Categorifying Zeta Functions of Hyperelliptic Curves

Jon Aycock and Andrew Kobin[1]

September 1, 2023

Abstract

The zeta function of a hyperelliptic curve C over a finite field factors into a product of L-functions, one of which is the L-function of C. We categorify this formula using objective linear algebra in the abstract incidence algebra of the poset of effective 0-cycles of C. As an application, we prove a collection of combinatorial formulas relating the number of ramified, split and inert points on C to the overall point count of C.

1 Introduction

Let $\mathbb{F}_q$ be a finite field and let C be an algebraic curve over $\mathbb{F}_q$. Its zeta function is defined as the formal power series

$$Z(C,t) = \exp\left[\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right]$$

where $\#C(\mathbb{F}_{q^n})$ denotes the number of $\mathbb{F}_{q^n}$-points of C and $\exp(t) = 1 + \sum_{n=1}^{\infty} \frac{1}{n!} t^n$ is the formal exponential power series. For example, the zeta function of $\mathbb{A}^1$ is

$$Z(\mathbb{A}^1, t) = \frac{1}{1-qt}$$

while the zeta function of $\mathbb{P}^1$ is

$$Z(\mathbb{P}^1, t) = \frac{1}{(1-t)(1-qt)}.$$

By the Weil Conjectures, $Z(C,t)$ is a rational function, satisfies a functional equation and its zeroes and poles satisfy an analogue of the Riemann Hypothesis.

Expanding further on the rationality property, it is well-known, though not at all obvious, that when C is smooth, projective and geometrically integral of genus g, its zeta function can be written

$$Z(C,t) = \frac{L(C,t)}{(1-t)(1-qt)} \tag{1}$$

where $L(C,t)$ is the L-function of C, a degree $2g$ polynomial with integer coefficients. In other words, $Z(C,t)$ factors in the ring of formal power series as $Z(\mathbb{P}^1,t)L(C,t)$. When C is a hyperelliptic curve, we lift formula (1) to an equivalence of linear functors in the abstract incidence algebra of the decomposition set of 0-cycles of $\mathbb{P}^1$, using techniques in objective linear algebra:

Theorem 1.1 (Theorem 4.2)**.** *Let $C/\mathbb{F}_q$ be a hyperelliptic curve. In the reduced incidence algebra $\widetilde{I}(Z_0^{\mathrm{eff}}(\mathbb{P}^1))$, there is an equivalence of linear functors*

$$\pi_*\zeta_C + \zeta_{\mathbb{P}^1} * L(C)^- \cong \zeta_{\mathbb{P}^1} * L(C)^+.$$

[1]The second author is partially supported by the American Mathematical Society and the Simons Foundation.

The symbol π_* is a pushforward map induced by the double cover $\pi : C \to \mathbb{P}^1$. The functors $L(C)^+$ and $L(C)^-$ in $\widetilde{I}(Z_0^{\text{eff}}(C))$ are defined in Section 4 in such a way that their images in the numerical incidence algebra satisfy $L(C)^+ - L(C)^- = L(C)$, where $L(C)$ represents the coefficients of $L(C,t)$, thereby recovering formula (1). In this way, Theorem 1.1 may be viewed as a categorical version of formula (1) for hyperelliptic curves. Theorem 1.1 also says that $L(C)$ is a *relative zeta function* for the cover π, in the terminology of [AK]. Or to be more precise, it is a "decomposed" relative zeta function and becomes a relative zeta function after passing to $I_\#(\mathbb{P}^1)$; see Remark 4.4. We plan to construct $L(C)$ directly as a single relative zeta function in a future article, using simplicial G-representations. See Appendix A.4 for an overview of the construction in the case that C is an elliptic curve.

When E is an elliptic curve (considered to be hyperelliptic in this paper), the L-function of E is of the form $L(E,t) = 1 - a_q t + qt^2$ where $a_q = q + 1 - \#E(\mathbb{F}_q)$. Using Theorem 1.1, we deduce the formulas

$$a_q = i_q(E) - s_q(E) \quad \text{and} \quad \#\operatorname{Sym}^n C(\mathbb{F}_q) = \sum_{i+j=n} (q^i + \ldots + q + 1) \sum_{\alpha \in \operatorname{Sym}^j \mathbb{P}^1(\mathbb{F}_q)} \chi(\alpha) \tag{2}$$

where $s_q(E)$ and $i_q(E)$ are the number of "split" and "inert" points of the cover $E \to \mathbb{P}^1$ over $\mathbb{F}_q$ and χ is a certain function on the points of $\operatorname{Sym}^j \mathbb{P}^1$, which can be identified with the effective 0-cycles of degree j on $\mathbb{P}^1$.

The point counting zeta function is only one generating function that encodes information about a curve $C/\mathbb{F}_q$. If C lifts to a curve $\widetilde{C}$ in characteristic 0, then the complex points of $\widetilde{C}$ have the structure of a Riemann surface whose Euler characteristic can be encoded by the Macdonald polynomial $(1-t)^{-\chi(\widetilde{C})}$. In fact, many formulas for χ can be encoded with Macdonald polynomials; for example, when $\pi : Y \to X$ is a branched cover of degree n,

$$\chi(Y) = n\chi(X) - r$$

where $r = r(\pi)$ is the ramification number of π. As an analogue of Theorem 1.1, we lift this formula to an equivalence of linear functors in an objective incidence algebra:

Theorem 1.2 (Theorem 5.3)**.** *Let $\pi : Y \to X$ be a branched cover of degree n of finite CW complexes. In the incidence algebra $I(S_\bullet(X))$ of the simplicial complex $S_\bullet(X)$, there is an equivalence of linear functors*

$$\pi_*\Phi_{even}(Y) * \Phi_{odd}(X)^n * \pi_* R \cong \pi_*\Phi_{odd}(Y) * \Phi_{even}^n.$$

The paper is organized as follows. In Section 2, we review the basic properties of algebraic curves over finite fields and their zeta and L-functions. In Section 3, we review the definitions of decomposition sets and their incidence algebras, following [GKT1] and [AK]. The proof of Theorem 1.1 is given in Section 4. In Section 4.3 we prove formula (2) relating the numbers of split and inert points of E to $a_q(E)$. Finally, we prove the topological analogue, Theorem 1.2, in Section 5.

The authors would like to thank Changho Han for many helpful discussions at the early stages of this project. The second author also thanks David Zureick-Brown for several conversations about covers of curves and Bogdan Krstic for his help with the details of objective characteristic polynomials.

2 Hyperelliptic Curves

For a smooth, projective, geometrically integral variety X over $k = \mathbb{F}_q$, let $|X|$ denote the set of closed points of X. Then the zeta function of X has the following product formula:

$$Z(X,t) = \prod_{x \in |X|} \frac{1}{1 - t^{\deg(x)}}$$

where $\deg(x) = [k(x) : k]$ is the degree of x. We denote by $Z_0(X)$ the group of 0-cycles on X, i.e. the free abelian group generated by $|X|$. A 0-cycle is *effective* if it is of the form $\alpha = \sum_{x \in |X|} a_x x$ for $a_x \geq 0$. The effective 0-cycles on X form a submonoid of $Z_0(X)$, denoted $Z_0^{\text{eff}}(X)$. The zeta function of X can also be written as a generating function for the effective 0-cycles on X:

$$Z(X,t) = \sum_{\alpha \in Z_0^{\text{eff}}(X)} t^{\deg(\alpha)}$$

where $\deg : Z_0(X) \to \mathbb{Z}$ is the degree map sending $\alpha = \sum_x a_x x$ to $\deg(\alpha) = \sum_x a_x \deg(x)$.

Let C be a hyperelliptic curve of genus $g \geq 1$, i.e. a smooth, projective algebraic curve given by an equation of the form

$$C : y^2 + h(x)y = f(x)$$

for $f, h \in k[x]$ with f monic, $\deg(f) = 2g+1$ and $\deg(h) \leq g$. (If $\operatorname{char} k \neq 2$, we can take $h = 0$.) Restricting the projection $\mathbb{P}^2 \to \mathbb{P}^1$ to C determines a smooth map $\pi : C \to \mathbb{P}^1$ which is a degree 2 cover ramified at $2g+2$ points.

Remark 2.1. Although it is not standard everywhere, in this paper we include elliptic curves in the class of hyperelliptic curves.

Fix a point $x \in |\mathbb{P}^1|$ and a point $y \in \pi^{-1}(x)$ on C. Let $e(y \mid x)$ denote the ramification index of π at y and let $f(y \mid x)$ denote the inertia degree, defined as $[k(y) : k(x)]$ where $k(x)$ (resp. $k(y)$) is the field of definition of x (resp. y). Then x has one of the following splitting types:

- **ramified** if $e(y \mid x) > 1$ for any $y \in \pi^{-1}(x)$;
- **split** if $e(y \mid x) = f(y \mid x) = 1$ for all $y \in \pi^{-1}(x)$;
- **inert** if $\pi^{-1}(x)$ consists of a single closed point y and $e(y \mid x) = 1$.

In this situation, the Riemann–Hurwitz formula reads

$$2 - 2g = 4 - \sum_{y \in |C|} (e(y \mid x) - 1).$$

Compare this to the formulas in Section 5.

