A CENSUS OF CUBIC FOURFOLDS OVER $\mathbb{F}_2$

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Bachelors in Science

in

Mathematics

by

Jonah Weinbaum

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 2023

Abstract

We compute a census of isomoprhism classes of cubic fourfolds over $\mathbb{F}_2$ using a new method of efficient orbit enumeration. With this census, we were able to compute the zeta functions of all smooth cubic fourfolds over $\mathbb{F}_2$. This analysis provides us with information about the point counts, cohomology, and other invariants of cubic fourfolds.

Acknowledgements

I would first like to extend my sincerest gratitude to the Dartmouth Mathematics department for their continued support in my mathematics education.

I would also like to extend thanks to my mathematics teachers who helped to inspire curiosity in the study of mathematics. I hope to carry this curiosity with me in all that I will study in years to come. I would like to specially thank teachers Asher Auel, Jack Petok, David Webb, and Craig Sutton who first introduced me to the world of Geometry and Abstract Algebra and have mentored me in my journey through the subject.

This thesis would not be possible without the advisement and mentorship of Avinash Kulkarni and Jack Petok who aided me, not just in writing this thesis, but in my mathematics education and the obstacles I have encountered along the way. They have been kind and patient as I have struggled through unpacking some of the more complicated subjects in this thesis and have always allowed my curiosity to expand.

Last but not least, I am indebted to my friends and family who believed in me and motivated me to finish this thesis at moments when such a task did not seem possible.

To that effect, I would like to dedicated this thesis to my closest friend, Samuel Gawel, who passed during its composition.

Introduction

The study of cubic fourfolds relates to a number of topics currently being investigated - the rationality problem, algebraic cycles, and hyperkähler varieties. In this thesis, we introduce a new method of orbit enumeration which was used to generate a census of isomoprhism classes of cubic fourfolds over $\mathbb{F}_2$. We additionally utilize this census to enumerate the zeta functions of all smooth cubic fourfolds over $\mathbb{F}_2$.

The census and its results are based on the paper *A census of cubic fourfolds over* $\mathbb{F}_2$ [1]. This thesis will attempt to expand upon some of the ideas necessary for an undergraduate to understand the paper.

In the first chapter, we will explore the new method of efficient orbit enumerations deemed **filtration**. We will review some elementary group theory, to both prove the efficacy of, and understand, this algorithm.

In the next chapter, we will develop the theory needed to understand both the Weil conjectures and the census results. This section serves as a brief introduction to étale cohomology and zeta functions.

In the final chapter we will explore the results of the census using some of the language and theory developed over the two prior chapters.

We will now examine an example which illustrates the central problem being discussed in this thesis.

0.1 Motivating Example

We will consider the problem of enumerating orbits of the action of linear transformations on cubic forms in two variables. Ultimately, this thesis will examine a slightly altered problem, that is, enumerating orbits of cubic forms in six variables (known as cubic fourfolds).

Definition 0.1. A **cubic form** in two variables is the vanishing locus of a homogenous cubic polynomial $f(x) \in \mathbb{F}_2[X, Y]$. That is the vanishing locus of

$$f(x) = aX^3 + bX^2Y + cXY^2 + dY^3$$

with $a, b, c, d \in \mathbb{F}_2$.

In the world of algebraic geometry, we view this equation, not strictly as a polynomial, but as the locus of points which satisfy $f(x) = 0$, known as the **vanishing locus** of $f(x)$ and this will be denoted $V(f(x))$. Suppose we wanted to enumerate all cubic forms and their vanishing loci.

Consider, for example, the cubic form given by $X^3 + Y^3$. This equation has vanishing locus over $\mathbb{F}_2$ given by

$$V(X^3 + Y^3) = \{(0, 0), (1, 1)\}$$

However, all the properties algebraic geometers care about (smoothness, point-counts, etc.) are preserved between cubic forms that are related by linear transformations.

For example, consider the invertible linear transformation

$$M \coloneqq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

We can think of this matrix as acting on the generators $\{X, Y\} \in \mathbb{F}_2[X, Y]$. In this case M will send these to $\{X + Y, Y\}$ and so this will send the cubic form $X^3 + Y^3$ to $X^3 + X^2Y + XY^2$. In this way, the cubic forms of these two polynomials are equivalent by invertible linear transformation and so all the relevant properties an algebraic geometer may care about are preserved. Then our problem of enumerating cubic forms is actually a reduced problem, that is, how can we enumerate cubic forms *up to invertible linear transformation*.

Though initially, this appears to be a problem of smaller scope compared to enumerating cubic forms as a whole, it requires us to consider all the ways in which invertible linear transformations can permute our cubic forms. It is easy to see based on the definition of a cubic form that there are $2^4 = 16$ total cubic forms, but how many *distinct* cubic forms are there (up to linear isomorphism)? Furthermore, how can we quickly find all the distinct forms (up to linear isomorphism)? These questions become increasingly more difficulty as the number of forms increases. For example, homogenous cubic forms in 6 variables have 2^{56} total forms, so answering the question of how many are distinct seems impossible without a complete enumeration over all forms and all invertible linear transformations. We will rephrase this complicated enumeration problem in the world of group theory to find a means to enumerate such cubic forms in a tractable manner.

Contents

Chapter 1

Enumerating Orbits

Section 1.1

Burnside's Lemma

As a general reference for this section, see [3, Part 1].

1.1.1. Group Actions

Definition 1.1. A **group** is an order-pair $(G, \cdot)$, consisting of a set equipped with a binary operation

$$\cdot : G \times G \to G$$

such that the following hold:

(a) $\forall\ g_1, g_2, g_3 \in G$

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3,$$

(b) $\exists\ e \in G$ such that $\forall\ g \in G$

$$e \cdot g = g \cdot e = g,$$

(c) $\forall\ g \in G$ we have $\exists\ g^{-1} \in G$ such that

$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

Definition 1.2. The **order** of a group $(G, \cdot)$ is the cardinality (number of elements) of G as a set, and is denoted $|G|$.

Definition 1.3. A **left group action** of the group $(G, \cdot)$ on a set X is a map

$$\cdot : G \times X \to X$$

such that the following hold:

(a) $\forall\ g_1, g_2 \in G$ and $x \in X$

$$g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x,$$

(b) $\forall\ x \in X$

$$e \cdot x = x.$$

In our example (0.1), we can think of the group as $\mathrm{GL}_2(\mathbb{F}_2)$, that is, the set of 2-by-2 invertible matrices. This a group with the binary operation of matrix multiplication. Note that the invertability criterion is necessary since we require that every element of the group have an inverse.

Furthermore, we can think of $\mathrm{GL}_2(\mathbb{F}_2)$ as acting on our set of cubic forms by left-multiplication of a matrix with the generators $\{X, Y\} \in \mathbb{F}_2[X, Y]$. For example, if we

fix a basis for binary cubics,

$$\mathcal{B} \coloneqq \{e_1 = X^3, e_2 = X^2Y, e_3 = XY^2, e_4 = Y^3\}.$$

Then the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

takes the element X to Y and Y to X and thus maps

$$e_1 \mapsto e_4,\ e_2 \mapsto e_3,\ e_3 \mapsto e_2, \text{ and } e_4 \mapsto e_1.$$

and thus we get an induced matrix on binary cubics with respect to our basis,

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_2).$$

Definition 1.4. For a group $(G, \cdot)$ acting on a set X via $\cdot$, the **orbit** of $x \in X$ is

$$G \cdot x \coloneqq \{g \cdot x \mid g \in G\}.$$

That is, the elements $y \in X$ which can be moved to x via the action of G.

This formalizes our example (0.1) on binary cubic forms, and rephrases our original question. We have now reduced our problem to answering the question of, how many *distinct* orbits are their of $\mathrm{GL}_2(\mathbb{F}_2)$ acting on the space of cubic forms? Furthermore, how can we quickly enumerate orbits of this action?

Since all orbit elements are equivalent up to permutation by the group action, we traditionally pick a representative for each orbit. So in reality our question becomes that of quickly enumerating orbit representatives since, in the context of cubic forms, we only need one element of an orbit to understand all of the elements of the orbit.

We consider a related notion to that of an orbit,

Definition 1.5. The **stabilizer** of an element $x \in X$ is

$$G_x \coloneqq \{g \in G \mid g \cdot x = x\}.$$

That is, elements $g \in G$ which do not affect (stabilize) the element x.

To see the relationship between orbits and stabilizers, consider the aptly named **orbit-stabilizer theorem**.

Theorem 1.6. *(Orbit-Stabilizer Theorem)*
For a group $(G, \cdot)$ acting on a set X via $\cdot$ we have $\forall\ x \in X$

$$|G \cdot x| = \frac{|G|}{|G_x|}.$$

A similar notion to that of a stabilizer is the set $X^g \coloneqq \{x \in X \mid g \cdot x = x\}$. These are related in the sense that

$$\sum_{g \in G} |X^g| = |\{(g, x) \in G \times X \mid g \cdot x = x\}| = \sum_{x \in X} |G_x|.$$

It then follows by the Orbit-Stabilizer Theorem

$$\begin{aligned}\sum_{g\in G}|X^g| &= \sum_{x\in X}|G_x| \\ &= \sum_{x\in X}\frac{|G|}{|G\cdot x|} \\ &= |G|\sum_{x\in X}\frac{1}{|G\cdot x|}.\end{aligned}$$

We will ultimately see a connection between this result and the number of orbits.

1.1.2. Burnside's Lemma

Definition 1.7. The set of orbits is

$$X/G \coloneqq \{G\cdot x \subseteq X \mid x\in X\}.$$

Lemma 1.8. *X is the disjoint union of its orbits, that is $X = \bigsqcup_{U\in X/G} U$.*

Proof. Clearly every element $x \in X$ is in the orbit $G\cdot x \in \bigsqcup_{U\in X/G} U$. We now prove, these orbits are actually disjoint. If $G\cdot x \cap G\cdot x' \neq \emptyset$ then $\exists\ g_1, g_2 \in G$ and $y \in X$ such that

$$g_1\cdot y = x$$

$$g_2\cdot y = x'.$$

Then it follows

$$(g^2\cdot g_1^{-1})\cdot x = g_2\cdot g_1^{-1}\cdot g_1\cdot y = g_2\cdot e\cdot y = g_2\cdot y = x'$$

and thus $G\cdot x \subseteq G\cdot x^{'}$. The opposite inclusion follows a similar argument so $G\cdot x =$

$G \cdot x^{'}$ and all the orbits are disjoint. □

From this it follows that any sum over elements in X can be broken into a summation over elements of each orbit in X/G. Then in our earlier equation we have

$$\begin{aligned}\sum_{g\in G} |X^g| &= |G| \sum_{x\in X} \frac{1}{|G\cdot x|} \\ &= |G| \sum_{U\in X/G} \sum_{x\in U} \frac{1}{|G\cdot x|}.\end{aligned}$$

We note that for any $U \in X/G$ we have that by definition all elements $x \in U$ are part of the same orbit $G \cdot x = U$. Then this reduces to

$$\begin{aligned}\sum_{g\in G} |X^g| &= |G| \sum_{U\in X/G} \sum_{x\in U} \frac{1}{|U|} \\ &= |G| \sum_{U\in X/G} \frac{|U|}{|U|} \\ &= |G| \sum_{U\in X/G} 1 \\ &= |G| \cdot |X/G|.\end{aligned}$$

Then to get the total number of orbits we can manipulate the above result.

Lemma 1.9. *(Burnside's Lemma)*

For a finite group $(G, \cdot)$ acting on a set X, we have

$$|X/G| = \frac{1}{|G|} \sum_{g\in G} |X^g|.$$

1.1.3. Application of Burnside's Lemma

We can apply Burnside's lemma to our motivating example (0.1), but we will develop some tools first to make the computation easier. Naively, one could apply Burnside's

lemma by looking at each element of the group $g \in \mathrm{GL}_2(\mathbb{F}_2)$, and consider which elements in our space our fixed by g. But in general, this require $\mathcal{O}(|G||X|)$ steps for a group G acting on a set X. Instead we would like to find a means to reduce the number of group elements we need to look at. Furthermore, we would like a quick means to evaluate $|X^g|$ for a given group element.

Definition 1.10. For a group G, two group elements $g, h \in G$ are **conjugate** provided that

$$\exists\ s \in G \text{ s.t. } g = s^{-1} \cdot h \cdot s.$$

Lemma 1.11. *If $a, b \in G$ are conjugate, then $|X^a| = |X^b|$.*

Proof. Since a and b are conjugate, there is some element $c \in G$ such that $a = c^{-1} \cdot b \cdot c$. Now if a fixes $x \in X$, we have that

$$x \in X^a \iff a \cdot x = x \iff c^{-1} \cdot b \cdot c \cdot x = x \iff b \cdot (c \cdot x) = (c \cdot x) \iff c \cdot x \in X^b.$$

Then consider the map

$$\begin{aligned} \phi : X^a &\to X^b \\ x &\mapsto c \cdot x \end{aligned}$$

This is well defined by the above argument. To see that these sets have the same cardinality, it suffices to show ϕ is a bijection.

