5to Coloquio del Departamento de Matemáticas

Acerca de Sucesiones Binarias

Horacio Tapia Recillas

Comité Organizador

Dr. Mario Pineda Ruelas
Dra. Blanca Rosa Pérez Salvador
Dr. Joaquín Delgado Fernández
Dr. Constancio Hernández García
Mat. Daniel Espinosa
Beatriz Arce Vargas (Apoyo logístico)

Material didáctico del Departamento de Matemáticas de la Universidad Autonóma Metropolitana-Iztapalapa con el apoyo de la División de Ciencias Básicas e Ingeniería.

Acerca de Sucesiones Binarias

Horacio Tapia Recillas

Departamento de Matemáticas, UAM-I

Casa abierta al tiempo

Universidad Autónoma Metropolitana

Contenido

Prólogo

El estudio de *sucesiones* ha sido muy importante en varias áreas de Matemáticas y estas se manifiestan de diversas maneras en diferentes contextos en la naturaleza y actividad humana, de las cuales la sucesión de Fibonacci es un representante. Debido al desarrollo de las comunicaciones digitales, las sucesiones sobre estructuras algebraicas finitas, particularmente campos de Galois es un tema de gran relevancia actualmente. Una pregunta interesante en este tema es la generación de sucesiones con propiedades particulares que permitan su aplicación en diversos contextos. Algunas de estas propiedades incluyen pseudoaleatoriedad, correlación, generación rápida y eficiente, entre otras. De particular importancia son las sucesiones binarias (por sus aplicaciones) que se obtienen por medio de recurrencias lineales, como es el caso de la sucesión de Fibonacci, y una forma de generarlas es por medio de los llamados *Registros de Corrimiento de Retro-alimentación Lineal* (Linear Feed-back Shift Register, LFSR), los cuales se pueden implementar en hardware para una mayor rapidez en la genenración de la sucesión y su aplicación en tiempo real. En el caso de sucesiones binarias generadas por recurrencias lineales, estas se pueden obtener por medio de la función traza definida sobre una extensión finita de los números binarios, es decir, sobre un campo de Galois. De particular importancia son las sucesiones de máxima longitud, las llamadas *m-sucesiones*. Aunque las sucesiones binarias son las mas estudiadas por sus aplicaciones, desde el punto de vista matemático se pueden usar campos de Galois mas generales y otras estructuras algebraicas que incluyen los ani-llos de enteros modulares, $\mathbb{Z}_m$, o bien los anillos de Galois. Cabe mencionar que el estudio de sucesiones, particularmente sobre estructuras discretas es de tal importancia que hay congresos internacionales dedicadas a este tema, una de ellas es la SETA (**Se**quences and **T**heir **A**pplications).

Las sucesiones, en particular las m-sucesiones, tienen aplicación en una gran va-riedad de contextos. A continuación se mencionan algunos de ellos.

(1) Los sistemas de posicionamiento global (Global Positioning Systems, GPS) usa un LFSR para transmitir rápidamente una sucesión que indica la posición de un objeto.
(2) Los LFSR se usan para generar números pseudoaleatorios para su uso, por ejemplo, en cifrados de cascada como es el A5/1 y A5/2, empleados en teléfonos celulares con GMS, y el E0 usado en Bluetooth. Sin embargo, debido a que la sucesión es generada a base de recurrencias lineales son suceptibles del criptoanálisis, pero se modifican para que sean más robustas y se puedan usar en otros contextos.
(3) Las sucesiones obtenidas por LSFR también se usan en transmisiones y comunicaciones digitales, por ejemplo para tener una modulación y demodulación robusta y eficiente. Entre las empresas transmisoras que usan LFSR se cuentan, entre otras, las siguientes: ATSC Standards (digital TV transmission system Ð North America), DAB (Digital Audio Broadcasting system Ð for radio), DVB-T (digital TV transmission system Ð Europe, Australia, parts of Asia), NICAM (digital audio system for television). Entre las empresas de comunicación digital que usan LFSR se pueden mencionar: IBS (INTELSAT business service), IDR (Intermediate Data Rate service), SDI (Serial Digital Interface transmission), Data transfer over PSTN (according to the ITU-T V-series recommendations), CDMA (Code Division Multiple Access) cellular telephony, 100BASE-T2 "fast" Ethernet (scrambles bits using an LFSR), 1000BASE-T Ethernet, the most common form of Gigabit Ethernet, (scrambles bits using an LFSR), PCI Express 3.0, SATA, USB 3.0, IEEE 802.11a (scrambles bits using an LFSR).

El objetivo de estas notas es el de dar una breve introducción a este tema, y su contenido es el siguiente: en la Sección 2 se recuerda una de las sucesiones mas famosas debido a que se encuentra en un gran número de contextos que incluyen la arquitectura, música y la naturaleza, entre otras. En la Sección 3 se recuerda la *relación áurea* y se describe su relación con la sucesión de Fibonacci. En la Sección 4 se introduce la sucesión de Fibonacci sobre los números binarios y otras estructuras algebraicas finitas. La Sección 5 esta dedicada a la generación de sucesiones binarias por medio de recurrencias lineales así como a los Registros de Corrimiento de Retroalimentación Lineal, una forma de generar sucesiones en forma eficiente. En la Sección 6 se tratan las m-sucesiones, en la Sección 7 se ven algunos aspectos de la correlación de sucesiones binarias, y en la última Sección se recuerdan las sucesiones de Gold, una de las mas usadas en la práctica.

Capítulo 1

La sucesión de Fibonacci

La sucesion de Fibonacci es una sucesión de números reales de las mas conocidas e importantes por su relación con varios fenómenos de la naturaleza entre las que se incluyen crecimiento de poblaciones, simetrias en el crecimiento de algunas plantas y flores así como en algunos animales, entre otras

(http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/fibnat.html).

En áreas como la música, pintura y arquitectura

(http://www.geom.uiuc.edu/ demo5337/s97b/spiral.html)

también aparece la sucesión de Fibonacci. Existe una gran conexión entre la relación áurea y la sucesión de Fibonacci como se podrá ver mas adelante. En las siguientes líneas de recordará su definición y una forma de obtenerla que facilitará la introducción de ‘‘sucesiones de Fibonacci" binarias y sobre otras estructuras algebraicas (campos finitos, anillo d enteros modulares). Esta sección sigue de cerca el material que aparece en [**2**].

La sucesión de Fibonacci, $(s_t)_{t\geq 0}$, se puede generar de las siguiente manera: sea $s_0 = 0$, $s_1 = 1$ y para $t \geq 2$ s_t es tal que

$$s_t = s_{t-1} + s_{t-2}. \tag{1.1}$$

Esta relación se llama de ‘‘*recurrencia*. Así, los primeros términos de la sucesión son:

$$(s_t) = \{0, 1, 1, 2, 3, 5, 8, 13, 21, ...\} \tag{1.2}$$

De especial importancia es la relación que existe entre dos elementos consecutivos de la sucesión de Fibonacci:

$$\frac{s_t}{s_{t+1}}.$$

Por ejemplo,

$$1/1 = 1\ 2/1 = 2\ 3/2 = 1.5\ 5/3 = 1.666\ldots\ 8/5 = 1.6$$

A continuacin se verá una una forma sistemática de obtener esta sucesión.