Proposition 2.2. *Let $\pi : C \to \mathbb{P}^1$ be a hyperelliptic curve over $\mathbb{F}_q$. Then $Z(C,t)$ factors as*

$$Z(C,t) = \prod_{x \in |\mathbb{P}^1|} Z_x(C,t)$$

where

$$Z_x(C,t) = \begin{cases} \dfrac{1}{1 - t^{\deg(x)}}, & \text{if } x \text{ is ramified} \\ \dfrac{1}{(1 - t^{\deg(x)})^2}, & \text{if } x \text{ is split} \\ \dfrac{1}{1 - t^{2\deg(x)}}, & \text{if } x \text{ is inert.} \end{cases}$$

Proof. The factorization of $Z(C,t)$ as a product over the closed points of C is well known:

$$Z(C,t) = \prod_{y \in |C|} \frac{1}{1 - t^{\deg(y)}}.$$

For each $x \in |\mathbb{P}^1|$, write

$$Z_x(C,t) = \prod_{y \in \pi^{-1}(x)} \frac{1}{1 - t^{\deg(y)}}.$$

Then the description of $Z_x(C,t)$ follows from the definitions of ramified, split and inert points. This will also follow from the objective description of $Z(C,t)$ as the pushforward $\pi_* \zeta_C$ (see Section 4.3). $\square$

When $\pi : C \to \mathbb{P}^1$ is a hyperelliptic curve and $x \in |\mathbb{P}^1|$ is a split point, we label the two points in $\pi^{-1}(x)$ by $\{y, \bar{y}\}$. The formulas proven in Section 4 will not depend on this labeling, although their proofs will. As we will mention later, this choice can be viewed as a section of π over the split locus.

3 Incidence Algebras and Objective Linear Algebra

In this section, we define an incidence algebra of 0-cycles on a variety and give a brief overview of decomposition sets, objective linear algebra and incidence algebras, following [GKT1, Kob, AK].

3.1 The Incidence Algebra of 0-Cycles

Our goal is to construct the incidence algebra of effective 0-cycles for a curve $C/\mathbb{F}_q$. In fact, the construction is valid for any variety X over any field. Let $Z_0^{\mathrm{eff}}(X)$ be the set of effective 0-cycles on X. This has the structure of a locally finite poset where $\alpha \leq \beta$ if and only if $\alpha = \sum_x a_x x$, $\beta = \sum_x b_x x$ and $a_x \leq b_x$ for all $x \in |X|$. For $\alpha, \beta \in Z_0^{\mathrm{eff}}(X)$, the interval $[\alpha, \beta]$ is defined as

$$[\alpha, \beta] = \{\gamma \in Z_0^{\mathrm{eff}}(X) \mid \alpha \leq \gamma \leq \beta\}.$$

Fix a field of coefficients k (usually $k = \mathbb{C}$ or $\mathbb{Q}_\ell$ for $\ell \nmid q$). The *incidence coalgebra of* 0*-cycles* of X, hereafter the incidence coalgebra of X, is the free k-vector space on the set of intervals in $Z_0^{\mathrm{eff}}(X)$:

$$C(X) := C(Z_0^{\mathrm{eff}}(X)) = \bigoplus_{I \in \mathrm{Int}(Z_0^{\mathrm{eff}}(X))} kI$$

with comultiplication and counit

$$\Delta : C(X) \longrightarrow C(X) \otimes_k C(X), \quad [\alpha, \beta] \longmapsto \sum_{\gamma \in [\alpha, \beta]} [\alpha, \gamma] \otimes [\gamma, \beta]$$

$$\text{and} \quad \delta : C(X) \longrightarrow k, \quad [\alpha, \beta] \longmapsto \delta_{\alpha\beta} = \begin{cases} 1, & \alpha = \beta \\ 0, & \alpha \neq \beta. \end{cases}$$

The *incidence algebra of* 0*-cycles* of X, hereafter the incidence algebra of X, is the dual of $C(X)$,

$$I(X) := I(Z_0^{\mathrm{eff}}(X)) = \mathrm{Hom}_k(C(X), k),$$

which is an algebra under convolution,

$$* : I(X) \otimes_k I(X) \longrightarrow I(X), \quad f \otimes g \longmapsto \left(f * g : [\alpha, \beta] \mapsto \sum_{\gamma \in [\alpha, \beta]} f(\alpha, \gamma) g(\gamma, \beta) \right)$$

with unit δ. Here, $f(\alpha, \beta) := f([\alpha, \beta])$.

The *zeta function* of $Z_0^{\mathrm{eff}}(X)$ is the element $\zeta \in I(X)$ defined by $\zeta(\alpha, \beta) = 1$ for every $\alpha \leq \beta$. The zeta function ζ lives in a subalgebra of $I(X)$ called the *reduced incidence algebra* $\widetilde{I}(X) := \widetilde{I}(Z_0^{\mathrm{eff}}(X))$, defined as the subalgebra of functions f that are constant on isomorphism classes of intervals in $Z_0^{\mathrm{eff}}(X)$. Here, two intervals $[\alpha, \beta], [\alpha', \beta'] \in \mathrm{Int}(Z_0^{\mathrm{eff}}(X))$ are isomorphic if they are isomorphic as subposets of $Z_0^{\mathrm{eff}}(X)$.

Example 3.1. While the reduced subalgebra is defined for any locally finite poset, for $Z_0^{\mathrm{eff}}(X)$ in particular it has a simpler description (compare to [AK, Exs. 3.4 - 3.5]). Note that every interval in $Z_0^{\mathrm{eff}}(X)$ is isomorphic to $[0, \alpha]$ for some $\alpha \geq 0$. To simplify notation, if $f \in \widetilde{I}(X)$, write $f(\alpha) := f(0, \alpha)$. Then $\widetilde{I}(X)$ is isomorphic to a power series ring:

$$\widetilde{I}(X) \xrightarrow{\sim} \prod_{x \in |X|} k[[t_x]], \quad f \longmapsto \prod_{x \in |X|} \sum_{n=0}^{\infty} f(nx) t_x^n.$$

Notice that under the map $\prod_{x \in |X|} k[[t_x]] \to k[[t]]$ induced by $t_x \mapsto t^{\deg(x)}$, $\zeta \in \widetilde{I}(X)$ is sent to the zeta function $Z(X, t)$:

$$\zeta = \prod_{x \in |X|} \sum_{n=0}^{\infty} t_x^n \longmapsto \prod_{x \in |X|} \sum_{n=0}^{\infty} t^{n \deg(x)} = \prod_{x \in |X|} \frac{1}{1 - t^{\deg(x)}} = Z(X, t).$$

This mapping $\prod_{x \in |X|} k[[t_x]] \to k[[t]]$, which constructs a generating function for every $f \in \widetilde{I}(X)$, is a special case of a pushforward between incidence algebras (see Section 3.3 as well as the description in [AK, Sec. 3.3]). We will see that formula (1) is a statement about the pushforward of $\zeta \in \widetilde{I}(C)$ along a map $C \to \mathbb{P}^1$.

3.2 Objective Linear Algebra

We next categorify the incidence algebra of 0-cycles using objective linear algebra and decomposition sets. This formalism is part of the general theory of *decomposition spaces* developed in [GKT1, GKT2, GKT3, GKT4, GKT5] and explained in more detail in [Kob, AK]. See Appendix A for a more general dictionary that extends beyond the category Set.

Informally, objective linear algebra is "linear algebra with sets". In lieu of a full description of the theory, which already appears in [GKT4, Kob, AK], here is a dictionary of some linear algebra terms and their objective counterparts.

Linear	**Objective**
field of scalars k	the category Set
scalar addition $+$	coproduct $\coprod$
scalar multiplication	product $\times$
a basis B	a set B
a vector v in the basis B	a set map $v : X \to B$
the vector space with basis B	the slice category $\mathtt{Set}_{/B}$
vector addition $v + w$	coproduct $v \amalg w : X \coprod Y \to B$
scalar multiplication av	$A \times (v : X \to B) := (A \times X \xrightarrow{\mathrm{id} \times v} A \times B \xrightarrow{\mathrm{proj}_B} B)$
a matrix M	a span $\begin{array}{ccc} & M & \\ {}^{v}\swarrow & & \searrow^{w} \\ B & & C \end{array}$
the linear map with matrix M	the linear functor $w_! v^* : \mathtt{Set}_{/B} \to \mathtt{Set}_{/C}$
matrix multiplication	span composition
tensor product $V \otimes W$	symmetric tensor $\mathtt{Set}_{/B} \otimes \mathtt{Set}_{/C} := \mathtt{Set}_{/B \times C}$
dual space $V^* = \mathrm{Hom}(V, k)$	functor space $(\mathtt{Set}_{/B})^* := \mathrm{Fun}(\mathtt{Set}_{/B}, \mathtt{Set})$

Here, for any span (as pictured), the composition $w_! v^*$ in the definition of linear functor consists of the pullback functor $v^* : \mathtt{Set}_{/B} \to \mathtt{Set}_{/M}, (X \to B) \mapsto (X \times_B M \to M)$ and the pushforward functor $w_! : \mathtt{Set}_{/M} \to \mathtt{Set}_{/C}, (Y \to M) \mapsto (Y \to M \xrightarrow{w} C)$.

To recover the objects in the left column of the table, one can often apply the cardinality functor to objects in the right column. For example, if $v : X \to B$ is an objective vector with finite fibres, then the collection of its fibre cardinalities defines a vector $\sum_{b \in B} |v^{-1}(b)| b$ in the k-vector space spanned by B.

3.3 The Objective Incidence Algebra

To distinguish the objective incidence algebra defined in this section from the k-vector space constructed in Section 3.1, we will denote the earlier construction by $I_{\#}(X)$, following the notation in [AK]. Likewise, we will denote the reduced subalgebra of $I_{\#}(X)$ by $\widetilde{I}_{\#}(X)$.

Abstract incidence algebras are defined at the objective level for any *locally finite decomposition set* in [GKT1]. For such a decomposition set S, the incidence algebra $I(S)$ is an associative, unital monoid object in the objective linear algebra category LIN. We give the construction here for the decomposition set $S = Z_0^{\mathrm{eff}}(X)$, where X is a k-variety.

