אוניברסיטת תל-אביב TEL AVIV UNIVERSITY

הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המחשב ע"ש בלבטניק

פונקציית זטא ותכונת רמנוג׳אן בגרפים רגולריים

חיבור זה מוגש כחלק ממילוי הדרישות לקבלת התואר
"מוסמך למדעים" בבית הספר למדעי המחשב באוניברסיטת תל-אביב

ע"י

בראטראם ראנגאראג׳אן

העבודה הוכנה בהנחיתו של פרופ׳ אמנון תא-שמע

יולי 2018

TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

Raymond and Beverly Sackler Faculty of Exact Sciences
The Blavatnik School of Computer Science

Zeta Functions and the Ramanujan Property for Regular Graphs

Thesis submitted in partial fulfillment of the requirements for the M.Sc. degree in the School of Computer Science, Tel-Aviv University

By

Bharatram Rangarajan

The research work for this thesis has been carried out at Tel-Aviv University under the supervision of Prof. Amnon Ta-Shma

July 2018

Acknowledgements

No amount of words can convey my gratitude to my sweet adviser Prof. Amnon Ta-Shma. His childlike enthusiasm for learning, his sharp and perceptive style of thinking, and his eye for detail will forever be an inspiration. But beyond all that, he had faith in me when even during my gloomiest phase when I had lost all faith in myself. I feel truly fortunate to have had him as my adviser, and will forever be indebted to him for his unwavering support and kindness.

I would also like to thank my parents for supporting me through thick and thin. I have given them much cause for stress and worry, but they have always believed I'll come through. I hope I can make them proud, and this thesis is the first step in that direction.

Abstract

We give an elementary combinatorial proof of Bass's determinant formula for the zeta function of a finite regular graph. This is done by expressing the number of non-backtracking cycles of a given length in terms of Chebychev polynomials in the eigenvalues of the adjacency operator of the graph.

In chapter one, zeta functions are introduced and explored in an abstract combinatorial setting. This paves the way for specialization to the case of graphs in chapter two, where the main definitions and tools are laid out.

A broad outline of the steps of the proof are described in chapter three, while the details are worked out in chapter four. We conclude with a brief overview of possible future directions in chapter five.

Contents

Chapter 1

Zeta Functions: A Combinatorial Perspective

In this chapter, we shall study an abstract formulation of a zeta function as a generating function. Zeta functions arise in many contexts, some of which are

- The Riemann zeta function $\zeta(s)$ defined as

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

- The Hasse-Weil zeta function $Z(t)$ of an algebraic function field F defined as

$$Z(t) = A_0 + A_1 t + A_2 t^2 + A_3 t^3 + \dots$$

  where for every $k \in \mathbb{Z}_{\geq 0}$, A_k is the number of positive divisors of F of degree k.

- The Ihara zeta function $\zeta_G(t)$ for a finite undirected graph $G = (V, E)$ defined as

$$\zeta_G(t) = exp\left(N_1 t + \frac{N_2}{2} t^2 + \frac{N_3}{3} t^3 + \dots\right)$$

  where for $k \in \mathbb{N}$, N_k is the number of non-backtracking closed walks on G of length k.

Broadly speaking, a zeta function is a complex function which when expressed as a series, yields a coefficient sequence that counts "objects" of a given "weight" assembled from an underlying set of building blocks or "primes". For instance, the Riemann

zeta function corresponds to a Dirichlet series where the coefficient of $1/k^s$ counts the number of positive integers (constructed using the primes of $\mathbb{Z}$ as building blocks) of absolute value k (which in this case is trivially 1 for every $k \in \mathbb{N}$). Similarly the Hasse Weil zeta function corresponds to an ordinary power series that counts the number of positive divisors (constructed using the places of the function field as building blocks).

Let $\mathcal{P}$ be a countable (finite or countably infinite) set. We shall be interested in multisets of elements of $\mathcal{P}$. Informally, a multiset is a set which allows repetitions (but is unordered). Formally, a multiset over $\mathcal{P}$ is a function

$$m : \mathcal{P} \to \mathbb{Z}_{\geq 0}$$

which assigns to every element $a \in \mathcal{P}$ a non-negative integer $m(a)$ which can be interpreted as the multiplicity of a. For our purposes, we shall be interested in multisets satisfying the additional (finiteness) condition that

$$m(a) = 0 \text{ for all but finitely many } a \in \mathcal{P}$$

This allows us to view a finite multiset intuitively as a finite subset but with possible repetitions, as mentioned earlier. In other words, a multiset α is a set of tuples of the form

$$\alpha = \{(a_1, m_\alpha(a_1)), (a_2, m_\alpha(a_2)), \ldots, (a_r, m_\alpha(a_r))\}$$

for distinct elements $a_1, a_2, \ldots, a_r \in m^{-1}(\mathbb{N})$. Clearly, the cardinality $\#\alpha$ of this multiset α, viewed as a set with repetitions, is

$$\#\alpha = \sum_{i=1}^{r} m_\alpha(a_i)$$

which is the sum of the multiplicities of the elements occurring in α, while the number of distinct elements in α is r. Denote by $\mathcal{M}$ the set of multisets of $\mathcal{P}$ of finite cardinality.

It is natural to ask what the number of multisets of a given cardinality is. This question, of course, is meaningful only if $\mathcal{P}$ is finite. So suppose we have a finite set expressed as

$$\mathcal{P} = \{1, 2, 3, \ldots, n\} = [n]$$

of cardinality n. We are interested in computing the number of multisets over $\mathcal{P}$ of cardinality k. Note that k could be arbitrarily large, unlike in the case of binomial coefficients, since we now allow for repetitions. This is also different from counting the number of strings of length k formed using an alphabet of size k, since permutations of a string may form different strings.

Let $\alpha = \{(1, m_\alpha(1)), (2, m_\alpha(2)), \ldots, (n, m_\alpha(n))\}$ be a multiset over $[n]$. Then for α to have cardinality k, we only require

$$m_\alpha(1) + m_\alpha(2) + \cdots + m_\alpha(n) = k$$

So the number of multisets over $[n]$ of cardinality k is the number of solutions to the equation

$$m_1 + m_2 + \cdots + m_n = k$$

such that $m_i \in \mathbb{Z}_{\geq 0}$ for every $1 \leq i \leq n$, and this is exactly

$$\binom{n+k}{k} = \left(\binom{n}{k}\right)$$

Another route to above expression is through the use of generating functions. If we fix an element $a \in \mathcal{P}$, then it is clear that for every $k \in \mathbb{Z}_{\geq 0}$, there is precisely one multiset of size k that can be constructed using only the element a, and is of the form

$$\{\underbrace{a, a, a, \ldots, a}_{k\text{times}}\} = (a, k)$$

This gives us a sequence

$$(a_k)_{k \in \mathbb{Z}_{\geq 0}} = (1, 1, 1, 1, \ldots)$$

where the k-th element of the sequence is the number of multisets of cardinality k constructed using only the element a. Similarly, for another element $b \in \mathcal{P}$ with $b \neq a$, the sequence counting the number of multisets of a given weight constructible using only the element b is again

$$(b_k)_{k \in \mathbb{Z}_{\geq 0}} = (1, 1, 1, 1, \ldots)$$

Now consider the number of multisets of weight k constructible using *both* a and b. It

is easy to see that this is exactly

$$\sum_{j=0}^{k} a_j b_{k-j}$$

or the (additive) *convolution* of the sequences $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$ and $(b_k)_{k\in\mathbb{Z}_{\geq 0}}$. This convolution of sequences is explicitly realized using ordinary generating functions for the sequences $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$ and $(b_k)_{k\in\mathbb{Z}_{\geq 0}}$. So the generating function for the number of multisets of weight k constructible using *both* a and b is

$$(1 + t + t^2 + t^3 + \dots)(1 + t + t^2 + t^3 + \dots) = \frac{1}{(1-t)^2}$$

This argument can be generalized to n elements to yield the following generating function for multiset counting:

$$\sum_{k=0}^{\infty} \left(\binom{n}{k} \right) t^k = \frac{1}{(1-t)^n}$$

We shall soon see more fundamental uses for generating functions especially when the terms of the sequence do not have simple expressions even though we understand how they "convolve".

The first step in studying the set $\mathcal{M}$ of finite multisets over $\mathcal{P}$ is to imbue it with some algebraic structure. The simplest and most natural structure on $\mathcal{M}$ is an order, reminiscent of set inclusion ordering. Define an ordering $\leq$ on $\mathcal{M}$ as follows: For two multisets $\alpha, \beta \in \mathcal{M}$, we denote

$$\alpha \leq \beta$$

if for every $a \in \mathcal{P}$,

$$m_\alpha(a) \leq m_\beta(a)$$

In other words,

- The underlying set of elements of α is a subset of the underlying set of elements of β.
- For an element $a \in \mathcal{P}$ that occurs in α, its multiplicity in α is at most its multiplicity in β.

So $\leq$ on $\mathcal{M}$ is an intuitive generalization of the set inclusion ordering to the case of

multisets. It is straightforward to check that this ordering is transitive, and is hence a *partial ordering* on the set $\mathcal{M}$ of multisets over $\mathcal{P}$. Thus, $\mathcal{M}$ is a partially ordered set, or a *poset*, under the multiset inclusion ordering.

We can also define a binary operation $\oplus$ on multisets in $\mathcal{M}$ as follows: for $\alpha, \beta \in \mathcal{M}$,

$$m_{\alpha \oplus \beta} = m_\alpha + m_\beta$$

In other words, the sum of two multisets is essentially a concatenation of the two multisets, upto ordering. The multiplicity of an element in $\alpha \oplus \beta$ is the sum of its multiplicity in α and its multiplicity in β. It is clear that $\alpha \oplus \beta \in \mathcal{M}$, and for any multisets $\alpha, \beta, \gamma \in \mathcal{M}$,

$$(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma)$$

$$\alpha \oplus \phi = \phi \oplus \alpha = \alpha$$

$$\alpha \oplus \beta = \beta \oplus \gamma$$

Thus the binary operation $\oplus$ on $\mathcal{M}$ is associative and has the null multiset ϕ as its identity. The operation is also commutative. So $\mathcal{M}$ forms a commutative semigroup under the operation $\oplus$. However, $\mathcal{M}$ is *not* a group under $\oplus$, since no element (except ϕ) has an inverse!
It is also clear that

$$\alpha, \beta \leq \alpha \oplus \beta$$

so $\oplus$ is well-behaved with respect to the partial ordering on $\mathcal{M}$. This allows us to define a "subtraction" as follows: for multisets $\beta \leq \gamma$, define

$$\gamma \ominus \beta = \alpha$$

where $\alpha \in \mathcal{M}$ is the unique multiset such that

$$\alpha \oplus \beta = \gamma$$

The uniqueness of such an element follows from the cancellation property of the semigroup. The multiset $\gamma \ominus \beta$ can be visualized as the analogue of set difference.

1.1 The Convolution Algebra $\mathbb{C}^{\mathcal{M}}$

So we have the partially ordered set $\mathcal{M}$ which is now also a semigroup under the binary operation $\oplus$. Consider the $\mathbb{C}$-space $\mathbb{C}^{\mathcal{M}}$ which can be interpreted as the vector space of complex functions on $\mathcal{M}$ under pointwise addition and multiplication. Every vector

$$f : \mathcal{M} \to \mathbb{C}$$

can be represented by a formal series sum

$$\sum_{\alpha \in \mathcal{M}} f(\alpha)\alpha$$

Note that this is simply a formal sum where α acts as a placeholder for $f(\alpha)$. For any two vectors $f, g : \mathcal{M} \to \mathbb{C}$ and $c \in \mathbb{C}$, observe that the pointwise addition and scalar multiplication of vectors f and g are realized as

$$f + g \longleftrightarrow \sum_{\alpha \in \mathcal{M}} (f(\alpha) + g(\alpha))\alpha$$

$$c \cdot f \longleftrightarrow \sum_{\alpha \in \mathcal{M}} cf(\alpha)\alpha$$

Now that $\mathcal{M}$ is not just a set but also a partially ordered semigroup, we can use this additional structure to define a product of vectors of $\mathbb{C}^{\mathcal{M}}$. This is best realized through the representation of the vectors as formal series over $\mathcal{M}$ as follows: define

$$\left(\sum_{\alpha \in \mathcal{M}} f(\alpha)\alpha\right) . \left(\sum_{\beta \in \mathcal{M}} g(\beta)\beta\right) = \sum_{\alpha,\beta \in \mathcal{M}} f(\alpha).g(\beta)(\alpha \oplus \beta)$$

That is, we define the product of elements α and β using the binary operation $\oplus$ of the semigroup $\mathcal{M}$ and then extend it $\mathbb{C}$-linearly to define products of formal sums.
We denote this product by

$$f * g$$

and observe that

$$(f * g)(\alpha) = \sum_{\beta \leq \alpha} f(\beta) \cdot g(\alpha \ominus \beta)$$

The vector space $\mathbb{C}^{\mathcal{M}}$ of complex functions on the partially ordered semigroup $\mathcal{M}$ endowed with this (convolution) product forms a semigroup algebra. As mentioned earlier, the element α in the formal sum

$$\sum_{\alpha \in \mathcal{M}} f(\alpha)\alpha$$

can be thought of as simply a placeholder for the index α, and the multiplication of formal series uses the semigroup structure of the set of indices. This means that we could just as well work with a semigroup homomorphism of $\mathcal{M}$ if it could help us realize this multiplication in simpler ways. More precisely, suppose S is an abelian semigroup with binary operation $+$, and

$$W : \mathcal{M} \to S$$

is a function from $\mathcal{M}$ to S that is well behaved with respect to their corresponding operations. That is, for every $\alpha, \beta \in \mathcal{M}$,

$$W(\alpha \oplus \beta) = W(\alpha) + W(\beta)$$

and

$$W(\phi) = 0$$

This can be extended to give us a map from the algebra $\mathbb{C}^{\mathcal{M}}$ to $\mathbb{C}^{S}$ as

$$\sum_{\alpha \in \mathcal{M}} f(\alpha)\alpha \mapsto \sum_{\alpha \in \mathcal{M}} f(\alpha)W(\alpha)$$