A continación se determinará el t-esimo término de las sucesión. Supongamos que el elemento t-ésimo, s_t, $t \geq 2$, de la sucsión es tal que $s_t = \alpha^t$ para algún número α distinto de cero. De la relación de recurrencia se sigue que

$$\alpha^t = \alpha^{t-1} + \alpha^{t-2} \tag{1.3}$$

Multiplicando ambas lados de esta relación por α^{2-t} se tiene que α satisface:

$$\alpha^2 - \alpha - 1 = 0, \tag{1.4}$$

es decir, α es raíz del polinomio

$$f(x) = x^2 - x - 1. \tag{1.5}$$

Este polinomio es llamado el *polinomio característico* de la sucesión de Fibonacci.

Considerando a este polinomio como elemento del anillo $\mathbb{R}[x]$, la ecuación $f(x) = 0$ tiene dos soluciones α_1 y α_2. Es fácil ver que las raices del polinomio caracteístico son:

$$\alpha_1 = \frac{1+\sqrt{5}}{2}, \quad \alpha_2 = \frac{1-\sqrt{5}}{2}. \tag{1.6}$$

Por consiguiente las sucesiones (α_1^t) y (α_2^t) satisfacen la relación de recurrencia de la sucesión de Fibonacci. Cualquier combinación lineal de esas sucesiones tambien satisface la misma relación de recurrencia, mas aun, estas sucesiones generan un espacio vectorial de dimensión 2 (sobre $\mathbb{R}$). Por lo tanto si a y b son números reales, entonces,

$$s_t = a\alpha_1^t + b\alpha_2^t, \tag{1.7}$$

tambien satisface la relación de recurrencia de la sucesión de Fibonacci. A continuación se determinarán los valores de a y b.

Como $s_0 = 0$ y $s_1 = 1$, de la relación anterior se tienen el siguiente sistema lineal:

$$s_0 = a + b = 0, \quad s_1 = a\alpha_1 + b\alpha_2 = 1, \tag{1.8}$$

el cual tiene como solución:

$$a = \frac{1}{\sqrt{5}}, \quad b = -\frac{1}{\sqrt{5}}. \tag{1.9}$$

Por lo tanto, el t-ésimo término de la suceción de Fibonacci es:

$$s_t = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^t - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^t \tag{1.10}$$

la cual es la expresión que aparece en la literatura.

El polinomio $f(x) = x^2 - x - 1$ es irreducible sobre los números racionales $\mathbb{Q}$ y dado que $\sqrt{5}$ es irracional, el campo de descomposición de $f(x)$ es $K = \mathbb{Q}(\sqrt{5})$, el cual es una extensión de grado 2 de $\mathbb{Q}$. El grupo de Galois G de K sobre $\mathbb{Q}$ es cíclico de orden 2 y esta generado por el automorfismo $\sigma(\sqrt{5}) = -\sqrt{5}$.

La función *traza* de K sobre $\mathbb{Q}$ esta definida como:

$$tr_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q},\ tr_{K/\mathbb{Q}}(\gamma) = \gamma + \sigma(\gamma).$$

Ejercicio. Porbar que $tr_{K/\mathbb{Q}}(\gamma) \in \mathbb{Q}$.

El siguiente resultado relaciona la función traza arriba definida con la sucesión de Fibonacci:

THEOREM 1.0.1. *Si f_t es el t-ésimo ($t \geq 1$) término de la sucesión de Fibonacci, entonces:*

$$tr_{K/\mathbb{Q}}(\beta) = f_t = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^t - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^t$$

donde $\beta = \frac{1}{\sqrt{5}}\alpha_1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)$.

Como severá en la Sección 4, la sucesión de Fibonacci sobre otras estructuras algebraicas tambien se puede describir en términos de la función traza correspondiente.

Capítulo 2

La relación áurea

A través de la Historia la relación en un segmento de recta AC como se muestra en la siguiente figura,

$$\frac{AC}{AB} = \frac{AB}{BC}$$

ha sido considerada como una relación de gran importancia, entre otras cosas por su estética. Los griegos la llamaron la *razón dorada* o *razón aúrea*, tambien conocida como la *razón de oro* y le dieron el nombre de ϕ, en honor al escultor griego *Phidias*.

Existe una gran cantidad de ejemplos en la que la razón de oro se manifiesta, tanto en la naturaleza (plantas, animales, flores etc.) como en la pintura, arquitectura, inclusive en arqueología como en la Gran Pirámide de Giza, la cual tiene 4,600 años de existencia, mucho antes de la aparición de la cultura griega en la cual sus dimensiones están basadas en la razón de oro. A continuación se mencionarán algunas de estas manifestaciones.

Varios artistas y arquitectos que vivieron después de Phidias han usado la razón de oro. Por ejemplo, Leonardo Da Vinci le dió el nombre de *proporción divina* y la usó en varias de sus pinturas, por ejemplo en la famosa "Mona Lisa". Además realizó un estudio del cuerpo humano encontrando la proporción divina en varias de sus partes. Como se mencionó antes, se tiene conocimiento que en la Gran Pirámide de Giza, así como en varias partes del Partenon y en la construcción de la catedral de Notre Dame, se manifiesta la razón áurea. Sería difícil mencionar todos los casos donde se encuentra esta relación, pero el lector interesado puede consultar por ejemplo las páginas http://www.goldenratio.org/info/, http://www.goldennumber.net/music.htm o bien buscar en la interner.

Lo importante en relación a estas notas, es que existe una relación entre la razón áurea y la sucesión de Fibonacci, como se muestra a continuación.

Si $a = AB$ y $b = BC$ entonces $a + b = AC$ y la relación entre los segmentos de recta dada anteriormente toma la forma:

$$\frac{a+b}{a} = \frac{a}{b}.$$

Si $b \neq 0$ y se denota por x a esta razón, se tiene la relación

$$x^2 - x - 1 = 0,$$

la cual, como ya se vió anteriormente, tiene como soluciones a $\alpha_1 = \frac{1+\sqrt{5}}{2} = 1.618033\cdots$ y $\alpha_2 = \frac{1-\sqrt{5}}{2}$, las soluciones del polinomio característico de la sucesión de Fibonacci.

Capítulo 3

La sucesión de Fibonacci sobre otras estructuras

Veamos ahora cual es la sucesión de Fibonacci pero sobre el campo de los números binarios.

Sea $\mathbb{F}_2 = \{0, 1\}$ el campo de los números binarios y sea $s_0 = 0$ y $s_1 = 1$ con la relación de recurrencia

$$s_t = s_{t-1} + s_{t-2} \tag{3.1}$$

es fácil ver que los primeros términos de esta sucesión son:

$$(s_t) = \{0, 1, 1, 0, 1, 1, 0, 1, 1, ...\} \tag{3.2}$$

Obsérvese que esta sucesión se repite cada $2^2 - 1 = 3$ términos y su polinomio caraterístico es:

$$f(x) = x^2 + x + 1 \tag{3.3}$$

pero ahora como un elemento del anillo de polinomios $\mathbb{F}_2[x]$.

Obsérvemos lo siguiente:

(1) $f(x)$ es irreducible. Por consiguiente se tiene el campo finito

$$\mathbb{F}_{2^2} = \mathbb{F}_2[x]/\langle f(x)\rangle = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}.$$

donde $\alpha = x + \langle f(x)\rangle$. Mas aún, las raices de $f(x)$ son $\alpha_1 = \alpha$ y $\alpha_2 = \alpha^2 = 1 + \alpha$. Es decir, $\mathbb{F}_{2^2}$ es el campo de descomposición de $f(x)$.

(2) $f(x)$ divide a $x^3 - 1$: $x^3 - 1 = (x - 1)f(x)$.

(3) $f(x)$ es primitivo: la raíz α es tal que $\mathbb{F}_4^* = \langle\alpha\rangle$.

Veamos ahora, como en el caso de la sucesión de Fibonacci clásica, cual es el término general s_t de la sucesión en consideración.

