Teorema de Equidistribucion de Weyl y Criptografia

Daniel Prelat, Martín Maulhardt y Tomas Cordero

Escuela Superior Técnica del Ejército

Abstract. Explicamos de una forma nueva que una clásica sucesión está equidistribuida. Damos también la demostración estándar de dicho Teorema y mostramos algunas de sus posibles aplicaciones a la seguridad criptografía.

1. PRELIMINARES PARA EL TEOREMA DE WEYL

Sea R el conjunto de los números reales. Denotemos con I al conjunto de los números irracionales de R y con Q al conjunto de los números racionales de R.

Sea $x \in R$. Definimos la "parte entera de x", denotado $[x]$ como el mayor entero menor o igual a x, y una vez calculado esto definimos la "mantisa de x", denotado $\{x\}$ como por la formula $\{x\} = x - [x]$. Por ejemplo, si $x = 3.14$ entonces $[3.14] = 3$ y $\{3.14\} = 0.14$. Observamos que $\{x\} \in [0, 1)$ para todo $x \in R$.

Tomemos ahora un numero real cualquiera x. Consideremos la sucesion $\{x\}, \{2x\}$, $\{3x\}, \{4x\} \ldots$. ¿Qué podemos decir de dicha sucesión? ¿Es finita? ¿Es infinita? Más importante, ¿cómo está distribuida?

Veamos primero un ejemplo. Consideremos $x = 0,4$. La sucesión correspondiente resulta entonces $\{0.4\}, \{0.8\}, \{1.2\}, \{1.6\}, \{2.0\}, \{2.4\}, \{2.8\}, \ldots$. Es decir, luego de evaluar la función mantisa $0.4,\ 0.8,\ 0.2,\ 0.6,\ 0,\ 0.4,\ 0.8, \ldots$. Es decir, la sucesión de mantisas resulta finita. Nuestro primer Lema nos muestra que esto ocurre siempre si $x \in Q$.

Lema 1. Si $x \in Q$ entonces la sucesión de mantisas $\{nx\}$ contiene sólo una cantidad finita de términos diferentes.

Demostración. Supongamos que $x \in Q$. Entonces $x = \frac{p}{q}$ con $p \in Z, q \in N$. Luego $\{x\}, \{2x\}, \{3x\}, \{4x\}, \ldots, \{(q-1)x\}, \{qx\}$ pueden ser diferentes pero $\{(q+1)x\}$ coincide con $\{x\}$. En efecto, $\{(q+1)x\} = \{\frac{(q+1)p}{q}\} = \{1 + \frac{p}{q}\} = \{\frac{p}{q}\} = \{x\}$. Análogamente se puede probar que $\{(q+2)x\}$ coincide con $\{2x\}$, y así sucesivamente.

Lema 2. Si $x \in I$ entonces la sucesión de mantisas $\{nx\}$ no contiene dos elementos iguales.

Demostración. Supongamos que $x \in I$ y que además $\{nx\} = \{mx\}$. Entonces $nx - mx = k \quad , k \in Z$. Entonces $x \in Q$. Absurdo.

Nota Histórica Hay dos teoremas que prepararon el terreno para el Teorema de Equidistribución de Weyl. El primero es el Teorema de Dirichlet y el segundo es el Teorema de Kronecker, sin duda la antesala del Teorema de Equidistribución de Weyl.

El primer Teorema afirma que si $\theta \in R$ y si $m \in N$ es cualquier número natural entonces existen dos enteros $0 < k \leq m$ y h tales que $|k\theta - h| < \frac{1}{m}$. En palabras multiplicando θ suficientes veces el resultado es casi un entero.

El segundo Teorema afirma que si $\theta \in I$ entonces la sucesión de mantisas $\{n\theta\}$ es densa en el intervalo $(0, 1)$. En palabras las mantisas de los múltiplos enteros de θ tocan cualquier subintervalo $(a, b) \subseteq (0, 1)$.

Nuestro estudio sobre el Teorema de Weyl apunta a más : a probar que la sucesión de mantisas no sólo llena el intervalo $(0, 1)$ sino que lo llena de forma uniforme.

2. DEFINICION DE EQUIDISTRIBUCIÓN.

Definición. Una sucesión de números $0 \leq \theta_n < 1 : n \in N$ está equidistribuida en $[0, 1)$ si para todo subintervalo $(a, b) \subset [0, 1)$:

$$\lim_{N\to\infty} \frac{|\{\theta_n \in (a,b) : 1 \leq n \leq N\}|}{N} = b - a.$$

El significado en palabras de esta definición es el siguiente : La cantidad de elementos de la sucesión θ_n que pertenecen al intervalo (a, b) es proporcional a la longitud del intervalo y en el infinito todos los intervalos de dicha longitud tienen la misma proporción de elementos θ_n.

