FACULTAD DE CIENCIAS

Sucesiones de recurrencia sobre cuerpos finitos y sus aplicaciones

Cristina Lozano Cuevas

Tutor: Félix Delgado de la Mata

Universidad de Valladolid

TRABAJO DE FIN DE GRADO
Grado en Matemáticas
Curso 2013-2014

Quiero agradecer a Félix por haberme propuesto hacer este trabajo que tanto me ha gustado y por el apoyo que me ha brindado a lo largo de estos meses.

Índice general

1. Preliminares **13**
1.1. Estructura de los cuerpo finitos 13
1.2. Las series formales 16

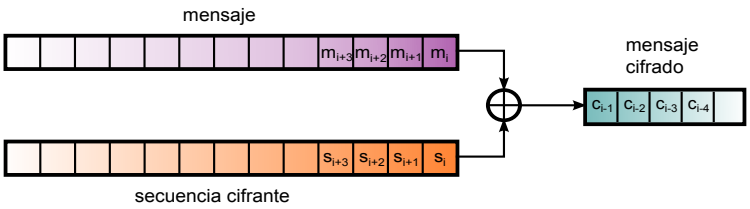
2. Sucesiones de recurrencia lineal **19**
2.1. Definiciones, periodo y sus propiedades 19
2.2. Matriz generadora 23
2.3. Sucesiones de impulso-respuesta 27
2.4. Polinomio característico 30
2.5. Funciones generatrices 32

3. Optimización de los LFSR. Complejidad lineal **37**
3.1. Orden del polinomio característico 38
3.2. Polinomios primitivos 43
3.3. Polinomio mínimo 45
3.4. El algoritmo de Berlekamp-Massey 50

4. Combinadores de LFSR. Aplicaciones **61**
4.1. Combinadores lineales 62
4.2. Combinadores producto 68
4.3. Combinadores no lineales en la práctica 72
4.4. Cadenas pseudoaleatorias de bits 78
4.5. Algunas aplicaciones 84

Introducción

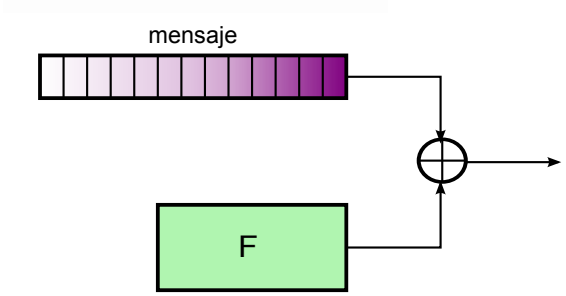
La motivación de utilizar las sucesiones de recurrencia lineal como secuencias cifrantes nace del cifrado de Vernam. En 1917 G. S. Vernam, un ingeniero de Estados Unidos ideó un procedimiento de cifrado de sustitución totalmente diferente a los que se habían utilizado hasta entonces. Para empezar el alfabeto que se emplea está formado únicamente por ceros y unos. Esto se debe a que el mensaje en claro a cifrar estaba escrito en código Baodot (procesador del código ASCII)sobre una cinta de papel perforada. Entonces el uno representaba un agujero y el cero ausencia de este. Después se hace uso de una clave secreta puesta en común entre el emisor y el receptor. Esta llave es de un solo uso por eso este procedimiento comenzó llamándose OTP (One Time Pad). Esto supuso un cambio radical respecto del tratamiento de llaves anterior ya que antes, en el momento en el que emisor y el receptor disponían de una llave, no se solía cambiar. Además la llave es una secuencia totalmente aleatoria tomando valores en el alfabeto bina rio y, al menos, con la misma longitud que el mensaje en claro que se iba a cifrar. Totalmente aleatoria significa que si nos faltara una pequeña parte de la sucesión, no podríamos predecir los valores que faltan a no ser que los supiéramos de antemano.
Una vez que se dispone de la llave, la función con la que se cifra es la operación lógica " O exclusiva" o disyunción exclusiva (XOR). Matemáticamente, esta función u operación se traduce en la suma módulo 2 y se denota por $\bigoplus$. Si m es un bit del mensaje y s uno de la llave y obtenemos el bit cifrado c mediante la operación XOR:



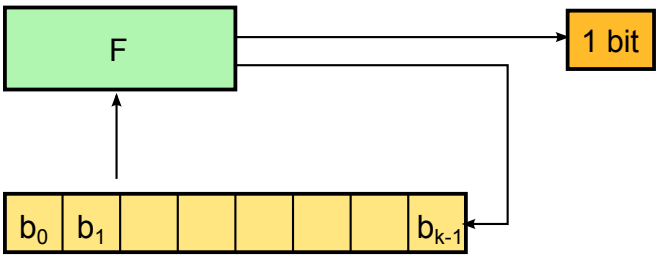
El cifrado consiste simplemente en: si en nuestra llave tenemos 0 dejamos el correspondiente bit como está; si por el contrario tenemos 1, ponemos su complementario. Puesto que estamos empleando el alfabeto binario la operación cifrado es la misma que la de descifrado. A este tipo de cifrados,

se les llama “cifrado involutivo”.
El cifrado de Vernam es un procedimiento incondicionalmente seguro ya que cumple las condiciones del secreto perfecto de Shannon. Es el único que tiene secreto perfecto, ya que es el único en el que el texto cifrado no proporciona ninguna información sobre el mensaje original.
Si tenemos garantías de que este tipo de cifrado es totalmente seguro ¿por qué no lo utilizamos? Uno de los inconvenientes que tiene es que para cada bit del mensaje en claro se necesita uno de la llave para cifrar. Es decir, nuestra llave va a tener por lo menos la misma longitud que el mensaje que vamos a cifrar y por tanto es igualmente complicado transmitir o concertar la clave que hacer lo propio con el mensaje en claro.

Un problema adicional es cómo se puede conseguir una sucesión perfectamente aleatoria y de cualquier longitud. Idílicamente nos gustaría disponer de un dispositivo con una función F capaz de generar bits aleatorios y mediante el cual, después pudiésemos recuperar la secuencia de bits aleatorios. De esta forma el cifrado quedaría del siguiente modo:

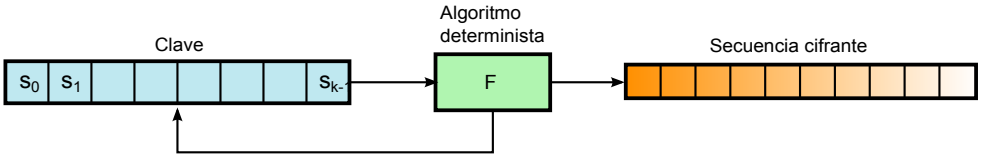


Pero claro, si tenemos un dispositivo que genere bits aleatorios, el problema es cómo los recuperamos después para el descifrado. No los podemos guardar ni transmitir ya que eso sería un blanco fácil para el enemigo.
Como queremos poder recuperar la cadena de bits, el siguiente paso es utilizar un dispositivo que implemente una función $F : \mathbb{F}_2^k \to \mathbb{F}_2$ que genere bits (que jugarán el papel de bits aleatorios) a partir de unos estados iniciales. La primera entrada $(b_0, b_1, \ldots b_{k-1}) \in \mathbb{F}_2^k$ es la llave, el primer bit de salida $F(b_0, \ldots, b_{k-1})$ retroalimenta el vector de entrada para obtener un nuevo bit y así sucesivamente.



Ahora bien, estamos trabajando en un cuerpo finito y cada nuevo bit se obtiene a partir de un número finito de elementos de nuestro cuerpo; por

lo que forzosamente la cadena que obtenemos al final va a ser periódica. Es decir, llega un momento en el que el vector de entrada de la función F $(b_0, b_1, \dots b_{k-1})$ se repite. En consecuencia todos los bits de salida a partir de ese momento se repiten y el proceso da lugar a sucesiones periódicas.
Por eso las sucesiones así generadas se denominan pseudoaleatorias, ya que no pueden ser realmente aleatorias en ningún caso. Un generador pseudoaleatorio es un algoritmo determinístico que a partir de una clave relativamente corta que conocen el emisor y el receptor, se obtiene una sucesión con la longitud que deseemos. A esta sucesión se la llama *secuencia cifrante*. En la actualidad la clave corta consta de 128 a 256 bits. Cuando conseguimos que el generador pseudoaleatorio esté bien diseñado se obtienen secuencias con un nivel de seguridad bastante alto. Esta variante del cifrado de Vernam es lo que se conoce por *cifrado en flujo*.



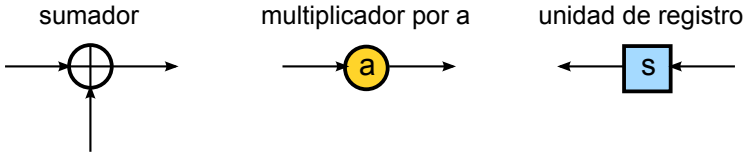
En la práctica se trabaja en código binario o $\mathbb{F}_2$, pero en realidad basta con que el cuerpo sea finito así que los resultados los expondremos sobre $\mathbb{F}_q$ para que sea lo más general posible.

Las funciones F más sencillas desde el punto de vista matemático que podemos utilizar son las funciones lineales. A las secuencias cifrantes que se producen a partir de ellas se las llama sucesiones de recurrencia lineal. Estas están determinadas a partir de una relación (de recurrencia) (**algortimo determinista**) y de una serie de elementos iniciales (**llave**).

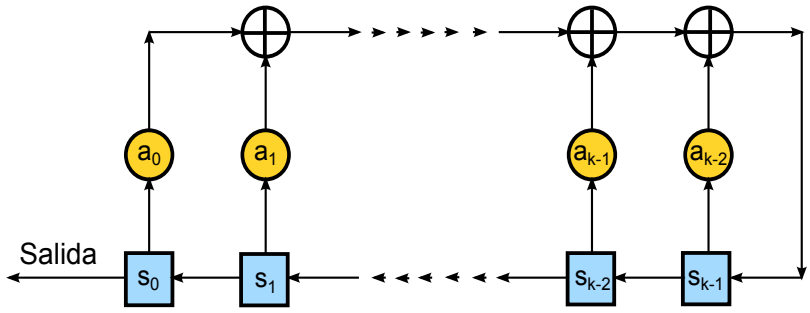
Supongamos que y que $s_0, s_1, \dots, s_{k-1}$ es la clave o llave y que fijamos elementos $a_0, a_1, \dots a_{k-1} \in \mathbb{F}_q$. A partir de estos datos se generan sucesivamente $\{s_n\}_{n=0}^{\infty}$ elementos de $\mathbb{F}_2$ de manera que si $n \geq 0$ el elemento s_{n+k} está definido por la relación de recurrencia lineal:

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n \ .$$

La generación de la sucesión (de recurrencia lineal) $\{s_n\}$ se implementa electrónicamente mediante un circuito que recibe el nombre genérico de *LFSR: Linear Feed-Back Shift Register* o k-LFSR. Las operaciones elctrónicas básicas que hace son:



Y el LFSR genérico que respnde a la relación de recurrencia que hemos descrito es:



En los cuadrados ponemos los términos de la sucesión que intervienen en la formación del siguiente término (en nuestro caso k). En un tic o impulso, los s_j que están en los cuadrados se multiplican por los a_i de los círculos y se suman todos los producto al pasar por el operador $\bigoplus$. Si alguno de los a_i fuera nulo, directamente no ponemos nada entre el registro y el sumador. Finalmente, el resultado sale por la salida y el resto de s_j avanzan una posición.

En el esquema anterior conviene diferenciar claramente el LFSR propiamente dicho (que depende de $a_0, a_1, \ldots, a_{k-1}$) del estado inicial (llave) $s_0, s_1, \ldots, s_{k-1}$ que se podrá fijar a conveniencia para un LFSR dado. Desde el punto de vista matemático el circuito LFSR (función F) se traduce en fijar una matriz cuadrada de tamaño k o un polinomio de grado k. El estado inicial (llave) es un elemento del espacio vectorial $\mathbb{F}_q^k$ (aunque en la práctica se utilizan sobre todo sucesiones binarias, no hay dificultades conceptuales para usar un cuerpo finito arbitrario con q elementos). Asímismo, la sucesión $\{s_n\}$ es conveniente representarla mediante la serie formal $\sum s_n x^n$.

Puesto que deseamos sucesiones lo más parecidas a una sucesión aleatoria, buscaremos estudiar las propiedades que han de cumplir la matriz (o equivalentemente el polinomio) para obtener periodos muy grandes. También estudiaremos, cuando el dispositivo está fijo, los periodos que resultan de las diferentes elecciones para el estado inicial. Una cuestión clave es caracterizar todos los polinomios (o circuitos LFSR o matrices) que dan lugar a la misma sucesión de salida. De todos ellos habrá uno con una longitud k mínima. Este entero k se conoce como la complejidad lineal de la sucesión y es el que realmente importa, no sólo en cuanto a la economía del circuito, sino en la fortaleza criptográfica del sistema tal y como nos muestra el algoritmo de Berlekamp-Massey.

Para terminar, describiremos una serie de combinadores lineales y no lineales que permitirán construir un sucesiones con periodos grandes a partir

de sucesiones con periodos más pequeños. Por lo tanto mediante estos combinadores podremos utilizar circuitos relativamente pequeños para generar sucesiones con una alta complejidad lineal. Además del sustrato matemático de los combinadores lineales y producto describiremos algunos combinadores utilizados de forma sistemática en la práctica.

Finalmente, describiremos algunos tests que permiten "certificar" el ni vel de aproximación de nuestras secuencias cifrantes a sucesiones realmente aleatorias y algunas aplicaciones de las sucesiones de recurrencia en el mundo de las telecomunicaciones.

Capítulo 1

Preliminares

Antes de nada, vamos a exponer algunos resultados y fijar algunas notaciones que se van a utilizar a lo largo del trabajo para aquellos que no estén familiarizados con estos conceptos. Será lo más breve posible y con apenas demostraciones. Si el lector está interesado con alguna en particular o simplemente profundizar más puede consultar [**POL**], [**BOU**], [**LIDL**] .

1.1. Estructura de los cuerpo finitos

Para comenzar, lo primero que tenemos que revisar es la estructura y el manejo de los cuerpos finitos ya que en sus características especiales se basan todos los resultados que veremos a lo largo del trabajo. Como el propio nombre indica, un cuerpo finito es un cuerpo cuyo cardinal es un número finito; pero como veremos ahora, este número, no es un número cualquiera ya que ha de ser una potencia de un número primo p. Una vez que fijamos su cardinal $q = p^n$, el cuerpo está unívocamente determinado salvo isomorfismo; puesto que es un cuerpo de descomposición del polinomio $x^q - x$ sobre el cuerpo primo $\mathbb{Z}_p$. Las propiedades de los cuerpo primos ya fueron enunciadas por matemáticos como Fermat, Euler, Lagrange, Legendre y Gauss aunque las establecieron para resolver y caracterizar las congruencias mód p no por los cuerpos en sí. No sería hasta años más tarde cuando el concepto de çuerpo finito.ªpareciera por primera vez en el artículo de Galois, *Sur la théorie des nombres*, del 1830 por ello a los cuerpos finitos también hay quien los denomina cuerpos de Galois. En este, también se trataba de resolver congruencias mód p pero en una extensión del cuerpo primo; lo que posteriormente se convertiría en resolver ecuaciones sobre cuerpo finitos.

Si F un cuerpo finito que contiene a un subcuerpo K con q elementos, entones F es un K espacio vectorial de dimensión finita, m, por tanto F tiene q^m elementos (el entero m es también el grado de la extensión F/K). En particular, F tiene p^n elementos, siendo p la característica de F ya que $\mathbb{Z}_p$ es un subcuerpo de F.

Si F es un cuerpo finito con q elementos, entonces para todo $a \in F \setminus \{0\}$ se tiene que $a^{q-1} = 1$. Por tanto, para todo $a \in F$ se tiene que $a^q = a$. El resultado siguiente va todavía un poco más allá:

Teorema 1.1. *Sea F un cuerpo finito con q elementos y sea $K \subset F$ un subcuerpo de F. Entonces el polinomio $x^q - x \in K[x]$ factoriza en $F[x]$. Es decir:*

$$x^q - x = \prod_{a \in F} (x - a),$$

y F es el cuerpo de descomposición de $x^q - x$ sobre K.

A partir de este resultado ya podemos enunciar el principal teorema que caracteriza a los cuerpos finitos.

Teorema 1.2 (**Existencia y unicidad de un cuerpo finito**)**.** *Para todo número p primo y para todo $m \in \mathbb{N}$, existe un único (salvo isomorfismo) cuerpo con $q = p^m$ elementos. De hecho, p es la característica de F.*

Notación. En lo que sigue, cuando hablemos de un cuerpo finito con q elementos, lo denotaremos por $\mathbb{F}_q$.

Una vez que tenemos un cuerpo finito, tenemos caracterizados todos los subcuerpos con el siguiente teorema.

Teorema 1.3 (**Subcuerpos de un cuerpo finito**)**.** *Sea $\mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos. Si K es un subcuerpo de $\mathbb{F}_q$, entonces el cardinal de K es p^m donde m es un divisor de n. Recíprocamente, si m es un divisor de n, entonces existe un único, salvo isomorfismo, subcuerpo de $\mathbb{F}_q$ de cardinal p^m.*

Es decir, para cada divisor m de n tenemos un subcuerpo que es justamente el cuerpo de descomposición de $x^{p^m} - x \in \mathbb{F}_q[x]$.

Con estos resultados ya tenemos caracterizados, en general, los cuerpos finitos; ahora necesitamos saber como se construyen y la estructura algebraica que llevan consigo.

A partir de los resultados anteriores es inmediato comprobar algunas propiedades útiles.

Proposición 1.4. *Sea $f \in \mathbb{F}_q$ irreducible de grado m, entonces*

1. *El cuerpo $\mathbb{F}_{q^m}$ es el cuerpo de descomposición de f sobre $\mathbb{F}_q$.*
2. *El polinomio f divide a $x^{p^n} - x$ si y sólo si m divide a n.*
3. *Todas las raíces de f son simples.*

Un resultado importante en esta memoria es:

Proposición 1.5. *El grupo multiplicativo $\mathbb{F}_q^*$ de un cuerpo finito $\mathbb{F}_q$ es cíclico de orden $q-1$. Es decir, existe un elemento $\alpha \in \mathbb{F}_q^*$ tal que $\mathbb{F}_q^* =< \alpha >$.*

Un elemento α que genera el grupo multiplicativo se dice que es un elemento primitivo de $\mathbb{F}_q^*$.

Construcción de los cuerpo finitos

Vemos como se construyen los cuerpos finitos. Sea p un número primo y n un entero positivo. Queremos construir un cuerpo finito con p^n elementos. Para ello tomamos un polinomio $f \in \mathbb{F}_p[x]$ de grado n irreducible. Ahora hacemos el cociente $\mathbb{F}_p[x]/(f(x))$. Este cociente es un cuerpo ya que $\mathbb{F}_p[x]$ es un dominio de ideales principales y el polinomio f es irreducible. Tenemos entonces,

$$\begin{aligned}
\mathbb{F}_q &= \frac{\mathbb{F}_p[x]}{f(x)} = \{g(x) + (f(x))\} \\
&= \{\overline{a_0 + ... + a_{n-1}x^{n-1}} \text{ con } a_i \in \mathbb{F}_p\} \\
&= \{a_0 + a_1\overline{x} + ... + a_{n-1}\overline{x}^{n-1} \text{ con } a_i \in \mathbb{F}_p\}, \\
&= \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \text{ con } a_i \in \mathbb{F}_p\},
\end{aligned}$$

dónde estamos denotando $\alpha := \overline{x} = x + (f(x))$ la clase de x. Por tanto, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $\mathbb{F}_p[x]/(f(x))$ sobre $\mathbb{F}_p$. Evidentemente el cuerpo $\mathbb{F}_p[x]/(f(x))$ es un cuerpo con p^n elementos.

La experesión de cualquier elemento del cuerpo en función de la base fijada es muy adecuada para manejar la operación suma, aunque la multiplicación es algo más compleja. En el caso en que además el elemento α sea primitivo podemos describir nuestro cuerpo del siguiente modo:

$$\mathbb{F}_q = \mathbb{F}_q * \cup\{0\} = \{\alpha,\ \alpha^2,\ ...,\ \alpha^{q-2},\ \alpha^{p^n-1} = 1\} \cup \{0\}.$$

Evidentemente esta descripción es muy adecuada para expresar la multiplicación.

Observación 1.6. Hemos de tener cuidado ya que auque el polinomio sea irreducible la clase α puede no ser un elemento primitivo.

Vamos a hacer un ejemplo sencillo de como se contruye un cuerpo finito.

Ejemplo 1.7. Supongamos que tomamos el cuerpo primo $\mathbb{F}_3$ y queremos construir un cuerpo finito con 9 elementos; consideramos el polinomio $x^2 + 1 \in \mathbb{F}_3$ irreducible. El elemento α que tomamos es una raíz del polinomio f por lo que satisface $\alpha^2 = -1 = 2$. Hacemos el cociente, y nuestro cuerpo finito es $\mathbb{F}_9 = \{0,\ 1,\ 2,\ \alpha,\ 1+\alpha,\ 2+\alpha,\ 2\alpha,\ 1+2\alpha,\ 2+2\alpha\}$. Observamos que $\{1,\ \alpha\}$ forman una base de la extensión $\mathbb{F}_9/\mathbb{F}_3$. En este caso, α no es un elemento primitivo ya que como $\alpha^4 = 1$ no puede generar el grupo multiplicativo.

Si tomamos ahora en $\mathbb{F}_2$ el polinomio $x^3 + x + 1 \in \mathbb{F}_2[x]$, y α satisfaciendo $\alpha^3 = \alpha + 1$, tenemos que

$$\mathbb{F}_8 = \{0, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1, \alpha^7 = 1\},$$

en este caso α si que es un elemento primitivo ya que como acabamos de ver, genera el grupo multiplicativo.

Grupo de Galois. Sea $q = p^n$ y $\mathbb{F}_q$ el cuerpo finito con q elementos. La aplicación $\varphi(x) = x^p$ es un $\mathbb{F}_p$-automorfismo de $\mathbb{F}_q$ (llamada el automorfismo de Frobenius). Nótese que $\varphi^n(x) = x$ para todo $x \in \mathbb{F}_q$. Por tanto φ tiene orden n. Además, si m divide a n se tiene que $\varphi^m(x) = x$ si y sólo si $x \in \mathbb{F}_{p^m}$. Tenemos entonces el siguiente:

Teorema 1.8. *La extensión $\mathbb{F}_p \subset \mathbb{F}_q$ es de Galois y su grupo de Galois es cíclico de orden n generado por el automorfismo de Frobenius. De la misma forma, para un divisor m de n, la extensión $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ es de Galois de grado n/m y su grupo de Galois es cíclico de orden n/m generado por φ^m.*

Como consecuencia, si $f \in \mathbb{F}_q$ es irreducible de grado m y $\alpha \in \mathbb{F}_{q^m}$ es una raíz de f tendremos que las raíces de f son los elementos $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$. En general, dado $\beta \in \mathbb{F}_{q^m}$ los conjugados de β respecto del grupo de Galois G de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ son los elementos $G\beta = \{\beta, \beta^q, \ldots, \beta^{q^{m-1}}\}$.

Nota 1.9. Este resultado fue establecido por Galois en el ya citado, *Sur la théorie des nombres* del año 1830 y lo que nos dice es, que cualquier extensión finita de un cuerpo finito $\mathbb{F}_q$, es una extensión normal; es decir, si un polinomio tiene una raíz en la extensión, entonces tiene todas. De hecho, el conjunto $\{\alpha, \alpha^q \ldots, \alpha^{q^{m-1}}\}$ forma una base de $\mathbb{F}_{q^m}$ y se la llama, precisamente, base normal.

Observación 1.10. Los conjugados de un elemento $\beta \in \mathbb{F}_{q^m}$ respecto de $\mathbb{F}_q$ son todos distintos si, y sólo si el polinomio $f = \prod_{i=0}^{m-1}(x - \beta^{q^i})$ es irreducible. Es decir, f es el polinomio mínimo de α sobre $\mathbb{F}_q$.

1.2. Las series formales

En esta sección veremos algunos resultados generales sobre las series formales para utilizarlos después cuando hablemos de las funciones generatrices.

Sea A un anillo. El conjunto de sucesiones $\mathbf{b} = \{b_n\}_{n=0}^{\infty}$ de elementos de A tiene una estructura natural de anillo. La sucesión suma de $\mathbf{b}$ y $\mathbf{a}$ es la sucesión $\mathbf{a}+\mathbf{b} = \{b_n+a_n\}_{n=0}^{\infty}$. El producto es la sucesión $\{c_n\}_{n=0}^{\infty}$ definido por el producto de convolución: $c_n = a_n b_0 + \cdots + a_0 b_n$. Identificando el elemento a de A con la sucesión $\{a, 0, \ldots, \}$ y denotando por x la sucesión $\{0, 1, 0 \ldots\}$,

la analogía con los polinomios (que se idenifican con las sucesiones que sólo tienen un número finito de elementos no nulos) sugiere que una forma natural de expresar la sucesión $\mathbf{b}$ es mediante la expresión formal:

$$\mathbf{b} \equiv b(x) = b_0 + b_1 x + b_2 x^2 + \cdots = \sum_{n=0}^{\infty} b_n x^n,$$

con $b_n \in A$ para todo $n \in \mathbb{N}$.

El anillo de sucesiones de elementos de A con estas operaciones se llama el anillo de series formales con coeficientes en A y se denota por $A[[x]]$. Nótese que en estos términos el producto de $a(x)$ y $b(x)$ se expresa del siguiente modo:

$$b(x)a(x) = \sum_{n=0}^{\infty} d_n x^n,$$

donde $d_n = \sum_{k=0}^{n} b_k a_{n-k}$, para $n = 0, 1, \ldots$.

Si A es un dominio de integridad (en particular si A es un cuerpo) entonces $A[[x]]$ es también un dominio. En este caso la serie $a(x) = \sum_{n=0}^{\infty} a_n x^n$ es una unidad (i.e. tiene inverso multiplicativo) siempre que el término constante a_0 sea no nulo.

Teorema 1.11. *La serie formal $a(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{F}_q[[x]]$ tienen inverso multiplicativo si, y sólo si, $a_0 \neq 0$.*

Demostración. Si nuestra serie tiene inverso $b(x)$, por como hemos definido los coeficientes de la serie producto, tenemos que $c_0 = a_0 b_0 = 1$, y como $\mathbb{F}_q$ es un cuerpo, en particular un dominio de integridad, $a_0 \neq 0$.
El recíproco lo vamos a demostrar de forma constructiva, es decir, vamos a dar un método explícito de como calcular el inverso de nuestra serie. Sea $a(x) \in \mathbb{F}_q[[x]]$ una serie con $a_0 \neq 0$. Tomamos $b(x) \in \mathbb{F}_q[[x]]$ una serie cualquiera. Lo que vamos a hacer es imponer que el producto $c(x) = a(x)b(x) = 1$ y que podemos encontrar los coeficientes de b para que ellos ocurra. El coeficiente n-ésimo de este producto es

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0,$$

el término constante, $n = 0$, es $c_0 = a_0 b_0 = 1$ entonces como $a_0 \neq 0$ por hipótesis, $b_0 = a_0^{-1}$. Para $n = 1$, tenemos $0 = c_1 = a_1 b_0 + a_0 b_1$, entonces tenemos b_1 determinado por a_0, a_1 y b_0 que son todos conocidos. Iteramos este proceso, y tenemos que para el térmno n-ésimo $0 = c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0$, b_n lo podemos determinar en función de los anteriores dado que $a_0 \neq 0$, del siguiente modo

$$b_n = (-a_1 b_{n-1} - \cdots - a_{n-1} b_1 - a_n b_0) a_0^{-1},$$

luego la inversa $b(x)$, si que existe ya que es la que tiene como coeficientes los que acabamos de construir. □

Capítulo 2

Sucesiones de recurrencia lineal

En este capítulo presentaremos los resultados matemáticos de las sucesiones de recurrencia lineal que nos servirán de herramienta para las aplicaciones que veremos en el último. Además también comentaremos, en cada caso, el significado de estos resultados para los dispositivos electrónicos LFSR.