To see injectivity, suppose $\phi(x) = \phi(y)$. Then $c \cdot x = c \cdot y$. It follows, $c^{-1} \cdot c \cdot x = y$, thus $x = y$ and the map is injective.

To see surjectivity, suppose $y \in X^b$. Consider $c^{-1} \cdot y$, for this we have

$$a \cdot (c^{-1} \cdot y) = c^{-1} \cdot b \cdot c \cdot c^{-1} \cdot y = c^{-1} \cdot b \cdot y = c^{-1} \cdot y.$$

Then it follows $c^{-1} \cdot y \in X^a$. Then note that $\phi(c^{-1} \cdot y) = c \cdot c^{-1} \cdot y = y$, and thus the map is surjective. It then follows that $|X^a| = |X^b|$. □

The upshot of Lemma 1.11 is that we need not enumerate every element in G to do our Burnside computation. Instead we only need one element from each collection of elements that are conjugate to one another (known as **conjugacy classes**).

For example, one may have originally thought that to perform a Burnside computation on binary cubic forms would require the fixed points of all 6 elements of $\mathrm{GL}_2(\mathbb{F}_2)$; however, since $\mathrm{GL}_2(\mathbb{F}_2)$ has only 3 conjugacy classes, we need only these 3 fixed point counts to complete our computation. These conjugacy classes are given by representatives:

$$\alpha_1 \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \alpha_2 \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \alpha_3 \coloneqq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

If we let $\mathrm{Cl}(g)$ denote the elements conjugate to $g \in G$, then we have

$$|\mathrm{Cl}(\alpha_1)| = 1 \quad |\mathrm{Cl}(\alpha_2)| = 3 \quad |\mathrm{Cl}(\alpha_3)| = 2$$

This can be seen via the equivalence of $\mathrm{GL}_2(\mathbb{F}_2)$ and the symmetric group on 3 elements (S_3) - this is left as an exercise to the reader. Then by Lemma 1.11 it follows that in our case

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{i=1}^{3} \sum_{g \in \mathrm{Cl}(\alpha_i)} |X^g| = \frac{1}{|G|} \sum_{i=1}^{3} \sum_{g \in \mathrm{Cl}(\alpha_i)} |X^{\alpha_i}| = \frac{1}{|G|} \sum_{i=1}^{3} |\mathrm{Cl}(\alpha_i)||X^{\alpha_i}|.$$

So we need only calculate the number of fixed points for each conjugacy class representative. We could enumerate over all points and check whether or not they are

fixed, but we will use some tools from linear algebra to make our computation more scalable.

Lemma 1.12. *For a representation (see def. 1.16) of V a $\mathbb{F}_p$-vector space*

$$\rho : G \to \mathrm{GL}(V),$$

we denote that vector subspace of null-solutions to $M \in \mathrm{GL}(V)$ as

$$\mathrm{Null}(M) \coloneqq \{x \in V \mid M \cdot v = 0\}$$

and we will denote the identity in $\mathrm{GL}(V)$ by I. Then we have that $\forall\ g \in G$

$$|X^g| = p^{\dim_{\mathbb{F}_p}(\mathrm{Null}(I-\rho(g)))}.$$

Proof. Fix $g \in G$. We note that vectors which are fixed by g have the property that $\forall\ x \in V$, $x - g \cdot x = 0$. We note that this also means $e \cdot x - g \cdot x = 0$ by the definition of a group action. Since G acts via the representation ρ, we have

$$I \cdot x - \rho(g) \cdot x = 0$$

That is, $x \in X^g$ if and only if $x \in \mathrm{Null}(I - \rho(g))$. Then these two sets have the same cardinality. We can quickly calculate the cardinality of $\mathrm{Null}(I - \rho(g))$ by considering that as a vector-space over a finite characteristic field, we simply get all linear combinations of basis elements of $\mathrm{Null}(I - \rho(g))$, that is, each basis element can have p scalars as a coefficient. Then there are $p^{\dim_{\mathbb{F}_p}(\mathrm{Null}(I-\rho(g)))}$, total linear combinations giving the desired result. □

Then by the above, to enumerate the orbits in our example we need to find the

dimension of the nullspace of $I - \rho(\alpha_i)$, where $\rho : \mathrm{GL}_2(\mathbb{F}_2) \to \mathrm{GL}_4(\mathbb{F}_2)$ is given by $\rho(M)(p(X,Y)) = p(M \cdot X, M \cdot Y)$. We can quickly find the dimension of the nullspace of a matrix by finding its rank when converted to row-echelon form. We will compute the example for α_2 and the remaining cases are left as an exercise.

Note, α_2 acts by taking $X \mapsto Y$ and $Y \mapsto X$. We fix an ordered basis for our vector-space of cubic forms as follows

$$\mathcal{B} = \{e_1 \coloneqq X^3, e_2 \coloneqq X^2Y, e_3 \coloneqq XY^2, e_4 \coloneqq Y^3\}.$$

Then we have that for a general cubic form $ae_1 + be_2 + ce_3 + de_4 \in V$

$$\rho(\alpha_2)(ae_1 + be_2 + ce_3 + de_4) = ae_4 + be_3 + ce_2 + de_1.$$

and in the chosen basis this transformation is given by the matrix

$$\rho(\alpha_2) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then taking $I - \rho(\alpha_2)$ and row-reducing, we get the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which is of rank 2. Then in this case we have that $|X^{\alpha_2}| = 2^2 = 4$ Similarly one can

compute $|X^{\alpha_1}| = 1$ and $|X^{\alpha_3}| = 4$. Putting all our results together we have that

$$|V/G| = \frac{1}{|G|}\sum_{i=1}^{3}|\mathrm{Cl}(\alpha_i)||X^{\alpha_i}| = \frac{1}{6}(1\cdot 1 + 3\cdot 4 + 2\cdot 4) = \frac{36}{6} = 6.$$

This tells us that we have 6 total distinct orbits - a much smaller number than our 16 total cubic forms in our space. In our case, this is a small enough set of orbits to do a complete manual enumeration; however, a larger space, such as that of cubic forms in 6 variables, has roughly 3.7 million orbits, a far more daunting task. In the next section we will examine standard methods of enumeration as well as a new method which can, in certain cases, perform faster than current enumeration methods.

Section 1.2

Efficient Enumeration of Orbits

1.2.1. Naive Enumeration

Burnside's Lemma is useful for knowing how many orbits exist under a group action, but to actually calculate a representative for each orbit we need another method. Naievely, one could calculate orbits as follows:

Algorithm 1 Naive Enumeration

```
1: procedure NaiveEnum(G, X)
2:     reps ← {}
3:     for x ∈ X do
4:         new_rep ← true
5:         for g ∈ G do
6:             if gx ∈ reps then
7:                 new_rep ← false
8:             end if
```

```
        end for
        if new_rep == true then
            reps.push(x)
        end if
    end for
end procedure
```

This method involves looking over every element of the acted upon set X, and seeing if any group element permutes the element to an already discovered orbit by checking if gx is already a found representative $\forall\ g \in G$. This implies that we have,

Lemma 1.13. *The naive orbit enumeration algorithm has $\mathcal{O}(|X|\cdot|G|)$ time complexity (where $\mathcal{O}$ is "Big-O" notation).*

1.2.2. Union-Find

However, this algorithm makes no use of new information gained other than the found representatives. To save steps in our algorithm, we can instead associate every element with the orbit it is contained in by mapping it to a representative. Thus, if we are trying to see if x is a new representative, we can see if for any $g \in G$, if gx has *ever* been found, thus reducing the number of checks needed. This algorithm is known as **union find** and requires that we first create an orbit representation. In our case, we will represent orbits via an associative array. This will map an element to a single representative of its orbit. Then, to find the list of representatives of the group action we need only look at the set of values in key-pairs of this hash map. We implement the actual enumeration as follows:

Algorithm 2 Union-Find Enumeration

```
procedure UFEnumerate(G, X)
    reps ← {}                                   ▷ create associative array
```

```
3:    for x ∈ X do                                  ▷ initialize array
4:        reps[x] ← null
5:    end for
6:    for x ∈ X do
7:        if reps[x] == null then                   ▷ G · x not yet enumerated
8:            for g ∈ G do                          ▷ enumerate G · X
9:                reps[gx] ← x
10:           end for
11:       end if
12:   end for
13:   return reps                                   ▷ return representatives array
14: end procedure
```

This algorithm begins by initializing our associative array and marking that no orbits have been explored via a *null* value. We then traverse our set, each time we find an element with an unenumerated orbit (say x), we associate every element $gx \in G \cdot x$ with the representative x. In this way, when we come across another element of $G \cdot x$ later in our search, we wont enumerate this orbit since it will have been marked as enumerated (not *null*).

Lemma 1.14. *The union find orbit enumeration algorithm has time-complexity*

$$\mathcal{O}(|G| \cdot |X/G|) = \mathcal{O}(|X| \cdot \mathbb{E}_{x \in X}|G_x|),$$

where $\mathbb{E}$ *denotes the expected value.*

Proof. It is clear that the dominant runtime component of `UFEnumerate` is in lines 6-12. This section loops over elements of X, and for every *new* orbit, will loop over elements of G. Since this loop does nothing when $x \in X$ is not in a new orbit, we are

effectively looping over G for each orbit in X/G. This has time-complexity

$$\mathcal{O}(|G| \cdot |X/G|).$$

Then by Lemma 1.9 we have that $|G| \cdot |X/G| = \sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|$. We then have

$$\sum_{x \in X} |G_x| = |X| \left(\frac{\sum_{x \in X} |G_x|}{|X|} \right) = |X| \left(\sum_{x \in X} \frac{|G_x|}{|X|} \right) = |X| \cdot \mathbb{E}_{x \in X} |G_x|$$

Thus giving our desired result. □

We can see that this is significantly faster than naive orbit enumeration in most cases. In the *worst* case, where G acts trivially, each stabilizer is the size of the whole group and $\mathbb{E}_{x \in X} |G_x| = |G|$, meaning that at worst it is only as bad as naive enumeration.

There are, however, ways that we can exploit the structure of the group action to gain even more signicant speed-ups. Lemma 1.14 tells us that if we can restrict either the size of the group or the set we are enumerating then we will have a decrease in running time. We can use this property to break down our orbit enumeration into smaller problems, to ultimately reconstruct a full set of orbit representatives in even smaller time-complexity than union-find.

1.2.3. Linear Group Actions

In our filtration algorithm, we will be using the structure of a vector space and its subsets which are invariant under the group action to try and gain a speed-up over the union-find enumeration. However, we must first consider the additional structure which a vector space provides (addition and scalar multiplication), and how this interacts with a group action.

Definition 1.15. A **linear group action** is a group action which preserves the additive and scalar structure of a vector space. That is, if $(V, +, \cdot)$ is a k-vector space and $(G, \cdot)$ is a group which acts on V, we say the action is linear provided that

(a) $\forall\ v, w \in V\ g \in G$ we have $g \cdot (v + w) = g \cdot v + g \cdot w$

(b) $\forall c \in k\ v \in V$ and $g \in G$ we have $g \cdot (c \cdot v) = c \cdot (g \cdot v)$

Definition 1.16. A **representation** of a group $(G, \cdot)$ is a group homomorphism

$$\rho : G \to \mathrm{GL}(V)$$

where $(V, +, \cdot)$ is a k-vector space, and $(\mathrm{GL}(V), \circ)$ is the general linear group of invertible linear transformations on V. Note that $\mathrm{GL}(V)$ acts linearly on V by evaluation of a linear transformation.

Lemma 1.17. *A representation $\rho : G \to \mathrm{GL}(V)$ induces a linear group action*

$$\begin{aligned} \cdot : G \times V &\to V \\ (g, v) &\mapsto \rho(g)(v) \end{aligned}$$

Furthermore, a linear group action by $(G, \cdot)$ induces a representation

$$\begin{aligned} \rho_G : G &\to \mathrm{GL}(V) \\ g &\mapsto q_g \end{aligned}$$

where

$$\begin{aligned} q_g : V &\to V \\ v &\mapsto g \cdot v \end{aligned}$$

Proof. These claims follow directly from the definitions. If ρ is a linear representation, then ρ associates each element of G with a linear transformation on V. Thus it is clear that $\forall\ c \in k$, $v, w \in V$, and $g \in G$, since $\rho(g)$ is a linear transformation

$$\rho(g)(c \cdot v + w) = c \cdot \rho(g)(v) + \rho(g)(w)$$

by linearity.

