ENCRIPTAMIENTO DE DATOS MEDIANTE CONVOLUCIÓN ARITMÉTICA

Prelat Daniel[†], Maulhardt Martín[†], Cordero Tomás[†] y Cipriano Marcelo[†]

[†]*Escuela Superior Técnica, IESE, CABA, Argentina.*

Resumen: La convolución aritmética (también llamada convolución de Dirichlet) es una operación ya clásica de la teorá analítica de números cuyas propiedades creemos pueden ser muy efectivas en su aplicación al procesamiento de señales de tiempo discreto. La transformación que convierte esta convolución en el producto usual de funciones es denominada "transformada de Dirichlet", pues su definición utiliza las series homónimas. En este trabajo presentamos una aplicación de la convolución aritmética y la transformada de Dirichlet al diseño de un sistema de encriptamiento de datos. Luego de una breve exposición de los conceptos y propiedades básicas de las herramientas matemáticas, describimos un sistema de encriptamiento transmisión desencriptamiento. Los datos consisten en señales de tiempo discreto y el encriptamiento y desencriptamiento se realizan mediante convoluciones aritméticas.

Palabras clave: *convolución de Dirichlet, encriptamiento de datos, procesamiento de señales.*
2000 AMS Subject Classification: 68P25-11M06-30B50

1. INTRODUCCIÓN - LA CONVOLUCIÓN ARITMÉTICA

Presentaremos la convolución aritmética y sus propiedades básicas, restringiéndonos principalmente a las que utilizaremos en las aplicaciones. Incluimos las demostraciones de algunas de ellas (las que no figuran en los textos de teoría de números), indicando la bibliografía correspondiente para las restantes.

En el álgebra de las funciones $f : \mathbb{N} \longrightarrow \mathbb{C}$, se define como convolución aritmética de dos funciones $f : \mathbb{N} \longrightarrow \mathbb{C}, g : \mathbb{N} \longrightarrow \mathbb{C}$ a la función $f * g : \mathbb{N} \longrightarrow \mathbb{C}$ tal que

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{d|n} g(d)f\Big(\frac{n}{d}\Big) \tag{1.1}$$

donde la suma se extiende a los divisores positivos de n. La primera igualdad es la definición y la segunda $-$ que significa que la convolución es conmutativa $-$ es consecuencia de que aplicación $d \longmapsto \dfrac{n}{d}$ es una permutación en el conjunto de los divisores de n. Otras propiedades importantes para las aplicaciones, de esta operación son: la bilinealidad, la asociatividad, la existencia de un neutro (se trata de la versión aritmética de la delta de Dirac): $\delta_1 : \mathbb{N} \longrightarrow \mathbb{C}$ tal que $\delta_1(1) = 1$ y $\delta_1(n) = 0$ si $n \neq 1$. Todas estas propiedades sugieren la posibilidad de aplicaciones al tratamiento de señales de tiempo discreto $f : \mathbb{N} \longrightarrow \mathbb{C}$ que se anulan en los enteros no positivos, lo mismo que ocurre con las señales de tiempo continuo que se consideran cuando se utiliza la transformación de Laplace. El tipo de sistema lineal a considerar es de la forma

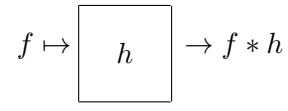

Figura 1: Sistema lineal.

donde h es una función determinada (se trata de la función del sistema). La bilinealidad de la convolución implica la linealidad de este tipo de sistema. La asociatividad implica que dos de estos sistemas, puestos en serie,

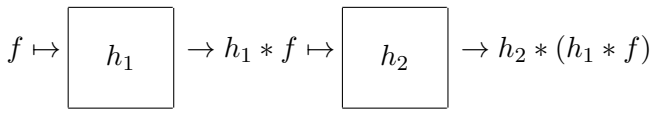

Figura 2: Propiedad asociativa.

sea equivalente al sistema convolucional dado por la función $h_2 * h_1$ (además, nuevamente, la conmutatividad de la convolución implica que el orden en que estos sistemas se colocan en serie es irrelevante).

