Introduction to zeta functions of various algebraic structures and their applications

Seungjai Lee

Incheon National University

May 9th, 2024

Overview

Zeta Functions from number theory

Definition

Euler defined the *zeta function*

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{m=1}^{\infty} m^{-s}$$

for $s \in \mathbb{R},\ s > 1$.

Euler proved $\zeta(2) = \frac{\pi^2}{6}$, which was known as the Basel problem.

Zeta Functions from number theory

Definition

Euler defined the *zeta function*

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{m=1}^{\infty} m^{-s}$$

for $s \in \mathbb{R},\ s > 1$.

Euler proved $\zeta(2) = \frac{\pi^2}{6}$, which was known as the Basel problem.

Zeta Functions from number theory

Definition

Euler defined the *zeta function*

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{m=1}^{\infty} m^{-s}$$

for $s \in \mathbb{R},\ s > 1$.

Euler proved $\zeta(2) = \frac{\pi^2}{6}$, which was known as the Basel problem.

About 100 years later, Riemann extended the zeta function to complex numbers, which we now call the Riemann zeta function.

What makes the zeta function so special and powerful is that its analytic properties somehow encapsulate a tremendous amount of arithmetic information.

- Prime Number Theorem
- Dirichlet's Theorem
- Class number formula
- Riemann Hypothesis

About 100 years later, Riemann extended the zeta function to complex numbers, which we now call the Riemann zeta function.

What makes the zeta function so special and powerful is that its analytic properties somehow encapsulate a tremendous amount of arithmetic information.

- Prime Number Theorem
- Dirichlet's Theorem
- Class number formula
- Riemann Hypothesis

The arithmetic interpretation of $\zeta(s)$

The zeta function satisfies the Euler product

$$\begin{aligned}\zeta(s) &= \sum_{m=1}^{\infty} m^{-s} \\ &= \prod_{p \text{ prime}} \left(\frac{1}{1-p^{-s}}\right) \\ &= (1+2^{-s}+4^{-s}+\cdots)(1+3^{-s}+9^{-s}+\cdots)\cdots,\end{aligned}$$

re-establishing the *Fundamental Theory of Arithmetic*. This makes $\zeta(s)$ a very power tool to understand the prime numbers.

Example

Note that P_m, the probability that two randomly chosen numbers in $\{1, 2, \ldots, m\}$ are coprime, is

$$\prod_{p \leq m} \left(1 - \frac{1}{p^2}\right).$$

One can observe that $P_m \to \frac{1}{\zeta(2)}$ as $m \to \infty$

Dirichlet generating series

Definition

Any function of the form

$$Z(s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

is called a *Dirichlet generating series*.

The Riemann zeta function

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s} = \sum_{m=1}^{\infty} 1 \cdot m^{-s}$$

can be seen as a Dirichlet generating series where $a_m = 1$ for all $m \in \mathbb{N}$.

Dirichlet generating series

Definition

Any function of the form

$$Z(s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

is called a *Dirichlet generating series*.

The Riemann zeta function

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s} = \sum_{m=1}^{\infty} 1 \cdot m^{-s}$$

can be seen as a Dirichlet generating series where $a_m = 1$ for all $m \in \mathbb{N}$.

What does a Dirichlet generating series

$$Z(s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

tell about a_m?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.
- If a_m is (totally) multiplicative, then it also has the Euler product.

My research interest: Study $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

tell about a_m?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.
- If a_m is (totally) multiplicative, then it also has the Euler product.

My research interest: Study $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

tell about a_m?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.
- If a_m is (totally) multiplicative, then it also has the Euler product.

My research interest: Study $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

tell about a_m?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.
- If a_m is (totally) multiplicative, then it also has the Euler product.

My research interest: Study $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

A classical example

Definition (Dedekind zeta function)

Let K be a finite extension of $\mathbb{Q}$. The Dedekind zeta function of the field K is defined by

$$\zeta_K(s) = \sum_{\mathfrak{a} \triangleleft K} |\mathcal{O}_K : \mathfrak{a}|^{-s},$$

where $\mathcal{O}_K$ is the ring of integers, $\mathfrak{a}$ a non-zero ideal in $\mathcal{O}_K$, and $|\mathcal{O}_K : \mathfrak{a}|$ is the index of the ideal $\mathfrak{a}$ in $\mathcal{O}_K$, which is by definition the Norm $N(\mathfrak{a}) < \infty$.

Note that

$$\zeta_K(s) = \sum_{\mathfrak{a} \triangleleft K} |\mathcal{O}_K : \mathfrak{a}|^{-s} = \sum_{m=1}^{\infty} a_m(K) m^{-s},$$

where $a_m(K)$ denotes the number of non-zero ideal $\mathfrak{a}$ where $|\mathcal{O}_K : \mathfrak{a}| = m$.

A classical example

Definition (Dedekind zeta function)

Let K be a finite extension of $\mathbb{Q}$. The Dedekind zeta function of the field K is defined by

$$\zeta_K(s) = \sum_{\mathfrak{a} \triangleleft K} |\mathcal{O}_K : \mathfrak{a}|^{-s},$$

where $\mathcal{O}_K$ is the ring of integers, $\mathfrak{a}$ a non-zero ideal in $\mathcal{O}_K$, and $|\mathcal{O}_K : \mathfrak{a}|$ is the index of the ideal $\mathfrak{a}$ in $\mathcal{O}_K$, which is by definition the Norm $N(\mathfrak{a}) < \infty$.