Similarly, if G acts linearly on V, then the map

$$\begin{aligned} q_g : V &\to V \\ v &\mapsto g \cdot v \end{aligned}$$

is linear by the definition of a linear group action. Furthermore, we have that $\forall$ $r, s \in G$

$$\rho_G(r \cdot s) = q_{r \cdot s}.$$

But note that $\forall\ v \in V$ we have

$$q_{r \cdot s}(v) = (r \cdot s) \cdot v = r \cdot (s \cdot v) = q_r(q_s(v)) = (q_r \circ q_s)(v)$$

Then $q_{r \cdot s} = q_r \circ q_s$ and the map ρ_G is a group homomorphism and thus a linear representation. □

In this way, linear group actions and representations are really the same since we can always recover one from the other. That is, all linear group actions really just act via a subgroup of $\mathrm{GL}(V)$. When we talk about group actions on vector spaces, we generally restrict to linear group actions (or representations) so for this section our group action is assumed to be a linear one. We note that this still fits within our

motivating example since we were already considering our group to be the set of all invertible linear transformations on $\mathbb{F}_2$.

1.2.4. Filtration

We now illustrate a means to reduce the problem of orbit enumeration to smaller subgroups and subspaces.

Definition 1.18. Let V be a k-vector space and $W \subseteq V$ a vector subspace. Define the equivalence relation $\sim_W$ on V by the condition that $\forall\ r, s \in V$

$$r \sim_W s \iff r - s \in W$$

Then the **quotient space** of V and W is $V/\sim_W$ (denoted V/W).

One can see that V/W is a smaller space than V. In fact, one can show that

$$\dim(V/W) = \dim(V) - \dim(W)$$

thus, if W is a particularly large space, we expect it to be far easier to enumerate orbits in V/W than V. In fact, However, there is one caveat; if a group action G can permute an element in $w \in W$ to an element $g \cdot w \notin W$ outside of W, then for the canonical quotient map

$$\pi : V \to V/W$$
$$v \mapsto [v]$$

we have that $\pi(w) = [0]$, but $\pi(g \cdot w) \neq [0]$. Since we have that group actions preserve the identity, it is clear that in this case we cannot recover information about our original orbits by examining the images of orbits under π. Instead, let us examine

a situation where this can be done.

Definition 1.19. Let G be a group which acts linearly on a k-vector space V. A vector subspace $W \subseteq V$ is G-**invariant** provided that

$$G \cdot W = \{g \cdot w \in W \mid g \in G, w \in W\} = W.$$

That is to say, G acts as a bijective permutation on the subset W.

We note that when $W \subseteq V$ is a G-invariant subspace, we have that $\forall\ g \in G$ and $v \in V$

$$g\pi(v) = g \cdot (v + W) = g \cdot v + g \cdot W = g \cdot v + W = \pi(g \cdot v).$$

Then we get an induced group action on V/W by

$$\begin{aligned} \cdot : G \times V/W &\to V/W \\ (g, [v]) &\mapsto [g \cdot v]. \end{aligned}$$

and this will be well-defined, unlike in the case where W is not G-invariant.

Lemma 1.20. *Let V be a k-vector space, acted upon by a group G. If $W \subseteq G$ is a G-invariant subspace, then for the canonical quotient map $\pi : V \to V/W$, we have*

$$V/G = \bigsqcup_{O \in (V/W)/G} \pi^{-1}(O)/G.$$

That is, we can recover V/G from the inverse image of orbits in $(V/W)/G$.

Proof. By the definition of the induced G action on V/W it is clear π must take

G-orbits in V to orbits in V/W, so we get an induced map

$$\tilde{\pi} : V/G \to (V/W)/G$$
$$G \cdot x \mapsto G \cdot \overline{x}$$

By the surjectivity of π it follows

$$V/G = \tilde{\pi}^{-1}((V/W)/G) = \bigsqcup_{O \in (V/W)/G} \tilde{\pi}^{-1}(O).$$

But note that $\forall\ O \in V/G$

$$\tilde{\pi}^{-1}(O) = \{G \cdot x \in V/G \mid G \cdot \overline{x} \subseteq O\} = \{x \in V \mid \overline{x} \in O\}/G = \pi^{-1}(O)/G.$$

□

We can see that when $W \subseteq V$ is a G-invariant subspace we actually can find a correspondence between orbits in V and orbits in V/W (a much simpler space to enumerate). To provide insight on how this correspondence can actually be used to enumerate orbits, consider

Lemma 1.21. *Let V be a k-vector space, acted upon by a group G. If $W \subseteq V$ is a G-invariant subspace, then for the canonical quotient map $\pi : V \to V/W$, we have if $\overline{v}$ is a representative for $O \in (V/W)/G$*

$$\psi : (v + W)/G_{\pi(v)} \to \pi^{-1}(O)/G$$
$$G_{\pi(v)} \cdot (v + w) \mapsto G \cdot (v + w)$$

is a bijection

Proof. We first show that $G \cdot (v + w)$ is actually in $\pi^{-1}(O)/G$. Consider $v + w \in v + W$.

Then $\pi(v+w) = \pi(v) = \overline{v} \in O$ by supposition. Then $G \cdot (v+w) \in \pi^{-1}(O)/G$ and the map is well-defined.

To see that ψ is injective, suppose $\psi(G_{\pi(v)}(v+w)) = \psi(G_{\pi(v)}(v+w'))$. Then $G \cdot (v+w) = G \cdot (v+w')$, so $\exists\ g \in G$ with $g \cdot (v+w) = (v+w')$. But then it follows that

$$g(v+W) = g(v+w+W) = g(v+w) + W = v + w' + W = v + W$$

Then $g \in G_{\pi(v)}$ so $g \cdot (v+w) = (v+w')$ means that $G_{\pi(v)} \cdot (v+w) = G_{\pi(v)} \cdot (v+w')$.

To see that ψ is surjective, fix $G \cdot s \in \pi^{-1}(O)/G$. Then $s \in \pi^{-1}(O)$ means $s+W \in O$. Then since $v+W$ is a representative for O, we know $\exists\ g \in G$ with $g \cdot (s+W) = (v+W)$. Then g maps $s+W$ to $v+W$ so we have $\exists\ v+w \in v+W$ such that $g \cdot s = v+w$. This means that $\psi(G_{\pi(v)}(v+w)) = G \cdot (v+w) = G \cdot s$. □

This result shows us that the representatives of orbits in $(v+W)/G_{\pi(v)}$ are the same as the representatives of orbits in $\pi^{-1}(O)/G$

Then in summary we have bijections:

$$\begin{array}{ccc} V/G & \longleftrightarrow & \bigsqcup_{O \in (V/W)/G} \pi^{-1}(O)/G \\ & & \Big\updownarrow \psi \\ & & \bigsqcup_{G \cdot \overline{v} \in (V/W)/G} (v+W)/G_{\pi(v)} \end{array}$$

This tells us that to enumerate orbits in V/G its actually sufficient to enumerate orbits in $\bigsqcup_{G \cdot \overline{v} \in (V/W)/G} (v+W)/G_{\pi(v)}$. Then we can break up our orbit enumeration problem into a much smaller one. First we must enumerate orbits in $(V/W)/G$. Once we have done this, then for each representative of orbits in $(V/W)/G$ (say $G \cdot \overline{v}$), we

can enumerate the orbits in $(v+W)/G_\pi(v)$. Then the total set of orbit representatives given by each of these enumerations will actually be the full set of orbit representatives of V/G. For the following algorithm, let $W_0 = 0$, then we have:

Algorithm 3 Filtration Enumeration

1: **procedure** Filter($G, 0 = W_0/W_0 \subseteq W_1/W_0 \subseteq \dots W_n/W_0 = V, d = 0$)
2: $reps_V \leftarrow \{\}$
3: **if** $d == n-1$ **then**
4: `return UFEnum`$(G, W_n/W_{n-1})$
5: **else**
6: $reps_{(W_n/W_{d+1})} \leftarrow$ `Filter`$(G, W_{d+1}/W_{d+1} \subseteq W_{d+2}/W_{d+1} \subseteq \dots W_n/W_{d+1}, d+1)$
7: **end if**
8: **for** $\overline{x} \in reps_{(W_n/W_{d+1})}$ **do**
9: $reps_V.push($`UFEnum`$(G_{(x+W_{d+1})}, x + W_{d+1}))$
10: **end for**
11: `return` $reps_V$
12: **end procedure**

There is one caveat that must be addressed. In this algorithm, it is assumed that we know $G_{(x+W_{d+1})}$. However, this is actually not a problem since our original `UFEnum` algorithm can be modified to calculate these stabilizers at no additional running time cost. To do this we simply perform a check when enumerating an orbit to see whether $gx = x$ for a given fixed x. As we range over G, this will allow us to concatenate elements of G_x. This will ultimately provide us with all of the stabilizers needed for our computation as they can be calculated along with the representatives recursively.

Now we consider how this compares to union find.

Lemma 1.22. *The filtration orbit enumeration algorithm for a single filtration ($W \subseteq$*

V) has time-complexity bounded by

$$\mathcal{O}(|V/W/G| \cdot |W/G| \cdot |G|).$$

Proof. We first note that the dominant runtime steps are in lines 8-10 whereas all others represent a single orbit enumeration via `UFEnum`. By Lemma 1.14 we know that that runtime of line 9 will have runtime $\mathcal{O}(|G_{\overline{x}}| \cdot |(x+W)/G_{\overline{x}}|)$, for each $\overline{x} \in reps_{V/W}$. This means that lines 8-10 will have runtime complexity of

$$\mathcal{O}\Big(\sum_{\overline{x} \in reps_{V/W}} |G_{\overline{x}}| \cdot |(x+W)/G_{\overline{x}}|\Big)$$

Then it suffices to show that

$$\sum_{\overline{x} \in reps_{V/W}} |G_{\overline{x}}| \cdot |(x+W)/G_{\overline{x}}| \leq \sum_{\overline{x} \in reps_{V/W}} |G| \cdot |W/G|$$

since then our runtime will be bounded by

$$\mathcal{O}\Big(\sum_{\overline{x} \in reps_{V/W}} |G| \cdot |W/G|\Big) = \mathcal{O}(|V/W/G| \cdot |W/G| \cdot |G|)$$

as desired.

We will show that sufficient condition term-wise. That is, fix $\overline{x} \in V/W$. We want to show

$$|G_{\overline{x}}| \cdot |(x+W)/G_{\overline{x}}| \leq |G| \cdot |W/G|$$

then by Burnside's lemma, this holds iff

$$\sum_{g \in G_{\overline{x}}} |(x+W)^g| \leq \sum_{g \in G} |W^g|$$

and since $\sum_{g\in G_{\overline{x}}} |W^g| \leq \sum_{g\in G} |W^g|$ it suffices to show

$$\sum_{g\in G_{\overline{x}}} |(x+W)^g| \leq \sum_{g\in G_{\overline{x}}} |W^g|$$

Again, we will show this term-wise. That is, fix $g \in G_{\overline{x}}$ and we want to show

$$|(x+W)^g| \leq |W^g|$$

To do this we will define an injection between these two sets.

In the case $|(v+W)^g| = 0$ it is clearly bounded by $|W^g| \geq 0$.

Otherwise, we can fix $z \in (x+W)^g$, that is $g \cdot z = z$. Also, note that $z = x + w$ for some $w \in W$, so we have

$$|(z+W)^g| = |(x+w+W)^g| = |(x+W)^g|$$

So an injection defined on $z + W$ will suffice to show our result. Now let

$$\begin{aligned} \tau_z : (z+W)^g &\to W^g \\ (z+w) &\mapsto (z+w) - z = w. \end{aligned}$$

We note that if $g(z+w) = z+w$, then we have

$$\begin{aligned} g(w) - w &= z - z + g(w) - w \\ &= g(z) - z + g(w) - w \text{ since } g(z) = z \\ &= g(z+w) - (z+w) \quad \text{by linearity} \\ &= 0 \qquad\qquad\qquad\quad \text{by assumption.} \end{aligned}$$

Then w is, in fact, in W^g and the map is well-defined. Also, the map is clearly injective as it is just translation-by-z. Then we have that $|(z+W)^g| \leq |W^g|$, thus giving our desired result. □

The upshot of Lemma 1.22, is that filtration, at its worst, is just as bad as union find. As noted in the proof, the actual runtime of filtration is proportional to

$$\sum_{\overline{x} \in reps_{V/W}} |G_{\overline{x}}| \cdot |(x+W)/G_{\overline{x}}| \leq \sum_{\overline{x} \in reps_{V/W}} |G| \cdot |(x+W)/G_{\overline{x}}| = |G| \cdot \sum_{\overline{x} \in reps_{V/W}} |(x+W)/G_{\overline{x}}|$$

Then by Lemma 1.21 we have that this is

$$|G| \cdot |V/G|$$

which is the runtime of union find orbit enumeration over V. However, there is also a more useful interpretation of our runtime bound in Lemma 1.22. A runtime bound of $\mathcal{O}(|V/W/G| \cdot |W/G| \cdot |G|)$ tells us that our algorithm runs like a union find over W performed $|V/W/G|$ times. This makes sense since our algorithm performs a union find over the fiber of each orbit representative in $V/W/G$ so this bound seems fitting for the nature of the algorithm.

Chapter 2

Calculating Zeta Functions

Section 2.1

Cubic Fourfolds

Now equipped with the powerful tool of filtration, we can begin to enumerate problems involving group orbits which were once thought intractable (at least on a personal computer). As mentioned, up to linear isomorphism, all the relevant properties of algebraic varieties are preserved, thus it makes sense to ask questions of the orbit representatives of cubic forms under linear isomorphism in order to answer questions about the behavior of cubic forms in generality.