Note that

$$\left(\sum_{\alpha \in \mathcal{M}} f(\alpha)W(\alpha)\right) . \left(\sum_{\beta \in \mathcal{M}} g(\beta)W(\beta)\right) = \sum_{\gamma \in \mathcal{M}} (f * g)(\gamma)W(\gamma)$$

If W is an injective map, then the above identity is equivalent to the original, and not of much additional value. However, if W were not injective, then the above identity

helps "collect" all terms corresponding to a specific value taken by W. That is,

$$\sum_{\alpha \in \mathcal{M}} f(\alpha) W(\alpha) = \sum_{s \in S} \left(\sum_{W(\alpha)=s} f(\alpha) \right) s$$

For example, let $S = \mathbb{Z}[t]$ under multiplication, and consider the function

$$W : \mathcal{M} \to \mathbb{Z}[t]$$

$$W(\alpha) = t^{\#\alpha}$$

where $\#\alpha$ is the cardinality of the multiset α. Then observe that the function

$$\sum_{\alpha \in \mathcal{M}} \alpha$$

gets mapped to

$$\sum_{\alpha \in \mathcal{M}} t^{\#\alpha}$$

and this is equal to

$$\sum_{k=0}^{\infty} \left(\sum_{\#\alpha=k} 1 \right) t^k$$

which, as an ordinary power series, counts the number of multisets of a given cardinality. However, in this specific case, this is not well-defined in general since if $\mathcal{P}$ is infinite, there are infinitely many multisets of any given cardinality $k \geq 1$. This situation can be worked around using a notion of weights and grading so that there exist only finitely many multisets of a given "weight", which we shall soon explore in more detail.

But first, let us see some simple examples of functions (or vectors) in the algebra $\mathbb{C}^{\mathcal{M}}$. Firstly, the multiplicative identity of the algebra is given by the delta function

$$\delta : \mathcal{M} \to \mathbb{C}$$

$$\delta(\alpha) = \begin{cases} 1 & \text{if } \alpha = \phi \\ 0 & \text{otherwise} \end{cases}$$

which corresponds to the trivial formal series 1.

The simplest non-trivial function in $\mathbb{C}^{\mathcal{M}}$ is the constant function. The constant 1 function, denoted $\vec{1}$, is called the *zeta function* of $\mathcal{M}$. The inverse of the zeta function (with respect to convolution) is the function $\mu_{\mathcal{M}}$ defined recursively as follows:

$$\mu_{\mathcal{M}} : \mathcal{M} \to R$$

$$\mu_{\mathcal{M}}(\alpha) = \begin{cases} 1 & \text{if } \alpha = \phi \\ -\sum\limits_{\beta<\alpha} \mu_{\mathcal{M}}(\beta) & \text{otherwise} \end{cases}$$

We can carefully compute $\mu_{\mathcal{M}}(\alpha)$ based on properties of α. For starters, suppose $\alpha_1 = \{(a, 1)\}$ or the multiset comprising just the element $a \in \mathcal{P}$ with multiplicity 1. Then

$$\mu_{\mathcal{M}}(\alpha_1) = -\mu_{\mathcal{M}}(\phi) = -1$$

Next suppose $\alpha_2 = \{(a, 2)\}$ or the multiset comprising just the element $a \in \mathcal{P}$ with multiplicity 2. Then

$$\mu_{\mathcal{M}}(\alpha_2) = -\mu_{\mathcal{M}}(\phi) - \mu_{\mathcal{M}}(\alpha_1) = 0$$

In fact, for a multiset $\alpha = \{(a, m)\}$ comprising the element a of multiplicity $m \geq 2$,

$$\mu_{\mathcal{M}}(\alpha) = 0$$

Next consider a multiset $\alpha = \{(a, 1), (b, 1)\}$. In this case

$$\mu_{\mathcal{M}}(\alpha) = -\mu_{\mathcal{M}}(\phi) - \mu_{\mathcal{M}}(a, 1) - \mu_{\mathcal{M}}(b, 1) = -1 + 1 + 1 = 1$$

More generally, we can prove by induction that for a multiset $\alpha \in \mathcal{M}$ of the form

$$\alpha = \{(a_1, m_\alpha(a_1)), (a_2, m_\alpha(a_2)), \ldots, (a_r, m_\alpha(a_r))\}$$

the value $\mu_{\mathcal{M}}(\alpha)$ is given by

$$\mu_{\mathcal{M}}(\alpha) = \begin{cases} 0 & \text{if } m(a_i) \geq 2 \text{ for some } 1 \leq i \leq r \\ 1 & \text{if } m(a_i) = 1 \text{ for every } 1 \leq i \leq r \text{ and } r \text{ is even} \\ -1 & \text{if } m(a_i) = 1 \text{ for every } 1 \leq i \leq r \text{ and } r \text{ is odd} \end{cases}$$

In other words, the function $\mu_{\mathcal{M}}$ is a function

$$\mu_{\mathcal{M}} : \mathcal{M} \to \{0, 1, -1\}$$

$$\mu_{\mathcal{M}}(\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ is not a set} \\ 1 & \text{if } \alpha \text{ is a set of even cardinality} \\ -1 & \text{if } \alpha \text{ is a set of odd cardinality} \end{cases}$$

The function $\mu_{\mathcal{M}}$, which is the multiplicative inverse of the constant 1 function, is called the *Mobius function* of the semigroup $\mathcal{M}$. In particular,

$$\mu_{\mathcal{M}} * \vec{1} = \vec{1} * \mu_{\mathcal{M}} = \delta$$

which leads to the following useful result:

Theorem 1 (Mobius inversion)**.**

$$f * \vec{1} = g \longleftrightarrow f = g * \mu_{\mathcal{M}}$$

In other words, suppose $f, g : \mathcal{M} \to \mathbb{C}$ are such that for every $\alpha \in \mathcal{M}$,

$$g(\alpha) = \sum_{\beta \leq \alpha} f(\beta)$$

then Mobius inversion tells us that for every $\alpha \in \mathcal{M}$,

$$f(\alpha) = \sum_{\beta \leq \alpha} g(\beta) \mu_{\mathcal{M}}(\alpha \ominus \beta)$$

So we started out with a countable set $\mathcal{P}$, and defined the partially-ordered set $\mathcal{M}$ of finite multisets over $\mathcal{P}$ where the ordering is intuitively just the inclusion ordering. We also saw how to count the number of multisets of a given cardinality when $\mathcal{P}$ is a finite set. To extend this approach to countably infinite sets too, we would need some kind of "grading" of $\mathcal{P}$ as a disjoint union of (an infinite number of) finite sets. This would allow us to grade the multisets too, allowing us to apply combinatorial tools to count the number of multisets in a particular grade. As we shall now see, the whole idea of a zeta function is to capture the combinatorial relationship between the grades of the weight function on $\mathcal{M}$ and those of $\mathcal{P}$.

We shall now associate each element of $\mathcal{P}$ with a weight so that we can study multisets of a given weight. Formally, this is done by defining a function from $\mathcal{P}$ to $\mathbb{N}$ and extending this function to $\mathcal{M}$. Let

$$w : \mathcal{P} \to \mathbb{N}$$

be a (weight) function that assigns a positive integer to every element of $\mathcal{P}$. This makes $\mathcal{P}$ a *graded set* of the form

$$\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \cup \dots$$

where for every $k \in \mathbb{N}$,

$$\mathcal{P}_k = w^{-1}(k)$$

That is, $\mathcal{P}_k$ is the set of elements of $\mathcal{P}$ which get mapped by w to $k \in \mathbb{N}$, or informally, the subset of elements of $\mathcal{P}$ of weight k.

In general, nothing so far stops $\mathcal{P}_k$ from being an infinite set. For our combinatorial purposes however, it is necessary to impose the constraint that $\mathcal{P}_k$ is finite for every $k \in \mathbb{N}$. In other words, even though $\mathcal{P}$ may be an infinite set, we shall assume that the weight function $w : \mathcal{P} \to \mathbb{N}$ is such that the subset of elements of weight k is finite for every $k \in \mathbb{N}$. Denote by B_k the cardinality of the set $\mathcal{P}_k$. So for every $k \in \mathbb{N}$,

$$B_k = |\mathcal{P}_k|$$

We now want to extend the domain of the weight function w from $\mathcal{P}$ to the partially-ordered semigroup $\mathcal{M}$ of multisets of $\mathcal{P}$. It is preferable to constrain the extension to respect the semigroup structure and partial ordering of $\mathcal{M}$. The two most natural semigroups that arise from $\mathbb{N}$ are the additive semigroup $(\mathbb{Z}_{\geq 0}, +)$ (with identity 0) and the multiplicative semigroup $(\mathbb{N}, \times)$ (with identity 1). This allows us to construct two useful extensions of the weight function to $\mathcal{M}$: Let $\alpha \in \mathcal{M}$ be a multiset represented as

$$\alpha = \{(a_1, m_\alpha(a_1)), (a_2, m_\alpha(a_2)), \dots, (a_r, m_\alpha(a_r))\}$$

- *Additive*: The weight of a multiset α is defined as

$$w_+(\phi) = 0$$

$$w_+(\alpha) = m_\alpha(a_1)\cdot w(a_1) + m_\alpha(a_2)\cdot w(a_2) + \cdots + m_\alpha(a_r)\cdot w(a_r) = \sum_{i=1}^{r} m_\alpha(a_i)w(a_i)$$

In other words, for multisets $\alpha, \beta \in \mathcal{M}$,

$$w_+(\alpha \oplus \beta) = w_+(\alpha) + w_+(\beta)$$

- *Multiplicative*: The weight of a multiset α is defined as

$$w_\times(\phi) = 0$$

$$w_\times(\alpha) = w(a_1)^{m_\alpha(a_1)} w(a_2)^{m_\alpha(a_2)} \ldots w(a_r)^{m_\alpha(a_r)} = \prod_{i=1}^{r} w(a_i)^{m_\alpha(a_i)}$$

In other words, for multisets $\alpha, \beta \in \mathcal{M}$,

$$w_\times(\alpha \oplus \beta) = w_\times(\alpha) w_\times(\beta)$$

Conceptually, the two are not different, though in practice, one of them would arise more naturally than the other based on the context.

Let us first study the additive weight extension $w_+ : \mathcal{M} \to \mathbb{Z}_{\geq 0}$ of $w : \mathcal{P} \to \mathbb{N}$. For $k \geq 0$, denote by $\mathcal{A}_k$ the subset of $\mathcal{M}$ comprising multisets of weight exactly k.

$$\mathcal{A}_k = w_+^{-1}(k) = \{\alpha \in \mathcal{M} : w_+(\alpha) = k\}$$

Clearly,

$$\mathcal{M} = \mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{A}_2 \cup \ldots$$

and so we have now obtained a graded decomposition of the set $\mathcal{M}$ based on the weights of the multisets.

The first question we need to address is whether $\mathcal{A}_k$ is finite. Note that

$$\mathcal{A}_0 = \{\phi\}$$

and so $\mathcal{A}_0$, being a singleton set, is trivially finite. Similarly

$$\mathcal{A}_1 = \mathcal{P}_1$$

and since we have assumed that $\mathcal{P}_k$ is finite for every $k \in \mathbb{N}$, $\mathcal{A}_1$ is also finite.

The first non-trivial case is $\mathcal{A}_2$. A multiset of weight 2 arises either as an element of $\mathcal{P}_2$ with multiplicity 1, or as an element of $\mathcal{P}_1$ with multiplicity 2, or as a set of two distinct elements of $\mathcal{P}_1$ both with multiplicity 1. Again, since $\mathcal{P}_1$ and $\mathcal{P}_2$ are finite, $\mathcal{A}_2$ is easily seen to be a finite set. In fact, we can compute the cardinality $|\mathcal{A}_2|$ to be

$$|\mathcal{A}_2| = B_2 + \binom{B_1}{2} + \binom{B_1}{1}$$

A better way to interpret the above would be as follows: the weight 2 can be partitioned in two distinct ways:

$$\begin{aligned} 2 &= 2 \\ &= 1 + 1 \end{aligned}$$

The first partition 2 corresponds to the set of multisets comprising just one element of $\mathcal{P}$ of weight 2, while the second partition $1 + 1$ corresponds to the set of multisets comprising two elements of order 1. Interpreted this way, an equivalent, but more illuminating, expression for the cardinality of $\mathcal{A}_2$ would be

$$|\mathcal{A}_2| = \left(\binom{B_2}{1}\right) + \left(\binom{B_1}{2}\right)$$

That is, we count $|\mathcal{A}_2|$ by first studying the different ways that 2 can be expressed as (an unordered) sum of positive integers. Each such sum corresponds to a set of multisets in $\mathcal{M}$ whose cardinalities we can easily compute.
More generally, consider $|\mathcal{A}_k|$ for $k \geq 3$. The first step in computing $|\mathcal{A}_k|$ is to write out the different ways that k can be expressed as an (unordered) sum of positive integers. That is, we are interested in the *partitions* of k. A partition λ of k, denoted $\lambda \vdash k$, can be uniquely represented by a tuple

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{Z}_{\geq 0}$$

that satisfies the equation

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + k\lambda_k = k$$

Here we can interpret λ_i as counting the number of occurences of weight i elements in the multiset. Each such partition corresponds to a finite collection of multisets of weight k, and of cardinality

$$\left(\binom{B_1}{\lambda_1}\right)\left(\binom{B_2}{\lambda_2}\right)\left(\binom{B_3}{\lambda_3}\right)\cdots\left(\binom{B_k}{\lambda_k}\right)$$

and so

$$|\mathcal{A}_k| = \sum_{\lambda \vdash k} \prod_{i=1}^{k} \left(\binom{B_k}{\lambda_k}\right)$$

Since the number of partitions of a positive integer is always finite, and $|\mathcal{A}_k|$ is a sum over partitions of k of finite positive integers,

Lemma 2. *For every $k \geq 0$, the set $\mathcal{A}_k \subseteq \mathcal{M}$ is finite.*

Denote

$$A_k = |\mathcal{A}_k|$$

As we just saw, we have an explicit expression for A_k as a sum over partitions of k of a product of multiset countings:

$$A_k = \sum_{\lambda \vdash k} \prod_{i=1}^{k} \left(\binom{B_k}{\lambda_k}\right)$$

However, we do not know any simple, precise expression for the number of partitions of an integer, so the above expression seems impervious to any further simplifications.