First, let $I_1 = I_1(X) = \mathrm{Int}(Z_0^{\mathrm{eff}}(X))$ denote the set of intervals in $Z_0^{\mathrm{eff}}(X)$. Equivalently, I_1 is the set of 1-simplices in the simplicial structure on $Z_0^{\mathrm{eff}}(X)$. Also, let I_0 denote the set of 0-simplices in $Z_0^{\mathrm{eff}}(X)$ (these are just the effective 0-cycles themselves) and let I_2 denote the set of 2-simplices, which is isomorphic to $I_1 \times I_1$.

The *incidence coalgebra* of S, which we will also refer to as the incidence coalgebra of X, is the objective vector space $C(X) := C(Z_0^{\mathrm{eff}}(X)) = \mathtt{Set}_{/I_1}$ equipped with a comultiplication linear functor $\Delta : C(X) \to C(X) \otimes C(X)$ corresponding to the span

$$\Delta = \left(\begin{array}{ccc} & I_2 & \\ {}^{d_1}\swarrow & & \searrow^{(d_2, d_0)} \\ I_1 & & I_1 \times I_1 \end{array} \right)$$

where d_0, d_1 and d_2 are the face maps $I_2 \to I_1$. $C(X)$ also comes equipped with a counit $\delta : C(X) \to \mathtt{Set}$ represented by the span

$$\delta = \left(\begin{array}{ccc} & I_0 & \\ {}^{s_0}\swarrow & & \searrow \\ I_1 & & * \end{array} \right)$$

where s_0 is the 0th degeneracy map. Dualizing $C(X)$ (in the objective sense) gives us the *incidence algebra* $I(X) := C(X)^* = \mathrm{Fun}(\mathtt{Set}_{/I_1}, \mathtt{Set})$, equipped with unit δ and multiplication given by convolution. Explicitly, convolution is a linear functor $* : I(X) \otimes I(X) \to I(X)$ which sends $f \otimes g \in I(X) \otimes I(X)$ to $f * g : \mathtt{Set}_{/I_1} \xrightarrow{\Delta} \mathtt{Set}_{/I_1} \otimes \mathtt{Set}_{/I_1} \xrightarrow{f \otimes g} \mathtt{Set} \otimes \mathtt{Set} \xrightarrow{\sim} \mathtt{Set}$, corresponding to the span

$$f * g = \left(\begin{array}{ccccccc} & & & P & & & \\ & & \swarrow & & \searrow & & \\ & I_2 & & & & I_1 \times I_1 & \\ {}^{d_1}\swarrow & & \searrow^{(d_2, d_0)} & & \swarrow^{f \times g} & & \searrow \\ I_1 & & & I_1 \times I_1 & & & * \end{array} \right).$$

The *zeta functor* of X is the linear functor $\zeta = \zeta_X$ represented by

$$\zeta = \left(\begin{array}{ccc} & I_1(X) & \\ {}^{id}\swarrow & & \searrow \\ I_1(X) & & * \end{array} \right).$$

Following [AK, Ex. 3.5], we define an objective notion of pushforward functor between incidence algebras. The general definition is in *loc. cit.*, but here is the definition for incidence algebras of 0-cycles. Let $\pi : Y \to X$ be a morphism of k-varieties. Pushforward of 0-cycles defines a simplicial map $Z_0^{\mathrm{eff}}(Y) \to Z_0^{\mathrm{eff}}(X)$, also denoted by π. This in turn induces a linear functor $\pi_* : I(Y) \to I(X)$: if $f \in I(Y)$ with span

$$f = \left(\begin{array}{ccc} & M & \\ {}^{v}\swarrow & & \searrow \\ I_1(Y) & & * \end{array} \right)$$

then $\pi_* f$ is the linear functor with span

$$\pi_* f = \left(\begin{array}{ccc} & M & \\ {}^{\pi_1 \circ v}\swarrow & & \searrow \\ I_1(X) & & * \end{array} \right).$$

For example, when $f = \zeta$, we get a linear functor

$$\pi_* \zeta = \left(\begin{array}{ccc} & I_1(Y) & \\ {}^{\pi_1}\swarrow & & \searrow \\ I_1(X) & & * \end{array} \right).$$

Finally, we discuss the objective version of the reduced incidence subalgebra of $I(X)$, following [GKT5, Sec. 1.5.3]. By [AK, Sec. 3.2], a decomposition set S admits a *numerical* reduced incidence algebra $\widetilde{I}_{\#}(S)$ as a subalgebra of its numerical incidence algebra when S is the decalage of another decomposition set $\widetilde{S}$, in particular when $S_r = \widetilde{S}_{r+1}$ for all $r \geq 0$. In this situation, it makes sense to view $I(\widetilde{S})$ as the *objective* reduced incidence algebra of S. The following example exhibits this subalgebra for the decomposition set of effective 0-cycles.

Example 3.2. When $S = (Z_0^{\mathrm{eff}}(X), \leq)$ for a k-variety X, $S = \mathrm{Dec}_\perp(\widetilde{S})$ where $\widetilde{S}$ is the monoid of isomorphism classes of effective 0-cycles under pointwise addition. By [GKT5, Lem. 2.1.2], this identification determines an injective linear functor

$$I(\widetilde{S}) \longrightarrow I(S).$$

The essential image of this functor may be regarded as the reduced incidence algebra of X. Passing to the numerical incidence algebras of $\widetilde{S}$ and S gives a k-linear map $I_\#(\widetilde{S}) \to I_\#(S)$ which is an isomorphism onto the numerical reduced incidence algebra $\widetilde{I}_\#(S)$. The zeta functor ζ lies in the reduced incidence algebra and its image in $\widetilde{I}_\#(S)$ corresponds to the arithmetic function $\zeta : \alpha \mapsto 1$ with generating function $Z(X,t)$. Equivalently, if $t : X \to \mathrm{Spec}\,\mathbb{F}_q$ is the structure map, then $Z(X) := t_*\zeta_X$ is the linear functor in $\widetilde{I}(\mathrm{Spec}\,\mathbb{F}_q)$ whose decategorification is precisely $Z(X,t)$.

4 Proof of the Main Theorem

For a hyperelliptic curve $\pi : C \to \mathbb{P}^1$ over a finite field $k = \mathbb{F}_q$, let $S = (Z_0^{\mathrm{eff}}(\mathbb{P}^1), \leq)$ and $T = (Z_0^{\mathrm{eff}}(C), \leq)$ and let $\pi_* : I(C) \to I(\mathbb{P}^1)$ be the pushforward on incidence algebras induced by π. Write $\widetilde{I}(\mathbb{P}^1)$ (resp. $\widetilde{I}(C)$) for the reduced incidence algebras described in Example 3.2. We will also abuse notation and write $\pi_* : \widetilde{I}(C) \to \widetilde{I}(\mathbb{P}^1)$ for the pushforward map induced by π on $\widetilde{S}$, though it is distinct from the restriction of π_* to $\widetilde{I}(C)$.

4.1 Local Theorem

For this section, fix a closed point $x \in |\mathbb{P}^1|$ and let $S_x = \{ax\}$ be the submonoid of effective divisors supported at x in $Z_0^{\mathrm{eff}}(\mathbb{P}^1)$. Let $T_x = \{\alpha : \pi_*\alpha \in S_x\}$ be the submonoid of $Z_0^{\mathrm{eff}}(C)$ consisting of divisors lying over divisors in S_x. Also let $\zeta_{\mathbb{P}^1,x}$ and $\zeta_{C,x}$ be the zeta functions in $I(S_x)$ and $I(T_x)$, respectively.

Theorem 4.1 (Local Version of Theorem 1.1)**.** *For each closed point $x \in |\mathbb{P}^1|$, in the incidence algebra $I(S_x)$, there is an equivalence of linear functors*

$$\pi_*\zeta_{C,x} + \zeta_{\mathbb{P}^1,x} * L_x(C)^- \cong \zeta_{\mathbb{P}^1,x} * L_x(C)^+. \tag{3}$$

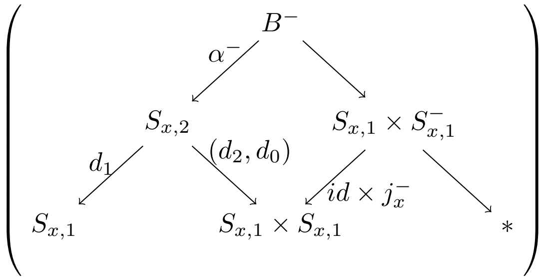
Proof. The terms in formula (3) are defined as follows. First, $\pi_*\zeta_{C,x}, L_x(C)^+$ and $L_x(C)^-$ are represented by the spans

$$\pi_*\zeta_{C,x} = \left(\begin{array}{ccc} & T_{x,1} & \\ \swarrow^{\pi_1} & & \searrow \\ S_{x,1} & & * \end{array}\right), \quad L_x(C)^+ = \left(\begin{array}{ccc} & S_{x,1}^+ & \\ \swarrow^{j_x^+} & & \searrow \\ S_{x,1} & & * \end{array}\right), \quad L(C)^- = \left(\begin{array}{ccc} & S_{x,1}^- & \\ \swarrow^{j_x^-} & & \searrow \\ S_{x,1} & & * \end{array}\right)$$

where $S_{x,1}^+, S_{x,1}^-, j_x^+$ and j_x^- are each defined below. Then the convolutions in formula (3) are given by the span convolutions

$$\zeta_{\mathbb{P}^1,x} * L_x(C)^+ = \left(\begin{array}{ccccc} & & B^+ & & \\ & \swarrow^{\alpha^+} & & \searrow & \\ & S_{x,2} & & S_{x,1} \times S_{x,1}^+ & \\ \swarrow^{d_1} & & \searrow^{(d_2,d_0)} \quad \swarrow^{id \times j_x^+} & & \searrow \\ S_{x,1} & & S_{x,1} \times S_{x,1} & & * \end{array}\right)$$

and

$$\zeta_{\mathbb{P}^1,x} * L_x(C)^- =$$ 

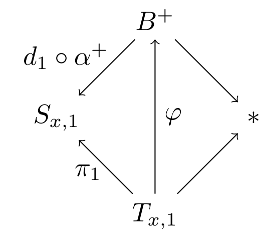
.

