Seminario de Tesis II: Análisis de distribución de los ceros de las sumas parciales de la función zeta de Riemann y funciones asociadas

Víctor Racsó Galván Oyola

27 de agosto de 2021

Índice

Función zeta de Riemann

Definición

La función $\zeta : \{z \in \mathbb{C} : \mathrm{Re}(s) > 1\} \to \mathbb{C}$ está definida por la siguiente expresión:

$$\zeta(s) = \sum_{i=1}^{\infty} \frac{1}{i^s}$$

Suma parcial

Definimos como suma parcial de la función zeta de Riemann con parámetro n a la siguiente expresión:

$$\zeta_n(s) = \sum_{i=1}^{n} \frac{1}{i^s} = \sum_{i=1}^{n} \mathrm{e}^{-s \log i}$$

Hipótesis de Riemann

Enunciado

La hipótesis de Riemann (HR) establece que todos los ceros no triviales de $\zeta(s)$ están en la recta $\mathrm{Re}(s) = 1/2$.

Consecuencias

Si la hipótesis de Riemann es verdadera, entonces:

1. Existe una constante $C > 0$ tal que:

$$|\pi(x) - Li(x)| \leq C\sqrt{x}\log x$$

   Donde $Li(x) = \int\limits_2^x \frac{dt}{\ln t}$.

2. Cota para el *prime gap*:

$$p_{k+1} - p_k = O\left(\sqrt{p_k}\log p_k\right)$$

   Donde p_k es el k-ésimo número primo.

Ceros especiales y la Hipótesis de Riemann

Cero especial

Se define como **cero especial de** ζ_n a todo elemento del conjunto:

$$\{s \in \mathbb{C} : 1 < \operatorname{Re}(s), \zeta_n(s) = 0\}$$

Nótese que $\zeta_n(s)$ es una suma parcial, ya que la función $\zeta(s)$ no presenta dichos ceros.

Teorema (Turán, 1948)

Si existen n_0, $K > 0$ y $0 \leq \varepsilon < \frac{1}{2}$ tales que:

$$\forall n > n_0, \zeta_n(s) \text{ no tiene ceros en } \operatorname{Re}(s) \geq 1 + Kn^{-\frac{1}{2}+\varepsilon}$$

entonces la hipótesis de Riemann es cierta.

Existencia de ceros en Re$(s) > 1$

Conclusiones a lo largo del tiempo

- La HR será cierta si, para todo n suficientemente grande, no existen ceros de $\zeta_n(s)$ en Re$(s) > 1$. (Turán, 1948)
- Para $1 \leq n \leq 5$, $\zeta_n(s)$ no tiene ceros en Re$(s) > 1$. (Turán)
- Para $6 \leq n \leq 9$, $\zeta_n(s)$ no tiene ceros en Re$(s) > 1$. (Spira, 1966)
- Para un n fijo, si $\zeta_n(s)$ tiene al menos un cero en Re$(s) > 1$, entonces tiene infinitos ceros en dicha región. (Spira)

Gracias a resultados de Spira (1968), Monach (1980) y Platt et Trudgian (2016) se concluye que:

Existencia de ceros según n

Para $1 \leq n \leq 18$, $n = 20, 21, 28$ no hay ceros de $\zeta_n(s)$ en Re$(s) > 1$. Para los demás enteros positivos n existen infinitos ceros en dicha región.

Retículos

Definición

Dados n vectores linealmente independientes $b_1, \ldots, b_n \in \mathbb{R}^m$, el retículo generado por ellos se define como:

$$\mathcal{L}(b_1, b_2, \ldots, b_n) = \left\{ \sum x_i b_i | x_i \in \mathbb{Z} \right\}$$

Se define a B como la matriz de $m \times n$ cuyas columnas son los vectores b_i. Se dice que el retículo es de rango n y dimensión m. Si $n = m$, entonces el retículo es un retículo de rango completo.