Como las sucesiones (α_1^t) y (α_2^t) son linealmente independientes, entonces

$$s_t = a\alpha_1^t + b\alpha_2^t \tag{3.4}$$

para algunas constantes $a, b \in \mathbb{F}_2$. Veamos cuales son esas consantes. De los valores iniciales de la sucesión se tiene el sistema lineal:

$$a + b = 0, \quad a\alpha_1 + b\alpha_2 = 0, \tag{3.5}$$

el cual tiene como solución $a = b = 1$. Por consiguiente el término geneal de la sucesión biaria de Fibonacci es:

$$s_t = \alpha_1^t + \alpha_2^t \tag{3.6}$$

Como en el caso de la sucesión clásica de Fibonacci, el grupo de automorfismos del campo $mathbbF_4$ sobre $\mathbb{F}_2$ esta generado por el automorfismo de Frobenius: $\sigma(\alpha_1) = \alpha_2$. La función traza se define de la misma manera que en el caso anterior: $tr_{\mathbb{F}_4/\mathbb{F}_2}(\beta) = \beta + \sigma(\beta)$, y tambien se tiene el siguiente resultado:

THEOREM 3.0.2. *Si s_t es el t-ésimo término de la sucesión de Fibonacci sobre los números binarios, entonces*

$$s_t = tr_{\mathbb{F}_4/\mathbb{F}_2}(\alpha_1) = \alpha_1^t + \alpha_1^{2t}.$$

3.1. La sucesión de Fibonacci sobre $\mathbb{F}_3$

Como un ejemplo mas, a continuación se determina la sucesión de Fibonacci sobre el campo $\mathbb{F}_3 = \mathbb{Z}_3 = \{0, 1, 2, 3\}$ de los enteros módulo 3.

Como en los casos anteriores, sea (s_t) la sucesión determinada por $s_0 = 0$, $s_1 = 1$ y la relación de recurrencia

$$s_t = s_{t-1} + s_{t-2}. \tag{3.7}$$

Es fácil ver que los primeros elementos de esta sucsión son:

$$(s_t) = \{0, 1, 1, 2, 0, 2, 2, 0, 1, 1, 2, 0, 2, 2, ...\} \tag{3.8}$$

Obsérvece que la sucesión tiene periodo $n = 3^2 - 1 = 8$.

Para determinar la expresión del término general, como en los casos anteriores, supogamos que $s_t = \alpha^t$ para alguna α. De la relación de recurrencia se sigue que α es raíz del polinomio (caracterśtico) $f(x) = x^2 - x - 1 \in \mathbb{F}_3[x]$, es decir, α satisface la relación

$$\alpha^2 = \alpha + 1 \tag{3.9}$$

Es fácil ver que este polinomio es irreducible (y primitivo) y sus raices son

$$\alpha_1 = \alpha, \quad \alpha_2 = \alpha^3 = 1 + 2\alpha. \tag{3.10}$$

Como el polinomio $f(x)$ es irreducible se tiene el campo

$$\mathbb{F}_{3^2} = \mathbb{F}_3[x]/\langle f(x)\rangle. \tag{3.11}$$

El polinomio es primitivo y divide a $x^{3^2-1} - 1$.

Tambien es fácil ver que el conjunto $\Omega(f)$ de las sucesiones (sobre $\mathbb{F}_3$) que tienen como polinomio característico a $f(x)$ es un $\mathbb{F}_3$-espacio vectorial de dimensión 2 y que una base esta dada por las sucsiones (α_1^t) y (α_2^t). Por lo tanto, el término general de la sucesión se puede expresar como

$$s_t = a\alpha_1^t + b\alpha_2^t \tag{3.12}$$

para algunos $a, b \in \mathbb{F}_3$.

Veamos ahora cuales son esos elementos. Como en los casos anteriores, de la relación de recurrencia se tiene el sistema

$$a + b = 0, \quad a\alpha + b\alpha^3 = 1, \tag{3.13}$$

el cual tiene como solución

$$a = 1 + \alpha, \quad b = -(1 + \alpha). \tag{3.14}$$

Por lo tanto, usando la aritmética del campo $\mathbb{F}_3$, la expresión del t-ésimo término es:

$$s_t = (1 + \alpha)\alpha^t + \left((1 + \alpha)\alpha^t\right)^3. \tag{3.15}$$

De la misma manera que en los casos anteriores se define el automorfismo de Frobenius y la función traza, y se puede ver que

$$s_t = tr((1 + \alpha)\alpha^t).$$

Ejercicio. Probar la afirmación anterior.

Pregunta: ¿cual es la relación de la sucesión con el código cíclico generado por $f(x)$?

3.1.1. Relación con los primos de Mersenne. Observése que en los casos anteriores, el polinomio característico es un trinomio de la forma

$$f(x) = x^2 + a_1 x + a_2 \tag{3.16}$$

con a_1, a_2 elementos del campo correspondiente. Veamos que estos son casos particulares del siguiente hecho:

PROPOSITION 3.1.1. *Sea (s_t) una sucesión con periodo $n = 2^r - 1$ dada por la relación de recurrencia*

$$s_t = s_{n-s} + s_{n-t}. \tag{3.17}$$

Entónces su polinomio característico $f(x)$ es el trinomio

$$f(x) = x^r + x^s + 1 \tag{3.18}$$

3.2. La sucesión de Fibonacci sobre $\mathbb{Z}_4$

En esta sección se determinarán sucesiones del tipo de Fibonacci sobre el anillo de enteros módulo 4, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

Sean $s_0 = 0,\ s_1 = 1$ y sea

$$s_t = s_{t-1} + s_{t-2}$$

la relación de recurrencia.

Es fácil ver que los primeros términos de la sucesión son:

$$(s_t) = \{0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, ...\}.$$

Obsérvese que el periodo de esta sucesión es $m = 6$.

Como en los casos anteriores, supóngamos que el término general de la sucesión es tal que $s_t = \alpha^t$ para algun elemento α. Suponiendo que el elemento α es invertible, de la relación de recurrencia se sigue que este elemento satisface

$$\alpha^2 = 1 + \alpha,$$

es decir, α es raíz del polinomio $f(x) = x^2 - x - 1 \in \mathbb{Z}_4[x]$.

Observaciones.

(1) El elemento α es tal que:

$$\alpha^2 = 1 + \alpha, \qquad \alpha^3 = 1 + 2\alpha,$$
$$\alpha^4 = 2 + 3\alpha, \qquad \alpha^5 = 3 + \alpha,\ \alpha^6 = 1$$

(2) La reducción módulo 2 de $f(x)$, $\overline{f}(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ es irreducible, es decir, $f(x)$ es *básico irreducible*.

(3) El polinomio $f(x)$ divide a $x^3 - 1$: $x^3 - 1 = (x - 1)f(x)$

Sea

$$R = GR(4, 2) = \mathbb{Z}_4[x]/\langle f(x)\rangle$$

el anillo de Galois determinado por $f(x)$. Este anillo es el $\mathbb{Z}_4$-módulo generado por $1, \alpha$, es decir, $R = \langle 1, \alpha\rangle$. El grupo de unidades de R es tal que $U = \langle 3\rangle \times \langle \alpha\rangle$ donde $3^2 = 1$ y $\alpha^6 = 1$. Los elementos de R son:

$$R = M \cup U,$$

donde

$$M = \{0, 2, 2\alpha, 2 + 2\alpha\},$$
$$U = \langle 3\rangle \times \langle \alpha\rangle = \{1, \alpha, 1 + \alpha, 1 + 2\alpha, 2 + 3\alpha, 3 + \alpha, 3,$$
$$3\alpha 3 + 3\alpha, 3 + 2\alpha, 2 + \alpha, 1 + 3\alpha\}.$$

Un cálculo directo muestra que

$$f(x) = (x - \alpha)(x - (1 + 3\alpha)).$$

Sea

$$\Omega(f) = \{(s_t) \text{ con polinomio caracteristico } f(x)\}.$$

Es fácil ver que $\Omega(f)$ es un $\mathbb{Z}_4$-módulo.