Una de las ventajas operacionales de esta convolución es que no presenta problemas de convergencia: para cada n, la suma (1.1) es finita. Por otra parte, el conjunto de divisores positivos de n está incluido en $\{1, 2, \ldots, n\}$, de donde se deduce fácilmente que para cualquier par de funciones $f : \mathbb{N} \longrightarrow \mathbb{C}, g : \mathbb{N} \longrightarrow \mathbb{C}$,

$$\|f * g\|_1 \leq \|f\|_1 \|g\|_1 \tag{1.2}$$

donde $\|f\|_1 = \sum_{n=1}^{\infty} |f(n)| < +\infty$ es la "potencia"de f. Entonces, un sistema como el de la figura 1, tal que $\|h\|_1 = \sum_{n=1}^{\infty} |h(n)| < +\infty$ es estable en el sentido de que para cada entrada $f : \mathbb{N} \longrightarrow \mathbb{C}$ tal que $\|f\|_1 < +\infty$ se obtiene una respuesta $f * g$ tal que $\|f * h\|_1 < +\infty$. La transformación adecuada para esta convolución está dada por las series de Dirichlet: para cada $f : \mathbb{N} \longrightarrow \mathbb{C}$ se define su correspondiente serie de Dirichlet (también denominada función generatriz; en el contexto del presente trabajo podríamos denominarla "transformada de Dirichlet"):

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \tag{1.3}$$

Dejando de lado cuestiones de convergencia (o bien pensando en estas series como series formales), se puede demostrar que si $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ y $G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ entonces se tiene la siguiente fórmula de convolución:

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s} \tag{1.4}$$

Hemos mencionado solamente algunas propiedades básicas que necesitaremos a continuación. Por ejemplo, no hemos expuestola relación entre la transformación de Möbius y la convolución aritmética, la fórmula de inversión de Perron, ni tampoco una tabla de transformadas importantes. Todo esto puede consultarse en la vasta bibliograía existente, dentro de la cual mencionamos dos obras clásicas del mismo autor ([1] y [2]): Tom M. Apostol.

2. Espectro de la convolución aritmética

Las señales que vamos a considerar son de la forma $f : \mathbb{Z} \longrightarrow \mathbb{C}$ y tales que $f(n) = 0, \forall n \leq 0$. Además son de potencia finita, es decir: $\|f\|_1 = \sum_{n=1}^{\infty} |f(n)| < +\infty$. La transformada de Fourier de este tipo de señales resulta ser una función continua (por la condición de convergencia): $\Im(f)(\omega) = \sum_{n=1}^{\infty} f(n)e^{-in\omega}$. Se trata, obviamente de una función periódica de período 2π.

Lema 1 *Sean dos señales $f : \mathbb{Z} \longrightarrow \mathbb{C}$ y $g : \mathbb{Z} \longrightarrow \mathbb{C}$ en l_1 (es decir: de potencia finita) tales que $f(n) = g(n) = 0$, $\forall n \leq 0$, se verifica:* $\Im(f * g)(\omega) = \sum_{k=1}^{\infty} g(k)\Im(f)(k\omega)$

Prueba. $\Im(f * g)(\omega) = \sum_{n=-\infty}^{+\infty} (f * g)(n)e^{-in\omega} = \sum_{n=1}^{+\infty} (f * g)(n)e^{-in\omega} = \sum_{n=1}^{+\infty} \left(\sum_{d|n} g(d) f\left(\frac{n}{d}\right) \right) e^{-in\omega} =$

$$= \sum_{k=1}^{+\infty} \sum_{m=1}^{+\infty} g(k)f(m)e^{-ikm} = \sum_{k=1}^{+\infty} g(k) \left(\sum_{n=1}^{+\infty} f(n)e^{-ikn\omega} \right) = \sum_{k=1}^{+\infty} g(k)\Im(f)(k\omega)$$

La segunda igualdad se debe a que $(f * g)(n) = 0, \forall n < 0$. $\square$

Nota 1: Para señales de soporte finito, todas estas sumas son finitas. Caso contrario deben considerarse señales en l_1, como hemos supuesto en el enunciado.

