiedades específicas que, por lo general, no cumplen el resto de SLRs.

Lema 3.18. *Dado un LFSR, sea s la sucesión impulso respuesta, se tiene que si $S_m = S_n$ entonces $A^m = A^n$.*

Demostración: Si $S_m = S_n$ entonces, es claro que, $S_{m+t} = S_{n+t}$ para todo $t \geq 0$. Además, $A^m S_t = S_{m+t} = S_{n+t} = A^n S_t$ para todo $t \geq 0$. En particular para $t = 0$, $A^m S_0 = A^n S_0$. Tomando $S_0 = (0, 0, ..., 0, 1)^T$ como estado inicial, tal como se mencionó en la demostración de la Proposición 3.11, los k primeros términos S_i de la sucesión vectorial son linealmente independientes, luego se tiene que si $A^m S_t = A^n S_t$ para todo $t \geq 0$ entones $A^m = A^n$. □

En particular, lo interesante de esta sucesión es que su periodo es el periodo máximo del LFSR que la genera.

Teorema 3.19. *El periodo de la sucesión impulso respuesta es el periodo máximo del LFSR que la genera y coincide con el orden de la matriz asociada.*

Demostración: Sean r el periodo de la sucesión impulso respuesta y m el orden de la matriz A asociada. Entonces, como r es el periodo, $S_r = S_0$, y por el Lema 3.18 se tiene que $A^r = A^0 = I$. Por lo tanto, se tiene que el orden de la matriz divide a r, ie. $m \mid r$. Por la Proposición 3.13 teníamos que $r \mid m$, luego el periodo de la sucesión impulso respuesta es $r = m$, que es el máximo posible. □

De los resultados anteriores, Proposición 3.13 y Teorema 3.19, se tiene el siguiente corolario.

Corolario 3.20. *Dado un LFSR, el periodo de cualquier SLR generada por él divide al periodo de la sucesión impulso respuesta.*

Ejemplo 3.21. *En el ejemplo 3.15 ya obtuvimos tres sucesiones de periodos 3, 4 y 6 de un mismo LFSR dado. Comprobemos ahora que es cierto que dividen al periodo máximo. La sucesión impulso respuesta del LFSR, estado inicial $S_0 = (0, 0, 0, 0, 1)^T$, es 000010111101000010 111101... con periodo 12, efectivamente múltiplo de 3, 4 y 6. A su vez, el orden de la matriz asociada dada en el ejemplo 3.15, 12, coincide con el periodo máximo.*
En la Tabla 3.1 se puede observar el periodo de cada sucesión obtenida partiendo de cada uno de los q^k estados iniciales posibles.

Estados iniciales	Periodo
(0,0,0,0,0), (1,1,1,1,1)	1
(0,1,0,1,0), (1,0,1,0,1)	2
(0,0,1,0,0), (0,1,0,0,1), (0,1,1,0,1), (1,0,0,1,0), (1,0,1,1,0), (1,1,0,1,1)	3
(0,0,1,1,0), (0,1,1,0,0), (1,0,0,1,1), (1,1,0,0,1)	4
(0,0,0,1,1), (0,0,1,1,1), (0,1,1,1,0), (1,0,0,0,1), (1,1,0,0,0), (1,1,1,0,0)	6
(0,0,0,0,1), (0,0,0,1,0), (0,0,1,0,1), (0,1,0,0,0), (0,1,0,1,1), (0,1,1,1,1), (1,0,0,0,0), (1,0,1,0,0), (1,0,1,1,1), (1,1,0,1,0), (1,1,1,0,1), (1,1,1,1,0)	12

Tabla 3.1: Periodos dependiendo del estado inicial tomado.

Capítulo 4

Irreducibilidad y orden del polinomio característico

En este capítulo veremos que el comportamiento del periodo de las SLRs va a depender de la irreducibilidad del polinomio de retroalimentación. Además, el orden del polinomio característico juega un papel importante, ya que el periodo viene dado en función de este. También se verá que si el polinomio de retroalimentación es primitivo, todas las sucesiones tendrán periodo igual que el máximo, un resultado esencial para el siguiente capítulo. Se toman como referencia [9], [10], [12] y [13].

Ejemplo 4.1. *Sea $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ el polinomio característico asociado a una SLR. Este polinomio es irreducible y no primitivo, ya que su orden es 5, pues $f(x)$ divide a $x^5 - 1$ y no divide a $x^4 - 1$, y $5 \neq 2^4 - 1 = 15$. Como se puede ver en la Tabla 4.1, el periodo de toda SLR no nula generada por $f(x)$ es exactamente 5.*

Estados iniciales	SLR	Periodo		Estados iniciales	SLR	Periodo
(0,0,0,0)	00000...	1		(1,0,0,0)	1000110001...	5
(0,0,0,1)	0001100011...	5		(1,0,0,1)	1001010010...	5
(0,0,1,0)	0010100101...	5		(1,0,1,0)	1010010100...	5
(0,0,1,1)	0011000110...	5		(1,0,1,1)	1011110111...	5
(0,1,0,0)	0100101001...	5		(1,1,0,0)	1100011000...	5
(0,1,0,1)	0101001010...	5		(1,1,0,1)	1101111011...	5
(0,1,1,0)	0110001100...	5		(1,1,1,0)	1110111101...	5
(0,1,1,1)	0111101111...	5		(1,1,1,1)	1111011110...	5

Tabla 4.1: SLRs dependiendo del estado inicial tomado.

Si en cambio, el polinomio de retroalimentación es $f(x) = x^4 + x + 1$, sigue siendo un polinomio irreducible pero en este caso es primitivo y todas las SLRs de orden 4 (excepto la constante igual a cero) tienen periodo 15, igual al orden del polinomio.

Para ver cómo afectan al periodo la irreducibilidad y si el polinomio es primitivo, hace falta entender antes unos resultados relacionados con el orden del polinomio asociado a la SLR.

Proposición 4.2. *Sea $f(x) \neq 0 \in \mathbb{F}_q[x]$ el polinomio de retroalimentación y A la matriz asociada, se tiene que $f(x)$ divide a $x^e - 1$ si y solo si $A^e = Id$.*

Demostración: Al ser $f(x)$ el polinomio mínimo de A tenemos que $f(A) = 0$. Como $x^e - 1 = f(x)g(x)$ para algún $g(x) \in \mathbb{F}_q[x]$, se tiene que $A^e - Id = f(A)g(A) = 0$, es decir, $A^e = Id$. Si en cambio suponemos que $A^e = Id$, podemos definir el polinomio $g(x) = x^e - 1$ y se tiene que anula a A. Al ser $f(x)$ el polinomio mónico de menor grado que anula a A se tiene que $f(x)$ divide a $g(x)$. □

Corolario 4.3. *El orden del polinomio de retroalimentación coincide con el orden de la matriz asociada. Además, el periodo de toda SLR divide al orden del polinomio característico y el periodo de la sucesión impulso respuesta coincide con el orden del polinomio.*

La siguiente propiedad del polinomio de retroalimentación nos servirá para poder demostrar que, cuando es irreducible, el orden del polinomio coincide con el periodo de la SLR asociada.

Teorema 4.4. *Dada la SLR de orden k y periodo r que cumple la ley de recurrencia $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n$, y sea $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_1 x - a_0 \in \mathbb{F}_q[x]$ su polinomio característico. Entonces, el polinomio cumple*

$$f(x)s(x) = (1 - x^r)h(x) \tag{4.1}$$

donde

$$s(x) = s_0 x^{r-1} + s_1 x^{r-2} + s_2 x^{r-3} + ... + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x] \tag{4.2}$$

y

$$h(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} s_i x^j \in \mathbb{F}_q[x], \qquad con \;\; a_k = -1 \tag{4.3}$$

Demostración: Comprobamos que los coeficientes a ambos lados de la igualdad (4.1) coinciden. Para $0 \leq t \leq k + r - 1$, sea c_t el coeficiente que acompaña a x^t en el lado izquierdo de la igualdad y sea d_t el coeficiente que acompaña a x^t en el lado derecho. Como los polinomios $f(x)$ y $s(x)$ se pueden reescribir como $f(x) = -\sum_{i=0}^{k} a_i x^i$ y $s(x) = \sum_{j=0}^{r-1} s_{r-1-j}x^j$, se tiene que

$$c_t = - \sum_{\substack{0 \leq i \leq k, 0 \leq j \leq r-1 \\ i+j=t}} a_i s_{r-1-j}, \qquad \text{para } \; 0 \leq t \leq k + r - 1 \tag{4.4}$$

Además, la ley de recurrencia se puede escribir como

$$\sum_{i=0}^{k} a_i s_{n+i} = 0, \qquad \text{para todo } \; n \geq 0 \tag{4.5}$$

Distinguimos cuatro casos. Si $k \leq t \leq r - 1$, entonces por (4.4) y (4.5) se tiene

$$c_t = - \sum_{i=0}^{k} a_i s_{r-1-t+i} = 0 = d_t$$

Si $t \leq r-1$ y $t < k$, entonces por (4.4), (4.5) y la periodicidad de la SLR se tiene

$$c_t = -\sum_{i=0}^{t} a_i s_{r-1-t+i} = \sum_{i=t+1}^{k} a_i s_{r-1-t+i} = \sum_{i=t+1}^{k} a_i s_{i-t-1} = \sum_{i=0}^{k-1-t} a_{i+t+1} s_i = d_t$$

Si $t \geq r$ y $t \geq k$, entonces por (4.4) se tiene

$$c_t = -\sum_{i=t-r+1}^{k} a_i s_{r-1-t+i} = -\sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i = d_t$$

Si $r \leq t < k$, entonces por (4.4) y la periodicidad de la SLR se tiene

$$c_t = -\sum_{i=t-r+1}^{t} a_i s_{r-1-t+i} = -\sum_{i=0}^{r-1} a_{i+t-r+1} s_i = \sum_{i=r}^{k-1-t+r} a_{i+t-r+1} s_i - \sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i =$$

$$= \sum_{i=0}^{k-1-t} a_{i+t+1} s_{i+r} - \sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i = \sum_{i=0}^{k-1-t} a_{i+t+1} s_i - \sum_{i=0}^{k-1-t+r} a_{i+t-r+1} s_i = d_t. \quad \square$$

Teorema 4.5. *Si el polinomio de retroalimentación $f(x)$ es irreducible, entonces el periodo de la SLR asociada coincide con el orden del polinomio asociado.*

Demostración: Sea r el periodo de la SLR. Por el Teorema 4.4 $f(x)$ divide a $(x^r-1)h(x)$. Como $s(x)$ y $h(x)$ no son polinomios nulos, y $deg(h) = k-1 < k = deg(f)$, al ser $f(x)$ irreducible se tiene que $f(x)$ divide a $x^r - 1$, y por tanto $r \geq ord(f)$. Por el Corolario 4.3 tenemos que r divide a $ord(f)$, luego $r = ord(f)$. $\square$

Gracias a este resultado se tiene que, cuando un polinomio es irreducible, toda sucesión generada, excepto la idénticamente nula, tiene el mismo periodo. Además, como el periodo coincide con el orden del polinomio de retroalimentación, cuando el polinomio es primitivo tenemos que el periodo de la SLR de orden k en $\mathbb{F}_q$ es $q^k - 1$, es decir, el máximo posible. En el siguiente capítulo nos centraremos en el estudio de las SLRs con polinomio asociado primitivo.

Los términos de una sucesión de recurrencia lineal se pueden determinar a partir de las raíces del polinomio de retroalimentación, como se indica a continuación.

Teorema 4.6. *Sea s una SLR sobre $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^k}$ una raíz del polinomio de retroalimentación. Si el polinomio es irreducible, entonces existe un único elemento $\beta \in \mathbb{F}_{q^k}$ tal que $s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i)$.*

Demostración: Como $\{1, \alpha, \alpha^2, ..., \alpha^{k-1}\}$ es base de $\mathbb{F}_{q^k}$ sobre $\mathbb{F}_q$, se puede definir una aplicación $\theta : \mathbb{F}_{q^k} \to \mathbb{F}_q$ tal que $\theta(\alpha^i) = s_i$ para $i = 0, 1, ..., k-1$. Por el Teorema 2.41, existe un único $\beta \in \mathbb{F}_{q^k}$ tal que $\theta(\gamma) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\gamma)$ para todo $\gamma \in \mathbb{F}_{q^k}$. En particular, se tiene que $s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i)$ para $i = 0, 1, ..., k-1$. Falta ver que $Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i)$, con $i = 0, 1, ...$, forma una SLR con polinomio característico $f(x)$. Sea $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} -$

$... - a_1x - a_0 \in \mathbb{F}_q[x]$, entonces tenemos la ley de recurrencia $s_{i+k} = a_{k-1}s_{i+k-1} + ... + a_0s_i$, y por la Proposición 2.40 se tiene

$$s_{i+k} - a_{k-1}s_{i+k-1} - ... - a_0s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+k}) - a_{k-1}Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+k-1}) - ... - a_0Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i) =$$

$$= Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+k} - a_{k-1}\beta\alpha^{i+k-1} - ... - a_0\beta\alpha^i) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i f(\alpha)) = 0$$

para todo $i \geq 0$. □

Si en cambio, el polinomio característico no es irreducible, se distinguen dos casos, cuando el polinomio característico es reducible sin raíces múltiples y cuando es reducible con raíces múltiples. Para poder dar la expresión de s en cada caso, es necesario reescribir la función generatriz asociada, definiendo antes el siguiente polinomio.