Determinante

Sea $\Lambda = \mathcal{L}(B)$ un retículo de rango n. Se define la determinante de Λ, denotada por $\det(\Lambda)$, como:

$$\det(\Lambda) = \sqrt{\det(B^T B)}$$

Ortogonalización Gram-Schmidt

Definición

Para una secuencia de n vectores linealmente independientes $b_1, b_2, \ldots, b_n$ se define su ortogonalización Gram-Schmidt como la secuencia de vectores $\widetilde{b}_1, \widetilde{b}_2, \ldots, \widetilde{b}_n$, los cuales son obtenidos de la siguiente manera:

$$\widetilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \widetilde{b}_j, \text{ con } \mu_{i,j} = \frac{\langle b_i, \widetilde{b}_j \rangle}{\langle \widetilde{b}_j, \widetilde{b}_j \rangle}$$

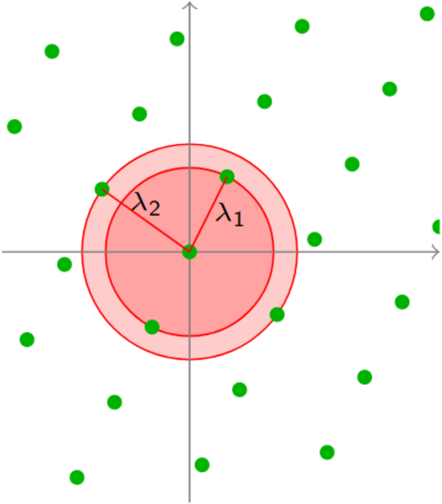
Mínimo sucesivo

Sea Λ un retículo de rango n, para cada $i = 1, \ldots, n$ se define el i-ésimo mínimo sucesivo a:

$$\lambda_i(\Lambda) = \inf \{ r | \dim(\operatorname{span}(\Lambda \cap \overline{B}(0, r))) \geq i \}$$

Donde $\overline{B}(0, r) = \{ x \in \mathbb{R}^m : ||x|| \leq r \}$ es la bola cerrada de radio r alrededor de 0.

Interpretación Geométrica de Mínimo sucesivo



Bases de retículos LLL-reducidas

Definición

Sea B la base de un retículo Λ y sea $\widetilde{B}$ su ortogonalización Gram-Schmidt. Considerando:

$$\mu_{i,j} = \frac{\langle b_i, \widetilde{b_j} \rangle}{\langle \widetilde{b_j}, \widetilde{b_j} \rangle}, \forall 1 \leq j < i \leq n$$

Y sea $\frac{1}{4} < \delta < 1$ fijo, entonces la base es LLL-reducida (con factor δ) si las siguientes condiciones se cumplen:

Reducidas en tamaño:

$$|\mu_{i,j}| < \frac{1}{2}, \forall 1 \leq i < j \leq n$$

Condición de Lovász

$$||\widetilde{b_i}||^2 \geq \left(\delta - \mu_{i,i-1}^2\right) ||\widetilde{b}_{i-1}||^2, \forall i = 2, \ldots, n$$

Propiedades de una base LLL-reducida

Sea B una base LLL-reducida con factor $\delta = \frac{3}{4}$ para un retículo $\Lambda \subset \mathbb{R}^m$ y $\widetilde{B}$ su ortogonalización Gram-Schmidt, se cumple:

1. $2^{i-j}||\widetilde{b}_i||^2 \geq ||\widetilde{b}_j||^2$, para todo $1 \leq j \leq i \leq n$.
2. $||\widetilde{b}_i||^2 \leq ||b_i||^2 \leq \left(\frac{1}{2} + 2^{i-2}\right) ||\widetilde{b}_i||^2$, para todo $i = 1, \ldots, n$.
3. $||b_j|| \leq 2^{\frac{i-1}{2}} ||\widetilde{b}_i||$, para todo $1 \leq j \leq i \leq n$.
4. $||b_1|| \leq 2^{\frac{n-1}{2}} \lambda_1$.
5. $||b_j|| \leq 2^{\frac{n-1}{2}} \lambda_i$ para todo $1 \leq j \leq i \leq n$.
6. $2^{\frac{1-i}{2}} \lambda_i \leq ||b_i|| \leq 2^{\frac{n-1}{2}} \lambda_i$.
7. $\det(\Lambda) \leq \prod_{i=1}^{n} ||b_i|| \leq 2^{\frac{n(n-1)}{4}} \det(\Lambda)$
8. $||b_1|| \leq 2^{\frac{n-1}{4}} \det(\Lambda)^{\frac{1}{n}}$.