From here, the proof divides into cases based on the splitting type of the point x (see Proposition 2.2).

First assume x is one of the 4 branch points of the covering $\pi : C \to \mathbb{P}^1$ and let y be its unique preimage. In this case we take $j_x^+ : S_{x,1}^+ \hookrightarrow S_{x,1}$ to be the inclusion of the subset $\{0x\}$. Also let $S_{x,1}^- = \varnothing$. Then formula (3) becomes

$$\pi_* \zeta_{C,x} \cong \zeta_{\mathbb{P}^1,x} * L_x(C)^+$$

which is verified by constructing an equivalence of spans

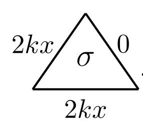


.

Note that B^+ can be described explicitly:

$$B^+ = \{\sigma \in S_{x,2} \mid d_0\sigma = 0x\}.$$

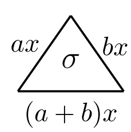
Define φ in the above diagram by

$$\varphi(ay) =$$ 

.

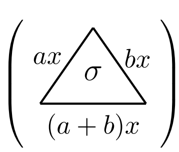
Since every 2-simplex in B^+ has this form, φ is invertible (send such a σ back to $2y \in T_{x,1}$). The diagram commutes by construction, proving formula (3) in the ramified case.

Next, suppose x splits in the covering π, with fibre $\pi^{-1}(x) = \{y, \bar{y}\}$. As in the ramified case, we take $S_{x,1}^- = \varnothing$, but set $S_{x,1}^+ = S_{x,1}$ so that $B^+ = S_{x,2}$ and $d_1 \circ \alpha = d_1$. To compare the linear functors $\pi_*\zeta_{C,x}$ and $\zeta_{\mathbb{P}^1,x} * L_x(C)^+$, we once again construct a map $\varphi : T_{x,1} \to B^+$ that makes the appropriate diagram commute. Define φ by

$$\varphi(ay + b\bar{y}) =$$ 

.

Every $\sigma \in B^+ = S_{x,2}$ has this form, so sending σ with $d_2\sigma = ax$ and $d_0\sigma = bx$ to $ay + b\bar{y} \in T_{x,1}$ gives an inverse to φ. In addition,

$$d_1 \circ \varphi(ay + b\bar{y}) = d_1$$ 

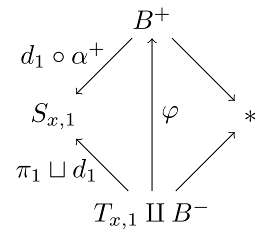
$$= ax + bx = \pi_1(ay + b\bar{y})$$

so the diagram commutes, proving formula (3) in the split case.

Finally, suppose x is inert. Here, we take $S^+_{x,1}$ and $S^-_{x,1}$ to be the even and odd degree divisors in $S_{x,1}$,

$$S^+_{x,1} = \{2kx \mid k \geq 0\} \quad \text{and} \quad S^-_{x,1} = \{(2k+1)x \mid k \geq 0\},$$

together with their natural inclusions $j^\pm : S^\pm_{x,1} \hookrightarrow S_{x,1}$. Then the equivalence $\pi_*\zeta_{C,x} + \zeta_{\mathbb{P}^1,x} * L_x(C)^- \cong L_x(C)^+$ is verified by constructing an isomorphism φ in the diagram

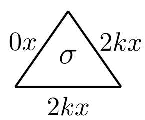


.

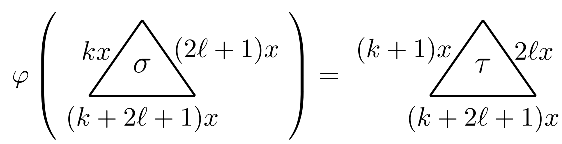
This time, B^+ and B^- have the following descriptions:

$$B^+ = \{\sigma \in S_{x,2} \mid d_0\sigma = 2kx, k \geq 0\} \quad \text{and} \quad B^- = \{\sigma \in S_{x,2} \mid d_2\sigma = (2k+1)x, k \geq 0\}.$$

We define φ on $T_{x,1}$ by

$\varphi(ay) =$ 

and on B^- by



.

It is routine to check φ is a bijection (cf. [AK, Thm. 4.2]), which proves formula (3) in all cases. □

Passing to the numerical incidence algebra $I_\#(S_x)$ and pushing forward to $I_\#(\operatorname{Spec} \mathbb{F}_q) \cong k[[t]]$ (as in Example 3.1) recovers the formula

$$Z_x(C,t) = Z_x(\mathbb{P}^1,t)(L_x(C,t)^+ - L_x(C,t)^-) = Z_x(\mathbb{P}^1,t)L_x(C,t)$$

where $L_x(C,t)$ is the local factor of the classical L-function of C, namely:

$$L_x(C,t) = \frac{1}{1 - \chi(F_x)t^{\deg(x)}}$$

where χ is the quadratic character associated to the extension $\mathbb{F}_q(E)/\mathbb{F}_q(t)$ and F is the Frobenius at x.

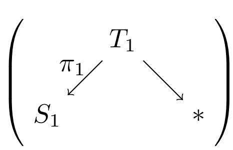
4.2 Global Theorem

Next, we prove the global formula of Theorem 1.1. Keep the notation $S = Z_0^{\text{eff}}(\mathbb{P}^1)$ and $T = Z_0^{\text{eff}}(C)$.

Theorem 4.2 (Theorem 1.1)**.** *In the reduced incidence algebra $\widetilde{I}(S) = \widetilde{I}(Z_0^{\text{eff}}(\mathbb{P}^1))$, there is an equivalence of linear functors*

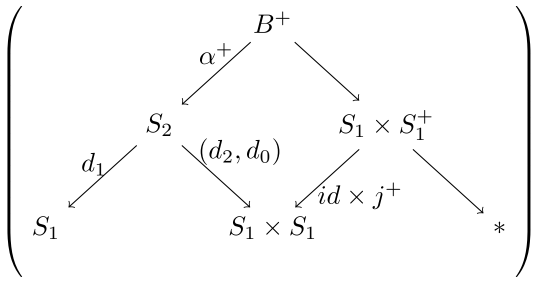
$$\pi_*\zeta_C + \zeta_{\mathbb{P}^1} * L(C)^- \cong \zeta_{\mathbb{P}^1} * L(C)^+.$$

Proof. As before, the terms in the formula are linear functors represented by the following spans:

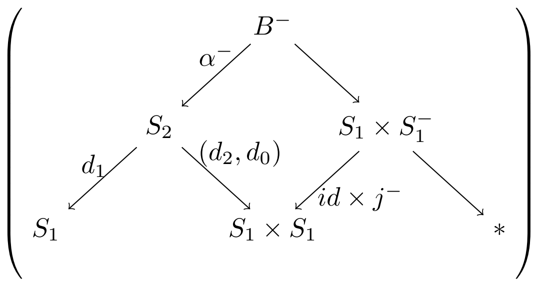
$\pi_*\zeta_C =$ 

as well as

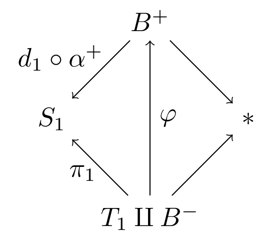
$\zeta_{\mathbb{P}^1} * L(C)^+ =$



and $\zeta_{\mathbb{P}^1} * L(C)^- =$



where $S_1^{\pm}$ and $j^{\pm}$ are defined below. We must then construct an isomorphism $\varphi : T_1 \amalg B^- \xrightarrow{\sim} B^+$ making the following diagram commute:



.

The proof is similar to that of [AK, Thm. 4.5]. For an effective 0-cycle $\alpha \in S$, write $\alpha = \sum_{x \in |\mathbb{P}^1|} a_x x$. Define S_1^+ and S_1^- as the following subsets of S_1:

$$S_1^+ = \left\{ \alpha \in S_1 \mid a_x = 0 \text{ for ramified } x, \sum_{x \text{ inert}} a_x \text{ is even} \right\}$$
$$S_1^- = \left\{ \alpha \in S_1 \mid a_x = 0 \text{ for ramified and split } x, \sum_{x \text{ inert}} a_x \text{ is odd} \right\}.$$

Their natural inclusions $j^+ : S_1^+ \hookrightarrow S_1$ and $j^- : S_1^- \hookrightarrow S_1$ define $L(C)^+$ and $L(C)^-$ and the span compositions above.