Definición 4.7. *Dado el polinomio* $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a_1x - a_0 \in \mathbb{F}_q[x]$, *al polinomio* $f^*(x) := -a_0x^k - a_1x^{k-1} - a_2x^{k-2}... - a_{k-1}x + 1 \in \mathbb{F}_q[x]$ *se le denomina polinomio recíproco de* $f(x)$.

Nótese que el polinomio recíproco de $f(x)$ se puede definir a partir del polinomio de retroalimentación como $f^*(x) = x^k f(\frac{1}{x})$. Además, si $\alpha \neq 0$ es una raíz de $f(x)$, se tiene que $1/\alpha$ es raíz de $f^*(x)$.

El polinomio recíproco de $f(x)$ se puede relacionar con la función generatriz como se hace a continuación. Dada la SLR s de orden k, sea $G(x) = \sum_{i=0}^{\infty} s_ix^i$ la función generatriz asociada a la sucesión, se puede multiplicar $G(x)$ por $-a_ix^{k-i}$ obteniendo:

$$G(x) = s_0 + s_1x + s_2x^2 + ... + s_{k-1}x^{k-1} + s_kx^k + s_{k+1}x^{k+1} + s_{k+2}x^{k+2} + ...$$

$$-a_{k-1}xG(x) = -a_{k-1}s_0x - a_{k-1}s_1x^2 - a_{k-1}s_2x^3 - ... - a_{k-1}s_{k-1}x^k - a_{k-1}s_kx^{k+1} - a_{k-1}s_{k+1}x^{k+2} - ...$$

$$-a_{k-2}x^2G(x) = \qquad -a_{k-2}s_0x^2 - a_{k-2}s_1x^3 - ... - a_{k-2}s_{k-2}x^k - a_{k-2}s_{k-1}x^{k+1} - a_{k-2}s_kx^{k+2} - ...$$

. . . . .

$$-a_1x^{k-1}G(x) = \qquad\qquad -a_1s_0x^{k-1} - a_1s_1x^k - a_1s_2x^{k+1} - a_1s_3x^{k+2} - ...$$

$$-a_0x^kG(x) = \qquad\qquad -a_0s_0x^k - a_0s_1x^{k+1} - a_0s_2x^{k+2} - ...$$

Si sumamos estas igualdades nos queda $(1 - a_{k-1}x - a_{k-2}x^2 - ... - a_1x^{k-1} - a_0x^k)G(x)$ a la izquierda de la igualdad, y a la derecha, como s satisface la ley de recurrencia lineal $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0s_n$, nos queda un polinomio de grado menor o igual que $k-1$. Este polinomio se puede definir como $g(x) \in \mathbb{F}_q[x]$ teniendo lo siguiente:

$$g(x) = G(x)(1 - \sum_{j=0}^{k-1} a_jx^{k-j}) = -\sum_{j=0}^{k-1}\sum_{i=0}^{j} a_{i+k-j}s_ix^j \tag{4.6}$$

Nótese que el polinomio $1 - \sum_{j=0}^{k-1} a_jx^{k-j} \in \mathbb{F}_q[x]$ es el polinomio recíproco de $f(x)$, y por tanto, la función generatriz puede escribirse como $G(x) = \dfrac{g(x)}{f^*(x)}$.

Teorema 4.8. *Sea s una SLR de orden k, sea $f(x) \neq 0 \in \mathbb{F}_q[x]$ el polinomio de retroalimentación y $\alpha_1, \alpha_2, ..., \alpha_k$ las raíces de $f(x)$. Si $f(x)$ no tiene raíces múltiples, entonces existen $b_j \in \mathbb{F}_q$ tales que*

$$s_i = \sum_{j=1}^{k} b_j \alpha_j^i$$

donde el valor de los b_j queda determinado por el estado inicial de la SLR.

Demostración: Como $\alpha_1, \alpha_2, ..., \alpha_k$ son las raíces de $f(x)$, $f(x) = \prod_{j=1}^{k}(x-\alpha_j)$, entonces el polinomio recíproco se puede escribir como $f^*(x) = x^k f(\frac{1}{x}) = \prod_{j=1}^{k}(1-\alpha_j x)$ y por tanto, $G(x) = \dfrac{g(x)}{f^*(x)} = \displaystyle\sum_{j=1}^{k} \frac{b_j}{1-\alpha_j x}$. Obtenida esta descomposición en fracciones simples y usando la serie geométrica $\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$, tenemos que la función generatriz puede escribirse como

$$G(x) = \sum_{j=1}^{k} \frac{b_j}{1-\alpha_j x} = \sum_{j=1}^{k} b_j \sum_{i=0}^{\infty} (\alpha_j x)^i = \sum_{i=0}^{\infty} (\sum_{j=1}^{k} b_j \alpha_j^i) x^i$$

de donde, por la Definición 2.3, se tiene $s_i = \sum_{j=1}^{k} b_j \alpha_j^i$. □

El siguiente teorema es la generalización de esta expresión para sucesiones con polinomio asociado reducible con raíces múltiples.

Teorema 4.9. *Sea s una SLR de orden k, sea $f(x) \neq 0 \in \mathbb{F}_q[x]$ el polinomio de retroalimentación y $\alpha_1, \alpha_2, ..., \alpha_s$ las raíces de $f(x)$. Si $f(x)$ tiene raíces múltiples, es decir, $f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}...(x-\alpha_s)^{k_s}$, entonces existen $b_{j,h} \in \mathbb{F}_q$, con $1 \leq j \leq s$ y $1 \leq h \leq k_j$, tales que*

$$s_i = \sum_{j=1}^{s} \left(\sum_{h=1}^{k_j} b_{j,h} \binom{i+h-1}{i} \right) \alpha_j^i$$

donde el valor de los $b_{j,h}$ queda determinado por el estado inicial de la SLR.

Demostración: Como $f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}...(x-\alpha_s)^{k_s}$, el polinomio recíproco de $f(x)$ es $f^*(x) = (1-\alpha_1 x)^{k_1}(1-\alpha_2 x)^{k_2}...(1-\alpha_s x)^{k_s}$, y por tanto, la función generatriz asociada a la SLR se puede escribir como

$$G(x) = \frac{g(x)}{f^*(x)} = \sum_{j=1}^{s} \left(\frac{b_{j,1}}{1-\alpha_j x} + \frac{b_{j,2}}{(1-\alpha_j x)^2} + ... + \frac{b_{j,k_j}}{(1-\alpha_j x)^{k_j}} \right) = \sum_{j=1}^{s} \left(\sum_{h=1}^{k_j} \frac{b_{j,h}}{(1-\alpha_j x)^h} \right)$$

Por la serie de Maclaurin sabemos que

$$\frac{1}{(1-x)^m} = 1 + mx + \frac{m(m+1)}{2}x^2 + \frac{m(m+1)(m+2)}{3!}x^3 + ...$$

Por tanto, por los números binomiales se tiene que

$$\frac{1}{(1-x)^m} = \sum_{i=0}^{\infty} \frac{(i+m-1)!}{i!(m-1)!} x^i = \sum_{i=0}^{\infty} \binom{i+m-1}{i} x^i$$

Utilizando esto, se obtiene entonces

$$G(x) = \sum_{j=1}^{s} \sum_{h=1}^{k_j} b_{j,h} \sum_{i=0}^{\infty} \binom{i+h-1}{i} (\alpha_j x)^i = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{s} \sum_{h=1}^{k_j} b_{j,h} \binom{i+h-1}{i} \alpha_j^i \right) x^i$$

de lo que, por la definición de función generatriz, se tiene que

$$s_i = \sum_{j=1}^{s} \sum_{h=1}^{k_j} b_{j,h} \binom{i+h-1}{i} \alpha_j^i$$

□

Para conocer el comportamiento del periodo de una SLR cuando el polinomio de retroalimentación no es irreducible, primero se necesita trabajar con el polinomio mínimo de la sucesión y las familias de SLRs.

4.1. Polinomio mínimo

Hasta ahora hemos partido siempre de un LFSR para obtener una sucesión de recurrencia lineal, ya sea mediante el polinomio característico, la ley de recurrencia o incluso la matriz asociada. Si en cambio, comenzamos teniendo una sucesión de recurrencia lineal, esta satisface varias leyes de recurrencia distintas, luego tiene asociados más de un polinomio característico. Es más, como un polinomio reducible se puede factorizar como producto de varios polinomios, es claro que si uno de los factores satisface una recurrencia de la SLR, ese factor es también polinomio característico de la sucesión. Es decir, por cada SLR se pueden obtener infinitos polinomios de retroalimentación multiplicando uno ya obtenido por otro factor.

Ejemplo 4.10. *Sea $s = 01110010111001...$ una SLR, satisface las leyes de recurrencia $s_{n+3} = s_{n+1} + s_n$, $s_{n+4} = s_{n+3} + s_{n+2} + s_n$ y $s_{n+5} = s_{n+2} + s_{n+1} + s_n$, es decir, tiene asociados los polinomios $f(x) = x^3+x+1$, $g(x) = x^4+x^3+x^2+1$ y $h(x) = x^5+x^2+x+1$. El polinomio $f(x)$ es irreducible y los polinomios $g(x)$ y $h(x)$ se pueden escribir como $g(x) = (x+1)f(x)$ y $h(x) = (x^2+1)f(x)$.*

Teorema 4.11. *Sea s una SLR en $\mathbb{F}_q$ y sea $f(x) \in \mathbb{F}_q[x]$ un polinomio mónico de grado positivo. Entonces, existe un único polinomio mónico $m(x) \in \mathbb{F}_q[x]$ que cumpla que $f(x)$ es polinomio característico de s si y solo si $m(x)$ divide a $f(x)$.*

Demostración: Sea $f_0(x) \in \mathbb{F}_q[x]$ el polinomio de grado k_0 asociado a una recurrencia que cumpla la sucesión s y sea $h_0(x) \in \mathbb{F}_q[x]$ el polinomio de la ecuación (4.3) determinado por $f_0(x)$. Si $d(x) \in \mathbb{F}_q[x]$ es el máximo común divisor de $f_0(x)$ y $h_0(x)$, entonces podemos escribir $f_0(x) = m(x)d(x)$ y $h_0(x) = b(x)d(x)$, con $m(x), b(x) \in \mathbb{F}_q[x]$. Queremos ver que $m(x)$ es el polinomio deseado. Es claro que $m(x)$ es mónico.

Supongamos que $f(x) \in \mathbb{F}_q[x]$ es un polinomio característico de s de grado k. Sean $s(x) \in \mathbb{F}_q[x]$ el polinomio de la ecuación (4.2) y $h(x) \in \mathbb{F}_q[x]$ el polinomio de la ecuación (4.3) determinados por $f(x)$. Por un lado, como s es periódica de periodo r, utilizando la

serie geométrica $\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$ tenemos que la función generatriz de s se puede escribir como

$$G(x) = \sum_{i=0}^{\infty} s_i x^i = (s_0 + s_1 x + s_2 x^2 + ... + s_{r-1} x^{r-1})(1 + x^r + x^{2r} + ...) = \frac{s^*(x)}{1 - x^r}$$

donde $s^*(x) = s_0 + s_1 x + s_2 x^2 + ... + s_{r-1} x^{r-1}$ es el polinomio recíproco de $s(x)$. Como $G(x) = \frac{g(x)}{f^*(x)}$, con $g(x)$ determinado por (4.6), se tiene entonces que $f^*(x)s^*(x) = (1 - x^r)g(x)$. De esto, obtenemos

$$f(x)s(x) = x^k f^*\left(\frac{1}{x}\right) x^{r-1} s^*\left(\frac{1}{x}\right) = x^{k+r-1}\left(1 - \frac{1}{x^r}\right) g\left(\frac{1}{x}\right) = (x^r - 1)x^{k-1} g\left(\frac{1}{x}\right)$$

luego por (4.1) se llega a

$$x^{k-1} g\left(\frac{1}{x}\right) = -h(x) \tag{4.7}$$

Por otro lado, hemos visto que la función generatriz de s se puede escribir como

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{g(x)}{f^*(x)}$$

con $g_0(x)$ determinado por (4.6). Por lo tanto, se tiene $g(x)f_0^*(x) = g_0(x)f^*(x)$, y usando (4.7) se obtiene que

$$h(x)f_0(x) = -x^{k-1} g\left(\frac{1}{x}\right) x^{k_0} f_0^*\left(\frac{1}{x}\right) = -x^{k_0 - 1} g_0\left(\frac{1}{x}\right) x^k f^*\left(\frac{1}{x}\right) = h_0(x)f(x)$$

Dividiendo entre $d(x)$ se llega a $h(x)m(x) = b(x)f(x)$, y como $m(x)$ y $b(x)$ son primos entre sí, se tiene que $m(x)$ divide a $f(x)$.