A particular class of cubic forms which long sat at the outskirts of computable enumeration was that of the **Cubic Fourfold** - the zero locus of a cubic form in six variables. Of prime interest will be understanding the **Zeta Function**s of these objects. These zeta functions have a deep connection to the cohomology of their associated fourfolds and concisely store much of the information about cubic fourfolds which is of interest to us; however, understanding these zeta functions require a fairly comprehensive understanding of algebraic geometry, homological algebra, generating functions, and a number of other topics often not discussed in an undergraduate math

education. So we begin by providing a brief refresher on the basics of algebraic geometry to help define the nature of Cubic Fourfolds, as well as the scope of the problem we are discussing.

Remark 2.1. Unlike the chapter on orbit enumeration, this chapter cannot be explained from the ground up without delving into topics out of the scope of this thesis. For this reason, the reader is assumed to have an introductory knowledge of (in no particular ordering of importance):

(a) (Co)Homology (Singular, De Rham, etc.),

(b) Multivariable Calculus,

(c) Abstract Algebra,

(d) Metric Spaces,

(e) Galois Theory,

(f) Linear Algebra.

It is worth noting, however, that although the reader is assumed to have some knowledge of these topics, to actually enumerate zeta functions of cubic fourfolds only requires a means to counts points of a variety as well as a bit of linear algebra. Readers strictly interested in the computation methods and the results of the census may want to skip this chapter as it is just meant to provide sufficient background to understand the results. For the sake of brevity, some definitions may be altered than what you may see in a textbook or course on the various topics discussed. This is intended to keep the narrative of information as linear as possible without introducing extraneous concepts. Where definitions differ, they are generally either a

diluted version of the full definition or an equivalent definition which is more useful for the concepts presented. The topics discussed here are intended to be roughly the bare minimum required to understand the cohomology groups of a cubic fourfold and their importance. For this reason, many topics will be covered in shallow detail simply to give the reader the impression of the roadmap one might take on their course to understanding the Weil Conjectures. With this goal of understanding the Weil conjectures we will need to cover a great deal of mathematical tools and objects. With this intended purpose, we have:

(a) The first section will cover generating functions and I-adic metrics. This is intended to give the reader an understanding of the ring in which zeta functions and cohomology groups are defined.

(b) The next section will cover homological algebra. This is intended to give the reader an understanding of what we mean when we say a "cohomology group".

(c) The next section will cover sites. This is intended to give the reader an understanding of the cohomology theory used in the Weil Conjectures.

(d) Finally, our last section will use all these tools to formalize and understand the Weil Conjectures which tells us how we can actually compute something about these intricately defined cohomology groups.

2.1.1. Projective Varieties

As a general reference for this section, see [7, Chapter 6]. In the interest of keeping our varieties compact, we will instead consider varieties over projective space, in which points at infinity collapse into a single point. To create this identification, we define

Definition 2.2. The projective line over the finite field $\mathbb{F}_q$ is

$$\mathbb{P}^1_q := (\mathbb{F}^2_q - \{(0,0)\})/\sim$$

where $a \sim b$ if and only if $a = \lambda b$ for some $\lambda \in \mathbb{F}_q^\times$

In this space, we have that $(1:1) = (2:2)$ (assuming $\text{char}(\mathbb{F}_q) \neq 2$). Then this reduces to a one-dimensional space which looks like $\mathbb{F}_q$ with a single point added at infinity. We note that in this space it is no longer well-defined to take the vanishing locus of an arbitrary polynomial

Example 2.3. In $\mathbb{P}^1_5$, we have that

$$f(X) = X - 1$$

has that $f(1:1) = 0$ and $f(2:2) = 1 \neq 0$, yet $(1:1) = (2:2)$.

To resolve this we, only consider homogenous polynomials. This is because for a homogenous polynomial of degree d we have

$$f(\lambda a) = \lambda^d f(a)$$

Then if $f(a) = 0$, any scalar multiple of a will also be a zero of the polynomial, thus giving us a well-defined zero locus for this polynomial. Thankfully in the case of cubic fourfolds, these are all homogenous so we will be considering cubic fourfolds as being defined over $\mathbb{P}^5_2$. This leads us to define,

Definition 2.4. A **Cubic Fourfold** is the vanishing locus of a projective, homogenous cubic in six variables.

Section 2.2

I-adic Metric Spaces

As a general reference for this section, see [5, Page 55-56]. In order to understand Zeta functions of a variety, we will need to become comfortable with a number of

topological spaces that behave quite differently than many classical examples. This section will consider the ring in which we define zeta functions as well as the base field of the vector spaces in the cohomology of a cubic fourfold. Consider the I-adic Metric

Definition 2.5. Let R be a ring. For an ideal $I \subseteq R$, such that $\cap_{n\in\mathbb{N}} I^n = (0)$, the **$I$-adic metric** is

$$\begin{aligned} \mu : R \times R &\to \mathbb{R}_{\geq 0} \\ (x, y) &\mapsto 2^{-\sup\{n\in\mathbb{N} \mid x-y \,\in\, I^n\}} \end{aligned}$$

That is, the inverse base two exponentiation of the largest natural number such that $x - y$ is in the n-th power of the ideal I. We also assert that, in this case, $2^{-\infty} = 0$

Lemma 2.6. *For a ring R and ideal $I \subseteq R$ such that $\cap_{n\in\mathbb{N}} I^n = (0)$, the I-adic metric is an ultrametric.*

Proof. (a) Fix $x \in R$. Then since $(0) = (x - x) = \cap_{n\in\mathbb{N}} I^n$, it follows that $\forall\ n \in \mathbb{N}$ that $x - x \in I^n$. Then

$$d(x, x) = 2^{-\sup\{n\in\mathbb{N} \mid x-x \,\in\, I^n\}} = 2^{-\infty} = 0$$

(b) Fix $x, y \in R$ such that $d(x, y) = 0$. Then we must have

$$\sup\{n \in \mathbb{N} \mid x - y \ \in \ I^n\} = \infty$$

That is, $\forall\ n \in \mathbb{N}$ we have $x - y \in I^n$. Thus $x - y \in (0) = \cap_{n\in\mathbb{N}} I^n$. Thus we conclude $x - y = 0$ and so $x = y$.

(c) We note that if $x - y \in I^n$ for some $n \in \mathbb{N}$, then so is $-1 \cdot (x - y) = y - x$ so

symmetry of the metric follows.

(d) Fix $x, y, z \in R$ we want to show $d(x,z) \leq \max(d(x,y), d(y,z))$.
If $x - y \in I^n$ and $y - z \in I^n$, then since I^n is an ideal, $x - z \in I^n$, then we must have that $d(x,z)$ is always at most $d(x,y)$ or $d(y,z)$, so

$$d(x,z) \leq \max(d(x,y), d(y,z))$$

□

The I-adic metric is particularly useful in the case of principal ideal domains. This is because every ideal has the form (q) for some $q \in R$ and in this metric definition, successive powers of q vanish. More formally,

Lemma 2.7. *In the (q)-adic metric, the sequence q^n converges to 0.*

Proof. We have that $\forall\ i \in \mathbb{N}$

$$d(q^i, 0) = 2^{-\sup\{n \in \mathbb{N} \mid q^i \in (q^n)\}} = 2^{-i}$$

since the largest power of the ideal (q) containing q^i is the i-th power. Then clearly this sequence converges to 0. □

2.2.1. Generating Functions

For further discussion of this section, see [10, Chapter 4]. Courses in analysis often consider convergent sequences of polynomials like Taylor expansions, but generally this is considered convergent in the standard Euclidean metric where we evaluate the function pointwise and examine its convergence as a real-number sequence.
Instead, we can think of the set of polynomial functions over a ring R (which we will assume is a unique factorization domain) more generally as $R[X]$. That is, the

free R-module we get by adjoining $\{1, X, X^2, \dots\}$. In this space, (X) is an ideal; moreover, we have that

$$\cap_{n\in\mathbb{N}}(X^n) = (0)$$

since polynomials always have finite degree. Then we can define an (X)-adic metric, as

$$\begin{aligned}\nu : R[X] \times R[X] &\to \mathbb{R}_{\geq 0} \\ (x, y) &\mapsto 2^{-\sup\{n\in\mathbb{N} \mid x-y \in (X^n)\}}\end{aligned}$$

We can think of this as the inverse base two exponentiation of the largest number for which the polynomials x and y differ. Suppose $x, y \in R[X]$ are such that the largest term up to which they agree is of degree 2, then their distance in this metric would be $\nu(x, y) = 2^{-2} = \frac{1}{4}$.

As in our previous lemma, we have that in this metric the sequence $(X^n)_{n\in\mathbb{N}} \in R[X]$ converges to 0.

Now equipped with a metric, we can consider the metric completion of the space $R[X]$ which we will denote $R[[X]]$ and is called the **ring of formal power series**. In this space it makes sense to consider the convergence of functions which may not converge in the Euclidean sense, but will converge to some polynomial in our completion. *This is the ring in which the zeta function is defined.* This space really consists of equivalence classes of cauchy sequences in our metric space. In this way, we can think of an element in $R[[X]]$ as an infinite sequence of polynomials, where elements take the form

$$\sum_{i=0}^{\infty} a_i X^i \in R[[X]]$$

Multiplication and addition are defined as multiplication and addition on the terms of the cauchy sequence.

Example 2.8. Consider the formal power series $f(X) = 1+X+X^2+\ldots$, $g(X) = 1-X \in R[[X]]$. We then have

$$\begin{aligned} f(X) \cdot g(X) &= (1 + X + X^2 + \ldots) \cdot (1 - X) \\ &= (1 + X + X^2 + \ldots) - (X + X^2 + \ldots) = 1 \end{aligned}$$

Then $f(X)$ is invertible with inverse $g(X)$. Then we can denote

$$\frac{1}{1-X} = 1 + X + X^2 + X^3 + \ldots$$

This is to say that the rational polynomials in X, whose denominators are coprime with X, are actually a subring of our formal power series ring.

Naturally, one might ask when these elements converge to a rational funtion in $R[[X]]$. In this space, an element is invertible whenever the constant term a_0 is invertible in R. The question of what form these rational functions take is more complicated.

Lemma 2.9. *Let $f(X) = a_0 + a_1X + a_2X + \ldots$ be a formal power series. Then $f(X)$ is a rational function of X whose denominator has degree at most d (when written in lowest terms) if and only if the sequence $\{a_i\}_{i=0}^{\infty}$ satisfies a linear recurrence of degree at most d.*

Proof.

$\Rightarrow$) Suppose $f(X) = \frac{h(X)}{g(X)}$ where $\gcd(h, g) = 1$ and $\deg(h) = n_h$ and $\deg(g) = n_g \leq d$. We will write

$$h(X) = \sum_{i=0}^{n_h} b_i X^i \text{ and } g(X) = \sum_{i=0}^{n_g} c_i X^i$$

Then

$$\begin{aligned} & f(X) \cdot g(X) = h(X) \\ \Rightarrow & \sum_{i=0}^{\infty} a_i X^i \cdot \sum_{i=0}^{n_g} c_i X^i = \sum_{i=0}^{n_h} b_i X^i \\ \Rightarrow & \sum_{i=0}^{\infty} d_i X^i = \sum_{i=0}^{n_h} b_i X^i \text{ where } d_i = \sum_{\alpha+\beta=i} c_\alpha a_\beta \end{aligned}$$

Then when $i \geq n_g$, all d_i's reduce to

$$d_i = a_i c_0 + a_{i-1} c_1 + \ldots a_{i-n_g} c_{n_g}$$

Then if $i \geq \max(n_f, n_g)$, we must have each d_i equates with a zero term in $h(X)$ so in particular,

$$d_i = a_i c_0 + a_{i-1} c_1 + \ldots a_{i-n_g} c_{n_g} = 0$$

Since $g(X)$ is invertible, we know that c_0 is a unit. Then

$$a_i = -\frac{c_1}{c_0} a_{i-1} - \cdots - \frac{c_{n_g}}{c_0} a_{i-n_g}$$

which is a linear recurrence of degree $n_g \leq d$ and holds for all subsequent terms.