1.2 The Zeta, Mobius and von Mangoldt functions

Here is where generating functions can greatly simplify matters by sidestepping the need to delve into partition functions. This is done by a counting of elements of $\mathcal{A}$ using the elements of $\mathcal{P}$ as building blocks. The argument is essentially how we counted the number of multisets of a given cardinality over a finite underlying set. But now we shall also use weights (and the additivity of the weight function for multisets), which

can be interpreted as a generalization of cardinality.

As before, for an element $a \in \mathcal{P}$ of weight 1, consider the multisets

$$\phi, \{a\}, \{a, a\}, \{a, a, a\}, \dots$$

The above sequence contains all possible multisets in $\mathcal{M}$ obtained using only the element $a \in \mathcal{P}$ of weight 1, and it is easy to see that this collection contains exactly 1 multiset of weight k for every $k \in \mathbb{Z}_{\geq 0}$. So the element a corresponds to the sequence $(a_k)_{k \in \mathbb{Z}_{\geq 0}}$

$$(a_k)_{k \in \mathbb{Z}_{\geq 0}} = (1, 1, 1, \dots)$$

where a_k is the number of multisets of weight k formed using only the element a.

Similarly, for an element $b \in \mathcal{P}$ of weight 1 with $b \neq a$, we have a sequence

$$(b_k)_{k \in \mathbb{Z}_{\geq 0}} = (1, 1, 1, \dots)$$

counting the number of multisets of a given weight constructed using only the element b.

Now consider the number of multisets of a given weight constructed only using both a and b. Observe that a multiset of weight k obtained using only a and b arises as

$$\alpha \oplus \beta$$

where α is constructed using only the element a and β is constructed using only the element b, and such that

$$w_+(\alpha \oplus \beta) = k$$

So the number of multisets of weight k obtained using only a and b is

$$\sum_{w_+(\alpha \oplus \beta) = k} 1$$

Here is precisely where we use the additive structure of the weight function for multisets: the weight of a multiset is the sum of the weights of its constituent elements counted with multiplicity. So the above sum is essentially the number of pairs (α, β) such that α is constructed using only the element a and β is constructed using only the element b,

and the sum of their weights is k. This is exactly additive convolution of the sequence $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$ and $(b_k)_{k\in\mathbb{Z}_{\geq 0}}$

$$\sum_{j=0}^{k} a_j b_{k-j}$$

which in this case happens to be exactly $k+1$ since $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$ and $(b_k)_{k\in\mathbb{Z}_{\geq 0}}$ are constant sequences.

The additive convolution used here guides our choice of generating function to be an ordinary power series, and we obtain the generating function for the number of multisets of a given weight constructed only using both a and b to be

$$(1+t+t^2+t^3+\dots)(1+t+t^2+t^3+\dots) = \frac{1}{(1-t)^2}$$

A similar argument can be used for elements of larger weight too, though now the sequence counting the multisets constructed using only an element c of weight $n \geq 2$ would be

$$(c_k)_{k\in\mathbb{Z}_{\geq 0}} = (1, \underbrace{0,0,\dots,0}_{\text{n-1 times}}, 1, \underbrace{0,0,\dots,0}_{\text{n-1 times}}, 1, 0, 0, \dots)$$

More precisely,

$$c_k = \begin{cases} 1 & \text{if } k \equiv 0 \mod n \\ 0 & \text{otherwise} \end{cases}$$

In this case, the generating function for $(c_k)_{k\in\mathbb{Z}_{\geq 0}}$ is

$$1 + t^n + t^{2n} + t^{3n} + \dots = \frac{1}{1-t^n}$$

Recall that in general, we denote by B_k the number of prime elements of weight k, and by A_k the number of multisets of weight k. Putting it all together, we see that

Theorem 3 (Euler Product)**.**

$$A_0 + A_1 t + A_2 t^2 + A_3 t^3 + \dots = \prod_{n=1}^{\infty} \left(\frac{1}{1-t^n}\right)^{B_n}$$

Let us denote the formal series above by $\zeta(t)$. So on the one hand, $\zeta(t)$ is a sum of the form

$$\zeta(t) = \sum_{k=0}^{\infty} A_k t^k$$

while it is also a product of the form

$$\zeta(t) = \prod_{n=1}^{\infty} \left(\frac{1}{1-t^n}\right)^{B_n}$$

The product formulation allows us to play around further with the generating function $\zeta(t)$. For instance, we now know what the reciprocal of $\zeta(t)$ looks like:

$$\frac{1}{\zeta(t)} = \prod_{n=1}^{\infty}(1-t^n)^{B_n}$$

Working out this expression further,

$$\begin{aligned}\frac{1}{\zeta(t)} &= \prod_{n=1}^{\infty}(1-t^n)^{B_n} \\ &= \prod_{n=1}^{\infty}\left(\sum_{j=0}^{B_n}(-1)^j\binom{B_n}{j}t^{n\cdot j}\right)\end{aligned}$$

Multiplying out the above product into an ordinary power series in t, we see that

- The constant term is 1.
- The coefficient of t is
$$-\binom{B_1}{1}$$
- The coefficient of t^2 is
$$\binom{B_1}{2} - \binom{B_2}{1}$$
- The coefficient of t^3 is
$$-\binom{B_1}{3} + \binom{B_2}{1}\binom{B_1}{1} - \binom{B_3}{1}$$

More generally, the coefficient of t^k would again involve a sum over partitions $\lambda = (\lambda_1, \ldots, \lambda_k)$ of k of products of binomial coefficients as follows:

$$\sum_{\lambda\vdash k}\prod_{i=1}^{k}(-1)^{\lambda_i}\binom{B_i}{\lambda_i} = \sum_{\lambda\vdash k}(-1)^{\sum_{i=1}^{k}\lambda_i}\binom{B_1}{\lambda_1}\binom{B_2}{\lambda_2}\cdots\binom{B_k}{\lambda_k}$$

Observe that for a partition λ, the term

$$(-1)^{\sum_{i=1}^{k} \lambda_i}$$

is an indicator for whether the number of elements in the partition is odd or even. And once we fix a partition λ, the term

$$\binom{B_1}{\lambda_1}\binom{B_2}{\lambda_2}\cdots\binom{B_k}{\lambda_k}$$

is the number of *sets* constructed using λ_i (distinct) elements of $\mathcal{P}_i$ for every $1 \leq i \leq k$.

Another more abstract way of interpreting the series $\zeta(t)$ is as the series summed over multisets in $\mathcal{M}$

$$\zeta(t) = \sum_{\alpha \in \mathcal{M}} t^{w_+(\alpha)}$$

This can be interpreted as the generating function for the constant 1 function

$$\vec{1} : \mathcal{M} \to \mathbb{Z}$$

$$\vec{1}(\alpha) = 1$$

for every $\alpha \in \mathcal{M}$. More generally, for functions

$$f, g : \mathcal{M} \to \mathbb{Z}$$

recall that

$$(f * g)(\alpha) = \sum_{\beta \leq \alpha} f(\beta).g(\alpha \ominus \beta)$$

So

$$\left(\sum_{\alpha \in \mathcal{M}} f(\alpha) t^{w_+(\alpha)}\right)\left(\sum_{\beta \in \mathcal{M}} g(\beta) t^{w_+(\beta)}\right) = \sum_{\gamma \in \mathcal{M}} \left((f * g)(\gamma)\right) t^{w_+(\gamma)}$$

That is, multiplication of formal series (summed over $\mathcal{M}$) where the function corresponding to an $\alpha \in \mathcal{M}$ is $t^{w_+(\alpha)}$ precisely reflects the convolution of the corresponding functions from $\mathcal{M}$ to $\mathbb{Z}$.

So the reciprocal of $\zeta(t)$ corresponds to the multiplicative inverse of the constant 1 function with respect to convolution, and this we know to be the Mobius function $\mu_{\mathcal{M}}$.

Thus,

$$\frac{1}{\sum\limits_{\alpha\in\mathcal{M}} t^{w_+(\alpha)}} = \sum_{\alpha\in\mathcal{M}} \mu_{\mathcal{M}}(\alpha) t^{w_+(\alpha)}$$

Now

$$\sum_{\alpha\in\mathcal{M}} \mu_{\mathcal{M}}(\alpha) t^{w_+(\alpha)} = C_0 + C_1 t + C_2 t^2 + \dots$$

where

$$C_k = \sum_{w_+(\alpha)=k} \mu_{\mathcal{M}}(\alpha) = \sum_{\mu\vdash k} (-1)^{\sum\limits_{i=1}^{k} \mu_i} \binom{B_1}{\mu_1}\binom{B_2}{\mu_2}\dots\binom{B_k}{\mu_k}$$

as we saw before.

So we have seen two important functions of $\mathcal{M}$:

- The constant 1 function $\vec{1} : \mathcal{M} \to \mathbb{Z}$ corresponding to the zeta function

$$\zeta(t) = \sum_{\alpha\in\mathcal{M}} t^{w_+(\alpha)} = \sum_{k=0}^{\infty} A_k t^k$$

- The Mobius function $\mu_{\mathcal{M}} : \mathcal{M} \to \{0, 1, -1\}$ corresponding to the generating function

$$\frac{1}{\zeta(t)} = \sum_{\alpha\in\mathcal{M}} \mu_{\mathcal{M}}(\alpha) t^{w_+(\alpha)}$$

The next natural function of $\mathcal{M}$ is the weight function itself. After all, the zeta function and the Mobius function were both defined independent of the notion of weight (the weight came in only later when we were interested in counting terms of a given weight). In contrast, the weight function is a function that obviously depends on the structure of the weights. Consider the function

$$w_+ : \mathcal{M} \to \mathbb{Z}_{\geq 0}$$

where

$$w_+(\phi) = 0$$

and for

$$\alpha = \{(a_1, m_\alpha(a_1)), (a_2, m_\alpha(a_2)), \dots, (a_r, m_\alpha(a_r))\}$$

the function value $w_+(\alpha)$ is

$$w_+(\alpha) = \sum_{i=1}^{r} m_\alpha(a_i) w(a_i)$$

It is interesting to ask if this sum itself can be expressed as a convolution of some two functions at α. Fortunately, the expression above itself motivates a candidate function

$$\Lambda : \mathcal{M} \to \mathbb{Z}_{\geq 0}$$

$$\Lambda(\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ has at least 2 distinct elements} \\ w(a) & \text{if } \alpha = \{(a, m)\} \end{cases}$$

In other words, Λ takes non-zero values only for multisets that contain only one distinct element, in which case Λ behaves as the weight function. The function $\Lambda : \mathcal{M} \to \mathbb{Z}_{\geq 0}$ is called the *Von Mangoldt* function. It is easy to see that

$$\sum_{\beta \leq \alpha} \Lambda(\beta) = w_+(\alpha)$$

What this means is that

$$\Lambda * \vec{1} = w_+$$

or equivalently,

$$\zeta(t) \left(\sum_{\alpha \in \mathcal{M}} \Lambda(\alpha) t^{w_+(\alpha)} \right) = \sum_{\beta \in \mathcal{M}} w_+(\beta) t^{w_+(\beta)}$$

Let

$$N_0, N_1, N_2, N_3 \ldots$$

be the sequence of non-negative integers such that

$$\sum_{\alpha \in \mathcal{M}} \Lambda(\alpha) t^{w_+(\alpha)} = N_0 + N_1 t + N_2 t^2 + \ldots$$

Note that

$$N_0 = 0$$

and for $k \geq 1$,

$$N_k = \sum_{w_+(\alpha) = k} \Lambda(\alpha)$$

So N_k is the number of multisets of weight exactly k that can be constructed using only one element. This means that the weight of that one element divides k, and it is straightforward that

$$N_k = \sum_{d|k} d \cdot B_d$$

The above results can be derived in another way simply using elementary manipulations of generating functions. Recall that

$$\zeta(t) = \prod_{k=1}^{\infty} \frac{1}{(1-t^k)^{B_k}}$$

Since the right hand side is a product, we can work with sums by taking a logarithm.

$$\log \zeta(t) = -\sum_{k=1}^{\infty} B_k \log (1-t^k)$$

Differentiating with respect to t on both sides,

$$\frac{\zeta(t)'}{\zeta(t)} = \sum_{k=1}^{\infty} B_k \frac{kt^{k-1}}{1-t^k}$$

Note that

$$t\frac{\zeta(t)'}{\zeta(t)} = \left(\sum_{\alpha \in \mathcal{M}} w_+(\alpha) t^{w_+(\alpha)} \right) \left(\sum_{\beta \in \mathcal{M}} \mu_{\mathcal{M}}(\beta) t^{w_+(\beta)} \right)$$

which is precisely the series

$$\sum_{\alpha \in \mathcal{M}} \Lambda(\alpha) t^{w_+(\alpha)} = N_1 t + N_2 t^2 + \dots$$

So N_k is simply the coefficient of t^k in the series

$$\sum_{k=1}^{\infty} B_k \frac{kt^k}{1-t^k} = \sum_{k=1}^{\infty} k.B_k(t^k + t^{2k} + t^{3k} + \dots)$$

which is clearly

$$N_k = \sum_{d|k} d.B_d$$

Note that while the zeta function and the Mobius function are simply functions on $\mathcal{M}$ to R independent of any weight function, the Von Mangoldt function explicitly depends on the precise structure (additive or multiplicative) of the weight function used.