2.1. Definiciones, periodo y sus propiedades

Definición 2.1. Sea k un entero positivo. Una sucesión $\{s_n\}_{n=0}^{\infty}$, $s_n \in \mathbb{F}_q$ para $n \geqslant 0$, es una sucesión de recurrencia lineal no homogénea de orden k, si existen $a, a_0, ..., a_{k-1} \in \mathbb{F}_q$ tales que:

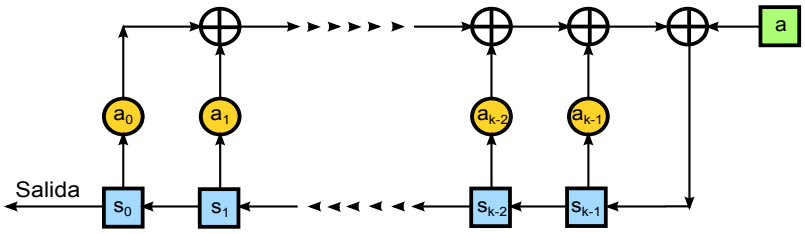
$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n + a; \quad n \in \mathbb{N}, \tag{2.1}$$

A los k primeros términos, $(s_0, s_1, ..., s_{k-1})$, se les denomina valores iniciales y al vector que forman, vector de estados iniciales. Fijada la relación de recurrencia, el vector de estados iniciales determina de forma única el resto de términos de la sucesión. En general, al vector $\mathbf{s}_m = (s_m, s_{m+1}, ..., s_{m+k-1})$, le llamaremos vector m-ésimo de estados.
Decimos que la sucesión es homogénea si $a = 0$ y expresamos su relación de recurrencia por

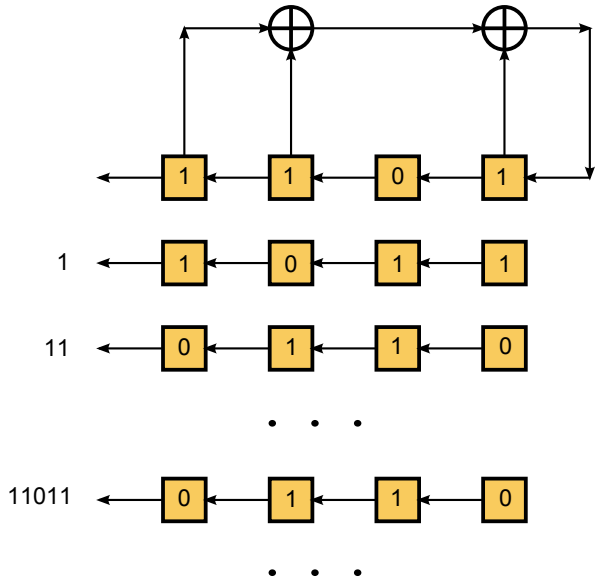
$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n; \quad n \in \mathbb{N}. \tag{2.2}$$

Observación 2.2. Es importante comprender que cuando demos una sucesión de recurrencia lineal tenemos que decir dos cosas: la relación de recurrencia y el vector de estados iniciales.

> Los coeficientes de la relación de recurrencia de una sucesión van a jugar el papel de los parámetros de nuestro dispositivo electrónico. Con ellos y con el vector de estados iniciales tenemos determinado de forma única el circuito.



Por ejemplo si nos dieran la sucesión de recurrencia lineal dada por la relación de recurrencia $s_{n+4} = s_{n+3} + s_{n+1} + s_n$ y con vector de estados iniciales $(1, 1, 0, 1)$, el LFSR que la implementa es:



Definición 2.3. Sea S un conjunto no vacío cualquiera y $\{s_n\}_{n=0}^{\infty}$ una sucesión de elementos de S. Si existen enteros $r > 0$ y $n_0 \geq 0$ tales que $s_{n+r} = s_n$, para todo $n \geq n_0$, entonces decimos que la sucesión es finalmente periódica. El entero r es el periodo de la sucesión.
Al periodo más pequeño, le llamamos periodo mínimo de la sucesión y al menor n_0 que verifica la igualdad, preperiodo. Éste depende del periodo r.
Equivalentemente, también podemos decir que $\{s_n\}_{n=0}^{\infty}$ es una sucesión finalmente periódica, si existen enteros $r > 0$ y $n_0 \geq 0$ tales que $\mathbf{s}_{n+r} = \mathbf{s}_n$ para $n \geqslant n_0$

Lema 2.4. *Todo periodo de una sucesión finalmente periódica es divisible por el periodo mínimo.*

Demostración. Sea r un periodo cualquiera de $\{s_n\}_{n=0}^{\infty}$ y sea r_1 el periodo mínimo. Tenemos

$$s_{n+r} = s_n \quad \forall n \geq n_0 \quad y \quad s_{n+r_1} = s_n \quad \forall n \geq n_1$$

para ciertos enteros positivos n_0, n_1.
Supongamos que $r_1 \nmid r$. Entonces, $r = mr_1 + t$ con $0 < t < r_1$ y $m \geqslant 1$. Entonces para todo $n \geqslant \text{máx}\{n_0, n_1\}$ tenemos

$$s_n = s_{n+r} = s_{n+mr_1+t} = s_{n+(m-1)r_1+t} = \cdots = s_{n+t}.$$

Por tanto $t < r_1$ también es periodo de la sucesión, en contra de que r_1 era el periodo mínimo. □

Definición 2.5. Si $\{s_n\}_{n=0}^{\infty}$ es una sucesión finalmente periódica , con periodo mínimo r y preperiodo 0, entonces se dice que es periódica. Es decir:

$$s_{n+r} = s_n \quad \forall n = 0, 1, ...$$

Lema 2.6. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión finalmente periódica. Entonces es periódica si, y sólo si, existe $r > 0$ tal que $s_{n+r} = s_n \quad \forall n = 0, 1, ...$*

Demostración. $\Longrightarrow$ Obvio. Es la definición.

$\Longleftarrow$ Dada la hipótesis, la sucesión es finalmente periódica con periodo mínimo r_1. Entonces, sabemos que para un cierto n_0, $s_{n+r_1} = s_n \quad \forall n \geqslant n_0$. Sea n un entero positivo arbitrario y tomamos $m \geqslant n_0$, tal que $m - n$ sea múltiplo de r. Entonces $s_{n+r_1} = s_{m+r_1} = s_m = s_n$. Por tanto $s_{n+r_1} = s_n \quad \forall n \geqslant 0$ y la sucesión es periódica. □

Ya tenemos un criterio para saber si una sucesión es periódica o no. Sin embargo nosotros estamos tratando las sucesiones de recurrencia lineal y el resultado siguiente nos dice que toda sucesión de recurrencia lineal es finalmente periódica.

Teorema 2.7. *: Sea $\mathbb{F}_q$ un cuerpo finito y k un entero positivo. Entonces toda sucesión de recurrencia lineal de orden k en $\mathbb{F}_q$ es finalmente periódica. Si r es su periodo mínimo se tiene que: $r \leqslant q^k$ si es no homogénea y $r \leqslant q^k - 1$ en el caso en sea homogénea.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal de orden k que satisface la relación (1.1). El $\mathbb{F}_q$-espacio vectorial de estados, $\mathbb{F}_q^k$, tiene q^k elementos. Es decir, hay exactamente q^k k-uplas distintas de elementos de $\mathbb{F}_q$.
Consideramos los vectores de estados $\mathbf{s}_m$ para $0 \leqslant m \leqslant q^k$ dados por la sucesión $\{s_n\}_{n=0}^{\infty}$ donde el primero es el vector de estados iniciales. Puesto que tenemos $q^k + 1$ vectores de estados y sólo teníamos q^k distintos,existen ciertos $0 \leqslant i < j < q^k$ tales que $\mathbf{s}_i = \mathbf{s}_j$. Puesto que $\mathbf{s}_{m+1}$ depende sólo de $\mathbf{s}_m$ y de $a_0, a_1, \ldots a_{k-1}$ es evidente que $\mathbf{s}_{i+k} = \mathbf{s}_{j+k}$ para todo $k \geqslant 0$.

Entonces si probamos que $\mathbf{s}_{n+j-i} = \mathbf{s}_n$, para todo $n \geqslant i$ habremos terminado ya esta esta es la definición de finalmente periódica. Ahora bien, si ponemos $n = l + i$ con $l \geqslant 0$, tenemos

$$\mathbf{s}_{n+j-i} = \mathbf{s}_{l+j} = \mathbf{s}_{l+i} = \mathbf{s}_n.$$

Con esta igualdad que acabamos de probar ya podemos decir que el periodo mínimo de la sucesión es

$$r \leqslant j - i \leqslant q^k.$$

En el caso en que la sucesión sea homogénea ($a = 0$) tenemos que quitar como posible estado inicial el vector idénticamente nulo ya que nos daría la sucesión cero. Por lo tanto tenemos $q^k - 1$ vectores posibles distintos de cero y con una demostración idéntica al caso no homogéneo, llegamos a que

$$r \leqslant j - i \leqslant q^k - 1.$$

□

Nota 2.8. Como veremos mas adelante, esta cota se alcanza cuando la relación de recurrencia lineal verifica una propiedad concreta.

> Que las sucesiones de recurrencia lineal sean periódicas no debería de sorprendernos ya que las secuencias cifrantes son sucesiones de elementos de un cuerpo finito y se obtienen en cada etapa mediante un procedimiento determinista a partir de una entrada de longitud k. Pese a eso, estamos tratando de fabricar sucesiones pseudoaleatorias, por lo que cuando mayor sea el periodo mayor será la seguridad de cifrado de nuestra secuencia cifrante. De hecho por lo menos el periodo debería de tener la misma longitud que el texto que vayamos a cifrar si pensamos en un uso criptográfico.

Proposición 2.9. *: El periodo mínimo de una sucesión de recurrencia lineal homogénea de orden uno, divide a $q - 1$.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal y supongamos que existe $a \in \mathbb{F}_q$ tal que $s_{n+1} = as_n$ para todo $n \geqslant 0$. Si $s_0 = 0$, la sucesión es $s_n = 0$ para todo $n \geqslant 0$ y el periodo es 1. Supongamos $s_0 \neq 0$. Tendremos que para todo $n \geqslant 0$

$$s_{n+r} = s_n = as_{n-1} = a^2 s_{n-2} = \cdots = a^n s_0.$$

Por tanto la condición $s_{n+r} = s_n$ para todo $n \geqslant n_0$ hace que $a^{n+r}s_0 = a^n s_0$ para todo $n \geqslant n_0$. Dado que $s_0 \neq 0$, se tiene $a^{n+r}s_0 = a^n s_0$ si, y sólo si, $a^n(1 - a^r) = 0$, es decir $a^r = 1$. Como consecuencia r es el periodo mínimo si, y sólo si, $r = ord(a)$. Por lo que $r \mid q - 1$. □

Nota 2.10. Si el orden de la sucesión es mayor o igual que dos, el resultado anterior no tiene porqué ser cierto como ilustra el ejemplo siguiente:

Ejemplo 2.11. Basta tomar la sucesión de recurrencia lineal de orden 2 $\{s_n\}_{n=0}^{\infty}$ dada por la relación de recurrencia $s_{n+2} = s_n$ para $n = 0, 1, \ldots$ y el vector de estados iniciales $(0, 1)$; ya que tenemos la sucesión $0, 1, 0, 1, 0, 1, 0, 1 \ldots$, que tiene periodo 2, y sin embargo, $q^k - 1 = 3$.

Por otra parte, cuando las sucesiones tengan $a_0 \neq 0$ van a ser periódicas lo cual nos va a ayudar para probar resultados que veremos posteriormente. En realidad podemos suponer siempre $a_0 \neq 0$ ya que si fuese igual a cero, la relación de recurrencia de orden k (2.2), se convertiría en una relación de orden $k - 1$ ya que el primer estado s_0 no se vuelve a utilizar.

Teorema 2.12. *: Si $\{s_n\}_{n=0}^{\infty}$ es una sucesión de recurrencia lineal en un cuerpo finito $\mathbb{F}_q$ que satisface (2.2) y además $a_0 \neq 0$, entonces la sucesión es periódica*

Demostración. Por el teorema 2.7, nuestra sucesión es finalmente periódica. Supongamos que r es el periodo mínimo y n_0 el preperiodo. i.e.: $s_{n+r} = s_n$, para $n \geqslant n_0$. Supongamos que $n_0 \geqslant 1$, es decir $s_{n_0-1+r} \neq s_{n_0-1}$.

Tomamos $n = n_0 + r - 1 \geqslant n_0$ entonces $s_{n+r} = s_n$ por lo que

$$s_{n_0+r+k-1} = a_{k-1}s_{n_0+r+k-2} + a_{k-2}s_{n_0+r+k-3} + \cdots + a_0 s_{n_0+r-1} + a$$

como $a_0 \neq 0$ y $a_0 \in \mathbb{F}_q$ despejamos s_{n_0+r-1}

$$\begin{aligned} s_{n_0+r-1} &= a_0^{-1}(s_{n_0+r-1+k} - a_{k-1}s_{n_0+r+k-2} - \cdots - a_1 s_{n_0+r} - a) \\ &= a_0^{-1}(s_{n_0+k-1} - a_{k-1}s_{n_0+k-2} - \cdots - a_1 s_{n_0} - a). \end{aligned} \tag{2.3}$$

Ya que r es periodo. Por otro lado, tomando $n = n_0 - 1$,

$$s_{n_0+k-1} = a_{k-1}s_{n_0+k-2} + a_{k-2}s_{n_0+k-3} + \cdots + a_0 s_{n_0-1} + a$$

despejamos en esta s_{n_0-1}, tenemos

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

Es la misma expresión que tenemos en 2.3 luego $s_{n_0-1+r} = s_{n_0-1}$ llegando así a un absurdo ya que n_0 era el preperiodo. □

2.2. Matriz generadora

Definición 2.13. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$, dada por la relación de recurrencia (2.2).

Asociamos a esta sucesión la matriz :

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix} \tag{2.4}$$

y la llamamos matriz asociada a la recurrencia. En el caso en que $k = 1$ entendemos que $A = a_0$.
Si $\{s_n\}_{n=0}^{\infty}$ es una sucesión de recurrencia lineal no homogénea de orden k que satisface (2.1). Definimos la matriz asociada C por:

$$C = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & a \\ 0 & 0 & 0 & \cdots & 0 & a_0 \\ 0 & 1 & 0 & \cdots & 0 & a_1 \\ 0 & 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix} \tag{2.5}$$

Y si el orden es uno consideramos

$$C = \begin{pmatrix} 1 & a \\ 0 & a_0 \end{pmatrix} \tag{2.6}$$

Por otra parte, definimos los vectores de estados por

$$\mathbf{s}_n^{'} = (1, s_n, s_{n+1}, \ldots, s_{n+k-1}), \quad n = 0, 1, \ldots$$

Proposición 2.14. *Toda sucesión de recurrencia lineal no homogénea de orden k en $\mathbb{F}_q$ que satisface (2.2), la podemos interpretar como una sucesión homogénea de orden $k+1$ en $\mathbb{F}_q$*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ de orden k. Tenemos que

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n + a$$

y por otro lado

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

restando la primera a esta segunda tenemos que

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

Es decir si llamamos $b_0 = -a_0$, $b_j = a_{j-1} - a_j \quad j = 1, 2, \ldots, k-1$ y $b_k = a_{k-1} + 1$, la diferencia anterior es una sucesión de recurrencia lineal homogénea de orden $k+1$. □

Los siguientes lemas los vamos a probar para el caso en que la sucesión sea homogénea, ya que utilizando la proposición anterior, también sirven para el caso en que la sucesión sea no homogénea.

Lema 2.15. *Sea $\{s_n\}_{n=0}^{\infty}$ es una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ que satisface (2.2) y A la matriz asociada. Entonces dado el vector de estados iniciales $\mathbf{s}_0 = (s_0, s_1, \ldots, s_{k-1})$, tenemos:*

$$\mathbf{s}_n = \mathbf{s}_0 A^n; \quad \forall n \in \mathbb{N}.$$

Demostración. La sucesión $\{s_n\}_{n=0}^{\infty}$ satisface la relación (2.2). Lógicamente podemos escribir el estado $m+1$ a partir del estado m-ésimo y la matriz asociada ya que:

$$\mathbf{s}_{m+1} = (s_{m+1}, s_{m+2}, \ldots, s_{m+k}) = (s_m, s_{m+1}, \ldots, s_{m+k-1})A = \mathbf{s}_m A.$$

En particular, $\mathbf{s}_1 = \mathbf{s}_0 A$ y para $n > 1$,

$$\mathbf{s}_n = s_{n-1}A = \cdots = \mathbf{s}_0 A^n,$$

por inducción sobre n. □

El resultado que acabamos de probar nos va a permitir tratar indistintamente a la matriz asociada y a la relación de recurrencia; por eso cuando demos una sucesión de recurrencia lineal de orden k, podemos dar la relación y el vector de estados iniciales o la matriz asociada y el vector de estados iniciales. Así pues la matriz asociada es el objeto matemático que juega el papel del dispositivo (LFSR) que genera la sucesión.

Nota sobre el grupo lineal sobre un cuerpo finito

El grupo formado por la matrices no singulares $k \times k$ sobre $\mathbb{F}_q$, con el producto usual como ley interna, se le llama grupo lineal y lo denotaremos por $GL(k, \mathbb{F}_q)$.

Si A es la matriz asociada a la relación de recurrencia (2.2), $det(A) = (-1)^{k-1}a_0$, por lo tanto si $a_0 \neq 0$ la matriz A es invertible. Es decir, $A \in GL(k, \mathbb{F}_q)$. Es importante conocer la estructura de este grupo ya que nos permitirá saber más sobre la sucesiones de recurrencia.

Dado el espacio vectorial $\mathbb{F}_q^k$ sobre $\mathbb{F}_q$. Estamos interesados en saber cual es el orden del grupo lineal; y esto es equivalente a saber cuantas bases distintas $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ tenemos en el espacio vectorial $\mathbb{F}_q^k$, ya que la matriz es no singular si, y sólo si, sus k vectores fila son linealmente independientes sobre $\mathbb{F}_q$.

Para fijar una base $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$, el primer vector se puede elegir de $q^k - 1$ formas distintas, ya que lo único que tenemos que imponer es que

sea distinto de cero. Una vez que tenemos éste primero, $\mathbf{v}_2$ tiene que ser independiente de él; es decir, no puede ser proporcional, por lo que tenemos $q^k - (q-1)$ posibilidades para $\mathbf{v}_2$ (podemos coger $q-1$ factores de proporcionalidad no nulos). Además el segundo vector también ha de ser distinto de cero por lo que tenemos $q^k - q$ formas de elegir $\mathbf{v}_2$. Sucesivamente, el vector $\mathbf{v}_i$ de la base tenemos $q^k - q^{i-1}$ formas de tomarlo ya que ha de ser linealmente independiente de los $i-1$ anteriores y no nulo. Entonces

$$\begin{aligned} \mid GL(k,\mathbb{F}_q) \mid &= (q^k-1)(q^k-q)\dots(q^k-q^{k-1}) \\ &= (q^k-1)(q^{k-1}-1)\dots(q-1)qq^2\dots q^{k-1} \\ &= q^{\frac{k(k-1)}{2}}\prod_{i=1}^{k}(q^i-1) \end{aligned}$$

Esta fórmula es un caso particular del número de matrices $m \times n$ sobre $\mathbb{F}_q$ de rango r dado por

$$q^{\frac{r^2-r}{2}}\prod_{i=1}^{r-1}(q^{m-i}-1)(q^{n-i}-1)(q^{i+1}-1)^{-1}; \quad 1 \leqslant r \leqslant \text{mín}\{m,n\}.$$

Ésta fue inicialmente dada por Landsberg en el libro *Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe* del 1893, para el caso en que q es primo. Más adelante se probó su generalización. Otros matemáticos como Klein, Carlitz, Brawley y J. D. Fulton también se dedicaron a problemas de matrices rectangulares sobre cuerpos finitos.
Hechos estos comentarios sobre el grupo lineal, volvamos a los resultados sobre el periodo de las sucesiones.

Teorema 2.16. *Sea $\{s_n\}_{n=0}^{\infty}$ es una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ con $a_0 \neq 0$ y A su matriz asociada (véase (2.4)). Entonces el periodo mínimo de la sucesión divide al orden de la matriz A en el grupo lineal $GL(k,\mathbb{F}_q)$*

Demostración. El determinante de la matriz A es $(-1)^{k-1}a_0 \neq 0$ luego efectivamente $A \in GL(k,\mathbb{F}_q)$. Sea m el orden de A. Por el lema 2.15, para $n \geqslant 0$ tenemos

$$\mathbf{s}_{n+m} = \mathbf{s}_0 A^{n+m} = \mathbf{s}_0 A^n = \mathbf{s}_n \quad \forall n \in \mathbb{N}$$

Luego m es un periodo de la sucesión $\{s_n\}_{n=0}^{\infty}$. Entonces por el lema 2.4, si el periodo mínimo es r, $r \mid m$. Tenemos así que el periodo mínimo divide al orden de A. □

Gracias a este resultado, sabemos que los periodos mínimos son todos ellos divisores de

$$q^{\frac{k(k-1)}{2}}\prod_{i=1}^{n}(q^i-1)$$

Además el lema 2.15 nos permite dar una demostración alternativa a 2.12 para el caso homogéneo y siempre que $a_0 \neq 0$.

2.3. Sucesiones de impulso-respuesta

Como ya comentamos en la introducción, si fijamos el dispositivo generador de la secuencia cifrante, el primer problema con el que nos enfrentamos es conseguir sucesiones con periodos lo más largos posibles. Dado que la sucesión queda determinada a partir del estado inicial se trata de analizar los posibles periodos y, si es posible, caracterizar los estados iniciales que optimizan la longitud del periodo.

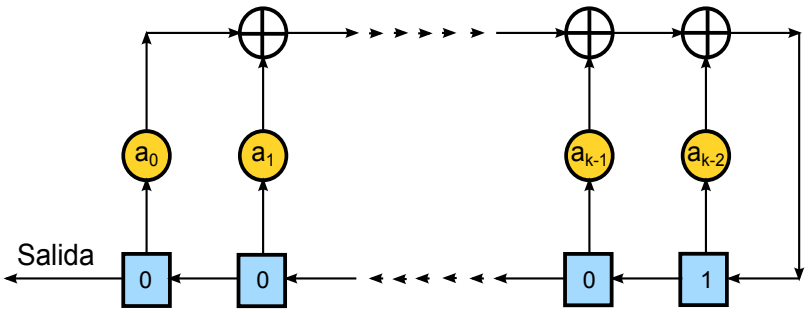
Definición 2.17. La sucesión de impulso-respuesta $\{d_n\}_{n=0}^{\infty}$ está unívocamente determinada por el vector de estados iniciales $\mathbf{d}_0$ con $d_0 = d_1 = \cdots = d_{k-2} = 0, d_{k-1} = 1$ y la recurrencia lineal

$$d_{n+k} = a_{k-1}d_{n+k-1} + a_{k-2}d_{n+k-2} + \cdots + a_0 d_n$$

En el caso en que el orden sea uno, $\mathbf{d}_0 = 1$

La sucesión de impulso-respuesta es simplemente una forma particular de llamar a la sucesión de recurrencia homogénea que tiene por vector de estados iniciales el vector $(0, 0, \ldots, 0, 1) \in \mathbb{F}_q^k$.

Las sucesiones de impulso-respuesta reciben este nombre por el vector de estados iniciales que tomamos. Recordemos que los LFSR funcionan con cada tic de reloj; entonces el circuito al principio está en reposo y con los registros vacios, es decir con 0 en todos ellos. Con el primer tic se introduce un bit en el último registro (el impulso). Posteriormente, el circuito empieza a funcionar, generando las respuestas sucesivas en cada tic. El LFSR de una sucesión de impulso-respuesta genérica es:



Lema 2.18. *Dada una sucesión de impulso-respuesta $\{d_n\}_{n=0}^{\infty}$, el conjunto de los k primeros vectores iniciales $\{\mathbf{d}_0, \mathbf{d}_1, \ldots, \mathbf{d}_{k-1}\}$ forman una base de $\mathbb{F}_q^k$ sobre $\mathbb{F}_q$*

Demostración. Si escribimos los vectores como columnas de una matriz, tenemos una matriz triangular con unos en la diagonal $a_{k-i+1,i}$ con $1 \leqslant i \leqslant k$. Son linealmente independientes y además todos ellos distintos luego son base. □

Lema 2.19. *Sea $\{d_n\}_{n=0}^{\infty}$ una sucesión de impulso-respuesta en $\mathbb{F}_q$ satisfaciendo una relación de recurrencia lineal y sea A su matriz asociada. Entonces, dos vectores de estados $\mathbf{d}_m$ y $\mathbf{d}_n$ son iguales si, y sólo si, $A^m = A^n$.*

Demostración. $\Longleftarrow$ Por el lema 2.15, $\mathbf{d}_m = \mathbf{d}_0 A^m$ y $\mathbf{d}_n = \mathbf{d}_0 A^n$. Entonces tenemos que

$$\mathbf{d}_m = \mathbf{d}_0 A^m = \mathbf{d}_0 A^n = \mathbf{d}_n$$

$\Longrightarrow$ Recíprocamente, del hecho de que los vectores de estados $\mathbf{d}_m$ y $\mathbf{d}_n$ sean iguales, tenemos que

$$\mathbf{d}_{m+t} = \mathbf{d}_{n+t}, \quad \forall t \geqslant 0$$

Podemos suponer $m > n$, por el lema 2.15,

$$\left.\begin{array}{r} \mathbf{d}_{n+t} = \mathbf{d}_t A^n \\ \\ \mathbf{d}_{m+t} = \mathbf{d}_t A^m \end{array}\right| \text{ entonces } \quad \mathbf{d}_t A^m = \mathbf{d}_t A^n \quad \forall t \geqslant 0.$$

Restando, $\mathbf{d}_t(A^m - A^n) = 0$ y, como $\{\mathbf{d}_0, \mathbf{d}_1, \ldots, \mathbf{d}_{k-1}\}$ son una base, $A^m = A^n$. □

Vistos estos lemas, veamos un teorema que va a contestar a la pregunta que planteábamos al principio.

Teorema 2.20. *El periodo mínimo de una sucesión de recurrencia lineal homogénea $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_q$ que verifique (2.2) , divide al periodo mínimo de su correspondiente sucesión de impulso-respuesta.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea que satisface (2.2), $\{d_n\}_{n=0}^{\infty}$ su correspondiente sucesión de impulso-respuesta y A su matriz asociada.
Supongamos que r es el periodo mínimo de $\{d_n\}_{n=0}^{\infty}$ y n_0 el preperiodo. Entonces por el lema 2.19, $A^{n+r} = A^n \quad \forall n \geqslant n_0$.
Como la matriz asociada es la misma para ambas sucesiones tendremos que $\mathbf{s}_{n+r} = \mathbf{s}_0 A^{n+r} = \mathbf{s}_0 A^n = \mathbf{s}_n$, para $n \geqslant n_0$ y r es también un periodo de $\{s_n\}_{n=0}^{\infty}$. Por el lema 2.4, el periodo mínimo r_0 de $\{s_n\}_{n=0}^{\infty}$ divide al periodo r. □

En la sección anterior vimos que si $a_0 \neq 0$ el periodo mínimo de una sucesión dividía al orden de la matriz en el grupo lineal.Ahora probaremos que el periodo de la sucesión de impulso-respuesta alcanza el máximo posible, es decir, el orden de la matriz A.

Teorema 2.21. *Si $\{d_n\}_{n=0}^{\infty}$ es una sucesión de impulso-respuesta de orden k en $\mathbb{F}_q$ que satisface (2.2) con $a_0 \neq 0$ y A es su matriz asociada, entonces su periodo mínimo es igual al orden de A en $GL(k, \mathbb{F}_q)$*

Demostración. Sea $\{d_n\}_{n=0}^{\infty}$ una sucesión impulso-respuesta de orden k y sea r su periodo mínimo. Por el teorema 2.16 sabemos que $r \mid ord(A)$.
Por otro lado $\mathbf{d}_r = \mathbf{d}_0$, entonces por el lema 2.19 $A^r = A^0 = Id$. Si esto ocurre, $ord(A) \mid r$ ya que recordemos que $ord(A) = \text{mín}\{n \in \mathbb{N}, \text{ tal que } A^n = Id\}$. Obteniendo así la igualdad. □

Las sucesiones de impulso-respuesta no son las únicas que optimizan la longitud del periodo. En el siguiente teorema vamos a comprobar que si existen k vectores de estados linealmente independientes, la sucesión alcanza el mismo periodo máximo que consiguen las sucesiones de impulso-respuesta.