Demos un ejemplo y un contraejemplo de esta definición.

Ejemplo 1. Consideremos la sucesión siguiente :

$0, \frac{1}{2}, 0, \frac{1}{3}, \frac{2}{3}, 0, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, 0, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \ldots$

Se observa que esta sucesión está equidistribuida pero daremos ahora una explicación formal de este hecho, uno de los valores agregados de nuestro trabajo.

Consideremos todos los puntos de coordenadas enteras en el primer cuadrante que satisfacen la condición $y < x$. Es decir la "mitad" del Lattice ZXZ en el primer cuadrante. Para cada valor de la sucesión $\frac{p}{q}$ asociemos el correspondiente punto del

Lattice (p, q). Luego un índice de esta sucesión está pertenece al intervalo (a, b) si y sólo si el correspondiente punto en el Lattice se encuentra en la región comprendida entre las rectas de pendientes a y b. Se observa entonces que el cociente:

$$\lim_{N\to\infty} \frac{|\{\theta_n \in (a,b) : 1 \leq n \leq N\}|}{N}$$

es igual a $b - a$ independientemente de los valores a y b, es decir, la sucesión está equidistribuida.

Ejemplo 2. Sea θ_n una sucesión que represente a los números racionales. Definamos la sucesión α_n de la siguiente manera :

$$\alpha_n = \begin{cases} \theta_{\frac{n}{2}} & si \quad n \quad es \quad par \\ 0.1 & si \quad n \quad es \quad impar \end{cases}$$

La sucesión α_n no está equidistribuida. En efecto, tomemos el subintervalo $(0.09, 0.11) \subset (0, 1)$. Entonces

$$\lim_{N\to\infty} \frac{|\{\alpha_n \in (0.09,0.11) : 1 \leq n \leq N\}|}{N} \geq 1/2 > 0.02.$$

3. RELACION ENTRE ANÁLISIS MATEMÁTICO Y TEORÍA DE NUMEROS.

Nuestra demostración del Teorema de Weyl será a traves de una conexion de la Teoría de Números con el Análisis Matemático, esta vez con el Análisis de Fourier.

Sea $(a, b) \subset [0, 1)$ un intervalo. Sea $\chi_{(a,b)}(x)$ la función característica en dicho intervalo. Extendamos dicha función periódicamente con período 1, es decir $\chi_{(a,b)}(x + 1) = \chi_{(a,b)}(x)$. Sea $x \in R$. Entonces $\{nx\} \in (a, b)$ si y sólo si $\chi_{(a,b)}(nx) = 1$. Luego

$|\{\{nx\} \in (a, b) : 1 \leq n \leq N\}| = \sum_{n=1}^{N} \chi_{(a,b)}(nx)$.

Con esta igualdad el Teorema de Weyl puede enunciarse así :

$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} \chi_{(a,b)}(nx)}{N} = \int_0^1 \chi_{(a,b)}(x)dx = b - a$$

para todo $x \in I$.

Probamos ahora un importante Lema. Será la clave para poder demostrar el Teorema de equidistribución.

Lema 3. Si $f(x)$ es continua en [0,1), periódica con período 1 y θ es irracional entonces

$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(n\theta) = \int_0^1 f(x)dx$

Probamos el lema en tres partes separadas.

Parte 1. El Lema vale para las funciones $f(x) = 1, f(x) = e^{2\pi ix}, f(x) = e^{4\pi ix}, \ldots$. En efecto, para $f(x) = 1$ resulta:

$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} 1 = \int_0^1 1dx$

que claramente se verifica resultando 1 ambos miembros.

Para $f(x) = e^{2\pi ix}$ resulta:

$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi in\theta} = \int_0^1 e^{2\pi ix}dx$

El miembro derecho resulta, después de una simple evaluación, 0 y el izquierdo, aplicando la fórmula para la suma de los primeros N términos resulta :

$\lim_{N\to\infty} \frac{1}{N} e^{2\pi i\theta} \frac{1-e^{2\pi i\theta N}}{1-e^{2\pi i\theta}}$

que tiende a 0 cuando $N \to \infty$. Análogamente para el resto de las exponenciales.