We can now retrace the steps traversed above in the reverse direction to get an expression for $\zeta(t)$ in terms of the sequence $(N_k)_{k\geq 1}$.

$$\frac{\zeta(t)'}{\zeta(t)} = N_1 + N_2 t + N_3 t^2 + \dots$$

Integrating on both sides, we get

$$\log \zeta(t) = N_1 t + \frac{N_2}{2} t^2 + \frac{N_3}{3} t^3 + \dots$$

Thus,

$$\zeta(t) = exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} t^k\right)$$

The zeta function is thus expressible in terms of three sequences that each count multisets satisfying certain conditions:

- The sequence $(A_k)_{k\geq 0}$ that counts the number of multisets of a given weight. The zeta function
$$\zeta(t) = \sum_{k=0}^{\infty} A_k t^k$$
is, by definition, the ordinary generating function for $(A_k)_{k\geq 0}$.

- The sequence $(B_k)_{k\geq 0}$ that counts the number of elements of $\mathcal{P}$ of a given weight (or equivalently, the number of singleton multisets in $\mathcal{M}$ of a given weight). The zeta function is related to the sequence $(B_k)_{k\geq 0}$ through the Euler product
$$\zeta(t) = \prod_{k=1}^{\infty} \frac{1}{(1-t^k)^{B_k}}$$

- The Von Mangoldt sequence $(N_k)_{k\geq 0}$ that counts the number of multisets of a given weight comprising only one distinct element. The generating function for $(N_k)_{k\geq 0}$ is the logarithmic derivative of $\zeta(t)$, and so
$$\zeta(t) = exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} t^k\right)$$

1.3 Example: Counting Irreducible polynomials in $\mathbb{F}_p[X]$

Consider the problem of counting the number of irreducible polynomials of a given degree over a finite field. Let $p \in \mathbb{N}$ be a prime, and let $M_p(d)$ be the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[X]$.

Trivially any polynomial of degree 1 in $\mathbb{F}_p[X]$ is irreducible. Also such polynomials are exceptions in the sense that these are the only irreducible polynomials which actually have a root in $\mathbb{F}_p$.

Keeping this exception in mind, let us move on to degree 2. It is easy to count the number of monic irreducibles of degree 2. This is because the number of monic irreducibles of degree 2 plus the number of polynomials with both roots in $\mathbb{F}_p$ is the total number of polynomials (this is not the case when we deal with higher degree, as we shall see).

Lemma 4. *The number of monic irreducible polynomials in $\mathbb{F}_p[X]$ of degree 2, denoted $M_p(2)$ is exactly*

$$M_p(2) = p^2 - \left(\binom{p}{2} + p\right) = \frac{p^2 - p}{2}$$

So we have used an exclusion method of counting, as opposed to counting directly. This is reasonable since it is easier to count polynomials with roots in the field as this would simply involve picking the roots. While in the case of irreducibles, the counting is complicated because of the specific algebraic condition satisfied by the coefficients.

What about monic irreducibles of degree 3? Should they even exist? For instance, over $\mathbb{R}$, there are no monic irreducibles of degree 3, as any polynomial of degree 3 either has all three roots in $\mathbb{R}$ or it has one root in $\mathbb{R}$ and the other two being conjugates in the extension $\mathbb{C}$. These are the only possibilities when working over $\mathbb{R}$. And this is essentially because $\mathbb{R}$ does not contain all three cube roots of unity. So when working over $\mathbb{F}_p$ too, we should consider whether $\mathbb{F}_p$ contains cube roots of unity or not. Thus we have two cases. Suppose $\mathbb{F}_p$ does contain cube roots of unity. That is, $p \equiv 1 \pmod 3$. Then an example of a monic irreducible of degree 3 would be $X^3 - a$ where a is not a cube in $\mathbb{F}_p$. So in this case, there do exist irreducibles of degree 3. In the case of $p = 3$ or $p \equiv 2 \pmod 3$, where every element of $\mathbb{F}_p$ is a cube, are there irreducible polynomials of degree 3? In this case, its harder to give an immediate example of such an irreducible, if it exists. So lets try counting again.

The possibilities for a monic cubic polynomial $f \in \mathbb{F}_p[x]$ are:

- f has no roots in $\mathbb{F}_p$. That is, f is irreducible.
- f has precisely 1 root in $\mathbb{F}_p$. Hence f is a product of $X - a$ (for some $a \in \mathbb{F}_p$) and a monic irreducible of degree 2.
- f has all three roots in $\mathbb{F}_p$.

The case which is not possible is f having two roots in $\mathbb{F}_p$ and one root not in $\mathbb{F}_p$. So we have

$$p^3 = M_p(3) + pM_p(2) + \left(\binom{p}{3} + p(p-1) + p\right)$$

Since we know $M_p(2) = p(p-1)/2$, simplifying the above gives the following expression for the number of monic cubic irreducibles $M_p(3)$:

Theorem 5. *The number of monic irreducibles of degree* 3 *in* $\mathbb{F}_p[x]$ *is*

$$M_p(3) = \frac{p^3 - p}{3}$$

Thus, even for $p \equiv 2 \pmod 3$ there exist irreducibles of degree exactly 3, though we were unable to give obvious examples. And we obtained this purely by counting.
When we consider monic irreducibles of degree 4, now there are some difficulties in the counting we didn't face in the case of $d = 2$ or $d = 3$. The main problem is that f being irreducible is not equivalent to f having no roots in $\mathbb{F}_p$. The former implies the latter, but irreducibility is, in general, stronger than simply not having any root in $\mathbb{F}_p$. For example, the product of two irreducible polynomials both of degree greater than 1 is not irreducible, but does not have any root in $\mathbb{F}_p$.
So the possibilities for a monic polynomial $f \in \mathbb{F}_p[x]$ of degree 4 are:

- f is irreducible.
- f is a product of two monic irreducibles of degree 2.
- f has exactly one root in $\mathbb{F}_p$. In this case f is a product of $X - a$ (for some $a \in \mathbb{F}_p$) and a monic irreducible of degree 3.
- f has exactly two roots in $\mathbb{F}_p$. In this case f is a product of $(X - a)(X - b)$ (for some $a, b \in \mathbb{F}_p$) and a monic irreducible of degree 2.
- f has all four roots in $\mathbb{F}_p$.

By a messier counting of the above cases, we have

$$p^4 = M_p(4)+\left(\binom{M_p(2)}{2}+M_p(2)\right)+pM_p(3)+\left(\binom{p}{2}+p\right)M_p(2)+\left(\binom{p}{4}+p(p-1)+\binom{p}{2}+p\binom{p-1}{2}+p\right)$$

Simplifying, we get

$$M_p(4) = \frac{p^4 - p^2}{4}$$

Clearly the counting has gotten messy already, and we need some better way of doing this. But lets push this further and make it less obstruse. Observe that as part of establishing the above results, we were faced with the problem of counting the number of monic polynomials of a given degree d which had all its roots in $\mathbb{F}_p$. Combinatorially, this reduces to counting the possible combinations of d elements from $\mathbb{F}_p$. but allowing for repetitions (or in polynomial terminology, multiplicities). We achieved this by considering all the possible cases: all d elements are different, or some are the same and others are different from those and from each other, and so on. In other words, this is the well-studied problem of counting the number of *multisets* of size k from a set of size n.

Given a set A, a multiset can be represented as a set of pairs $\{(a, N_a) : a \in A \text{ and } N_a \in \mathbb{Z}_{\geq 0}\}$. Here N_a counts the number of times a occurs in the multiset, and is a non-negative integer. Note that restricting N_a to be 0 or 1 for every a gives us our conventional notion of sets.

The cardinality of a multiset $\{(a, N_a) : a \in A \text{ and } N_a \in \mathbb{Z}_{\geq 0}\}$ is just

$$\sum_{a \in A} N_a$$

When A is a finite set of size n, this sum is always meaningful (otherwise we would require N_a to be 0 everywhere for finitely many elements a, but we don't have to bother with these things here). So for simplicity of notation, let $A = \{1, 2, 3, \ldots, n\}$. So the problem of counting the number of multisets of size k of a set A of size n reduces to the number of solutions to the equation:

$$N_1 + N_2 + N_3 + \cdots + N_n = k$$

for non-negative integers N_i. But we know this value! It is simply the number of

permutations of k 1's and $n-1$ +'s. The exact value, denoted $\left(\binom{n}{k}\right)$ is

$$\left(\binom{n}{k}\right) = \binom{n+k-1}{k}$$

With this notation, the expressions for $M_p(1), M_p(2), M_p(3)$ and $M_p(4)$ can be rewritten as

$$p = M_p(1)$$

$$p^2 = M_p(2) + \left(\binom{p}{2}\right)$$

$$p^3 = M_p(3) + pM_p(2) + \left(\binom{p}{3}\right)$$

$$p^4 = M_p(4) + pM_p(3) + \left(\binom{M_p(2)}{2}\right) + \left(\binom{p}{2}\right) M_p(2) + \left(\binom{p}{4}\right)$$

Putting $p = M_p(1) = \left(\binom{M_p(1)}{1}\right)$ and more generally $M_p(i) = \left(\binom{M_p(i)}{1}\right)$ we can get expressions involving only the functions M_p and the multiset counter as:

$$p = \left(\binom{M_p(1)}{1}\right)$$

$$p^2 = \left(\binom{M_p(2)}{1}\right) + \left(\binom{M_p(1)}{2}\right)$$

$$p^3 = \left(\binom{M_p(3)}{1}\right) + \left(\binom{M_p(1)}{1}\right)\left(\binom{M_p(2)}{1}\right) + \left(\binom{M_p(1)}{3}\right)$$

$$p^4 = \left(\binom{M_p(4)}{1}\right)+\left(\binom{M_p(1)}{1}\right)\left(\binom{M_p(3)}{1}\right)+\left(\binom{M_p(2)}{2}\right)+\left(\binom{M_p(1)}{2}\right)\left(\binom{M_p(2)}{1}\right)+\left(\binom{M_p(1)}{4}\right)$$

Observe that each summand in the expression for p^4 corresponds to a *partition* of 4. There are 5 partitions of 4 as follows:

$$\begin{aligned} 4 &= 1+1+1+1 \\ &= 2+1+1 \\ &= 2+2 \\ &= 3+1 \\ &= 4 \end{aligned}$$

The partition $(1,1,1,1)$ corresponds to $\left(\binom{M_p(1)}{4}\right)$ or the number of monic polyno-

mials factored as 4 irreducibles of degree 1. The partition $(2,1,1)$ corresponds to $\left(\binom{M_p(1)}{2}\right)\left(\binom{M_p(2)}{1}\right)$ or the number of monic polynomials factored as product of an irreducible of degree 2 and two irreducibles of degree 1. irreducibles of degree 1. The partition $(2,2)$ corresponds to $\left(\binom{M_p(2)}{2}\right)$ or the number of monic polynomials factored as the product of 2 irreducibles of degree 2. The partition $(3,1)$ corresponds to $\left(\binom{M_p(1)}{1}\right)\left(\binom{M_p(3)}{1}\right)$ or the number of monic polynomials factored as product of an irreducible of degree 3 and an irreducible of degree 1. Finally the partition (4) corresponds to $\left(\binom{M_p(4)}{1}\right)$ or the number of monic polynomials which are irreducible and of degree 4. Now we see a pattern which can be generalized to give a recurrence for $M_p(d)$ for general d.

So lets now consider the general case: number of monic irreducibles of degree d in $\mathbb{F}_p[x]$. Then p^d is a sum over the partitions of d. Now determining the number of partitions of an integer is not a trivial problem, and there is no simple expression for it. However, that is not our concern here.

We need some standard notation for partitions. Let λ be a partition of d, denoted $\lambda \vdash d$. Then λ can be represented as $1^{\lambda_1}2^{\lambda_2}\dots d^{\lambda_d}$, where $\lambda_i \in \mathbb{Z}_{\geq 0}$ and $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + d\lambda_d = d$. That is λ is the partition comprising 1 repeated λ_1 times, 2 repeated λ_2 times and so on. This is sometimes called a frequency representation of the partition. Then, a general recurrence for $M_p(d)$ can be established the same way we did for $p = 4$ and smaller.