$\Leftarrow$) Suppose $a_n = \sum_{i=0}^{r} c_i a_{n-i}$ with $r \leq d$. Then we have that adding together terms

$$f(X) - c_1 X f(X) - c_2 X^2 f(X) - \cdots - c_r X^r f(X) = a_0 + \cdots + (a_n - \sum_{i=0}^{r} c_i a_{n-i}) X^n + \ldots$$

$$\Rightarrow f(X)(1 - c_1 X - c_2 X^2 - \cdots - c_r X^r) = h(X)$$

for some finite degree $n-1$ polynomial since the higher order terms are cancelled out

by the linear recurrence in their coefficients. Then it follows

$$f(X) = \frac{h(X)}{(1 - c_1X - c_2X^2 - \cdots - c_rX^r)}$$

which has denominator $r \leq d$. □

Example 2.10. Consider the Fibonacci sequence $a_0 = 0$, $a_1 = 1$, and $a_n = a_{n-1} + a_{n-2}$ for $n > 1$. This function clearly satisfies a linear recurrence of degree 2. Then we expect the formal sum $f(X) = \sum_{i=0}^{\infty} a_nX^n$ converges to a rational function with denominator of degree 2 when written in lowest form. The recurrence tells us that as in our proof of Lemma 2.9 we should consider the polynomial

$$f(X)-XF(X)-X^2f(X) = a_0+(a_1-a_0)X+(a_2-(a_1+a_0))X^2\cdots+(a_n-(a_{n-1}+a_{n-2}))X^n+\ldots$$

but by our linear recurrence this tells us

$$(1 - X - X^2)f(X) = X$$

meaning that

$$f(X) = \frac{X}{1 - X - X^2}$$

a rational function whose denominator is degree 2.

Furthermore, one can use the quadratic formula to calculate the roots of the denominator:

$$\phi = \frac{1 + \sqrt{5}}{2} \text{ and } \tau = \frac{1 - \sqrt{5}}{2}.$$

Then we have

$$\frac{X}{1 - X - X^2} = \frac{1}{(1 - \phi X)(1 - \tau X)} = \frac{A}{1 - \phi X} + \frac{B}{1 - \tau X}$$

for some $A, B \in \mathbb{R}$. We then have

$$\frac{X}{1-X-X^2} = \frac{A(1-\tau X)+B(1-\phi X)}{1-X-X^2} = \frac{(A+B)-(A\tau+B\phi)X}{1-X-X^2}.$$

This means that $(A+B) = 0$ and $(A\tau + B\phi) = -1$, so $A = \frac{1}{\sqrt{5}}$ and $B = -\frac{1}{\sqrt{5}}$. Plugging this into our equation, we gets

$$f(X) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\phi X} - \frac{1}{1-\tau X}\right).$$

But each component in this summation is a rational function which some geometric sequence converges to. That is,

$$f(X) = \sum_{i=0}^{\infty} a_i X^i = \frac{1}{\sqrt{5}}\left(\sum_{i=0}^{\infty}(\phi X)^i - \sum_{i=0}^{\infty}(\tau X)^n\right).$$

Finally, equating coefficients, we have

$$a_n = \frac{1}{\sqrt{5}}(\phi^n - \tau^n).$$

In this example, we can see that formal sums which converge to rational functions have the property that their coefficients can be recovered in a closed-form expression from their rational function.

This example also provides inside on how one can calculate the rational function to which a formal sum converges. In particular, note that

Lemma 2.11. *If $f(X) = \sum_{i=0}^{\infty} b_i X^i \in R[[X]]$ is a rational function of the form $\frac{h(X)}{g(X)}$ with*

$$\deg(g) < \deg(h) \leq d, \ (gcd)(h,g) = 1 \text{ and } \gcd(g, X) = 1$$

then $g(X)$ and $h(X)$ can be determined from, at most, the first $2d$ coefficients of $f(X)$.

Proof. Write $h(X) = r_0 + r_1 X + \dots r_n X^n$ and $g(X) = 1 + s_1 X + \dots s_m X^m$ (we assume without loss of generality that the denominator has normalized constant coefficient since it is invertible so we can always divide out by the first term). Then

$$\begin{aligned} & f(X) \cdot g(X) = h(X) \\ \Rightarrow & \sum_{i=0}^{\infty} d_i X^i = \sum_{i=0}^{m} s_i X^i \text{ where } d_i = \sum_{\alpha+\beta=i} r_\alpha b_\beta \end{aligned}$$

Then

$$d_0 = r_0,\, d_1 = r_1,\, \dots,\, d_{2d} = r_{2d}$$

This gives us linear equations

$$\begin{aligned} & b_0 = r_0, \\ & b_0 s_1 + b_1 = r_1, \\ & \vdots, \\ & b_0 s_n + b_1 s_{n-1} + \dots + a_n = r_n, \text{ and} \\ & d_k = 0 \;\forall\; k > n \end{aligned}$$

Since $\gcd(h, X) = 1$, we know that s_0 is non-zero, and thus we can divide by s_0 in our first equation and recursively solve for the terms in terms of the knowns b_i. In general, this system of equations need not be solvable, but the criteria that $\gcd(g, h) = 1$ means that this system is necessarily solvable (CITE?). Since there are at most $2d$ unknowns, and we have $2d$ distinct linear equations, this will give us all the necessary coefficients to solve for the rational equation. □

This construction assumed that h and g are of maximally allowed degree, but in general, we can solve for these rational functions knowing only $\deg(g) + \deg(h)$ coefficients of the formal power series. We will later see that since the coefficients of the zeta function of a fourfold are given by the point counts over various finite fields, this tells us not only how to compute the numerator and denominator of our zeta function, but also how many point counts are required to do so.

2.2.2. p-adic Integers

Similar to our construction of generating functions, we will define the space of p-adic integers and rationals as the metric completion of the (p)-adic metric in $\mathbb{Z}$ and $\mathbb{Q}$ respectively. More information on the p-adic rationals, and an alternate construction, can be found at [11, Example 1.4.3].

Definition 2.12. The p-adic integers (resp. rationals) are the completion of the space $\mathbb{Z}$ (resp. $\mathbb{Q}$) with respect to the (p)-adic metric (and in the case of rationals its extension to the field of fractions) and it is denoted $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$).

That is, just like our formal power series, we have that an element of $\mathbb{Q}_p$ has, for some $k \in \mathbb{Z}$, the form

$$\sum_{i=k}^{\infty} a_i p^i \text{ with } a_i < p$$

Just as in our formal power series ring, addition and multiplication are defined on points in the sequences.

The p-adic space of integers and rationals will be used in defining the cohomology groups of a cubic fourfold used in the Weil conjectures.

Section 2.3

Homological Algebra

As a general reference for this section, see [11, Chapters 2,23] and [6, Chapter 1]. Homology theory is at the heart of many fields of math. Underlying the theory is the seemingly simple concept of **exact-sequence**.

Definition 2.13. An **exact-sequence** in an abelian category $\mathcal{C}$ is a sequence of objects $G_0, \dots G_n \in \text{obj}(\mathcal{C})$ along with morphisms $f_i : G_{i-1} \to G_i \in \hom(\mathcal{C})$ such that the diagram

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \dots \xrightarrow{f_n} G_n$$

preserves $\text{im}(f_i) = \ker(f_{i+1})$ at each arrow.

Exact sequences provide a quick means to talk about the properties of morphisms, for example, the sequence

$$0 \xrightarrow{d_1} A \xrightarrow{d_2} B$$

is exact $\iff$ $\text{im}(d_1) = \ker(d_2)$, $\iff$ $0 = \ker(d_2)$, $\iff$ d_2 is injective. Similarly, the sequence

$$A \xrightarrow{r_1} B \xrightarrow{r_2} 0$$

is exact $\iff$ r_1 is surjective. Properties like these make exactness a quick means of identifying isomorphisms or chains of isomorphisms. We would hope that as covariant functors preserve the shape and commutativity of diagrams, that they would also preserve exactness, but in general this is not true.

Definition 2.14. Let

$$0 \longrightarrow A \xrightarrow{f_1} B \xrightarrow{f_2} C \longrightarrow 0$$

be an arbitrary exact-sequence in $\mathcal{C}$ an abelian category. A covariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ to $\mathcal{D}$ an abelian category, is said to be

(a) (**left-exact**) provided that

$$0 \longrightarrow \mathcal{F}(A) \xrightarrow{\mathcal{F}(f_1)} \mathcal{F}(B) \xrightarrow{\mathcal{F}(f_2)} \mathcal{F}(C)$$

is exact in $\mathcal{D}$.

(b) (**right-exact**) provided that

$$\mathcal{F}(A) \xrightarrow{\mathcal{F}(f_1)} \mathcal{F}(B) \xrightarrow{\mathcal{F}(f_2)} \mathcal{F}(C) \longrightarrow 0$$

is exact in $\mathcal{D}$.

(c) (**exact**) provided that

$$0 \longrightarrow \mathcal{F}(A) \xrightarrow{\mathcal{F}(f_1)} \mathcal{F}(B) \xrightarrow{\mathcal{F}(f_2)} \mathcal{F}(C) \longrightarrow 0$$

is exact in $\mathcal{D}$.

These definitions give us a means by which can describe how a functor fails to be exact. We will see a classic example of a functor which fails to be exact, but in doing so tells us a great deal of information about the structure of the object we are examining.

2.3.1. Sheaf Cohomology

Presheaves and Sheaves. For this subsection more information can be found at [11, Chapter 2].

Definition 2.15. For a topological space X, the category Top($\mathbf{X}$) is the category

whose objects are open sets $U \subseteq X$ and whose arrows are inclusions between open sets $V \subseteq U$ ($V \overset{i}{\hookrightarrow} U$).

Definition 2.16. An **$\mathcal{S}$-valued presheaf** is a contravariant functor on the category $\mathrm{Top}(X)$

$$\mathcal{P} : \mathrm{Top}(X) \to \mathcal{S}$$

we denote $res_{V,U} : \mathcal{P}(U) \to \mathcal{P}(V) \coloneqq \mathcal{P}(V \overset{i}{\hookrightarrow} U)$. We also call elements in $\mathcal{P}(U)$ **sections** of the presheaf at U.

Example 2.17. The functor $\mathcal{P}$ which takes open sets in $U \subseteq \mathbb{R}$ to functions $\mathcal{P}(U) = \{f : U \to \mathbb{R} \mid |f| < \infty\}$ and has for $V \subseteq U$ that

$$\begin{aligned} res_{V,U} : \mathcal{P}(U) &\to \mathcal{P}(V) \\ (f : U \to \mathbb{R}) &\mapsto (f|_V : V \to \mathbb{R}) \end{aligned}$$

is a presheaf which takes values in the ring of bounded real functions.

Presheaves are essentially just a functor, but we would like more structure to be able to more deeply relate the topological space we are examining to the value category of our presheaf.

Definition 2.18. An **$\mathcal{S}$-valued sheaf** is a presheaf $\mathcal{F}$ on (X, τ) such that

(a) (Locality) $\forall\, U \in \tau$ and $\{U_i\}_{i \in I} \subseteq \tau$ an open cover of U, and objects $x, y \in \mathcal{F}(U)$, if $res_{U_i,U}(x) = res_{U_i,U}(y)\ \forall\ i \in I$, then $x = y$,

(b) (Gluability) $\forall\, U \in \tau$ and $\{U_i\}_{i \in I} \subseteq \tau$ an open cover of U, and sections $\{x_i \in \mathcal{F}(U_i)\}_{i \in I}$, if

$$res_{U_i \cap U_j, U}(x_i) = res_{U_i \cap U_j, U}(x_j)\ \forall\ i, j \in I,$$

then there exists a global section $x \in \mathcal{F}(U)$ such that

$$res_{U_i}(x) = x_i \ \forall \ i \in I.$$

The locality axiom tells us that if two sections agree on an open cover then they must be the same section. The gluability axiom, on the other hand, tells us that when a family of sections defined on each set of an open cover agree on the intersections of the open cover, then we can "glue" them all together to form one global section which restricts to each section in the family.

Example 2.19. Consider our earlier example of the presheaf of bounded functions on $\mathbb{R}$. This is not an actual sheaf since we can find a family of bounded functions which cannot be glued into a global bounded function. To see this, consider the identity function defined on $(n, n+2) \subseteq \mathbb{R} \ \forall \ n \in \mathbb{N}$. This is a family of bounded functions, but clearly there is no bounded function which is bounded on all of $\mathbb{R}$ but is locally the identity everywhere.

Example 2.20. On the other hand, we can take the presheaf which has sections that are continuous functions on $\mathbb{R}$, that is

$$\begin{aligned} \mathcal{F} : (\mathbb{R}, \tau_{euc}) &\to \mathbf{Ab} \\ U &\mapsto \{f : U \to \mathbb{R} \mid f \text{ is continuous}\} \end{aligned}$$

It turns out that this is an actual sheaf. That is, we can always glue a family of continuous functions together into a global continuous function.

Definition 2.21. The **Global Sections Functor** is a functor on the category of sheaves which returns global sections of that sheaf for some set $U \subseteq X$. It is denoted

$$\Gamma(U, \mathcal{F}) \coloneqq \mathcal{F}(U)$$

Clearly the global sections operation is a functor in the U component, but it is also a functor in the $\mathcal{F}$ component. That is, a functor which takes us from the category of sheaves to their value categories. Naturally, one asks what the category of sheaves actually is. In this category, the objects are sheaves, and the morphisms are maps between sheaves $r : \mathcal{F} \to \mathcal{F}^{'}$, such that $\forall\ (V \overset{i}{\hookrightarrow} U)$ with $V, U \in (X, \tau)$, we have maps $r_U : \mathcal{F}(U) \to \mathcal{F}^{'}(U)$ and $r_V : \mathcal{F}(V) \to \mathcal{F}^{'}(V)$, such that

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{r_U} & \mathcal{F}^{'}(U) \\ \downarrow{\scriptstyle \mathcal{F}(i)} & & \downarrow{\scriptstyle \mathcal{F}^{'}(i)} \\ \mathcal{F}(V) & \xrightarrow{r_V} & \mathcal{F}^{'}(V) \end{array}$$

commutes.