Note that

$$\zeta_K(s) = \sum_{\mathfrak{a} \triangleleft K} |\mathcal{O}_K : \mathfrak{a}|^{-s} = \sum_{m=1}^{\infty} a_m(K) m^{-s},$$

where $a_m(K)$ denotes the number of non-zero ideal $\mathfrak{a}$ where $|\mathcal{O}_K : \mathfrak{a}| = m$.

A lesser-known example

Let G be a (finitely generated) group. For $* \in \{\leq, \triangleleft\}$, let $a_m^*(G)$ denote the number of subgroups/normal subgroups of G of index m.

Definition (Grunewald, Segal, Smith (1988))

We define the (normal) subgroup zeta functions of G as a Dirichlet generating series

$$\zeta_G^*(s) = \sum_{H * G} |G : H|^{-s} = \sum_{m=1}^{\infty} a_m^*(G) m^{-s}.$$

Motivation

Let P be a property that is common to all finite groups F. Now, let G be an arbitrary group having property P.

Does it follow that G is finite?

Burnside Problem

Let P="there exist m and n such that F is generated by m elements and every element x of F satisfies $x^n = 1$."

In other words, let G be a finitely generated group with a fixed exponent. Then is G always finite?

This is the Burnside Problem. We know this is false (Tarski Monster).

Restricted Burnside Problem

What if we force G to be "residually finite"?

Theorem (Zelmanov)

Every finitely generated residually finite group of finite exponent is finite

This result gave him a Fields medal in 1994.

Residually Finite Groups

Definition

A Group G is **residually finite** if and only if the intersection of all its subgroups/normal subgroups of finite index is trivial.

In an informal way, one can think that G is residually finite if it has many subgroups/normal subgroups of finite index; enough so that their intersection is trivial.

Now it is entirely natural to ask "How many subgroups/normal subgroups of each finite index n exist?" This is called a **subgroup growth** problem.

Residually Finite Groups

Definition

A Group G is **residually finite** if and only if the intersection of all its subgroups/normal subgroups of finite index is trivial.

In an informal way, one can think that G is residually finite if it has many subgroups/normal subgroups of finite index; enough so that their intersection is trivial.

Now it is entirely natural to ask "How many subgroups/normal subgroups of each finite index n exist?" This is called a **subgroup growth** problem.

Residually Finite Groups

Definition

A Group G is **residually finite** if and only if the intersection of all its subgroups/normal subgroups of finite index is trivial.

In an informal way, one can think that G is residually finite if it has many subgroups/normal subgroups of finite index; enough so that their intersection is trivial.

Now it is entirely natural to ask "How many subgroups/normal subgroups of each finite index n exist?" This is called a **subgroup growth** problem.

Zeta Functions of Groups

Let For $* \in \{\leq, \lhd\}$, let $a_m^*(G)$ denote the number of subgroups/normal subgroups of G of index m.

Fact

A finitely generated group G has only a finite number of subgroups/normal subgroups of each finite index. In other words,

$$a_m^*(G) := \#\{H : H * G \text{ and } |G : H| = m\} < \infty$$

for each $m \in \mathbb{N}$, where $* \in \{\leq, \lhd\}$.

We want to study the asymptotic behaviour of the sequence $((a_m^*(G)))$.

Zeta Functions of Groups

Let For $* \in \{\leq, \lhd\}$, let $a_m^*(G)$ denote the number of subgroups/normal subgroups of G of index m.

Fact

A finitely generated group G has only a finite number of subgroups/normal subgroups of each finite index. In other words,

$$a_m^*(G) := \#\{H : H * G \text{ and } |G : H| = m\} < \infty$$

for each $m \in \mathbb{N}$, where $* \in \{\leq, \lhd\}$.

We want to study the asymptotic behaviour of the sequence $((a_m^*(G)))$.

Back to our lesser-known example

Definition (Grunewald, Segal, Smith (1988))

We define the (normal) subgroup zeta functions of G as a Dirichlet generating series

$$\zeta_G^*(s) = \sum_{H * G} |G : H|^{-s} = \sum_{m=1}^{\infty} a_m^*(G) m^{-s}.$$

Example

Consider $(\mathbb{Z}, +)$ as an infinite cyclic group. Since $a_m^*(\mathbb{Z}) = 1$ for all $m \in \mathbb{N}$, we get

$$\zeta_{\mathbb{Z}}^*(s) = \zeta_{\mathbb{Z}}^{\leq}(s) = \zeta_{\mathbb{Z}}^{\lhd}(s) = \sum_{m=1}^{\infty} m^{-s} = \zeta(s).$$

Back to our lesser-known example

Definition (Grunewald, Segal, Smith (1988))

We define the (normal) subgroup zeta functions of G as a Dirichlet generating series

$$\zeta_G^*(s) = \sum_{H * G} |G : H|^{-s} = \sum_{m=1}^{\infty} a_m^*(G) m^{-s}.$$