Nota 2: Un teorema análogo es válido para dominios temporales y también para la transformada Z, con demostraciones similares.

3. APLICACIÓN AL ECRIPTAMIENTO DE DATOS.

Se trata de un sistema que puede esquematizarse de la siguiente manera

Figura 3: Sistema de encriptamiento.

y la clave de su funcionamiento es, obviamente, la función de transferencia h, que deber elegirse adecuadamente. Pasamos a exponer nuestra elección.

Sean $a \in \mathbb{Z}$ tal que $a > 1$ y $r \in \mathbb{R}$ tal que $0 < r < 1$. Definimos $h : \mathbb{Z} \longrightarrow \mathbb{C}$ tal que $h\left(a^k\right) = r^k$, $\forall k = 0, 1, 2, 3, \ldots$ y $h(n) = 0$ si $n \notin \left\{1, a, a^2, a^3, \ldots\right\}$ (en particular, $h(n) = 0\ \forall n \leq 0$). Entonces:

I. h es de potencia finita: $\|h\|_1 = \sum_{n=-\infty}^{+\infty} |h(n)| = \sum_{k=0}^{+\infty} \left|h(a^k)\right| = \sum_{k=0}^{+\infty} r^k \overset{0<r<1}{=} \frac{1}{1-r} < +\infty$

II. h tiene inversa convolucional aritmética: se puede calcular fácilmente mediante su transformada de Dirichlet: $H(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s} = \sum_{k=0}^{\infty} \frac{h(a^k)}{(a^k)^s} = \sum_{k=0}^{\infty} \frac{r^k}{(a^k)^s} \overset{|\frac{r}{a^s}|<1}{=} \frac{1}{1-\frac{r}{a^s}}$ por lo tanto, $\frac{1}{H(s)} = 1 - \frac{r}{a^s}$ y resulta $h^{(1)} : \mathbb{N} \longrightarrow \mathbb{C}$ tal que $h^{(1)}(1) = 1$, $h^{(1)}(a) = -r$ y $h^{(1)}(n) = 0$ si $n \notin \{1, a\}$

III. $h^{(1)}$ es obviamente de potencia finita: $\left\|h^{(1)}\right\|_1 = \sum_{n=-\infty}^{+\infty} \left|h^{(1)}(n)\right| = 1 + r.$

IV. Del Lema 1 tenemos, para cualquier $f : \mathbb{Z} \longrightarrow \mathbb{C}$ tal que $f(n) = 0\ \forall n \leq 0$ y de potencia finita:

$$\Im(f * h)(n) = \sum_{n=-\infty}^{+\infty} h(n)\Im(f)(n\omega) = \sum_{k=0}^{+\infty} r^k \Im(f)(a^k\omega)$$

$$\Im(f * h^{(1)})(n) = \sum_{n=-\infty}^{+\infty} h^{(1)}(n)\Im(f)(n\omega) = \Im(f)(\omega) - r\Im(f)(a\omega)$$

Veamos un ejemplo del efecto producido por esta función de transferencia en los espectros de las señales convolucionadas y su recuperación final.

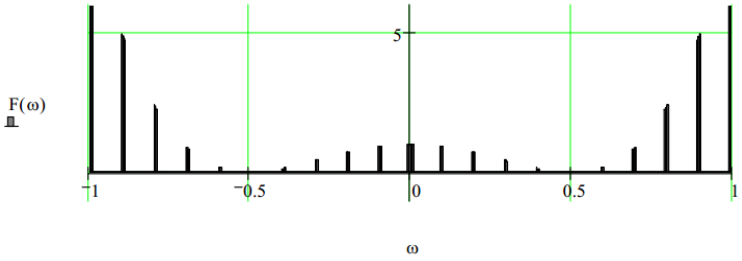

Figura 4: Espectro de la señal inicial.
La información está contenida en la banda central $[0.5, 0.5]$

