PROBABILISTIC ZETA FUNCTIONS FOR PROFINITE GROUPS

Dr Ged Corob Cook

Zeta Functions

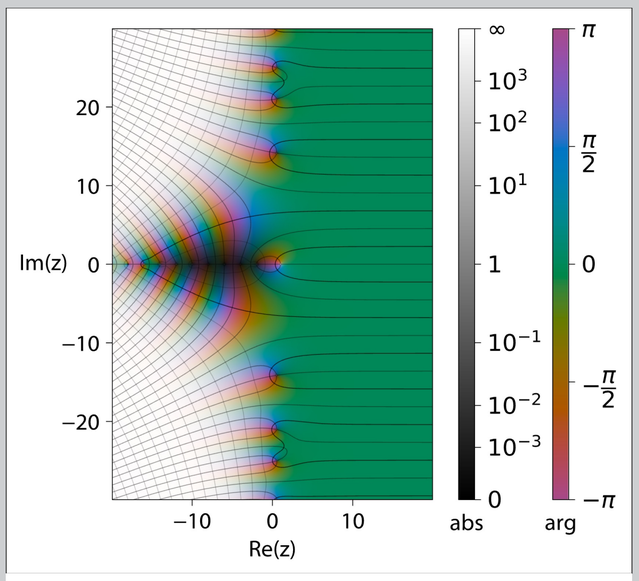
Zeta functions are ubiquitous tools in pure mathematics. The best known, and most important, zeta function was first studied by Riemann in the 1850s, given by the infinite sum

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

for a complex variable s with real part $Re(s) > 1$. The study of ζ has created fundamental breakthroughs in number theory, since the values of s for which $\zeta(s) = 0$ are intimately connected to the distribution of the prime numbers, which is the key to many fundamental questions. Other zeta functions, defined by infinite sums of the form

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

for some complex numbers a_n, have led to important progress in such areas as number theory and algebraic geometry.



The Riemann zeta function $\zeta(z)$, on the complex plane. (Source: Wikimedia Commons)

The Riemann Hypothesis

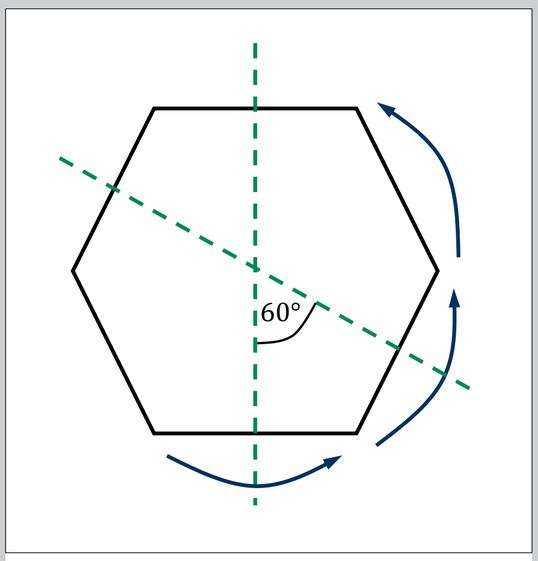
Riemann's zeta function can be analytically continued to the rest of the complex plane (that is, for values of s such that $Re(s) \leq 1$). The Riemann Hypothesis asks whether, for $Re(s) > 0$, $\zeta(s) = 0$ implies that $Re(s) = \frac{1}{2}$. This is considered by many mathematicians to be the most important unsolved problem in mathematics; there is a one-million-dollar prize for an answer to this question.

The Prime Number Theorem, proved using the Riemann zeta function, shows that the number of primes less than x is approximately $\frac{x}{\log(x)}$. The Riemann hypothesis would allow much more precise estimates.

Groups

Groups are one of the most important types of mathematical object, which describe symmetries in a precise way. The symmetries of shapes like a hexagon, or a cube, form a group. Groups keep track of how symmetries combine: rotating a hexagon by $60°$, then reflecting it, is not the same as reflecting then rotating.

Mathematicians have been studying groups for hundreds of years, to use in other parts of maths like geometry and algebra. I research profinite groups, a type of infinite group which is 'built out of' finite groups.



Any rotation of a regular hexagon by a multiple of $60°$ is a symmetry, and so is a reflection in any of the six lines of symmetry.

Probabilistic Zeta Functions

A fundamental piece of data associated to G is the completed group ring $\widehat{\mathbb{Z}}[\![G]\!]$. We can study this using a corresponding zeta function ζ_G.