Example

Consider $(\mathbb{Z}, +)$ as an infinite cyclic group. Since $a_m^*(\mathbb{Z}) = 1$ for all $m \in \mathbb{N}$, we get

$$\zeta_{\mathbb{Z}}^*(s) = \zeta_{\mathbb{Z}}^{\leq}(s) = \zeta_{\mathbb{Z}}^{\lhd}(s) = \sum_{m=1}^{\infty} m^{-s} = \zeta(s).$$

Zeta Functions of Rings

Definition (Grunewald, Segal, Smith (1988))

Let L be a ring additively isomorphic to $\mathbb{Z}^n$. For $* \in \{\leq, \lhd\}$, let $a_m^*(L)$ denote the number of subring/ideal of L of index m. We define the zeta function of a ring L as

$$\zeta_L^*(s) = \sum_{H * L} |L : H|^{-s} = \sum_{m=1}^{\infty} a_m^*(L) m^{-s}.$$

One can see that

$$\zeta_{\mathbb{Z}}^*(s) = \zeta(s) = \sum_{m=1}^{\infty} m^{-s},$$

meaning for each $m \geq 1$ there is only one subring/ideal of $\mathbb{Z}$ of index m.

Submodule zeta functions

Definition (Solomon (1977), Rossmann (2015))

Let $\mathcal{V}$ be a finitely generated R-module and $\Omega \subseteq \mathrm{End}_R(\mathcal{V})$ be a set of R-endomorphisms of $\mathcal{V}$. The (*submodule*) *zeta function of* Ω *acting on* $\mathcal{V}$ is the Dirichlet generating series enumerating the finite-index Ω-invariant submodules $\mathcal{U}$ of $\mathcal{V}$:

$$\zeta_{\Omega \curvearrowright \mathcal{V}}(s) = \sum_{\mathcal{U} \leq \mathcal{V}, \Omega(\mathcal{U}) \leq \mathcal{U}} |\mathcal{V} : \mathcal{U}|^{-s}.$$

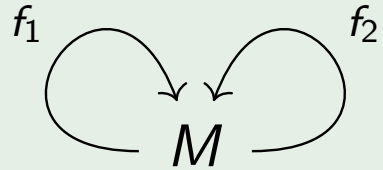
Again, one can see that

$$\zeta^*_{\{0\} \curvearrowright \mathbb{Z}}(s) = \zeta(s) = \sum_{m=1}^{\infty} m^{-s},$$

Quiver representation zeta functions

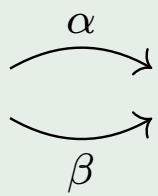
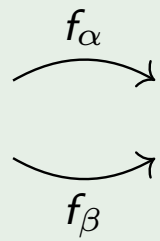
Let Q be a *quiver*, basically a directed graph with vertices and directed edges. For a ring R, an R-quiver representation $V = V_Q$ of Q is an association of an R-module to each vertex of Q and a morphism between each module for each directed edge.

Examples of quivers and quiver representations

Q :  and V_Q : 

,

or

Q : 1  2 and V_Q : M_1  M_2

Definition (L.-Voll (2023))

For $m \in \mathbb{N}$, let $a_m(V)$ denotes the number of subrepresentations V' of V of index m. We define the *quiver representation zeta function* of V to be the Dirichlet generating series

$$\zeta_V(s) := \sum_{m=1}^{\infty} a_m(V) m^{-s}.$$

Let

Q : and V_Q : $\mathbb{Z}$.

Then we have

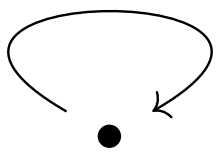
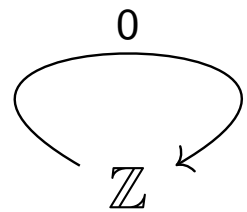
$$\zeta_V(s) = \zeta(s) = \sum_{m=1}^{\infty} m^{-s}.$$

Definition (L.-Voll (2023))

For $m \in \mathbb{N}$, let $a_m(V)$ denotes the number of subrepresentations V' of V of index m. We define the *quiver representation zeta function* of V to be the Dirichlet generating series

$$\zeta_V(s) := \sum_{m=1}^{\infty} a_m(V) m^{-s}.$$

Let

Q :  and V_Q : 

.

Then we have

$$\zeta_V(s) = \zeta(s) = \sum_{m=1}^{\infty} m^{-s}.$$

Aim: Study Γ and $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \zeta_\Gamma(s) = \sum_{m=1}^{\infty} a_m(\Gamma) m^{-s}$$

tell about $a_m(\Gamma)$?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.

Aim: Study Γ and $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \zeta_\Gamma(s) = \sum_{m=1}^{\infty} a_m(\Gamma) m^{-s}$$

tell about $a_m(\Gamma)$?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.

Aim: Study Γ and $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \zeta_\Gamma(s) = \sum_{m=1}^{\infty} a_m(\Gamma) m^{-s}$$

tell about $a_m(\Gamma)$?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.