Suponemos ahora que $f(x) \in \mathbb{F}_q[x]$ es un polinomio mónico de grado positivo y que $f(x) = m(x)c(x)$, con $c(x) \in \mathbb{F}_q[x]$. Si pasamos a los polinomios recíprocos se tiene $f^*(x) = m^*(x)c^*(x)$. Además, tenemos que $h_0(x)m(x) = b(x)f_0(x)$, y usando (4.7) se obtiene

$$g_0(x)m^*(x) = -x^{k_0 - 1} h_0\left(\frac{1}{x}\right) x^{deg(m(x))} m\left(\frac{1}{x}\right) = -x^{deg(m(x))-1} b\left(\frac{1}{x}\right) x^{k_0} f_0\left(\frac{1}{x}\right)$$

Como $deg(h_0(x)) = k_0 - 1 < k_0 = deg(f_0(x))$, tenemos $deg(b(x)) < deg(m(x))$, luego $-x^{deg(m(x))-1} b\left(\frac{1}{x}\right)$ es un polinomio $a(x) \in \mathbb{F}_q[x]$. Se tiene entonces $g_0(x)m^*(x) = a(x)f_0^*(x)$, y por tanto

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{a(x)}{m^*(x)} = \frac{a(x)c^*(x)}{m^*(x)c^*(x)} = \frac{a(x)c^*(x)}{f^*(x)}$$

Como $deg(a(x)c^*(x)) = deg(a(x)) + deg(c^*(x)) < deg(m(x)) + deg(c(x)) = deg(f(x))$, tenemos que $f(x)$ es polinomio de retroalimentación de s. Es claro que solo puede existir un polinomio $m(x)$ con las propiedades indicadas. □

El polinomio $m(x) \in \mathbb{F}_q[x]$ definido en el Teorema 4.11 se llama polinomio mínimo de la sucesión. Si se tiene la sucesión nula, entonces es claro, por el teorema anterior, que el

polinomio mínimo asociado es $m(x) = 1$, ya que todos los polinomios generan la sucesión nula tomando el estado inicial nulo.

Al ser $m(x)$ polinomio característico, se tiene que el orden de $m(x)$ coincide con el orden de la matriz asociada, el periodo de toda SLR divide al orden de $m(x)$ y el periodo de la sucesión impulso respuesta coincide con el orden de $m(x)$. En el Teorema 4.5 ya vimos que cuando un polinomio característico de la SLR es irreducible, el orden del polinomio coincide con el periodo de la sucesión. Este resultado se tiene también para el polinomio mínimo, como se muestra a continuación.

Teorema 4.12. *Sea s una SLR en $\mathbb{F}_q$ con polinomio mínimo $m(x) \in \mathbb{F}_q[x]$, entonces el periodo de s coincide con el orden de $m(x)$.*

Demostración: Sea r el periodo de la sucesión s, es claro que s satisface la recurrencia $s_{n+r} = s_n$ para todo $n \geq 0$. Por el Teorema 4.11, $m(x)$ divide a $x^r - 1$, y de la definición de orden de un polinomio se tiene que $ord(m) \leq r$. Por el Corolario 4.3, r divide a $ord(m)$, luego el periodo de s coincide con el orden del polinomio mínimo. □

Ejemplo 4.13. *En el Ejemplo 4.10 se dieron tres polinomios característicos de s, $f(x)$, $g(x)$ y $h(x)$, y se vio que $f(x)$ es irreducible, $g(x) = (x+1)f(x)$ y $h(x) = (x^2+1)f(x)$. Además, se tiene que $f(x)$ es el polinomio mínimo de s, como muestra el siguiente teorema.*

Teorema 4.14. *Sea $f(x)$ un polinomio mónico e irreducible sobre $\mathbb{F}_q$ y sea s una SLR en $\mathbb{F}_q$. Si $f(x)$ es polinomio de retroalimentación de s, entonces $f(x)$ es además el polinomio mínimo de s.*

Demostración: Como por el Teorema 4.11, el polinomio mínimo $m(x)$ de s divide a $f(x)$, la irreducibilidad de $f(x)$ implica que o bien $m(x) = 1$ o bien $m(x) = f(x)$. Pero como no consideramos las SLRs nulas en este trabajo, $m(x) \neq 1$ ya que sino se tendría $s \equiv 0$. □

Aparte de la irreducibilidad, existen otros criterios para saber si un polinomio característico es además el polinomio mínimo.

Ejemplo 4.15. *Sea $s = 01100110...$ una sucesión de recurrencia lineal sobre $\mathbb{F}_2$. Su polinomio mínimo es $f(x) = x^3 + x^2 + x + 1 = (x+1)^3 \in \mathbb{F}_2[x]$, ya que es el polinomio característico de s que divide al resto de los polinomios asociados a la sucesión y ningún otro divide $f(x)$, pues $(x+1)$ no es polinomio característico de s. Además, las sucesiones vectoriales $S_0 = (0,1,1)$, $S_1 = (1,1,0)$ y $S_2 = (1,0,0)$ son linealmente independientes, que como se muestra a continuación, es una condición necesaria y suficiente para determinar si un polinomio característico es el polinomio mínimo.*

Teorema 4.16. *Sea s una SLR de orden k en $\mathbb{F}_q$ con polinomio característico $f(x) \in \mathbb{F}_q[x]$. Entonces, $f(x)$ es el polinomio mínimo de s si y solo si las sucesiones vectoriales $S_0, S_1, ..., S_{k-1}$ son linealmente independientes sobre $\mathbb{F}_q^k$.*

Demostración: Suponemos que $f(x)$ es el polinomio mínimo de s. Supongamos por reducción al absurdo que $S_0, S_1, ..., S_{k-1}$ son linealmente dependientes sobre $\mathbb{F}_q^k$. Tendríamos entonces que $b_0S_0 + b_1S_1 + ... + b_{k-1}S_{k-1} = 0$ con los coeficientes $b_0, b_1, ..., b_{k-1} \in \mathbb{F}_q$ no todos

nulos. Si multiplicamos esta ecuación por la matriz asociada a la SLR, por la Proposición 3.8 se tiene que $b_0S_n + b_1S_{n+1} + ... + b_{k-1}S_{n+k-1} = 0$ para todo $n \geq 0$. Si $b_j = 0$ para $1 \leq j \leq k-1$, se tiene que $S_n = 0$ para todo $n \geq 0$, en contra con que la sucesión no es la constante igual a 0. Luego se tiene el otro caso, existe un $j \geq 1$ tal que $b_j \neq 0$ y j es el máximo con esta propiedad. Se sigue entonces que la sucesión satisface una recurrencia lineal de orden $j < k$, en contra con que $f(x)$ sea el polinomio mínimo. Por tanto, $S_0, S_1, ..., S_{k-1}$ son linealmente independientes sobre $\mathbb{F}_q^k$.

Suponemos ahora que $S_0, S_1, ..., S_{k-1}$ son linealmente independientes sobre $\mathbb{F}_q^k$. Como $S_0 \neq 0$, pues no tomamos el estado inicial nulo, el polinomio mínimo tiene grado positivo. Suponiendo por reducción al absurdo que $f(x)$ no es el polinomio mínimo de s, se tiene que la sucesión satisface una relación de recurrencia de orden $1 \leq m < k$ dada por su polinomio mínimo $m(x) = x^m - a_{m-1}x^{m-1} - ... - a_1x - a_0$. Sea la recurrencia $s_{n+m} = a_{m-1}s_{n+m-1} + ... + a_0s_n$ para $n \geq 0$, se tiene entonces que $S_m = a_{m-1}S_{m-1} + ... + a_0S_0$, en contra con que $S_0, S_1, ..., S_{k-1}$ sean linealmente independientes. Por tanto, $f(x)$ es el polinomio mínimo de s. □

Tal como se vio en la Proposición 3.11, si $S_0 = (0, ..., 0, 1)$ es el estado inicial de un LFSR, los k primeros términos de la sucesión vectorial $S_0, S_1, ..., S_{k-1}$ son linealmente independientes y se deduce el siguiente resultado.

Corolario 4.17. *Sea s la sucesión impulso respuesta de un LFSR, entonces el polinomio mínimo de s coincide con el polinomio de retroalimentación asociado al LFSR.*

4.2. Familias de sucesiones de recurrencia lineal

Siendo $f(x) \in \mathbb{F}_q$ un polinomio mónico de grado positivo, se puede definir el conjunto de todas las SLRs con polinomio asociado $f(x)$, y lo denotamos por $S(f(x))$. Si $f(x)$ es de grado k, entonces $S(f(x))$ contiene q^k SLRs, ya que existen q^k opciones distintas de estado inicial. Además, es fácil ver que $S(f(x))$ es un espacio vectorial de dimensión k sobre $\mathbb{F}_q$.

Lema 4.18. *Sea s una SLR sobre $\mathbb{F}_q$, sea $f(x) = x^k - a_{k-1}x^{k-1} - ... - a_1x - a_0 \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ y $\alpha \in \mathbb{F}_{q^k}$ una raíz de $f(x)$. Si $s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i)$ con $\beta \in \mathbb{F}_{q^k}$ para $i \geq 0$, entonces $s \in S(f(x))$.*

Demostración: Si $\beta = 0$, entonces s es la sucesión constante igual a cero y $s \in S(f(x))$. Si $\beta \neq 0$, entonces

$$s_{i+k} - a_{k-1}s_{i+k-1} - ... - a_0s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+k}) - a_{k-1}Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+k-1}) - ... - a_0Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i) =$$

$$= Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+k} - a_{k-1}\beta\alpha^{i+k-1} - ... - a_0\beta\alpha^i) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i f(\alpha)) = 0$$

y se tiene que $f(x)$ es polinomio característico de s. □

Teorema 4.19. *Sean $f(x), g(x) \in \mathbb{F}_q[x]$ dos polinomios mónicos no constantes, entonces $S(f(x))$ es subconjunto de $S(g(x))$ si y solo si $f(x)$ divide a $g(x)$.*

Demostración: Suponemos que $S(f(x))$ es subconjunto de $S(g(x))$. Sea s la sucesión impulso respuesta perteneciente a $S(f(x))$, por el Corolario 4.17, el polinomio mínimo de s es $f(x)$. Además, s también pertenece a $S(g(x))$, luego por el Teorema 4.11, $f(x)$ divide a $g(x)$. Si suponemos ahora que $f(x)$ divide a $g(x)$, sea s una sucesión perteneciente a $S(f(x))$, entonces, por el Teorema 4.11, el polinomio mínimo $m(x)$ de s divide a $f(x)$. Por tanto, $m(x)$ también divide a $g(x)$, luego, otra vez por el Teorema 4.11, s pertenece a $S(g(x))$. Es decir, $S(f(x))$ es subconjunto de $S(g(x))$. □

Teorema 4.20. *Sean $f_1(x), ..., f_h(x) \in \mathbb{F}_q[x]$ polinomios mónicos no constantes.*

(i) Si $f_1(x), ..., f_h(x)$ son primos entre sí, entonces $S(f_1(x)) \cap ... \cap S(f_h(x))$ contiene únicamente a la sucesión nula.

(ii) Si $f_1(x), ..., f_h(x)$ no son primos entre sí, dado $d(x) = mcd(f_1(x), ..., f_h(x))$ se tiene $S(f_1(x)) \cap ... \cap S(f_h(x)) = S(d(x))$.

Demostración: Sea s una sucesión perteneciente a $S(f_1(x)) \cap ... \cap S(f_h(x))$, entonces, por el Teorema 4.19, el polinomio mínimo $m(x)$ de s divide a $f_1(x), ..., f_h(x)$. Si $f_1(x), ..., f_h(x)$ son primos entre sí, $m(x)$ es necesariamente el polinomio constante igual a 1, y como la única sucesión con polinomio mínimo igual a 1 es la sucesión nula, se tiene el resultado. Si en cambio, $f_1(x), ..., f_h(x)$ no son primos entre sí, $m(x)$ divide a $d(x)$, y por el Teorema 4.11, se tiene que $S(f_1(x)) \cap ... \cap S(f_h(x))$ está contenido en $S(d(x))$. Como $d(x) = mcd(f_1(x), ..., f_h(x))$, por el Teorema 4.19 se tiene que $S(d(x))$ está contenido en $S(f_1(x)) \cap ... \cap S(f_h(x))$. □

Además, se puede definir $S(f(x)) + S(g(x))$ como el conjunto de todas las sucesiones de recurrencia lineal de la forma $s + \bar{s}$ con $s \in S(f(x))$ y $\bar{s} \in S(g(x))$. Esta definición se puede extender a un número finito de conjuntos de SLRs, pudiendo enunciar así el siguiente resultado.