Teorema 2.22. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ con preperiodo n_0. Si existen k vectores de estados $\mathbf{s}_{m_1}$, $\mathbf{s}_{m_2}, \ldots, \mathbf{s}_{m_k}$ con $m_i \geqslant n_0$ para $1 \leqslant i \leqslant k$ que sean linealmente independientes sobre $\mathbb{F}_q$, entonces, tanto $\{s_n\}_{n=0}^{\infty}$ como su correspondiente sucesión de impulso-respuesta son periódicas y tienen el mismo periodo mínimo.*

Demostración. Sea r el periodo mínimo de $\{s_n\}_{n=0}^{\infty}$. Para cada m_j con $1 \leqslant j \leqslant k$ tenemos por el lema 2.15

$$\mathbf{s}_{m_j} A^r = \mathbf{s}_{m_j+r} = \mathbf{s}_{m_j}.$$

Entonces $A^r = Id$, en particular $a_0 \neq 0$ y $ord(A) \mid r$. En este caso tenemos $\mathbf{s}_r = \mathbf{s}_0 A^r = \mathbf{s}_0$. Por lo tanto $\{s_n\}_{n=0}^{\infty}$ es periódica de periodo r.
Por otro lado, $\mathbf{d}_r = \mathbf{d}_0 A^r = \mathbf{d}_0$. Entonces $\{d_n\}_{n=0}^{\infty}$ también es periódica de periodo r.
Aplicando el teorema 2.20, tenemos que r divide al periodo mínimo de $\{d_n\}_{n=0}^{\infty}$, pero como sabemos que $\{d_n\}_{n=0}^{\infty}$ tiene periodo r ha de ser el mismo. □

Nota 2.23 (del teorema 2.22). 1. El recíproco del teorema no es cierto. Por ejemplo, considérese la sucesión $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_2$ generada por la relación de recurrencia $s_{n+3} = s_n, \quad n = 0, 1, \ldots$ y con vector de estados iniciales $\mathbf{s}_0 = (1, 0, 1)$:

$$1 \quad 0 \quad 1_{\lrcorner} \quad 1 \quad 0 \quad 1_{\lrcorner} \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad \ldots$$

tiene periodo 3 y la sucesión de impulso-respuesta $\{d_n\}_{n=0}^{\infty}$:

$$0 \quad 0 \quad 1_{\lrcorner} \quad 0 \quad 0 \quad 1_{\lrcorner} \quad 0 \quad 0 \quad 1_{\lrcorner} \quad \ldots$$

también tiene periodo 3. En cambio, tres vectores de estados de $\{s_n\}_{n=0}^{\infty}$ cualesquiera son linealmente dependientes. Como tiene periodo tres, solo tenemos tres posibles vectores: $(1,0,1)$, $(0,1,1)$, $(1,1,0)$; y la suma de los dos primeros, es el tercero.

2. La condición $m_j \geqslant n_0, \quad 1 \leqslant j \leqslant k$ es necesaria ya que si tomamos por ejemplo la sucesión en $\mathbb{F}_2$ dada por la recurrencia $s_{n+3} = s_{n+1}$ y con vector de estados iniciales $\mathbf{s}_0 = (0,1,1)$:

$$0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad \ldots$$

los dos primeros vectores de estados $(0,1,1)$ y $(1,1,1)$ son linealmente independientes y la sucesión no es periódica ya que tiene preperiodo 1.

2.4. Polinomio característico

Para una sucesión de recurrencia lineal homogénea con relación de recurrencia (2.2), vamos a definir un polinomio asociado a esta relación, el polinomio característico. Dicho polinomio codifica la relación de recurrencia, de forma semejante a como lo hace la matriz asociada. De esta forma tendremos dos forma de representar la relación. Además nos permitirá conocer nuevas propiedades de la sucesión.
Más adelante veremos que el polinomio característico de una sucesión, junto con el vector de estados iniciales, determinan toda la sucesión.

A partir de ahora todas las sucesiones de recurrencia lineales serán homogéneas salvo que se diga otra cosa. También las sucesiones de recurrencia lineal $\{s_n\}_{n=0}^{\infty}$ todas satisfacen la relación de recurrencia (2.2).

Definición 2.24. Llamamos polinomio característico de la relación de recurrencia lineal de orden k (2.2) al polinomio

$$f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0 \in \mathbb{F}_q[x] \tag{2.7}$$

Es claro que $f(x)$ es el polinomio característico de la matriz compañera A, es decir, $f(x) = \det(xI - A)$. Evidentemente la matriz A es la matriz compañera de f.
La relación de recurrencia, la matriz compañera y el polinomio característico son tres formas de expresar la misma información. A partir de ahora cuando demos una sucesión de recurrencia lineal para expresar su relación de recurrencia usaremos indistintamente, además de la propia relación, el polinomio característico o la matriz compañera.

El teorema siguiente nos va a permitir representar los términos de una sucesión en función del polinomio característico.

Teorema 2.25. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ y $f(x)$ su polinomio característico.*
Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ las raíces de $f(x)$ y supongamos que son todas distintas. Entonces existen $\beta_1, \beta_2, \ldots, \beta_k \in \mathbb{F}_q(\alpha_1, \alpha_2, \ldots, \alpha_k)$, unívocamente determinados a partir del vector de estado inicial $\mathbf{s}_0$, de manera que:

$$s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n \quad \forall n = 0, 1, \ldots$$

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k y $f(x)$ el polinomio característico de la sucesión. Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ las raíces de f en una extensión de $\mathbb{F}_q$, supongamos que son todas distintas y que $\mathbb{F}_q(\alpha_1, \alpha_2, \ldots, \alpha_k)$ es el cuerpo de descomposición de f. Sean $\beta_1, \beta_2, \ldots, \beta_k \in \mathbb{F}_q(\alpha_1, \alpha_2, \ldots, \alpha_k)$ arbitrarios y tomamos $t_n := \sum_{j=1}^{k} \beta_j \alpha_j^n$ para $n \geqslant 0$. Veamos que $\{t_n\}_{n=0}^{\infty}$ es una sucesión de recurrencia lineal homogénea de orden k asociada a f. Tenemos que comprobar por tanto que

$$t_{n+k} = a_{k-1} t_{n+k-1} + a_{k-2} t_{n+k-2} + \cdots + a_0 t_n.$$

Sustituyendo $t_n = \sum_{j=1}^{k} \beta_j \alpha_j^n$ se tiene:

$$\sum_{j=1}^{k} \beta_j \alpha_j^{n+k} - a_{k-1} \sum_{j=1}^{k} \beta_j \alpha_j^{n+k-1} - \cdots - a_0 \sum_{j=1}^{k} \beta_j \alpha_j^n =$$

$$\sum_{j=1}^{k} \alpha_j^n \beta_j (\alpha_j^k - a_{k-1} \alpha_j^{k-1} - \cdots - a_0) = \sum_{j=1}^{k} \alpha_j^k \beta_j f(\alpha_j) = 0,$$

ya que $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ son las raíces del polinomio.

Veamos ahora que, dado $\mathbf{s}_0 = (s_0, s_1, \ldots, s_{k-1})$, podemos determinar unívocamente $\beta_1, \beta_2, \ldots, \beta_k \in \mathbb{F}_q(\alpha_1, \alpha_2, \ldots, \alpha_k)$ de manera que $\mathbf{s}_0 = \mathbf{t}_0$ y como consecuencia $s_n = t_n$ para cualquier $n \geqslant 0$. En efecto como

$$\beta_1 \alpha_1^i + \beta_2 \alpha_2^i + \cdots + \beta_k \alpha_k^i = s_i$$

para $0 \leqslant i \leqslant k-1$, es la ecuación i-ésima del sistema. La matriz de este sistema es de Vandermonde y puesto que $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ son todas distintas por hipótesis, $\{\beta_1, \beta_2, \ldots, \beta_k\}$ están determinados unívocamente.
Por otro lado, cuando resolvemos el sistema aplicando la regla de Cramer, escribimos los $\{\beta_j\}$ en función de las raíces $\{\alpha_j\}$, así que pertenecen al cuerpo de descomposición $\mathbb{F}_q(\alpha_1, \alpha_2, \ldots, \alpha_k)$. □

Veamos un ejemplo que ilustre el teorema.

Ejemplo 2.26. Supongamos que tomamos la sucesión de recurrencia dada por la relación $s_{n+3} = s_{n+1} + s_n$ sobre $\mathbb{F}_2$ y con vector de estados iniciales $\mathbf{s}_0 = (0, 1, 1)$.
El polinomio característico de la sucesión $f(x) = x^3 + x + 1$ es irreducible y el conjunto de sus raíces está dado por $\{\alpha_1 = \alpha, \alpha_2 = \alpha^2, \alpha_3 = \alpha + 1\}$.
Sea $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ el cuerpo de descomposición del polinomio característico. Planteamos el sistema que hemos visto en la demostración del teorema:

$$\begin{cases} \beta_1 + \beta_2 + \beta_3 & = & 0 \\ \alpha\beta_1 + \alpha^2\beta_2 + (\alpha+1)\beta_3 & = & 1 \\ \alpha^2\beta_1 + \alpha(\alpha+1)\beta_2 + \alpha^2\beta_3 & = & 1 \end{cases}$$

Lo resolvemos y llegamos a que la solución es:

$$\begin{aligned} \beta_1 &= 1 + \alpha + \alpha^2 \\ \beta_2 &= \alpha^2 + 1 \\ \beta_3 &= \alpha \end{aligned}$$

Entonces por el teorema anterior la relación de la sucesión es:

$$s_n = \alpha^n(1 + \alpha + \alpha^2) + \alpha^{2n}(\alpha^2 + 1) + (\alpha + 1)^n\alpha, \quad \forall n \geqslant 0.$$

Además puesto que $\gamma^7 = 1$ para todo $\gamma \in \mathbb{F}_8^*$, tenemos que $s_{n+7} = s_n$ para todo $n \geqslant 0$.
De hecho, el periodo mínimo de la sucesión es precisamente 7 que es el valor máximo que puede tener.

Con esto hemos visto que podemos representar los elementos de la sucesión en función de las raíces del polinomio característico.

2.5. Funciones generatrices

Como ya sabemos una forma de representar la sucesión $\{s_n\}_{n=0}^{\infty}$ mediante un objeto algebraico es la serie formal $\sum_{n=0}^{\infty} s_n x^n$. De esta forma podemos operar algebraicamente las sucesiones y en particular, es el marco actual para establecer la relación con el polinomio característico estableciendo el papel de este último como "dispositivo" algebraico que sustituye al LFSR.

Definición 2.27. Dada $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal sobre un cuerpo finito $\mathbb{F}_q$, definimos su función generatriz como la serie formal cuyos coeficientes son los términos de la sucesión. En general la denotaremos por $G(x)$. Es decir

$$G(x) = \sum_{n=0}^{\infty} s_n x^n. \tag{2.8}$$

Pese a que le demos este nombre, nunca vamos a considerar una función generatriz como una función en el sentido habitual, por lo que nunca la vamos a evaluar. Notese que tampoco tendría mucho sentido ya que para poder tratar la convergencia de la serie resultante, tendríamos que evaluar en un cierto x_0 real o complejo y nosotros estamos trabajando en un cuerpo finito.

Como ya introdujimos en el anillo de las series formales podemos calcular el inverso multiplicativo de los polinomios (y de las series, claro) cuyo término constante sea no nulo.

Como sabemos, la serie formal $P(x) = \sum_{n=0}^{\infty} p_n x^n \in \mathbb{F}_q[[x]]$ es inversible siempre que p_0. Con frecuencia es conveniente invertir el polinomio característico de una sucesión de recurrencia, sin embargo esto no es posible si $a_0 = 0$. Una forma de solventar esta dificultad es la siguiente. Dado $f(x) = a_n x^n + \dots a_1 x + a_0 \in \mathbb{F}_q[x]$ con $a_n \neq 0$, el polinomio recíproco de f es el polinomio

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + \cdots + a_{n-1}x + a_n. \tag{2.9}$$

En particular, si $f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0 \in \mathbb{F}_q[x]$ es el polinomio característico de una sucesión de recurrencia lineal, su polinomio recíproco es $f^*(x) = 1 - a_{k-1}x - \cdots - a_0 x^k$. Nótese que ahora f^* es irreducible en $\mathbb{F}_q[[x]]$.

El "traslado" de la ecuación de recurrencia lineal a la función generatriz se expresa mediante el polinomio característico recíproco y el vector de estados iniciales de la siguiente forma.

Teorema 2.28. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$, que satisface la relación (2.2). Sea f^* el polinomio recíproco del polinomio característico de la sucesión y sea $G(x) \in \mathbb{F}_q[[x]]$ su función generatriz. Entonces*

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

donde

$$g(x) = -\sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_{i+k-j}s_i x^j\right) \in \mathbb{F}_q[x],$$

siendo $a_k = -1$.

Recíprocamente, si $g(x) \in \mathbb{F}_q[x]$ es un polinomio cualquiera de grado menor estrictamente que k y $f^*(x) = 1 - a_{k-1}x - \cdots - a_0 x^k \in \mathbb{F}_q[x]$, entonces la

serie $G(x) = \dfrac{g(x)}{f^*(x)}$, *es la función generatriz de una sucesión de recurrencia lineal en* $\mathbb{F}_q$ *que satisface la relación (2.2).*

Demostración. Consideramos f^* el polinomio recíproco del característico de nuestra sucesión y $G(x)$ su función generatriz. Hacemos el producto y llegamos a

$$\begin{aligned} f^*(x)G(x) &= \sum_{j=0}^{k-1} \left(\sum_{i=0}^{j} a_i s_{j-k+i} \right) x^j - \sum_{j=k}^{\infty} \left(\sum_{i=0}^{j} a_i s_{j-k+i} \right) x^j \\ &= g(x) - \sum_{j=k}^{\infty} \left(\sum_{i=0}^{k} a_i s_{j-k+i} \right) x^j. \end{aligned} \tag{2.10}$$

Puesto que la sucesión $\{s_n\}_{n=0}^{\infty}$ satisface la relación (2.2), $\sum_{i=0}^{k} a_i s_{j-k+i} = 0$ para cualquier $j \geqslant k$. El polinomio f^* tiene inverso multiplicativo porque el término constante es no nulo, entonces tenemos ya la igualdad $G(x) = \dfrac{g(x)}{f^*(x)}$.

Recíprocamente, supongamos que tomamos $g(x) \in \mathbb{F}_q[x]$ un polinomio cualquiera de grado menor o igual que $k-1$ y f^* un polinomio de la forma $1 - a_{k-1}x - \cdots - a_0 x^k$ con coeficientes en $\mathbb{F}_q$. Sea $G(x) = \sum S_n x^n$ una serie formal con coeficientes $\{S_n\}$ indeterminados. La serie $f^*(x)G(x)$ es un polinomio de grado menor que k si sólo si $\sum_{i=0}^{k} a_i S_{j-k+i} = 0$ para $j \geqslant k$. Llamamos $n = j-k$ y tenemos que esta igualdad es equivalente a $\sum_{i=0}^{k} a_i S_{n+i} = 0$ para cada $n \geqslant 0$. Pero esto es, justamente, que los coeficientes S_i de la serie formal $G(x)$ que queremos definir, satisfagan la relación $a_k S_{n+k} + a_{k-1} S_{n+k-1} + a_{k-2} S_{n+k-2} + \cdots + a_0 S_n = 0$, para cada $n \geqslant 0$. Finalmente, tomando los k primeros coeficientes de la serie $G(x)$ y el polinomio inicial $g(x)$ podemos definir el vector de estados iniciales $(s_0, \ldots, s_{k-1})$ que junto, con la relación de recurrencia anterior, define la sucesión de recurrencia lineal homogénea de orden k que buscamos. □

Nota 2.29. El polinomio $g(x)$ recoge la información del estado inicial $\mathbf{s}_0$ en relación a f^*. Nos referiremos a él como el polinomio inicial de $\{s_n\}_{n=0}^{\infty}$ o de $G(x)$.

Vamos a hacer un par de ejemplos que muestran como se utiliza este teorema.

Ejemplo 2.30. Supongamos que tenemos la relación de recurrencia $s_{n+3} = s_{n+2} + s_n$ para $n = 0, 1, \ldots$ en $\mathbb{F}_2$. El polinomio característico es $f(x) = x^3 + x^2 + 1$ y su polinomio recíproco es $f^*(x) = x^3 f(\frac{1}{x}) = 1 + x + x^3$. Su pon ga mos que tenemos el vector de estados iniciales $\mathbf{s}_0 = (1, 1, 1)$. El polinomio g del teorema es $g(x) = 1$, entonces hacemos la división y resulta que la

función generatriz es $G(x) = 1+x+x^2+x^4+x^7+x^8+x^9+x^{11}+x^{14}+\ldots$, y como la hemos definido, la sucesión es $1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\ldots$. La sucesión tiene periodo mínimo 7. Esto no es una casualidad ya que f, el polinomio característico, es irreducible y tiene orden 7 .

Hagamos otro ejemplo en el que el polinomio ni siquiera sea irreducible. Supongamos que tenemos la relación $s_{n+4} = s_{n+2} + s_{n+1} + s_n$ para $n \in \mathbb{N}$. El polinomio característico es $f(x) = x^4 + x^2 + x + 1$ y su polinomio recíproco $f^*(x) = x^4 + x^3 + x^2 + 1$. Consideramos, por ejemplo, el vector de estados iniciales $\mathbf{s}_0 = (1, 0, 1, 0)$; entonces el polinomio g es $g(x) = 1 + x^3$. Hacemos la división y obtenemos la función generatriz $G(x) = 1 + x^2 + x^5 + x^6 + x^7 + x^9 + x^{12} + x^{13} + \ldots$ cuyos coeficientes son los términos de la sucesión $1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\ldots$, la sucesión tiene periodo 7.

Veamos el recíproco del teorema. Tomamos el polinomio recíproco de antes $f^*(x) = x^4+x^3+x^2+1$ y cogemos $g(x) = x$ (podríamos coger cualquier polinomio con grado menor estricto que 4). Hacemos la división y tenemos $G(x) = x + x^3 + x^4 + x^8 + x^{10} + x^{11} + x^{15} + \ldots$; sus coeficientes forman la sucesión $0\,1\,0\,1\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1\ldots$
Por otra parte, cogemos ahora el polinomio recíproco del primer ejemplo, el que era irreducible, $f^*(x) = 1+x+x^3$ y el polinomio $g(x) = x$. Hacemos la división y calculamos la función generatriz $G(x) = x + x^2 + x^3 + x^5 + x^8 + x^9+x^{10}+x^{12}+\ldots$. La sucesión que obtenemos es $0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\ldots$, que es casi la misma que la del primer ejemplo. De hecho podemos decir que esta es la anterior, pero con preperiodo 0. Es lo que se denomina *sucesión desplazada.*

Si $\{s_n\}_{n=0}^{\infty}$ es periódica de periodo r también la sucesión satisface la relación de recurrencia lineal $s_{n+r} = s_n$, por tanto $x^r - 1$ es también un polinomio característico para la sucesión y tendremos que

$$G(x) = \frac{g(x)}{f^*(x)} = \frac{\widehat{g}(x)}{1 - x^r},$$

para un polinomio inicial $\widehat{g}(x)$ de grado menor que r. Esta sencilla relación permite adaptar, en términos de polinomios sin la necesidad de utilizar la función generatriz, el resultado anterior:

Teorema 2.31. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ con polinomio característico $f(x)$ y que es periódica con periodo r. Entonces se da la igualdad*

$$f(x)s(x) = (1 - x^r)h(x), \tag{2.11}$$

donde

$$s(x) = s_0x^{r-1} + s_1x^{r-2} + \cdots + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x],$$

y

$$h(x) = \sum_{j=0}^{k-1} \left(\sum_{i=0}^{k-1-j} a_{i+j+1} s_i \right) x^j \in \mathbb{F}_q[x], \tag{2.12}$$

considerando $a_k = -1$.

Demostración. La sucesión $\{s_n\}_{n=0}^{\infty}$ es periódica de periodo r, entonces $x^r - 1$ es polinomio característico de la sucesión. Calculamos la función generatriz como hemos visto en el teorema 2.28

$$G(x) = \frac{s^*(x)}{1 - x^r} = \frac{s_0 + s_1 x + \cdots + s_{r-1} x^{r-1}}{1 - x^r}.$$

Por otro lado, utilizando el mismo teorema también sabemos que $G(x) = \frac{g(x)}{f^*(x)}$. Igualando ambas expresiones, tenemos

$$\frac{s^*(x)}{1 - x^r} = \frac{g(x)}{f^*(x)},$$

o lo que es lo mismo $s^*(x) f^*(x) = g(x)(1 - x^r)$. Si f y s son de la forma del enunciado del teorema, tenemos que

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

Si comparamos ahora los coeficientes de g en el teorema 2.28 con los de 2.12 vemos que

$$h(x) = -x^{k-1} g \left(\frac{1}{x} \right) = -g^*(x) \tag{2.13}$$

y obtenemos así la identidad $f(x)s(x) = (1 - x^r)h(x)$. □

El polinomio $h(x)$ juega un papel semejante al del polinomio $g(x)$ en el teorema 2.28, pero en relación a f. Nos referiremos a él también como polinomio inicial y en el caso de que haya lugar a confusión aclararemos cuál es.

Capítulo 3

Optimización de los LFSR. Complejidad lineal

En este capítulo los ingredientes matemáticos de los que nos hemos dotado para estudiar las sucesiones de recurrencia lineal se utilizan de forma exhaustiva para resolver dos problemas de optimización fundamentales. El primero de ellos consiste en caracterizar los LFSR (es decir los polinomios característicos) que garantizan sucesiones con periodos lo más grandes posibles. Puesto que en el mejor de los casos el periodo es $q^k - 1$, probaremos que dicho periodo se alcanza cuando usamos los que llamaremos polinomios primitivos. Es claro que esta clase de polinomios será la única que se utilice en la práctica.

Si fijamos ahora una sucesión de recurrencia lineal, es evidente que la misma sucesión se puede generar a partir de varios polinomios. Por ejemplo si la sucesión satisface la relación (2.2) y tiene periodo r, obviamente, además del polinomio característico $f(x)$, podemos tomar el polinomio $x^r - 1$. En la sección segunda probaremos que entre todos ellos existe uno privilegiado, el polinomio mínimo. Dicho polinomio se caracteriza porque tiene grado el menor posible, por tanto el LFSR asociado a dicho polinomio tendrá el mínimo número de registros posible y es perfectamente natural tomar este entero como medida de la complejidad de la sucesión.

Finalmente, si conocemos una cadena de bits con el doble de longitud que el orden de la sucesión, con el algoritmo que nos proporciona el teorema de Berlekamp-Massey, podemos calcular el polinomio mínimo de la sucesión. Esto debilita la seguridad de las sucesiones de recurrencia ya que una vez que conocemos el polinomio mínimo podemos obtener toda la sucesión y de esta forma el atacante tendría la clave. Por ello queremos encontrar los LFSR que optimicen las propiedades de las sucesiones y así hacer más costoso el aplicar el citado algoritmo.

3.1. Orden del polinomio característico

Definamos en primer lugar el orden de un polinomio f en $\mathbb{F}_q[x]$.

Definición 3.1. Sea $f \in \mathbb{F}_q[x]$ un polinomio no constante. Si $f(0) \neq 0$, entonces al menor entero positivo e tal que $f(x) \mid x^e - 1$, le llamamos orden de f y lo denotamos por $ord(f)$ u $ord(f(x))$. Por otro lado, si $f(0) = 0$, lo podemos escribir de la siguiente forma $f(x) = x^t g(x)$ con $g(x) \in \mathbb{F}_q[x]$ y $g(0) \neq 0$ y definimos el orden de f como el orden de g.

La razón por la cual a dicho entero lo llamamos orden es la siguiente: Tomamos $f \in \mathbb{F}_q[x]$ un polinomio no constante y construimos el anillo cociente $A = \mathbb{F}_q[x]/(f)$; en este anillo denotamos por $[x]$ la clase de x. Si $f(0) \neq 0$ entonces x y $f(x)$ son primos entre si y por tanto $[x]$ es una unidad en A. Por ello existe un entero positivo n tal que $[x]^n = 1$ en A. Además si $e = ord([x])$, $x^e = 1$ en A si, y sólo si, $[x]^e \equiv 1 \bmod(f)$, que es lo mismo que decir $f \mid x^e - 1$.

Nota 3.2. Sea $f \in \mathbb{F}_q[x]$ un polinomio no nulo en $\mathbb{F}_q$ y f^* su polinomio recíproco. Entonces $ord(f) = ord(f^*)$. La demostración es sencilla del hecho de que el recíproco del producto de polinomios es igual al producto de los polinomios recíprocos.

De todas formas, el siguiente lema también ilustra el porqué del nombre; ya que como vamos a ver el orden del polinomio coincide con el orden de la matriz compañera en el grupo lineal.

Lema 3.3. *Sea $f \in \mathbb{F}_q[x]$ un polinomio no constante de grado k y tal que $f(0) \neq 0$. Entonces el orden de f es igual al orden de su matriz A compañera en el grupo lineal $GL(k, \mathbb{F}_q)$.*

Demostración. Puesto que A es la matriz compañera de nuestro polinomio f, este es el polinomio característico de A. Consecuentemente, tenemos que existe un entero positivo e tal que $A^e = Id$ si, y sólo si, $f(x) \mid x^e - 1$. Tomamos el mínimo entero positivo e que verifica esta equivalencia, es decir, $e = ord(f)$ y por la equivalencia es el orden de A. □

Proposición 3.4. *Sea $f \in \mathbb{F}_q[x]$ un polinomio no nulo de grado $m \geqslant 1$ y con $ord(f) = e$. Entonces $e \leqslant q^m - 1$.*

Demostración. El grupo de unidades $(\mathbb{F}_q[x]/(f))^*$ tiene cardinal $t \leqslant q^m - 1$ donde m es el grado de f. Por tanto $x^t \equiv 1 \bmod f$ y como consecuencia $e \leqslant t \leqslant q^m - 1$. □

La relación entre el periodo mínimo de la sucesión y el orden de la matriz compañera o el del polinomio característico la da el siguiente teorema.

Teorema 3.5. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k y $f \in \mathbb{F}_q[x]$ su polinomio característico. Entonces:*

1. *El periodo mínimo de la sucesión divide al orden de $f(x)$.*
2. *El periodo mínimo de la sucesión de impulso-respuesta asociada es igual al orden de $f(x)$.*

Demostración. Si $f(0) \neq 0$, sabemos por el lema anterior que el orden del polinomio coincide con el orden de la matriz compañera. Utilizando esto, veamos la prueba de cada apartado:

El apartado primero es el teorema 2.16 y el segundo es justamente el teorema 2.21.

Supongamos ahora que $f(0) = 0$, entonces podemos escribir el polinomio $f(x) = x^h g(x)$ con $g(0) \neq 0$. Por definición de orden, sabemos que el orden de f es el de g. Definimos $t_n = s_{n+h}$ para $n = 0, 1, \dots$. La sucesión $\{t_n\}_{n=0}^{\infty}$, es una sucesión de recurrencia lineal homogénea, g es su polinomio característico y de grado estrictamente positivo (si el grado fuese cero, tendríamos la sucesión idénticamente nula). El periodo mínimo de $\{t_n\}_{n=0}^{\infty}$ es el mismo que el de $\{s_n\}_{n=0}^{\infty}$ ya que los h primeros términos no intervienen. Entonces ya estamos en condiciones de aplicar los teoremas 2.16 y 2.21 como en el caso anterior. □

Con este resultado, sabemos que el periodo mínimo de una sucesión de recurrencia lineal homogénea divide al orden de su polinomio característico y que el de la sucesión de impulso-respuesta asociada lo alcanza; sin embargo, no son solo estas las que lo alcanzan. Basta con que el polinomio característico sea irreducible, independientemente del vector de estados iniciales (siempre que sea no nulo, claro), para que coincida con el orden del polinomio.

Teorema 3.6. *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado m. Entonces $ord(f)$ es igual al orden de cualquier raíz de f en el grupo multiplicativo $\mathbb{F}_{q^m}^*$. De hecho en cualquier extensión en la que esté la raíz.*

Demostración. Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$. La extensión $\mathbb{F}_{q^m}$, es el cuerpo de descomposición de f sobre $\mathbb{F}_q$ y además todas las raíces de f tienen el mismo orden en $\mathbb{F}_{q^m}^*$. Sea $\alpha \in \mathbb{F}_{q^m}^*$ una de las raíces entonces $\alpha^s = 1$ si, y sólo si, $f(x)$ divide a $x^s - 1$. Puesto que el orden es el menor entero e tal que $f(x)$ divide a $x^e - 1$, este e es el orden de la raíz α. □

Corolario 3.7. *Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible sobre $\mathbb{F}_q$ de grado m, entonces $ord(f)$ divide a $q^m - 1$.*

Demostración. Dado $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$, por el teorema anterior $ord(f)$ es el orden de una de sus raíces en el grupo multiplicativo asociado al cuerpo de descomposición; entonces, este, ha de dividir al orden del grupo que es $q^m - 1$. □

Nota 3.8. Este corolario fue demostrado por Gauss; uno de los primeros matemáticos que estudió las propiedades del orden de los polinomios sobre cuerpos finitos.