Example

It is a well-known fact that

$$\zeta^*_{\mathbb{Z}^2}(s) = \zeta(s)\zeta(s-1),$$

and from this one can deduce

$$s^*_m(\mathbb{Z}^2) \sim \frac{\pi^2}{12} m^2.$$

In general,

$$\zeta^*_{\mathbb{Z}^d}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-(d-1)).$$

and

$$s^*_m(\mathbb{Z}^d) = \frac{\zeta(d)\zeta(d-1)\cdots\zeta(2)}{d} m^d + O(m^{d-1}\log(m)).$$

However, it is very difficult to show this by purely algebraic way.

Aim: Study Γ and $a_m = a_m(\Gamma)$ where $a_m(\Gamma)$ comes from a counting problem related to an algebraic object Γ.

What does a Dirichlet generating series

$$Z(s) = \zeta_\Gamma(s) = \sum_{m=1}^{\infty} a_m(\Gamma) m^{-s}$$

tell about $a_m(\Gamma)$?

- Let $s_m = \sum_{i=1}^{m} a_i$ denote the partial sum of a_m. If s_m grows polynomially, then $Z(s)$ is an analytic function, and its abscissa of convergence is the precise degree of its polynomial growth.
- If a_m is (totally) multiplicative, then it also has the Euler product.

The arithmetic interpretation of $\zeta(s)$

The zeta function satisfies the Euler product

$$\begin{aligned}\zeta(s) &= \sum_{m=1}^{\infty} m^{-s} \\ &= \prod_{p \text{ prime}} \left(\frac{1}{1-p^{-s}}\right) \\ &= (1+2^{-s}+4^{-s}+\cdots)(1+3^{-s}+9^{-s}+\cdots)\cdots,\end{aligned}$$

re-establishing the *Fundamental Theory of Arithmetic*. This makes $\zeta(s)$ a very power tool to understand the prime numbers.

Call

$$\zeta_p(s) := \frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \cdots$$

the local Riemann zeta function.

The arithmetic interpretation of $\zeta(s)$

The zeta function satisfies the Euler product

$$\begin{aligned}\zeta(s) &= \sum_{m=1}^{\infty} m^{-s} \\ &= \prod_{p \text{ prime}} \left(\frac{1}{1-p^{-s}}\right) \\ &= (1+2^{-s}+4^{-s}+\cdots)(1+3^{-s}+9^{-s}+\cdots)\cdots,\end{aligned}$$

re-establishing the *Fundamental Theory of Arithmetic*. This makes $\zeta(s)$ a very power tool to understand the prime numbers.

Call

$$\zeta_p(s) := \frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \cdots$$

the local Riemann zeta function.

Definition

If Γ is a $\mathbb{Z}$-module, then

$$\zeta_\Gamma(s) = \prod_{p \text{ prime}} \zeta_{\Gamma,p}(s),$$

where

$$\zeta_{\Gamma,p}(s) = \sum_{i=0}^{\infty} a_{p^i}(\Gamma) p^{-is} = a_1(\Gamma) + a_p(\Gamma) p^{-s} + \cdots .$$

We call $\zeta_{\Gamma,p}(s)$ the **local zeta function** of Γ.

Example

$$\zeta^*_{\mathbb{Z},p}(s) = \zeta^{\leq}_{\mathbb{Z},p}(s) = \zeta^{\lhd}_{\mathbb{Z},p}(s) = \zeta_p(s) = \sum_{i=0}^{\infty} p^{-is} = \frac{1}{1-p^{-s}}.$$

Definition

If Γ is a $\mathbb{Z}$-module, then

$$\zeta_\Gamma(s) = \prod_{p \text{ prime}} \zeta_{\Gamma,p}(s),$$

where

$$\zeta_{\Gamma,p}(s) = \sum_{i=0}^{\infty} a_{p^i}(\Gamma) p^{-is} = a_1(\Gamma) + a_p(\Gamma) p^{-s} + \cdots .$$

We call $\zeta_{\Gamma,p}(s)$ the **local zeta function** of Γ.

Example

$$\zeta^*_{\mathbb{Z},p}(s) = \zeta^{\leq}_{\mathbb{Z},p}(s) = \zeta^{\lhd}_{\mathbb{Z},p}(s) = \zeta_p(s) = \sum_{i=0}^{\infty} p^{-is} = \frac{1}{1-p^{-s}}.$$

Rationality of local factors

Example

Let $\Gamma = G = L = \mathcal{V} = V = \mathbb{Z}^d$. Then we have

$$\begin{aligned}\zeta_\Gamma(s) &= \zeta(s)\zeta(s-1)\cdots\zeta(s-(d-1)),\\ \zeta_{\Gamma,p}(s) &= \zeta_p(s)\zeta_p(s-1)\cdots\zeta_p(s-(d-1))\\ &= \frac{1}{(1-p^{-s})(1-p^{1-s})\cdots(1-p^{(d-1)-s})}.\end{aligned}$$