Parte 2. Si f y g satisfacen las condiciones del enunciado y A y B son escalares reales entonces $Af + Bg$ satisface las condiciones del enunciado. Por la parte 1 concluimos que el lema se verifica para cualquier polinomio trigonométrico de período 1.

Parte 3. Consideremos un polinomio trigonométrico $P(x)$ tal que $sup_{x\in R}|f(x) - P(x)| < \frac{\epsilon}{3}$. Además para N suficientemente grande :

$\left| \frac{1}{N} \sum_{n=1}^{N} P(n\theta) - \int_0^1 P(x)dx \right| < \frac{\varepsilon}{3}$

Luego :

$\left| \frac{1}{N} \sum_{n=1}^{N} f(n\theta) - \int_0^1 f(x)dx \right| =$

$\left| \frac{1}{N} \sum_{n=1}^{N} f(n\theta) - \frac{1}{N} \sum_{n=1}^{N} P(n\theta) + \frac{1}{N} \sum_{n=1}^{N} P(n\theta) + \int_0^1 P(x)dx - \int_0^1 P(x)dx + \int_0^1 f(x)dx \right| \leq$

$\left| \frac{1}{N} \sum_{n=1}^{N} f(n\theta) - \frac{1}{N} \sum_{n=1}^{N} P(n\theta) \right| + \left| \frac{1}{N} \sum_{n=1}^{N} P(n\theta) + \int_0^1 P(x)dx \right| + \left| - \int_0^1 P(x)dx + \int_0^1 f(x)dx \right|$

$< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon$

es decir, $\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(n\theta) = \int_0^1 f(x)dx$.

4. DEMOSTRACIÓN DEL TOEREMA DE EQUIDISTRIBUCIÓN

Hasta ahora tenemos probado el lema para cualquier función continua periódica de período 1 y para cualquier θ irracional. Pero precisamos justamente el lema para la función característica $\chi_{(a,b)}$. Dicha función es discontinua en $x = a$ y en $x = b$. A tal efecto sea $\epsilon > 0$. Construyamos dos funciones $f_\epsilon^+(x)$ y $f_\epsilon^-(x)$ definidas geométricamente así:

$$f_\epsilon^+(x) = \begin{cases} 0 & si \quad x \in [0, a-\epsilon) \cup [b+\epsilon, 1) \\ 1 & si \quad x \in [a, b] \\ unión \quad de \quad las \quad rectas \quad que \quad hacen \quad continua \quad la \quad función \end{cases}$$

$$f_\epsilon^-(x) = \begin{cases} 1 & si \quad x \in [a+\epsilon, b-\epsilon] \\ 0 & si \quad x \in [0, a] \cup [b, 1] \\ unión \quad de \quad las \quad rectas \quad que \quad hacen \quad continua \quad la \quad función \end{cases}$$

Si extendemos estas funciones periódicamente con período 1 vemos que :

$$b - a - 2\epsilon \leq \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_{(a,b)}(n\theta) \leq b - a + 2\epsilon$$

Al valer estas desigualdades para todo ϵ concluimos que:

$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} \chi_{(a,b)}(nx)}{N} = \int_0^1 \chi_{(a,b)}(x)dx = b - a$$

es decir, el Teorema de Equidistribución de Weyl queda completamente demostrado.

APLICACIONES A LA CRIPTOGRAFIA

En el libro "Equidistribution in Number Theory : An Introduction" leemos que " ... el tópico es de importacia creciente en muchas áreas incluyendo Criptografía, ceros de las L-Funciones, puntos de Heegner, teoría de formas cuadráticas y los aspectos aritméticos del caos cuántico." Los autores del libro son expertos en el tema y una sóla aplicación de las mencionadas constituye suficiente excusa para estudiar el tema.

En criptografía, el tópico que más nos interesa a nosotros, el Teorema de Equidistribución de Weyl encuentra una aplicación inmediata : Una gran secuencia de números pseudoaleatorios se utiliza en generación de claves, enmascarado de protocolos, encriptación, etc.

En general, no es sencillo a nivel práctico (no teórico) hallar una secuencia larga de números aleatorios, mucho menos una gran cantidad de ellas. Muchas métodos de

encriptar información comienzan asi "Consideremos una secuencia de números pseusoaleatorios ....", pero no explican claramente cómo hacerse de dicha secuencia. La respuesta la encontramos en el Teorema de Equidistribución : tomamos cualquier números irracional θ, le calculamos sus multiplos $n\theta$, y tomamos la sucesión de mantisas. Dicha secuencia está equidistribuida, es decir, en jerga criptográfica es pseudoaleatoria.