Si $\alpha_1 = \alpha$ y $\alpha_2 = 1+3\alpha$ entonces $s'_t = \alpha_1$ y $s''_t = \alpha_2$ son elementos de $\Omega(f)$ y si $s_t = as'_t + bs''_t$. De los valores de s_t se tiene que

$$a + b = 0,\ a\alpha_1 + b\alpha_2 = 1$$

Resolviendo este sistema de ecuaciones se tiene que

$$a = 3 + 2\alpha,\ b = 1 + 2\alpha = \alpha^3.$$

Por lo tanto,

$$s_t = (3 + 2\alpha)\alpha^t + (1 + 2\alpha)(1 + 3\alpha)^t.$$

Observemos que

$$\langle\alpha\rangle = \{1, \alpha^2 = 1 + \alpha, \alpha^3 = 1 + 2\alpha, \alpha^4 = 2 + 3\alpha, \alpha^5 = 3 + \alpha\}$$

y por lo tanto,

$$s_t = 3\alpha^{t+3} + 3\alpha^{5t+3}.$$

Recordemos que el automorfismo de Frobenius τ sobre el anillo de Galois R, esta definido como

$$\tau(\beta_0 + 2\beta_1) = \beta_0^2 + 2\beta_1^2,$$

donde β_0, β_2 son elementos del conjunto de Teichüller $\Lambda = \{0\} \cup \langle\alpha\rangle$, es decir, el elemento de R esta en su representación 2-ádica.

La función *traza* de R sobre $\mathbb{Z}_4$, esta definida como

$$Tr : R \longrightarrow \mathbb{Z}_4,\ Tr(\gamma) = \gamma + \tau(\gamma)$$

Se afirma que $\tau(3\alpha^{t+3}) = 3\alpha^{5t+3}$, y por consiguiente:

$$s_t = Tr(3\alpha^{t+3}).$$

En efecto como $\alpha^6 = 1$ es suficiente ver que $\tau(3\alpha^{t+3}) = 3\alpha^{5t+3}$ es cierto para $t = 0, 1, ..., 5$, y un cálculo directo muestra que esta relación es válida. En efecto,

Caso $t = 0$**.** Como $3\alpha^3 = 1 + 2(1 + \alpha) = 1 + 2\alpha^2$ se tiene que

$$\tau(3\alpha^3) = \tau(1 + 2\alpha^2) = 1 + 2\alpha^4 = 1 + 2\alpha = \alpha^3.$$

Por otro lado,

$$3^t\alpha^{5t+3} = 3^0\alpha^3,$$

de lo cual se sigue la afirmación.

Caso $t = 1$**.** Como $3\alpha^4 = \alpha + 2$ se tiene que

$$\tau(3\alpha^4) = \alpha^2 + 2 = +2\alpha^4 = \alpha^5.$$

Por otro lado,

$$3^t\alpha^{5t+3} = 3^1\alpha^8 = 3\alpha^2,$$

y la afirmación se sigue.

Caso $t = 2$**.** Como $3\alpha^5 = 1 + 3\alpha = \alpha^2 + 2\alpha$ se tiene que

$$\tau(3\alpha^5) = \alpha^4 + 2\alpha^2 = \alpha.$$

Por otro lado,

$$3^t\alpha^{5t+3} = 3^2\alpha^{5(2)+3} = \alpha$$

de lo cual se sigue la afirmación.

Es trivial ver que la afirmación es cierta para $t = 3$ y se deja como ejercicio al lector comprobar la relación para $t = 4$ y $t = 5$.

En conlcusión se tiene la siguiente

PROPOSITION 3.2.1. *Con la notación anterior, el término general de la sucesión de Fibonacci sobre el anillo de enteros módulo 4,* $\mathbb{Z}_4$*, esta dado por*

$$s_t = Tr(3\alpha^{t+3}).$$

3.3. Sucesiones binarias

En os últimos años, con el desarrollo de la información digital y sus múltiples aplicaciones (telefonia digital, GPS, cifrado en cascada, etc.), de gran importancia es el estudio de sucesiones binarias. En esta sección se presentarán algunos resultados en esta dirección. Aunque para fines de las presentes notas se hace énfasis en sucesiones binarias, varios de los argumentos y resultados se tienen para sucesiones en otras estructuras algebraicas como son los campos de Galois o bien anillos finitos (por ejemplo enteros modulares).

3.4. Generación de sucesiones binarias

Una de las formas mas comunes, rápidas y sistemáticas de generar sucesiones es por medio de relaciones de recurrencia, de las cuales, como ya se vió, la sucesión de Fibonacci es un ejemplo. A continuación se retoma nuevamente esta sucesión para obtener algunos resultados que permitan dar una indicación para otros casos.

Recordemos que la sucesión de Fibonacci, $\{f_n\}$, esta dada por la relación de recurrencia lineal:

$$f_{n+1} = f_n + f_{n-1}, \text{ para } n \geq 1,$$

donde $f_0 = 1$ y $f_1 = 1$. A estos valores se les conoce como la *semilla* de la sucesión.

La relación anterior es equivalente a,

$$f_{n+1} - f_n - f_{n-1} = 0$$

a la cual se le puede asociar el polinomio:

$$f(x) = x^2 - x - 1 \in \mathbb{R}[x],$$

donde el grado del polinomio corresponde al número de términos de la relación de recurrencia y los coeficientes de la indeterminada corresponden a los términos de la sucesión en orden decreciente y el coeficiente de la máxima potencia de x es igual a 1, es decir, el polinomio es mónico. A este polinomio asociado a la sucesión se le llama *característico*.

Obsérvese que el polinomio $f(x)$ es irreducible sobre el campo de los números racionales $\mathbb{Q}$, por lo tanto se puede definir el campo:

$$K = \mathbb{Q}[x]/\langle f(x)\rangle,$$

donde $\langle f(x)\rangle$ es el ideal (principal) del anillo $\mathbb{Q}[x]$ generado por $f(x)$. Este campo es una extensión de Galois de grado 2 de los números racionales $\mathbb{Q}$ y es fácil ver que es isomorfo al campo $\mathbb{Q}(\sqrt{5})$. Ademas K es el campo de descompocición de $f(x)$ cuyas raíces son

$$\alpha_1 = \frac{1+\sqrt{5}}{2},\ \alpha_2 = \frac{1-\sqrt{5}}{2}.$$

Basados en el ejemplo de la sucesión de Fibonacci veamos ahora el caso de sucesiones binarias.

Para muchas cuestiones prácticas de las sucesiones es muy importante que estas sean lo mas impredecible posible, es decir, sean *aleatorias*. En general es difícil producir tales sucesiones, sin embargo para sucesiones binarias periódicas existen métodos para obtener las llamadas sucesiones *pseudo-aleatorias* las cuales deben satisfacer las siguientes condiciones, conocidas como los *postulados de Golomb*:

(1) El número de ceros y el número de unos sea el mismo en la medida de lo posible, es decir si n es el periodo de la sucesión, haya $\lceil n/2 \rceil$ ceros y unos.
(2) La mitad de las corridas en u ncíclo tengan longitud 1, un cuarto de las corridas tengan longitud 2, un octavo de las corridas tengan longitud 3, etc.
(3) La *autocorrelación* de la sucesión sea constante.