Como anunciábamos, las sucesiones de impulso-respuesta no son las únicas en las que el periodo mínimo coincide con el orden del polinomio característico. Ahora veremos que basta con que el polinomio sea irreducible.

Teorema 3.9. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k con un vector de estados iniciales no nulo. Supongamos además que $f(x) \in \mathbb{F}_q[x]$, su polinomio característico, es irreducible y $f(0) \neq 0$. Entonces la sucesión es periódica, con periodo mínimo igual al orden de $f(x)$.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea satisfaciendo las hipótesis del enunciado. Por el teorema anterior sabemos que la sucesión es periódica y que el periodo mínimo r divide al orden de f. Por otra parte, tenemos de la igualdad 2.11: $f(x)s(x) = (1 - x^r)h(x)$, con $s(x)$ y $h(x)$ polinomios no nulos, luego $f(x)$ divide a $(1-x^r)h(x)$. Entonces, como el grado de h es estrictamente menor que el de f y f es irreducible, por el corolario 3.7, $f(x)$ divide a $x^r - 1$; así $r \geqslant ord(f(x))$, y obtenemos la igualdad. □

Los resultados anteriores ponen de manifiesto el interés en usar como polinomios característicos polinomio irreducibles, ya que en este caso el orden de divide a $q^m - 1$ y además se obtienen sucesiones con periodo óptimo.

Afortunadamente hay resultados que nos aseguran la existencia de suficientes polinomios irreducibles sobre el cuerpo $\mathbb{F}_q$ de grado m para cualquier entero positivo m. De hecho es conocido que el número de tales polinomios viene dado por la fórmula

$$I_{mq} = \frac{1}{m} \sum_{d|m} \mu(d) q^{\frac{m}{d}},$$

donde $\mu(d)$ es la función μ de Moebius y la definimos del siguiente modo:

$$\mu(d) = \begin{cases} 1 & si\ d = 1 \\ (-1)^k & si\ d = p_1 ... p_k \text{ son primos distintos} \\ 0 & \text{en otro caso} \end{cases}$$

Si $e \geq 2$ es un divisor de $q^m - 1$, siempre que q tenga orden m módulo e, se tiene también que el número de polinomios irreducibles en $\mathbb{F}_q[x]$ de grado m y orden e es igual a

$$\phi(e) \mid m \,. \tag{3.1}$$

Ejemplo 3.10. Supongamos que tomamos la sucesión de recurrencia lineal homogénea $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_3$ de orden 4 que satisface la relación $s_{n+4} = 2s_{n+3} + 2s_{n+2} + 2s_{n+1} + 2s_n$, para $n = 0, 1, \ldots$. El polinomio característico asociado es $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_3$, es irreducible y tiene orden 5 ya que $x^5 - 1 = f(x)(x+2)$. Tomamos el vector de estados iniciales $\mathbf{s}_0 = (1, 0, -1, 1)$; tenemos que la sucesión es

$$1 \quad 0 \quad -1 \quad 1 \quad -1 \quad 1 \quad 0 \quad -1 \quad 1 \quad -1 \quad 1 \quad 0 \quad -1 \quad 1 \ldots,$$

y tiene, efectivamente, periodo 5.

Cálculo del orden de un polinomio

Lema 3.11. *Sea c un entero positivo y $f \in \mathbb{F}_q[x]$. Entonces, f divide a $x^c - 1$ si, y sólo si, $ord(f) \mid c$.*

Demostración. $\Leftarrow$ Supongamos que existe $h \in \mathbb{F}_q$ tal que $c = eh$, y con $e = ord(f)$. De la igualdad $y^h - 1 = (y-1)(y^{h-1} + \cdots + y + 1)$, resulta que tras el cambio de variable $y = x^e$, tenemos que

$$x^c - 1 = (x^e - 1)(x^{e(h-1)} + \cdots + x^e + 1),$$

y por tanto $x^e - 1 \mid x^c - 1$. Como $f \mid x^e - 1$ ya que $e = ord(f)$, también $f \mid x^c - 1$.

$\Rightarrow$ Sea $ord(f) = e$. Si f divide a $x^c - 1$ entonces $c \geqslant e$ y $x^c - 1 = f(x)g(x)$. Haciendo la división euclídea de c entre e, tenemos que $c = \lambda e + \mu$, con $\lambda, \mu \in \mathbb{N}$ y $\mu < e$. Luego $x^c - 1 = x^{\lambda e + \mu} - 1 = x^{\lambda e} x^{\mu} - 1 = x^{\lambda e} x^{\mu} - 1 + x^{\mu} - x^{\mu} = x^{\mu}(x^{\lambda e} - 1) + x^{\mu} - 1$. Puesto que $f \mid x^c - 1$ y $f^{\lambda e} - 1$, tenemos que $f(x)/x^{\mu} - 1$, pero como $\mu < e$, sólo es posible si $\mu = 0$; y de este modo, e divide a c. $\square$

Un tipo especial de polinomios son aquellos que los podemos expresar como potencia de un polinomio irreducible, para estos, veamos como podemos calcular el orden en función del orden del polinomio de la base.

Teorema 3.12. *Sea $g \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ y con $ord(g) = e$. Por otra parte, sea $f = g^b$ con b un entero positivo y sea t el menor entero tal que $p^t \geqslant b$, donde p es la característica del cuerpo. Entonces $ord(f) = ep^t$.*

Demostración. Supongamos que $ord(f) = c$ entonces, $f(x) \mid x^c - 1$ y como $f = g^b$, g también divide a $x^c - 1$. Por el lema 3.11, el orden de g divide a c, es decir e divide a c y g divide a $x^e - 1$; además como $f = g^b$, f divide a $(x^e - 1)^b$. Si tomamos t el menor entero tal que $b \leqslant p^t$, siendo p la característica del cuerpo, $f(x) \mid (x^e - 1)^{p^t} = x^{ep^t} - 1$, y por el lema 3.11, c ha de dividir a ep^t. Por otro lado, si $c = ep^u$ para $0 \leqslant u \leqslant t$. Ya sólo nos queda probar que $u = t$.
Como $ord(g) = e$ y g es irreducible $e \mid q^m - 1$, siendo m el grado del polinomio g. En particular, e no es múltiplo de p y las raíces de $x^e - 1$ son todas simples. Puesto que $g \mid x^e - 1$, las raíces de g también son todas simples y por tanto todas las raíces de $f = g^b$ tienen multiplicidad b. Ahora g^b divide a $x^c - 1 = x^{ep^u} - 1 = (x^e - 1)^{p^u}$ cuyas raíces tienen multiplicidad exactamente p^u. Como consecuencia $b \leqslant p^u$ y como $u \leqslant t$, por la multiplicidad $u = t$. □

Veamos ahora cual es el orden de un polinomio en función del orden de los polinomios en los que se descompone.

Teorema 3.13. *Sean $g_1, g_2, \ldots g_k \in \mathbb{F}_q[x]$ polinomios primos entre sí dos a dos y distintos de cero sobre $\mathbb{F}_q$. Tomamos $f = g_1 g_2 \ldots g_k$ entonces, $ord(f) = \text{mcm}(ord(g_1), ord(g_2), \ldots, ord(g_k))$*

Demostración. Sea $f = g_1 g_2 \ldots g_k$ con los $\{g_i\}$, verificando las hipótesis del teorema. Supongamos que $ord(f) = e$, $ord(g_i) = e_i$ para $1 \leqslant i \leqslant k$ y sea $c = \text{mcm}(e_1, e_2, \ldots, e_k)$. Para cada i, g_i divide a $x^{e_i} - 1$ y como e_i divide a c, g_i divide a $x^c - 1$; entonces, como los g_i son primos dos a dos, $f(x)$ es el $\text{mcm}(g_1 g_2 \ldots g_k)$ y por tanto divide a $x^c - 1$ y por el lema 3.11, e divide a c. Por otro lado, $f(x) \mid x^e - 1$ y como $f = g_1 g_2 \ldots g_k$, g_i divide a $x^e - 1$ para todo $i \in \{1, 2, \ldots, k\}$. De nuevo, por el lema 3.11 tenemos que $e_i \mid e$ para todo i, luego c divide a e. □

Gracias a estos dos teoremas podemos saber el orden de cualquier polinomio en función de los órdenes de cada uno de los polinomios irreducibles en los que se descompone. Para dejarlo más claro, lo escribiremos en forma de teorema.

Teorema 3.14. *Sea $\mathbb{F}_q$ un cuerpo finito de característica p. Sea $f \in \mathbb{F}_q[x]$ tal que $f = a f_1^{b_1} f_2^{b_2} \ldots f_k^{b_k}$ es su descomposición como producto de polinomios irreducibles con $a \in \mathbb{F}_q$, $b_1, b_2, \ldots, b_k \in \mathbb{N}$ y $f_1, f_2, \ldots f_k \in \mathbb{F}_q$ irreducibles y distintos. Entonces $ord(f) = ep^t$, donde $e = \text{mcm}(ord(f_1), ord(f_2), \ldots, ord(f_k))$ y t es el menor entero tal que $p^t \geqslant \text{máx}\{b_1, b_2, \ldots, b_k\}$.*

Computacionalmente, cuando se desea calcular el orden de un polinomio sobre $\mathbb{F}_q$ no se utiliza la definición. Para calcularlo lo que hacemos es descomponer como producto de factores primos el entero $q^m - 1$, ya que

como nos dice el corolario 3.7, el orden divide a este entero. Una vez que tenemos la descomposición $q^m - 1 = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, si $x^{(q^m-1)/p_j} \neq 1 \bmod f(x)$, entonces e ha de ser múltiplo de $p_j^{r_j}$. Si $x^{(q^m-1)/p_j} \equiv 1 \bmod f(x)$, entonces e no es múltiplo de $p_j^{r_j}$. Y de este modo calculamos el orden. La gracia de este procedimiento está en la factorización de $q^m - 1$, pero no es un entero cualquiera, sino el orden del grupo multiplicativo y tenemos tablas con las factorizaciones de estos números para distintos valores de q y de m.

3.2. Polinomios primitivos

Si fijamos el orden de la recurrencia, k, es claro que cuanto mayor sea el periodo de la sucesión más segura será; por ello estamos interesados en construir sucesiones con el periodo lo más grande posible. Sabemos que el periodo mínimo de una sucesión homogénea tiene como cota superior $q^k - 1$ donde q es el cardinal del cuerpo y k el grado del polinomio, también hemos visto ya las ventajas de tomar polinomios irreducibles.

Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible mónico, el anillo $A = \mathbb{F}_q[x]/(f)$, es un cuerpo y por tanto su grupo de unidades coincide con el conjuto de elementos no nulos:

$$(\mathbb{F}_q[x]/(f))^* = \mathbb{F}_q[x]/(f) \backslash \{0\}.$$

Ahora bien, como sabemos que si K es un cuerpo cualquiera y G un subgrupo finito de $(K^*, \cdot)$, entonces G es cíclico, tenemos que existe un elemento $\alpha \in \mathbb{F}_q[x]/(f)$ con $ord(\alpha) = q^k - 1$; donde k es el grado del polinomio f. Diremos que α es un elemento primitivo de $\mathbb{F}_{q^k}$. Nótese que, en general, si $K \subset L$ es una extensión de cuerpos un elemento $\beta \in L$ es un elemento primitivo de la extensión si $L = K(\beta)$. Sin embargo, en el caso de cuerpos finitos, decimos que un elemento $\alpha \in \mathbb{F}_{q^k}$ es un elemento primitivo de $\mathbb{F}_{q^k}$ si es un generador del grupo multiplicativo del cuerpo.

Definición 3.15. Un polinomio $f \in \mathbb{F}_q[x]$ de grado positivo $m \geqslant 1$ se dice que es primitivo sobre $\mathbb{F}_q$ si es el polinomio mínimo de un elemento primitivo de $\mathbb{F}_{q^m}$.

La siguiente caracterización de los polinomios primitivos justifica su uso en nuestro contexto.

Teorema 3.16. *Sea $f \in \mathbb{F}_q[x]$ un polinomio de grado $m \geqslant 1$ en $\mathbb{F}_q$. Entonces, f es primitivo si, y sólo si, es mónico, $f(0) \neq 0$ y $ord(f) = q^m - 1$.*

Demostración. Supongamos que $f \in \mathbb{F}_q[x]$ es un polinomio primitivo en $\mathbb{F}_q$, entonces f es mónico y $f(0) \neq 0$ ya que ha de ser el polinomio mínimo de un elemento primitivo de $\mathbb{F}_q^m$. Además, por eso y por el teorema 3.6, tenemos

que el orden es $q^m - 1$.
Recíprocamente, primero vamos a ver que es irreducible. Supongamos que f, cumpliendo las hipótesis, fuera reducible sobre $\mathbb{F}_q$; entonces tenemos dos opciones: o es una potencia de un polinomio irreducible o lo podemos escribir como producto de dos polinomios coprimos. En el primer caso, por el teorema 3.12, $ord(f) = ep^t$ donde e es el orden del polinomio de la base y p la característica del cuerpo, pero en ese caso, p dividiría a $q^m - 1$ y no puede ser. En el segundo, $f = gh$ y si $e_g = ord(g)$ y $e_f = ord(f)$ tendremos que por el teorema 3.13, el $ord(f) = \text{mcm}(e_g, e_h)$; en particular, $ord(f) \leqslant e_g e_h$. También por la proposición 3.4, tenemos que $e_g \leqslant q^{m_g} - 1$ y $e_h \leqslant q^{m_h} - 1$, siendo m_g y m_h los grados de g y h respectivamente. Uniendo todo llegamos a que

$$ord(f) \leqslant e_g e_h \leqslant (q^{m_g} - 1)(\leqslant q^{m_h} - 1) < q^{m_g m_h} - 1 = q^m - 1,$$

y no puede ser ya que el orden era igual a $q^m - 1$. Luego ya podemos concluir que el polinomio es irreducible y con eso tenemos todo porque por el lema 3.6 el polinomio f es el polinomio mínimo de un elemento primitivo de $\mathbb{F}_{q^m}$. □

Definición 3.17. Una sucesión de recurrencia lineal homogénea de orden k, en $\mathbb{F}_q$, $\{s_n\}_{n=0}^{\infty}$ cuyo polinomio característico es primitivo sobre $\mathbb{F}_q$ y con vector de estados iniciales distinto de cero, se la llama sucesión de periodo maximal en $\mathbb{F}_q$.

El siguiente resultado garantiza que la cota del periodo se alcanza.

Teorema 3.18. *Toda sucesión de periodo maximal de orden k en $\mathbb{F}_q$ es periódica y su periodo mínimo es igual a $q^k - 1$.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de periodo maximal de orden k en $\mathbb{F}_q$. Por el teorema 3.9, nuestra sucesión $\{s_n\}_{n=0}^{\infty}$ es periódica con periodo igual al orden de f. Además el teorema 3.16 nos dice que este orden vale exactamente $q^k - 1$. □

Nota 3.19. Una de las hipótesis del teorema 3.9 es que $f(0) \neq 0$ y nosotros no lo tenemos como hipótesis; la razón es que el hecho de que sea primitivo lleva intrínseco esta propiedad como hemos demostrado en el teorema 3.16. A las secuencias de periodo maximal también se las llama *secuencias de Bruijin.*

> Por lo que las secuencias cifrantes con periodo más largo las obtenemos cuando el polinomio es primitivo. Por suerte tenemos garantía de que siempre vamos a poder tomar un polinomio primitivo ya que el número de ellos de grado k sobre $\mathbb{F}_q$ es $\phi(q^k - 1)/k$, como consecuencia del teorema 3.1.

Ejemplo 3.20. En el ejemplo que acabamos de ver, el 3.10, teníamos una sucesión de orden 4 en $\mathbb{F}_3$ y el periodo era 5. Si en vez de ese polinomio ca rac te rís ti co, nuestra sucesión tuviese $f(x) = x^4 + x + 2 \in \mathbb{F}_3$, tendría periodo 80 tomando un vector de estados iniciales no nulo cualquiera. Y no solo eso, si no que el hecho de que el periodo sea $q^k - 1$, hace que todos los posibles vectores de $\mathbb{F}_q^k$ no nulos aparezcan en los $q^k - 1$ primeros elementos de la sucesión.
Esta gran diferencia entre el valor de los periodos nos tiene que hacer reflexionar en la gran ventaja que hay entre elegir un polinomio característico primitivo y otro que no lo es.

3.3. Polinomio mínimo

Como ya vimos, el polinomio característico de una sucesión de recurrencia lineal no es único. El polinomio no es único ya que si nuestra sucesión tiene periodo r, los polinomios $x^r - 1$, $x^{2r} - 1$, $x^{3r} - 1$, etc, también son polinomios característicos de la sucesión. ¿Habrá alguna relación entre ellos? La respuesta, de nuevo, es afirmativa.

Teorema 3.21. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$. Entonces existe un único polinomio mónico $m(x) \in \mathbb{F}_q[x]$ que verifica la siguiente propiedad: un polinomio $f(x) \in \mathbb{F}_q[x]$ de grado positivo es el polinomio característico de la sucesión si, y sólo si, $m(x)$ divide a $f(x)$.*

Demostración. Esta demostración la vamos a dividir en dos partes. En la primera vamos a definir un polinomio $m(x)$, el cual veremos que es único y en la segunda, veremos que satisface la propiedad deseada.
Tomamos $f_0(x) \in \mathbb{F}_q[x]$ un polinomio característico de una sucesión de recurrencia lineal homogénea de orden k y sea $h_0(x) \in \mathbb{F}_q[x]$ el polinomio inicial (ver (2.12) en el teorema 2.31) de esta sucesión. Sea $d(x) = \text{mcd}(f_0, h_0)$ y $m(x) = f_0(x)/d(x)$, entonces tenemos que $f_0(x) = d(x)m(x)$ y $g_0(x) = b(x)m(x)$. Ya tenemos definido $m(x)$ cuya unicidad es evidente dado que lo hemos definido como el cociente de dos polinomios mónicos. Ahora tenemos que ver que cumple la propiedad enunciada.
$\longrightarrow$ Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio característico cualquiera de nuestra sucesión y sea $h(x) \in \mathbb{F}_q[x]$ el polinomio inicial definido en 2.12 determinado por los coeficientes del polinomio característico f. Por el teorema 2.28 sabemos que la función generatriz $G(x)$ verifica

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

siendo g_0 y g polinomios inicial en la forma enunciada en el teorema 2.28. Haciendo el producto en cruz tenemos que $g(x)f_0^*(x) = g_0(x)f^*(x)$. Su pon

ga mos que r es el grado del polinomio f y r_0 el de f_0 utilizando la igualdad 2.13 tenemos que

$$\begin{aligned} h(x)f_0(x) &= -x^{r-1}g(\tfrac{1}{x})x^{r_0}f_0^*(\tfrac{1}{x}) \\ &= -x^{r_0-1}g_0(\tfrac{1}{x})x^r f^*(\tfrac{1}{x}) \\ &= h_0(x)f(x), \end{aligned}$$

por lo tanto $h(x)m(x) = b(x)f(x)$ y como $m(x)$ y $b(x)$ son primos entre sí, $m(x)$ divide a $f(x)$.

$\longleftarrow$ Recíprocamente, supongamos ahora que $f(x) \in \mathbb{F}_q[x]$ es un polinomio mónico divisible por $m(x) \in \mathbb{F}_q[x]$; tenemos entonces, $f(x) = m(x)c(x)$, para un cierto polinomio $c(x) \in \mathbb{F}_q[x]$. Del mismo modo que en la otra implicación tenemos que $h_0(x)m(x) = b(x)f_0(x)$. Si ahora t es el grado de $m(x)$, aplicando una vez más 2.13 obtenemos que

$$\begin{aligned} g_0(x)m^*(x) &= -x^{r_0-1}h_0(\tfrac{1}{x})x^t m(\tfrac{1}{x}) \\ &= -x^{t-1}b(\tfrac{1}{x})x^{r_0}f_0(\tfrac{1}{x}) \\ &= a(x)f_0^*(x), \end{aligned}$$

usando ahora el teorema 2.28 la función generatriz es

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

Para concluir con el recíproco de este teorema, veamos que el grado del numerador es estrictamente menor que el grado del denominador

$$\begin{aligned} \deg(a(x)c^*(x)) &= \deg(a(x)) + \deg(c^*(x)) \\ &< \deg(m(x)) + \deg(c(x)) \\ &= \deg(f(x)). \end{aligned}$$

Entonces $f(x)$ es un polinomio característico de la sucesión $\{s_n\}_{n=0}^{\infty}$. $\square$

El polinomio $m(x)$ está unívocamente determinado con la caracterización que acabamos de ver.

Definición 3.22. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal de orden k en $\mathbb{F}_q$. El polinomio $m(x) \in \mathbb{F}_q[x]$ descrito en el teorema anterior se llama polinomio mínimo de la sucesión. Si la sucesión es la idénticamente nula decimos que el polinomio mínimo es el polinomio constante igual a 1.

En definitiva, lo que estamos diciendo es que el polinomio mínimo de una sucesión es el polinomio característico mónico de menor grado. La prueba del teorema nos proporciona una forma constructiva de calcular el polinomio mínimo, en la práctica para calcularlo sólo hay que hacer las divisiones adecuadas.

Al grado d del polinomio mínimo también se le llama complejidad lineal ya que es la longitud mínima del LFSR que implementa a la sucesión de recurrencia lineal. Pero donde más importancia tiene la complejidad lineal es en la implementación del algoritmo de Berlekamp-Massey que veremos más adelante.

Ejemplo 3.23. Hemos de tener cuidado y no dejarnos llevar por la intuición ya que el polinomio mínimo no tiene porqué ser irreducible. En efecto, sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden 4 en $\mathbb{F}_3$ que satisface $s_{n+4} = s_{n+3} + s_{n+1}$ y con vector de estados iniciales $\mathbf{s}_0 = (0, 1, 0, -1)$. El polinomio característico es $f(x) = x^4 - x^3 - x = x(x^3 - x^2 - 1) \in \mathbb{F}_3[x]$. El polinomio x no es característico de la sucesión ya que si lo fuera no daría la sucesión $0\,1\,0\,1\,\ldots$. Y el polinomio $x^3 - x^2 - 1$ ya que nos daría $0\,1\,0\,0\,1\,0\,\ldots$ y ninguna de estas es la $0\,1\,0\,-1\,0\,0\,-1\,-1\,-1\,\ldots$. Por lo tanto, f es el polinomio mínimo y no es irreducible.

Como ya nos podíamos ir imaginando, cuando el polinomio característico de una sucesión es irreducible, este es justamente el polinomio mínimo.

Proposición 3.24. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea en $\mathbb{F}_q$ y sea $f(x) \in \mathbb{F}_q[x]$ un polinomio característico de la sucesión. Entonces, si f es irreducible sobre $\mathbb{F}_q$ entonces f es el polinomio mínimo de la sucesión.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea, f un polinomio característico y m el polinomio mínimo. Por el teorema 3.21, el polinomio mínimo divide al polinomio característico de la sucesión. Por ello, como f es un polinomio irreducible en $\mathbb{F}_q$, tenemos dos opciones o $m = 1$ o $m = f$; la primera opción la descartamos ya que si el polinomio mínimo fuese el 1, la sucesión de recurrencia lineal homogénea sería la idénticamente nula. Por tanto, $m(x) = f(x)$. □

Otra forma de calcular el periodo mínimo de la sucesión es calculando el orden del polinomio mínimo.

Proposición 3.25. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ y sea $m(x) \in \mathbb{F}_q[x]$ el polinomio mínimo. Entonces el periodo mínimo de la sucesión es igual al orden de $m(x)$.*

Demostración. Supongamos que la sucesión $\{s_n\}_{n=0}^{\infty}$ tiene periodo mínimo r y preperiodo n_0. Entonces, como $s_{n+r} = s_n$ para todo $n \geqslant n_0$, también $s_{n+n_0+r} = s_{n+n_0}$ para todo $n \geqslant 0$. Por ello podemos decir que el polinomio $f(x) = x^{n_0+r} - x^{n_0}$ es un polinomio característico de la sucesión. Aplicando el teorema 3.21, $m(x)$ divide a $x^{n_0+r} - x^{n_0} = x^{n_0}(x^r - 1)$. Si escribimos $m(x) = x^h g(x)$ con $g(0) \neq 0$, tendremos entonces que $h \leqslant n_0$ y $g(x)$ divide a $x^r - 1$. Aplicando la definición de orden tenemos que $ord(m(x)) = ord(g(x)) \leqslant r$.

Por otro lado, por el teorema 3.5, el periodo mínimo divide al orden del polinomio característico, i.e. $r \mid ord(m(x))$. Así ya podemos concluir que $r = ord(m(x))$. □

Este resultado nos permite calcular el periodo mínimo de una forma mucho más eficiente que como lo estábamos haciendo hasta ahora; ya que si por ejemplo el polinomio mínimo es irreducible, el orden va a ser un divisor de $q^k - 1$ como vimos en el primer capítulo y si es primitivo va a ser justamente $q^k - 1$. Por lo que una vez que sabemos el orden ya casi tenemos el periodo mínimo de la sucesión.

Ejemplo 3.26. Consideramos en $\mathbb{F}_5$ la sucesión de recurrencia lineal de orden 2 cuyo polinomio característico es $f(x) = x^2 + 4x + 1$ y con vector de estados iniciales distinto de cero. Puesto que es irreducible $f(x)$ es el polinomio mínimo. Un sencillo cálculo nos hace comprobar que el orden de f es 6. Por lo que ya podemos concluir aplicando el resultado anterior que el periodo mínimo de la sucesión es 6.

Ya vimos en un ejemplo de la sección pasada que dos polinomios nos podían dar la misma sucesión, pero una siendo la desplazada de la otra. Si esto ocurriese, los polinomios mínimos también tienen algún tipo de relación.

Proposición 3.27. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ y $\{s_b, s_{b+1}, \dots\}$ con b un entero positivo, la sucesión desplazada. Si $m_1(x)$ es el polinomio mínimo de la desplazada y $m(x)$ el polinomio mínimo de la sucesión original, entonces $m_1(x)$ divide a $m(x)$. En el caso en que $\{s_n\}_{n=0}^{\infty}$ sea periódica, los polinomios mínimos coinciden i.e.: $m_1(x) = m(x)$.*

Demostración. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ y $m(x)$ el polinomio mínimo de la sucesión. Por el teorema 3.21, para probar la primera afirmación bastaría probar que la relación que define el polinomio $m(x)$ también la satisface la sucesión trasladada $\{s_{b+n}\}_{n=0}^{\infty}$; porque así $m(x)$ sería polinomio característico de la trasladada y su polinomio mínimo $m_1(x)$ lo dividiría. Pero esto es obvio por ser la sucesión trasladada. Veamos que en el caso en que la sucesión es periódica el polinomio mínimo coincide. Tomamos

$$s_{n+b+k} = a_{k-1}s_{n+b+k-1} + a_{k-2}s_{n+b+k-2} + \cdots + a_0 s_{n+b},$$

para $n = 0, 1, \dots$, la relación de recurrencia lineal de la sucesión trasladada. Sea r el periodo mínimo de la sucesión de partida $\{s_n\}_{n=0}^{\infty}$, entonces $s_{n+r} = s_n$, para $n \geqslant 0$. Si tomamos ahora c un entero tal que $cr \geqslant b$ y sustituimos n por $n + cr - b$ en la relación de recurrencia lineal de la sucesión trasladada, tenemos que se verifica

$$s_{n+cr+k} = a_{k-1}s_{n+cr+k-1} + a_{k-2}s_{n+cr+k-2} + \cdots + a_0 s_{n+cr},$$

ahora, como tenemos que r es el periodo de la sucesión y c es un entero positivo se verifica $s_{n+cr} = s_n$ y llevándolo a la relación de recurrencia lineal anterior, obtenemos que

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n,$$

es decir, la relación de recurrencia lineal original, $\{s_n\}_{n=0}^{\infty}$, satisface la misma relación de recurrencia que la trasladada y por el teorema 3.21 el polinomio mínimo es el mismo. □

Otra forma de saber si el polinomio característico es el polinomio mínimo de la sucesión es mediante el estudio de los vectores de estados.