To define the global sections functor, we also need to stipulate how it acts on morphisms between sheaves. Given a morphism of sheaves $r : \mathcal{F} \to \mathcal{F}^{'}$, we have $\Gamma(X, -)$ acts on this morphism via

$$\Gamma(X, r) \coloneqq (r_X : \mathcal{F}(X) \to \mathcal{F}^{'}(X))$$

One means to turn a sheaf into something in its value category is by applying it to an open set (taking the global sections functor). Alternately, we can consider a collection

Definition 2.22. For an $\mathcal{S}$-valued sheaf on (X, τ), we have that the **stalk** at $x \in X$ is

$$\mathcal{F}_x = \{(U, s) \mid x \in U \in \tau \text{ and } s \in \mathcal{F}(U)\}/\sim,$$

where $(U, s) \sim (U^{'}, t) \iff \exists\ U^{''} \subseteq U \cap U^{'}$ open s.t. $x \in U^{''}$ and $s|_{U^{''}} = t|_{U^{''}}$. The elements $[(U, s)] \in \mathcal{F}_x$ are called **germs**.

We can think of $\mathcal{F}_x$ as an object in $\mathcal{S}$ centered around x. For example, if $\mathcal{F}$ takes values in the category of abelian groups, then $\mathcal{F}_x$ can be thought of as an abelian group where the group operation is performed locally around x. This is allowed since we can compare two germs since we can always restrict to a common open set around x where both are defined and group operations occur over the same group.
We note that a morphism of sheaves

$$r : \mathcal{F} \to \mathcal{F}^{'}$$

induces a morphism on stalks in the value category for $x \in X$

$$r_x : \mathcal{F}_x \to \mathcal{F}_x^{'}$$
$$[(U, s)] \mapsto [U, r_U(s)]$$

We will think of our sheaves from here on out as being valued in the category of abelian groups, making the definitions of injective and surjective morphisms on groups clear. This leads us to the following definition:

Definition 2.23. A morphism of sheaves $r : \mathcal{F} \to \mathcal{F}^{'}$ is injective (resp. surjective) provided that the induced map on stalks $r_x : \mathcal{F}_x \to \mathcal{F}^{'}$ is injective (resp. surjective) $\forall\ x \in X$.

Lemma 2.24. *A morphism of sheaves $r : \mathcal{F} \to \mathcal{F}^{'}$ is injective if and only if for each $U \in \tau$ the map $r_U : \mathcal{F}(U) \to \mathcal{F}^{'}(U)$ is injective.*

Proof.
$\Leftarrow$) Suppose $\forall\ U \in \tau$, $r_U : \mathcal{F}(U) \to \mathcal{F}^{'}(U)$ is injective. Fix $x \in X$ and consider the

map

$$r_x : \mathcal{F}_x \to \mathcal{F}_x^{'}$$
$$[U, s] \mapsto [U, r_U(s)]$$

Fix $[U, s], [V, t] \in \mathcal{F}_x$ such that

$$r_x([U, s]) = [U, r_U(s)] = [V, r_V(t)] = r_x([V, t]).$$

Then there exists a neighborhood of x, $W_x \subset U \cap V$ such that

$$r_{W_x}(s) = r_U(s)|_{W_x} = r_V(t)|_{W_x} = r_{W_x}(t).$$

Then, by injectivity of r_{W_x} we must have $[U, s] = [V, t]$.
$\Rightarrow$) Suppose $\forall\ x \in X$ that $r_x : \mathcal{F}_x \to \mathcal{F}_x^{'}$ is injective. Fix $U \in \tau$, we want to show that $r_U : \mathcal{F}(U) \to \mathcal{F}^{'}(U)$ is injective. Then fix $s, t \in \mathcal{F}(U)$ such that $r_U(s) = r_U(t)$. Then clearly,

$$[U, r_U(s)] = [U, r_U(t)] \text{ in } \mathcal{F}_x^{'}$$

for all $x \in U$. Then by injectivity of r_x, we must have $[U, s] = [U, t]$ in $\mathcal{F}_x$. Then $\exists$ $V \subseteq U \cap U = U$ open such that $x \in V$ and $s|_V = t|_V$. Then since this holds for all $x \in U$, by locality, $s = t$ on U. $\square$

Equipped with our understanding of injections and surjections, it makes sense to talk about how the global sections functor $\Gamma(X, -)$ acts on exact sequences. That is, consider a short-exact-sequence of sheaves

$$0 \xrightarrow{d_0} \mathcal{F}^{'} \xrightarrow{d_1} \mathcal{F} \xrightarrow{d_2} \mathcal{F}^{''} \xrightarrow{d_3} 0.$$

then we get an induced diagram

$$0 \xrightarrow{d_0(X)} \Gamma(X, \mathcal{F}') \xrightarrow{d_1(X)} \Gamma(X, \mathcal{F}) \xrightarrow{d_2(X)} \Gamma(X, \mathcal{F}'') \xrightarrow{d_3(X)} 0.$$

We would like to know to what extent is this diagram exact. This question can be separated into the questions:

(a) (left-exact) Does $\Gamma(X, -)$ take injective maps to injective maps? Let

$$0 \xrightarrow{d_0} \mathcal{F}' \xrightarrow{d_1} \mathcal{F} \xrightarrow{d_2} \mathcal{F}'' \xrightarrow{d_3} 0.$$

be an exact sequence of sheaves. We claim that

$$0 \xrightarrow{d_0(X)} \Gamma(X, \mathcal{F}') \xrightarrow{d_1(X)} \Gamma(X, \mathcal{F}) \xrightarrow{d_2(X)} \Gamma(X, \mathcal{F}'')$$

is exact, that is, $\mathrm{im}(d_1(X)) = \ker(d_2(X))$. By Lemma 2.24 it suffices to ask if the sequence on stalks

$$0 \xrightarrow{d_{0_x}} \mathcal{F}'_x \xrightarrow{d_{1_x}} \mathcal{F}_x \xrightarrow{d_{2_x}} \mathcal{F}''_x$$

is exact $\forall\ x \in X$. But since to be injective is to be injective on stalks, this is clear.

(b) (right-exact) Does $\Gamma(X, -)$ take surjective maps to surjective maps? To show the global sections functor was left-exact, we used the fact that injective sheaf morphisms are injective on open sets; however, such a property does not hold for surjections. Consider the sequence of sheaves

$$\mathcal{O}^{hol} \xrightarrow{exp} (\mathcal{O}^{hol})^{\times} \longrightarrow 0$$

where $\mathcal{O}^{hol}$ is the sheaf on $\mathbb{C}$ taking an open set to holomorphic functions on that set, and $(\mathcal{O}^{hol})^\times$ is a sheaf on $\mathbb{C}$ taking open sets to holomorphic functions on that set which are invertible (non-zero). Then exponential map for $U \in \tau$ is given by

$$exp(U) : \mathcal{O}^{hol}(U) \to (\mathcal{O}^{hol})^\times(U)$$
$$(f : U \to \mathbb{C}) \mapsto (e^f : U \to \mathbb{C})$$

We note that the exp map is surjective on stalks. That is, for $x \in \mathbb{C}$ we have

$$exp_x : {\mathcal{O}^{hol}}_x \to {(\mathcal{O}^{hol})^\times}_x$$
$$[U, f] \mapsto [U, e^f]$$

is surjective since any exponential around a non-zero complex point can be lifted locally via the logarithm map. However, $exp(x)$ is certainly not surjective since no global logarithm exists. To see this we note that $0 \neq 2\pi i$ but $e^0 = e^{2\pi i}$ so we must have $log(0) = log(2\pi i)$ and the function is not globally well defined (hence why we use branch cuts is complex analysis). This tells us that in general we cannot expect that the global sections functor is right-exact.

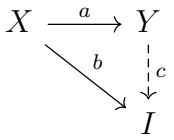
In order to reconcile this issue, we will introduce cohomology, a tool for correcting the inexactness of exact sequences under $\Gamma(X, -)$.

2.3.2. Cohomology of $\Gamma(X, -)$

This section will explain how we can resolve the inexactness of our global sections functor, more information can be found at [11, Chapter 23], [6, Chapter 1], and [4, Chapter III Part 1].

Definition 2.25. For an abelian category $\mathcal{C}$ an object $I \in \text{obj}(\mathcal{C})$ is **injective** pro-

vided that $\forall$ injective maps $a : X \to Y$, and maps $b : X \to I$, we have that there exists a unique map $c : Y \to I$ such that



commutes.

Definition 2.26. For an abelian category $\mathcal{C}$ an **injective resolution** of $X \in \text{obj}(\mathcal{C})$ is an exact-sequence

$$0 \longrightarrow X \longrightarrow I_1 \longrightarrow I_2 \longrightarrow \dots$$

where each I_i is injective.

Definition 2.27. An abelian category $\mathcal{C}$ has **enough injectives** provided that $\forall$ $X \in \text{obj}(\mathcal{C})$, $\exists$ an injective $I \in \text{obj}(\mathcal{C})$ and an injective map $f : X \to I$.

We would hope that with enough injectives, we can always find an injective resolution. To see this, note

Lemma 2.28. *An abelian category $\mathcal{C}$ with enough injectives always has an injective resolution for any $X \in \text{obj}(\mathcal{C})$.*

Proof. Fix $X \in \text{obj}(\mathcal{C})$. We will show inductively that we can always make a sequence of length $n \in \mathbb{N}$ of injectives.
($n = 1$) This is clear since we have sufficient injectives we get an exact sequence

$$0 \longrightarrow X \longrightarrow I_1$$

for some $I_1 \in \text{obj}(\mathcal{C})$.

($n > 1$) We assume by hypothesis that there is a sequence of injectives

$$0 \longrightarrow X \longrightarrow I_1 \longrightarrow \dots I_{n-2} \xrightarrow{d_{n-2}} I_{n-1}$$

Since $\mathcal{C}$ has sufficient injectives, we know that there is an injective I_n such that the map $g_{n-1} : I_{n-1}/\mathrm{im}(d_{n-2}) \to I_n$ is injective, then pre-composing with the quotient map $q_{n-1} : I_{n-1} \to I_{n-1}/\mathrm{im}(d_{n-2})$, we get a map $(q_{n-1} \circ g_{n-1}) \coloneqq d_{n-1} : I_{n-1} \to I_n$ which continues the resolution as desired. □

Then for a left-exact functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ of abelian categories with sufficient injectives, we have that for any $X \in \mathrm{obj}(\mathcal{C})$, the sequence

$$0 \longrightarrow X \longrightarrow I_1 \longrightarrow \dots$$

induces a (not necessarily exact) sequence given by cutting out X from our sequence and applying $\mathcal{F}$

$$0 \xrightarrow{\mathcal{F}(d_0)} \mathcal{F}(I_1) \xrightarrow{\mathcal{F}(d_1)} \mathcal{F}(I_2) \xrightarrow{\mathcal{F}(d_2)} \dots$$

Lemma 2.29. *Consider the induced map on sections of $\mathcal{F}$ of an injective resolution,*

$$0 \xrightarrow{\mathcal{F}(d_0)} \mathcal{F}(I_1) \xrightarrow{\mathcal{F}(d_1)} \mathcal{F}(I_2) \xrightarrow{\mathcal{F}(d_2)} \dots$$

Then for $i = 0, 1, \dots$ we have that $\mathrm{im}(\mathcal{F}(d_i)) \subseteq \ker(\mathcal{F}(d_{i+1}))$

Proof. Since our original sequence

$$0 \longrightarrow X \longrightarrow I_1 \longrightarrow \dots$$

is exact, we have that $\mathrm{im}(d_i) = \ker(d_{i+1})$, then anything in the image of d_i is annihilated by d_{i+1}, so $d_{i+1} \circ d_i = 0$. Then after applying $\mathcal{F}$, we get $\mathcal{F}(d_{i+1} \circ d_i) = 0$,

thus

$$\mathcal{F}(d_{i+1}) \circ \mathcal{F}(d_i) = 0,$$

Thus anything in the image of $\mathcal{F}(d_i)$ is annihilated by $\mathcal{F}(d_{i+1})$ so the result follows. □

Then we can define our cohomology groups via

Definition 2.30.

$$H^i(\mathcal{F}) \coloneqq \ker(d_{i+1})/\mathrm{im}(d_i) \text{ for } i = 0, 1, \ldots$$

It may seem that there is an issue of well-definedness, that is, it seems like our definition of $H^i(\mathcal{F})$ depended on the choice of injective resolution, but it turns out that this definition is independent of choice ([12, Theorem 2.2.6], [4, Theorem III.1.1A]) and so there is a single group which can be used to resolve all failures to be exact for a particular sheaf. In particular, for our global sections functor, we will denote for $i = 0, 1, \ldots$

$$H^i(X, -) \coloneqq H^i(\Gamma(X, -)).$$

It can be shown that this is exactly the next step in our sequence which failed to be right-exact that can continue the sequence while preserving exactness. That is, for our original exact sequence of sheaves

$$0 \longrightarrow \mathcal{F}' \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}'' \longrightarrow 0$$

we get an induced long exact sequence on cohomology groups

$$0 \longrightarrow H^0(X, \mathcal{F}') \longrightarrow H^0(X, \mathcal{F}) \longrightarrow H^0(X, \mathcal{F}'') \longrightarrow H^1(X, \mathcal{F}') \longrightarrow \ldots.$$

Note that this construction is not specific to our global sections functor and in general, any left-exact functor has derived cohomology groups (provided it has enough injectives) that allow us to convert short exact sequences in one abelian category into long exact sequences in the target category of the functor (see [11, Page 52] for more details).