Algoritmo LLL

Historia

- Publicado en 1982 por Lenstra et al.
- Presentado como herramienta para factorizar polinomios.
- Su complejidad propuesta era de $O(n^5 \log n)$ operaciones aritméticas.
- Optimizado por Claus Peter Schnorr en dos ocasiones: $O(n^4 \log n)$ operaciones aritméticas en 1986 y $O(n^3 \log n)$ en 2005.
- Actualmente, hay variaciones del algoritmo usando paralelismo. Werner Backes y Susanne Wetzel propusieron una primera versión en 2009 y una incluso mejor en 2011.

Funcionamiento

El algoritmo recibe una base B de un retículo Λ y modifica los valores de B hasta volverlo una base LLL-reducida.

Algoritmo 1: Algoritmo LLL

Entrada: $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ linealmente independientes, $\frac{1}{4} < \delta < 1$
Salida: Una base LLL-reducida $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$
Ejecutar el algoritmo Gram-Schmidt para obtener $\widetilde{b}_1, \ldots, \widetilde{b}_n$ y los coeficientes $\mu_{i,j}$
Procesar $B_i \leftarrow \langle \widetilde{b}_i, \widetilde{b}_i \rangle$ para todo $1 \leqslant i \leqslant n$
$k \leftarrow 2$
mientras $k \leqslant n$ **hacer**
  para $j = k - 1 \to 1$ **hacer**
    $q_{k,j} \leftarrow \lfloor \mu_{k,j} \rceil$
    $b_k \leftarrow b_k - q_{k,j} b_j$
    Actualizar los valores de $\widetilde{b}_1, \ldots, \widetilde{b}_n$ y $\mu_{i,j}$ correspondientemente
  si $B_k \geqslant \left(\delta - \mu_{k,k-1}^2\right) B_{k-1}$ **entonces**
    $k \leftarrow k + 1$
  en otro caso
    Intercambiar b_k y b_{k-1}
    Actualizar los valores $\widetilde{b}_i$, $\mu_{i,j}$ y B_i que se vean afectados
    $k \leftarrow \text{máx}\{2, k - 1\}$
Devolver $\{b_1, b_2, \ldots, b_n\}$

Complejidad del LLL

Complejidad del algoritmo de Gram-Schmidt

La construcción de la ortogonalización de Gram-Schmidt requiere de $O(n)$ iteraciones, con cada una de ellas tomando $O(n)$ productos internos. Su complejidad total es $O(n^3)$ operaciones aritméticas.

Complejidad del algoritmo LLL

Se puede probar que el algoritmo LLL necesita $O(n^2 \log n)$ intercambios. Ya que en cada intercambio se debe reconstruir por completo la ortogonalización, la complejidad final será de $O(n^5 \log n)$ operaciones aritméticas.

¿Greedy?

Se puede notar que el algoritmo usa una variación de la técnica *Exchange Arguments* para modificar la base como convenga. Este principio se usa para resolver problemas con un enfoque *greedy*.

Aplicación del LLL

Proposición (Lenstra et al. 1982)

Existe un algoritmo de complejidad polinomial tal que, dado un entero positivo n y racionales $\alpha_1, \alpha_2, \dots, \alpha_n, \varepsilon$, con $0 < \varepsilon < 1$, encuentra enteros $p_1, p_2, \dots, p_n, q$ que satisfacen:

$$|p_i - q\alpha_i| \leq \varepsilon, \forall 1 \leq i \leq n$$

$$1 \leq q \leq 2^{\frac{n(n+1)}{4}} \varepsilon^{-n}$$

Análisis

La proposición es demostrada considerando el retículo Λ formado por:

$$b_i = e_i, \forall 1 \leq i \leq n$$

$$b_{n+1} = \left(-\alpha_1, -\alpha_2, \dots, -\alpha_n, 2^{-\frac{n(n+1)}{4}} \varepsilon^{n+1}\right)^T$$

Análisis sobre las sumas parciales ζ_n - I

Una idea de aproximación

Consideraremos tener un cero especial s_0 y un real T. Al comparar las funciones $\zeta_n(s_0)$ y $\zeta_n(s_0 + \hat{j}T)$ llegamos a la siguiente expresión:

$$\zeta_n(s + \hat{j}T) - \zeta_n(s) = \sum_{i=1}^{n} \mathrm{e}^{-s \log i} \left(\mathrm{e}^{-\hat{j}T \log i} - 1 \right)$$

Deseamos que $\zeta_n(s_0 + \hat{j}T) \approx \zeta_n(s_0) = 0$ para encontrar un nuevo cero especial usando T.