We now define $\varphi : T_1 \amalg B^- \xrightarrow{\sim} B^+$. Recall that the map $\pi_* : Z_0^{\text{eff}}(C) \to Z_0^{\text{eff}}(\mathbb{P}^1)$ is given by $\pi_*(y) = [k(y) : k(\pi(y))]\pi(y)$ and extended linearly. For $\varphi = \sum_{y \in |C|} b_y y \in T_1$, put $\varphi(\beta) = \tau \in S_2$ with faces

$$d_2\tau = \sum_{\substack{y \in \text{supp}(\beta) \\ \text{ramified}}} b_y \pi_*(y) + \sum_{\substack{y \in \text{supp}(\beta) \\ \text{split}}} b_y \pi_*(y)$$
$$d_0\tau = \sum_{\substack{\bar{y} \in \text{supp}(\beta) \\ \text{split}}} b_{\bar{y}} \pi_*(\bar{y}) + \sum_{\substack{y \in \text{supp}(\eta) \\ \text{inert}}} b_y \pi_*(y)$$
$$d_1\tau = \pi_*\beta = \sum_{y \in |\mathbb{P}^1|} b_y \pi_*(y).$$

Then since $d_0\tau$ is supported away from the ramification locus of π and $[k(y) : k(x)] = 2$ for inert $y \mapsto x$, we see that $\tau \in B^+$. On the other hand, for $\sigma \in B^-$ with $d_2\sigma = \alpha, d_0\sigma = \beta$ and $d_1\sigma = \gamma = \alpha + \beta$, define $\varphi(\sigma) = \tau$ with faces

$$d_2\tau = \sum_{x \text{ ramified}} a_x x + \sum_{x \text{ split}} a_x x + \sum_{x \text{ inert}} (a_x + 1)x$$
$$d_0\tau = \sum_{\substack{x \in \operatorname{supp}(\beta) \\ \text{inert}}} (b_x - 1)x \quad \text{and} \quad d_1\tau = \gamma = \alpha + \beta.$$

Then as above, $d_0\tau$ is supported away from the ramified points in $\mathbb{P}^1$ and $\beta = d_0\sigma \in S_1^-$ implies $b_x - 1$ is even, so $\tau \in B^+$.

To show φ is an isomorphism, we construct an inverse $\varphi^{-1} : B^+ \to T_1 \amalg B^-$ as follows. If $\tau \in B^+$ has $d_2\tau = \alpha, d_0 = \beta$ and $d_1\tau = \gamma = \alpha + \beta$, with α supported away from all inert points in $\mathbb{P}^1$, send it to

$$\varphi^{-1}(\tau) = \sum_{x \text{ ramified}} c_x y + \sum_{x \text{ split}} (a_x y + b_x \bar{y}) + \sum_{\substack{x \text{ inert} \\ b_x \text{ even}}} \frac{b_x}{2} y + \sum_{\substack{x \text{ inert} \\ b_x \text{ odd}}} b_x y \ \in T_1.$$

If α is supported on any inert points, send τ to $\beta^{-1}(\tau) = \sigma \in B^-$ with faces

$$d_2\sigma = \sum_{x \text{ ramified}} a_x x + \sum_{x \text{ split}} a_x x + \sum_{\substack{x \in \operatorname{supp}(\alpha) \\ \text{inert}}} (a_x - 1)x$$
$$d_0\sigma = \sum_{x \text{ ramified}} b_x x + \sum_{x \text{ split}} b_x x + \sum_{x \text{ inert}} (b_x + 1)x$$
$$d_1\sigma = d_1\tau = \gamma.$$

By construction, φ is a bijection and it satisfies $d_1 \circ \varphi = \pi \amalg d_1$, completing the proof. $\square$

Remark 4.3. Recall that for each split point $x \in |\mathbb{P}^1|$, we are choosing a labeling $\pi^{-1}(x) = \{y, \bar{y}\}$ in order to write down the formulas in the above proof. This implies that the isomorphism φ is not canonical: it depends on a choice of section of π over the split locus.

Remark 4.4. Taking the cardinality of the formula in Theorem 4.2 recovers formula (1), so Theorem 4.2 can be considered a categorification of that formula for the zeta function of a hyperelliptic curve. Explicitly, cardinality is a map from the reduced objective incidence algebra $\widetilde{I}(\mathbb{P}^1)$ to the reduced numerical incidence algebra $\widetilde{I}_\#(\mathbb{P}^1)$:

$$|\cdot| : \widetilde{I}(\mathbb{P}^1) \longrightarrow \widetilde{I}_\#(\mathbb{P}^1)$$
$$f = \left(\begin{array}{ccc} & M & \\ {\scriptstyle v}\swarrow & & \searrow \\ S_1 & & * \end{array} \right) \longmapsto \Big(|f| : \alpha \mapsto |v^{-1}(\alpha)| \Big).$$

Applying $|\cdot|$ to the formula $\pi_*\zeta_C + \zeta_{\mathbb{P}^1} * L(C)^- \cong \zeta_{\mathbb{P}^1} * L(C)^+$ produces a formula which, upon further applying the "generating function map"

$$\widetilde{I}_\#(\mathbb{P}^1) \longrightarrow k[[t]], \quad f \longmapsto \prod_{x \in |\mathbb{P}^1|} \sum_{n=0}^{\infty} f(nx) t^{n \deg(x)}$$

from Example 3.1, recovers formula (1).

Remark 4.5. As in [AK], it is possible to formulate a version of Theorem 4.2 in the "full" incidence algebra of the poset $Z_0^{\text{eff}}(\mathbb{P}^1)$, rather than treating it as a monoid. This corresponds to first taking the decalage of the monoid structure, then applying the same techniques as above. We have elected to omit further discussion of this formula since it doesn't appear to have practical applications. Nevertheless, it provides new relations not just among effective 0-cycles in a cover (and therefore points), but also intervals of effective 0-cycles (and therefore families of points).

Remark 4.6. The proof of Theorem 4.2 generalizes easily to arbitrary double covers of algebraic curves $C \to D$ over $\mathbb{F}_q$, giving interesting formulas for their zeta functions in $k[[t]]$:

$$Z(C,t) = Z(D,t)L(C/D,t)$$

for an appropriate "relative L-function" $L(C/D,t)$.

4.3 Application to Point Counting

Let E be an elliptic curve over $\mathbb{F}_q$ with L-polynomial $L(E,t) = 1 - a_q(E)t + qt^2$ where $a_q(E) = q + 1 - \#E(\mathbb{F}_q)$. On one hand, formula (1) says that

$$Z(E,t) = Z(\mathbb{P}^1,t)L(E,t).$$

On the other hand, Theorems 4.1 and 4.2, through Remark 4.4, show that $L(E,t) = L(E,t)^+ - L(E,t)^-$ can be written as

$$L(E,t) = \prod_{x \in |\mathbb{P}^1|} (1 - \chi(x)t^{\deg(x)})^{-1}$$

where χ is the following quadratic character:

$$\chi(x) = \begin{cases} 0, & x \text{ is ramified} \\ 1, & x \text{ is split} \\ -1, & x \text{ is inert} \end{cases}$$

which can be extended multiplicatively to all effective 0-cycles.

Let's spell this out explicitly. The t^n coefficient of $L(E,t)^+$ is the cardinality of the fibre of $j^+ : S_1^+ \to S_1$ over the set $S_1(n)$ of 0-cycles of degree n in S_1:

$$\begin{array}{ccccc} & & S_1(n)^+ & & \\ & \swarrow & & \searrow & \\ S_1(n) & & & & S_1^+ \\ & \searrow & & \swarrow_{j^+} & \\ & & S_1 & & \end{array}.$$

Then $\#S_1(n)^+$ is equal to the number of effective 0-cycles $\alpha = \sum_x a_x x$ on $\mathbb{P}^1$ of degree n with $a_x = 0$ for ramified x and the sum of the a_x even for inert x. On the other hand, $\#S_1(n)^-$ (defined similarly) is 0 if n is even and is equal to the number of α of degree n supported only on inert points if n is odd. Putting these together,

$$\#S_1(n)^+ - \#S_1(n)^- = \sum_{\deg(\alpha)=n} \chi(\alpha).$$

This allows us to reinterpret the L-polynomial in terms of the character χ, as claimed. Write

$$\prod_{x \in |\mathbb{P}^1|} (1 - \chi(x)t^{\deg(x)})^{-1} = \sum_{n=0}^{\infty} f(n)t^n \quad \text{where} \quad f(n) = \sum_{\deg(\alpha)=n} \chi(\alpha).$$

As an element of the numerical incidence algebra $I_\#(Z_0^{\text{eff}}(\mathbb{P}^1))$, f is the sequence

$$f(0) = 1, \quad f(1) = -a_q(E), \quad f(2) = q \quad \text{and} \quad f(n) = 0 \text{ for } n > 2.$$

For $n = 1$, this implies the first part of formula (2):

$$a_q(E) = -\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi(x) = \#\{\text{inert } x \in \mathbb{P}^1(\mathbb{F}_q)\} - \#\{\text{split } x \in \mathbb{P}^1(\mathbb{F}_q)\} =: i_q(E) - s_q(E) \qquad (4)$$

while for $n = 2$, we obtain

$$q = \sum_{\deg(\alpha)=2} \chi(\alpha).$$

Formula (1) then implies

$$\#\operatorname{Sym}^2 E(\mathbb{F}_q) = (q^2 + q + 1) - (q+1)a_q + \sum_{\deg(\alpha)=2} \chi(\alpha). \tag{5}$$

A similar proof shows the rest of formula (2):

$$\#\operatorname{Sym}^n E(\mathbb{F}_q) = \sum_{i+j=n} (q^i + \ldots + q + 1) \sum_{\deg(\alpha)=j} \chi(\alpha). \tag{6}$$

These are the recursions which generate all point counts $\#E(\mathbb{F}_{q^r})$ from knowledge of just $\#E(\mathbb{F}_q)$. (To go from the sequence $\#\operatorname{Sym}^n E(\mathbb{F}_q)$ to the sequence $\#E(\mathbb{F}_{q^n})$, take ghost components, or equivalently, apply the logarithmic derivative to $Z(E,t)$.) Our proof demonstrates that they come directly from an objective L-function and, more importantly, that this L-function enumerates points (weighted by χ) *on the projective line.*