Proposición 3.28. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea de orden k en $\mathbb{F}_q$ con $f(x) \in \mathbb{F}_q[x]$ el polinomio característico. Entonces f es el polinomio mínimo de la sucesión si, y sólo si, los k primeros vectores de estados $\{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}\}$ son linealmente independientes sobre $\mathbb{F}_q$.*

Demostración. ⟵ Supongamos que los vectores de estados $\{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}\}$ son linealmente independientes sobre $\mathbb{F}_q$. Puesto que $\mathbf{s}_0 \neq 0$, el polinomio mínimo tiene grado positivo ya que la sucesión no es la idénticamente nula. Supongamos ahora que f no es el polinomio mínimo de la sucesión, entonces la sucesión $\{s_n\}_{n=0}^{\infty}$ satisface una relación de recurrencia lineal de orden m con $0 < m < k$ ya el polinomio mínimo sería un divisor propio del polinomio característico f. Es decir

$$s_{n+m} = b_{m-1}s_{n+m-1} + b_{m-2}s_{n+m-2} + \cdots + b_0 s_n,$$

para $n = 0, 1, \ldots$ y con $b_i \in \mathbb{F}_q$ para $i = 0, 1, \ldots, m-1$, no todos nulos. Esta relación implica

$$\mathbf{s}_m = b_{m-1}\mathbf{s}_{m-1} + b_{m-2}\mathbf{s}_{m-2} + \cdots + b_0\mathbf{s}_0,$$

por lo que los vectores son linealmente dependientes, en contra de la hipótesis. Luego f ha de ser el polinomio mínimo.
⟶ Recíprocamente, supongamos que nuestro polinomio $f(x)$ es el polinomio mínimo de la sucesión y que los vectores $\{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}\}$ son linealmente dependientes sobre $\mathbb{F}_q$. Entonces existen escalares $b_0, b_1, \ldots b_{k-1} \in \mathbb{F}_q$ no todos nulos tales que $b_{k-1}\mathbf{s}_{k-1} + b_{k-2}\mathbf{s}_{k-2} \cdots + b_0\mathbf{s}_0 = \mathbf{0}$. Utilizando la relación del lema 2.15, tenemos

$$b_{k-1}\mathbf{s}_{n+k-1} + b_{k-2}\mathbf{s}_{n+k-2} \cdots + b_0\mathbf{s}_n = \mathbf{0}$$

para $n = 0, 1, \ldots$. Sea j el mayor entero tal que $b_j \neq 0$, entonces la sucesión satisface una relación de recurrencia de orden j con $j < k$ y el polinomio tiene grado j. Esto contradice la hipótesis de que el polinomio f es el polinomio mínimo de la sucesión. □

Gracias a este resultado junto con el teorema 2.22, podemos afirmar que el polinomio mínimo de una sucesión de impulso-respuesta es igual al polinomio característico de su relación de recurrencia lineal.

3.4. El algoritmo de Berlekamp-Massey

En las secciones anteriores hemos estudiado los polinomios característicos que nos permiten obtener sucesiones en recurrencia lineal con periodos óptimos, permitiendo de esta forma "secuencias cifrantes" con buenas pers pec ti vas, al menos desde el punto de vista de su periodo. No obstante, la Proposición 3.28 es la clave que nos permitirá establecer fuertes límites a la utilidad criptográfica de estas sucesiones.

Supongamos que $\{s_n\}_{n=0}^{\infty}$ tiene complejidad lineal k y su polinomio mínimo es $f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0$. Dados, $n \geq 0$, $r \geq 1$, denotaremos por $\mathcal{D}_n^{(r)}$ la matriz

$$\mathcal{D}_n^{(r)} = \begin{pmatrix} s_n & s_{n+1} & \cdots & s_{n+r-1} \\ s_{n+1} & s_{n+2} & \cdots & s_{n+r} \\ \vdots & \vdots & & \vdots \\ s_{n+r-1} & s_{n+r} & \cdots & s_{n+2r-2} \end{pmatrix}.$$

La Proposición 3.28 permite asegurar que el determinante $D_0^{(k)} = \det(\mathcal{D}_0^{(k)})$ de la matriz $\mathcal{D}_0^{(k)}$ es no nulo. Además, tendremos que

$$\mathcal{D}_0^{(k)}(a_0, \ldots, a_{k-1})^t = (s_k, \ldots, s_{2k-1})^t ,$$

es decir, el vector $(a_0, \ldots, a_{k-1})$ es la solución única del sistema de ecuaciones $\mathcal{D}_0^{(k)}\mathbf{X}^t = \mathbf{s}_k^t$. Es claro que tenemos el mismo resultado si tomamos la matriz $\mathcal{D}_n^{(k)}$ y el sistema lineal $\mathcal{D}_n^{(k)}\mathbf{X}^t = \mathbf{s}_{n+k}^t$ para un $n \geq 0$ arbitrario.

Dicho de otra forma, si conocemos un fragmento de $2k$ bits consecutivos $(m_n, \ldots, m_{n+2k-1})$ y su correspondiente cifrado $(c_n, \ldots, c_{n+2k-1})$ con $(s_n, \ldots, s_{n+2k-1})$ (es decir, $c_i = s_i + m_i$ para $n \leq i \leq n + 2k - 1$) podemos recuperar $2k$ bits consecutivos $(s_n, \ldots, s_{n+2k-1})$ de la sucesión y, resolviendo el sistema anterior, conocer el polinomio mínimo. Por tanto el sistema de cifrado es claramente vulnerable a un ataque con texto claro conocido de longitud relativamente baja: el doble de la complejidad lineal.

El algoritmo de Berlekamp-Massey nos proporciona un método eficiente, basado en el resultado anterior, para, a partir de un fragmento suficientemente largo de la sucesión $\{s_n\}_{n=0}^{\infty}$ encontrar el polinomio mínimo. Hechas estas definiciones, veamos el principal objetivo de este capítulo.

En la teoría que hemos expuesto hasta ahora partíamos siempre de conocer el polinomio característico, el polinomio mínimo o la matriz compañera y después con un vector de estados iniciales, obteníamos toda la sucesión. En

esta sección el problema que vamos a tratar es el contrario. Vamos a partir de una sucesión $\{s_n\}_{n=0}^{\infty}$ (sólo la cadena de números) en $\mathbb{F}_q$ y nuestro objetivo va a ser saber si esta es una sucesión de recurrencia lineal homogénea o no y, en el caso en que lo sea, calcular su polinomio mínimo.

Comencemos dando un criterio que permite identificar las sucesiones que son de recurrencia lineal homogéneas.

Definición 3.29. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de elementos de $\mathbb{F}_q$. Para los enteros $n \geqslant 0$ y $r \geqslant 1$ definimos el determinante de Hankel $D_n^{(r)}$por

$$D_n^{(r)} = \begin{vmatrix} s_n & s_{n+1} & \cdots & s_{n+r-1} \\ s_{n+1} & s_{n+2} & \cdots & s_{n+r} \\ \vdots & \vdots & & \vdots \\ s_{n+r-1} & s_{n+r} & \cdots & s_{n+2r-2} \end{vmatrix}.$$

Lema 3.30. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión cualquiera en $\mathbb{F}_q$ y sean los enteros $n \geqslant 0$ y $r \geqslant 1$. Si $D_n^{(r)} = D_n^{(r+1)} = 0$, entonces $D_{n+1}^{(r)} = 0$.*

Demostración. Puesto que $D_n^{(r)} = 0$ tenemos que los vectores columna de la matriz, $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$; siendo $\mathbf{s}_i = (s_i, s_{i+1}, \ldots, s_{i+r-1}) \in \mathbb{F}_q^r$, son linealmente dependientes sobre $\mathbb{F}_q$. Para probar que $D_{n+1}^{(r)} = 0$ tenemos que probar que los vectores $\mathbf{s}_{n+1}, \mathbf{s}_{n+2}, \ldots, \mathbf{s}_{n+r}$ son linealmente dependientes. Si $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$ son linealmente dependientes entonces también lo son $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$. En otro caso, el vector $\mathbf{s}_n$ es una combinación lineal de $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$. Si denotamos por $\mathbf{s}'_i = (s_i, s_{i+1}, \ldots s_{i+r}) \in \mathbb{F}_q^r$, $n \leq i \leq r$, los vectores columna del determinante $D_n^{(r+1)}$, los vectores $\mathbf{s}'_n, \mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r}$ son linealmente dependientes sobre $\mathbb{F}_q$ ya que el determinante de Hankel $D_n^{(r+1)}$ es nulo. Distingamos dos casos:
Si los vectores $\mathbf{s}'_n, \mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r-1}$ son linealmente dependientes sobre $\mathbb{F}_q$, entonces con la aplicación proyección

$$\mathbb{F}_q^{r+1} \longrightarrow \mathbb{F}_q^r\,; \quad (a_0, \ldots, a_r) \longrightarrow (a_1, \ldots, a_r)\ ,$$

probamos que los vectores $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r}$ son linealmente dependientes y en consecuencia $D_{n+1}^{r} = 0$.
En otro caso $\mathbf{s}'_n, \mathbf{s}'_{n+1}, \ldots, \mathbf{s}'_{n+r-1}$ son linealmente independientes y $\mathbf{s}'_{n+r}$ es una combinación lineal de los otros r vectores, utilizando la aplicación

$$\mathbb{F}_q^{r+1} \longrightarrow \mathbb{F}_q^r\,; \quad (a_0, \ldots, a_r) \longrightarrow (a_0, \ldots, a_{r-1})\ ,$$

probamos que $\mathbf{s}_{n+r}$ es una combinación lineal de $\mathbf{s}_n, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r-1}$. Pero $\mathbf{s}_n$ es combinación lineal de $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r}$ y por tanto $\mathbf{s}_{n+r}$ es también combinación lineal de $\mathbf{s}_{n+1}, \ldots, \mathbf{s}_{n+r}$. Por tanto $D_n^{(r)} = 0$. □

Demos los dos resultados que caracterizan a las sucesiones de recurrencia lineal homogéneas sobre $\mathbb{F}_q$.

Teorema 3.31. *Una sucesión $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_q$ es una sucesión de recurrencia lineal si, y sólo si, existe un entero positivo r tal que $D_n^r = 0$ para todo $n \geqslant 0$ salvo un número finito.*

Demostración. Puesto que ya dimos un procedimiento para transformar una sucesión no homogénea de orden k a una homogénea de orden $k+1$, la demostración la haremos para el caso homogéneo.
$\Longrightarrow$ Supongamos que $\{s_n\}_{n=0}^{\infty}$ es una sucesión de recurrencia lineal homogénea de orden k, y sea (2.2) la relación de recurrencia que satisface. Para cualquier $n \geqslant 0$ consideramos $D_n^{(k+1)}$ el determinante de Hankel a so cia do. Puesto que la sucesión satisface la relación de recurrencia lineal citada, te nemos que las $k+1$ primeras columnas son una combinación lineal de las k primeras y en consecuencia $D_n^{(k+1)} = 0$.
$\Longleftarrow$ Recíprocamente, sea $k+1$ el menor entero positivo tal que el determinante de Hankel $D_n^{k+1} = 0$ se anula para todo n mayor o igual que un cierto entero m. Si $k+1 = 1$ habríamos terminado ya que el determinante se convierte en el valor absoluto del término n-ésimo de la sucesión que se anula para todo n positivo salvo para una cantidad finita; por lo que si tomamos m el mayor de todos los subíndices para los que s_n es distinto de cero, tenemos que $s_n = 0$ para $n \geqslant m$ y obviamente es una sucesión de recurrencia lineal homogénea. Por lo que vamos a suponer que $k+1 > 1$. Si tuviésemos un determinante de Hankel $D_{n_0}^{(k)} = 0$ para un cierto $n_0 \geqslant m$ entonces todos los determinantes a partir de este n_0 serían nulos y esto iría en contra de la minimalidad de k. Por ello $D_n^{(k)} \neq 0$ para todo $n \geqslant m$. Si tomamos $\mathbf{s}_n = (s_n, s_{n+1}, \ldots s_{n+k})$, los vectores $\mathbf{s}_n$,$\mathbf{s}_{n+1}, \ldots \mathbf{s}_{n+k}$ son li ne al men te dependientes ya que son las columnas del determinante $D_n^{(k+1)}$ que ya sabemos que es nulo. Por otra parte como $D_n^{(k)} \neq 0$ los vectores $\mathbf{s}_n$,$\mathbf{s}_{n+1}, \ldots \mathbf{s}_{n+k-1}$ son linealmente independientes sobre $\mathbb{F}_q$, así que $\mathbf{s}_{n+k}$ lo podemos escribir como una combinación lineal de los otros $n+k-1$ vectores. Entonces de forma recursiva es fácil ver que para cada $n \geqslant m$ $\mathbf{s}_n$ lo podemos escribir como combinación lineal de los k primeros vectores $\mathbf{s}_m, \ldots, \mathbf{s}_{m+k-1}$. Entonces para cada $n \in \{m, m+1, \ldots, m+k-1\}$ tenemos

$$a_0 s_n + a_1 s_{n+1} + \cdots + a_k s_{n+k} = 0,$$

con los a_i elementos de nuestro cuerpo $\mathbb{F}_q$. La expresión anterior es equivalente a

$$a_0 s_{n+m} + a_1 s_{n+m+1} + \cdots + a_k s_{n+m+k} = 0 \quad \text{para todo } n \geqslant 0$$

Y esto es lo mismo que decir que la sucesión $\{s_n\}_{n=0}^{\infty}$ satisface una relación de recurrencia lineal homogénea como la que tenemos definida en (2.2) de orden a lo sumo $m+k$. □

Teorema 3.32. *Una sucesión $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_q$ es una sucesión de recurrencia lineal homogénea con polinomio mínimo de grado k si, y sólo si, $D_0^{(r)} = 0$ para todo $r \geqslant k+1$, siendo $k+1$ el menor entero positivo para el que se tiene esta condición.*

Demostración. $\Longrightarrow$ Sin pérdida de generalidad vamos a suponer que $k \geqslant 1$ ya que si la sucesión es la idénticamente nula el resultado es trivial. El determinante $D_0^{(r)}$ se anula para todo $r \geqslant k+1$ ya que la fila $k+1$-ésima es combinación lineal de las k primeras. Además cuando $r = k$ tenemos que el determinante es distinto de cero ya que como ilustra la proposición 3.28 los k primeros vectores de estados son linealmente independientes.
$\Longleftarrow$ Veamos ahora el recíproco. De forma recurrente en n por el lema 3.30, $D_n^{(r)} = 0$ para todo $r \geqslant k+1$ y $n \geqslant 0$. En particular $D_n^{(k+1)} = 0$ para todo $n \geqslant 0$ y por el teorema anterior nuestra sucesión $\{s_n\}_{n=0}^{\infty}$ es de recurrencia lineal. Finalmente, si el polinomio mínimo tiene grado d, la anulación del determinante también se cumple para todo $r \geqslant d+1$ y puesto que $d+1$ es el menor entero para el que se verifica nuestra hipótesis, k ha de ser igual a d. □

Lógicamente no podemos comprobar que todos los determinantes sean nulos a partir del $k+1$ ya que físicamente es imposible. Por esos hemos de entender estos dos teoremas que acabamos de ver como criterio negativo para saber si una sucesión es de recurrencia o no. Es decir, si encontramos un determinante D_0^r que sea distinto de cero pues ya sabemos que la sucesión dada no era de recurrencia lineal homogénea de orden $\leqslant r-1$.

Esta relación tan estrecha entre los determinantes de Hankel y las sucesiones de recurrencia lineal homogéneas fue dada por Pólya y Szegö. Además el segundo teorema que hemos dado fue probado por primera vez por Kronecker en el libro *Zur Theorie der Elimination einer Variabeln aus zwei algebraischen Gleichungen* para el caso real, aunque en realidad servía para cualquier cuerpo.
Obviamente el problema que tenemos que resolver ahora es cómo calculamos este polinomio mínimo. Para ello vamos a exponer un algoritmo recursivo cuya entrada ha de ser una cota superior del grado del polinomio mínimo y los términos de la sucesión.

El algoritmo de Berlekamp-Massey

Dada una sucesión $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_q$ de la que ya sabemos que es de recurrencia lineal, vamos a dar un procedimiento para buscar su polinomio mínimo en un numero finito de pasos. Este algoritmo es el ya mencionado, "algoritmo de Berlekamp-Massey". Para ello necesitamos una cota del grado

del polinomio mínimo (hemos de advertir en la práctica no siempre vamos a tener esta cota).
Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de elementos en $\mathbb{F}_q$ y sea $G(x) = \sum_{n=0}^{\infty} s_n x^x$ la función generatriz de la sucesión. Para $j = 0, 1, \ldots, 2k$, vamos a construir recursivamente polinomios $g_j(x)$ y $h_j(x)$ en $\mathbb{F}_q[x]$ y enteros m_j y los $b_j \in \mathbb{F}_q$. Iniciamos el algoritmo con

$$g_0(x) = 1, \quad h_0(x) = x \quad \text{y} \quad m_0 = 0 \quad b_0 = s_0$$

Para $j = 0, 1, \ldots$

$$g_{j+1}(x) := g_j(x) - b_j h_j(x),$$

$$h_{j+1} := \begin{cases} b_j^{-1} x g_j(x) & \text{si } b_j \neq 0 \text{y } m_j \geqslant 0, \\ x h_j(x) & \text{en otro caso,} \end{cases}$$

$$m_{j+1} := \begin{cases} -m_j & \text{si } b_j \neq 0 \text{y } m_j \geqslant 0, \\ m_j + 1 & \text{en otro caso,} \end{cases}$$

$$b_{j+1} := \text{ coeficiente de } x^{j+1} \text{ en } g_{j+1} G(x)$$

A estas igualdades las llamaremos esqueleto del algoritmo. Si $\{s_n\}_{n=0}^{\infty}$ es una sucesión cuyo polinomio mínimo tiene grado k tenemos que el polinomio $g_{2k}(x) \in \mathbb{F}_q[x]$ es igual al polinomio recíproco del polinomio mínimo de la sucesión. Por lo tanto, si $m(x)$ es el polinomio mínimo y sabemos que tiene grado k, tenemos que está dado por $m(x) = x^k g_{2k}(\frac{1}{x})$. Si lo único que sabemos es que el polinomio mínimo tiene grado $\leqslant k$, entonces tomando $r = \lfloor k + \frac{1}{2} - \frac{1}{2} m_{2k} \rfloor$,tenemos que $m(x) = x^r g_{2k}(\frac{1}{x})$. En cualquiera de los dos casos lo único que necesitamos es conocer los $2k$ primeros términos de la sucesión por eso en el algoritmo en vez de tomar la función generatriz, basta con tomarla truncada en el grado $2k - 1$. Esto no es otra cosa que sustituir $G(x)$ por

$$G_{2k-1}(x) = \sum_{n=0}^{2k-1} s_n x^n.$$

La complejidad lineal del LFSR asociado a la sucesión de recurrencia homogénea es k, es decir, el grado del polinomio mínimo de la sucesión. Si conocemos $2k$ términos consecutivos de la sucesión, con el algoritmo de Berlekamp-Massey podemos obtener el polinomio mínimo y así construir el LFSR. Por eso en criptografía al grado del polinomio mínimo lo llamamos así y por eso es necesario que la complejidad lineal sea lo mayor posible. A esta complejidad lineal la vamos a denotar por $L(\sigma)$ donde $\sigma = \{s_n\}_{n=0}^{\infty}$.

Implementación del algoritmo en Maple:

```
berlmass:=proc(G, dk,p)
# El usuario nos da un truncamiento de la serie generatriz
# o de la sucesion, dk el doble del grado del polinomio mínimo
# y p la característica del cuerpo

   local g,h,m,i,gg, b, invb,M ,g1 , r, F ;
   with(PolynomialTools);

# si nos lo dan como sucesión (lista) la convierto a polinomio.
if type(G,list)=true then
   F:=0;
   for i from 1 to nops(G) do
      F:=F+G[i]*x^(i-1);
   end do;
else
   F:=G;
end if;
   # arrancamos el algoritmo
   g[0]:= 1;
   gg := expand(g[0]*F);
   h[0]:= x; m[0]:= 0;  b[0]:= eval(gg, x=0);

   for i from 1 to dk do
      g[i] := expand(g[i-1]-b[i-1]*h[i-1]) mod(p);
      gg := expand(g[i]*F) mod(p);
      b[i]:=coeff(gg, x, i);

      if (b[i-1]<>0) and (m[i-1]>=0) then
              invb := 1/b[i-1] mod(p);
              h[i] := invb*x*g[i-1] mod(p);
              m[i] := -m[i-1];
      else
              h[i] := x*h[i-1] mod(p);
              m[i] := m[i-1]+1;
       end if;
     end do;
 r:=floor((dk/2)+1/2-m[dk]/2);
 g1 := eval(g[dk],x=1/x) mod(p);

# obtenemos el polinomio mínimo.
   M:=sort(expand((x^r)*g1));

end proc:
```

Antes de dar la demostración del algoritmo vamos a ver un ejemplo.

Ejemplo 3.33. Vamos a buscar la sucesión de recurrencia lineal homogénea

en $\mathbb{F}_2$ cuyos ocho primeros términos son

$$0\ 1\ 0\ 1\ 0\ 0\ 1\ 0.$$

Para ello vamos a utilizar el algoritmo de Berlekamp-Massey. La función generatriz truncada es $G_7(x) = x + x^3 + x^6$. Las etapas las vamos a recoger en la siguiente tabla:

etapa j-ésima	$g_j(x)$	$h_j(x)$	m_j	b_j
0	0	x	0	0
1	1	x^2	1	1
2	$1+x^2$	x	-1	0
3	$1+x^2$	x^2	0	0
4	$1+x^2$	x^3	1	0
5	$1+x^2$	x^4	2	1
6	$1+x^2+x^4$	$x+x^3$	-2	1
7	$1+x+x^2+x^3+x^4$	x^2+x^4	-1	0
8	$1+x+x^2+x^3+x^4$	x^3+x^5	0	1

El algoritmo nos dice que el polinomio mínimo tiene grado

$$r = \lfloor k + \frac{1}{2} - \frac{1}{2}m_{2k} \rfloor = \lfloor 4 + \frac{1}{2} \rfloor = 4,$$

por lo que nos y tenemos que el polinomio mínimo de nuestra sucesión es $m(x) = 1 + x + x^2 + x^3 + x^4$. La relación de recurrencia lineal en $\mathbb{F}_2$ es entonces para $n \geqslant 0$

$$s_{n+4} = s_{n+3} + s_{n+2} + s_{n+1} + s_n,$$

y el vector de estados iniciales $(0, 1, 0, 1)$. Además también sabemos que esta es la de menor orden. Si utilizamos el programa de Maple donde tenemos implementado el algoritmo nos da como salida
berlmass([0,1,0,1,0,0,1,0],8,2);

$$x^4 + x^3 + x^2 + x + 1.$$

Prueba de validez del algoritmo.

Para empezar lo que vamos a hacer es definir unos polinomios auxiliares $u_j, v_j \in \mathbb{F}_q[x]$ y después procederemos a hacer la demostración en cuatro etapas.
Definimos los polinomios citados recurrentemente. Iniciamos con

$$u_0(x) = 0, v_0(x) = -1 \tag{3.2}$$

y para cada $j = 0, 1, \ldots$

$$\begin{aligned} u_{j+1}(x) &= u_j(x) - b_j v_j(x), \\ v_{j+1} &= \begin{cases} b_j^{-1} x u_j(x) & \text{si } b_j \neq 0 \text{y } m_j \geqslant 0, \\ x v_j(x) & \text{en otro caso,} \end{cases} \end{aligned} \tag{3.3}$$

Destaquemos la relación tan estrecha que hay entre los del esqueleto del algoritmo y estos que acabamos de definir.
► Estudiemos los grados de los polinomios del esqueleto.
En el caso en que $b_j \neq 0$ y $m_j \geqslant 0$ tenemos que

$$\begin{aligned} \deg(g_{j+1}(x)) &\leqslant \text{máx}(\deg(g_j(x)), \deg(h_j(x))) \\ &\leqslant \tfrac{1}{2}(j + 2 + m_j) = \tfrac{1}{2}(j + 2 - m_{j+1}). \end{aligned}$$

En el otro caso, cuando no se dan alguna de las condiciones de los b_j o m_j, tenemos

$$\deg(g_{j+1}(x)) \leqslant \frac{1}{2}(j + 1 - m_j) = \frac{1}{2}(j + 2 - m_{j+1}).$$

Del mismo modo lo probamos para $h_j(x), u_j(x)$ y $v_j(x)$ Y podemos concluir por una parte que

$$\deg(g_j(x)) \leqslant \tfrac{1}{2}(j + 1 - m_j) \quad \text{y} \quad \deg(h_j(x)) \leqslant \tfrac{1}{2}(j + 2 + m_j), \tag{3.4}$$

y por otro lado

$$\deg(u_j(x)) \leqslant \tfrac{1}{2}(j - 1 - m_j) \quad \text{y} \quad \deg(v_j(x)) \leqslant \tfrac{1}{2}(j + m_j). \tag{3.5}$$

► Veamos explícitamente la relación que hay entre los polinomios auxiliares que hemos definido y los del esqueleto del algoritmo. Lo que vamos a demostrar es que

$$g_j(x)G(x) \equiv u_j(x) + b_j x^j \bmod x^{j+1}, \tag{3.6}$$

$$h_j(x)G(x) \equiv v_j(x) + x^j \bmod x^{j+1}. \tag{3.7}$$

Para el caso $j = 0$ el resultado es evidente ya que simplemente hay que utilizar los polinomios con los que hemos arrancado la definición recursiva de los polinomios tanto del esqueleto como los auxiliares de esta demostración. Así que ahora lo haremos para un $j \geqslant 0$ arbitrario.

$$\begin{aligned} g_{j+1}(x)G(x) &= g_j(x)G(x) - b_j h_j(x)G(x) \\ &\equiv u_j(x) + b_j x^j + c_{j+1} x^{j+1} \\ &\quad -b_j(v_j(x) + x^j + d_{j+1} x^{j+1}) \bmod x^{j+2} \\ &\quad \equiv u_{j+1}(x) + (c_{j+1} + d_{j+1}) x^{j+1} \bmod x^{j+2}, \end{aligned}$$

para unos ciertos coeficientes $c_j, d_j \in \mathbb{F}_q$ que los obtenemos al desarrollar las expresiones de la primera igualdad. Razonando del mismo modo, pero distinguiendo los dos casos obtenemos la congruencia 3.7. Además también tenemos, por como hemos definido los enteros m_j que $\mid m_j \mid \leqslant j$ y por lo tanto, podemos probar por inducción que $\deg(u_j(x)) \leqslant j$ utilizando 3.5. Y si definimos $e_j = c_j - d_j$ para todo $j \geqslant 0$, e_j es el coeficiente de x^j en el producto $g_j(x)G(x)$ luego $b_j = e_j$ por definición.