Teorema 4.21. *Sean $f_1(x), ..., f_h(x) \in \mathbb{F}_q[x]$ polinomios mónicos no constantes, entonces $S(f_1(x)) + ... + S(f_h(x)) = S(c(x))$, con $c(x) = mcm(f_1(x), ..., f_h(x))$.*

Demostración: Basta demostrar el resultado para $h = 2$. Por el Teorema 4.19, toda sucesión perteneciente a $S(f_1(x))$ o a $S(f_2(x))$ pertenece también a $S(c(x))$, y como $S(c(x))$ es un espacio vectorial, $S(f_1(x)) + S(f_2(x))$ está contenido en $S(c(x))$. Sea $d(x) = mcd(f_1(x), f_2(x))$, si comparamos las dimensiones de los espacios vectoriales y aplicando el Teorema 4.20, se tiene que

$$dim(S(f_1(x)) + S(f_2(x))) = dim(S(f_1(x))) + dim(S(f_2(x))) - dim(S(d(x))) =$$

$$= deg(f_1(x)) + deg(f_2(x)) - deg(d(x))$$

Como $c(x) = f_1(x)f_2(x)/d(x)$, se tiene $dim(S(f_1(x)) + S(f_2(x))) = deg(c(x)) = dim(S(c(x)))$. Por tanto, como ambos espacios vectoriales tienen misma dimensión y $S(f_1(x)) + S(f_2(x))$ está contenido en $S(c(x))$, se tiene que los espacios vectoriales coinciden. □

Por tanto, si dos polinomios mónicos $f(x)$ y $g(x)$ son no constantes y primos entre sí se tiene que $S(f(x)g(x)) = S(f(x)) + S(g(x))$. Además, $S(f(x)g(x))$ es suma directa de los

subespacios $S(f(x))$ y $S(g(x))$, es decir, toda sucesión $s \in S(f(x)g(x))$ se puede expresar de forma única como $s = s_1 + s_2$ con $s_1 \in S(f(x))$ y $s_2 \in S(g(x))$.

Sea $f(x) \in \mathbb{F}_q[x]$ mónico de grado positivo, se tiene que si s pertenece a $S(f(x))$, entonces para todo $\tau \geq 0$ la sucesión desplazada s^τ pertenece a $S(f(x))$. Para referirse a esta propiedad se dice que el espacio vectorial $S(f(x))$ es cerrado bajo desplazamientos de sucesiones.

Teorema 4.22. *Sea E un conjunto de sucesiones en $\mathbb{F}_q$. Entonces, $E = S(f(x))$ para algún polinomio $f(x) \in \mathbb{F}_q[x]$ mónico de grado positivo si y solo si E es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión finita y cerrado bajo desplazamientos de sucesiones.*

Demostración: Es claro que todo espacio vectorial $S(f(x))$ es cerrado bajo desplazamientos de sucesiones, ya que las sucesiones periódicas desplazadas satisfacen la misma recurrencia lineal, luego tienen el mismo polinomio característico. Sea s una sucesión no nula perteneciente al espacio vectorial E, que suponemos cerrado bajo desplazamientos de sucesiones, se tiene que las sucesiones desplazadas $s^0, s^1, s^2, ..., s^{k-1}$ pertenecen a E. Por el Teorema 4.11, s tiene un polinomio mínimo $m_s(x) \in \mathbb{F}_q[x]$ de grado positivo. Además, por el Teorema 4.16, las sucesiones vectoriales $S_0, S_1, ..., S_{k-1}$ de s son linealmente independientes sobre $\mathbb{F}_q^k$, luego las sucesiones $s^0, s^1, s^2, ..., s^{k-1}$ son elementos linealmente independientes de $S(m_s(x))$ y forman una base de $S(m_s(x))$. Como $s^0, s^1, s^2, ..., s^{k-1}$ pertenecen al espacio vectorial E, $S(m_s(x))$ es un subespacio de E. Sea $E^* = E - \{0\}$, con 0 denotando la sucesión constante igual a 0, se tiene que $\sum_{s \in E^*} S(m_s(x))$ es un subespacio vectorial de E. Es claro que E está contenido en $\sum_{s \in E^*} S(m_s(x))$, luego $E = \sum_{s \in E^*} S(m_s(x))$. Finalmente, por el Teorema 4.21 tenemos que $E = \sum_{s \in E^*} S(m_s(x)) = S(f(x))$, con $f(x)$ el mínimo común múltiplo de los polinomios $m_s(x)$ con $s \in E^*$. □

Del Teorema 4.21 se sigue que la suma de sucesiones de recurrencia lineal es otra SLR, y además se puede obtener su polinomio característico. En casos especiales, el polinomio mínimo de la suma y el periodo también se pueden determinar.

Teorema 4.23. *Sean $s_1, ..., s_h$ SLRs en $\mathbb{F}_q$. Para cada $i = 1, ..., h$, sea $m_i(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de s_i. Si $m_1(x), ..., m_h(x)$ son primos entre sí, entonces el polinomio mínimo de $s = s_1 + ... + s_h$ es $m(x) = m_1(x) \cdot ... \cdot m_h(x)$.*

Demostración: Es suficiente considerar el caso $h = 2$. Si los polinomios mínimos $m_1(x)$ y $m_2(x)$ son los constantes igual a 1 es trivial, y si el polinomio mínimo $m(x)$ de $s = s_1 + s_2$ es el constante igual a 1, también se tiene el caso trivial. Por tanto, asumimos que los polinomios $m(x)$, $m_1(x)$ y $m_2(x)$ son de grado positivo. Por el Teorema 4.21, se tiene que $s = s_1 + s_2 \in S(m_1(x)) + S(m_2(x)) = S(m_1(x)m_2(x))$, luego $m(x)$ divide a $m_1(x)m_2(x)$. Sea $m(x) = x^k - a_{k-1}x^{k-1} - ... - a_1x - a_0$, y sean $r_0, r_1, r_2...$ los términos de la sucesión s_1, y $t_0, t_1, t_2...$ los términos de la sucesión s_2, entonces se tiene la siguiente recurrencia para la sucesión $s = s_1 + s_2$

$$r_{n+k} + t_{n+k} = a_{k-1}(r_{n+k-1} + t_{n+k-1}) + ... + a_0(r_n + t_n)$$

Definimos la sucesión u como $u_n = r_{n+k} - a_{k-1}r_{n+k-1} - ... - a_0r_n = -t_{n+k} + a_{k-1}t_{n+k-1} + ... + a_0t_n$ para $n \geq 0$. Por el Teorema 4.22, $S(m_1(x))$ y $S(m_2(x))$ son espacios vectoriales

cerrados bajo desplazamientos de sucesiones, luego la sucesión u pertenece a $S(m_1(x))$ y a $S(m_2(x))$, y por el Teorema 4.20, u es la sucesión nula. De esto se sigue que tanto $m_1(x)$ como $m_2(x)$ dividen a $m(x)$, por tanto, $m_1(x)m_2(x)$ divide a $m(x)$, luego $m(x) = m_1(x)m_2(x)$. □

Si los polinomios $m_1(x), ..., m_h(x)$ no son primos entre sí, para determinar el polinomio mínimo de $s = s_1+...+s_h$ se pueden utilizar las funciones generatrices. Si $G_i(x)$ es la función generatriz de s_i, entonces $G(x) = G_1(x)+...+G_h(x)$ es la función generatriz de s. Sabemos que cada $G_i(x)$ se puede escribir como $G_i(x) = \dfrac{g_i(x)}{m_i^*(x)}$, luego, $G(x) = \displaystyle\sum_{i=1}^{h} \frac{g_i(x)}{m_i^*(x)} = \frac{g_0(x)}{f_0^*(x)}$, con $g_0(x), f_0^*(x) \in \mathbb{F}_q[x]$. Sea k_0 el grado de $f_0^*(x)$, sabemos que $f_0(x) = x^{k_0} f_0^*(\frac{1}{x})$ es polinomio característico de s, y siguiendo el mismo procedimiento de la demostración del Teorema 4.11 se puede obtener el polinomio mínimo de s.

Ejemplo 4.24. *Sea s_1 la sucesión impulso respuesta en $\mathbb{F}_2$ perteneciente a $S(x^3+x^2+x+1)$ y sea s_2 la sucesión impulso respuesta en $\mathbb{F}_2$ perteneciente a $S(x^4+x^2+x+1)$. Por el Corolario 4.17, el polinomio mínimo de s_1 es $m_1(x) = x^3+x^2+x+1 = (x+1)^3$, y el polinomio mínimo de s_2 es $m_2(x) = x^4+x^2+x+1 = (x+1)(x^3+x^2+1)$. Sabemos que la función generatriz de la sucesión $s = s_1 + s_2$ es*

$$G(x) = \frac{g_1(x)}{m_1^*(x)} + \frac{g_2(x)}{m_2^*(x)} = \frac{x^2}{(x+1)^3} + \frac{x^3}{(x+1)(x^3+x+1)} = \frac{x^2}{(x+1)^3(x^3+x+1)}$$

con $g_1(x), g_2(x) \in \mathbb{F}_2[x]$ determinados por (4.6). Sea $f_0^*(x) = (x+1)^3(x^3+x+1)$, su polinomio recíproco $f_0(x) = (x+1)^3(x^3+x^2+1)$ es polinomio característico de s. Por (4.7) tenemos $h_0(x) = -x^5(\frac{1}{x})^2 = -x^3 = x^3$, y como $f_0(x)$ y $h_0(x)$ son primos entre sí, siguiendo la demostración del Teorema 4.11, el polinomio mínimo de s es $m(x) = (x+1)^3(x^3+x^2+1)$.

Teorema 4.25. *Sean $s_1, ..., s_h$ SLRs en $\mathbb{F}_q$. Para cada $i = 1, ..., h$, sea r_i el periodo de s_i y sea $m_i(x) \in \mathbb{F}_q[x]$ el polinomio mínimo. Si $m_1(x), ..., m_h(x)$ son primos entre sí, entonces el periodo de $s = s_1 + ... + s_h$ es $r = mcm(r_1, ..., r_h)$.*

Demostración: Demostramos el resultado considerando $h = 2$. Por los teoremas 4.12 y 4.23, se tiene que $r = ord(m_1(x)m_2(x))$. Por otro lado, por el Teorema 2.34 se tiene que $ord(m_1(x)m_2(x))$ es igual al mínimo común múltiplo de $ord(m_1(x))$ y $ord(m_2(x))$, es decir, $r = mcm(r_1, r_2)$. □

Ejemplo 4.26. *Sean s_1 y s_2 las sucesiones del Ejemplo 4.24, entonces, por el Teorema 2.33, el periodo de s_1 es $r_1 = ord(m_1) = 4$, y por el Teorema 2.34, el periodo de s_2 es $r_2 = ord(m_2) = 7$ y el periodo de $s = s_1 + s_2$ es $r = ord(m) = 28$.*

$$\begin{aligned} s_1 &= 00110011001100110011001100110011001100110011001100110011... \\ s_2 &= 00010110001011000101100010110001011000101100010110001011... \\ \hline s = s_1 + s_2 &= 00100101000111110110101110000010010100011111011010111000... \end{aligned}$$

A pesar de que $m_1(x)$ y $m_2(x)$ no son primos entre sí, condiciones que deben darse para poder usar los teoremas 4.23 y 4.25, coincide que el polinomio mínimo de s es

$m(x) = mcm(m_1(x), m_2(x))$ y el periodo es $r = mcm(r_1, r_2)$. Esto es casualidad, ya que el polinomio mínimo $m(x)$ es un divisor de $mcm(m_1(x), m_2(x))$ y el periodo r es un divisor de $mcm(r_1, r_2)$.

Sea s una sucesión sobre $\mathbb{F}_2$, si sumamos la sucesión constante igual a uno a s nos queda una sucesión $\bar{s}$ con unos en las posiciones donde s tenía ceros y viceversa. A la sucesión $\bar{s}$ se la denomina complementaria de s, y es claro que tiene el mismo periodo que s. Como $\bar{s}$ se obtiene como suma de dos sucesiones, si s es sucesión de recurrencia lineal entonces $\bar{s}$ también. Además, el polinomio mínimo de $\bar{s}$ se puede obtener a partir del polinomio mínimo de s.

Teorema 4.27. *Sea s una SLR sobre $\mathbb{F}_2$ y sea $\bar{s}$ su complementaria. Si $m(x) \in \mathbb{F}_2[x]$ es el polinomio mínimo de s, se puede escribir como $m(x) = (x+1)^h m_1(x)$, con $h \geq 0$ un entero y $m_1(x) \in \mathbb{F}_2[x]$ tal que $m_1(1) = 1$. Entonces, el polinomio mínimo de $\bar{s}$ es*

$$\overline{m}(x) = \begin{cases} (x+1)m(x) & si\ h = 0, \\ m_1(x) & si\ h = 1, \\ m(x) & si\ h > 1 \end{cases}$$

Demostración: Sea σ la sucesión constante igual a uno sobre $\mathbb{F}_2$. Como $\bar{s} = s + \sigma$ y el polinomio mínimo de σ es $x + 1$, por el Teorema 4.23, se tiene el caso $h = 0$. Si $h \geq 1$, por el Teorema 4.21 se tiene que $\bar{s} = s + \sigma \in S(m(x))$, y entonces $\overline{m}(x)$ divide a $m(x)$. Si $\overline{m}(x)$ es el polinomio constante igual a 1, entonces $\bar{s}$ es la sucesión constante igual a cero y $s = \sigma$, y se tiene el caso $h = 1$ con $m_1(x) = 1$. Suponemos entonces que $\overline{m}(x)$ es de grado positivo. Por el Teorema 4.21, se tiene que $s = \bar{s} + \sigma \in S(c(x))$, con $c(x) = mcm(\overline{m}(x), (x+1))$, y como $c(x)$ divide a $\overline{m}(x)(x+1)$, por el Teorema 4.19, se tiene que $s = \bar{s} + \sigma \in S(\overline{m}(x)(x+1))$. Por tanto, $m(x)$ divide a $\overline{m}(x)(x+1)$, y entonces, para $h \geq 1$ se tiene o bien $\overline{m}(x) = m(x)$ o bien $\overline{m}(x) = (x+1)^{h-1} m_1(x)$. Si $h > 1$, se sigue que $s = \bar{s} + \sigma \in S(\overline{m}(x))$, luego $m(x)$ divide a $\overline{m}(x)$ y se tiene $\overline{m}(x) = m(x)$. Si $h = 1$, sean $s_0, s_1, ...$ los términos de s y sea $m_1(x) = x^k - a_{k-1}x^{k-1} - ... - a_0$ de grado positivo, definimos $u_n = s_{n+k} - a_{k-1}s_{n+k-1} - ... - a_0 s_n$ para $n \geq 0$. Como $m(x) = (x+1)m_1(x)$ es polinomio característico de la sucesión s, se tiene que $u_{n+1} = u_n$ para todo $n \geq 0$, luego $u_0 = u_n$ para todo $n \geq 0$. Por tanto, $u_0 = 1$, porque si no $m_1(x)$ sería el polinomio mínimo de s. Es decir, tenemos $s_{n+k} + 1 = a_{k-1}s_{n+k-1} + ... + a_0 s_n$ para todo $n \geq 0$. Como $m_1(1) = 1 + a_{k-1} + ... + a_0 = 1$, se tiene $a_{k-1} + ... + a_0 = 0$ y se puede escribir $s_{n+k} + 1 = a_{k-1}(s_{n+k-1} + 1) + ... + a_0(s_n + 1)$ para todo $n \geq 0$. Por tanto, $m_1(x)$ es polinomio característico de $\bar{s}$, y se sigue que $\overline{m}(x) = m_1(x)$ si $h = 1$. □

Sea $f(x) \in \mathbb{F}_q[x]$ mónico de grado positivo, queremos determinar exactamente los periodos posibles de las sucesiones de $S(f(x))$ (dependiendo de su estado inicial, cuando $f(x)$ no es irreducible) y cuántas sucesiones de $S(f(x))$ tienen cada periodo (ver Tabla 3.1).