In this case, for each p, the local zeta function $\zeta_{\Gamma,p}(s)$ is a rational function in p and p^{-s}. In other words, for each p there exists

$$W_p(X,Y) = \frac{N_p(X,Y)}{D_p(X,Y)} = \frac{1}{(1-Y)(1-XY)\cdots(1-X^{d-1}Y)} \in \mathbb{Q}(X,Y)$$

such that

$$\zeta_{\Gamma,p}(s) = W_p(p,p^{-s}).$$

Rationality of local factors

Example

Let $\Gamma = G = L = \mathcal{V} = V = \mathbb{Z}^d$. Then we have

$$\begin{aligned}\zeta_\Gamma(s) &= \zeta(s)\zeta(s-1)\cdots\zeta(s-(d-1)),\\ \zeta_{\Gamma,p}(s) &= \zeta_p(s)\zeta_p(s-1)\cdots\zeta_p(s-(d-1))\\ &= \frac{1}{(1-p^{-s})(1-p^{1-s})\cdots(1-p^{(d-1)-s})}.\end{aligned}$$

In this case, for each p, the local zeta function $\zeta_{\Gamma,p}(s)$ is a rational function in p and p^{-s}. In other words, for each p there exists

$$W_p(X,Y) = \frac{N_p(X,Y)}{D_p(X,Y)} = \frac{1}{(1-Y)(1-XY)\cdots(1-X^{d-1}Y)} \in \mathbb{Q}(X,Y)$$

such that

$$\zeta_{\Gamma,p}(s) = W_p(p,p^{-s}).$$

Recursive relations

Theorem (Stanley EC1 Theorem 4.1.1)

A generating function

$$G(x) = \sum_{n=0}^{\infty} f(n)x^n$$

is a rational function, i.e, $G(x) = \frac{N(x)}{D(x)}$ *if and only if* $f(n)$ *satisfies some 'linear recurrence relation'.*

Example

Let $(f(n))$ denote the Fibonacci sequence defined as $f(0) = 0, f(1) = 1, f(n) = f(n-1) + f(n-2)$. Then

$$\sum_{n=0}^{\infty} f(n)x^n = \frac{x}{1 - x - x^2}.$$

In fact, we know more than this.

Theorem (du Sautoy & Grunewald, Rossmann, L-Voll)

Let Γ be an algebraic structure defined as above. There are smooth algebraic varieties V_i, $i \in [k]$, defined over $\mathbb{Q}$, and rational functions $W_i(X, Y) \in \mathbb{Q}(X, Y)$ such that, for almost all primes p,

$$\zeta_{\Gamma,p}(s) = \sum_{i=1}^{k} \overline{V_i}(\mathbb{F}_p) W_i(p, p^{-s}).$$

In other words, $\zeta_{\Gamma,p}(s)$ is of *Denef type*.

Zeta functions of submodules and quiver representations

Let $\mathbb{Z}$ be the ring of integers, p a prime, and $\mathbb{Z}_p$ the ring of p-adic integers. Note that in $\mathbb{Z}_p$, we have

- 1 subring of $\mathbb{Z}_p$ of index 1, namely $\mathbb{Z}_p$ itself,
- 1 subring of $\mathbb{Z}_p$ of index p, namely $p\mathbb{Z}_p$,
- 1 subring of $\mathbb{Z}_p$ of index p^2, namely $p^2\mathbb{Z}_p$,
- and so on...

In other words,

$$\begin{aligned}\zeta_{\mathbb{Z}_p}(s) &= \sum_{m=1}^{\infty} a_m(\mathbb{Z}_p) m^{-s} \\ &= 1 + p^{-s} + p^{-2s} + \cdots \\ &= \zeta_{\mathbb{Z},p}(s)\end{aligned}$$

Zeta functions of submodules and quiver representations

Let $\mathbb{Z}$ be the ring of integers, p a prime, and $\mathbb{Z}_p$ the ring of p-adic integers. Note that in $\mathbb{Z}_p$, we have

- 1 subring of $\mathbb{Z}_p$ of index 1, namely $\mathbb{Z}_p$ itself,
- 1 subring of $\mathbb{Z}_p$ of index p, namely $p\mathbb{Z}_p$,
- 1 subring of $\mathbb{Z}_p$ of index p^2, namely $p^2\mathbb{Z}_p$,
- and so on...

In other words,

$$\begin{aligned}\zeta_{\mathbb{Z}_p}(s) &= \sum_{m=1}^{\infty} a_m(\mathbb{Z}_p) m^{-s} \\ &= 1 + p^{-s} + p^{-2s} + \cdots \\ &= \zeta_{\mathbb{Z},p}(s)\end{aligned}$$

Consider the following quiver representation:

$$\mathrm{V}\colon \mathbb{Z}_p \xleftarrow[\varphi = id]{} \mathbb{Z}_p.$$

$V' = (M_1, M_2)$ is a subrepresentation of V if $M_1, M_2 \leq \mathbb{Z}_p$, and $M_2 \leq M_1$. For example, we can have $(\mathbb{Z}_p, \mathbb{Z}_p)$, $(\mathbb{Z}_p, p\mathbb{Z}_p)$, $(\mathbb{Z}_p, p^2\mathbb{Z}_p)$, $(p\mathbb{Z}_p, p\mathbb{Z}_p)$,.... However, we cannot have, for example, $(p\mathbb{Z}_p, \mathbb{Z}_p)$.