Theorem 6.

$$p^d = \sum_{\lambda\vdash d}\left(\binom{M_p(1)}{\lambda_1}\right)\left(\binom{M_p(2)}{\lambda_2}\right)\left(\binom{M_p(3)}{\lambda_3}\right)\cdots\left(\binom{M_p(d)}{\lambda_d}\right) = \sum_{\lambda\vdash d}\prod_{i=1}^{d}\left(\binom{M_p(i)}{\lambda_i}\right)$$

All these results we have derived so far have been established by explicit counting. We shall now see another useful way of obtaining combinatorial information: using generating functions. Consider monic polynomials built only using building blocks of size 1 (that is, monic irreducibles of degree 1). The generating function for the number of such monic polynomials is

$$(1 + t + t^2 + t^3 + \dots)^{M_p(1)}$$

Similarly the generating function for the monic polynomials constructed only using

irreducibles of degree d is

$$(1 + t^d + t^{2d} + t^{3d} + \dots)^{M_p(d)}$$

Now since any monic polynomial in $\mathbb{F}_p[X]$ can be uniquely expressed as a product of monic irreducibles, this implies that

$$\begin{aligned} 1 + pt + p^2t^2 + \dots &= (1 + t + t^2 + t^3 + \dots)^{M_p(1)}(1 + t^2 + t^4 + t^6 + \dots)^{M_p(2)}(1 + t^3 + t^6 + t^9 + \dots)^{M_p(3)} \dots \\ &= \prod_{d=1}^{\infty} \frac{1}{(1 - t^d)^{M_p(d)}} \end{aligned}$$

What we have used here is a product rule for generating functions. In fact, the above formulation of the generating function is simply a restatement of the ugly result we had derived earlier that

$$p^d = \sum_{\lambda \vdash d} \binom{M_p(1)}{\lambda_1} \binom{M_p(2)}{\lambda_2} \binom{M_p(3)}{\lambda_3} \cdots \binom{M_p(d)}{\lambda_d} = \sum_{\lambda \vdash d} \prod_{i=1}^{d} \binom{M_p(i)}{\lambda_i}$$

We have simply expressed this combinatorial result succinctly using generating functions. While the above expression was dismissed as not particularly useful, we shall see that the equivalent statement in terms of generating functions can be quite useful since we can now play around with the rational functions corresponding to these series. So far we have not used any non-trivial algebraic structure except the fact that monic polynomials in $\mathbb{F}_p[X]$ have a unique factorization in terms of irreducibles.

Theorem 7. *The generating function $\zeta(t)$ counting the number of monic polynomials in $\mathbb{F}_p[X]$ has an Euler product of the form*

$$\zeta(t) = \prod_{d=1}^{\infty} \frac{1}{(1 - t^d)^{M_p(d)}}$$

This function $\zeta(t)$ is called the zeta function of $\mathbb{F}_p[X]$. Observe the following features of the zeta function above:

- Let $Irr(p)$ denote the set of monic irreducible polynomials in $\mathbb{F}_p[X]$. The Euler product formulation of the zeta function can then be expressed as

$$\zeta(t) = \prod_{f \in Irr(p)} \frac{1}{1 - t^{deg(f)}}$$

- When multiplied out as an ordinary power series in t, the coefficient of t^k for $k \in \mathbb{Z}_{\geq 0}$ is the number of monic polynomials of degree k. This is because every monic polynomial of degree k corresponds uniquely to a product of powers of irreducible polynomials.

- Let us associate each monic polynomial in $\mathbb{F}_p[X]$ with the multiset of monic irreducible polynomials that occur in its unique factorization. Then the coefficient of t^k can be interpreted as the number of *multisets* of elements of $Irr(p)$ of total degree k.

1.4 The Riemann hypothesis

In our discussion so far, we started with a set $\mathcal{P}$ and a weight function $w : \mathcal{P} \to \mathbb{N}$ such that for every $k \in \mathbb{N}$, $w^{-1}(k)$ is finite, and of cardinality B_k. We then extended the weight function to multisets in $\mathcal{M}$ additively (or multiplicatively) and noted that the number of multisets of weight k is again finite, and its cardinality is denoted A_k. We then saw how to express A_k in terms of B_k using sums over partitions

$$A_k = \sum_{\lambda \vdash k} \prod_{i=1}^{k} \left(\binom{B_i}{\lambda_i} \right)$$

which is succinctly represented using the Euler product formulation of the corresponding generating function as

$$\zeta(t) = A_0 + A_1 t + A_2 t^2 + \cdots = \prod_{k=1}^{\infty} \frac{1}{(1-t^k)^{B_k}}$$

This approach made it seem as if we know $(B_k)_{k\geq 1}$ and would like to obtain $(A_k)_{k\geq 1}$. However, in many situations the zeta function is immediate, or at least easily obtained using extraneous techniques. So in such cases, we know $(A_k)_{k\geq 1}$ and we are interested in obtaining $(B_k)_{k\geq 1}$ in terms of $(A_k)_{k\geq 1}$.
So it is natural to ask if the Euler product formulation can yield some useful expression for $(B_k)_{k\geq 1}$ in terms of $(A_k)_{k\geq 1}$. That is, we would like an "inversion" of the formula

$$A_k = \sum_{\lambda \vdash k} \prod_{i=1}^{k} \left(\binom{B_i}{\lambda_i} \right)$$

We can try to use the Von Mangoldt sequence $(N_k)_{k\geq 1}$ as a bridge between $(A_k)_{k\geq 0}$ and $(B_k)_{k\geq 1}$ since intuitively, $(N_k)_{k\geq 1}$ is closely related to both sequences as seen from

$$\sum_{k=0}^{\infty} A_k t^k = exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} t^k\right)$$

and

$$N_k = \sum_{d|k} d.B_d$$

The latter equation immediately gives us an expression for B_k in terms of the Von Mangoldt sequence as

$$B_k = \frac{1}{k} \sum_{d|k} N_d \mu_{\mathbb{N}}(k/d)$$

where $\mu_{\mathbb{N}} : \mathbb{N} \to \{0, 1, -1\}$ is the number-theoretic Mobius function that indicates whether the given positive integer is square-free (if not, it takes the value 0), and if so then whether it has an even or odd number of prime factors. This Mobius function too fits into the framework of the more general multiset Mobius function that we have seen so far, by interpreting $\mathbb{N}$ as the collection of multisets over the set of primes. We shall see this in more detail when we study the Riemann zeta function.

So we have reduced the problem of determining $(B_k)_{k\geq 1}$ from $(A_k)_{k\geq 0}$ to the problem of determining $(N_k)_{k\geq 1}$ from $(A_k)_{k\geq 0}$. We know that

$$t\frac{\zeta(t)'}{\zeta(t)} = N_1 t + N_2 t^2 + N_3 t^3 + \dots$$

So what we want is an expression for the logarithmic derivative of $\zeta(t)$ as a power series in t. While it is easy to compute the derivative of $\zeta(t)'$ as

$$\zeta(t)' = A_1 + 2A_2 t + 3A_3 t^2 + \dots$$

we do not have any immediate expression for the reciprocal $1/\zeta(t)$ in terms of $(A_k)_{k\geq 0}$. However, our aim is not necessarily to "express" $(N_k)_{k\geq 1}$ in terms of $(A_k)_{k\geq 1}$, but simply to determine N_k explicitly using the zeta function $\zeta(t)$. This subtle difference in approach here is significant enough to make the problem much easier to tackle. After all, $\zeta(t)$ encodes the sequence $(A_k)_{k\geq 1}$ so indirectly we can go one step further and develop an expression for $(N_k)_{k\geq 1}$ in terms of $(A_k)_{k\geq 1}$ too if necessary.

Observe that the whole problem is because we do not have a workable expression for $1/\zeta(t)$ in terms of the coefficients of $\zeta(t)$ as a power series. But suppose (and this is a *big* assumption), for the moment, that the zeta function is a rational function in t. That is,

$$\zeta(t) = \frac{f(t)}{g(t)} \in \mathbb{C}(t)$$

for $0 \neq f(t), g(t) \in \mathbb{C}[t]$. Then it is easy to see that

$$\frac{\zeta(t)'}{\zeta(t)} = \frac{g(t)f'(t) - f(t)g'(t)}{f(t)g(t)} = \frac{f'(t)}{f(t)} - \frac{g'(t)}{g(t)}$$

First consider the polynomial $f(t) \in \mathbb{C}[t]$ and its logarithmic derivative $f'(t)/f(t)$ as a power series. While this is again hard to write down in terms of the coefficients of $f(t)$, we can work around this problem by expressing the coefficients of $f'(t)/f(t)$ in terms of the *roots* of $f(t)$ and well-studied symmetric polynomials in those roots!
First note that $f(t)$ (and $g(t)$ too) are non-zero at $t = 0$ since $\zeta(0) = f(0)/g(0) = A_0 = 1$. In particular, this means that $f(t)$ is a polynomial of the form

$$f(t) = c_f(1 - \alpha_1 t)(1 - \alpha_2 t)\dots(1 - \alpha_n t)$$

where $\alpha_1^{-1}, \alpha_2^{-1}, \dots, \alpha_n^{-1} \in \mathbb{C}$ are the n zeros of the complex polynomial $f(t) \in \mathbb{C}[t]$ and $0 \neq c_f \in \mathbb{C}$. Using the Leibnitz product rule on the above expression, we can express $f'(t)$ as

$$f'(t) = c_f \sum_{j=1}^{n} -\alpha_j \left(\prod_{l \neq j} 1 - \alpha_l t \right)$$

Now observe that

$$\begin{aligned}
t\frac{f'(t)}{f(t)} &= \frac{\sum_{j=1}^{n} -\alpha_j t \left(\prod_{l \neq j} 1 - \alpha_l t \right)}{(1 - \alpha_1 t)(1 - \alpha_2 t)\dots(1 - \alpha_n t)} \\
&= -\frac{\alpha_1 t}{1 - \alpha_1 t} - \frac{\alpha_2 t}{1 - \alpha_2 t} - \dots - \frac{\alpha_n t}{1 - \alpha_n t} \\
&= -(\alpha_1 t + \alpha_1^2 t^2 + \alpha_1^3 t^3 + \dots) - \dots - (\alpha_n t + \alpha_n^2 t^2 + \alpha_n^3 t^3 + \dots) \\
&= \left(-\sum_{j=1}^{n} \alpha_j \right) t + \left(-\sum_{j=1}^{n} \alpha_j^2 \right) t^2 + \left(-\sum_{j=1}^{n} \alpha_j^3 \right) t^3 + \dots \\
&= \sum_{k=1}^{\infty} -p_k(\alpha_1, \alpha_2, \dots, \alpha_n) t^k
\end{aligned}$$

where $p_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the k-th *power sum* of $\alpha_1, \alpha_2, \ldots, \alpha_n$, which is a symmetric function of $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Similarly, suppose

$$g(t) = c_g(1 - \beta_1 t)(1 - \beta_2 t)\ldots(1 - \beta_m)t$$

where $\beta_1, \beta_2, \ldots, \beta_m \in \mathbb{C}$ are the m zeros of $g(t) \in \mathbb{C}[t]$. Then

$$t\frac{g'(t)}{g(t)} = \sum_{k=1}^{\infty} -p_k(\beta_1, \beta_2, \ldots, \beta_m)t^k$$

Putting these together, we now have an expression for N_k in terms of the zeros and poles of the zeta function $\zeta(t)$ when $\zeta(t)$ is a rational function!

$$N_k = -p_k(\alpha_1, \alpha_2, \ldots, \alpha_n) + p_k(\beta_1, \beta_2, \ldots, \beta_m)$$

Theorem 8. *Suppose the zeta function $\zeta(t) = f(t)/g(t)$ where $f(t), g(t) \in \mathbb{C}[t]$ where*

$$f(t) = c_f(1 - \alpha_1 t)(1 - \alpha_2 t)\ldots(1 - \alpha_n t)$$

$$g(t) = c_g(1 - \beta_1 t)(1 - \beta_2 t)\ldots(1 - \beta_m)t$$

Then for every $k \in \mathbb{N}$,

$$N_k = (\beta_1^k + \beta_2^k + \cdots + \beta_m^k) - (\alpha_1^k - \alpha_2^k - \ldots \alpha_n^k)$$

Thus when the zeta function is a rational function, we can express N_k as the k-th power sum of the reciprocals of the poles of $\zeta(t)$ minus the k-th power sum of the reciprocals of the zeros of $\zeta(t)$. In fact, much of the utility of the sequence $(N_k)_{k\geq 1}$ arises from this fact that it is a power sum over the zeros and poles of the zeta function $\zeta(t)$, and is also related to the sequence $(B_k)_{k\geq 1}$ through

$$B_k = \frac{1}{k}\sum_{d|k} N_d \mu_{\mathbb{N}}(k/d)$$

This allows us to compute the number of elements of $\mathcal{P}$ of a given weight k in terms of the zeros and poles of the zeta function $\zeta(t)$.

In fact, this is precisely the motivation for the Riemann hypothesis in different contexts. In most cases, the zeta function would be forced to have certain "trivial" zeros (or

poles). The Riemann hypothesis, in a sense, is an upper bound on the absolute value of the remaining non-trivial zeros and poles with respect to the trivial zeros. This would ensure that N_k is well approximated by the sum of k-th power of the trivial zeros (or poles), which would dominate the other terms in the sum, thus allowing us to obtain a good approximation of B_d with vanishing error term. This intuition can be made precise in examples of the zeta function in different settings.

Chapter 2

Zeta Function of a Graph: Preliminaries

2.1 Non-backtracking cycles and the Ihara Zeta Function

For an integer $d \geq 2$, let $G = (V, E)$ be a finite d-regular undirected graph with adjacency matrix A. A *walk* on the graph G is a sequence $v_0 v_1 \dots v_k$ where $v_0, v_1, \dots, v_k$ are (not necessarily distinct) vertices in V, and for every $0 \leq i \leq k-1$, $(v_i, v_{i+1}) \in E$. The vertex v_0 is referred to as the *root* (or origin) of the above walk, v_k is the terminus of the walk, and the walk is said to have length k.