Teorema 4.28. *Sea $f(x) = g(x)^b$ con b un entero positivo y $g(x) \in \mathbb{F}_q[x]$ mónico de grado k e irreducible sobre $\mathbb{F}_q$, tal que $g(0) \neq 0$ y $ord(g) = e$. Sea t el menor entero tal que $p^t \geq b$, con p la característica de $\mathbb{F}_q$. Entonces, si $b = 1$, $S(f(x))$ contiene una sucesión de periodo 1 y $q^k - 1$ sucesiones de periodo e. Si $b \geq 2$, $S(f(x))$ contiene una sucesión de periodo 1,*

q^k-1 sucesiones de periodo e, $q^{kp^j}-q^{kp^{j-1}}$ sucesiones de periodo ep^j, con $j=1,2,...,t-1$, y $q^{kb}-q^{kp^{t-1}}$ sucesiones de periodo ep^t.

Demostración: El caso $b=1$ se tiene por el Teorema 4.5. Si $b\geq 2$, el polinomio mínimo de toda sucesión de $S(f(x))$, con estado inicial no nulo, es de la forma $g(x)^c$, con $1\leq c\leq b$. Como $g(x)$ es irreducible, por el Teorema 4.14, $g(x)$ es el polinomio mínimo de todas las sucesiones de $S(g(x))$ con estado inicial no nulo. Por tanto, hay q^k-1 sucesiones de $S(f(x))$ con polinomio mínimo $g(x)$. Sabemos que las sucesiones pertenecientes a $S(g(x)^2)$ tienen polinomio característico $g(x)^2$, por tanto, por definición de polinomio mínimo (ver Teorema 4.11), el polinomio mínimo de las sucesiones de $S(g(x)^2)$ es o bien $g(x)^2$ o bien $g(x)$. Por el Teorema 4.19, se tiene que $S(g(x))\subseteq S(g(x)^2)\subseteq ...\subseteq S(f(x))$, luego, el número de sucesiones con polinomio mínimo $g^2(x)$ es el número de sucesiones de $S(g(x)^2)$ menos el número de sucesiones de $S(g(x))$. Es decir, hay $q^{2k}-1-(q^k-1)=q^{2k}-q^k$ sucesiones en $S(f(x))$ con polinomio mínimo $g(x)^2$. En general, para $1\leq c\leq b$ hay $q^{ck}-q^{(c-1)k}$ sucesiones de $S(f(x))$ con polinomio mínimo $g(x)^c$.

Por el Teorema 4.12, el periodo de una sucesión coincide con el orden de su polinomio mínimo, por tanto, en $S(f(x))$ hay q^k-1 sucesiones de periodo $e=ord(g)$. Para una potencia arbitraria $g(x)^c$, con $2\leq c\leq p$, claramente $h=1$ es el menor entero que cumple $p^h\geq c$, y por el Teorema 2.33, se tiene que el orden de $g(x)^c$ es ep. Por tanto, las sucesiones con polinomio mínimo $g(x)^c$ tienen periodo ep. Como esto ocurre para $2\leq c\leq p$, y como $S(g(x))\subseteq S(g(x)^2)\subseteq ...\subseteq S(g(x)^b)$, las sucesiones con periodo ep son las sucesiones de $S(g(x)^p)$ menos las sucesiones de $S(g(x))$. Es decir, en $S(f(x))$ hay $q^{pk}-1-(q^k-1)=q^{pk}-q^k$ sucesiones de periodo ep. Siguiendo este razonamiento, si $p+1\leq c\leq p^2$, las sucesiones con polinomio mínimo $g(x)^c$ tienen periodo ep^2, es decir, se tiene que en $S(f(x))$ hay $q^{p^2k}-1-(q^{pk}-1)=q^{p^2k}-q^{pk}$ sucesiones de periodo ep^2. En general, sea t el menor entero tal que $p^t\geq b$, si $p^{j-1}+1\leq c\leq p^j$, las sucesiones con polinomio mínimo $g(x)^c$ tienen periodo ep^j, y se tiene que en $S(f(x))$ hay $q^{p^jk}-q^{p^{j-1}k}$ sucesiones de periodo ep^j, para $1\leq j\leq t-1$. Nos queda el caso $p^{t-1}+1\leq c\leq b$. Por el mismo argumento, las sucesiones con polinomio mínimo $g(x)^c$ tienen periodo ep^t, pero como $b\leq p^t$, en $S(f(x))$ no hay sucesiones con polinomio mínimo $g(x)^a$ con $a>b$, por tanto, en $S(f(x))$ hay $q^{bk}-q^{p^{t-1}k}$ sucesiones de periodo ep^t. □

Si en cambio, $f(x)=g_1(x)^{b_1}\cdot ...\cdot g_h(x)^{b_h}\in\mathbb{F}_q[x]$ tal que $f(0)\neq 0$, con $g_i(x)$ polinomios mónicos, irreducibles y distintos sobre $\mathbb{F}_q$ y siendo b_i enteros positivos. Se sigue del Teorema 4.21 que $S(f(x))=S(g_1(x)^{b_1})+...+S(g_h(x)^{b_h})$. Además, toda sucesión de $S(f(x))$ se obtiene formando todas las posibles sumas $s_1+...+s_h$ con $s_i\in S(g_i(x)^{b_i})$ para $1\leq i\leq h$. Por el Teorema 4.28 sabemos cómo son los periodos de las sucesiones de $S(g_i(x)^{b_i})$, por tanto la información análoga del periodo de $S(f(x))$ se deduce del Teorema 4.25.

Ejemplo 4.29. *Sea $f(x)=(x^3+x^2+1)^2(x^4+x+1)\in\mathbb{F}_2$. Por el Teorema 4.28, $S((x^3+x^2+1)^2)$ contiene una sucesión de periodo 1, 7 sucesiones de periodo 7, y 56 sucesiones de periodo 14. Por otro lado, $S((x^4+x+1))$ contiene una sucesión de periodo 1 y 15 sucesiones de periodo 15. Si formamos todas las posibles sumas de las sucesiones de $S((x^3+x^2+1)^2)$ y $S((x^4+x+1))$, por el Teorema 4.25, $S(f(x))$ contiene una sucesión de periodo 1, 7 sucesiones de periodo 7, 56 sucesiones de periodo 14, 15 sucesiones de periodo 15, 105 sucesiones de periodo 105, y 840 sucesiones de periodo 210.*

Ejemplo 4.30. *Sea* $f(x) = x^5 + x^3 + x^2 + 1 = (x+1)^3(x^2+x+1)$ *sobre* $\mathbb{F}_2$*, el polinomio del Ejemplo 3.21. Por el Teorema 4.28,* $S((x+1)^3)$ *contiene 2 sucesiones de periodo 1, 2 sucesiones de periodo 2 y 4 sucesiones de periodo 4, y* $S((x^2+x+1))$ *contiene una sucesión de periodo 1 y 3 sucesiones de periodo 3. Por tanto,* $S(f(x))$ *contiene 2 sucesiones de periodo 1, 2 sucesiones de periodo 2, 6 sucesiones de periodo 3, 4 sucesiones de periodo 4, 6 sucesiones de periodo 6 y 12 sucesiones de periodo 12. Es decir, la Tabla 3.1 es coherente.*

Por tanto, es posible generar sucesiones con periodo largo sin necesidad de disponer de polinomios primitivos de grado alto, aunque depende del estado inicial encontrar una sucesión de periodo largo.

Capítulo 5

Sucesión máxima

Previamente, en el Lema 3.4, vimos que el periodo de una sucesión de recurrencia lineal puede ser a lo sumo $q^k - 1$. En este capítulo se estudiarán resultados relacionados con el periodo de las SLRs, profundizando en sucesiones con propiedades particulares y explicando en qué condiciones el periodo de una SLR, con polinomio característico y estado inicial dados, es el máximo posible en $\mathbb{F}_q$. Se toman como referencia [1], [3], [4], [6], [9] y [11].

Definición 5.1. *Dada una SLR de orden k sobre $\mathbb{F}_q$, se llama sucesión máxima o m-sucesión si el polinomio característico es primitivo.*

El nombre de m-sucesión viene de que es la SLR con máximo periodo. Por los resultados vistos en el capítulo anterior, el Teorema 4.5 y la definición de polinomio primitivo, sabemos que las m-sucesiones tienen periodo $q^k - 1$, el máximo que se puede alcanzar en $\mathbb{F}_q$. Estas sucesiones son importantes ya que, en muchos aspectos, se comportan como si fueran realmente aleatorias. Por ello, reciben también el nombre de PN-sucesión, que viene del término inglés pseudo-noise sequence, donde noise es un término usado en electrónica que se atribuye a señales de origen aleatorio, como si fuera ruido.

Ejemplo 5.2. *Si tomamos el polinomio primitivo $x^3 + x + 1$ de orden 7, su sucesión impulso respuesta es $s = 00101110010111...$, de periodo 7. Además, se tienen las siguientes 7 sucesiones vectoriales: (0,0,1), (0,1,0), (1,0,1), (0,1,1), (1,1,1), (1,1,0) y (1,0,0). Se puede observar que son todas distintas entre sí y que aparece toda sucesión vectorial posible de tamaño 3 excepto la nula. Esto ocurre siempre, como se muestra en el siguiente resultado.*

Teorema 5.3. *Sea s una m-sucesión de orden k sobre $\mathbb{F}_q$, en todo periodo $s_n, s_{n+1}, ..., s_{n+q^k-2}$, cada sucesión vectorial $S_i = (s_i, s_{i+1}, ..., s_{i+k-1})$ no nula, con $s_j \in \mathbb{F}_q$, aparece una sola vez.*

Demostración: La sucesión vectorial nula no puede ocurrir, ya que entonces se tendría la SLR constante igual a cero. Dado que el periodo es $q^k - 1$, las $q^k - 1$ sucesiones vectoriales $S_i = (s_i, s_{i+1}, ..., s_{i+k-1})$ de tamaño k son $S_0, S_1, ..., S_{q^k-2}$, ya que $S_0 = S_{q^k-1}$. Supongamos por reducción al absurdo que existen $i, j \in \mathbb{N}$ con $0 \leq i < j \leq q^k - 2$ tales que $S_i = S_j$. Ahora, como el elemento s_{i+k} depende de S_i y el elemento s_{j+k} depende de S_j, al ser $S_i = S_j$, entonces $s_{i+m} = s_{j+m}$ para todo $m \geq 0$. Es decir, el periodo es como mucho $j - i - 1 \leq q^k - 2$, en contra con que el periodo es $q^k - 1$. □

Ejemplo 5.4. *Dados los polinomios primitivos* x^2+x+1, x^3+x^2+1, x^4+x^3+1 *y* $x^5+x^4+x^3+x+1$ *sobre* $\mathbb{F}_2[x]$, *de órdenes 3, 7, 15 y 31 respectivamente, sus sucesiones impulso respuesta son las siguientes:*

Polinomio de retroalimentación	Sucesión impulso respuesta
x^2+x+1	011011...
x^3+x^2+1	00111010011101...
x^4+x^3+1	000111101011001000111101011001...
$x^5+x^4+x^3+x+1$	000011010100100010111110110011100001101010010 0...

Tabla 5.1: Sucesiones impulso respuesta del Ejemplo 5.4.