How do we compute $\zeta_V(s)$?

$$\mathrm{V}\colon \mathbb{Z}_p \xleftarrow[\varphi = id]{} \mathbb{Z}_p.$$

Let $V' = (M_1, M_2)$ be a subrepresentation of V. If $M_1 = p^a\mathbb{Z}_p$ and $M_2 = p^b\mathbb{Z}_p$, then (write $t = p^{-s}$)

$$\begin{aligned}
\zeta_V(s) &= \sum_{V' \leq V} |V : V'|^{-s} = \sum_{\substack{M_1, M_2 \leq \mathbb{Z}_p \\ M_2 \leq M_1}} |\mathbb{Z}_p : M_1|^{-s} |\mathbb{Z}_p : M_2|^{-s} \\
&= \sum_{0 \leq a \leq b} t^{a+b} \\
&= \sum_{0 \leq a, c} t^{2a+c} \\
&= \sum_{0 \leq a} t^{2a} \sum_{0 \leq c} t^{c} = \frac{1}{(1-t)(1-t^2)}
\end{aligned}$$

Posets and its Hasse diagram

What we just saw is in fact the Hasse quiver of a poset $x \leq y$.

Let P be a partially ordered set (or poset) of cardinality n. A *P-partition of $m \in \mathbb{N}_0$* is an order-preserving/reversing (!) map $\sigma : P \to \mathbb{N}_0$ satisfying $|\sigma| := \sum_{i \in P} \sigma(i) = m$. We write $a_{m,P} := \#\{\sigma \mid |\sigma| = m\}$ for the number of P-partitions of m. Set

$$G_P(X) := \sum_{m=0}^{\infty} a_{m,P} X^m,$$

for a variable X.

Theorem (R. Stanley (2012))

$$G_P(X) = \frac{\sum_{\pi \in \mathbb{L}(P)} X^{maj(\pi)}}{\prod_{i=1}^{n}(1 - X^i)}.$$

In fact, P-partitions may be viewed as integral thin quiver representations of Hasse quivers of posets. Indeed, let Q_P be the Hasse quiver of P. Consider the thin $\mathbb{Z}$-representation V_P of Q_P where all arrows are represented by identity maps.

Theorem (L.-Voll (2023))

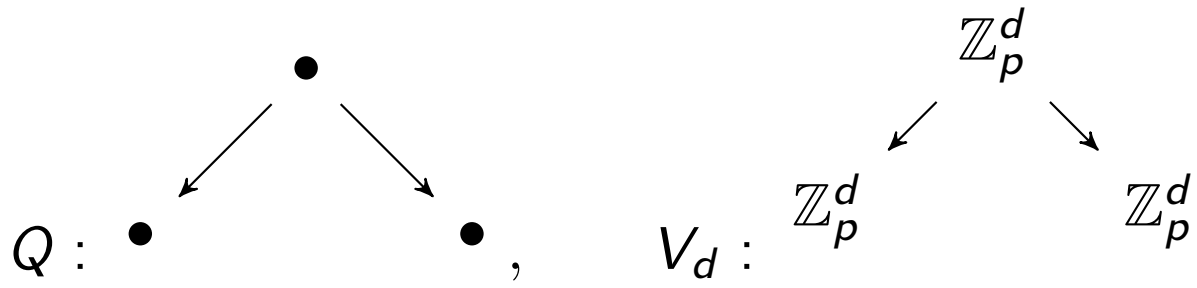
$$\zeta_{V_{Q_P}^{thin}}(s) = G_P(t) = \frac{\sum_{\pi \in \mathbb{L}(P)} X^{maj(\pi)}}{\prod_{i=1}^{n}(1-X^i)}.$$

In fact, P-partitions may be viewed as integral thin quiver representations of Hasse quivers of posets. Indeed, let Q_P be the Hasse quiver of P. Consider the thin $\mathbb{Z}$-representation V_P of Q_P where all arrows are represented by identity maps.

Theorem (L.-Voll (2023))

$$\zeta_{V_{Q_P}^{thin}}(s) = G_P(t) = \frac{\sum_{\pi \in \mathbb{L}(P)} X^{maj(\pi)}}{\prod_{i=1}^{n}(1-X^i)}.$$

Consider the following quiver representation



Theorem (L.-Voll (2023))

We have

$$\zeta_{V_1,p}(s) = \frac{1+t^2}{(1-t)(1-t^2)(1-t^3)},$$

$$\zeta_{V_2,p}(s) = \frac{(1+t^2)(1-pt^4)}{(1-t)(1-t^2)(1-t^3)(1-pt)(1-pt^2)^2(1-pt^3)}$$

Uniformity of $\zeta_V(s)$

Note that all the examples we studied so far had one single rational function to describe $\zeta_{V,p}(s)$ for almost all p. In other words, there exists one rational function $W(X, Y) \in \mathbb{Q}(X, Y)$ where

$$\zeta_{V,p}(s) = W(p, t)$$

for almost all p. In this case we say $\zeta_V(s)$ is *uniform*.