It is often useful to equivalently define a walk as a sequence of directed or oriented edges. Associate each edge $e = (v, w) \in E$ with two directed edges (or rays) denoted

$$\vec{e} = (v \to w) \text{ and } \vec{e}^{-1} = (w \to v)$$

The origin $org(\vec{e})$ is the vertex v and its terminus $ter(\vec{e})$ is the vertex w. Similarly, the origin $org(\vec{e}^{-1})$ is the vertex w and its terminus $ter(\vec{e})$ is the vertex v. Let $\vec{E}$ denote the set of $m = nd$ directed edges of G. So a walk of length k can equivalently be described as a sequence $\vec{e}_1 \vec{e}_2 \dots \vec{e}_k$ of k (not necessarily distinct) oriented edges in $\vec{E}$ such that for every $1 \leq i \leq k-1$, $ter(\vec{e}_i) = org(\vec{e}_{i+1})$. This is a walk that starts at $org(\vec{e}_1)$ and ends at $ter(\vec{e}_k)$.

It is easy to show that for any $k \in \mathbb{N}$, the number of walks of length k between vertices $u, v \in V$ is exactly $(A^k)_{u,v}$. In particular, the total number of closed walks of length k in G is exactly $Tr(A^k)$.

Definition 9. *A* non-backtracking walk *of length k from $v_0 \in V$ to $v_k \in V$ is a walk $v_0 v_1 \dots v_k$ such that for every $1 \leq i \leq k-1$, $v_{i-1} \neq v_{i+1}$. Equivalently, a non-backtracking walk of length k from $v \in V$ to $w \in V$ is a walk $\vec{e}_1 \vec{e}_2 \dots \vec{e}_k$ such that $org(\vec{e}_1) = v$, $ter(\vec{e}_k) = w$ and for every $1 \leq i \leq k-1$, $\vec{e}_{k+1} \neq \vec{e}_k^{-1}$.*

Definition 10. *A* non-backtracking cycle *of length k with root v is a non-backtracking closed walk $v, v_1, v_2, \dots, v_{k-1}, v$ with the additional boundary constraint that $v_1 \neq v_{k-1}$.*

Non-backtracking random walks (NBRW) on graphs have been studied in the context of mixing time [1], cut-offs [8], and exhibit more useful statistical properties than simple random walks (SRW).

Let $\mathcal{C}$ denote the set of all non-backtracking cycles in G, and for $C \in \mathcal{C}$, let $|C|$ denote the length of the cycle C. There are two elementary constructions we can carry out to generate more elements of $\mathcal{C}$ from a given cycle C:

- *Powering*: Given a non-backtracking cycle $C \in \mathcal{C}$ of length k of the form $C = \vec{e}_1 \vec{e}_2 \dots \vec{e}_k$ and $m \geq 1$, define the power

$$C^m = \underbrace{\vec{e}_1 \dots \vec{e}_k . \vec{e}_1 \dots \vec{e}_k \dots \vec{e}_1 \dots \vec{e}_k}_{\text{m times}}$$

  which is the concatenation of the string of edges corresponding to the walk C with itself m times. Note that C^m is also a non-backtracking cycle in G of length mk. Essentially, C^m represents the walk obtained by repeating or winding the walk C m times. Also note that C and C^m are both rooted at the same vertex. A cycle $P \in \mathcal{C}$ shall be called a *prime* cycle if there exists no element $C \in \mathcal{C}$ and $m \geq 2$ such that $P = C^m$. Essentially, a prime cycle in $\mathcal{C}$ is one that is not a repeated winding of a simpler cycle in $\mathcal{C}$. Note that every element of $\mathcal{C}$ is either a prime or a prime power.

- *Cycle Equivalence*: Given a non-backtracking cycle $C \in \mathcal{C}$ of length k of the form $C = \vec{e}_1 \vec{e}_2 \dots \vec{e}_k$, we can form another walk $C^{(2)} = \vec{e}_2 \vec{e}_3 \dots \vec{e}_k \vec{e}_1$ which is also a non-backtracking cycle in G of length k, but now rooted at the origin of the directed edge $\vec{e}_2$ (or the terminus of $\vec{e}_1$). More generally, for $1 \leq j \leq k$, define

$$C^{(j)} = \vec{e}_j \vec{e}_{j+1} \dots \vec{e}_k \vec{e}_1 \vec{e}_2 \dots \vec{e}_{j-1}$$

which is a cyclic permutation of the walk C obtained by choosing a different root. So given a cycle $C \in \mathcal{C}$ of length k, we get $k-1$ additional cycles in $\mathcal{C}$ of length k for free this way. In fact, this defines an equivalence class $\sim$ on $\mathcal{C}$, and the set $[C] = \{C^{(1)}, C^{(2)}, \ldots, C^{(k)}\}$ is called the equivalence class of C. An element $[C] \in \mathcal{C}/\sim$ represents a non-backtracking cycle modulo a choice of root.

We can now formally define the zeta function of the graph G. For simplicity, let us assume that G is connected and does not have any leaves (or vertices of degree 1).

Definition 11. *Let $\mathcal{P}$ denote the set of equivalence classes of prime non-backtracking cycles in G. The Euler product*

$$\prod_{[P]\in\mathcal{P}} \frac{1}{1-t^{|P|}}$$

is called the Ihara zeta function *of the graph G, denoted $\zeta_G(t)$.*

Let N_k denote the number of non-backtracking cycles in G of length k. Then observe that

$$\sum_{k=1}^{\infty} N_k \frac{t^k}{k} = \sum_{\text{prime } P} \frac{1}{|P|}\left(\sum_{m=1}^{\infty} \frac{t^{m|P|}}{m}\right) = -\sum_{[P]\in\mathcal{P}} \log\left(1-t^{|P|}\right)$$

Thus,

$$\zeta_G(t) = \prod_{[P]\in\mathcal{P}} \frac{1}{1-t^{|P|}} = exp\left(\sum_{k=1}^{\infty} N_k \frac{t^k}{k}\right)$$

Just like the number of cycles in G of length k is $Tr(A^k)$, we can describe the number N_k of non-backtracking cycles in G of length k as the trace of the matrix H^k where H is the *Hashimoto non-backtracking walk matrix* of G defined as follows: $H \in \mathbb{C}^{dn\times dn}$ with

$$H_{i,j} = \begin{cases} 1 & \text{if } \vec{e}_j \neq \vec{e}_i^{-1} \text{ and } ter(\vec{e}_i) = org(\vec{e}_j) \\ 0 & \text{otherwise} \end{cases}$$

In other words, the entry $H_{i,j}$ is an indicator for whether the oriented edge $\vec{e}_i$ feeds into the oriented edge $\vec{e}_j$ allowing us to form a non-backtracking walk $\vec{e}_i\vec{e}_j$ of length 2. Note that unlike A, the Hashimoto matrix H is *not* a symmetric matrix, and hence it need not have all real eigenvalues and an associated orthonormal eigenbasis. The interested reader is referred to [8] where the authors work out the precise eigendecomposition of the Hashimoto matrix H.

It is clear that for every $k \in \mathcal{N}$,

$$N_k = Tr(H^k)$$

and so by Jacobi's formula relating the trace of the logarithm of a matrix to the logarithm of its determinant, we get

$$\zeta_G(t) = exp\left(\sum_{k=1}^{\infty} Tr(H^k)\frac{t^k}{k}\right) = exp\left(-Tr\left(\log\left(I - tH\right)\right)\right)$$

Simplifying, we get

$$\zeta_G(t) = \frac{1}{det(I - Ht)}$$

In particular, this establishes the rationality of the Ihara zeta function of a regular graph, and further implies that the reciprocal $\zeta_G(t)^{-1}$ is a polynomial in t over $\mathbb{Z}$ of degree at most $m = nd$. However, it is not immediate what the spectrum of H is. This brings us to the result of Bass [2] who gives an elegant expression for the Ihara zeta function of a graph $G = (V, E)$ as follows:

Theorem 12 (Bass)**.** *For a finite connected graph $G = (V, E)$,*

$$\zeta_G(t) = \frac{1}{(1-t^2)^{|E|-|V|}det(I - tA + (D - I)t^2)}$$

where A is the adjacency matrix of G and D is the diagonal matrix of degrees of the vertices of G, or in other words, $D = diag(A\vec{1})$.

In particular, if G is a d-regular connected graph, then

$$\zeta_G(t) = \frac{1}{(1-t^2)^{|E|-|V|}det(I - tA + (d - 1)t^2)}$$

Bass's determinant formula for regular graphs can be interpreted as a way to determine the spectrum of the Hashimoto matrix H in terms of the spectrum of the adjacency matrix A.

We shall now briefly sketch a previous proof of Bass's determinant formula (from [6]) involving expressing both the matrix H and the adjacency matrix A in terms of two directed edge incidence matrices S and T and a backtracking matrix B defined as follows: For a directed edge $(u \to v)$ and a vertex $w \in V$, define

$$S_{w,(u\to v)} = \begin{cases} 1 & \text{if } u = w \\ 0 & \text{otherwise} \end{cases} \qquad T_{(u\to v),w} = \begin{cases} 1 & \text{if } v = w \\ 0 & \text{otherwise} \end{cases}$$

and the matrix B is a $dn \times dn$ backtracking indicator matrix defined as

$$B_{(u\to v),(w\to z)} = \begin{cases} 1 & \text{if } v = w \text{ and } u = z \\ 0 & \text{otherwise} \end{cases}$$

Note that S is an $n \times dn$ edge incidence matrix that indicates the origin or starting vertex of the directed edge, while T is a $dn \times n$ edge incidence matrix that indicates the terminating vertex of the directed edge. It is easy to see that

$$A = ST$$

$$H = TS - B$$

$$SBT = dI$$

Now that A and H are related through S, T and B, standard matrix manipulation would suffice to show that

$$det(I - Ht) = (1 - t^2)^{\frac{dn}{2} - n} det\left(I - At + (d-1)t^2\right)$$

In fact, this proof works even when the graph G is not regular. However, the linear-algebraic calculations, though simple, tend to mask the underlying combinatorial structure.

2.2 Ramanujan graphs and the Riemann Hypothesis

For a fixed $d \geq 3$, a family G_n of d-regular n-vertex connected graphs is said to be an *expander* family if the second largest eigenvalues of the corresponding adjacency matrices are uniformly bounded away from d. It is easy to show (using a simple application of the probabilistic method) that a random d-regular graph family is an expander family with high probability. The question as to how small the second largest eigenvalue can get is answered by the Alon-Bopanna bound [14]: For fixed $d \geq 3$, the second largest eigenvalue, in absolute value, is at least $2\sqrt{d-1} - o_n(1)$. The occurrence of the term $2\sqrt{d-1}$ in this setting is related to it being the spectral radius of (the adjacency operator of) the *universal cover* of a d-regular graph (which is the infinite d-regular tree).

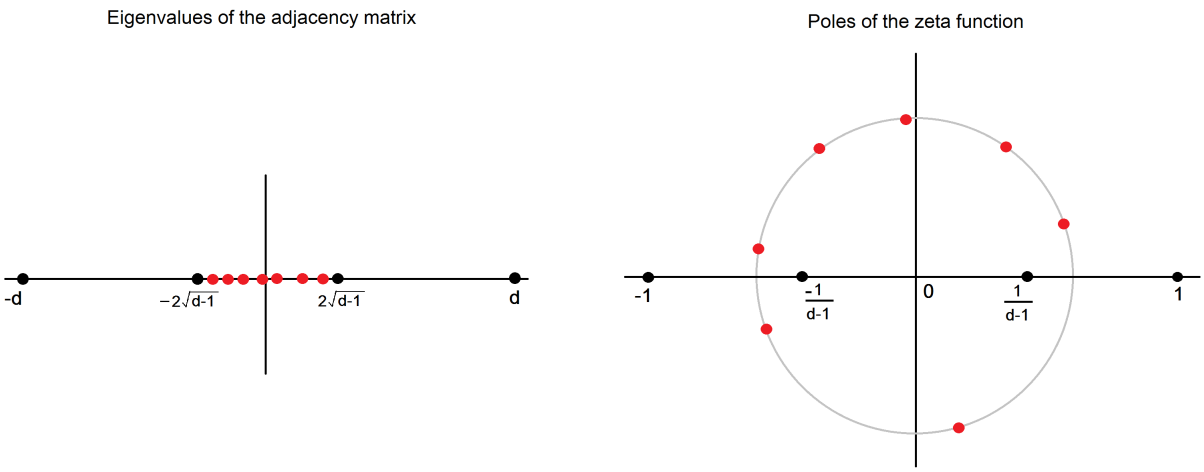
Definition 13. *For $d \geq 3$, a finite connected d-regular graph G is said to be* Ramanujan *if every eigenvalue $\lambda \in \mathbb{R}$ of the adjacency matrix A of G with $|\lambda| \neq d$ satisfies*

$$|\lambda| \leq 2\sqrt{d-1}$$

In other words, a family of Ramanujan graphs is the "optimal" expander family in light of the Alon-Bopanna lower bound. Ramanujan graphs were defined and explicitly constructed by Lubotzky, Phillips and Sarnak [9] for $d-1$ being a prime, and extended by Morgenstern [12] for $d-1$ being a prime power. Their constructions used deep results from modern number theory (in particular a conjecture of Ramanujan which was later settled by Deligne et al). However, the existence (leave alone explicit constructions) of Ramanujan graph families for general $d \geq 3$ remained open for a long time until Marcus, Spielman and Srivastava [11] used the method of interlacing polynomials to establish the existence of bipartite Ramanujan families for every $d \geq 3$. For a broad survey of Ramanujan graphs, expander families and their applications, the reader is referred to Murty's monograph [13] and the survey by Hoory, Linial and Wigderson [5]. The Ramanujan property of a graph is equivalent to a Riemann hypothesis condition of its Ihara zeta function. This can be seen by combining the eigenvalue conditions with Bass's determinant formula for the zeta function of $G$to show [13] that