► Lo siguiente que vamos a probar es para todo $j \geqslant 0$

$$h_j(x)u_j(x) - g_j(x)v_j(x) = x^j, \tag{3.8}$$

ya que después lo utilizaremos para probar que el polinomio enunciado $m(x)$ en el algoritmo es, efectivamente, el polinomio mínimo de la sucesión. Sean $s(x), u(x) \in \mathbb{F}_q[x]$ dos polinomios sobre $\mathbb{F}_q$ tales que $s(x)G(x) = u(x)$ y con $s(0) = 1$. Utilizando la congruencia 3.7 tenemos

$$\begin{aligned} h_j(x)u(x) - s(x)v_j(x) &= s(x)(h_j(x)G(x) - v_j(x)) \\ &\equiv s(x)x^j \bmod x^{j+1} \equiv x^j \bmod x^{j+1}, \end{aligned}$$

dándose esta última equivalencia por $s(0) = 1$. Además para un cierto $U_j(x) \in \mathbb{F}_q[x]$ con $U_j(0) = 1$ tenemos también

$$h_j(x)u(x) - s(x)v_j(x) = x^j U_j(x) \tag{3.9}$$

De forma similar, pero con la congruencia 3.6 probamos que existe un $V_j(x) \in \mathbb{F}_q[x]$ tal que

$$g_j(x)u(x) - s(x)u_j(x) = x^j V_j(x) \tag{3.10}$$

► Supongamos que $m(x)$ es el polinomio mínimo de la sucesión de recurrencia lineal $\{s_n\}_{n=0}^{\infty}$ tal que $\deg(m(x)) \leqslant k$ y sea $s(x)$ su polinomio recíproco. Por el teorema 2.28 sabemos que existe un polinomio $u(x)$ con coeficientes en $\mathbb{F}_q$ tal que $s(x)G(x) = u(x)$ y con $\deg(u(x)) \leqslant \deg(m(x)) - 1 \leqslant k - 1$. Entonces llevando estos polinomios a la relación 3.9 en el caso $j = 2k$ y utilizando las cotas de los grados de los polinomios involucrados en la igualdad obtenemos que

$$\deg(h_{2k}(x)u(x)) \leqslant \frac{1}{2}(2k + 2 + m_{2k}) + k - 1 = 2k + \frac{1}{2}m_{2k}$$

y

$$\deg(s(x)v_{2k}) \leqslant k + \frac{1}{2}(2k + m_{2k}) \leqslant 2k + \frac{1}{2}m_{2k},$$

luego el grado de la diferencia $h_{2k}(x)u(x) - s(x)v_{2k}$ tendrá la siguiente cota

$$\deg(h_{2k}(x)u(x) - s(x)v_{2k}) = \deg(x^{2k}U_{2k}(x)) \geqslant 2k,$$

estas desigualdades sólo son posibles si $m_{2k} \geqslant 0$. Utilizando las mismas relaciones que hemos empleado para ver estas cotas, obtenemos las desigualdades

$\deg(g_{2k}(x)u(x)) \leqslant 2k - \frac{1}{2} - \frac{1}{2}m_{2k}$ y $\deg(s(x)u_{2k}(x)) \leqslant 2k - \frac{1}{2} - \frac{1}{2}m_{2k}$. Por lo que por la relación 3.10, tenemos

$$\deg(x^{2k}V_{2k}(x)) = \deg(g_{2k}(x)u(x) - s(x)u_{2k}(x)) < 2k,$$

pero esta desigualdad estricta sólo es posible si $V_{2k} = 0$. Lo llevamos a 3.10 y obtenemos $g_{2k}(x)u(x) = s(x)u_{2k}(x)$. Multiplicamos ahora 3.9 cuando $j = 2k$ por $g_{2k}(x)$ y resulta cuando agrupamos

$$\begin{aligned} &h_{2k}(x)g_{2k}(x)u(x) - s(x)g_{2k}(x)v_{2k} \\ &\quad = s(x)(h_{2k}(x)u_{2k}(x) - g_{2k}(x)v_{2k}) \\ &\quad = x^{2k}U_{2k}(x)g_{2k}(x) \\ &\quad = s(x)x^{2k}, \end{aligned}$$

luego $s(x) = U_{2k}(x)g_{2k}(x)$ y llevándolo a 3.10 $u(x) = U_{2k}(x)u_{2k}(x)$. Como $s(x)$ es el polinomio reciproco del polinomio mínimo $m(x)$ de la sucesión, por la segunda parte del teorema 2.28 tenemos que $s(x)$ y $u(x)$ son primos entre sí y por ello $U_{2k}(x)$ ha de ser un polinomio constante; de hecho constante igual a 1 ya que verificaba $U_j(0) = 1$ para todo $j \geqslant 0$. Entonces

$$s(x) = g_{2k}(x) \quad \text{y} \quad u(x) = u_{2k}(x)$$

Si $\deg(m(x)) = k$ ya podemos decir

$$m(x) = x^k s(\frac{1}{x}) = x^k g_{2k}(\frac{1}{x}).$$

Si $\deg(m(x)) = t \leqslant k$, entonces $s(x) = g_{2t}(x)$, $u(x) = u_{2t}(x)$ y $m_{2t} \geqslant 0$. Ahora bien, $\max(\deg(s(x)), 1, \deg(u(x))) \leqslant t$ y la segunda parte del teorema 2.28 implica que

$$t = \max(\deg(s(x)), 1, \deg(u(x))),$$

y por las cotas de los grados auxiliares

$$t = \max(\deg(g_{2t}(x)), 1\deg(u_{2t}(x))) \leqslant t + \frac{1}{2} - \frac{1}{2}m_{2t},$$

por lo que $m_{2t} = 0$ o 1 ya que si no, no se da la desigualdad. Además para $j \geqslant 2t$ tenemos que $g_j(x) = s(x)$ y $b_j = 0$, luego $m_j = m_{2t} + j - 2t$ por definición. Tomamos $j = 2k$ y obtenemos $t = k + \frac{1}{2}m_{2t} - \frac{1}{2}m_{2k}$ y como $m_{2t} = 0$ o 1, concluimos que

$$t = \lfloor k + \frac{1}{2} - \frac{1}{2}m_{2k} \rfloor = r,$$

y que

$$m(x) = x^r s\left(\frac{1}{x}\right) = x^r g_{2k}\left(\frac{1}{x}\right).$$

Con este algoritmo demostramos también la fragilidad de las sucesiones de

recurrencia lineal ya que si tenemos la suficiente información, es decir, si conocemos suficientes términos de la sucesión y una cota, podemos conseguir el polinomio mínimo.
Este algoritmo, como su propio nombre indica, fue ideado por Berlekamp y Massey. Burton en *Inversionless decoding of binary BCH codes* hizo una simplificación del algoritmo para el caso en que q es par. Berlekamp, Fredricksen y Proto se dieron cuenta que con $2k$ términos consecutivos podían obtener el polinomio mínimo de la sucesión $m(x)$ de grado k, que si $q = 2$ se puede obtener con $2k - 1$, pero que con $2k - 2$ nunca. Otros matemáticos, como Dillon o Morris, indagaron más en el caso $q = 2$ por el lógico interés.

Capítulo 4

Combinadores de LFSR. Aplicaciones

El Teorema de Berlekamp-Massey pone fuertes límites a la eficacia de las sucesiones de recurrencia lineal (o a los LFSR) como sistema de cifrado, o si preferimos como generador de sucesiones supuestamente aleatorias de bits (secuencias cifrantes). A pesar de conseguir periodos grandes con un coste computacional bajo, dicho algoritmo precisa del conocimiento de sólo el doble de bits de la complejidad.

En este capítulo estudiaremos en primer lugar algunas técnicas que permiten aumentar la complejidad lineal (y por supuesto el periodo de la sucesión) mediante la combinación de varios LFSR de "baja complejidad". Estas técnicas se usan en la práctica, ya que permiten la implementación de ge ne ra do res de secuencias cifrantes de complejidad aceptable basados en varios dispositivos LFSR sencillos. Las dos primeras secciones describen, desde el punto de vista teórico, las dos principales técnicas que se utilizan: combinaciones lineales y productos de sucesiones. Ambas proporcionan el fundamento para comprender los diferentes combinadores no lineales utilizados en la práctica y de los que describimos algunos de los más conocidos en la sección tercera.

La sección cuarta describe muy someramente algunos de los tests estadísticos estándar para "certificar" que una sucesión de bits pseudo-aleatoria generada por un dispositivo determinista es asimilable hasta cierto punto a una sucesión realmente aleatoria de bits.

En la última sección se describen algunos usos reales y de completa actualidad de los generadores de sucesiones pseudo-aleatorias utilizados como secuencias cifrantes en la seguridad de la telefonía móvil.

4.1. Combinadores lineales

Comenzaremos por describir la técnica más simple de combinadores: los lineales. A pesar de que se trata de nuevo de una operación lineal, la suma de sucesiones procedentes de varios dispositivos (p.e. LFSR) es una técnica básica.

El conjunto $\mathcal{S}$ de sucesiones de elementos de $\mathbb{F}_q$ tiene una estructura natural de $\mathbb{F}_q$-espacio vectorial (de dimensión infinita) mediante las operaciones: $\{s_n\}_{n=0}^{\infty} + \{t_n\}_{n=0}^{\infty} = \{s_n + t_n\}_{n=0}^{\infty}$ y $\alpha\{s_n\}_{n=0}^{\infty} = \{\alpha s_n\}_{n=0}^{\infty}$. Si fijamos un polinomio $f(x) \in \mathbb{F}_q[x]$ mónico de grado positivo, denotaremos por $S(f(x))$ al conjunto de todas las sucesiones de recurrencia lineal homogéneas que satisfacen la relación de recurrencia determinada por el polinomio f. Este conjunto es un subespacio vectorial de $\mathcal{S}$, ya que si nuestro polinomio f tiene grado k la relación de recurrencia lineal que determina este polinomio es de la forma 2.2; entonces si $\sigma = \{s_n\}_{n=0}^{\infty}$ y $\tau = \{d_n\}_{n=0}^{\infty}$ son dos sucesiones que satisfacen esta relación la diferencia $\sigma - \tau$ también la verifica.

Es claro que los distintos elementos de $S(f(x))$ quedan determinados unívocamente por el estado inicial $\mathbf{v} \in \mathbb{F}_q^k$ de la sucesión. Por lo tanto es un espacio vectorial de dimensión k y una base del mismo está formada por k sucesiones $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, de manera cada una de ellas σ_i tienen vector de estados iniciales $\mathbf{v}_i$, para cada $i = 1, 2, \ldots, k$ y de forma que $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ forman una base de $\mathbb{F}_q^k$. Una forma de elegir la base $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ es tomar los k primeros vectores de estado de la sucesión de impulso-respuesta.

o Una vez que tenemos bien definido este espacio vectorial y que sabemos como operar con él, vamos a estudiar las relaciones que hay entre los distintos espacios vectoriales.

Proposición 4.1. *Sean $f(x)$ y $g(x)$ dos polinomios mónicos no constantes en $\mathbb{F}_q$ y sean $S(f(x))$ y $S(g(x))$ sus respectivos espacios vectoriales asociados. Entonces, $S(f(x))$ es un subconjunto de $S(g(x))$ si, y sólo si, el polinomio $f(x)$ divide a $g(x)$.*

Demostración. $\longrightarrow$ Supongamos que el espacio vectorial $S(f(x))$ es un subconjunto de $S(g(x))$. Sea $\{d_n\}_{n=0}^{\infty} \in S(f(x))$ la sucesión de impulso-respuesta; entonces, por la proposición 3.28 $f(x)$ es el polinomio mínimo de la sucesión. Por hipótesis, la sucesión también pertenece a $S(g(x))$ luego por el teorema 3.21 f divide a g.
$\longleftarrow$ Recíprocamente, tomamos $\sigma \in S(f(x))$ una sucesión cualquiera. Por el teorema 3.21 el polinomio mínimo $m(x)$ divide a $f(x)$ luego también divide a $g(x)$. Aplicando de nuevo el teorema 3.21 $g(x)$ es polinomio característico de la sucesión σ y por tanto pertenece al espacio vectorial $S(g(x))$. □

En primer lugar veremos que el conjunto de sucesiones de recurrencia lineal es cerrado para la intersección y la suma de espacios vectoriales

Teorema 4.2. *Sean $V_1 = S(f_1(x))$, $V_2 = S(f_2(x))$, $\ldots, V_n = S(f_n(x))$ con $f_1(x), f_2(x), \ldots, f_n(x) \in \mathbb{F}_q[x]$ polinomios mónicos no constantes.*

Si éstos son primos entre sí, entonces

$$V_1 \cap V_2 \cap \cdots \cap V_n = \{\mathbf{0}\},$$

donde $\mathbf{0}$ es la sucesión idénticamente nula. En caso contrario,

$$V_1 \cap V_2 \cap \cdots \cap V_n = S(d(x)),$$

donde $d(x)$ es el máximo común divisor (mónico) de los polinomios $f_1, \ldots, f_n$.

Demostración. El polinomio mínimo de una sucesión de la intersección divide a cada polinomio de $\{f_1, f_2, \ldots, f_n\}$ por el teorema 3.21. Puesto que los polinomios son primos entre sí, el polinomio mínimo ha de ser constante e igual a 1 y como ya sabemos, la única sucesión que tiene a este como polinomio característico es la idénticamente nula.
Por otro lado, sea $d(x) = m.c.d\{f_1, f_2, \ldots, f_n\}$. De nuevo, por el teorema 3.21 el polinomio mínimo $m(x)$ de una sucesión de la intersección divide a $d(x)$. Además tenemos que el polinomio $d(x)$ divide a cada $f_i(x)$ para cada $i \in \{1, 2, \ldots, n\}$, luego por la proposición 4.1 $S(d(x))$ es un subconjunto de la intersección de los espacios vectoriales y tenemos así la igualdad. □

Teorema 4.3. *Sean $V_1 = S(f_1(x)), V_2 = S(f_2(x)), \ldots, V_n = S(f_n(x))$ con $f_1(x), f_2(x), \ldots, f_n(x) \in \mathbb{F}_q[x]$ polinomios mónicos no constantes. Entonces*

$$V_1 + V_2 + \cdots + V_n = S(g(x)),$$

donde $g(x) \in \mathbb{F}_q[x]$ es el mínimo común múltiplo (mónico) de $f_1, f_2, \ldots, f_n$.

Demostración. Lo vamos a probar para el caso en que $n = 2$ ya que después por inducción lo podemos probar para un n arbitrario. En primer lugar, sabemos que V_1 y V_2 son subconjuntos de $S(g(x))$ por la proposición 4.1 luego la suma $V_1 + V_2$ está contenida en el espacio vectorial $S(g(x))$. Nos quedaría ver la contención contraria, pero en lugar de eso vamos a utilizar la fórmula de las dimensiones. Sea $d(x) = \text{mcd}\{f_1, f_2\}$; la fórmula de las dimensiones nos dice que

$$\begin{aligned} \dim(V_1 + V_2) &= \dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2) \\ &= \deg(f_1(x)) + \deg(f_2(x)) - \deg(d(x)), \end{aligned}$$

ahora como $f_1(x)f_2(x) = d(x)g(x)$,

$$\dim(V_1 + V_2) = \dim(g(x)) = \dim(S(g(x))),$$

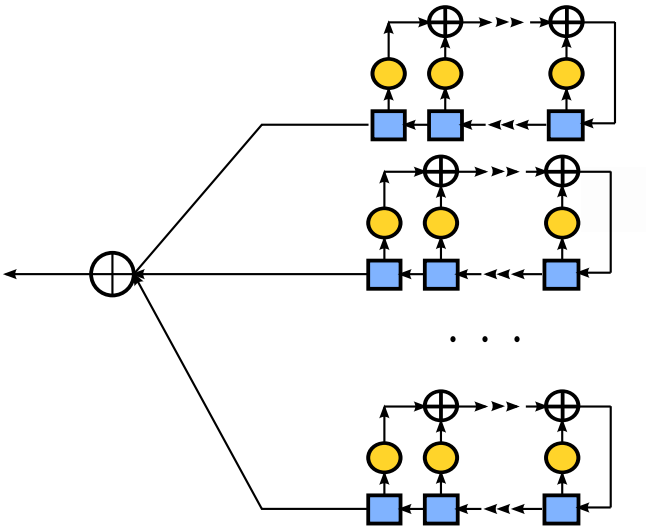
por ello, como las dimensiones son iguales y tenemos una contención se da la igualdad. □

Nota 4.4. Evidentemente, cuando f y g son primos entre sí tenemos que

$$S(f(x)g(x)) = S(f(x)) + S(g(x)).$$

Una consecuencia del resultado anterior es que el subconjunto $\mathcal{SL} \subset \mathcal{S}$ formado por todas las sucesiones de recurrencia lineal son un subespacio vectorial de $\mathcal{S}$.

Dado un conjunto de sucesiones de recurrencia lineal, podemos definir un combinador lineal fruto de la suma que tenemos definida entre las sucesiones de recurrencia lineal.



Este proporciona una nueva sucesión donde cada término n-ésimo es la suma de las salidas que ha tenido cada LFSR.

Ya sabemos calcular el polinomio característico de la suma de dos sucesiones de recurrencia lineal homogéneas y caracterizar el espacio vectorial al que pertenecen. Ahora vamos a estudiar cómo se calcula el polinomio mínimo de la suma y por lo tanto el orden de sucesión resultante.

Proposición 4.5. *Sea $\{\sigma_1, \sigma_2, \ldots, \sigma_l\}$ un conjunto de sucesiones de recurrencia lineal homogéneas sobre $\mathbb{F}_q$ y sea $\sigma = \sigma_1 + \cdots + \sigma_l$. Para cada $i = 1, \ldots, l$ sea r_i el periodo mínimo y $m_i(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de σ_i. Si los polinomios $\{m_i(x)\}_{1 \leqslant i \leqslant l}$ son primos entre sí dos a dos entonces:*

1. *El polinomio mínimo de σ es $m_1(x)m_2(x)\cdots m_l(x)$.*
2. *El periodo mínimo de σ es* m.c.m.$\{r_1, r_2, \ldots, r_l\}$.

Demostración. Lo probaremos para la suma de dos sucesiones ya que para una suma finita arbitraria se probaría después por inducción.

1. Sean σ y τ dos sucesiones de recurrencia lineal homogéneas. Si alguna de las dos es la idénticamente nula, el resultado es trivial ya que el polinomio mínimo es el 1; y si el polinomio mínimo de la suma $m(x)$ es el 1 también estamos en un caso trivial; por ello supongamos que ambas son distintas de la 0 y que $m_\sigma(x)$, $m_\tau(x)$ y $m(x)$ son todos de grado positivo. Por el teorema de la suma de espacios vectoriales tenemos que

   $$\sigma + \tau \in S(m_\sigma(x)) + S(m_\tau(x)) = S(m_\sigma(x)m_\tau(x)),$$

   entonces por ser $m(x)$ el polinomio mínimo del subespacio suma, ha de dividir al producto $m_\sigma(x)m_\tau(x)$ y de este modo tenemos la contención, $S(m(x)) \subset S(m_\sigma(x)m_\tau(x))$. Veamos ahora la otra contención.
   Supongamos que $\sigma = \{s_n\}_{n=0}^{\infty}$, que $\tau = \{t_n\}_{n=0}^{\infty}$ y que $m(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$. Tenemos por lo tanto la relación de recurrencia lineal

   $$s_{n+k} + t_{n+k} = a_{k-1}(s_{n+k-1} + t_{n+k-1}) + \cdots + a_0(s_n + t_n),$$

   para $n = 0, 1, \ldots$. Definimos ahora la sucesión $\{u_n\}_{n=0}^{\infty}$ donde el término n-ésimo está dado por

   $$\begin{aligned} u_n &= s_{n+k} - a_{k-1}s_{n+k-1} - \cdots - a_0 s_n \\ &= -t_{n+k} + a_{k-1}t_{n+k-1} + \cdots + a_0 t_n \end{aligned}$$

   Puesto que, por el teorema anterior, los espacios vectoriales $S(m_\sigma(x))$ y $S(m_\tau(x))$ son cerrados para las traslaciones, esta sucesión $\{u_n\}_{n=0}^{\infty}$ pertenece a ambos, luego sólo puede ser la idénticamente nula ya que los polinomios eran primos entre sí. Por eso, tanto $S(m_\sigma(x))$ como $S(m_\tau(x))$, dividen a $S(m(x))$ y tenemos así la otra contención buscada.

2. Por el teorema 3.25 sabemos que orden de una sucesión es igual a orden del polinomio mínimo. Por ello, si r es el periodo de σ, por la proposición 4.5, $r = ord(m_1(x)m_2(x))$ ya que los polinomios son primos entre sí. Además por el teorema 3.13, ya podemos concluir que $r = \text{mcm}(ord(m_1), ord(m_2)) = \text{mcm}(r_1, r_2)$.

□

En el caso en que conozcamos los periodos mínimos de cada sucesión y sepamos que son primos entre sí, basta hacer el producto de los periodos mínimos para conocer el periodo mínimo de la suma.

Teorema 4.6. *Sean σ_i, para $i = 1, 2, \ldots, l$ sucesiones de recurrencia lineal homogéneas finalmente periódicas en $\mathbb{F}_q$ con periodo mínimo r_i. Si los enteros $\{r_1, r_2, \ldots, r_l\}$ son primos dos a dos, entonces el periodo mínimo de la suma $\sigma_1 + \sigma_2 + \cdots + \sigma_l$ es igual al producto de los periodos mínimos r_i con $i = 1, 2, \ldots l$.*

Demostración. Vamos a demostrarlo para el caso en que tenemos dos sumandos; para un número arbitrario se hace por inducción. Supongamos que σ_1 y σ_2 son dos sucesiones finalmente periódicas con periodos mínimos r_1 y r_2 respectivamente. El producto $r_1 r_2$ es periodo de la sucesión suma $\sigma = \sigma_1 + \sigma_2$; por lo que el periodo mínimo r divide a $r_1 r_2$. El periodo r lo podemos escribir de la forma $r = d_1 d_2$, donde d_1 y d_2 son divisores de r_1 y r_2 respectivamente. Veamos que estos divisores son justamente los periodos r_1 y r_2. El entero $r_1 d_2$ es un periodo de la sucesión σ, pero para un n lo suficientemente grande también lo es de σ_1 y de σ_2; entonces r_2 divide a $r_1 d_2$ y como r_1 y r_2 son primos entre sí, $d_2 = r_2$. Del mismo modo, pero con $d_1 r_2$, probamos que $d_1 = r_1$ y concluim os así que el periodo mínimo de la suma es el producto de los periodos mínimos. □

Nota 4.7. Como es lógico, los polinomios mínimos no tienen porqué ser primos dos a dos. En ese caso, vamos a dar un procedimiento de como se calcula el polinomio mínimo de la suma. Nos basta hacerlo para dos sucesiones. Sean σ y τ dos sucesiones de recurrencia lineal homogéneas y $m_\sigma(x)$ y $m_\tau(x))$ sus polinomios mínimos no necesariamente primos entre sí. ¿Cuál es el polinomio mínimo de la suma ? Una forma de dar la suma de dos sucesiones es mediante la función generatriz; es decir, si $G_1(x)$ es la función generatriz de σ y $G_2(x)$ la de τ, la función generatriz de la suma es $G(x) = G_1(x) + G_2(x)$. Por el teorema 2.28, $G(x) = \frac{g_1(x)}{m^*_\sigma(x)} + \frac{g_2(x)}{m^*_\tau(x)}$. Puesto que los polinomios mínimos no son necesariamente primos entre sí, supongamos que los podemos escribir de la forma $m_\sigma(x) = p(x)m_1(x)$ y $m_\tau(x) = p(x)m_2(x)$, con $m_1(x)$ y $m_2(x)$ primos entre sí. Hacemos la suma y tenemos

$$G(x) = \frac{g_1(x)m_2^*(x) + g_2 m_1^*(x)}{p^*(x)m_1^*(x)m_2^*(x)},$$

y por el recíproco del teorema 2.28, el polinomio recíproco de $p^*(x)m_1^*(x)m_2^*(x)$ es el polinomio característico de la sucesión suma. Finalmente, utilizando el método que vimos en la demostración del teorema 3.21 calculamos el polinomio mínimo.

Ejemplo 4.8. Veamos un ejemplo que ilustre esta forma de calcular el polinomio mínimo de la suma cuando los polinomios mínimos de las sucesiones sumando no son primos entre sí. Supongamos que tomamos los espacios vectoriales $S(x^4 + x^3 + x + 1)$ y $S(x^4 + x^3 + x^2 + 1)$ sobre $\mathbb{F}_2$ y en cada uno de ellos la sucesión de impulso-respuesta. Por la proposición 3.28, los polinomios mínimos son

$$m_1(x) = x^4 + x^3 + x + 1 = (x^2 + x + 1)(x + 1)^2 \in \mathbb{F}_2[x]$$

y

$$m_2(x) = x^4 + x^3 + x^2 + 1 = (x^3 + x + 1)(x + 1) \in \mathbb{F}_2[x]$$

Tenemos, respectivamente, $g_1(x) = x^3$ y $g_2(x) = x^3$ polinomios en $\mathbb{F}_q[x]$ requeridos para aplicar el teorema 2.28. La función generatriz de la suma es

$$\begin{aligned} G(x) &= \frac{x^3}{(x^2+x+1)(x+1)^2} + \frac{x^3}{(x^3+x^2+1)(x+1)} \\ &= \frac{x^5}{(x^3+x^2+1)(x+1)^2(x^2+x+1)}, \end{aligned}$$

y el polinomio recíproco de $f(x) = (x^3 + x^2 + 1)(x + 1)^2(x^2 + x + 1)$ el característico de la suma de las dos sucesiones. Por la igualdad 2.13, $x^6(\frac{1}{x})^5 = x$ es el polinomio $h(x)$. Entonces como f y h son primos entre sí, concluimos que el polinomio mínimo es $m(x) = (x^3 + x + 1)(x + 1)^2(x^2 + x + 1)$.

Las sucesiones de recurrencia lineal sobre cuerpos finitos son una herramienta, como veremos más adelante, para campos como la informática, la criptografía y los códigos. Por ello, el cuerpo finito en el que trabajan es $\mathbb{F}_2$. Las sucesiones de recurrencia sobre $\mathbb{F}_2$ se las denomina sucesiones binarias. Una operación habitual es sustituir una sucesión por su ccmplementaria, es decir, intercambiar los ceros por unos y viceversa. La nueva sucesión tiene el mismo periodo mínimo que la de partida.

Ya hemos estudiado las principales características de los espacios vectoriales $S(f(x))$ sobre $\mathbb{F}_q$ donde $f \in \mathbb{F}_q[x]$ y que gracias a estas características, con polinomios de grado relativamente pequeños, podemos obtener sucesiones con periodo grande. Ahora lo que vamos a ver es que si partimos de un espacio vectorial $S(f(x))$ lo podemos escribir como suma de subespacios vectoriales del mismo tipo.

En primer lugar, supongamos que tenemos $f(x) \in \mathbb{F}_q[x]$ un polinomio mónico cualquiera de grado positivo k y con $f(0) \neq 0$. Escribimos ahora el polinomio como producto de polinomios irreducibles; es decir

$$f(x) = \prod_{i=1}^{h} g_i(x)^{b_i},$$

donde los polinomios $g_i(x) \in \mathbb{F}_q[x]$ son irreducibles sobre $\mathbb{F}_q$, distintos dos a dos y los b_i son enteros positivos. Por el teorema 4.3 tenemos que

$$S(f(x)) = S(g_1(x)^{b_1}) + \cdots + S(g_h(x)^{b_h}).$$

Esta suma es directa ya que como los polinomios g_i son irreducibles y distintos dos a dos el máximo común divisor es 1 lo que da como intersección el cero. Por ello, todas las sucesiones de $S(f(x))$ las obtenemos de sumar las sucesiones de cada uno de los subespacios. Por la proposición 4.1 tenemos además, para cada $i \in \{1, 2, \ldots, h\}$

$$S(g_i(x)) \subseteq S(g_i(x)^2) \subseteq \cdots \subseteq S(g_i(x)^{b_i}),$$

luego si el grado de g_i es k_i para cada $i \in \{1, 2, \ldots, h\}$, tenemos $q^{k_i} - 1$ sucesiones de $S(g_i(x)^{b_i})$ con polinomio mínimo g_i, $q^{2k_i} - q^k$ sucesiones con polinomio mínimo g_i^2; en general para $a \in \{1, 2, \ldots, b_i\}$, tenemos $q^{ak_i} - q^{(a-1)k_i}$ sucesiones de $S(g_i(x)^{b_i})$ con polinomio mínimo g_i^a. A partir de esto y de la forma que hemos dado de calcular el orden de un polinomio a partir del orden de los polinomios en los que descompone, tenemos el siguiente resultado para el caso especial en que nuestro polinomio lo podamos escribir como una potencia de un polinomio irreducible, que nos da el número de sucesiones que hay en un espacio vectorial $S(f(x))$ con cada uno de los periodos mínimos posibles.

Teorema 4.9. *Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio tal que $f(x) = g(x)^b$ donde $g(x) \in \mathbb{F}_q[x]$ es un polinomio irreducible y mónico de grado k, orden e y tal que $g(0) \neq 0$. Sea b un entero positivo y t el menor entero tal que $p^t \geqslant b$, siendo p la característica del cuerpo. Entonces tenemos el siguiente número de sucesiones con los siguientes periodos mínimos en $S(f(x))$: una sucesión con periodo mínimo 1; $q^k - 1$ sucesiones de periodo mínimo e; para $b \geqslant 2$, $q^{kp^j} - q \geqslant^{kp^{j-1}}$ sucesiones de periodo mínimo ep^j para $j \in \{1, 2, \ldots, t-1\}$; y finalmente $q^{kb} - q^{kp^{t-1}}$ sucesiones de periodo mínimo ep^t.*

4.2. Combinadores producto

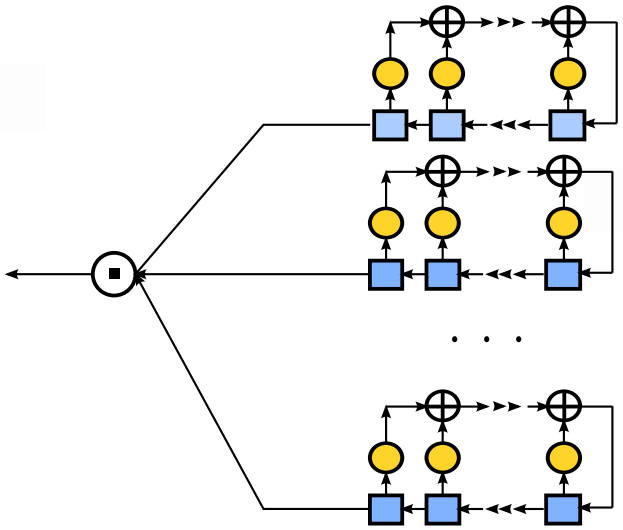
Describiremos a continuación la primera operación no lineal: el producto de dos o más sucesiones (entendido como producto término a término).