Example 2.31. Consider $H^0(X, \mathcal{F})$ for some sheaf on X. Consider any injective resolution

$$0 \longrightarrow X \longrightarrow I_1 \longrightarrow \dots$$

which, after applying $\mathcal{F}$ a left-exact functor, becomes

$$0 \longrightarrow \mathcal{F}(X) \longrightarrow \mathcal{F}(I_1) \longrightarrow \mathcal{F}(I_2) \longrightarrow \dots.$$

which will also be exact. Then we have an identification between $\mathrm{im}(\mathcal{F}(X) \to \mathcal{F}(I_1))$ and $\ker(\mathcal{F}(I_1) \to \mathcal{F}(I_2))$. Since any injective function is a bijection onto its image, we have an isomorphism

$$\mathcal{F}(X) \cong \ker(\mathcal{F}(I_1) \to \mathcal{F}(I_2))$$

Then it follows that

$$\mathcal{F}(X) \cong \ker(\mathcal{F}(I_1) \to \mathcal{F}(I_2))/0 \cong \ker(\mathcal{F}(I_1) \to \mathcal{F}(I_2))/\mathrm{im}(0 \to \mathcal{F}(I_1)) = H^0(X, \mathcal{F})$$

That is, the zero-th cohomology given by this derived functor is really just the global sections functor (up to isomoprhism). This tells us that our long exact sequence induced by a short exact sequence of sheaves has the first three groups given by the respective global sections of the sheaves. That is,

$$0 \longrightarrow \Gamma(X, \mathcal{F}') \longrightarrow \Gamma(X, \mathcal{F}) \longrightarrow \Gamma(X, \mathcal{F}'') \longrightarrow H^1(X, \mathcal{F}') \longrightarrow H^1(X, \mathcal{F}) \longrightarrow \dots$$

is exact. That is, this is exactly the extension we desired to make this global sections sequence exact.

Section 2.4

Étale Cohomology

As a general reference for this section, see [6, Chapter 1, Sections 1-10]. In Algebraic Geometry, introductory classes will often teach of a new topology known as the **Zariski Topology** in which open sets are defined as the complements of vanishing loci of functions; however, one can see this is a very coarse topology, since most vanishing loci are small we would expect open sets to be very large. In a sense, this makes local properties less useful than spaces where we can get open sets which "close in" on a point. For this reason, we will consider a wider class than topologies.

Sites. For more details about this section see, [6, Chapter 1, Section 5]. In this new "topology", we will transition from thinking of open sets to instead thinking of coverings, and instead of inclusions between open sets we will think of maps between coverings.

Just as in a topology, we require relationships hold between subsets, we will want specific relationships to hold between covers, but first, we must define,

Definition 2.32. Let $\mathcal{C}$ be a category and let $f : A \to C$ and $g : B \to C$ be morphisms. Then the **fibre product** of A and B (over f and g) is the unique object $D \in \text{obj}(\mathcal{C})$ (provided it exists), together with morphisms $\pi_1 : D \to A$ and

$\pi_2 : D \to B$ such that

$$\begin{array}{ccc} D & \xrightarrow{\pi_1} & B \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

commutes, that is $\pi_1 \circ f = \pi_2 \circ g$. We often denote $A \times_C B \coloneqq A \times_{f,g} B \coloneqq (D, \pi_1, \pi_2)$.

Equipped with this categorical fiber product, we can now introduce,

Definition 2.33. A **site** is an ordered pair $(\mathcal{C}, cov(\mathcal{C}))$ such that $\mathcal{C}$ is a category and $cov(\mathcal{C})$ is a collection such that

(a) (Isomorphism) if $f : V \to U$ is an isomorphism, then

$$f \in cov(\mathcal{C}),$$

(b) (Locality) If $U \in \text{obj}(\mathcal{C})$ and $\{\phi_i : U_i \to U\}_{i \in I} \in cov(\mathcal{C})$, and $\{\phi_{ij} : U_{ij} \to U_i\}_{j \in I_i} \in cov(\mathcal{C})$, we have that

$$\{\phi_{ij} \circ \phi_i : U_{ij} \to U\}_{(i,j) \in \prod_{i \in I} i \times I_i} \in cov(\mathcal{C})$$

(c) (Base Change) If $\{U_i \to U\}_{i \in I} \in cov(\mathcal{C})$, and we have a morphism $f : V \to U$ in $\mathcal{C}$, we have that $U_i \times_U V$ exists, and

$$\{U_i \times_U V \to V\}_{i \in I} \in cov(\mathcal{C})$$

The isomorphism property tells us of the simplest types of coverings, that is, coverings where these set effectively covers itself (up to isomorphism). The locality condition tells us that a covering of a covering is a covering. Finally, the base change criterion tells us that given a morphism $V \to U$ we can change our covering from a covering of U to a covering of V.

2.4.1. Étale Topology

For this section, definitions can be found in the *Stacks Project* [9]. For more information on the subject see, [6, Chapter 1, Sections 2-7,9]. In fact, our homology construction will be slightly more refined than this, but requires even more tools to define. Consider,

Definition 2.34. A ring map $f : R \to S$ is of **finite presentation** provided that for some $n \in \mathbb{N}$ and $\{f_1, \ldots, f_m\} \in R[x_1, \ldots, x_n]$,

$$R[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle \cong S$$

as R-algebras where the R-algebra structure of S is given by f.

Definition 2.35. A morphism of schemes $(f, f^{\#}) : (X, \mathcal{O}_x) \to (S, \mathcal{O}_s)$ is of **locally finite presentation** provided that $\forall\ x \in X$, there are affine open sets $U \subseteq X$ and $V \subseteq S$ with $f(U) \subseteq V$ such that induced ring map

$$f^{\#} : \mathcal{O}_S(V) \to \mathcal{O}_X(U)$$

is of finite presentation.

Definition 2.36. For B an A-module, B is said to be **flat**, provided that

$$- \otimes_A B : Mod_A \to Mod_A$$

is an exact functor.

Then we say,

Definition 2.37. A map of rings $f : A \to B$ is **flat** if B is flat as an A-module where the module structure is induced by f.

Definition 2.38. A morphism of schemes $(f, f^{\#}) : (X, \mathcal{O}_X) \to (S, \mathcal{O}_S)$ is said to be **flat** provided that $\forall\ p \in X$, the induced map on schemes

$$f_p^{\#} : \mathcal{O}_{S,f(p)} \to \mathcal{O}_{X,p}$$

is flat as a ring map.

Then we have that

Definition 2.39. A morphism of schemes $(f, f^{\#}) : (X, \mathcal{O}_X) \to (S, \mathcal{O}_S)$ is **unramified** provided that it is of locally finite presentation and, $\forall\ x \in X$ and $s = f(x)$, we have that for $\mathfrak{m}_x$ and $\mathfrak{m}_s$ the maximal ideals of local rings $\mathcal{O}_{X,x}$ and $\mathcal{O}_{S,s}$ respectively.

(a) The residue field $k(x) \cong \mathcal{O}_{X,x}/\mathfrak{m}_x$ is a separable algebraic extension of $k(y) \cong \mathcal{O}_{S,s}/\mathfrak{m}_s$.

(b) $\mathfrak{m}_s \cdot \mathcal{O}_{X,x} = \mathfrak{m}_x$, that is, the extension of the ideal $\mathfrak{m}_s$ is $\mathfrak{m}_x$.

Finally, we have that

Definition 2.40. A morphism of schemes $(f, f^{\#}) : (X, \mathcal{O}_X) \to (S, \mathcal{O}_S)$ is an **étale morphism** provided that it is flat and unramified.

Example 2.41. A map $\phi : \mathbb{A}^n \to \mathbb{A}^n$ for affine spaces over k a field with $\text{char}(k) = 0$ is étale if, $\forall\ p \in \mathbb{A}^n$, it satisfies the jacobian condition that

$$\det(\frac{\partial \phi_i}{\partial x_j}(p)) \neq 0$$

This can be found in [11, Definition 12.6.2] and [6, Corollary 2.2]. In the case of differential geometry, this means that the map is locally invertible at each point by the inverse function theorem (see [8, Page 35 Theorem 2-11]).

It is not true in general that étale morphisms are local isomorphims as in the case of differential geometry; however, étale morphisms capture the idea of being "close" to a local isomorphism. Formally, an étale morphism in characteristic 0 is a local homeomorphism after a base change to the algebraic completion of the source and the target - hence the unramified condition (see [4, Page 275, Exercise 10.4]).

We would like to define a similar notion of sheaves but instead of the sheaf being defined on the poset of a topological space, instead we will define it on the étale site with inclusions given by morphisms between étale maps. That is,

Definition 2.42. For two étale morphisms with the same target,

$$(\phi_U, \phi_U^{\#}) : (U, \mathcal{O}_U) \to (X, \mathcal{O}_X) \text{ and } (\phi_V, \phi_V^{\#}) : (V, \mathcal{O}_V) \to (X, \mathcal{O}_X),$$

a **mapping between étale morphisms** is defined as a morphism of ringed spaced

$$(f, f^{\#}) : (U, \mathcal{O}_U) \to (V, \mathcal{O}_V)$$

such that the diagrams

$$\begin{array}{ccc} U & \xrightarrow{\phi_U} & X \\ & \searrow^{f} & \uparrow{\scriptstyle \phi_V} \\ & & V \end{array}$$

and

$$\begin{array}{ccc} \phi_{U*}\mathcal{O}_U & \xleftarrow{\phi_U^{\#}} & \mathcal{O}_X \\ & \nwarrow^{f^{\#}} & \downarrow{\scriptstyle \phi_V^{\#}} \\ & & \phi_{V*}\mathcal{O}_V \end{array}$$

commute.

Definition 2.43. The category $X_{\text{ét}}$ is the category whose objects are étale morphims with target $(X, \mathcal{O}_X)$, and arrows are mappings between étale morphisms.

Further, consider

Definition 2.44. An **étale cover** of an étale morphism $(\phi, \phi^{\#})$ is a surjective morphism between étale morphisms, with target $(\phi, \phi^{\#})$. We denote all étale covers in $X_{\text{ét}}$ as the collection $\text{Ét}(X)$.

Putting these together, we have a site,

Definition 2.45. The small **Étale site** (**Étale Topology**) of a scheme $(X, \mathcal{O}_X)$ is $(X_{\text{ét}}, \text{Ét}(X))$.

We claim this is a site, that is

Theorem 2.46. *For a scheme $(X, \mathcal{O}_X)$, we have $(X_{\acute{e}t}, \acute{E}t(X))$ is a site*

Proof. See Milne [6, Proposition 2.11]. □

The étale site is exactly the space we will be defining our cohomology groups over for the Weil Conjectures.

2.4.2. ℓ-adic Sheaf

An étale sheaf is really just a sheaf as we had defined it before, but now the objects are étale morphism with ordering given by the above maps.

Then it makes sense to consider the following étale sheaf,

Definition 2.47. Assume X is an irreducible variety. Then the **the constant sheaf with value** $\mathbb{Z}/\ell\mathbb{Z}$ is the sheaf $\underline{\mathbb{Z}/\ell\mathbb{Z}}$ is the sheaf

$$\begin{aligned} \underline{\mathbb{Z}/\ell\mathbb{Z}} : X_{\text{ét}} &\to \mathbf{Ab} \\ (\phi_U : (U, \mathcal{O}_U) \to (X, \mathcal{O}_X)) &\mapsto \mathbb{Z}/\ell\mathbb{Z} \\ (f : U' \to U) &\mapsto id_{\mathbb{Z}/\ell\mathbb{Z}} \end{aligned}$$

Note that we employ a condition of irreducibility since otherwise this need not be a sheaf. A constant presheaf may have constant values on each component but not satisfy gluability since we cannot find a global constant function which takes more than one value.