However, recall

Theorem (du Sautoy & Grunewald, Rossmann, L-Voll)

Let Γ be an algebraic structure defined as above. There are smooth algebraic varieties V_i, $i \in [k]$, defined over $\mathbb{Q}$, and rational functions $W_i(X, Y) \in \mathbb{Q}(X, Y)$ such that, for almost all primes p,

$$\zeta_{\Gamma,p}(s) = \sum_{i=1}^{k} \overline{V_i}(\mathbb{F}_p) W_i(p, t).$$

Uniformity of $\zeta_V(s)$

Note that all the examples we studied so far had one single rational function to describe $\zeta_{V,p}(s)$ for almost all p. In other words, there exists one rational function $W(X, Y) \in \mathbb{Q}(X, Y)$ where

$$\zeta_{V,p}(s) = W(p, t)$$

for almost all p. In this case we say $\zeta_V(s)$ is *uniform*.

However, recall

Theorem (du Sautoy & Grunewald, Rossmann, L-Voll)

Let Γ be an algebraic structure defined as above. There are smooth algebraic varieties V_i, $i \in [k]$, defined over $\mathbb{Q}$, and rational functions $W_i(X, Y) \in \mathbb{Q}(X, Y)$ such that, for almost all primes p,

$$\zeta_{\Gamma,p}(s) = \sum_{i=1}^{k} \overline{V_i}(\mathbb{F}_p) W_i(p, t).$$

Consider the following $\mathbb{Z}$-representation V of the Kronecker quiver K_2

$$\mathsf{K}_2: \quad \mathbb{Z}^2 \underset{f_2}{\overset{f_1}{\rightrightarrows}} \mathbb{Z}^2$$

with maps $f_1 = id$, $f_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Theorem (L.-Voll (2023))

$$\zeta_{V,p}(s) = \begin{cases} \frac{(1+t^2)(1-t^3)}{(1-t)(1-t^2)(1-t^4)(1-pt)(1-pt^3)}, & \text{if } p \equiv 1 \bmod (4), \\ \frac{1+t^3}{(1-t)(1-t^4)(1-pt)(1-pt^3)}, & \text{if } p \equiv 3 \bmod (4). \end{cases}$$

Theorem (Rossmann (2017))

If Q is a quiver with one vertex and one loop, then $\zeta_V(s)$ is uniform.

Theorem (Stanley (2012), L.-Voll (2023))

A quiver representation zeta function of thin quiver representations are uniform.

Conjecture

If Q is a simply laced quiver, in other words, if Q is a quiver of A, D, E type, then $\zeta_V(s)$ is uniform.

The local functional equation

Theorem (L.-Voll (2023))

If V satisfies certain "homogeneity condition", then $\zeta_V(s)$ satisfy the local functional equation, that there exist unique $a, b, c \in \mathbb{Z}$, such that

$$\zeta_{V,p}(s)\big|_{p\to p^{-1}} = (-1)^a p^{b-cs}\zeta_{V,p}(s).$$

Example

The local ideal zeta function

$$\zeta_{\mathbb{Z}^2}(s) = \frac{1}{(1-p^{-s})(1-p^{1-s})}.$$

satisfies the local functional equation

$$\zeta_{\mathbb{Z}^2,p}(s)\big|_{p\to p^{-1}} = p^{1-2s}\zeta_{\mathbb{Z}^2,p}(s).$$

Example

Even the above example

$$\zeta_{V,p}(s) = \begin{cases} \frac{(1+t^2)(1-t^3)}{(1-t)(1-t^2)(1-t^4)(1-pt)(1-pt^3)}, & \text{if } p \equiv 1 \bmod (4), \\ \frac{1+t^3}{(1-t)(1-t^4)(1-pt)(1-pt^3)}, & \text{if } p \equiv 3 \bmod (4). \end{cases}$$

satisfies, in both cases, the local functional equation

$$\zeta_{V,p}(s)|_{p \to p^{-1}} = p^2 t^6 \zeta_{V,p}(s).$$

Example

The quiver representation zeta function

$$\zeta_{V,p}(s) = \frac{1}{(1-t)(1-t^2)}.$$

satisfies the local functional equation

$$\zeta_{V,p}(s)|_{t \to t^{-1}} = t^3 \zeta_{V,p}(s).$$

Theorem (Stanley (2012))

The poset P satisfies the δ-chain condition if and only if the following functional equation holds:

$$G_P(X^{-1}) = (-1)^n X^{\delta(P)} G_P(X).$$

The "homogeneity condition" is equivalent to the δ-chain condition.

Problem

Can we prove that $\zeta_V(s)$ satisfy the local functional equation if and only if V satisfies certain "homogeneity condition"?

Zeta functions of algebraic structures

With Γ an algebraic object and $a_m(\Gamma) \in \mathbb{N}_0$ a sequence to study, define

$$\zeta_{(\Gamma, a_m(\Gamma))}(s) = \zeta_\Gamma(s) = \sum_{m=1}^{\infty} a_m(\Gamma) m^{-s}.$$

It normally satisfies an Euler factorization

$$\zeta_\Gamma(s) = \prod_{p \text{ prime}} \zeta_{\Gamma,p}(s).$$

Like zeta functions of groups and rings, we check

1. Rationality (Model Theory)
2. Abscissa of Convergence (Analytic Number Theory)
3. Uniformity (Algebraic Geometry)
4. Functional Equations (Combinatorics)

Finite groups and p-groups

Theorem (The Classification of Finite Simple Groups)

Every finite simple group is isomorphic to one of the following groups:

1. *A cyclic group C_p of prime order*
2. *An alternating group A_n of degree at least 5*
3. *A simple group of Lie type*
4. *The 26 sporadic simple groups*

Finite p-group G, a **group of prime power order** p^n for a prime p, is another important building block:

- Sylow theorems and Sylow p-subgroups,
- Most finite groups are p-groups.