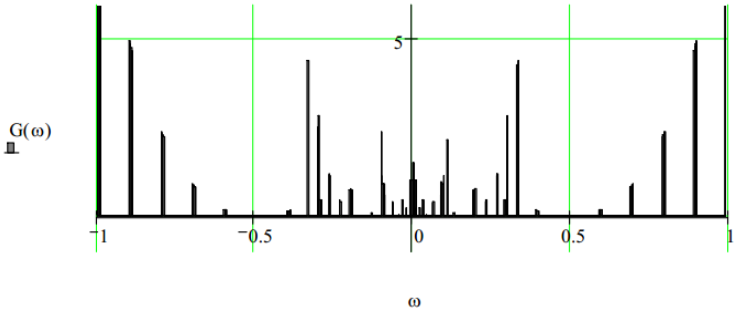

Figura 5: Espectro de la señal resultante de la convolución aritmética de la señal anterior con la función de transferencia h

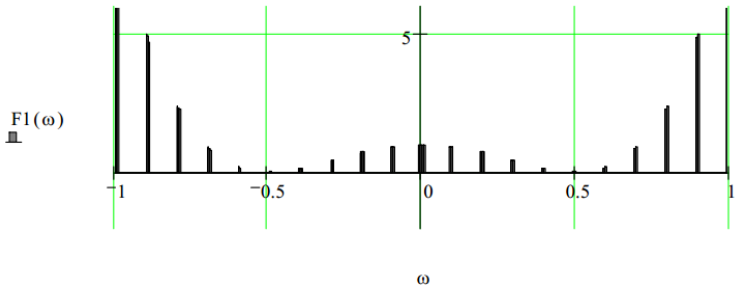

Figura 6: Espectro de la señal resultante de la convolución aritmética de la señal anterior con la inversa convolucional de h. Esta señal es exactamente la señal inicial.

El fenómeno de perturbación central, fundamental para el objetivo buscado, está relacionado con los siguientes parámetros: el entero positivo a y las frecuencias discretas $\omega_m = \frac{m}{M}$ de la señal inicial $-M \leq m \leq M$ (hemos puesto el espectro de f entre -1 y 1 sin pérdida de generalidad).

4. Implementación práctica

Utilizaremos estas herramientas para diseñar un sistema de comunicacíon transmisor/receptor en el que el transmisor conoce la función f y el receptor la función $h^{(1)}$. La idea es distorsionar (encriptar) f con la función h de tal forma que no pueda ser escuchada por cualquier otro receptor, salvo aquel que conoce la función $h^{(1)}$. Para la simulación del sistema, se puede utilizar el siguiente esquema:

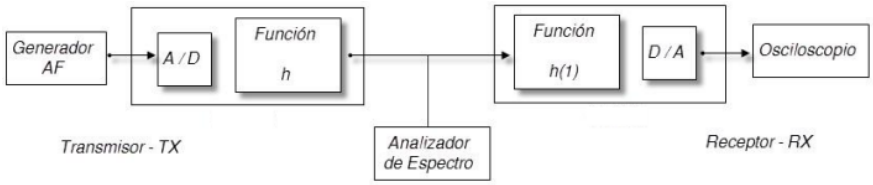

Figura 7: Sistema de comuniciones.

Funcionamiento del Sistema de comunicación: lo que se va utilizar como señal de información f es una función senoidal de $1kHz$, esta se muestrea para obtener una señal discreta y luego se aplica la función transferencia h mediante la convolución aritmética. La señal obtenida $f * h$ es transmitida hacia el receptor. Luego, el receptor, aplica la inversa convolucional de h a la señal que le llega del transmisor, y obtiene la señal f de $1kHz$. En el analizador de espectro se podrá ver la señal $f * h$ y en el osciloscopio se espera ver simplemente la señal f original.

Referencias

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Undegraduate Texs in Math, Springer-Verlag, NY, (1979)

[2] T.M. Apostol, *Modular Funions and Dirichlet Series in Number Theory*, Undegraduate Texs in Math, Springer-Verlag, NY, 2d edition (1989).