Se puede observar que los periodos de las sucesiones son 3, 7, 15 y 31 respectivamente, es decir, 2^k-1 *con* k *el grado del polinomio.*

En el ejemplo anterior se dan polinomios primitivos de grados 2, 3, 4 y 5 respectivamente. El polinomio x^2+x+1 es el único polinomio irreducible de grado 2 sobre $\mathbb{F}_2[x]$, que además es primitivo. De grado 3 existen dos polinomios primitivos, x^3+x^2+1 y x^3+x+1, pero de grado 4 hay tres polinomios irreducibles, x^4+x+1, x^4+x^3+1 y $x^4+x^3+x^2+x+1$, los dos primeros primitivos y el último no, ya que tiene orden 5 pues $(x^4+x^3+x^2+x+1)(x-1)=(x^5-1)$.

Si $f(x)\in\mathbb{F}_q[x]$ es un polinomio primitivo de grado k, cada estado inicial S_0 distinto del nulo genera una m-sucesión. Del Teorema 5.3 se deduce que si S_0 y $\bar{S}_0$ son dos estados iniciales distintos, las sucesiones que generan s y $\bar{s}$ son una trasladada de la otra (pues en s aparecerá $\bar{S}_0$ en el periodo y en $\bar{s}$ aparece S_0). Por tanto, ambas sucesiones pueden considerarse la misma. Además, dos polinomios primitivos distintos no pueden generar la misma sucesión porque entonces deben satisfacer dos recurrencias distintas de mismo orden. Por tanto, el número de m-sucesiones es igual al número de polinomios primitivos de grado k. En consecuencia, y a partir del Teorema 2.38, se tiene el siguiente resultado.

Corolario 5.5. *Sobre* $\mathbb{F}_q$ *existen* $\varphi(q^k-1)/k$ *m-sucesiones de orden k.*

Sea s una sucesión de recurrencia lineal sobre $\mathbb{F}_{p^n}$, y sean $\{\alpha_0,\alpha_1,...,\alpha_{n-1}\}$ y $\{\beta_0,\beta_1,...,\beta_{n-1}\}$ bases duales de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_p$. Por el Teorema 2.44, el i-ésimo término de la sucesión s se puede escribir como

$$s_i=\sum_{j=0}^{n-1} Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta_j s_i)\alpha_j\in\mathbb{F}_{p^n}$$

Se puede definir entonces la sucesión $c_j=(c_{i,j})_{i=0}^{\infty}$ en $\mathbb{F}_p$, donde $c_{i,j}=Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\beta_j s_i)\in\mathbb{F}_p$. Para $0\le j\le n-1$, la sucesión c_j se llama la sucesión de componentes de s j-ésima respecto a $\mathbb{F}_p$.

Proposición 5.6. *Sea* s *una m-sucesión de orden* k *sobre* $\mathbb{F}_q$, *con* $q=p^n$, *entonces todas las sucesiones de componentes de* s *respecto a* $\mathbb{F}_p$ *son m-sucesiones de orden* nk *sobre* $\mathbb{F}_p$.

Demostración: Como s es m-sucesión con polinomio mínimo $m(x)$, $m(x)$ es primitivo. Sea $\alpha \in \mathbb{F}_{q^k}$ una raíz de $m(x)$, por el Teorema 4.6, $s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma\alpha^i)$ con $\gamma \in \mathbb{F}_{q^k}$. Por definición, el i-ésimo término de la sucesión de componentes de s j-ésima respecto a $\mathbb{F}_p$ se escribe como $c_{i,j} = Tr_{\mathbb{F}_q/\mathbb{F}_p}(\beta_j s_i)$. Por tanto, $c_{i,j} = Tr_{\mathbb{F}_q/\mathbb{F}_p}(\beta_j Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma\alpha^i))$, y por la transitividad de la traza del Teorema 2.42, $c_{i,j} = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_p}((\beta_j\gamma)\alpha^i)$, con $\beta_j\gamma \in \mathbb{F}_{q^k}$. Como α es un elemento primitivo de la extensión $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^k}$, con $\mathbb{F}_{q^k} = \mathbb{F}_{p^{nk}}$, se tiene que α es un elemento primitivo de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Es decir, α satisface un polinomio primitivo con coeficientes en $\mathbb{F}_p$ de grado nk. Sea este polinomio $\widehat{m}(x)$, por el Lema 4.18, $c_j \in S(\widehat{m}(x))$, y por tanto, c_j es una m-sucesión de grado nk sobre $\mathbb{F}_p$. □

5.1. Postulados de Golomb y distribución de rachas

En general, las sucesiones que vamos a considerar son las binarias, es decir, trabajamos sobre $\mathbb{F}_2$. Como las sucesiones que estudiamos no son aleatorias, para poder aceptarlas como pseudoaleatorias deben cumplir ciertas propiedades que se asocian a la aleatoriedad:

1. El número de ceros es aproximadamente igual al número de unos.

2. Bloques de ceros o unos consecutivos aparecen frecuentemente. Los bloques de tamaño más grande ocurren con menor frecuencia que los de menor tamaño. Es más, aproximadamente la mitad de los bloques son de tamaño 1, un cuarto de ellos son de tamaño 2, un octavo de tamaño 3, y así sucesivamente.

3. El número de coincidencias entre una sucesión y su desplazada τ posiciones no debe aportar información acerca del periodo de la sucesión. Esta propiedad tiene que ver con la función de autocorrelación.

Definición 5.7. *Sea s una sucesión periódica de periodo r, su función de autocorrelación se define como* $C(\tau) = \sum_{i=0}^{r-1}(-1)^{s_i}(-1)^{s_{i+\tau}}$, *donde* $\tau \geq 0$.

La función de autocorrelación $C(\tau)$ mide la similitud entre la sucesión s y su desplazada s^τ. Si la sucesión s es aleatoria, no hay similitud entre las sucesiones para casi todo valor de $\tau \neq 0$.

Las propiedades vistas de aleatoriedad introducen los postulados de Golomb, pero primero, para poder enunciar los postulados, se debe definir el concepto de racha.

Sea la sucesión periódica 000111110100001111... de periodo 18, esta sucesión tiene un bloque de 0's seguidos de tamaño 3, un bloque de 1's seguidos de tamaño 5, un bloque de 0's seguidos de tamaño 4 y un bloque de 1's seguidos de tamaño 4. Estos bloques de bits seguidos se denominan rachas.

Definición 5.8. *Sea s una sucesión binaria, se define racha de tamaño t de 1's (respectivamente de 0's) a la secuencia de exactamente t bits seguidos de 1's (respectivamente de 0's) de la sucesión.*

Es evidente que el número de rachas es en realidad infinito, ya que la sucesión es infinita, es por ello que, siendo r el periodo de la sucesión, se toma como número de rachas el número de ellas que se encuentren entre los r primeros bits. Además, es claro que, salvo las sucesiones constantes, no se puede hablar de rachas de tamaño mayor que el periodo de la sucesión.

Las rachas son interesantes de estudiar ya que las m-sucesiones tienen una distribución de rachas muy regular y predecible.

Ejemplo 5.9. *Dado el polinomio primitivo* $f(x) = x^6 + x^5 + x^3 + x^2 + 1$*, la m-sucesión impulso respuesta asociada a* $f(x)$ *es:*

$$000001110000100100011011001011010111011110011000101010011111101...$$

y tiene la distribución de rachas de 0's y 1's descrita en la Tabla 5.2.

Tamaño de la racha	Nº de rachas de 0's	Nº de rachas de 1's
1	8	8
2	4	4
3	2	2
4	1	1
5	1	0
6	0	1
Nº total:	16	16

Tabla 5.2: Distribución de rachas de la m-sucesión del Ejemplo 5.9.

Hay un total de 16 rachas de 0's, la mitad son de tamaño 1, un cuarto de tamaño 2, un octavo de tamaño 3 y un dieciseisavo de tamaño 4. Esta misma distribución tan ordenada se da también para las rachas de 1's. Sin embargo, el número de rachas de tamaño 5 y 6 no coincide para 0's y 1's. Esto ocurre para toda m-sucesión, como se ve a continuación.

Teorema 5.10. *La distribución de rachas de toda m-sucesión binaria de orden* k *cumple:*

- *Si* $k \geq 3$*: para* $1 \leq i \leq k-2$*, existen* 2^{k-i-2} *rachas tanto de 0's como de 1's de tamaño* i*. De tamaño* $k-1$ *existe una racha de 0's y ninguna de 1's, y de tamaño* k*, existe una racha de 1's y ninguna de 0's. En total, toda m-sucesión tiene* 2^{k-2} *rachas tanto de ceros como de unos.*

- *Si* $k = 2$*: de tamaño 1 existe una racha de 0's y ninguna de 1's, y de tamaño 2, existe una racha de 1's y ninguna de 0's.*

- *Si* $k = 1$*: las sucesiones generadas son las constantes igual a 0 o igual a 1, luego no tiene sentido hablar de rachas.*

Demostración: Para contar las rachas que hay de cada tamaño nos va a servir diferenciar entre tres casos y utilizar el Teorema 5.3.

- Tamaño k: por el Teorema 5.3 no hay rachas de 0's de tamaño k y hay una única racha de 1's de tamaño k.

- Tamaño $k-1$: sea la sucesión vectorial $S_i = (1, ..., 1)$ la única racha de 1's de tamaño k, para algún $0 \leq i \leq 2^k - 2$, entonces se tiene que dar $s_{i-1} = 0 = s_{i+k}$. Si no fuera así, se tendría otra racha de 1's de tamaño k distinta a S_i, contradiciendo el Teorema 5.3. De esto se tiene la subsucesión 011...10 de tamaño $k+2$ y en esta subsucesión aparecen las dos sucesiones vectoriales $S_{i-1} = (0, 1, ..., 1)$ y $S_{i+1} = (1, ..., 1, 0)$. Si suponemos por reducción al absurdo que hay una racha de 1's de tamaño $k-1$ en algún lugar $j \neq i$ de la sucesión, tendríamos de nuevo que $s_{j-1} = 0 = s_{j+k-1}$ y la subsucesión 011...10 de tamaño $k+1$. Teniendose $S_{j-1} = (0, 1, ..., 1)$ y $S_j = (1, ..., 1, 0)$, en contra con el Teorema 5.3. Por lo tanto, no puede haber una racha de 1's de tamaño $k-1$. En cambio, sí hay una racha de 0's de tamaño $k-1$. Por el Teorema 5.3, las sucesiones vectoriales $(1, 0, ..., 0)$ y $(0, ..., 0, 1)$ aparecen una única vez en la sucesión y, siguiendo el mismo procedimiento anterior, tenemos que además aparecen seguidas, siendo $S_l = (1, 0, ..., 0)$ y $S_{l+1} = (0, ..., 0, 1)$ para algún $0 \leq l \leq 2^k - 2$.

- Tamaño $r \leq k-2$: cada racha de 1's de tamaño $r \leq k-2$ corresponde a una sucesión vectorial de la forma

$$\overbrace{0, \underbrace{1, 1, ..., 1}_{r}, 0, \underbrace{x, ..., x}_{k-r-2}}^{k}$$

  donde los x's son bits binarios arbitrarios. Hay claramente 2^{k-r-2} sucesiones vectoriales de este tipo, luego hay 2^{k-r-2} rachas de 1's de tamaño r. Siguiendo el mismo argumento, se tiene que hay 2^{k-r-2} rachas de 0's de tamaño r. □

Sea s una sucesión binaria periódica de periodo r y orden k, entonces los postulados de Golomb son los siguientes:

(G1) *Test de distribución:* en cada periodo, el número de 1's y 0's es aproximadamente el mismo. Es más, la diferencia entre el número de 1's y el número de 0's es como mucho 1:

$$\left| \sum_{i=0}^{r-1} (-1)^{s_i} \right| \leq 1$$

(G2) En todo periodo, la mitad de las rachas son de tamaño 1, un cuarto de tamaño 2, un octavo de tamaño 3 y así sucesivamente siempre que el tamaño de las rachas sea menor que $k-1$. Además, para cada tamaño menor que $k-1$, el número de rachas de 1's coincide con el número de rachas de 0's.

(G3) *Test de autocorrelatión:* la función de autocorrelación $C(\tau)$ toma únicamente dos valores:

$$C(\tau) = \sum_{i=0}^{r-1} (-1)^{s_i} (-1)^{s_{i+\tau}} = \begin{cases} 2^k - 1 & \text{si } \tau = 0, \\ -1 & \text{si } 0 < \tau < 2^k - 1 \end{cases} \tag{5.1}$$

La importancia de los postulados de Golomb es que toda sucesión que los cumpla se acepta como pseudoaleatoria, como por ejemplo, las m-sucesiones.

Teorema 5.11. *Toda m-sucesión de orden $k \geq 2$ satisface (G1)-(G3).*

Demostración: Dado que el Teorema 5.10 nos indica la distribución de rachas de toda m-sucesión de orden k, los postulados (G1) y (G2) se siguen directamente de la siguiente forma.

Si $k = 2$, en cada periodo de $r = 2^k - 1 = 3$ términos, el número total de rachas es 2, una racha de 0's de tamaño 1 y una racha de 1's de tamaño 2. Por tanto, se tiene $\left|\sum_{i=0}^{2}(-1)^{s_i}\right| = |-1| = 1$, luego se cumple (G1). Además, en este caso no tiene sentido hablar del postulado (G2), ya que el tamaño de las rachas es $k-1$ y k.