La tercera condición es quizá la mas importante y mas difícil de cumplir en una sucesión para que esta sea pseudo-aleatoria. En la sección 7 se abundará en el concepto de correlación de una sucesión.

Para usar las sucesiones binarias en criptografía, estas deben satisfacer las siguientes condiciones:

(1) El periodo n de la sucesión debe ser lo mas grande posible.
(2) La sucesión debe ser fácil y rápido de generar.
(3) El conocimiento de alguna parte del texto en claro con la correspondiente del texto cifrado no debe ser suficiente para determinar la sucesión completa empleada en el cifrado (este criptoanálisis se conoce como ataque de texto en claro conocido.)

Por consiguiente, si se desea tener sucesiones binarias para ser empleadas en criptografía, hay que ver la manera de obtener estas que satisfagan las condiciones antes mencionadas.

Sea $\{s_t\}$ una sucesión binaria, es decir, $s_t \in \mathbb{F}_2$ para toda $t \geq 0$. El *periodo* n de la sucesión $\{s_t\}$ es el menor entero positivo tal que $s_{t+n} = s_t$ par todo $t \geq 0$. Es decir, el periodo de la sucesión es el menor entero tal que los elementos de esta comienzan a repetirse.

Sea $\{s_0, s_1, ..., s_{n-1}\}$ la semilla y supóngase que el término s_n esta dado por la relación de recurrencia lineal

$$s_n = a_{n-1}s_{n-1} + a_{n-2}s_{n-2} + \cdots + a_1x + a_0,$$

donde $a_{n-1}, a_{n-2}, ..., a_0 \in \mathbb{F}_2$.

Como en el caso de la sucesión de Fibonacci, el polinomio *característico* de la sucesión $\{s_t\}$ es:

$$f(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^{n-2} - \cdots - a_1x - a_0.$$

Si $a = (a_{n-1}, a_{n-2}, ..., a_1, a_0)$ y $X = (x^n, x^{n-1}, ..., x, 1)$, recordando que $a = -a$ para todo elemento $a \in \mathbb{F}_2$, el polinomio $f(x)$ se puede escribir como

$$f(x) = (1, a) \cdot X = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x - a_0.$$

Para ilustrar los conceptos anteriores veamos algunos ejemplos.

Ejemplo 1. Sea $n = 4$, la longitud de la sucesión, semilla $(1, 0, 0, 0)$ y relación de recurrencia $s_{k+n} = s_k + s_{k+1}$ para $k \geq 1$. Por consiguiente,

$$s_5 = s_1 + s_2 = 1,\ s_6 = s_2 + s_3 = 0,\ s_7 = s_3 + s_4 = 0,\ s_8 = s_4 + s_5 = 1,\ \text{etc.}$$

Ejercicio. Determinar el periodo de esta sucesión.

Es fácil ver que el polinomio característico de esta sucesión es:

$$f(x) = x^2 + x + 1$$

Ejemplo 2. Sea $\{1, 0, 1, 1, 0, 0, 1, 1\}$ la semilla de una sucesión binaria $\{s_t\}$ con relación de recurrencia lineal

$$s_n = s_{n-1} + s_{n-4} + s_2 + s_0$$

para $n \geq 8$.

Por consiguiente se tiene que:

$$s_8 = s_7 + s_4 + s_2 + s_0 = 1 + 0 + 1 + 1 = 1,$$
$$s_9 = s_8 + s_5 + s_2 + s_0 = 1 + 0 + 1 + 1 = 1, \text{etc.}$$

Ejercicio. Determinar cual es la longitud de la sucesión, es decir, cuando se repiten los elementos de esta sucesión.

El polinomio caraterístico de esta sucesión es:

$$f(x) = x^8 + x^7 + x^2 + 1$$

3.5. Registros de Corrimiento de Retroalimentación Lineal

Una forma eficiente para obtener sucesiones binarias es por medio de los llamados *Registros de Corrimiento de Retroalimentación Lineal, RCRL* (Linear Feedback Shift Register, LFSR), el cual se describirá a continuación. El siguiente diagrama muestra el funcionamiento de estos registros.

Para iniciar se elige la longitud n del registro (sucesión) y se da un *estado* inicial $S_0 = (s_0, s_1, ..., s_{n-1})$ donde $s_i \in \mathbb{F}_2$ (bits). Obsérvese que el estado inicial se puede pensar como un elemento del espacio vectorial $\mathbb{F}_2^n$. El siguiente paso es generar el primer elemento de la sucesión. Con el estado inicial se considera la siguiente función lineal:

$$f(S_0) = S_0 \cdot C = c_0 s_0 + c_1 s_1 + \cdots + c_{n-1} s_{n-1},$$

la cual servirá como la función de retroalimentación para el *RCRL*. Por consiguiente el elemento s_n de la sucesión es

$$s_n = f(S_0) = S_0 \cdot C = c_0 s_0 + c_1 s_1 + \cdots + c_{n-1} s_{n-1},$$

y los elementos que aparecen el el registro son:

$$(s_1, s_2, ..., s_{n-1}, s_n).$$

Nuevamente, este se puede ver como un elemento del espacio vectorial $\mathbb{F}_2^n$.

Para ilustrar el funcionamiento de un *RCRL* veamos algunos ejemplos.

Ejemplo 1. Sea $n = 4$ la longitud del *RCRL*, $c_0 = c_1 = 1, c_2 = c_3 = 0$ y $S_0 = (1, 0, 0, 0)$ el estado inicial. Entonces $s_5 = s_) + s_1 = 0 + 1 = 1$, y el estado que produce el *RCRL* es $(0, 0, 0, 1)$. El siguiente estado que se produce en este *RCRL* es $(0, 0, 1, 0)$ ya que $f(0, 0, 0, 1) = 0 + 0 = 0$.

Ejercicio.

(1) ¿cuántos estados se obtienen en el ejemplo anterior?

(2) Si en cada aplicación del *RCRL* se obtiene un elemento de una sucesión, en el ejemplo anterior, ¿cual es el periodo de la sucesión?

3.6. Las m-sucesiones

En esta sección se introducirán las sucesiones binarias de máxima longitud, también conocidas como m-sucesiones, se darán algunas de sus propiedades así como algunos ejemplos.

En la sección anterior se mencionó que una propiedad que deben satisfacer las sucesiones para poder ser usadas en criptografía es que sean de longitud máxima. Así la pregunta natural es: ¿como obtener sucesiones de periodo máximo?.

Como se mencionó anteriormente, una manera de obtener sucesiones es por medio de un *RCRL*. Se dice que una sucesión generada por un *RCRL* con m entradas es una m-sucesión si su longitud es $2^m - 1$. Las m-sucesiones son tambien conocidas como *PN*-sucesiones (*pseudo-noise*).

Si las sucesiones son generadas por un *RCRL*, ¿como determinar si un *RCRL* genera una m-sucesión? A continuación se dará una respuesta a esta pregunta.

Si $c_0, c_1, ..., c_{n-1}$ son los coeficientes asociados a un *RCRL*, el polinomio *característico* del *RCRL* esta definido como:

$$f(x) = 1 + c_1 x_1 + \cdots + c_{n-1} x^{n-1} + x^n,$$

Ahora se tiene el siguiente,

LEMMA 3.6.1. *Sea $f(x)$ el polinomio característico de un RCRL. Entonces,*

$$\Omega(f) = \{(s_i)_{i\geq 0} \ : \ s_{k+n} = \sum_{i=0}^{n-1} c_i s_{k+i}\}$$

es un espacio vectorial de dimensión n sobre $\mathbb{F}_2$.