Example 4.7. Consider the elliptic curve $E/\mathbb{F}_5$ [LMFDB, Abelian Variety 1.5.d] with Weierstrass equation

$$E : y^2 = x^3 + x + 1.$$

It is known that $\#E(\mathbb{F}_5) = 9$ (see below), giving $L(E,t) = 1 + 3t + 5t^2$. Projecting to $\mathbb{P}^1$, there are 3 more split points than inert points. Since $x^3 + x + 1$ is irreducible over $\mathbb{F}_5$, ∞ is the only ramified point on $\mathbb{P}^1$. Split points contribute 2 rational points on E, so there must be exactly 4 split points and 1 inert point downstairs. Here's a table of the closed points of E with images in $\mathbb{P}^1(\mathbb{F}_5)$.

ramified points	split points	inert points
∞	$(0,1)$	$(1,\alpha)$
	$(0,4)$	$(1,-\alpha)$
	$(2,1)$	
	$(2,4)$	
	$(3,1)$	
	$(3,4)$	
	$(4,2)$	
	$(4,3)$	

The 8 split points cover the 4 split points on $\mathbb{P}^1$ identified above. The inert points $(1,\pm\alpha)$ cover the inert point $1 \in \mathbb{P}^1(\mathbb{F}_5)$, with α a square root of 3 in $\mathbb{F}_{25}$. Moreover, formula (5) quickly allows us to compute that $\#E(\mathbb{F}_{25}) = 27$. We can further deduce then that in $\mathbb{P}^1(\mathbb{F}_{25})$, there are 12 split points, lifting to 24 of the 27 points in $E(\mathbb{F}_{25})$, and 13 inert points. Similarly, $\#E(\mathbb{F}_{125}) = 108$ and the 126 points in $\mathbb{P}^1(\mathbb{F}_{125})$ consist of 4 ramified points, 31 split points and 91 inert points.

Example 4.8. Up to isogeny, the elliptic curve E in Example 4.7 has a unique quadratic twist over $\mathbb{F}_5$ [LMFDB, Abelian Variety 1.5.ad],

$$E' : y^2 = x^3 + 4x + 2$$

with $\#E'(\mathbb{F}_5) = 3$ and $L(E',t) = 1 - 3t + 5t^2$. This time, there are 3 more inert points than split points, from which we can deduce that on $\mathbb{P}^1$, there is a single ramification point at ∞, 4 inert points and 1 split point. Here's the corresponding table of points for E':

ramified points	split points	inert points
∞	$(3,1)$	$(0,\beta)$
	$(3,4)$	$(0,-\beta)$
		$(1,\beta)$
		$(1,-\beta)$
		$(2,\alpha)$
		$(2,-\alpha)$
		$(4,\beta)$
		$(4,-\beta)$

Here, α is the same as above and β is a square root of 2 in $\mathbb{F}_{25}$. Using formula (5), we quickly deduce that $\#E'(\mathbb{F}_{25}) = 27$, which is as expected since $E' \cong E$ over $\mathbb{F}_{25}$.

An interesting consequence of our interpretation of $a_q(E)$ is that E is supersingular over $\mathbb{F}_q$ if and only if the $\mathbb{F}_q$-points of E project to an equal number of split and inert points in $\mathbb{P}^1$. Here is an example of such a curve.

Example 4.9. Consider the following supersingular elliptic curve over $\mathbb{F}_7$ [LMFDB, Abelian Variety 1.7.a]:

$$E : y^2 = x^3 + 5x.$$

Then $\#E(\mathbb{F}_7) = 8$ and $L(E,t) = 1 + 7t^2$, so formula (4) says there are an equal number of split and inert points on $\mathbb{P}^1$. With 4 ramified points downstairs, this forces 2 split points and 2 inert points:

ramified points	split points	inert points
∞	$(2,2)$	$(1,\sqrt{6})$
$(0,0)$	$(2,5)$	$(1,-\sqrt{6})$
$(3,0)$	$(6,1)$	$(5,\sqrt{3})$
$(4,0)$	$(6,6)$	$(5,-\sqrt{3})$

Also, formula (5) gives us $\#E(\mathbb{F}_{49}) = 64$.

Example 4.10. Consider the same elliptic curve $E : y^2 = x^3 + 5x$ over $\mathbb{F}_{37}$, where it is no longer supersingular [LMFDB, Abelian Variety 1.37.am]. This time, $\#E(\mathbb{F}_{37}) = 26$ and $L(E,t) = 1 - 12t + 37t^2$, so formula (4) implies there are 12 more inert points than split points on $\mathbb{P}^1$. With 2 ramified points downstairs, there must be 12 split points and therefore 24 inert points. (The split points have x-coordinates $4, 8, 9, 12, 15, 17, 20, 22, 25, 28, 29$ and 33.) Formula (5) also confirms that $\#E(\mathbb{F}_{1369}) = 1300$.

In this section, we showed how Theorem 4.2 gives an objective interpretation of the coefficients of the L-polynomial $L(E,t)$. Famously, these coefficients also have a cohomological origin, namely $L(E,t) = \det(1 - Ft \mid H^1(E))$ where $H^1(E, \mathbb{Q}_\ell)$ is the 1st ℓ-adic cohomology group of E and F is the Frobenius operator. In Appendix A.4, we explain how these cohomological coefficients can be interpreted objectively as well, though not in the category of sets as was done in Theorem 4.2.

5 Topological Covers

As suggested in [AK], we can use objective linear algebra to categorify a well-known formula describing how the Euler characteristic changes in a branched cover of Riemann surfaces. This is a topological analogue to Theorem 4.2.

Before describing branched double covers, suppose $\pi : Y \to X$ is an unbranched cover of degree $n \geq 2$. Then the Euler characteristics of X and Y satisfy the following relation:

$$\chi(Y) = n\chi(X). \tag{7}$$

Let's lift this formula to an objective formula in an incidence algebra.

Let $S_\bullet(X)$ (resp. $S_\bullet(Y)$) be the simplicial complex associated to X (resp. Y) and let $S(\pi) : S_\bullet(Y) \to S_\bullet(X)$ be the simplicial map induced by π. By definition, $S_\bullet(X)$ and $S_\bullet(Y)$ are decomposition sets. Denote the zeta functor in $S_\bullet(X)$ by ζ_X.

For $X = *$, the objective incidence algebra $I(S_\bullet(*))$ is isomorphic to $\mathtt{Set}_{/*} = \mathtt{Set}$; its numerical incidence algebra $I_\#(S_\bullet(*))$ is isomorphic to the ring of power series $k[[t]]$; and the zeta functor $\zeta_* \in I(S_\bullet(*))$ decategorifies to $(1,1,1,\ldots)$ in $I_\#(S_\bullet(*))$, corresponding to $(1-t)^{-1} \in k[[t]]$. Notice that in this case,

$$|\zeta_*| = (1-t)^{-\chi(*)}.$$

In dimension 0, a degree n cover $Y \to *$ is just a set of n points $Y = \{y_1, \ldots, y_n\}$, so formula (7) in this case is the decategorification of

$$\zeta_Y \cong \underbrace{\zeta_* * \cdots * \zeta_*}_{n}.$$

This works because points have no nondegenerate simplices of higher dimension.

Unfortunately, this only applies to 0-simplices. The Möbius function is better suited to computing Euler characteristic objectively. For any X, the zeta functor in $I(S_\bullet(X))$ is

$$\zeta_X = \left(\begin{array}{ccc} & S_1(X) & \\ {}^{id}\swarrow & & \searrow \\ S_1(X) & & * \end{array} \right).$$

Define $\zeta_X^{(k)} \in I(S_\bullet(X))$ by

$$\zeta_X^{(k)} = \left(\begin{array}{ccc} & S_k(X)^\circ & \\ {}^{d_1^k}\swarrow & & \searrow \\ S_1(X) & & * \end{array} \right)$$

where $S_k(X)^\circ \subseteq S_k(X)$ is the subset of nondegenerate k-simplices. (This is not to be confused with the k-fold convolution ζ_X^k.) Following [GKT2], we also put $\zeta_X^{(0)} = \delta_X$, the unit of convolution in $I(S_\bullet(X))$, and define

$$\Phi_{even} = \sum_{k=0}^{\infty} \zeta_X^{(2k)} \quad \text{and} \quad \Phi_{odd} = \sum_{k=0}^{\infty} \zeta_X^{(2k+1)}.$$

These functors satisfy an objective form of Möbius inversion [GKT2, Thm. 3.8]:

$$\zeta_X * \Phi_{even} \cong \delta + \zeta_X * \Phi_{odd}.$$

In the numerical incidence algebra $I_\#(S_\bullet(X))$, this formula descends to

$$\delta = \zeta_X * (\Phi_{even} - \Phi_{odd}) = \zeta_X * \mu_X$$

where μ_X is the numerical Möbius function for $S_\bullet(X)$.