Conclusión

Se puede probar que T debe ser tal que, para $\varepsilon > 0$:

$$|T \log p_i - 2\pi k_i| < \varepsilon, \forall p_i \leq n$$

Con p_i primos y k_i entero.

Análisis sobre las sumas parciales ζ_n - II

Condiciones sobre los valores

Podemos aprovechar la proposición anterior y la aritmética limitada para aproximar valores irracionales con racionales.

Modelamiento de la solución

Podemos elegir

$$\alpha_i = \frac{\log p_i}{2\pi}$$

De esta manera, al aplicar la reducción, obtendremos T y k_i tales que:

$$\left| T\left(\frac{\log p_i}{2\pi}\right) - k_i \right| < \varepsilon \to |T \log p_i - 2\pi k_i| < \varepsilon \cdot 2\pi$$

Si queremos una tolerancia de ε_1, basta con tomar $\varepsilon = \frac{\varepsilon_1}{2\pi}$

s_0 hallados

Los siguientes ceros especiales fueron obtenidos con el programa para hallar ceros en una región diseñado en Seminario I.

n	$\mathrm{Re}(s_0)$	$\mathrm{Im}(s_0)$
23	1.01044334922698341898	8502832.39912065772578142170
24	1.00404186833602031723	32520751.78599510357179634043
25	1.00044920152434295543	32520751.80223907180402332765
26	1.00635284737135701011	36323746.32695248213955443469
31	1.00710368676439502484	52331955.65876127657415336860

Cuadro: Recopilación de los ceros especiales iniciales s_0

T hallados

Los siguientes valores de T fueron obtenidos aplicando el algoritmo LLL como se había planteado.

n	T
23-28	55387506632377994764662267526285
29-30	58708856695178414451367875415749947
31-36	8188013923661234341208117417875493140 15
37-40	1197632059719333470023010432912340909634 6397
41-42	684662329827288256179200837652072817808026 2598
43-46	178966696696026729062133558671975332854893205674 7747

Cuadro: Recopilación de los T obtenidos

Es sencillo notar que el valor de T hallado cambia cuando n es un nuevo número primo.

Ceros especiales generados

Los siguientes resultados fueron obtenidos con el T asociado a cada n y buscando los ceros en una vecindad del valor de $s_i \approx s_0 + \hat{j}iT$.

n	Ceros obtenidos	$\min\{\text{Re}(s)\}$	$\max\{\text{Re}(s)\}$
23	195	1.00002145180704	1.010443349226983
24	353	1.000019665810482	1.005149876873392
25	394	1.000034306376722	1.003589728240308
26	184	1.000000721843266	1.006352847371357
31	446	1.000021773656535	1.007104993843435

Cuadro: Recopilación de los ceros especiales obtenidos

Discusión

Optimizaciones de LLL

Es relativamente fácil relacionar el algoritmo LLL con algo similar a un ordenamiento, principalmente el algoritmo *Insertion Sort*, el cual realiza intercambios entre elementos consecutivos para reducir la cantidad de inversiones hasta que esta sea 0.

Sobre la precisión

El detalle de la precisión es bastante influyente al momento de resolver el problema planteado, pues a medida que el ε disminuye, los límites de T aumentan exponencialmente. Esta problemática nos hace dar cuenta de que el factor de aproximación exponencial sigue siendo insuficiente, por lo que es necesario realizar estudios para mejorarlo.

Otras aplicaciones del algoritmo LLL

- Factorización de polinomios en tiempo polinomial.
- Ataque de reducción de retículos contra el *knapsack cryptosystem*
- Aproximación del vector más corto.
- Programación lineal entera con dimensión acotada.

Referencias

- A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. Mathematische annalen, 261(ARTICLE):515–534, 1982.
- P. Turán. On some approximative Dirichlet-polynomials in the theory of the zeta-function of Riemann, volume 24. I kommission hos Munksgaard, 1948.
- P. Q. Nguyen and B. Vallée.The LLL algorithm. Springer, 2010.