Let $f(n)$ denote the number of groups of order n.

Example (The number of groups of order 1 to 40)

n	$f(n)$	n	$f(n)$	n	$f(n)$	n	$f(n)$
1	1	11	1	21	2	31	1
2	1	12	5	22	2	32	51
3	1	13	1	23	1	33	1
4	2	14	2	24	15	34	2
5	1	15	1	25	2	35	1
6	2	16	14	26	2	36	14
7	1	17	1	27	5	37	1
8	5	18	5	28	4	38	2
9	2	19	1	29	1	39	2
10	2	20	5	30	4	40	14

Total: 181 groups, p-groups: 92

Let $f(p, n)$ denote the number of groups of order p^n.

Example

	$p = 2$	$p \geq 3$
$f(p, 1)$	1	1
$f(p, 2)$	2	2
$f(p, 3)$	5	5
$f(p, 4)$	14	15

However, when $n = 5$ it becomes more interesting.

Theorem (Bagnera (1898))

For $p \geq 5$,

$$f(p,5) = 2p + 2gcd(p-1,\,3) + gcd(p-1,\,4) + 61$$

$$= \begin{cases} 2p+71 & if\ \ p \equiv 1 \mod 12, \\ 2p+67 & if\ \ p \equiv 5 \mod 12, \\ 2p+69 & if\ \ p \equiv 7 \mod 12, \\ 2p+65 & if\ \ p \equiv 11 \mod 12. \end{cases}$$

So $f(p,5)$ is one of 4 polynomials in p, with the choice of polynomials depending on the residue class of p modulo 12.

Higman's PORC conjecture

This is now known as Higman's PORC conejcture:

Conjecture (Higman's PORC conjecture (1960))

For fixed n, there is an integer $N(n)$ and polynomials $g_{n,i}(X)$ for $0 \leq i \leq M-1$ such that if $p \equiv i \bmod N(n)$ then

$$f(p,n) = g_{n,i}(p).$$

PORC stands for **Polynomial On Residue Classes.**

Current Results

Theorem (Newman, O'Brien & Vaughan-Lee (2004))

For $p > 5$,

$$f(p,6) = 3p^2 + 39p + 344 + 24\gcd(p-1,\,3) + 11\gcd(p-1,\,4) + 2\gcd(p-1,\,5).$$

Theorem (O'Brien & Vaughan-Lee (2005))

For $p > 5$,

$$\begin{aligned} f(p,7) = {} & 3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 \\ & + (4p^2 + 44p + 291)\gcd(p-1,\,3) \\ & + (p^2 + 19p + 135)\gcd(p-1,4) + (3p + 31)\gcd(p-1,\,5) \\ & + 4\gcd(p-1,\,7) + 5\gcd(p-1,\,8) + \gcd(p-1,\,9) \end{aligned}$$

Recent Results

Definition

A group G of order p^n is called a p-group with **Maximal Class** if its "nilpotency class" is $n-1$.

Theorem (L.–Vaughan-Lee (2022))

Let $m(p,n)$ denote the number of (isomorphism classes) of groups of order p^n with maximal class. For $p \geq 11$ the number of groups of order p^8 with **Maximal Class** *is*

$$\begin{aligned} m(p,8) = {} & 4p^3 + 7p^2 + 9p + 6 + (6p+11)\gcd(p-1,3) \\ & + 4\gcd(p-1,5) + (p+2)\gcd(p-1,7) \\ & + (p+3)\gcd(p-1,8) + 2\gcd(p-1,9) + \gcd(p-1,12). \end{aligned}$$

Theorem (L.-Vaughan-Lee (2022))

We have

$$
\begin{aligned}
m(p,4) &= 3 + \gcd(p-1,2),\\
m(p,5) &= 3 + 2\gcd(p-1,3) + \gcd(p-1,4),\\
m(p,6) &= 2p + 7 + 4\gcd(p-1,3) + 4\gcd(p-1,4)\\
&\quad + 2\gcd(p-1,5),\\
m(p,7) &= 2p^2 + 5p + 3 + (2p+2)\gcd(p-1,3)\\
&\quad + (p+4)\gcd(p-1,5) + \gcd(p-1,7) + \gcd(p-1,8),\\
m(p,8) &= 4p^3 + 7p^2 + 9p + 6 + (6p+11)\gcd(p-1,3)\\
&\quad + 4\gcd(p-1,5) + (p+2)\gcd(p-1,7)\\
&\quad + (p+3)\gcd(p-1,8) + 2\gcd(p-1,9) + \gcd(p-1,12).
\end{aligned}
$$

Moreover, $M(4) = 2, M(5) = 12, M(6) = 60, M(7) = 840, M(8) = 2520.$

Q&A

Thank you very much!