Define spaces $E_{even}(X), E_{odd}(X) \in \mathtt{Top}$ by

$$E_{even}(X) = \coprod_{s \in S_1(X)} \Phi_{even}(s) \quad \text{and} \quad E_{odd}(X) = \coprod_{s \in S_1(X)} \Phi_{odd}(s).$$

Here, $F(s)$ denotes the fibre $M_s = p^{-1}(s)$ for any linear functor F represented by a span

$$F = \left(\begin{array}{ccc} & M & \\ {}^{p}\swarrow & & \searrow \\ S_1(X) & & * \end{array} \right).$$

Already, this categorifies the Euler product:

Proposition 5.1. *If X is a finite CW complex, then $\chi(X) = |E_{even}(X)| - |E_{odd}(X)|$.*

The objects $E_{even}(X)$ and $E_{odd}(X)$ can be viewed as linear functors in $I(S_\bullet(X))$:

$$\Phi_{even}(X) = \left(\begin{array}{ccc} & * & \\ \swarrow & & \searrow \\ S_1(X) & & E_{even}(X) \end{array} \right) \quad \text{and} \quad \Phi_{odd}(X) = \left(\begin{array}{ccc} & * & \\ \swarrow & & \searrow \\ S_1(X) & & E_{odd}(X) \end{array} \right).$$

In this way, the construction can be interpreted as an "objective Macdonald polynomial": pushing forward $\Phi_{even}(X)$ and $\Phi_{odd}(X)$ along the terminal map $t : X \to *$ produces linear functors $t_*\Phi_{even}(X), t_*\Phi_{odd}(X) \in I(S_\bullet(*))$ and, as discussed above, their decategorifications in $I_\#(S_\bullet(*)) \cong k[[t]]$ are

$$|t_*\Phi_{even}(X)| = (1-t)^{-|E_{even}(X)|} \quad \text{and} \quad |t_*\Phi_{odd}(X)| = (1-t)^{-|E_{odd}(X)|}$$

so that

$$\frac{|t_*\Phi_{even}(X)|}{|t_*\Phi_{odd}(X)|} = (1-t)^{-|E_{even}(X)|+|E_{odd}(X)|} = (1-t)^{-\chi(X)}.$$

Theorem 5.2. *For a degree n cover $\pi : Y \to X$ of finite CW complexes, there is an equivalence of linear functors*

$$\pi_*\Phi_{even}(Y) * \Phi_{odd}(X)^n \cong \pi_*\Phi_{odd}(Y) * \Phi_{even}(X)^n$$

in the objective incidence algebra $I(S_\bullet(X))$. Here, $(-)^n$ denotes the n-fold convolution.

Proof. Each nondegenerate k-cell in X lifts to exactly n nondegenerate k-cells in Y. This gives us bijections $E_{even}(Y) \xrightarrow{\sim} \coprod_{i=1}^n E_{even}(X)$ and $E_{odd}(Y) \xrightarrow{\sim} \coprod_{i=1}^n E_{odd}(X)$ which assemble into the stated formula. □

Pushing forward to the incidence algebra of a point and taking cardinalities recovers Formula (7) via generating functions:

$$(1-t)^{-\chi(Y)} = \frac{|t_*\Phi_{even}(Y)|}{|t_*\Phi_{odd}(Y)|} = \left(\frac{|t_*\Phi_{even}(X)|}{|t_*\Phi_{odd}(X)|}\right)^n = (1-t)^{-n\chi(X)}.$$

Next, suppose $\pi : Y \to X$ is a branched cover. Call the irreducible components of the branch locus $X_1, \dots, X_r \subset X_{br}$ and for each component $Z_i \subseteq \pi^{-1}(X_i)$, let $e(Y_i)$ be the ramification index of X_i. Setting $e(Z) = 1$ for any irreducible component $Z \subseteq Y, Z \not\subseteq \pi^{-1}(X_1 \cup \dots \cup X_r)$, we have

$$\sum_{Z \subseteq \pi^{-1}(X')} e(Z) = n$$

for *any* irreducible component $X' \subseteq X$. The analogue of Formula (7) for branched covers is

$$\chi(Y) = n\chi(X) - \sum_{Z \subseteq Y} (e(Z) - 1). \tag{8}$$

Theorem 5.3 (Theorem 1.2)**.** *For a connected, degree n branched cover $\pi : Y \to X$, there is a linear functor $R \in I(S_\bullet(Y))$ and an equivalence*

$$\pi_*\Phi_{even}(Y) * \Phi_{odd}(X)^n * \pi_* R \cong \pi_*\Phi_{odd}(Y) * \Phi_{even}(X)^n$$

in $I(S_\bullet(X))$.

Proof. For simplicity, we give the proof in the case when $\pi : Y \to X$ is a branched cover of surfaces. Let $X_{br} = \{x_1, \dots, x_r\}$ be the branch locus of π and for each x_i, write $\pi^{-1}(x_i) = \{y_{i1}, \dots, y_{ik_i}\}$ for each $1 \le i \le r$. Each nondegenerate k-cell $\sigma \in S_k(X)$ lifts to n nondegenerate k-cells in $S_k(Y)$ *except* when when $k = 0$ and $\sigma = x_i$ for some $1 \le i \le r$. In this case, there are $n - k_i = \sum_{j=1}^{k_i}(e(y_{ij}) - 1)$ points "missing" from the count. Said another way, there is a bijection

$$\coprod_{i=1}^n E_{even}(X) \xrightarrow{\sim} E_{even}(Y) \amalg \{z_{i1}, \dots, z_{i,n-k_i}\}_{i=1}^r$$

where $z_{i1}, \dots, z_{i,n-k_i}$ are these "missing points" in $\pi^{-1}(x_i)$. Setting $R = \{z_{i1}, \dots, z_{i,n-k_i}\}_{i=1}^r$, we obtain the stated formula. □

Remark 5.4. Let G be the group of deck transformations of $\pi : Y \to X$. Then it should be possible to lift formula (8) to an equivalence of linear functors of G-representations, eliminating the need to separate Φ_{even} and Φ_{odd} in the above formulation.

Question 5.5. *Is it also possible to prove $\chi(X \times Y) = \chi(X)\chi(Y)$ this way? And more generally $\chi(E) = \chi(B)\chi(F)$ for a fibration $F \to E \to B$?*

6 Future Directions

Higher Degree Extensions. As explained in Section 1, anytime there is a map $C \to \mathbb{P}^1$ (or more generally a map between curves) the zeta function of C factors into a product of L-functions over $\mathbb{P}^1$ (resp. the base curve). We can categorify zeta functions of hyperelliptic curves essentially because the coefficients of their L-functions can be recovered as cardinalities of sets of 0-cycles. Equivalently, the "character" χ is quadratic; compare to [AK]. In the degree ≥ 3 situation, $L(C)^+$ and $L(C)^-$ will need to be replaced with a more general categorical L-functor (see Appendix A).

L-Functions. In modern number theory and arithmetic geometry, results for zeta functions are often subsumed by more general statements for L-functions, making these a natural target for our categorification program. Fortunately, we have made progress towards a theory of *L-functors* which adapts the techniques in [AK] and the present work to a more general framework that accommodates L-functions. We will present this work in a future article, using an objective linear algebra theory that replaces simplicial sets with simplicial objects in other categories (see Appendix A for a brief introduction). For Artin L-functions, their corresponding L-functors are linear functors of continuous Galois representations.

Motivic Zeta and L-Functions. To push beyond the point counting applications in this article, it's natural to ask for a categorification of motivic zeta and L-functions, as suggested in [Kob, Sec. 4]. In this direction, the authors in [DH] have constructed a numerical version of Kapranov's motivic zeta function $Z_{mot}(X,t)$ for a k-variety X that lies in an incidence algebra[1] constructed from the Grothendieck ring of k-varieties, $K_0(\mathtt{Var}_k)$. As $K_0(\mathtt{Var}_k)$ is itself a decategorification of the category $\mathtt{Var}_k$, it should still be possible to lift $Z_{mot}(X,t)$ further to an objective incidence algebra, as originally suggested in [Kob]. Using the language of L-functors, we will offer such a construction in future work. This will also provide a natural home for motivic L-functions, defined as $L(X,V,t) = Z_{mot}((X \otimes V)^G, t)$ for an algebraic group G acting on X and a G-representation V. We also plan to unify these with the L-functions in the previous paragraph by extending the whole formalism to stacks.

A Objective Linear Algebra

A.1 Objective Linear Algebra Using the Category $\mathtt{Set}$

In Section 3, we constructed objective incidence algebras for the decomposition sets of effective 0-cycles for an algebraic curve C/k. The theory of *decomposition spaces* from [GKT1, GKT2, GKT3, GKT4, GKT5] extends far beyond "objective" techniques in the category of sets, allowing for greater flexibility in our categorifications. To summarize the general theory, we reproduce below the dictionary from Section 3 in an arbitrary category of spaces.

A.2 Replacing the Category of Sets

Let $(\mathcal{C}, \otimes, \mathbb{1})$ be a symmetric monoidal category with coproduct $\oplus$. Furthermore, assume $\mathcal{C}$ has a terminal object $*$, and fix a section $s\colon * \to \mathbb{1}$. By abuse of notation, let s also refer to the composition $A \to * \xrightarrow{s} \mathbb{1}$ for any object A of $\mathcal{C}$.

With this setup, we revise the table given in section A.1.

[1] the authors in [DH] call it the *reduced incidence algebra for the poscheme of effective 0-cycles* of X

Linear	Objective
field of scalars k	a symmetric monoidal category $\mathcal{C}$
scalar addition $+$	$\oplus$
scalar multiplication	$\otimes$
a basis B	an object B
a vector v in the basis B	a morphism $v : X \to B$
the vector space with basis B	the slice category $\mathcal{C}_{/B}$
vector addition $v + w$	coproduct $v \oplus w : X \oplus Y \to B$
scalar multiplication av	$A \otimes (v : X \to B) := (A \otimes X \xrightarrow{\mathrm{id} \otimes v} A \otimes B \xrightarrow{s \otimes \mathrm{id}_B} B)$
a matrix M	a span $B \xleftarrow{v} M \xrightarrow{w} C$
the linear map with matrix M	the linear functor $w_! v^* : \mathcal{C}_{/B} \to \mathcal{C}_{/C}$
matrix multiplication	span composition

Example A.1. Fix the base field $\mathbb{F}_q$ and an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}_q$. Let $G = \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_q)$ be the absolute Galois group of $\mathbb{F}_q$; it is isomorphic to the profinite completion of the integers $\widehat{\mathbb{Z}}$, and is topologically generated by the q-power Frobenius Fr_q. We define the category G-`Rep` to have objects which are complex vector spaces which have a continuous action of G, with G-equivariant morphisms. For our purposes, its terminal object is not interesting, as it is the zero vector space. So we use instead the slice category $G\text{-mod}_{/\mathbb{C}[G]}$.