Si $k \geq 3$, en cada periodo de $r = 2^k - 1$ términos, el número total de rachas tanto de 0's como de 1's es 2^{k-2}, luego hay un total de 2^{k-1} rachas. Además, de tamaño $1 \geq i \geq k-2$ hay un total de 2^{k-i-1} rachas de 0's y 1's. Para $i = 1$ se tiene la mitad del total, para $i = 2$ un cuarto, para $i = 3$ un octavo, y así sucesivamente. Por otro lado, como hay 2^{k-i-2} rachas tanto de 0's como de 1's de tamaño $1 \geq i \geq k-2$, se tiene que hay el mismo número de 0's y de 1's si contamos solo las rachas hasta tamaño $k-2$. De tamaño $k-1$ existe una única racha de 0's y ninguna de 1's, y de tamaño k existe una racha de 1's y ninguna de 0's, por lo tanto, la diferencia entre el número total de 1's y el número total de 0's en el periodo es exactamente 1. Quedan probados (G1) y (G2).

Si tomamos $\tau = 0$ se tiene que $C(0) = 2^k - 1$ es uno de los valores que toma la función de autocorrelación. Probamos ahora que $C(\tau) = -1$ con $0 < \tau < 2^k - 1$ para demostrar (G3). Por el Teorema 4.6 y siendo α raíz del polinomio de retroalimentación, como es primitivo tenemos que $s_i = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\beta\alpha^i)$ con $\beta \in \mathbb{F}_{2^n}$. Además, como la sucesión $s_{i+\tau} = s_i^\tau$ es su desplazada, $s_{i+\tau}$ satisface la misma ley de recurrencia y por tanto tienen mismo polinomio característico, luego se tiene $s_{i+\tau} = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\bar{\beta}\alpha^i)$ con el mismo α para ambas igualdades. Por la Proposición 2.40 se tiene entonces que $s_i + s_{i+\tau} = Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}((\beta+\bar{\beta})\alpha^i)$. Por tanto, $(s_i + s_{i+\tau})_{i=0}^{\infty}$ es también una m-sucesión. Por (G1) tenemos que en la m-sucesión $(s_i + s_{i+\tau})_{i=0}^{\infty}$ la diferencia entre el número total de 1's y el número total de 0's en el periodo es exactamente 1. Por lo tanto, $C(\tau) = \sum_{i=0}^{r-1}(-1)^{s_i+s_{i+\tau}} = -1$, es decir, la función de autocorrelación toma únicamente los valores $2^k - 1$ y -1. □

En algunos libros, como en [9], se enuncian como postulados de Golomb (G1), (G3) y el siguiente:

(G4) *Test de serie:* sea a una n-tupla, denotemos como $N(a)$ el número de veces que aparece a en el periodo. Entonces, para todo n, con $0 \leq n < k$, se tiene

$$| N(a) - N(b) | \leq 1$$

para cualesquiera n-tuplas a y b.

El test de serie es una generalización de (G2), ya que las rachas de 0's y 1's son un caso particular de n-tuplas. Como hemos visto, por (G2) tenemos que existen el mismo número de rachas de 0's y 1's hasta tamaño $k-2$, y para tamaño $k-1$ y k se diferencian en una unidad, por lo tanto, $N(0, ..., 0) - N(1, ..., 1)$ es o bien 0 o bien ± 1.

Proposición 5.12. *Toda m-sucesión satisface (G4).*

Demostración: Sea s una m-sucesión en $\mathbb{F}_2$. Por el Teorema 5.3, para $0 \leq i \leq 2^k - 1$, $S_i = (s_i, ..., s_{i+k-1})$ toma todo valor de $\mathbb{F}_2^k - \{(0, ..., 0)\}$. Sea $t < k$ y $a_i \in \mathbb{F}_2$ para $1 \leq i \leq t$, vamos a demostrar que se tiene que

$$N(a_1, ..., a_t) = \begin{cases} 2^{k-t} - 1 & \text{si } a_1 = ... = a_t = 0, \\ 2^{k-t} & \text{en otro caso} \end{cases} \tag{5.2}$$

Sea $A = (a_1, ..., a_t) \neq 0$, el número de listas de longitud k que contienen A es $(k-t+1)2^k$. Basta con ver cuántas posiciones quedan libres

$$(A, \underbrace{\_\ \_ \ ... \ \_}_{k-t}) \ , \ (\underbrace{\_}_{1}, A, \underbrace{\_\ \_ \ ... \ \_}_{k-t-1}) \ , \ (\underbrace{\_\ \_}_{2}, A, \underbrace{\_\ \_ \ ... \ \_}_{k-t-2}) \ , \ ..... \ , \ (\underbrace{\_\ \_ \ ... \ \_}_{k-t}, A),$$

Por cada posición libre tenemos 2 posibilidades. Por tanto, la lista A aparece en $(k - t + 1)2^{k-t}$ sucesiones vectoriales. Sin embargo, cada aparición de A en el periodo se está contando varias veces. Sea S_j la sucesión vectorial donde aparece la lista A en primer lugar, es decir, $S_j = (a_1, a_2, ..., a_t, s_{j+t}, s_{j+t+1}, ..., s_{j+k-1}) = (A, s_{j+t}, ..., s_{j+k-1})$.

Si $j \geq k-t+1$, entonces A también aparecerá en $S_{j-1}, S_{j-2}, ..., S_{j-(k-t+1)}$, pues $S_{j-1} = (s_{j-1}, A, s_{j+t}, ..., s_{j+k-2})$, ..., $S_{j-(k-t+1)} = (s_{j-(k-t+1)}, ..., s_{j-1}, A)$. Es decir, A se repite en $k - t + 1$ sucesiones vectoriales.

Si $j < k-t+1$, A también aparece en $k-t+1$ sucesiones vectoriales, en $S_0, S_1, ..., S_{j-1}$ y en $S_{2^k-2}, S_{2^k-3}, ..., S_{j+2^k-(k-t+1)}$. Por tanto, A aparece en cada periodo 2^{k-t} veces, es decir, $N(a_1, ..., a_t) = 2^{k-t}$.

Si en cambio, $A = (a_1, ..., a_t) = (0, ..., 0)$, como la sucesión vectorial nula no aparece, siguiendo el mismo procedimiento anterior se tiene que A aparece en $(k - t + 1)(2^{k-t} - 1)$ sucesiones vectoriales. En este caso también tenemos que cada vez que A aparece en una sucesión vectorial, se cuenta $(k-t+1)$ veces de más, por tanto, A aparece en cada periodo $2^{k-t} - 1$ veces, es decir, $N(a_1, ..., a_t) = 2^{k-t} - 1$.

Se ha demostrado que se cumple (5.2), luego, toda m-sucesión satisface el test de serie. □

5.2. La propiedad shift-and-add y la constancia de clases laterales

A parte de los postulados de Golomb, las sucesiones máximas también satisfacen otras propiedades importantes.

Teorema 5.13. *Sea s una m-sucesión, entonces existe τ, $1 \leq \tau \leq q^k - 1$, tal que $s_{iq^j+\tau} = s_{i+\tau}$ para todo $i, j \geq 0$. Esta propiedad se llama constancia de las clases laterales del grupo cíclico.*

Demostración: Por el Teorema 4.6 sabemos que $s_i = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^i)$ para algún $\beta \in \mathbb{F}_{q^k}$ y $\alpha \in \mathbb{F}_{q^k}$ raíz del polinomio característico. Como α es elemento primitivo, existe $1 \leq \tau \leq q^k - 1$ tal que $\alpha^\tau = \beta^{-1}$. Se tiene entonces

$$s_{i+\tau} = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{i+\tau}) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha^i) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha^{iq^j}) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta\alpha^{iq^j+\tau}) = s_{iq^j+\tau}$$

teniendo en cuenta que $Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha^{iq^j}) = \alpha^{iq^j} + \alpha^{iq^{j+1}} + ... + \alpha^{iq^{k-1}} + \alpha^{iq^k} + ... + \alpha^{iq^{k+j-1}} = \alpha^{iq^j} + \alpha^{iq^{j+1}} + ... + \alpha^{iq^{k-1}} + \alpha^i + ... + \alpha^{iq^{j-1}} = \alpha^i + \alpha^{iq} + ... + \alpha^{iq^{j-1}} + \alpha^{iq^j} + \alpha^{iq^{j+1}} + ... + \alpha^{iq^{k-1}} = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha^i)$ en $\mathbb{F}_{q^k}/\mathbb{F}_q$, pues α tiene orden $q^k - 1$, lo que implica que $\alpha^{q^k} = \alpha$. □

Sea s una sucesión de periodo r en $\mathbb{F}_q$, se dice que s cumple la propiedad shift-and-add si para todo $0 \leq n < r$ existe $\delta \geq 0$ tal que $s + s^n = s^\delta$, o escrito término a término, $s_i + s_{i+n} = s_{i+\delta}$ para todo $i \geq 0$. En otras palabras, s cumple la propiedad shift-and-add si y solo si el conjunto de las r sucesiones desplazadas de s junto a la sucesión constante igual a cero es cerrado bajo la suma de sucesiones término a término. El desplazamiento $\delta \geq 0$ puede tomarse $0 \leq \delta < r$ sin pérdida de generalidad, ya que $s_i = s_{i+r}$, y por tanto, si $\delta = hr + (\delta \mod r)$, se tiene $s_{i+\delta} = s_{i+(\delta \mod r)}$.

Teorema 5.14. *Toda m-sucesión satisface la propiedad shift-and-add.*

Demostración: En la demostración del test de autocorrelación del Teorema 5.11 se ha probado que, para cada $0 \leq n < q^k - 1$, $s + s^n$ es una m-sucesión con el mismo polinomio característico que s y s^n. Tal como se ha señalado tras el Teorema 5.3, como la sucesión $s + s^n$ satisface la misma regla de recurrencia, es una sucesión desplazada de s, y por tanto, existe $\delta \geq 0$ tal que para todo $i \geq 0$ se tiene $s_i + s_{i+n} = s_{i+\delta}$. □

La propiedad shift-and-add es más interesante ya que caracteriza unívocamente las m-sucesiones sobre $\mathbb{F}_p$, con p un número primo. El siguiente resultado sirve de ayuda para demostrar esta caracterización.

Lema 5.15. *Sea s una sucesión periódica sobre $\mathbb{F}_p$ de periodo r, entonces son equivalentes:*

(i) La sucesión s cumple la propiedad shift-and-add.

(ii) La sucesión s cumple la propiedad shift-and-subtract: para todo $0 \leq n < r$ existe $\delta \geq 0$ tal que $s_i - s_{i+n} = s_{i+\delta}$ para todo $i \geq 0$.

(iii) La sucesión s cumple la propiedad shift-and-add con coeficientes en $\mathbb{F}_p$: para todo $0 \leq n < r$ y para todo $\alpha, \beta \in \mathbb{F}_p$ existe $\delta \geq 0$ tal que $\alpha s_i + \beta s_{i+n} = s_{i+\delta}$ para todo $i \geq 0$.

Demostración: Suponemos que s cumple la propiedad shift-and-add con coeficientes en $\mathbb{F}_p$, entonces tomando $\alpha = 1$ y $\beta = 1$ se tiene (i), y tomando $\alpha = 1$ y $\beta = -1$ se tiene (ii).

Suponemos ahora que s cumple la propiedad shift-and-add. Claramente $ps_i = 0$ para todo $i \geq 0$, por lo que $(p-1)s_i = -s_i$ para todo $i \geq 0$. En particular, se tiene que $s_i + (p-1)s_{i+k} = s_i - s_{i+k}$. Aplicando la propiedad shift-and-add, se tiene que

$$s_i + s_{i+k} + (p-2)s_{i+k} = s_{i+\delta_1} + (p-2)s_{i+k}$$

para algún δ_1. Como no se puede volver a aplicar directamente la propiedad en la sucesión s, distinguimos casos. Si $\delta_1 \geq k$, se puede escribir $\delta_1 = k + m = k + hr + (m \mod r)$ para algún $m \geq 0$. Por otra parte, como s cumple la propiedad shift-and-add, si tomamos

$i = i + k$ se tiene que s^k también cumple la propiedad shift-and-add, es decir, para todo $0 \leq n < r$ existe $\sigma \geq 0$ tal que $s_{i+k} + s_{i+k+n} = s_{i+k+\sigma}$ para todo $i \geq 0$. Por tanto,

$$s_{i+\delta_1}+(p-2)s_{i+k} = s_{i+k+(m \mod r)}+s_{i+k}+(p-3)s_{i+k} = s_{i+k+\sigma_1}+(p-3)s_{i+k} = s_{i+\delta_2}+(p-3)s_{i+k}$$

para algún δ_2. Si $\delta_1 < k$, de manera similar se llega a $s_{i+\delta_1}+(p-2)s_{i+k} = s_{i+\delta_2}+(p-3)s_{i+k}$, descomponiendo en este caso k en función de δ_1. Siguiendo el mismo procedimiento se tiene

$$s_{i+\delta_1} + (p-2)s_{i+k} = s_{i+\delta_2} + (p-3)s_{i+k} = s_{i+\delta_3} + (p-4)s_{i+k} = ... = s_{i+\gamma}$$

para algún γ, y por tanto, $s_{i+\gamma} = s_i + (p-1)s_{i+k} = s_i - s_{i+k}$ y se tiene (ii).