Si $\sigma = \{s_n\}_{n=0}^{\infty}$ y $\tau = \{t_n\}_{n=0}^{\infty}$ son dos sucesiones de recurrencia lineal homogéneas en $\mathbb{F}_q$, definimos el producto por $\sigma\tau = \{s_n t_n\}_{n=0}^{\infty}$.

Si tenemos $f_1(x), f_2(x), \ldots, f_r(x)$ polinomios mónicos en $\mathbb{F}_q[x]$, definimos el producto $S(f_1(x))S(f_2(x)) \ldots S(f_r(x))$ como el subespacio vectorial generado por los productos $\sigma_{\mathbf{1}}\sigma_{\mathbf{2}} \ldots \sigma_{\mathbf{r}}$ donde $\sigma_{\mathbf{i}} \in S(f_i(x))$ para cada $1 \leqslant i \leqslant r$.

Como ya sabemos, el subespacio $\mathcal{SL}$ es cerrado para las traslaciones, es decir si la sucesión $\sigma \in S(f(x))$ entonces la sucesión trasladada σ_b también pertenece a $S(f(x))$, para cualquier $b \geqslant 0$.

Para esta operación que hemos definido entre sucesiones de recurrencia lineal podemos implementar, también, un circuito generador de la sucesión que obtenemos del producto término a término. Su esquema es el siguiente:



De hecho, la propiedad de la traslación de sucesiones caracteriza las sucesiones de recurrencia lineal:

Teorema 4.10. *Sea $V \subset \mathcal{S}$. Entonces $V = S(f(x))$ para un cierto polinomio mónico de grado positivo $f(x) \in \mathbb{F}_q[x]$ si, y sólo si V es un subespacio vectorial de dimensión finita cerrado para la traslación de sucesiones.*

Demostración. $\longrightarrow$ Esta condición es trivial ya que como hemos comentado anteriormente el espacio vectorial $S(f(x))$ es cerrado para las traslaciones para cualquier polinomio mónico $f(x) \in \mathbb{F}_q[x]$ que tomemos.
$\longleftarrow$ Para cualquier sucesión σ, denotamos por $\sigma^b = \{s_b, s_{b+1}, \dots\}$, con $b \geqslant 0$, a la sucesión trasladada.Sea V un espacio de dimensión finita, σ una sucesión no nula de V y supongamos que todas sus trasladadas $\sigma^0, \sigma^1, \dots$ pertenecen a V. Como V tiene dimensión finita existen dos enteros positivos $i < j$ tales que $\sigma^i = \sigma^j$. Por ello, la sucesión original σ satisface la relación de recurrencia $s_{n+i} = s_{n+j}$ para todo $n \geqslant 0$. Sea $m(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de la sucesión σ de grado k; por la proposición 3.28, los vectores $\mathbf{s}_0, \mathbf{s}_1, \dots, \mathbf{s}_{k-1}$ son linealmente independientes sobre $\mathbb{F}_q$. Entonces las k primeras sucesiones trasladadas de σ son elementos linealmente independientes de $S(m(x))$ sobre $\mathbb{F}_q$. Además como pertenecen a V, $S(m(x))$ es un subespacio vectorial de V. Finalmente, como V tiene dimensión finita y para cada sucesión no nula σ de V el conjunto $S(m_\sigma)$ es un subespacio vectorial,

$$V = \sum_{\sigma \in V^*} S(m_\sigma(x)) = S(f(x)),$$

donde $f(x)$ es el mínimo común múltiplo de todos los polinomio mínimos m_σ. □

Ahora sí, el resultado que describe el producto de espacios vectoriales es este.

Teorema 4.11. *Si $f_1(x), f_2(x), \ldots, f_r(x)$ son polinomios mónicos en $\mathbb{F}_q[x]$ de grado positivo, entonces existe un polinomio mónico $g(x) \in \mathbb{F}_q[x]$ tal que*

$$S(f_1(x))S(f_2(x)) \ldots S(f_r(x)) = S(g(x)).$$

Demostración. Sea E el subespacio $S(f_1(x))S(f_2(x)) \cdots S(f_r(x))$. Como cada uno de los $S(f_i(x))$ contiene al menos una sucesión cuyo primer término es 1, el conjunto E también tiene, como mínimo, una sucesión no nula. El subespacio E está generado por un número finito de sucesiones por tanto tiene dimensión finita. Ya solo nos queda probar que E es cerrado para la traslación de sucesiones y así podremos concluir, aplicando el teorema 4.10, la existencia del polinomio g. Cada uno de los subespacios $S(f_i(x))$ es cerrado para la traslación de sucesiones luego una sucesión que la obtengamos como producto también ha de cumplir esa propiedad, ya que si todas las desplazadas están en cada uno de los subespacios, por definición de E, el producto de ellas también estará. □

Ahora el problema que se nos plantea es cómo obtenemos este polinomio $g(x)$. En general, no vamos a saber como calcularlo, pero en el caso en que podamos tomar una raíz distinta de cada polinomio dentro del cuerpo de descomposición podremos hacerlo. Para ver el procedimiento tenemos que dar una definición previa.

Definición 4.12. Sean $f_1(x), f_2(x), \ldots, f_r(x) \in \mathbb{F}_q[x]$ polinomios no constantes sobre $\mathbb{F}_q$. Definimos el polinomio $f_1(x) \vee f_2(x) \vee \cdots \vee f_r(x)$ como el polinomio mónico en $\mathbb{F}_q$ cuyas raíces son todos los elementos distintos de la forma $\alpha_1\alpha_2 \cdots \alpha_r$ donde para cada $1 \leqslant i \leqslant r$, α_i es una raíz del polinomio $f_i(x)$ en el cuerpo de descomposición, K, del polinomio $f_1 f_2 \cdots f_r$.

Denotamos por $\mathcal{R}$ el conjunto de productos $\alpha_1\alpha_2 \cdots \alpha_r$ tales que $\alpha_i \in K$ es una raíz del polinomio $f_i(x)$ para $1 \leqslant i \leqslant r$. Entonces el grupo de Galois de la extensión $K/\mathbb{F}_q$ actúa sobre $\mathcal{R}$, por lo tanto el polinomio $f_1(x) \vee f_2(x) \vee \cdots \vee f_r(x)$ queda invariante por la acción del grupo y por consiguiente tiene coeficientes en $\mathbb{F}_q$.

Cuando podemos tomar todas las raíces distintas tenemos definido el polinomio $g(x)$ del teorema anterior como ilustra la siguiente proposición.

Proposición 4.13. *Sean $f_1(x), f_2(x), \ldots, f_r(x) \in \mathbb{F}_q[x]$ polinomios no constantes y sin raíces múltiples. Entonces tenemos que*

$$S(f_1(x))S(f_2(x)) \ldots S(f_r(x)) = S(f_1(x) \vee f_2(x) \vee \cdots \vee f_r(x)).$$

Demostración. Para hacerlo más sencillo y no enturbiar la notación vamos a hacer cuando tenemos dos subespacios.
Sean $S(f(x))$ y $S(g(x))$ dos espacios vectoriales. Supongamos que f y g

tienen raíces simples $\alpha_1, \ldots, \alpha_k$ y $\beta_1, \ldots, \beta_m$ respectivamente y tomamos $\{s_n\}_{n=0}^{\infty}$ y $\{t_n\}_{n=0}^{\infty}$ sucesiones una de cada espacio. Entonces por el teorema 2.25, tenemos

$$s_n = \sum_{i=1}^{k} b_i \alpha_i^n \quad \text{y} \quad t_n = \sum_{i=1}^{m} c_i \beta_i^n \quad \text{para } n = 0, 1, \ldots ,$$

donde b_i y c_i pertenecen a una extensión del cuerpo $\mathbb{F}_q$. Hacemos el producto y resulta la sucesión producto $\{u_n\}_{n=0}^{\infty}$ cuyo término n-ésimo es

$$u_n = s_n t_n = \sum_{i=1}^{k} \sum_{j=1}^{m} b_i c_i (\alpha_i \beta_i)^n = \sum_{i}^{r} d_i \gamma_i^n \quad \text{para } n \geqslant 0.$$

Los coeficientes d_i pertenecen de nuevo a una extensión de $\mathbb{F}_q$. Ahora tomamos

$$h(x) = f(x) \vee g(x) = x^r - a_{r-1}x^{r-1} + \cdots + a_0 \in \mathbb{F}_q[x],$$

y por como hemos definido el término general de la sucesión comprobamos que efectivamente $h(x)$ es su polinomio característico. □

Nota 4.14. Los polinomios irreducibles y primitivos tienen, precisamente, raíces simples y para un uso criptográfico éstos últimos son los polinomios en los que estamos interesados. Por eso hemos puesto este resultado; ya que la demostración nos da un procedimiento para calcular el polinomio característico del producto. Este resultado se puede generalizar para el caso en que los polinomios tengan raíces múltiples.

Entenderemos mejor con un ejemplo, como se calcula el polinomio.

Ejemplo 4.15. Sean $S(x^3+x+1)$ y $S(x^2+x+1)$ dos espacios vectoriales sobre $\mathbb{F}_2$. Tomamos $0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, \ldots$ del primero y $0, 1, 1, 0, 1, 1, 0, 1, \ldots$ del segundo. Si hacemos el producto de estas dos sucesiones término a término obtenemos la sucesión $0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, \ldots$. Ahora calculamos el polinomio $(x^3 + x + 1) \vee (x^2 + x + 1)$. Las raíces del primero son $\alpha_1 = \alpha, \alpha_2 = \alpha^2$ y $\alpha_3 = \alpha + 1$, donde $\alpha^3 = \alpha + 1$. Las del segundo son $\beta_1 = \beta$ y $\beta_2 = \beta + 1$, donde $\beta^2 = \beta + 1$ todas ellas pertenecientes al cuerpo de descomposición del polinomio producto. Ahora sí, tenemos que $h(x) = (x^3 + x + 1) \vee (x^2 + x + 1) = (x - \alpha\beta)(x - \alpha(\beta + 1))(x - \alpha^2\beta)(x - \alpha^2(\beta + 1))(x - (\alpha + 1)\beta)(x - (\alpha + 1)(\beta + 1))$.

Igual que teníamos para la suma de subespacios un teorema que nos decía cual era el periodo mínimo de la suma de sucesiones, ahora lo vamos a tener para el producto. Por razones obvias hemos de descartar aquellas sucesiones que, salvo un número finito, tengan todos los términos nulos; ya que el producto de esta sucesión por cualquier otra nos daría una con el mismo número de ceros si es la idénticamente igual a uno, y en cualquier otro caso, con más. Y evidentemente estudiar sucesiones las cuales a partir de un término en adelante sean nulas, no tiene ningún tipo de interés.

Teorema 4.16. *Sean σ_i para $i = 1, 2, \ldots, h$ sucesiones finalmente periódicas en $\mathbb{F}_q$ tales que ninguna de ellas tenga un número finito de términos no nulos. Supongamos que r_i es el periodo mínimo de cada una de ellas. Entonces, si $r_1, r_2, \ldots, r_h$ son primos dos a dos, el periodo mínimo de la sucesión producto $\sigma_1\sigma_2\cdots\sigma_h$ es igual a $r_1r_2\cdots r_h$.*

Demostración. Como ya es habitual en demostraciones de este tipo, vamos a probarlo para el caso en que $h = 2$ ya que para un h cualquiera se sigue por inducción.
Sean σ_1 y σ_2 dos sucesiones de recurrencia lineal homogéneas tal que ninguna de ellas tienen un número finito de términos no nulos y con periodos r_1 y r_2 respectivamente y primos entre si. Hacemos el producto de ambas $\sigma 1\sigma 2$ y tenemos que r_1r_2 es periodo de estas. Por tanto, si r es el periodo mínimo de la sucesión producto, r divide a r_1r_2 y podemos decir que $r = d_1d_2$, donde d_1 y d_2 son divisores de r_1 y r_2 respectivamente. En particular tenemos que d_1r_2 es periodo de la sucesión producto. Por lo que si $\sigma_1 = \{s_n\}_{n=0}^{\infty}$ y $\sigma_2 = \{t_n\}_{n=0}^{\infty}$, tenemos que

$$s_{n+d_1r_2}t_n = s_{n+d_1r_2}t_{n+d_1r_2} = s_nt_n,$$

a partir de un cierto n. Puesto que ninguna de ellas tiene un número finito de términos no nulos existe un entero b tal que $t_n \neq 0$ para n suficientemente grande $n \equiv b \bmod r_2$; de esta forma en la igualdad de arriba podemos cancelar t_n y obtenemos que $s_{n+d_1r_2} = s_n$ para n suficientemente grande. Ahora por el Teorema Chino de los Restos podemos tomar un m tal que $m \equiv n \bmod r_1$ y $m \equiv b \bmod r_2$. De esta forma tenemos

$$s_n = s_m = s_{m+d_1r_2} = s_{n+d_1r_2},$$

y en consecuencia d_1r_2 es periodo de la sucesiones $\{s_n\}_{n=0}^{\infty}$. por lo que r_1 que era su periodo mínimo, divide a d_1r_2 y como r_1 y r_2 eran primos entre sí, en particular, divide a d_1, pero d_1 era un divisor de r_1 por lo que $d_1 = r_1$. Razonando del mismo modo llegamos a que $d_2 = r_2$, y ya podemos concluir para el caso $h = 2$, el resultado deseado. □

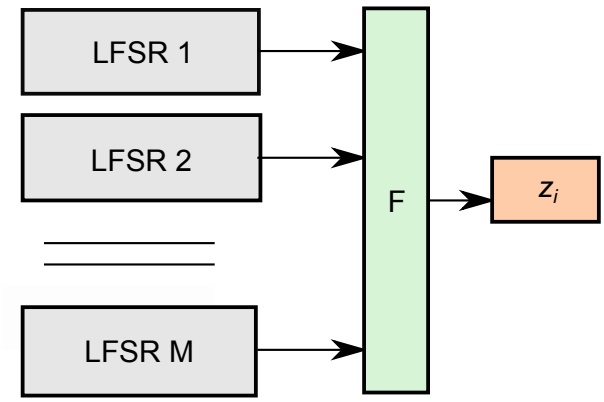
4.3. Combinadores no lineales en la práctica

Las sucesiones de recurrencia lineal reciben este nombre porque cada término de la sucesión, salvo los del estado inicial, se expresa como una combinación lineal de los anteriores. En el caso de las no lineales, los términos se obtienen mediante una combinación no lineal de un número finito de entradas $b_0, b_1, \ldots, b_{r-1} \in \mathbb{F}_q$, es decir, mediante una función no lineal $F : \mathbb{F}_q^r \to \mathbb{F}_q$. Al circuito asociado a la sucesión de recurrencia no lineal lo llamamos NLFSR *No Linear Feed-Back Shift Register*. En general, esta combinación se obtiene al aplicar una función no lineal a sucesiones lineales.

Se suelen distinguir dos tipos de funciones no lineales, dependiendo de su implementación electrónica más que de su naturaleza matemática. Así, un *combinador no lineal* es una función no lineal F en la que $(b_0, \ldots, b_{r-1})$ son los dígitos de salida de r LFSR distintos. En cambio se suele denominar *filtrado no lineal* a una función no lineal en la que $(b_0, \ldots, b_{r-1})$ es un vector de estado de un LFSR (también se pueden utilizar varios).

Combinadores no lineales

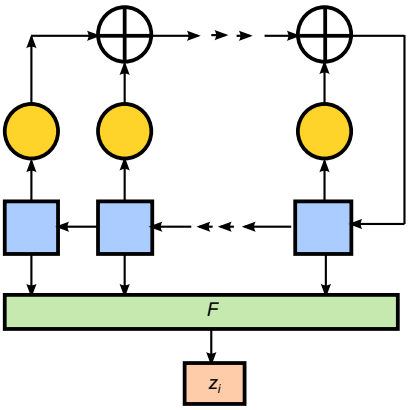
Una forma de obtener los NLFSR es mediante un combinador no lineal, antes de explicar en que consisten, veamos un diagrama.



En este caso, tomamos M circuitos lineales (LFSR) y F una aplicación no lineal. La salida de los LFSR la *combinamos* con la aplicación F y lo que obtenemos es la sucesión no lineal $\{z_n\}_{n=0}^{\infty}$. Gracias a este combinador no lineal, mediante sucesiones con complejidad lineal pequeña, obtenemos una con complejidad lineal mucho más grande. Podemos llamarla de nuevo complejidad lineal ya que, pese a que el filtrado sea no lineal lo que obtenemos en la salida es una secuencia de elementos del cuerpo que en el fondo, es de nuevo una sucesión lineal, pero de orden y periodo mayor. De entre las técnicas más habituales para generar combinadores no lineales está la de tomar relojes con distintas velocidades. Es lo que se suele llamar circuitos asíncronos.

Filtrado no lineal

La otra forma de conseguir un NLFSR es mediante un filtrado no lineal. En este caso disponemos de un LFSR y a todas o a una parte de las unidades de registro le aplicamos una función no lineal F. Es decir, la diferencia con el tipo anterior es que antes cogíamos la salida que nos daba en cada tic de reloj un conjunto finito de LFSR y ahora cogemos en cada tic, las unidades de registro de uno (o varios) LFSR. El esquema general de este tipo es el que sigue:



En parte superior tenemos un LFSR, pero después del tic de reloj las unidades de registro en vez de avanzar una posición y la situada más a la izquierda salir como ocurría en los LFSR, ahora lo que pasa es que a los s_i que están en las unidades de registro los *filtramos* con la función F que es una función no lineal y así obtenemos el elemento z_i de la sucesión que queremos generar. Si tenemos un filtrado F de orden k (intervienen k términos) y lo aplicamos a un LFSR con complejidad lineal L, podemos obtener una nueva sucesión en la que la complejidad lineal está acotada superiormente por $\sum_{i=1}^{k} \binom{L}{i}$. Pero lo más interesante es tener una cota inferior de la complejidad lineal ya que cuanto mayor sea, más segura será la secuencia cifrante. Cuando tomamos la cota inferior, nos estamos refiriendo a la mayor de las cotas inferiores ya que si no, nos aportaría ninguna información. Una de las cotas inferiores para la complejidad lineal cuando en la función no lineal sólo interviene un término de orden máximo, es

$$\frac{\phi(L)}{2}L,$$

siendo ϕ la función phi de Euler. A partir de estas características y otras que se pueden ver en *Avances en el Estudio de la Complejidad Lineal del Filtrado no Lineal*(P.Caballero, Tesis Doctoral, Universidad de la Laguna, 1995), podemos enunciar una serie criterios para la construcción del NLFSR con filtrado.

- Tomar un LFSR que genere una m-secuencia, es decir, la sucesión es de orden m cuyo polinomio característico es primitivo.
- Tomar funciones no lineales que sólo involucren un término de orden máximo. Así tenemos la cota inferior citada antes.
- Elegir el orden k aproximadamente $L/2$.
- Tomar la longitud L un número primo para que la cota inferior de la complejidad lineal sea lo mayor posible. En caso de que esto no sea posible, escoger al menos L y k primos entre sí.

Ahora lo que vamos a estudiar son las distintas familias de generadores no lineales basados en sucesiones de recurrencia lineal.

► **Generadores basados en una combinación no lineal de *LFSR*:** Los generadores de este tipo son los más sencillos ya que la función F característica del NLFSR es simplemente una función no lineal. En estas estructuras a cada impulso de reloj la salida de cada LFSR se convierte en la variable de entrada de la función no lineal cuyo bit de salida se convierte en un término de la secuencia cifrante.
Uno de los ejemplos más representativos de esta familia es **el generador de Geffe.** Este generador implementa una combinación no lineal de tres LFSR de forma que uno determina la salida de cada uno de los otros dos. Si denotamos por $\{z_n\}_{n=0}^{\infty}$ la secuencia cifrante que queremos construir y $\{s_n\}_{n=0}^{\infty}$, $\{t_n\}_{n=0}^{\infty}$ y $\{u_n\}_{n=0}^{\infty}$ las sucesiones que se construyen en LFSR1, LFSR2 y LFSR3 respectivamente, para cada $i \geqslant 0$ tenemos:

$$z_i = F(s_i, t_i, u_i) = \begin{cases} t_i & si\ s_i = 0 \\ u_i & si\ s_i = 1 \end{cases}$$

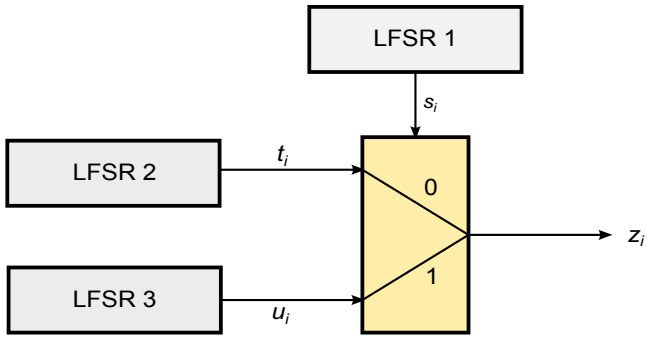
Esta función se puede reescribir de la siguiente forma

$$z_i = F(s_i, t_i, u_i) = t_i + t_i s_i + u_i s_i,$$

para cada $i \geqslant 0$. Si cada una de las sucesiones se han formado a partir de polinomios primitivos con complejidad lineal L_1, L_2 y L_3 respectivamente, se tiene que la complejidad lineal de la sucesión resultante del generador de Geffe es

$$L_2 + L_1 L_2 + L_1 L_3,$$

y su periodo es $\text{mcm}(2^{L_1} - 1, 2^{L_2} - 1, 2^{L_3} - 1)$. En cada tic i de reloj el NLFSR es de la siguiente forma.

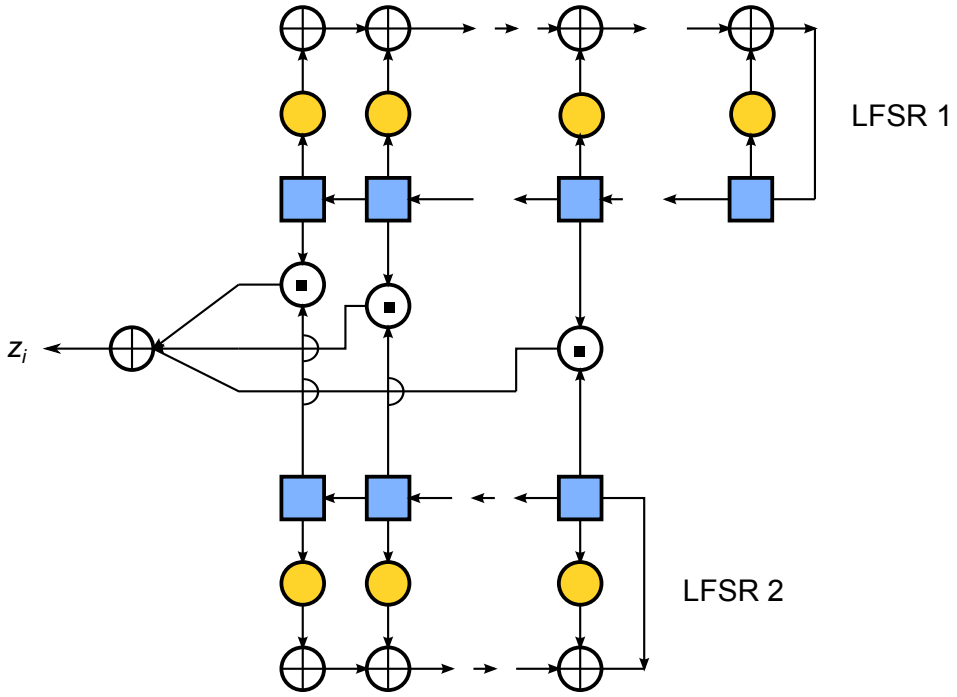


► **Generadores de secuencia multivelocidad:** La principal característica de los generadores de esta familia es que los LFSR que intervienen en el generador no se desplazan de forma sincronizada. Estos tiempos de desplazamiento o velocidad, también forman parte de la clave.

El ejemplo que vamos a destacar de esta familia es el **generador de Massey-Rueppel**. Este generador se basa en dos LFSR (llamémoslos LFSR1 y LFSR2) de longitudes distintas L_1 y L_2 con $L_1 \geqslant L_2$. El LFSR1 va d veces más rápido que el LFSR2 con $d \geqslant 2$ y en cada instante se combinan de un modo no lineal. Entonces si $\sigma = \{s_n\}_{n=0}^{\infty}$ es la sucesión que produce el primer LFSR y $\tau = \{t_n\}_{n=0}^{\infty}$ la sucesión que produce el segundo, el término i-ésimo de la sucesión $\{z_n\}_{n=0}^{\infty}$ que produce el generador de Massey-Rueppel es

$$z_i = \sum_{j=0}^{L_2-1} t_{di+j} s_{i+j},$$

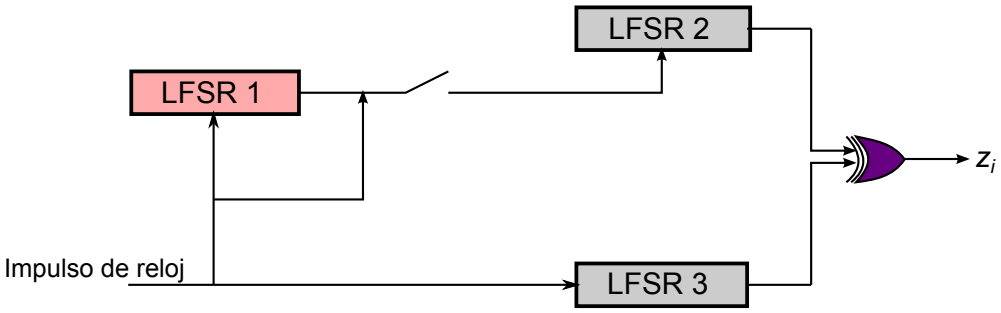
con $i \geqslant 0$. El NLFSR para un instante cualquiera es el siguiente

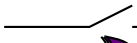


donde ⊙ es un multiplicador y) significa que hay un puente entre los cables, es decir, que los cables no se cortan. La complejidad lineal de la sucesión resultante $\{z_n\}_{n=0}^{\infty}$ es $L_1 L_2$ y el periodo que se obtiene $(2^{L_1} - 1)(2^{L_2} - 1)$, siempre que L_1 y L_2 sean primos entre sí.

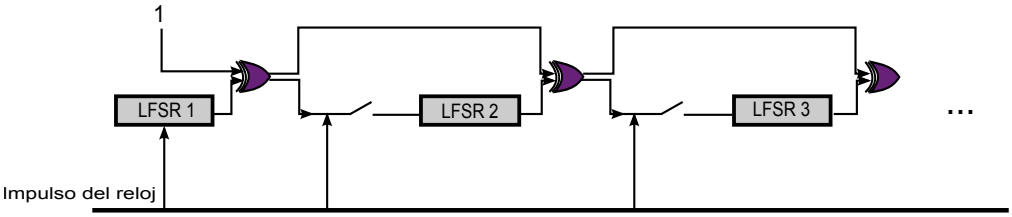
► **Generadores de secuencia con desplazamiento irregular o de paso a paso:** En esta familia de generadores, tenemos un LFSR que controla el funcionamiento del reloj de los otros registros que intervienen en la formación del nuevo término de la sucesión. Los términos de la nueva sucesión se obtienen sumando términos de las sucesiones asociadas a los LFSR que se desplazan según el reloj irregularmente.

De esta familia vamos a señalar dos ejemplos. En primer lugar describamos el **generador de Beth-Piper.** Este generador utiliza tres LFSR (pongamos LFSR1, LFSR2 y LFSR3). Uno de ellos, supongamos LFSR1, controla el reloj de uno de los otros dos registros, digamos LFSR2. Entonces el LFSR2 sólo desplaza los registros si el LFSR1 en el tic anterior tuvo como salida un 1. La salida final se obtiene a partir de una función que vamos a describir a continuación. Para entenderlo mejor, veamos el circuito.



donde  es un interruptor que deja pasar el tic del reloj o no y el operador  hace primero la operación lógica "AND" con los dos bits que entran y después con los tres, la operación XOR. Cuando la unidad de registro del LFSR1 es 1, deja pasar el tic del reloj y si es cero, no. En caso de que no deje pasar el tic, cuando llegamos al operador, la unidad de registro del LFSR2 que entra en el operador es el último término que tengamos en el LFSR2. Si L_1, L_2 y L_3 son las complejidades lineales de cada uno de los tres LFSR involucrados en el generador y son primos entre sí, tenemos que la complejidad lineal de la sucesión $\{z_n\}_{n=0}^{\infty}$ resultante es $(2^{L_1}-1)L_2+L_3$ y el periodo $(2^{L_1}-1)(2^{L_2}-1)(2^{L_3}-1)$. Pese a estos datos, el problema que tiene este generador es que la probabilidad de que la sucesión resultante sea igual a la que asociada al LFSR3 es muy elevada (aproximadamente 0.75) por lo que el coste de aplicar el combinador, en realidad, es fácil que no sirva de nada.