The coproduct in G-`Rep` is the direct sum $\oplus$, and it can be made into a symmetric monoidal category by way of the tensor product $\oplus$.

A.3 Using G-Representations

The main advantage to using a category such as G-`Rep` over `Set` is that objects in G-`Rep` have richer decategorifications than those in `Set`. Take, for instance, an ordinary 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If a, b, c, d are all nonnegative integers, then A is easily lifted to an objective matrix

$$A = \left(B \xleftarrow{s} X \xrightarrow{t} B \right)$$

where $B = \{1, 2\}$ and $X = X_a \amalg X_b \amalg X_c \amalg X_d$, with $|X_i| = i$ and s (resp. t) sending elements in $X_a, \ldots, X_d$ to the number of the column (resp. row) their label appears in in A. However, if any of a, b, c, d are negative, rational, real, complex or beyond, it is only possible to lift A to an objective matrix over a more general category.

For an explicit example, take

$$A = \begin{pmatrix} 1 & -3 \\ -2 & -1 \end{pmatrix}.$$

In the category C_2-`Rep` (say, over $\mathbb{C}$), there are two irreducible representations up to isomorphism: V_1 and V_{-1}, where V_d is 1-dimensional with the nontrivial element in C_2 acting as multiplication by d. Set $V = V_1 \oplus V_{-1}$ and consider the objective matrix

$$A = \left(V \oplus V \xleftarrow{s} W \xrightarrow{t} V \oplus V \right)$$

where $W = V_1 \oplus V_{-1}^{\oplus 3} \oplus V_{-1}^{\oplus 2} \oplus V_{-1}$ and s (resp. t) sends the first and third factors V_1 and $V_{-1}^{\oplus 2}$ (resp. the first two factors V_1 and $V_{-1}^{\oplus 3}$) onto their corresponding factors in the first component of $V \oplus V$, and the remaining factors to their corresponding factors in the second component. Taking the trace of the action of a generator of C_2 on components recovers the original matrix A. If A had entries which were roots of unity, we could replace C_2 with the appropriate cyclic group C_n and recover these entries as well. For more general entries, more general structures are required (i.e. Galois representations over an appropriate extension of $\mathbb{Q}$ containing the coefficients of the matrix, but possibly more generality is also required).

In this more general framework, it is possible to categorify formula (1) without splitting up the L-function, in contrast to the formula in Theorem 4.2. In short, negative coefficients must be passed off as positive coefficients on the other side of an objective formula over `Set`, but they can be represented directly over C_2-`Rep` using V_{-1}. We will describe a vast generalization of this procedure in a future article. For now, we give a brief description of an L-functor approach to formula (1).

A.4 Objective L-Polynomials

In this section, we will show how the L-polynomial $L(E,t) = 1 - a_q t + qt^2$ of an elliptic curve $E/\mathbb{F}_q$ can be interpreted cohomologically in the objective setting. It is well-known that $L(E,t)$ is a characteristic polynomial, namely $\det(1 - tF)$ where $F = \mathrm{Frob}_q$ is the Frobenius operator acting on $H^1(E, \mathbb{Q}_\ell)$. There is a general notion of characteristic polynomial in objective linear algebra, but we will only need the following version.

As in Section A.3, let $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and let V be any continuous G-representation. Define the *L-functor* of V to be the span

$$L(V) = \begin{pmatrix} & \bigoplus_{n\geq 0} \mathrm{Sym}^n V & \\ \swarrow & & \searrow \\ \bigoplus_{n\geq 0} \mathbb{Q}_\ell & & \mathbb{Q}_\ell \end{pmatrix}.$$

This defines an element in the incidence algebra of $\bigoplus_{n=0}^\infty \mathbb{Q}_\ell$, viewed as a simplicial G-representation with trivial structure in each level. When V is finite dimensional, taking traces of Frobenius yields the following sequence in the numerical incidence algebra $I_\#(\mathbb{N}_0; \mathbb{Q}_\ell)$:

$$|L(V)|(n) := \mathrm{Tr}(F \mid \mathrm{Sym}^n V).$$

These assemble into the *reciprocal* characteristic polynomial of V:

$$\sum_{n=0}^\infty |L(V)|(n) t^n = \sum_{n=0}^\infty \mathrm{Tr}(F \mid \mathrm{Sym}^n V) t^n = \frac{1}{\det(1 - tF \mid V)}.$$

In the case of an elliptic curve $E/\mathbb{F}_q$, let $V = H^1(E, \mathbb{Q}_\ell)$ so that $\det(1 - tF \mid V) = L(E,t)$. Remark 4.4 also implies that

$$L(E,t) = \sum_{n=0}^\infty (\chi^+(n) - \chi^-(n)) t^n$$

so as a consequence, the arithmetic functions $L(E) := L(E)^+ - L(E)^-$ and $|L(V)|$ are inverses in the numerical incidence algebra $I_\#(\mathbb{N}_0; \mathbb{Q}_\ell)$. In fact, these are inverses in an objective incidence algebra. To show this, we have to realize $L(E)$ in the category of G-representations. Using the notation from Section 4.2, define

$$L(E) = \begin{pmatrix} & \mathbb{Q}_\ell S_1^+ \oplus \mathbb{Q}_\ell S_1^- & \\ \swarrow & & \searrow \\ \bigoplus_{n\geq 0} \mathbb{Q}_\ell & & \mathbb{Q}_\ell \end{pmatrix}$$

where $F = \mathrm{Frob}_q$ acts on $\mathbb{Q}_\ell S_1^+$ by the identity and on $\mathbb{Q}_\ell S_1^-$ by -1. Then in the objective incidence algebra $I\left(\bigoplus_{n\geq 0} \mathbb{Q}_\ell\right)$, we get a convolution $L(V) * L(E)$, which has the same trace generating function[2] as the unit functor δ. This shows that we can view $L(V)$ is an objective lift of the reciprocal L-polynomial of E.

[2] In general, we cannot expect linear functors to have objective inverses [GKT2].

References

[AK] Aycock, J. and Kobin, A. “Categorifying quadratic zeta functions”. Preprint (2022), arXiv:2205.06298.

[CLL] Content, M., Lemay, F. and Leroux, P. “Catégories de Möbius et fonctorialités: un cadre général pour l'inversion de Möbius”. J. Combinatorial Theory Ser. A, 28 (1980), 164 - 190.

[DH] Das, R. and Howe, S. “Cohomological and motivic inclusion-exclusion”. Preprint (2022), arXiv:2204.04165.

[Dür] Dür, A. *Möbius functions incidence algebras and power series representations.* Lecture Notes in Mathematics, vol. 1202. Springer-Verlag, Berlin (1986).

[DK] Dyckerhoff, T. and Kapranov, M. “Higher Segal spaces I”. Preprint (2012), arXiv:1212.3563v1.

[GKT1] Gálvez-Carrillo, I., Kock, J. and Tonks, A. “Decomposition spaces, incidence algebras and Möbius inversion I: basic theory”. Advances in Mathematics, 331 (2018), 952 - 1015.

[GKT2] Gálvez-Carrillo, I., Kock, J. and Tonks, A. “Decomposition spaces, incidence algebras and Möbius inversion II: completeness, length filtration and finiteness”. Advances in Mathematics, 333 (2018), 1242 - 1292.

[GKT3] Gálvez-Carrillo, I., Kock, J. and Tonks, A. “Decomposition spaces, incidence algebras and Möbius inversion III: the decomposition space of Möbius intervals”. Advances in Mathematics, 334 (2018), 544 - 584.

[GKT4] Gálvez-Carrillo, I., Kock, J. and Tonks, A. “Homotopy linear algebra”. Proceedings of the Royal Society of Edinburgh Section A: Mathematics 148, 2 (2018), 293 - 325.

[GKT5] Gálvez-Carrillo, I., Kock, J. and Tonks, A. “Decomposition spaces in combinatorics”. Preprint (2016), arXiv:1612.09225.

[Joy] Joyal, A. “Une théorie combinatoire des séries formelles”. Adv. Math., 42 (1981), 1 - 82.

[Kob] Kobin, A. “A primer on zeta functions and decomposition spaces”. Moduli, Motives and Bundles - New Trends in Algebraic Geometry, *London Mathematical Society Lecture Notes Series* (to appear). Available at arXiv:2011.13903.

[Koc] Kock, J. “Incidence Hopf algebras”. Notes (2010), mat.uab.es/ kock/seminars/incidence-algebras.pdf.

[Law] Lawvere, F.W. “Ordinal sums and equational doctrines”. *Seminar on triples and categorical homology theory, ETH 1966/67*, ed. B. Eckmann, *Lecture Notes in Mathematics*, no. 80, 141 - 155. Springer-Verlag, New York (1967). Reprinted in Repr. Theory Appl. Categ., 18 (2008).

[LM] Lawvere, F.W. and Menni, M. “The Hopf algebra of Möbius invervals”. Theory Appl. Categ., 24 (2010), 221 - 265.

[Ler] Leroux, P. “Les catégories de Möbius”. Cahiers Topol. Géom. Diff., 16 (1976), 280 - 282.

[LMFDB] The LMFDB Collaboration, The L-Functions and Modular Forms Database. Accessed 2023, available at `https://www.lmfdb.org`.

[Mus] Mustaţă, M. “Zeta functions in algebraic geometry”. Unpublished, available online at http://www.math.lsu.umich.edu/~mmustata/zeta_book.pdf.

[Rot] Rota, G.-C. “On the foundations of combinatorial theory I: theory of Möbius functions”. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 2 (1964), 340 - 368.