Obsérvese que $\Omega(f)$ es el conjunto de sucesiones cuyo polinomio característico es $f(x)$.

Ejercicio. Dar una demostración del Lema anterior.

El siguiente resultado caracteriza las m-sucesiones:

THEOREM 3.6.2. *Una sucesión binaria (distinta de cero) producida por un RCRL con polinomio característico $f(x)$ es una m-sucesión si y sólo si $f(x)$ es un polinomio primitivo.*

Para ilustrar este resultado veamos un ejemplo. $m = 5$ y

Ejemplo. Sea $f(x) = 1 + x^3 + x^5$ (probar que este polinomio es primitivo). Es fácil ver que en cada etapa el estado generado por el *RCRL* correspondiente se puede ver como un elemento (distinto de cero) del espacio vectorial $\mathbb{F}_2^5$, el cual tiene cardinalidad 32. Por ejemplo si el estado inicial es $(1, 0, 0, 0, 0)$, el siguiente estado es $(0, 0, 0, 0, \mathbf{1})$, y el siguiente $(0, 0, 0, 1, \mathbf{0})$, etc. La sucesión que se va obteniendo es $0, \mathbf{1}, \mathbf{0}, \ldots$

De acuerdo al Teorema anterior, para obtener m- sucesiones (binarias), es decir, de máxima longitud $2^m - 1$, es necesario obtener polinomios primitivos de grado m, y esto conlleva a la pregunta natural: dado un entero $m > 3$, ¿cómo se obtienen polinomios primitivos de grado m? Obviamente para cuestiones prácticas se requieren sucesiones binarias de longitud

Capítulo 4

Correlación cruzada

En esta sección se introducirá la función de *correlación cruzada* de dos sucesiones cuyos elementos estan en el conunto $\{+1, -1\}$, en particular aquellas que provienene de suscesiones binarias de máxima longitud. Se determinarán los valores de la función de correlación cruzada de las llamadas sucesiones de Gold ([**1**]] las cuales son de gran importancia por sus aplicaciones en sistemas de comunicación multi-usuario.

4.1. La función de correlación cruzada

En las siguientes líneas se recordará la definición de *correlación curzada (crosscorrelaction)* de dos sucesiones cuyas componentes son elementos del conjunto (grupo) $\{+1, -1\}$.

Sean $x = (x_0, x_1, ..., x_{n-1}), y = (y_0, y_1, ..., y_{n-1})$ dos sucesiones de longitd n cuyas componentes son elementos de $\{+1, -1\}$ y sea τ un entero tal que $0 \leq \tau \leq n-1$. La función de correlación cruzada de x y y, $C(x, y)(\tau)$ o simplemente $C(\tau)$, se define como

$$C(\tau) = \sum_{i=0}^{n-1} x_i y_{i+\tau},$$

donde los índices son reducidos módulo n.

A continuación se darán algunas oservaciones.

(1) Sea A un conjunto (no-vacio) y A^n su producto cartesiano n veces. El *corrimiento cíclico,* σ, sobre A^n se define como

$$\sigma : A^n \longrightarrow A^n, \sigma(a_0, a_1, ..., a_{n-1}) = (a_{n-1}, a_0, ..., a_{n-2})$$

Obsérvese que esta función es una permutación de A^n. Si τ es tal que $0 \leq \tau \leq n-1$ se define

$$\sigma_\tau = \sigma \circ \cdots \circ \sigma, \ (\tau - \text{veces})$$

done " $\circ$ " denota composición de funciones.

(2) Si $y = (y_0, y_1, ..., y_{n-1})$ es una sucesión y τ es tal que $0 \leq \tau \leq n-1$, entonces

$$\sigma_\tau(y) = (y'_0, y'_1, ..., y'_{n-1})$$

donde $y'_{\tau+i} = y_i$.

En términos de la función σ_τ y del producto "punto" $\cdot$, la función de correlación cruzada de dos scesiones se puede expresar como

$$C(\tau) = x \cdot \sigma_\tau(y).$$

Ejemplo. Considérese las sucesiones $x = (-1, -1, -1, +1, -1, +1, +1)$ y $y = (-1, +1, +1, -1, +1, -1, -1, -1)$. Es fácil ver que

$$C(0) = -5, C(1) = 3, C(2) = 3, C(3) = -1, C(4) = 3, C(5) = -1, C(6) = -1.$$

Una forma alternativa de definir la funcion de correlación cruzada de dos sucesiones $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, ..., y_{n-1})$ donde sus entradas estan en el mismo conjnto, es la siguiente([]):

$$C(x, y) = A - D$$

donde A es el úmero de elementos que coinciden de ambas sucesiones y D el número de elementos que no coinciden.

Si x, y son dos sucesiones de longitd n y σ_τ es como antes, entonces la función de correlación cruzada $C(\tau)$ es:

$$C(\tau) = A(\tau) = D(\tau)$$

donde $A(\tau)$ y $D(\tau)$ es el úmero de elementos que coinciden de las sucesiones x y $\sigma(y)$, y $D(\tau)$ el número de elementos de esas sucesiones que no coinciden.

Es fácil ver que en el Ejemplo anterior:

$$C(0) = A(0) - D(0) = 1 - 6 = -5, C(1) = A(1) - D(1) = 5 - 2 = 3, \text{etc.}$$

4.2. Correlación cruzada y distancia de Hamming

Veamos como la función de correlacióncruzada introducida en la secciónanterior se puede expresar en términos del peso de Hamming cuando las sucesiones en cuestión son binarias.

Recordemos que el peso de Hamming de $a = (a_0, a_1, ..., a_{n-1}) \in \mathbb{F}_2^n$ es:

$$p_H(a) = |\{i : a_i \neq 0\}|$$

es decir, $p_H(a)$ es el número de coordenadas distintas de cero de a.

Si

Si $a = (a_0, a_1, ..., a_{n-1}), b = (b_0, b_1, ..., b_{n-1}) \in \mathbb{F}_2^n$ su distancia de Hamming es:

$$d_H(a, b) = p_H(a - b)$$

es decir, $d_H(a, b)$ es igual al número de coordenadas donde a y b no coinciden. Por lo tanto, el úmero de coordenadas donde ambas sucesiones coinciden es:

$$A = n - d_H(a, b)$$

Por consiguiente, en términos de la distancia de Hamming, la función de correlación cruzada de las sucesiones a y b se puede expresar como:

$$\begin{aligned} C(0) &= A(0) - D(0) = (n - d_H(a, b)) - d_H(a, b) \\ &= n - 2d_H(a, b) = n - 2p_H(a - b). \end{aligned}$$

Por ejemplo, si consideramos las sucesiones del ejemplo anterior y si $C(3) = -1$, de la relación previa se sigue que:

$$d_H(a, \sigma_3(b)) = 2^{3-1} = 2^2 = 4.$$

Como se puede ver, este ejemplo es un caso particular del siguiente resultado, el cual es obvio de la relación dada anteriormente entre la función de relación cruzada y la distancia de Hamming:

Si a y b son dos sucesiones binarias de longitud $n = 2^m - 1$, entonces $C(0) = -1$ si y sólo si $d_H(a, b) = 2^{m-1}$.

4.3. Correlación cruzada de m-sucesiones

Por el resto de este trabajo se trabajará con m-sucesiones, en particular se obtendrá la correlación curzada de dos sucesiones de esta naturaleza.