Esto nos invita a hablar del segundo tipo del que íbamos a hablar en esta familia: **el generador en cascada de Gollmann**. Este combinador es una generalización del de Beth-Piper en el que en vez de tener sólo tres LFSR tenemos un número cualquiera (se recomienda tener al menos 15) donde cada uno de ellos está generado con un polinomio primitivo, es decir, tenemos $PN-$secuencias. Estas son las que verifican los tres postulados de pseudoaleatoriedad de Golomb. En este generador el reloj de cada LFSR está controlado por el anterior, es decir, si el LFSRi ha dado como salida un 1, entonces el siguiente funciona, en caso contrario no. La salida del combinador es la del último LFSR. El circuito es el siguiente



Para este tipo de generador, los LFSR involucrados han de tener todos la misma longitud o complejidad lineal. Si suponemos que esta es L, entonces la complejidad lineal del generador cuando tenemos n LFSR es mayor o igual que $L(2^L-1)^{n-1}$ y el periodo es exactamente igual a $(2^L-1)^n$.

4.4. Cadenas pseudoaleatorias de bits

Ya conocemos casi todo sobre las sucesiones de recurrencia lineal. Somos capaces de generar sucesiones con buenas propiedades e incluso, con suficientes términos, capaces de obtener el polinomio mínimo. Según el cifrado de Vernam la secuencia cifrante ideal es aquella de la que podemos obtener infinitos términos perfectamente aleatorios. Pero claro, como ya hemos dicho, esto no es viable; por lo que lo ideal ahora es poder construir una sucesión lo más aleatoria posible a partir de una clave finita. Para el caso en que tenemos una función determinista a partir de una clave finita ya sabemos que la sucesión que obtenemos no es aleatoria, de hecho es periódica. Así que nos quedaremos con secuencias a las que llamaremos *pseudoaleatorias*. Para comprobar la semejanza con una sucesión realmente aleatoria existen diferentes tests que permiten "certificarla". Mencionaremos, sin profundizar demasiado, algunos de los más frecuentes.

Distribución de bits.

Dada una secuencia binaria, llamamos racha de longitud l al bloque de k dígitos consecutivos iguales entre dos distintos. Si la racha es de ceros se la llama gaps y si es de unos, blocks. Por ejemplo

$$\ldots 00101101011110011000001010010110\ldots$$

tiene un gap de longitud 5 y un block de longitud 4.
Si tomamos un N-grama, que es una muestra de N dígitos consecutivos de la sucesión $\{s_n\}_{n=0}^{\infty}$, $\{s_n, s_{n+1}, \ldots, s_{n+N}\}$ con $n < N$ ambos números naturales, llamamos secuencia k-desplazada a la secuencia que obtenemos de desplazar cíclicamente k posiciones el N-grama. Este desplazamiento puede ser hacia la izquierda o hacia la derecha. En otras palabras, la secuencia k-desplazada hacia la izquierda es

$$s_{n+k}, s_{n+k+1}, \ldots, s_{n+N}, s_n, \ldots, s_{n+k-1},$$

y la k-desplazada hacia la derecha

$$s_{n+N-k}, s_{n+N-k+1}, \ldots, s_{n+N}, s_n, \ldots, s_{n+N-1}.$$

Ahora para estudiar la pseudoaleatoriedad podemos utilizar los tres **Postulados de pseudoaleatoriedad de Golomb**:

1. El número de ceros y de unos en cada periodo deben de ser similares. Concretamente, la diferencia no debe de ser mayor que uno.

2. En cada periodo, del total de rachas la mitad de rachas debe de ser de longitud 1, un cuarto de longitud 2, etc. Además en cada caso habrá el mismo número de rachas de ceros que de unos.

3. Sobre cada período de la secuencia, los sucesivos desplazamientos deben producir un número de coincidencias y diferencias entre ambas secuencias cuya diferencia sea constante. Esto significa que los desplazamientos no aportan información sobre el periodo de la sucesión.

Si una secuencia cifrante verifica estos tres postulados se la llama PN-secuencia (Pseudo-Noise sequence). Si el polinomio característico de la sucesión es primitivo, tenemos garantía de que la secuencia va a ser una PN-secuencia.

Función de autocorrelación.

A partir de este tercer postulado se enuncia la función de autocorrelación. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión binaria con periodo mínimo r. Se define la función de autocorrelación por

$$\begin{array}{rccc} AC: & [1,r] & \longrightarrow & [-1,1] \\ & k & \longrightarrow & \frac{C-D}{r} \end{array}$$

donde D es el número de discrepancias y C el número de coincidencias entre la sucesión original y la k-desplazada. Si $k = r$ entonces $AC(r) = 1$ ya que estamos desplazando a la sucesión el mismo número de posiciones que el periodo que tiene y por lo tanto la desplazada, es de nuevo la sucesión original y el número de coincidencias coincide con el periodo. A esto se le llama estar en fase. Por el contrario si $k \neq r$ se dice que la autocorrelación está fuera de fase. Veamos un ejemplo

Ejemplo 4.17. Supongamos que tomamos la secuencia en $\mathbb{F}_2$ generada por $s_{n+3} = s_{n+2} + s_n$ y con vector de estados iniciales $(0, 1, 0)$. La secuencia es $010011101001110\ldots$ tiene periodo 7. Tomamos el 7-grama 0100111. La secuencia desplazada 3 posiciones a la izquierda es 0111010. El número de coincidencias $C = 3$ y número de discrepancias $D = 4$. Por lo que $AC(4) = \frac{3-4}{7} = \frac{-1}{7}$

Cuando la autocorrelación toma valores cercanos a 1 significa que por una parte k es cercano al valor del periodo y que el número D de discrepancias es pequeño. Si toma valores cercanos a cero, indistintamente del valor de k, el número de discrepancias y coincidencias es muy similar. Finalmente, si toma valores cercanos a -1, de nuevo k es cercano al valor de periodo y la sucesión desplazada es casi la complementaria de la original ya que casi no hay coincidencias y el número de discrepancias es alto.
Si tuviésemos una sucesión perfectamente aleatoria y calculásemos la autocorrelación, sería muy cercana a cero ya que eso significa que el número de coincidencias es muy similar al número de discrepancias.
Los N-gramas se pueden generalizar al caso en que los elementos de la sucesión que lo forman no sean consecutivos y los llamamos patrón.

Distribución de patrones.

Definición 4.18. Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia lineal homogénea en $\mathbb{F}_q$ con periodo mínimo r. Al vector $(s_n, s_{n+\tau_1}, \ldots, s_{n+\tau_{k-1}})$ lo llamamos patrón de longitud k con distancias $(\tau_1, \tau_2 - \tau_1, \ldots, \tau_{k-1} - \tau_{k-2})$.

Ejemplo 4.19. Por ejemplo si tomamos la sucesión del ejemplo anterior, $010011101001110\ldots$ y un patrón de longitud 6 es

$$0 * *0 * 1,$$

y el vector de distancias $(0, 4, 2)$.

Supongamos que tenemos un patrón de longitud k y con vector de distancias $(\tau_1, \tau_2 - \tau_1, \ldots, \tau_{k-1} - \tau_{k-2})$, de una sucesión de recurrencia $\{s_n\}_{n=0}^{\infty}$ en $\mathbb{F}_q$ y con periodo mínimo r. Definimos $n((s_n, s_{n+\tau_1}, \ldots, s_{n+\tau_{k-1}}) = \mathbf{a})$ como el número de veces que el vector $(s_n, s_{n+\tau_1}, \ldots, s_{n+\tau_{k-1}})$ es igual a $\mathbf{a} \in \mathbb{F}_q^k$ cuando $n \in \{0, 1, \ldots, r-1\}$. Dicho esto, podemos enunciar la ley de conservación de los patrones.

La ley de conservación de los patrones. *Sea $\{s_n\}_{n=0}^{\infty}$ una sucesión de recurrencia en $\mathbb{F}_q$. Tomamos un patrón de longitud k y vector de distancias $(\tau_1, \tau_2 - \tau_1, \ldots, \tau_{k-1} - \tau_{k-2})$. Entonces*

$$\sum_{\mathbf{a} \in \mathbb{F}_q^k} n((s_n, s_{n+\tau_1}, \ldots, s_{n+\tau_{k-1}}) = \mathbf{a}) = r.$$

A partir de esta ley, como la suma es constante, podemos definir una probabilidad: La constante $n((s_n, s_{n+\tau_1}, \ldots, s_{n+\tau_{k-1}}) = \mathbf{a})/r$ es la probabilidad de que el patrón tome el valor $\mathbf{a}$, y lo denotamos por $Pr(\mathbf{a})$. Entonces, por la ley de conservación de los patrones,

$$\sum_{\mathbf{a} \in \mathbb{F}_q^k} Pr(\mathbf{a}) = 1.$$

En una sucesión aleatoria, de forma ideal, debería ocurrir que la distribución de probabilidad anterior para cualquier patrón prefijado fuese uniforme, es decir, $Pr(\mathbf{a}) = 1/q^k$ para todo $\mathbf{a} \in \mathbb{F}_q$. Por tanto el grado de aproximación a una distribución de probabilidad uniforme es también una medida de la aleatoriedad de una sucesión.

Complejidad de la esfera.

La secuencia cifrante, para que nos sea útil, también ha de ser imprevisible. Es decir, si un atacante interceptara un fragmento de nuestra secuencia, independientemente del tamaño, no debería de predecir cual es el siguiente bit con probabilidad mayor que un medio.(Recordemos que estamos trabajando en un cuerpo finito $\mathbb{F}_q$; lógicamente si la secuencia es binaria, la probabilidad de que acierte es un medio ya que sólo hay dos posibilidades.) Otra forma de medir la imprevisibilidad es con la complejidad lineal. Recordemos que la complejidad lineal es el grado del polinomio mínimo de la sucesión de recurrencia lineal. Cuanto mayor sea, más unidades de memoria vamos a necesitar en la implementación del LFSR, lo que se traduce en que más bits vamos a tener que conocer para poder determinar el resto de elementos. Además en cuanto a la seguridad, un atacante va a necesitar más bits para poder aplicar Berlekamp-Massey y encontrar el polinomio mínimo. Utilizando la complejidad lineal que hemos definido vamos a definir la complejidad de la esfera. Para ello antes tenemos que definir la complejidad del peso.
Sea x una secuencia finita de elementos de $\mathbb{F}_q$ de longitud n. Tomamos un natural u menor o igual que n y definimos la **complejidad de peso u de** x por

$$WC_u(x) = \min_{WH(y)=u} L(x+y), \tag{4.1}$$

donde $L(x+y)$ es la complejidad lineal de $x+y$ y WH denota el peso de Hamming (número de términos de y distintos de cero). Es decir, la complejidad de peso u de x no es otra cosa que el mínimo de la complejidad lineal de la sucesión $x+y$, donde y es una secuencia finita de longitud n con u términos distintos de cero. A partir de este peso podemos definir una distancia d_H en $\mathbb{F}_q^n$, que es la distancia de Hamming que la denotamos por $d_H(x,y)$ y la definimos como el número de términos $x_i \neq y_i$ para $1 \leqslant i \leqslant n$, siendo n la longitud de x e y. Con esta distancia definimos la esfera $S(x,u) = \{y \ : \ d_H(x,y) = u\}$ y la igualdad 4.1 se convierte

$$WC_u(x) = \min_{y \in S(x,u)} L(y).$$

Por lo que la complejidad del peso u es la mayor de las cotas inferiores de las complejidades lineales de todas las secuencias finitas de longitud n y con

peso de Hamming u en la superficie $S(x,u)$.
Si ahora definimos $O(x,u) = \{y \ : \ 0 < d_H(x,y) \leqslant u\}$, es decir, el conjunto de sucesiones finitas de longitud n que distan de x a lo sumo u, la **complejidad de la esfera** es

$$SC_u(x) = \min_{y \in O(x,u)} L(y) = \min_{0<v\leqslant u} WC_v(x). \tag{4.2}$$

Es decir, la complejidad de la esfera nos devuelve la complejidad lineal más pequeña de todas las sucesiones finitas de longitud n que distan de x a lo sumo u.
Con la complejidad de la esfera, para un pequeño margen que fijemos, podemos obtener la complejidad lineal de otra sucesión que difiera de la nuestra ese margen que hemos fijado. Esto proporciona un criptoanálisis hacia las secuencias cifrantes, aunque debemos de tener cuidado puesto que como sólo nos devuelve la complejidad lineal, la sucesión todavía tenemos que encontrarla.
De forma análoga hacemos estas definiciones para sucesiones $\sigma = \{s_n\}_{n=0}^{\infty}$ con periodo r:

$$WC_u(\sigma) = \min_{WH(\sigma)=u, per(\tau)=r} L(\sigma + \tau), \tag{4.3}$$

y

$$SC_u(\sigma) = \min_{0<v\leqslant u} WC_u(\sigma), \tag{4.4}$$

donde $per(\tau) = r$, significa que la sucesión τ tiene periodo r.

El significado de la complejidad lineal ya lo conocemos, ahora tenemos que ver lo que significa la complejidad del peso y la complejidad de la esfera y ver para qué nos van a servir en nuestra cuestión. En concreto diseñaremos un ataque basado en estos conceptos.

Sea $\sigma = \{s_n\}_{n=0}^{\infty}$ una sucesión de periodo r y complejidad lineal $L(\sigma) = k$. Supongamos que tenemos enteros t, ℓ de manera que t es "pequeño" y que ℓ es pequeño en relación a k ($\ell << k$) y de manera que $SC_t(\sigma) = \ell$. Supongamos además que conocemos un fragmento, digamos $s_0, \ldots, s_{2\ell-1}$, de longitud 2ℓ de la sucesión σ. Es claro que la aplicación del algoritmo de Berlekamp-Massey al fragmento conocido no proporciona una solución válida, es decir que la sucesión se alejará bastante de σ. Sin embargo, si encontramos un fragmento $v_0, v_1, \ldots, v_{r-1}$ de una sucesión $\rho = \{v_n\}_{n=0}^{\infty}$ que diste de σ a lo sumo t y de manera que $L(\rho) = \ell$ entonces la aplicación de Berlekamp-Massey al fragmento $v_0, v_1, \ldots, v_{2\ell-1}$ nos permitirá recuperar completamente la sucesión ρ y por tanto tendremos una aproximación a la sucesión original σ bastante aproximada (distará a lo sumo en t posiciones en cada periodo).

Ahora vamos a describir como sería el ataque en la práctica a un texto cifrado en el que tenemos un fragmento de la secuencia cifrante $s^n =$

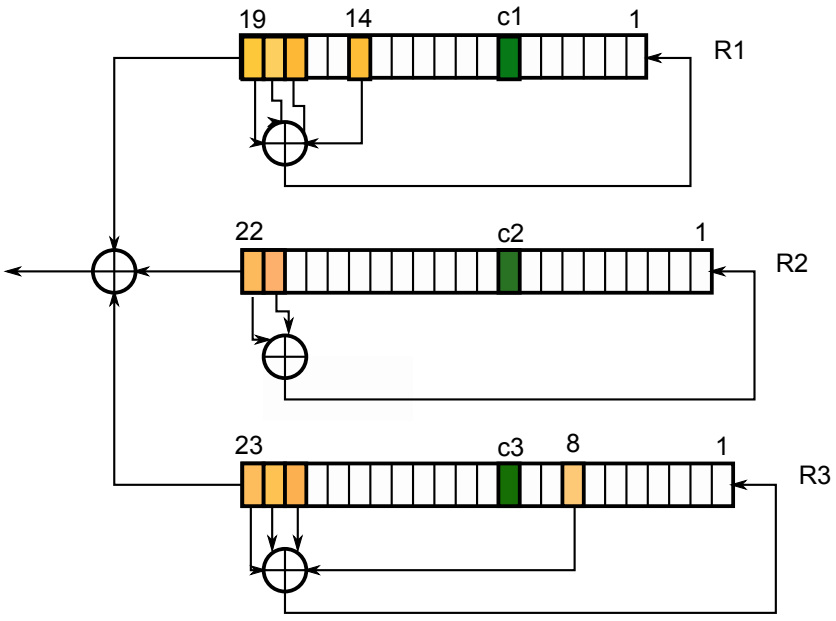
$s_0 s_1 \dots s_{n-1}$. También vamos a suponer que la sucesión es binaria ya que en la práctica las secuencias que se utilizan así lo son, pero se podría generalizar a un cuerpo finito $\mathbb{F}_q$ cualquiera.
El procedimiento consta de tres etapas:
Etapa 1: Utilizamos el algoritmo de Berlekamp-Massey con el fragmento s^n para construir un LFSR que genere una secuencia cuyos primeros términos sean los de s^n. Una vez que la tenemos, la utilizamos para descifrar un fragmento grande del texto cifrado. Si a lo sumo el 15 % carece de sentido, entonces damos por válida la secuencia que hemos obtenido y hemos terminado. En caso contrario, pasamos a la etapa 2.
Etapa 2: Para cada $i \in \{0, 1, \dots n-1\}$, cambiamos s_i por $s_i \oplus 1$ y utilizamos el algortimo de Berlekamp-Massey con este nuevo fragmento, para construir un LFSR que genere una secuencia con los primeros términos de $s^n \oplus 1$. Con ella desciframos un fragmento grande del texto cifrado y, de nuevo, si a lo sumo el 15 % carece de sentido, damos por válida la secuencia y hemos terminado. En caso contrario, repetimos esta etapa para $i+1$ con $i < n-1$ y si $i = n-1$ vamos a la etapa 3.
Etapa 3: Para un par (s_i, s_j) con $i < j$ e $i, j \in \{0, 1, \dots n-1\}$, sustituimos s_i por $s_i \oplus 1$ y s_j por $s_j \oplus 1$ aplicamos el algoritmo de Berlekamp-Massey a esta secuencia nueva para construir un LFSR, y con la secuencia que genera desciframos un fragmento grande de texto cifrado. Una vez más, si el a lo sumo el 15 % carece de sentido, damos la secuencia por válida y hemos terminado. En caso contrario, repetimos esta etapa con otro par (s_i, s_j). Si con ninguna pareja resulta satisfactorio, paramos y escribimos un mensaje de "fallo".

En primer lugar, no debemos pensar que este ataque nos va a servir siempre, ya que como vemos en la última etapa, puede que se pare el algoritmo y no haber descifrado el mensaje. Por eso, vamos a estudiar cuándo funciona ya que sabiéndolo podemos hacer la sucesión más segura, por lo menos para que no sea vulnerable a este ataque.
La idea básica es el suponer que la sucesión $\sigma = \{s_n\}_{n=0}^{\infty}$ se puede expresar como suma de otras dos $\tau = \{t_n\}_{n=0}^{\infty}$ y $\vartheta = \{u_n\}_{n=0}^{\infty}$ tales que τ y ϑ tengan periodo r, que el entero $WH(u^r)/r$ sea muy pequeño y que τ tenga una complejidad lineal también pequeña.
Cuando esto ocurre, si $n < 2r/k$, para un cierto k, tenemos que $s^n = t^n + u^n$ con $WH(u^n) \leqslant 2$. Entonces para todo k pequeño, la complejidad de la esfera, $SC_k(\sigma)$, es grande. Cuanto más grande sea complejidad de la esfera, más garantías tenemos de que no vamos a encontrar una sucesión en una esfera más pequeña, que aproxime la sucesión original.
Con este algoritmo estamos aproximando la secuencia original independientemente de que esta sea lineal o no con una lineal. Por ello es tan importante estudiar el criptoanálisis de la sucesiones lineales.

4.5. Algunas aplicaciones

Las sucesiones de recurrencia o cadenas cifrantes nos permiten obtener una clave para el cifrado en flujo. A continuación vamos a presentar algunas de las aplicaciones más importantes de hoy en día de las secuencias cifrantes.
▶ **Generador A5 en la telefonía movil:** La seguridad de una llamada telefónica se lleva a cabo mediante el generador A5. Existen dos versiones de este generador la A5/1 que se utiliza en países de la Unión Europea y la A5/2 que se emplea en el resto de países. Con este generador se encripta la conexión entre el teléfono y la estación base, es decir, tanto en el teléfono como en la estación base tenemos implementado este generador en un chip. El resto de la conversación no se cifra por lo que si rompemos este cifrado, podemos pinchar una llamada telefónica.
Veamos una breve descripción de estos dos generadores:

- **A5/1:** Este primer generador consta de tres LFSR con complejidades lineales: 19,22 y 23 respectivamente(en la imagen sólo ponemos las unidades de registro) cuyos polinomios característicos son primitivos. En cada una de las etapas, tics del reloj, intervienen un número concreto de bits de cada una de las unidades de registro en la formación del nuevo bit de la secuencia cifrante. Por otra parte, se utiliza la función "mayoría" la cual analiza los bits de las celdas c1,c2 y c3. Se desplazan los registros en los que hay mayoría ya sea de ceros o de unos y en el que hay minoría permanece quieto; al menos dos registros se van a desplazar siempre. El esquema de este generador es el siguiente:



El periodo de la secuencia de salida es aproximadamente $\frac{4}{3}(2^{23}-1)$.

Uno de los puntos débiles de este algoritmo es un problema llamado colisión: diferentes vectores de estados iniciales de cada LFSR pueden producir la misma secuencia cifrante final. Este algoritmo ya ha sido criptoanalizado por A. Biryokov y A. Shamir del Instituto Weizmann de Israel y se lleva a cabo en tiempo real utilizando una tabla de estados internos.

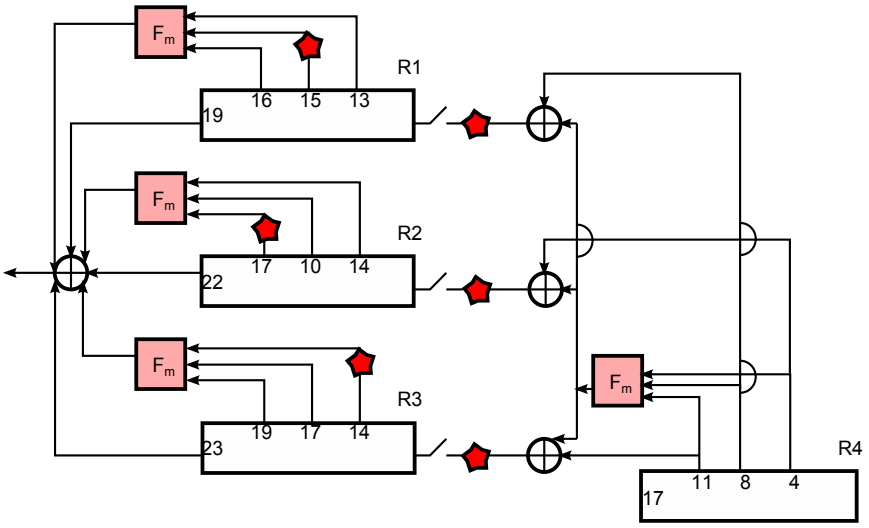
- **A5/2:** En este segundo se emplean cuatro LFSR con complejidades lineales: 19,22,23 y 17 respectivamente y los polinomios característicos también son primitivos. Los tres primeros LFSR son los mismos que los del generador anterior, y el cuarto tiene como polinomio característico $f(x) = 1 + x^5 + x^{17}$. Este cuarto LFSR determina el desplazamiento de los otros tres. En este generador la parte de no linealidad la otorga también la función "mayoría" que la definimos por

$$F_m(s_1, s_2, s_3) = s_1 s_2 + s_1 s_3 + s_2 s_3 \bmod 2.$$

Por otra parte, las variables $c1$, $c2$ y $c3$ controlan el desplazamiento del LFSR correspondiente; si $c_i = 1$ se desplaza y si es nulo, no. Las citadas variables las definimos como:

$$\begin{aligned} c_1 &= F_m([11]_4, [8]_4, [4]_4) + [8]_4 + 1 \bmod 2, \\ c_2 &= F_m([11]_4, [8]_4, [4]_4) + [4]_4 + 1 \bmod 2, \\ c_3 &= F_m([11]_4, [8]_4, [4]_4) + [11]_4 + 1 \bmod 2, \end{aligned}$$

donde $[x]_4$ denota al contenido de la unidad de registro x del LFSR4. El esquema es el siguiente:



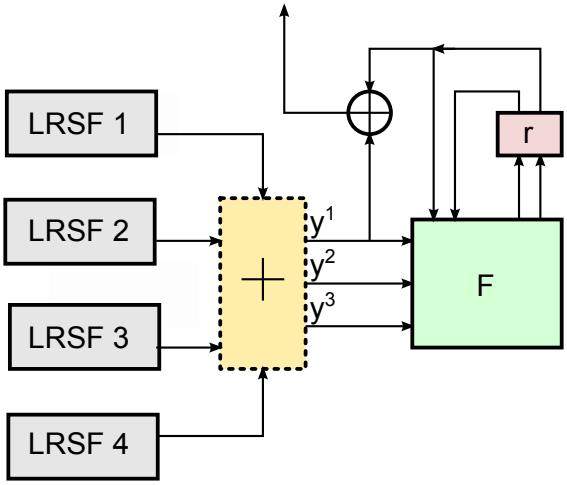
Donde ⬟ devuelve el complementario del bit que entra. Este algoritmo también ha sido criptoanalizado. En este caso, fue por S. Petrovic y A.

Fúster Sabater, del Consejo Superior de Investigaciones Científicas de España. En la actualidad este criptoanalisis se lleva a cabo en tiempo real, aunque en su momento se necesitaban 10 horas. Se basa en la búsqueda de relaciones lineales entre los bits de la secuencia cifrante y con 620 bits se puede romper casi totalmente lo cual es suficiente para poder entender la conversación que estemos interceptando.

► **Generador E0 en Bluetooth:** El cifrado de la información transmitida vía Bluetooth se hace a través del cifrado en flujo. El generador de la secuencia cifrante se llama E0 y en el intervienen cuatro LFSR de complejidades lineales 25,31,33 y 39 respectivamente, una función no lineal F y la función r que ralentiza los tics del reloj (tradicionalmente se denota por z^{-1}, pero para que no haya lugar a confusión he decidido denotarla asi). Los polinomios primitivos que generan los LFSR son los siguientes

$$f_1(x) = x^{25} + x^{20} + x^{12} + x^8 + 1,$$
$$f_2(x) = x^{31} + x^{24} + x^{16} + x^{12} + 1,$$
$$f_3(x) = x^{33} + x^{28} + x^{24} + x^4 + 1,$$
$$f_4(x) = x^{39} + x^{36} + x^{28} + x^4 + 1.$$

Tanto en la placa emisora como en la placa receptora tenemos implementado en un chip el circuito que presentamos a continuación:



La operación suma que tenemos punteada, representa la operación suma habitual de enteros, es decir, si hacer la congruencia módulo 2 y la posterior conversión a binario de la suma efectuada. Por otra parte y^1, y^2 y y^3 son los últimos bits del número en binario; es decir y^1 el último, y^2 el penúltimo y y^3 el antepenúltimo.
El cifrado de Bluetooth se realiza por bloques o tramas de longitud 2746 bits por lo que si se quiere realizar un ataque sólo disponemos de este número de bits para hacerlo y puede resultar escaso. Pese a eso, la inseguridad del generador radica en la mala elección del vector de estados iniciales con el comencemos cada LFSR en cada bloque.

Bibliografía

[**POL**] Maurice Mignotte and Doru Stefanescu, *Polynomials. An Algorithmic Approach.*

[**BOU**] Nicolas Bourbaki , *Elements of Mathematics. Algebra II Chapters 4-7.*

[**LIDL**] Rudolf Lidl and Harald Niederreiter, *Finite Fields.*

[**CIP**] Thomas W. Cusick, Cunsheng Ding and Ari Renvall, *Stream Ciphers and Number Theory.*

[**DAT**] Amparo Fúster Sabater (y otros), *Criptografía, protección de datos y aplicaciones.*

[**ICRI**] Pino Caballero Gil, *Introducción a la Criptografía.*

[**APPLI**] Bruce Schneier, *Applied Cryptography.*

[**E0**] Yi Lu and Serge Vaudenay, *Faster Correlation Attack on Bluetooth Keystream Generator E0. (Artículo).*

[**CL**] Pino Caballero Gil, Tesis Doctoral Universidad de La Laguna (1995), *Avances en el estudio de la Complejidad Lineal del Filtrado no lineal.*

[**CFLU**] Jordi Herrera Joancomartí, *Criptosistemas de clave compartida: cifrado en flujo. (Apuntes).*