With S. Kionke (FernUniversität in Hagen) and M. Vannacci (Universidad del País Vasco) [CCKV], I have defined ζ_G by:

$$\zeta_G(s) = \sum_{p \text{ prime}} \sum_{j=1}^{\infty} \sum_{n=1}^{\infty} r^*(G, \mathbb{F}_{p^j}, n) \frac{p^{-snj}}{j} \frac{p^{nj} - 1}{p^j - 1}$$

where $r^*(G, \mathbb{F}_{p^j}, n)$, a measure of the complexity of the group, is the number of absolutely irreducible representations of G over the finite field $\mathbb{F}_{p^j}$ of dimension n. When s is a positive integer, $\frac{1}{\zeta_G(s)}$ is the probability that s random elements of $\widehat{\mathbb{Z}}[\![G]\!]$ generate it.

Example

One important profinite group is $\widehat{\mathbb{Z}}$, which is the profinite version of the integers. We can calculate the zeta function of $\widehat{\mathbb{Z}}$ exactly:

$$\zeta_{\widehat{\mathbb{Z}}}(s) = \frac{\zeta(s-1)}{\zeta(s)},$$

where ζ is the Riemann zeta function. This tells us the probability of generating the completed group ring of $\widehat{\mathbb{Z}}$ with two random elements is 0, but the probability with three random elements is $\zeta(3)/\zeta(2) \approx 0.73$.

Abscissae of Convergence

For a profinite group G, we would like to know for which values of s the infinite sum $\zeta_G(s)$ converges to a finite limit. The infimum (lower bound) of the real s for which $\zeta_G(s)$ converges is known as the abscissa of convergence of ζ_G, written $a(G)$. We can calculate this in many important cases.

Just as profinite groups are built out of finite groups, we can study pro-$\mathfrak{C}$ groups built out of groups in a subset $\mathfrak{C}$ of finite groups. For good classes $\mathfrak{C}$, there is a 'biggest' r-generated pro-$\mathfrak{C}$ group $F_r^{\mathfrak{C}}$, which is a free group in the category of pro-$\mathfrak{C}$ groups. Assume $r > 1$.

When $\mathfrak{C}$ contains all finite groups, $a\left(F_r^{\mathfrak{C}}\right) = \infty$.

Let p be a prime number. When $\mathfrak{C}$ contains all finite groups whose size is a power of p, $a\left(F_r^{\mathfrak{C}}\right) = \frac{r-1}{K(p)} + 1$ where $K(p)$ is a constant depending on p.

- $K(2) = \frac{2\log(3)}{5\log(2)} \approx 0.634$;
- $K(p) = \frac{(p-1)\log(p+1)}{p\log(p)} < 1$ when p is a Mersenne prime;
- $1 \leq K(p) \leq 2.1115$ otherwise.

So the probability of generating $\widehat{\mathbb{Z}}[\![F_r^{\mathfrak{C}}]\!]$ with n random elements is > 0 whenever $n > r$, unless p is 2 or a Mersenne prime, in which case more elements are required.

Mersenne primes have the form $2^n - 1$. Currently the largest eight known primes are Mersenne primes, and large primes are essential to cryptographic algorithms like RSA, so this connection is highly significant for potential applications.

The Babai-Cameron-Pálfy class $\mathfrak{C}(c_0)$ contains all the finite groups whose level of complexity is below c_0. In technical terms: we do not allow composition factors to be alternating groups of degree $> c_0$ or groups of Lie type of dimension $> c_0$. In this case, we get

$$a\left(F_r^{\mathfrak{C}}\right) = \left(c_0 + \frac{(c_0 - 1)\log(\prod_{i=1}^{c_0}(1 - 2^{-i})) + \log(c_0!)}{c_0(c_0 - 1)\log(2)}\right)(r-1) + 1.$$

Applications

Just as the prime numbers studied by Riemann have been used in cryptographic algorithms like RSA, the zeta functions defined here generalise Riemann's to the world of groups. Groups are being studied as candidates for post-quantum cryptography: algorithms which cannot be broken by quantum computers.

There are also applications to other areas of mathematics: progress in studying these zeta functions can answer questions about other zeta functions, such as in number theory.

Future Research

Riemann proved many important properties of his zeta function which we would like our own version of. For example, he showed how to define his zeta function for complex numbers where the definition as a sum is infinite; many applications of his work rely on this. Our probabilistic zeta functions should have analogous properties to explore.

References

[CCKV] Corob Cook, G, Kionke, S, Vannacci, M: *Weil Zeta Functions of Group Representations over Finite Fields*. Submitted (2022); to appear. https://arxiv.org/abs/2212.03748

UNIVERSITY OF LINCOLN

STEM for BRITAIN