Si $x = (x_i), y = (y_i)$ son dos m-sucesiones de longitd $n = 2^m - 1$, de la sección ... los elementos de esas sucesines tienen la forma $Tr(y^t)$ donde y es un elemento primitivo delcampo $\mathbb{F}_2^m$ y Tr es la función traza de $\mathbb{F}_2^m$ en $\mathbb{F}_2$. Mas aún por el Teorema ... se puede suponer que cada elemento de las scesiones tiene la siguiente expresión:

$$x_t = Tr(\alpha^t), \quad y_t = Tr(\alpha^{dt})$$

donde α es un elemento primitivo de $\mathbb{F}_2^m$ y d es un entero tal que $1 \leq d \leq n - 1$ y primo relativo con n, es decir, d es un elemento del grupo de unidades de $\mathbb{Z}_n$.

En este caso la definición de correlación cruzada tiene la siguiente expresión:

$$C(\tau) = \sum_{t=0}^{n-1} (-1)^{Tr(\alpha^{t+\tau} + \alpha^{dt})}.$$

Si $\beta = \alpha^{\tau}$, la cual es una constante y como t toma los valores de 1 a $n-1$, α^t recorre los elementos no-cero del campo $\mathbb{F}_2^m = GF(2^m)$, la función $C(\tau)$ se puede expresar como:

$$C(\tau) = \sum_{x \in GF(2^m)^*} (-1)^{Tr(\beta x + x^d)}$$

Esta última expresión de la función $C(\tau)$ es un caso particular de las llamadas *sumas exponenciales*, las cuales son de gran interés y ampliamente estudiadas en Teoría de Números asi como en Teorá de Códigos Lineales. Por ejemplo, si $d = -1$, la expresión corespondiente es conocida como la *suma de Kloosterman*.

4.4. Propiedades criptográficas de las m-sucesiones

Sabiendo como se generan sucesiones binarias de máxima longitud, las m-sucesiones, veamos hasta que punto estas satisfacen las condiciones para ser usadas en criptografía mencionados en la Sección 5.1.

C1. Como las sucesiones generadas por un *RCRL* de m etapas puede alcanzar un periodo de longitud $2^m - 1$, se pueden tener sucesiones lo suficientemente grandes (por ejemplo si $m = 166$ el periodo es del orden de 10^{50}).

C2. Los *RCRL* son bastante fáciles de implementar.

C3. Las m-sucesiones son muy inseguras ! y por lo tanto no se pueden usar en sistemas de cifrado robustos. A continuación se da un argumento el porque estas sucesiones no son seguras.

Capítulo 5

Las sucesiones de Gold

Como se mencionó anteriormente, las sucesiones binarias se usan en varios contextos, pero estas deben tener propiedades muy particulares. Una de estas sucesiones es la llamada *sucesión de Gold* la cual tiene la particularidad de que su función de correlación tomo pocos valores. Estas sucesiones (o variaciones de estas) son actualmente usadas en los Sistemas de Posicionamiento Global (Global Positioning System, GPS). En esta sección se introduces estas sucesiones y se determina su función de correlación cruzada para lo cual se segue el trabajo original ([**1**]). El resultado principal es el siguiente:

THEOREM 5.0.1. *Sean* $a = (a_i), b = (b_i)$ *dos sucesiones binarias de máxima longitud dadas por* $a_i = (-1)^{Tr(\alpha^{-i})}$ *y* $b_i = (-1)^{Tr((\alpha^{2^e+1})^{-1})}$ *donde* α *es un elemento primitivo del campo* $GF(2^m)$*,* m *impar y* e *es tal que* $1 \leq e \leq n-1$ *y* $(e,n) = 1$*. Entonces,*

$$C(\tau) = \quad -1 \text{ si } a_\tau = 1,$$
$$C(\tau) = \quad -(2^{(n+1)/2}+1) \text{ o } (2^{(n+1)/2}-1) \text{ si } a_\tau = -1$$

La demostración de este resultado será basada en el trabajo [**1**] pero antes se dará una conexión con Códigos cíclicos.

THEOREM 5.0.2. *Sea* m *impar,* $f_1(x)$ *el polinomio primitivo que tiene como raíz a* α *y* $f_2(x)$ *el polinomio irreducible que tiene como raíz a* α^{2^e+1}*. Sea* $\mathscr{C} = \langle f_1(x)f_2(x)\rangle$ *el código cíclico generado por* $f_1(x)f_2(x)$ *y sea* $\mathscr{D} = \mathscr{C}^\perp = \langle h(x)\rangle$ *el código dual de* $\mathscr{C}$ *generado por el polinmio* $h(x) = ...$ *Si* $0 \neq c$ *es una palabra de* $\mathscr{D}$ *y* $p_H(c)$*su peso de Hamming, entonces*

$$p_H(c) \in \{2^{m-1}, 2^{m-1}+2^{(m-1)/2}, 2^{m-1}-2^{(m-1)/2}\}$$

En [**2**] se enuncia la distribución de pesos del código $\mathscr{D}$.

Antes de dar la demostración del Teorema 3, veamos su relación con el Teorema 4.

En la subsección ... la función de correlación cruzada para dos sucesiones a y b de longitud $n = 2^m - 1$, se expresó como:

$$C = n - 2d_H(a,b)$$

Consideremos ahora las sucesiones $\sigma_\tau(a)$ y b. De la relación anterior se sigue que:

$$C = n - 2d_H(\sigma_\tau(a), b)$$

Por consiguiente,

$$C = -1 \iff d_H(\sigma_\tau(a), b) = 2^{m-1},$$
$$C = -(2^{(n+1)/2} + 1) \iff d_H(\sigma_\tau(a), b) = 2^{m-1} + 2^{(m-1)/2},$$
$$C = (2^{(n+1)/2} - 1) \iff d_H(\sigma_\tau(a), b) = 2^{m-1} - 2^{(m-1)/2}.$$

Para la demostración de el Teorema 3 se requieren los siguientes resultados:

PROPOSITION 5.0.3. *Sea* $(m, e) = 1$. *Entonces la ecuación* $x^{2^{-e}+1} + x^{2^e} + c = 0$ *tiene solución en* $GF(2^m)$ *si y sólo si* $Tr(c) = 0$.

PROPOSITION 5.0.4. *Si* a, b *son dos sucesiones binarias de period* p *entonces,*

$$\sum_{i=0}^{p-1} [C_{a,b}(\tau)]^2 = \sum_{i=0}^{p-1} [C_{a,a}(\tau)][C_{b,b}(\tau)].$$

Demostración del Teorema 3.

Sea $S(\alpha^{-i}) = a_i = (-1)^{Tr(\alpha^{-i})}$ y $S((\alpha^{2^e+1})^{-i}) = b_i = (-1)^{Tr((\alpha^{2^e+1})^{-i})}$. Entonces,

$$\begin{aligned} C(\tau) &= \sum_{i=0}^{2^n-2} a(i+\tau)b(i) = \sum_{i=0}^{2^n-2} S(\alpha^{-(i+\tau)})S((\alpha^{2^e+1})^{-i}) \\ &= \sum_{i=0}^{2^n-2} S[(\alpha^{-(i+\tau)}) + (\alpha^{2^e+1})^{-i})] = \sum_{i=0}^{2^n-2} S[(\alpha^{-\tau}(\alpha^{-i}) + (\alpha^{-i})^{2^e+1}]. \end{aligned}$$

Sea $c = \alpha^{-\tau}$. Como $S(0) = 1$, se tiene que

$$C(\tau) = [\sum_{x \in GF(2^m)} S(cx + x^{2^+1})] - 1.$$

Obsérvese que la función $x \longrightarrow x + y$ es una permutación del campo $GF(2^m)$, para cualquier $y \in GF(2^m)$, la expresión para la correlación cruzada se puede expresar como:

$$\begin{aligned} C(\tau) &= [\sum_{x \in GF(2^m)} S[c(x+y) + (x+y)^{2^+1}]] - 1 \\ &= [\sum_{x \in GF(2^m)} S[cx + cy + x^{2^e+1} + x^{2^e}y + xy^{2^e} + y)^{2^+1}]] - 1 \end{aligned}$$

Observando que para todo $y \in GF(2^m)$, $Tr(y) = Tr(y^{2^e+1})$ se tiene que $S(x^{2^e}y) = S(xy^{2^{-e}})$, y por lo tanto,

$$C(\tau) = [\sum_{x \in GF(2^m)} S[x(c + y^{2^{-e}} + y^{2^e}) + x^{2^e+1} + (cy + y)^{2^e+1}]] - 1$$

A continuación se analizarán los dos casos: $a(\tau) = 1$ y $a(\tau) = -1$.