Suponemos que s cumple la propiedad shift-and-subtract y seguimos un argumento similar al anterior para obtener (i). En este caso, como $-(p-1)s_i = s_i$ para todo $i \geq 0$, $s_i - (p-1)s_{i+k} = s_i + s_{i+k}$. Aplicando la propiedad shift-and-subtract, se tiene que

$$s_i - s_{i+k} - (p-2)s_{i+k} = s_{i+\delta_1} - (p-2)s_{i+k}$$

para algún δ_1. Distinguimos casos. Si $\delta_1 \geq k$, descomponiendo δ_1 y siguiendo el mismo procedimiento anterior, se llega a $s_{i+\delta_1} - (p-2)s_{i+k} = -s_{i+\delta_2} - (p-3)s_{i+k}$ para algún δ_2. Si $\delta_1 < k$, de la misma manera, $s_{i+\delta_1} - (p-2)s_{i+k} = s_{i+\delta_2} - (p-3)s_{i+k}$ para algún δ_2. Nótese que si $\delta_1 \geq k$, nos queda $-s_{i+\delta_2}$, y no se va a poder aplicar la propiedad shift-and-subtract, pues tendremos $-s_{i+\delta_2} - s_{i+k} - (p-4)s_{i+k}$. Vamos a corregir entonces el caso $\delta_1 \geq k$. Como r es el periodo de s, tenemos que

$$s_{i+\delta_1}-(p-2)s_{i+k} = s_{i+k+(m \mod r)}-s_{i+k}-(p-3)s_{i+k} = s_{i+k+(m \mod r)}-s_{i+k+r}-(p-3)s_{i+k}$$

Como $r > (m \mod r)$, podemos escribir $r = (m \mod r) + m_1$ para algún $0 < m_1 < r$, y

$$s_{i+k+(m \mod r)}-s_{i+k+(m \mod r)+m_1}-(p-3)s_{i+k} = s_{i+k+(m \mod r)+\sigma_1}-(p-3)s_{i+k} = s_{i+\delta_2}-(p-3)s_{i+k}$$

De esta forma, el término queda positivo en ambos casos y se puede seguir el mismo argumento hasta llegar a $s_{i+\delta_2} - (p-3)s_{i+k} = s_{i+\gamma}$ para algún γ. Por tanto, $s_{i+\gamma} = s_i - (p-1)s_{i+k} = s_i + s_{i+k}$ y se tiene (i).

Finalmente, suponiendo que s cumple la propiedad shift-and-add, como hemos visto, s^n también la cumple para todo $0 \leq n < r$, luego, sea $\beta \in \mathbb{F}_p$, repitiendo el procedimiento de los párrafos anteriores se tiene que $\beta s_{i+n} = s_{i+n+\sigma}$ para algún σ. Por tanto, sea $\alpha \in \mathbb{F}_p$, se llega a $\alpha s_i + \beta s_{i+n} = (\alpha-1)s_i + s_i + s_{i+n+\sigma} = (\alpha-1)s_i + s_{i+\delta_1} = s_{i+\gamma}$ para algún γ con el mismo argumento, y se tiene (iii). □

Teorema 5.16. *Toda sucesión periódica en $\mathbb{F}_p$ que satisface la propiedad shift-and-add es una m-sucesión.*

Demostración: Sea r el periodo de s, del lema anterior se deduce que el conjunto de las r sucesiones desplazadas de s, $D := \{s^\tau : 0 \leq \tau \leq r-1\}$, junto con la sucesión constante igual a cero $\varepsilon = 000...$, forman un espacio vectorial $V := \{\varepsilon\} \cup D$ sobre $\mathbb{F}_p$. Claramente es de dimensión finita, de cardinal p^n para algún n. Del Teorema 4.22 se tiene entonces que

existe un polinomio $f(x)$ mónico de grado positivo k tal que $V = S(f(x))$, es decir, s es una sucesión de recurrencia lineal con polinomio característico $f(x)$. Además, el número de elementos de V es $r+1$, pues todas las sucesiones desplazadas son distintas; con lo que $r-1 = p^n$. Como el conjunto $S(f(x))$ tiene cardinal p^k, se tiene que $r = p^k - 1$. Por tanto, $f(x)$ es primitivo, pues genera una sucesión de orden máximo, y s es una m-sucesión. □

Nótese que esta caracterización de las m-sucesiones se da únicamente en cuerpos finitos de cardinal un número primo. En el Teorema 6 de [15], Zierler clasifica las sucesiones periódicas sobre $\mathbb{F}_q$, con $q = p^m$, que cumplen la propiedad shift-and-add. Establece que una sucesión cumple la propiedad shift-and-add si y solo si es una m-sucesión. Esto es falso, como señalan Gong, Di Porto y Wolfowicz en [5]. En [1], Blackburn facilita un contraejemplo:

Ejemplo 5.17. *Sea $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ un cuerpo finito, con α raíz de x^2+x+1. Entonces, $s = 1, 0, \alpha, 1, \alpha, 1+\alpha, 1+\alpha, 1, 0, \alpha, 1, \alpha, 1+\alpha, 1+\alpha, ...$ es una sucesión de periodo 7 sobre $\mathbb{F}_4$. Se tiene que*

$$s + s^1 = 1, \alpha, 1+\alpha, 1+\alpha, 1, 0, \alpha, ... = s^3 \qquad s + s^4 = 1+\alpha, 1+\alpha, 1, 0, \alpha, 1, \alpha, ... = s^5$$

$$s + s^2 = 1+\alpha, 1, 0, \alpha, 1, \alpha, 1+\alpha, ... = s^6 \qquad s + s^5 = \alpha, 1+\alpha, 1+\alpha, 1, 0, \alpha, 1, ... = s^4$$

$$s + s^3 = 0, \alpha, 1, \alpha, 1+\alpha, 1+\alpha, 1, ... = s^1 \qquad s + s^6 = \alpha, 1, \alpha, 1+\alpha, 1+\alpha, 1, 0, ... = s^2$$

Es decir, s cumple la propiedad shift-and-add. Pero s no es m-sucesión, ya que las m-sucesiones sobre $\mathbb{F}_4$ tienen periodo $4^k - 1$ para algún $k \in \mathbb{N}$.

5.3. Correlación

La correlación es una medida de similitud entre dos sucesiones. En esta sección se estudiarán resultados de correlación sobre $\mathbb{F}_2$ para conocer mejor el comportamiento de las SLRs. Al igual que en la Definición 5.7 se definió la autocorrelación como la coincidencia de una sucesión s con su desplazada s^τ, esta noción se puede dar de manera general para dos sucesiones.

Definición 5.18. *Sean $s = s_0 s_1 s_2 ...$ y $t = t_0 t_1 t_2 ...$ sucesiones binarias, ambas de periodo r. Su correlación $C(s,t)$ se define como el número de coincidencias menos el número de no coincidencias entre s y t. Como son sucesiones periódicas de mismo periodo, basta ver el comportamiento en los r primeros términos:*

$$C(s,t) = A - D \quad con \quad A = |\{0 \le i \le r-1 : s_i = t_i\}| \quad y \quad D = |\{0 \le i \le r-1 : s_i \neq t_i\}|$$

Ejemplo 5.19. *Sean $s = 0111001...$ y $t = 0011010...$, se tiene que $A = |\{0, 2, 3, 4\}|$ y $D = |\{1, 5, 6\}|$, por tanto $C(s,t) = 1$.*

Claramente, si $s = t$ se tiene que $C(s,t) = r$, y si una es la complementaria de la otra, $C(s,t) = -r$. En cualquier caso, $-r \le C(s,t) \le r$.

Lema 5.20. *Sean s y t sucesiones binarias de periodo r. Si s tiene w_1 1's en el periodo, y t tiene w_2 1's en el periodo, entonces $C(s,t) = r - 2(w_1 + w_2) \mod 4$.*

Demostración: Definimos

$$n_{0,0} = |\{0 \le i \le r-1 : s_i = 0 = t_i\}|, \qquad n_{0,1} = |\{0 \le i \le r-1 : s_i = 0, t_i = 1\}|,$$

$$n_{1,1} = |\{0 \le i \le r-1 : s_i = 1 = t_i\}|, \qquad n_{1,0} = |\{0 \le i \le r-1 : s_i = 1, t_i = 0\}|$$

Por tanto, $C(s,t) = (n_{0,0} + n_{1,1}) - (n_{0,1} + n_{1,0})$. Como w_1 es número de 1's de s, y w_2 es el número de 1's de t, entonces

$$n_{1,0} = w_1 - n_{1,1} \qquad n_{0,1} = w_2 - n_{1,1} \qquad n_{0,0} = r - w_1 - w_2 + n_{1,1}$$

y por tanto, $C(s,t) = r - 2w_1 - 2w_2 + 4n_{1,1}$. □

La función de autocorrelación definida previamente es por tanto un caso particular de correlación, pues, sea s una sucesión y $\tau \ge 0$, $C(\tau) = C(s, s^\tau)$. Del Lema 5.20 se sigue el siguiente resultado.

Corolario 5.21. *Sea s una sucesión binaria de periodo r. Si denotamos por w_1 el número de 1's de s, entonces su función de autocorrelación es $C(\tau) = r - 4w_1 + 4n_{1,1}$, donde $n_{1,1} = |\{0 \le i \le r-1 : s_i = 1 = s_{i+\tau}\}|$.*

Gracias a esto se puede obtener el número de coincidencias de 1's y 0's entre una m-sucesión s y su desplazada s^τ.

Proposición 5.22. *Sea s una m-sucesión de orden k y sea $0 < \tau < 2^k - 1$, entonces se tiene*

$$n_{1,1} = |\{i : s_i = 1 = s_{i+\tau}\}| = 2^{k-1} - 2^{k-2} \quad y \quad n_{0,0} = |\{i : s_i = 0 = s_{i+\tau}\}| = 2^{k-1} - 2^{k-2} - 1$$

Demostración: Sea w_1 el número de 1's de s en el periodo y w_0 el número de 0's en el periodo. Del Corolario 5.21 se tiene que $C(\tau) = 2^k - 1 - 4w_1 + 4n_{1,1}$. En la demostración del Teorema 5.11 se llegó a que $w_1 - w_0 = 1$, luego, como el número de bits en el periodo es $2^k - 1$, $w_1 = 2^{k-1}$. Por el Teorema 5.11 sabemos que

$$C(\tau) = \begin{cases} 2^k - 1 & \text{si } \tau = 0, \\ -1 & \text{si } 0 < \tau < 2^k - 1 \end{cases}$$

Por tanto, se tiene $-1 = 2^k - 1 - 4 \cdot 2^{k-1} + 4n_{1,1}$ y se llega a $n_{1,1} = 2^{k-1} - 2^{k-2}$. Del Lema 5.20, $n_{0,0} = 2^k - 1 - 2w_1 + n_{1,1} = 2^{k-1} - 2^{k-2} - 1$. □

Como ya vimos por el test de autocorrelación, el número de coincidencias entre una m-sucesión y su desplazada τ posiciones no aporta información acerca del periodo de la sucesión. Es decir, si se toma una m-sucesión de orden lo suficientemente grande como palabra clave en el cifrado de Vernam, este código no podrá romperse con el método de Kasiski (manera de descifrar el código de Vigenère). Al cumplir los postulados de Golomb, y como son las sucesiones de periodo máximo, las m-sucesiones son buenas candidatas para tomar como clave en el cifrado de Vernam.

Bibliografía

[1] Blackburn, S. R. (1996). *A Note on Sequences with the Shift and Add Property. Designs, Codes and Cryptography.* Springer.

[2] Fernández-Ferreirós, P. (2019). *Apuntes de Teoría de Galois.* Universidad de Cantabria.

[3] Golomb, S. W. y Gong, G. (2005). *Signal Design for Good Correlation.* Cambridge University Press.

[4] Golomb, S. W. (revised edition 1982). *Shift Register Sequences.* Laguna Hills, Calif., Aegean Park Press.

[5] Gong G., Di Porto, A. and Wolfowicz, W. (1993). Performance testing of galois linear group sequences. In *Proceedings of SPRC '93*, pages 90–105, Rome, Italy.

[6] Goresky, M. y Klapper, A. (2012). *Algebraic Shift Register Sequences.* Cambridge University Press.

[7] Hernández, L. (2016). *La criptografía.* Los Libros de La Catarata.

[8] Jiménez, J. (2021). *Estructuras Algebraicas. Notas transitorias.* Universidad de Cantabria.

[9] Klein, A. (2013). *Stream Ciphers.* Springer London.

[10] Lidl, R. y Niederreiter, H. (1996). *Finite Fields.* Cambridge University Press.

[11] McEliece, R. J. (1996). *Finite Fields for Computer Scientists and Engineers.* Springer New York.

[12] Mullen, G. L. y Shiue, P. J. S. (1993). *Finite fields, coding theory, and advances in communications and computing.* M. Dekker.

[13] Sadornil, D. (2022). *Apuntes de Matemática Discreta.* Universidad de Cantabria.

[14] Wagstaff, S. S. (2019). *Cryptanalysis of Number Theoretic Ciphers.* CRC Press.

[15] Zierler, N. (1959). Linear recurring sequences. *Journal of the Society for Industrial and Applied Mathematics.*