Lemma 14 (Riemann Hypothesis for graphs)**.** *A d-regular graph G is Ramanujan iff every pole $\theta \in \mathbb{C}$ of $\zeta_G(t)$ such that $|\theta| \neq 1$ and $|\theta| \neq (d-1)^{-1}$ satisfies*

$$|\theta| = \frac{1}{\sqrt{d-1}}$$



2.3 Non-backtracking Walks and Chebyshev Polynomials

Just like $(A^k)_{v,w}$ counts the total number of walks on G from v to w (with backtrackings) of length k, we can construct a family

$$A_0, A_1, A_2, A_3, \ldots$$

of $n \times n$ matrices over $\mathbb{C}$ such that the value $(A_k)_{v,w}$ is the number of non-backtracking walks on G from v to w of length k. This family $\{A_k\}_{k\in\mathbb{N}}$ can be inductively defined using powers of A as follows:

- $A_0 = I$ and $A_1 = A$
- $A_2 = A^2 - dI$
- For $k \geq 3$,

$$A_k = A_{k-1}A - (d-1)A_{k-2}$$

The recurrence relation above can be used to easily show that the ordinary (matrix) generating function for the above sequence, with some mild abuse of notation, is

$$\sum_{k=0}^{\infty} t^k A_k = \frac{1-t^2}{I - At + (d-1)t^2}$$

The generating function above is closely related to the generating function of a well-studied family of orthogonal polynomials. Consider the family of Chebyshev polynomials $\{U_k\}_{k\geq 0}$ of the second kind, which are univariate complex polynomials defined by the recurrence

$$U_0(x) = 1 \text{ and } U_1(x) = 2x$$

and for $k \geq 2$,

$$U_k(x) = 2xU_{k-1}(x) - U_{k-2}(x)$$

and with generating function

$$\sum_{k=0}^{\infty} U_k(x)t^k = \frac{1}{1 - 2xt + t^2}$$

It can be shown [3] that for every $k \geq 2$,

$$\sum_{0 \leq j \leq k/2} A_{k-2j} = (d-1)^{k/2} U_k \left(\frac{A}{2\sqrt{d-1}} \right)$$

and so by taking trace on both sides we get

$$\sum_{0 \leq j \leq k/2} Tr(A_{k-2j}) = (d-1)^{k/2} \sum_{j=0}^{n-1} U_k \left(\frac{\lambda_j}{2\sqrt{d-1}} \right)$$

where

$$d = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1} \geq -d$$

are the n eigenvalues of the adjacency matrix A. Thus we have an expression for the trace of A_k as a polynomial in the eigenvalues of A. This approach is used in the seminal work of Lubotzky, Phillips and Sarnak in their construction of Ramanujan graphs [9], and for a more detailed exposition of Chebyshev polynomials and non-backtracking walks on regular graphs, the reader is referred to the monograph by Davidoff, Sarnak and Valette [3].

While $(A_k)_{v,w}$ counts the number of walks on G from vertex v to vertex w without backtracking, observe that the diagonal element $(A_k)_{v,v}$ does *not* count the number of non-backtracking cycles of length k rooted at v. This is because $(A_k)_{v,v}$ also counts walks of the form $\vec{e}_1 \vec{e}_2 \ldots \vec{e}_k$ where $\vec{e}_{i+1} \neq \vec{e}_i^{-1}$ for any $1 \leq i \leq k-1$ but $\vec{e}_k = \vec{e}_1^{-1}$. That is, $\vec{e}_1 \vec{e}_2 \ldots \vec{e}_k$ is non-backtracking as a walk from v to v, but when considered as a closed walk, the two end edges form a backtracking and is hence not a non-backtracking cycle! Such an instance of a backtracking that gets overlooked in $Tr(A_k)$ shall be referred to as a *tail*.

So $Tr(A_k)$ counts the number of closed walks of length k that could have at most 1 tail (and hence does *not* count the non-backtracking cycles of length k). Denote $Tr(A_k)$ by M_k. In the following section, we shall establish a simple but useful combinatorial lemma relating M_k with N_k.

Chapter 3

Proof Outline and Consequences

There exist several proofs [7] [15] of theorem 12, and most proofs start by expressing the zeta function in terms of not the adjacency matrix A of G, but the adjacency matrix H of the oriented line digraph of G (the Hashimoto non-backtracking walk matrix). After all, $\zeta_G(t)^{-1} = det(I - Ht)$, and so the problem reduces to expressing $det(I - Ht)$ in terms of the adjacency matrix A. We shall briefly sketch the standard proof in the next section once we have the preliminaries in place. There also exists another purely combinatorial proof by Foata and Zeilberger [4].

In this work, we shall see an alternate combinatorial proof of theorem 12 for the special case when G is d-regular. While the assumption of regularity is certainly a limitation, it allows for a more transparent proof. The basic idea is outlined as follows:

- We use the fact that the zeta function $\zeta_G(t)$ has an expansion of the form

$$\zeta_G(t) = exp\left(\sum_{k=1}^{\infty} N_k \frac{t^k}{k}\right)$$

  where for $k \in \mathbb{N}$, N_k is the number of non-backtracking cycles in G of length k. This is explored in section 2.

- While an expression for N_k is not immediate, a natural starting point is the study of non-backtracking walks on G. We can construct the family $\{A_k\}_{k \in \mathbb{Z}_{\geq 0}}$ of $n \times n$ matrices such that for every $k \in \mathbb{Z}_{\geq 0}$ and every $v, w \in V$, $(A_k)_{v,w}$ is the number of non-backtracking walks on G of length k from v to w. We shall discuss the construction of these non-backtracking walk matrices in section 3.

- While it might be tempting to claim that $N_k = Tr(A_k)$, unfortunately that is not the case! However, while they may not be equal, they are indeed precisely related. In section 4, we develop a combinatorial lemma to relate N_k and $Tr(A_k)$. This expression, while simple, could prove useful and is of independent interest.

- The combinatorial lemma greatly simplifies the problem since $Tr(A_k)$ is well-understood in terms of the eigenvalues of A and a family of orthogonal polynomials called the Chebyshev polynomials. We shall put these ingredients together in section 5 to arrive at Bass's determinant formula.

Essentially, the main contribution of this paper is a proof of following lemma:

Lemma 15. *Let G be a finite, connected d-regular graph on n vertices, and suppose $d = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1} \geq -d$ are the n real eigenvalues of its adjacency matrix A. Let N_k be the number of non-backtracking cycles of length k on G. Then*

$$N_k = \begin{cases} \sum_{j=0}^{n-1} 2(d-1)^{k/2} T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right) & \text{if } k \text{ is odd} \\ n(d-2) + \sum_{j=0}^{n-1} 2(d-1)^{k/2} T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right) & \text{if } k \text{ is even} \end{cases}$$

where T_k is the k-th Chebyshev polynomial of the first kind.

While the above expression is easy to derive given Bass's determinant formula for the zeta function, our proof proceeds in the other direction: by establishing this expression first and then using it to derive Bass's determinant formula using the generating function for Chebyshev polynomials of the first kind.

An interesting consequence of the above formula for N_k is an interpretation of the summand corresponding to the trivial eigenvalue d of G. Using a standard explicit formula for the polynomial T_k given by

$$T_k(x) = \begin{cases} \cos(k \arccos x) & \text{if } |x| \leq 1 \\ \frac{1}{2}(x - \sqrt{x^2-1})^k + \frac{1}{2}(x + \sqrt{x^2-1})^k & \text{if } |x| > 1 \end{cases}$$

we can compute $T_k(d/2\sqrt{d-1})$ to get

$$T_k\left(\frac{d}{2\sqrt{d-1}}\right) = (d-1)^k + 1$$

So if G is non-bipartite, we get

$$N_k = \begin{cases} (d-1)^k + 1 + \sum_{j=1}^{n-1} 2(d-1)^{k/2} T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right) & \text{if k is odd} \\ (d-1)^k + 1 + (d-2) + \sum_{j=1}^{n-1} \left((d-2) + 2(d-1)^{k/2} T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right)\right) & \text{if k is even} \end{cases}$$

In particular, when G is Ramanujan,

$$N_k = \begin{cases} (d-1)^k + 1 + O(nd^{k/2}) & \text{if k is odd} \\ (d-1)^k + 1 + (d-2) + O(nd^{k/2}) & \text{if k is even} \end{cases}$$

It is known that T_k is an odd function when k is odd, and an even function when k is even. So when G is bipartite,

$$N_k = \begin{cases} 0 & \text{if k is odd} \\ 2(d-1)^k + 2 + 2(d-2) + \sum_{j=1}^{n-2} \left((d-2) + 2(d-1)^{k/2} T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right)\right) & \text{if k is even} \end{cases}$$

and in particular when G is a bipartite Ramanujan graph,

$$N_k = \begin{cases} 0 & \text{if k is odd} \\ 2(d-1)^k + 2 + 2(d-2) + O(nd^{k/2}) & \text{if k is even} \end{cases}$$

It is interesting to ask what these dominant terms represent. It is known [10] that the number of *cyclically reduced words* of length k in a free group of rank m is exactly $(2m-1)^k + 1$ when k is odd, and $(2m-1)^k + 2m - 1$ when k is even. So if G were a Cayley graph of a group Γ and a symmetric generating set S (without involutive elements) of size d, then consider the walks on G corresponding to a choice of root and a cyclically reduced word over S of length k. The total number of such walks is $n\left((d-1)^k + 1\right)$ if k is odd, and $n\left((d-1)^k + 1 + (d-2)\right)$ if k is odd. If G is non-bipartite, we would expect a $1/n$ fraction of these walks to return to the root (that is, become non-backtracking cycles). If G is bipartite, then for even k, we would expect a $2/n$ fraction of these walks to be non-backtracking cycles (as there are now only $n/2$ candidates for the end vertex). These quantities are precisely the ones that appear as the dominant terms in the expressions for N_k.

So the Ramanujan property (or the graph Riemann hypothesis) implies that the number

N_k of non-backtracking cycles is close to the expected value, with optimally tight error term.

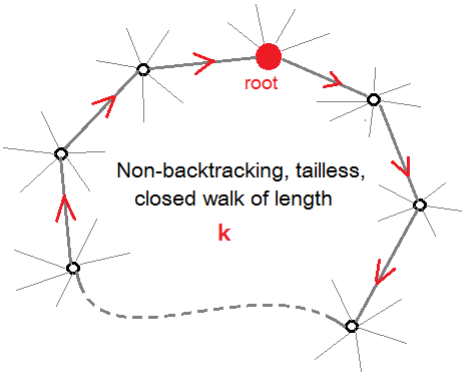
Chapter 4

Main Results

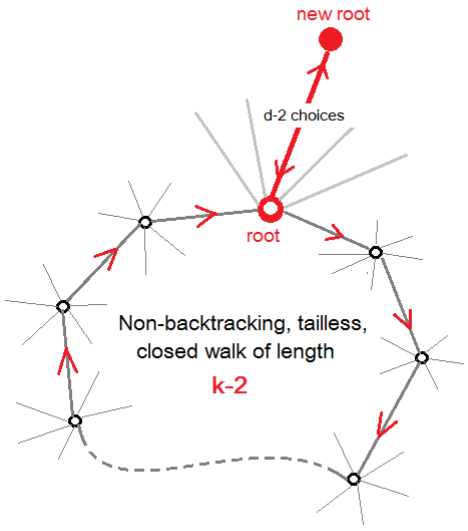
4.1 The Combinatorial Lemma

Recall that $N_k = Tr(H^k)$ counts the non-backtracking cycles of G. Firstly it is clear that $N_1 = N_2 = 0$. For $k \geq 3$, we can count the number M_k of *tailed* non-backtracking, closed walks of length k based on the length of the tail as illustrated below:

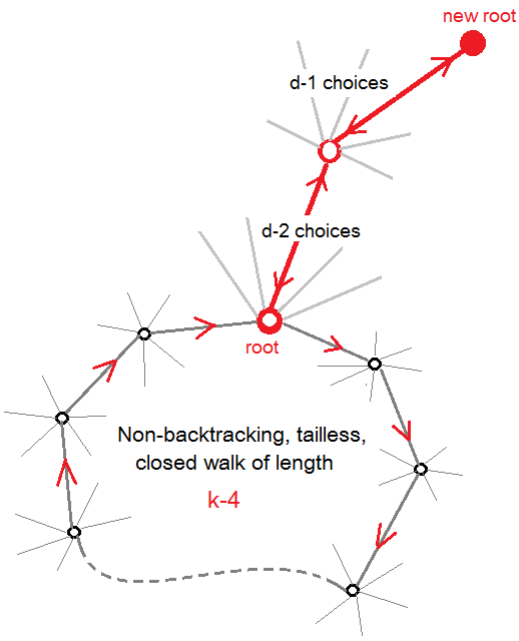
- A tailless, non-backtracking closed walk of length k, and there are N_k of them.



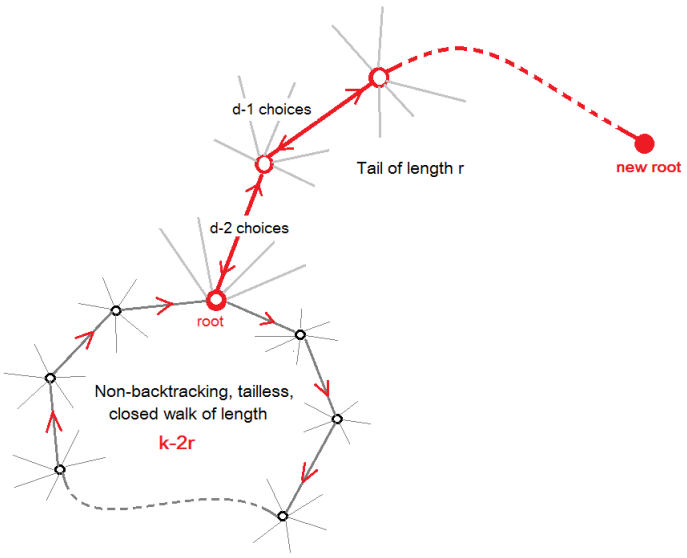
- A tailless, non-backtracking closed walks of length $k-2$ and a tail of length 1. Since there are $d-2$ choices for the tail (and consequently, the new root), the number of non-backtracking closed walks of length k with a tail of length 1 is $(d-2)N_{k-2}$.