Caso 1: $a(\tau) = 1$.

Obsérvese que

$$a(\tau) = 1 \iff S(\alpha^{-\tau}) = 1 \iff Tr(\alpha^{-\tau}) = Tr(c) = 0.$$

En este caso, de la Proposición 5 (ver mas adelante) se sigue que la ecuación $c + x^{2^{-e}} + x^{2^e} = 0$ tiene solución en el campo $GF(2^m)$. Sea β una tal solución. Observando que $S(u + v) = S(u)S(v)$, la expresión para $C(\tau)$ queda como:

$$\begin{aligned} C(\tau) &= [\sum_{x \in GF(2^m)} S[x^{2^e+1} + c\beta + \beta)^{2^e+1}]] - 1 \\ &= [\sum_{x \in GF(2^m)} S(x^{2^e+1})S(c\beta + \beta^{2^e+1})] - 1 \\ &= [S(c\beta + \beta^{2^e+1})][\sum_{x \in GF(2^m)} S(x^{2^e+1})] - 1 \end{aligned}$$

Como

$$\sum_{x \in GF(2^m)} S(x^{2^e+1}) = \left(\sum_{i=0}^{2^m-2} b(i)\right) - 1 = 0$$

se concluye que

$$C(\tau) = -1$$

Caso 2: $a(\tau) = -1$.

Obsérvese que

$$a(\tau) = -1 \iff S(\alpha^{-\tau}) = S(c) = -1 \iff Tr(\alpha^{-\tau}) = Tr(c) = 1.$$

Como m es impar, $Tr(1) = 1$ y por lo tanto, $Tr(c + 1) = 0$. Nuevamente por la Proposición 5 sea $\beta \in GF(2^m)$ una solución de la ecuación

$(c+1)+x^{2^{-e}}+x^{2^e}=0$.Por lo tanto,

$$\begin{aligned} C(\tau) &= [\sum_{x\in GF(2^m)} S[x+x^{2^e+1}+c\beta+\beta)^{2^e+1}]]-1 \\ &= [S(c\beta+\beta^{2^e+1})][\sum_{x\in GF(2^m)} S(x)S(x^{2^e+1})]-1 \\ &= \pm 1\left[[\sum_{i=0}^{2^m-2} S(\alpha^{-i}S(\alpha^{2^e+1})^{-i})]+1\right]-1 \\ &= \pm 1\left[[\sum_{i=0}^{2^m-2} a(i)b(i)+1]\right]-1 \\ &= \pm 1[C(0)+1]-1 \end{aligned}$$

Por lo tanto,

Si $a(\tau)=-1$ y $S(c\beta+\beta^{2^e+1})=1$ se tiene que

$$C(\tau)=C(0)$$

y si $a(\tau)=-1$ y $S(c\beta+\beta^{2^e+1})=-1$,

$$C(\tau)=C(0)+2$$

Si $c\in GF(2^m)$ es tal que $Tr(c)=1$ sea $\beta\in GF(2^m$ una solución de la ecuación $c+x^{2^{-e}}+x^{2^e}=1$. Obsérvese que $\beta+1$ es tambien solucion de esta ecuación, y como m es impar, se puede tomar a la solución β de tal manera que $Tr(\beta)=1$.

De la relación $c+\beta^{2^{-e}}+\beta^{2^e}=1$ se sigue que $c\beta+\beta^{2^{-e}+1}=\beta+\beta^{2^e+1}$ y por lo tanto $S(c\beta+\beta^{2^{-e}+1})=S(\beta+\beta^{2^e+1})$.

Dado que hay una biyección entre los conjuntos

$$\{c\in GF(2^m): Tr(c)=1\} \text{ y } \{\beta\in GF(2^m): Tr(\beta)=1\}$$

entonces,

$$\begin{aligned} &|\beta\in GF(2^m): S(c\beta+\beta^{2^{-e}+1})=S(\beta+\beta^{2^e+1})=-1| \\ &\quad =|\beta\in GF(2^m): Tr(\beta)=1 \text{ y } Tr(\beta^{2^e+1})=0| \end{aligned}$$

y se puede ve que

$$|\beta\in GF(2^m): Tr(\beta)=1 \text{ y } Tr(\beta^{2^e+1}=0)|=[(2^m-1)-C(0)]/4.$$

Por lo tanto,

$$\begin{aligned} C(\tau) &= -[C(0)+2]\frac{(2^m-1)-C(0)}{4} \text{ veces} \\ C(\tau) &= C(0)\frac{(2^m-1)+[C(0)+2}{4} \text{ veces} \\ C(\tau) &= (-1)\frac{(2^m-1)-1}{2} \text{ veces} \end{aligned}$$

Para determinar los valores de la función $C(\tau)$ se usará el resultado de la Proposición 2:

$$\sum_{i=0}^{2^m-2} C^2(a,b)(\tau) = \sum_{i=0}^{2^m-2} C(a,a)(\tau)C(b,b)(\tau).$$

Si x es una sucesión de máxima longitud, $C(x,x)(\tau) = -1$ para $\tau \neq 0$ y $C(x,x)(0) = 2^m - 1$, se tiene que

$$\sum_{i=0}^{2^m-2} C^2(a,b)(\tau) = (2^m-1)^2 + (2^m-1) - 1$$

Si $p = 2^m - 1$ y $C_{a,b}(0) = \theta$, substituyendo para $C_{a,b}(\tau)$ se tiene que

$$\frac{\theta^2[p+\theta+2]}{4} + \frac{[\theta+2]^2[p=\theta]}{4} + \frac{[p-1]}{2} = p^2 + p - 1$$

y esta relación se reuce a:

$$2\theta(p-1) + 4\theta(p-1) + 2(p-1) = 4(p-1)(p+1)$$
$$\theta^2 + 2\theta - (2p+1) = [\theta + (2^{(m+1)/2}+1)][\theta - (2^{(m+1)/2}-1)]$$

y por lo tanto,

$$C_{a,b}(0) = -(2^{(m+1)/2}+1),$$

o bien,

$$C_{a,b}(0) = (2^{(m+1)/2}-1).$$

Bibliografía

[1] Gold, R. Maximal Recursive sequences with 3-Valued Recursive Cross-Correlation Functions, IEEE Trans. on Inf. Theory, January, 1968, pp.154-156.

[2] Robert J. McEllice, *Finite Fields for Computer and Scientist and Engineers*, Kluwer Academic Publishers

[3] Henk C.A. van Tilborg, *Fundamentals of Cryptology, A Professional Reference and Interactive Tutorial*, Kluwer Academic Publishers, 2010