- A tailless, non-backtracking closed walks of length $k-4$ and a tail of length 2. In this case the first vertex of the tail can be chosen in $d-2$ ways, and the next vertex (the new root) can be chosen in $d-1$ ways. So the number of non-backtracking closed walks of length k with a tail of length 2 is $(d-1)(d-2)N_{k-4}$.



More generally, for $2 \leq r \leq \lfloor k/2 \rfloor$, the number of non-backtracking closed walks of length k with a tail of length r is $(d-1)^{r-1}(d-2)N_{k-2r}$.



Thus for every $k \geq 3$,

$$M_k = N_k + (d-2)N_{k-2} + (d-2)(d-1)N_{k-4} + (d-2)(d-1)^2 N_{k-6} + \cdots + (d-2)(d-1)^{\lfloor \frac{k-1}{2} \rfloor - 1} N_{k-2\lfloor \frac{k-1}{2} \rfloor}$$

While this expression looks cumbersome, observe that

$$M_k - N_k = (d-2)\left(N_{k-2} + (d-1)N_{k-4} + \cdots + (d-1)^{\lfloor \frac{k-1}{2} \rfloor - 1} N_{k-2\lfloor \frac{k-1}{2} \rfloor}\right)$$

and a straightforward summation shows that

$$\sum_{j=1}^{\lfloor \frac{k-1}{2} \rfloor} M_{k-2j} = N_{k-2} + (d-1)N_{k-4} + \cdots + (d-1)^{\lfloor \frac{k-1}{2} \rfloor - 1} N_{k-2\lfloor \frac{k-1}{2} \rfloor}$$

Lemma 16. *For every $k \geq 3$,*

$$N_k = \begin{cases} M_k - (d-2)(M_{k-2} + M_{k-4} + \cdots + M_1) & \text{if } k \text{ is odd} \\ M_k - (d-2)(M_{k-2} + M_{k-4} + \cdots + M_2) & \text{if } k \text{ is even} \end{cases}$$

4.2 The Determinant Formula

From the combinatorial lemma established in the previous section, and the linearity of trace, we get

$$N_k = \begin{cases} Tr\left(A_k - (d-2)(A_{k-2} + A_{k-4} + \cdots + A_1)\right) & \text{if k is odd} \\ Tr\left(A_k - (d-2)(A_{k-2} + A_{k-4} + \cdots + A_2)\right) & \text{if k is even} \end{cases}$$

Recall that

$$\sum_{0 \le j \le k/2} A_{k-2j} = (d-1)^{k/2} U_k\left(\frac{A}{2\sqrt{d-1}}\right)$$

So for odd k

$$\begin{aligned} A_k - (d-2)(A_{k-2} + A_{k-4} + \cdots + A_1) &= (A_k + A_{k-2} + \cdots + A_1) - (d-1)(A_{k-2} + A_{k-4} + \cdots + A_1) \\ &= (d-1)^{k/2} U_k\left(\frac{A}{2\sqrt{d-1}}\right) - (d-1)^{k/2} U_{k-2}\left(\frac{A}{2\sqrt{d-1}}\right) \end{aligned}$$

Similarly, for even k,

$$\begin{aligned} A_k - (d-2)(A_{k-2} + \cdots + A_2) &= (A_k + A_{k-2} + \cdots + A_2) - (d-1)(A_{k-2} + A_{k-4} + \cdots + A_2) \\ &= (d-1)^{k/2} U_k\left(\frac{A}{2\sqrt{d-1}}\right) - (d-1)^{k/2} U_{k-2}\left(\frac{A}{2\sqrt{d-1}}\right) + (d-2)I \end{aligned}$$

As it so happens,

$$U_k(x) - U_{k-2}(x) = 2T_k(x)$$

where $T_k(x)$ is called the *Chebyshev polynomial of the first kind* of order k. The Chebyshev polynomials of the first kind are defined in a way very similar to the Chebyshev polynomials of the second kind:

$$T_0(x) = 1$$

$$T_1(x) = x$$

and for $k \ge 2$,

$$T_k(x) = 2xT_{k-1}(x) - T_{k-2}(x)$$

It is easy to show that $T_k(x)$ has a generating function

$$\sum_{k=0}^{\infty} T_k(x)t^k = \frac{1-xt}{1-2xt+t^2}$$

It is convenient to express N_k in terms of Chebyshev polynomials of the first kind as follows:

$$N_k = \begin{cases} Tr\left(2(d-1)^{k/2}T_k\left(\frac{A}{2\sqrt{d-1}}\right)\right) & \text{if k is odd} \\ Tr\left(2(d-1)^{k/2}T_k\left(\frac{A}{2\sqrt{d-1}}\right) + (d-2)I\right) & \text{if k is even} \end{cases}$$

This simplifies to

$$N_k = \begin{cases} \sum_{j=0}^{n-1} 2(d-1)^{k/2}T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right) & \text{if k is odd} \\ n(d-2) + \sum_{j=0}^{n-1} 2(d-1)^{k/2}T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right) & \text{if k is even} \end{cases}$$

The generating function for N_k is given by

$$\begin{aligned} \sum_{k=1}^{\infty} N_k t^k &= n(d-2)(t^2+t^4+t^6+\dots) + \sum_{k=1}^{\infty} t^k \left(\sum_{j=0}^{n-1} 2(d-1)^{k/2}T_k\left(\frac{\lambda_j}{2\sqrt{d-1}}\right)\right) \\ &= n(d-2)(t^2+t^4+t^6+\dots) + \sum_{j=0}^{n-1}\left(\frac{2-\lambda_j t}{1-\lambda_j t+(d-1)t^2} - 2\right) \\ &= n(d-2)\frac{t^2}{1-t^2} + \sum_{j=0}^{n-1}\frac{\lambda_j t - 2(d-1)t^2}{1-\lambda_j t+(d-1)t^2} \end{aligned}$$

Thus,

$$N_1 + N_2 t + N_3 t^2 + \cdots = n(d-2)\frac{t}{1-t^2} + \sum_{j=0}^{n-1}\frac{\lambda_j - 2(d-1)t}{1-\lambda_j t+(d-1)t^2}$$

While this expression does not seem very elegant stated this way, observe that the derivative of $1-t^2$ is $-2t$, and the derivative of $1-\lambda_j t+(d-1)t^2$ is $-\lambda_j + 2(d-1)t$. Rewriting the above expression to highlight this observation,

$$N_1 + N_2 t + N_3 t^2 + \cdots = -\frac{n(d-2)}{2}\frac{-2t}{1-t^2} - \sum_{j=0}^{n-1}\frac{-\lambda_j + 2(d-1)t}{1-\lambda_j t+(d-1)t^2}$$

This suggests that we could integrate both sides to obtain

$$\begin{aligned} N_1 t + N_2 \frac{t^2}{2} + N_3 \frac{t^3}{3} + \ldots &= -\frac{n(d-2)}{2} \log(1-t^2) - \sum_{j=0}^{n-1} \log(1 - \lambda_j t + (d-1)t^2) \\ &= -\left(\frac{nd}{2} - n\right) \log(1-t^2) - \log\left(\prod_{j=0}^{n-1} 1 - \lambda_j t + (d-1)t^2\right) \\ &= -(|E| - |V|) \log(1-t^2) - \log\left(det(I - At + (d-1)t^2)\right) \end{aligned}$$

Now since we know that the Ihara zeta function $\zeta_G(t)$ has the expression

$$\zeta_G = exp\left(N_1 t + N_2 \frac{t^2}{2} + N_3 \frac{t^3}{3} + \ldots\right)$$

we now have the familiar determinant formula for the zeta function in terms of the adjacency matrix:

Theorem 17 (Bass's determinant formula)**.** *Let $d \geq 3$ and $G = (V, E)$ be a d-regular connected graph with adjacency matrix A. Then*

$$\zeta_G(t) = \frac{(1-t^2)^{|V|-|E|}}{det(I - At + (d-1)t^2)}$$

Chapter 5

Related Work and Future Directions

While there have been several algebraic proofs of the Bass determinant formula, the work of [8] goes further by explicitly obtaining not only the eigenvalues of the Hashimoto matrix, but also its eigendecomposition and eigenvectors. For the sake of completeness (and the intrinsic interest of this result), we shall now state their result without proof.

Theorem 18 ([8])**.** *Consider a finite undirected d-regular graph $G = (V, E)$ on n vertices, whose adjacency matrix A has eigenvalues $d = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1} \geq -d$. Let H be the Hashimoto edge-adjacency operator of G. Then*

- *The matrix H is unitarily similar to the block diagonal matrix*

$$\Lambda = diag\left(d-1, \begin{pmatrix} \theta_1 & \alpha_1 \\ 0 & \overline{\theta_1} \end{pmatrix}, \begin{pmatrix} \theta_2 & \alpha_2 \\ 0 & \overline{\theta_2} \end{pmatrix}, \ldots, \begin{pmatrix} \theta_{n-1} & \alpha_{n-1} \\ 0 & \overline{\theta_{n-1}} \end{pmatrix}, \underbrace{-1, -1, \ldots, -1}_{nd/2-n}, \underbrace{1, 1, \ldots, 1}_{nd/2-n}\right)$$

  where for every $i \in [1, n-1]$, $|\alpha_i| < 2\sqrt{d-1}$ and $\theta_i, \overline{\theta_i} \in \mathbb{C}$ are the two complex roots of the polynomial equation

$$x^2 - \lambda_i x + d - 1 = 0$$

- *In particular, this implies that for every eigenvalue λ_i of A we have two complex conjugate eigenvalues θ_i and $\overline{\theta_i}$ of the Hashimoto matrix H which are roots of the quadratic equation $x^2 - \lambda_i x + d - 1 = 0$.*

- *For each $i \in [1, n-1]$, the precise value of $|\alpha_i|$ is given by*

$$|\alpha_i| = \begin{cases} d-2 & \text{if } |\lambda_i| \leq 2\sqrt{d-1} \\ \sqrt{d^2 - \lambda_i^2} & \text{if } |\lambda_i| > 2\sqrt{d-1} \end{cases}$$

- *For every $\theta \in \mathbb{C}$, define the map $T_\theta : \ell^2(V) \to \ell^2(\vec{E})$ by*

$$T_\theta f(v \to w) = \theta f(w) - f(v)$$

Let $f_i \in \ell^2(V)$ be the eigenfunction of A corresponding to the eigenvalue λ_i. Then the eigenfunction corresponding to the eigenvalue θ_i of H is precisely $T_{\theta_i} f_i$.

While their proof is linear-algebraic, it is interesting to ask if we can provide an alternate combinatorial interpretation of the result, particularly the eigenfunctions of H, in terms of the cycle structure of G.

Another problem is to generalize our combinatorial proofs to the case of irregular graphs. This has been done in [4], but it is reasonable to hope for a simpler construction. One can also ask the same question of directed graphs, in which case the situation gets way more complicated due to non-commutativity.

Bibliography

[1] Noga Alon, Itai Benjamini, Eyal Lubetzky, and Sasha Sodin. Non-backtracking random walks mix faster. *Communications in Contemporary Mathematics*, 9(04):585–603, 2007. 2.1

[2] Hyman Bass. The ihara-selberg zeta function of a tree lattice. *International Journal of Mathematics*, 3(06):717–797, 1992. 2.1

[3] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary number theory, group theory and Ramanujan graphs*, volume 55. Cambridge University Press, 2003. 2.3

[4] Dominique Foata and Doron Zeilberger. A combinatorial proof of basss evaluations of the ihara-selberg zeta function for graphs. *Transactions of the American Mathematical Society*, 351(6):2257–2274, 1999. 3, 5

[5] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006. 2.2

[6] Mark Kempton. Non-backtracking random walks and a weighted ihara's theorem. *arXiv preprint arXiv:1603.05553*, 2016. 2.1

[7] Motoko Kotani and Toshikazu Sunada. Zeta functions of finite graphs. *J. Math. Sci. Univ. Tokyo*, 7:7–25, 2000. 3

[8] Eyal Lubetzky and Yuval Peres. Cutoff on all ramanujan graphs. *Geometric and Functional Analysis*, 26(4):1190–1216, 2016. 2.1, 2.1, 5, 18

[9] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988. 2.2, 2.3

[10] Avinoam Mann. *How groups grow*, volume 395. Cambridge university press, 2011. 3

[11] Adam Marcus, Daniel A Spielman, and Nikhil Srivastava. Interlacing families i: Bipartite ramanujan graphs of all degrees. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 529–537. IEEE, 2013. 2.2

[12] Moshe Morgenstern. Existence and explicit constructions of q+ 1 regular ramanujan graphs for every prime power q. *Journal of Combinatorial Theory, Series B*, 62(1):44–62, 1994. 2.2

[13] M Ram Murty. Ramanujan graphs. *Journal-Ramanujan Mathematical Society*, 18(1):33–52, 2003. 2.2

[14] Alon Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991. 2.2

[15] Harold M Stark and Audrey A Terras. Zeta functions of finite graphs and coverings. *Advances in Mathematics*, 121(1):124–165, 1996. 3