Our entire homological algebra construction will still hold with étale sheaves since they functionally satisfy the same conditions, that is, having enough injectives (see [6, Pages 8,12,61-63]). Similarly, we can construct a derived functor for the global sections functor of our our étale sites, which we will denote

$$H^i_{\text{ét}}(X, \mathbb{Z}/\ell\mathbb{Z}) \coloneqq H^i(X_{\text{ét}}, \underline{\mathbb{Z}/\ell\mathbb{Z}})$$

Further,

Definition 2.48. The étale cohomology group of ℓ-adic integers is

$$H^i_{\text{ét}}(X, \mathbb{Z}_\ell) = \varprojlim_n (H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z}))$$

This is a colimit of groups in the categorical sense. Keep in mind that this is *not* the same thing as the étale cohomology with the constant ℓ-adic sheaf (see [6, Page 123]); however, even though we are not taking the limit with respect to the sheaf, it does turn out that for projective, smooth varieties (where $\ell \neq \text{char}(k)$), we have that $H^i_{\text{ét}}(X, \mathbb{Z}_\ell) = \mathbb{Z}_\ell^m$ for some $m \in \mathbb{N}$ (see [6, Theorem 19.2]). This means that the ℓ-adic cohomology really does take values in the ℓ-adic integers for the case of smooth cubic fourfolds. Moreover, we can switch to thinking of these groups in the ℓ-adic rationals by changing scalars via a tensor product over $\mathbb{Z}_\ell$. That is, we can define

Definition 2.49. The ℓ-adic étale cohomology group is

$$H^i_{\text{ét}}(X, \mathbb{Q}_\ell) = H^i_{\text{ét}}(X, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}$$

For the étale site of a smooth, projective variety (where $\ell \neq \text{char}(k)$), this gives us a collection of groups of the form $\mathbb{Q}_\ell^m$ for some $m \in \mathbb{N}$ that stores deep information about the algebraic structure of our projective variety.

Section 2.5

Zeta Functions

The zeta function of a variety is a generating function depending on the point counts of the variety over various finite fields. As we have seen in the case of the Fibonacci generating function, these generating functions sometimes allow us to recover information about the coefficients of the generating series (in our case, the point counts), but in the case of the zeta function, we will see that it holds much deeper information about its associated variety than just the point counts.

For this section, we let E be an algebraic variety over the finite field $\mathbb{F}_q$, let N_k be the number of solutions to the defining equation over the field $\mathbb{F}_{q^k}$.

2.5.1. Zeta Functions

We can construct a generating function:

$$G(T) = N_1 T + \frac{N_2}{2}T^2 + \frac{N_3}{3}T^3 + \cdots = \sum_{i=1}^{\infty} \frac{N_i}{i}T^i,$$

which is simply a generating function in the point counts of the defining equation over various finite fields $\mathbb{F}_{q^k}$. We note that this has the structure of a logarithmic expansion, that is, it follows the form of the Taylor expansion $-\log(1-t) = t + \frac{t^2}{2} + \frac{t^3}{3} + \ldots$.

In general, we have no reason to suspect that this generating function converges (in the (X)-adic metric) to any rational function; however, by exponentiating this function we can say a great deal about the shape of its convergent function. Thus

the actual Zeta function is defined as

Definition 2.50. The **Zeta Function** of a variety is

$$Z(E,T) \coloneqq \exp(G(T)) = \exp\left(\sum_{i=1}^{\infty} \frac{N_i}{i} T^i\right).$$

Let us examine some simpler examples of Zeta functions.

Example 2.51. When all point counts are trivial, that is $N_i = 1 \ \forall \ i \in \mathbb{N}$ (e.g. when the variety is a point), then the generating series converges to $G(T) = -\log(1-T)$, thus the Zeta function is

$$Z(E,T) = \exp(-\log(1-T)) = \frac{1}{\exp(\log(1-T))} = \frac{1}{1-T}$$

Example 2.52. Let $E = \mathbb{P}^1_q$ (the projective line over $\mathbb{F}_q$). In this case, over $\mathbb{P}^1_{q^i}$, we have that there are $(q^i)^2 - 1$ total combinations of coefficients (note that we take off 1 since $(0,0)$ is not included). However, we must consider that all $q^i - 1$ scalar multiples are equivalent in this space (again, we take off 1 to remove $0 \in \mathbb{F}_q$) This tells us that

$$N_i = \frac{(q^i)^2 - 1}{q^i - 1} = \sum_{j=0}^{1} q^{ij} = 1 + q^i$$

Plugging this into our Zeta function definition we get

$$\begin{aligned} Z(\mathbb{P}^1_q, T) &= \exp\left(\sum_{i=1}^{\infty} \frac{N_i}{i} T^i\right) \\ &= \exp\left(\sum_{i=1}^{\infty} \frac{1+q^i}{i} T^i\right) \\ &= \exp\left(\sum_{i=1}^{\infty} \frac{1}{i} T^i\right) \cdot \exp\left(\sum_{i=1}^{\infty} \frac{q^i}{i} T^i\right) \end{aligned}$$

We have already seen in Example 2.51 that

$$\exp\left(\sum_{i=1}^{\infty}\frac{1}{i}T^i\right)=\frac{1}{(1-T)}$$

Similarly, we note that

$$\exp\left(\sum_{i=1}^{\infty}\frac{q^i}{i}T^i\right)=\exp\left(\sum_{i=1}^{\infty}\frac{1}{i}(qT)^i\right)$$

is really just the logarithmic expansion in the variable qT meaning that this converges to

$$\exp\left(\sum_{i=1}^{\infty}\frac{q^i}{i}T^i\right)=\frac{1}{1-qT}$$

Giving the full Zeta function

$$Z(\mathbb{P}^1_q,T)=\frac{1}{(1-T)(1-qT)}$$

2.5.2. Frobenius Endomorphism

Crucial to understanding the Weil conjectures is understanding the Frobenius Endomorphism and its induced action on the cohomology of a cubic fourfold. We will begin by considering the Frobenius on rings.

Definition 2.53. For a commutative ring A with characteristic p, the map

$$\begin{aligned}\phi : A &\to A\\ a &\mapsto a^p\end{aligned}$$

is called the **Frobenius Endomorphism** on A.

Lemma 2.54. *The Frobenius endomorphism is an endomorphism on A.*

Proof. To show this we must show that ϕ is a ring map on A.

(a) We have that for $a, b \in A$,

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$$

(b) We have that for $a, b \in A$,

$$\phi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^{p-k} b^k$$

Then because $p | \frac{p!}{k!(p-k)!}$ for $k = 1, 2, \ldots, p-1$ all these terms will be zero in a ring of characteristic p, so we are left with terms

$$\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$$

(c)

$$\phi(1) = 1^p = 1$$

Then ϕ is an endomorphism on A. □

We note that this map is an automoprhism whenever it has trivial kernel. This tells us that rings which have no nonzero elements satisfying $a^p = 0$ are rings in which the Frobenius is an automoprhism.

On schemes we have

Definition 2.55. For a scheme $(X, \mathcal{O}_X)$ over $\mathbb{F}_p$ is the scheme map

$$(\phi, \phi^{\#}) : (X, \mathcal{O}_X) \to (X, \mathcal{O}_X)$$

where ϕ is the identity on X and $\phi^{\#}$ is the Frobenius endomorphism on each section $\mathcal{O}_X(U)$.

Similarly we can define Frobenius for $X_{\text{ét}}$ over $\mathbb{F}_q$ by considering Frobenius maps between étale morphisms. Via this Frobenius map on the étale category, we get induced map which acts on the $\mathbb{Q}_\ell$-vector space $H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ for all $i = 0, 1, \ldots$. We will call this map the **Frobenius acting on the étale cohomology** and it will simply be denoted $\phi^* : H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \to H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$. We note that as each cohomology group is a vector space over $\mathbb{Q}_\ell$ of some finite dimension, we can consider the Frobenius endomorphism as a matrix and compute its characteristic polynomial. As in linear algebra, this will be

$$p(x) = \det(\mathbb{1} - x\phi^* | H^i_{\text{ét}}(X, \mathbb{Q}_\ell))$$

where $\phi^* | H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ denotes the matrix representation of ϕ acting on the i-th étale cohomology group. For more information on the Frobenius endomorphism, see [6, Pages 154-155]. With this, we are now equipped to understand and appreciate the significance of the Weil conjectures.

2.5.3. Weil Conjectures

Theorem 2.56 (Weil Conjectures – posited 1949 [6, Chapter 2, Section 26])**.**
For a non-singular, n-dimensional, projective variety E:

(a) (Dwork 1960) The Zeta function is a rational function which can be written in terms of integral polynomials as:

$$Z(E, T) = \frac{P_1(T) \ldots P_{2n-1}(T)}{P_0(T) \ldots P_{2n}(T)}$$

where each $P_i(T) = \det(\mathbb{1} - T\phi^* | H^i_{ét}(X, \mathbb{Q}_\ell))$ is the characteristic polynomial of Frobenius acting on the i-th cohomology group.

(b) (Deligne 1974) The roots of $P_i(T)$ all lie on the complex circle of radius $q^{-\frac{i}{2}}$

(c) (Grothendieck 1965) The Zeta function satisfies a functional equation:

$$Z(E, \frac{1}{T}) = \pm q^{\frac{\chi(E)\cdot n}{2}} \cdot T^{\chi(E)} \cdot Z(E, T)$$

Where $\chi(E)$ is the Euler characteristic of the variety.

The Weil conjectures tell us about the shape of the zeta function as an integral rational function, but it also explains the relationship that emerges between the zeta function and the étale cohomology of the variety. Because counting points is, in general, much simpler than computing the cohomology of our variety this allows us to deduce a great deal about the cohomology groups and how Frobenius acts on them.

2.5.4. Computing Zeta Functions

We will show by example how the Weil conjectures aid in computing zeta functions. We first note that some of the ranks of the étale cohomology groups of a variety can be quickly deduced. This is due to the **Comparison Theorem for Étale Cohomology** ([6, Chapter 1, Section 21]) which effectively tells us that the étale cohomology groups are isomoprhic as vector spaces to the ordinary cohomology on a modified version of the variety (its analytification). In conjunction with other comparison theorems on cohomology, we can quickly compute certain cohomology groups via knowledege of alternate cohomology constructions.

Consider $E : y^2 = x^3 + Ax + B$, the general elliptic curve over $\mathbb{F}_q$ and its projectivization $\overline{E}$. This is a 1-dimensional curve so its largest nonzero cohomology will be $H^2_{\text{ét}}(X, \mathbb{Q}_\ell)$ (this follows from the comparison theorem). Additionally,

$$H^0_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell) \cong H^2_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$$

since $H^0_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell)$ will have dimension equal to the number of connected components. Further, étale cohomology has a number of duality theorems that tell us that $H^2_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell)$ has the same dimension in this case. Additionally, since the elliptic curve is homeomorphic to a torus, we know its fundamental group has two generators (see [4, Theorem IV.4.14B]). Then $H^1_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell)$ will be a 2-dimensional vector space.
Since the characteristic polynomial of Frobenius acting on a cohomology group will have the same degree as the dimension of that space, we know that in the Weil conjectures

$$\deg(P_0(T)) = 1,\ \deg(P_1(T)) = 2, \text{ and } \deg(P_2(T)) = 1$$

Since the roots of $P_i(T)$ lie on the complex circle of radius $q^{-\frac{i}{2}}$, we know that for the degree 1 polynomials we must have

$$P_0(T) = (1 - T) \text{ and } P_2(T) = (1 - qT)$$

Then we know that our zeta function has the form

$$Z(E, T) = \frac{P_1(T)}{(1 - T)(1 - qT)} = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

where $|\alpha| = |\beta| = 5$. Then we have

$$\begin{aligned} P_1(T) &= (1 - \alpha T)(1 - \beta T) \\ &= (1 - (\alpha + \beta)T + \alpha\beta T^2) \\ &= (1 - \gamma T + qT^2) \end{aligned}$$

where $\gamma = \alpha + \beta$. Then we need only solve for γ. That is, we have 1 unknown, so we expect that we need 1 point count to be able to solve for our full zeta function. Recall $G(T) = N_1 T + \frac{N_2}{2}T^2 + \frac{N_3}{3}T^3 + \dots$, and

$$Z(E,T) = \frac{(1 - \gamma T + qT^2)}{(1-T)(1-qT)} = \exp(G(T))$$

So by Taylor expansion

$$\frac{(1 - \gamma T + qT^2)}{(1-(q+1)T + qT^2)} = (1 + G(T) + \frac{(G(T))^2}{2} + \dots)$$
$$\Rightarrow (1 - \gamma T + qT^2) = (1-(q+1)T + qT^2)(1 + G(T) + \frac{(G(T))^2}{2} + \dots)$$

We can see that the term associated with T on the right hand side will be given by $-\gamma = N_1 - (q+1)$. and so our Zeta function is

$$Z(E,T) = \frac{(1 + (N_1 - (q+1))T + qT^2)}{(1-T)(1-qT)}$$

2.5.5. Zeta Function of a Cubic Fourfold

As a cubic fourfold is of dimension 4, it has many more nonzero cohomology groups than an elliptic curve. However, there are general statements we can make about the cohomology groups that will help us to reduce the number of point counts needed to solve for the zeta function. We have that for a cubic fourfold E:

(a) $H^i_{\text{ét}}(E, \mathbb{Q}_\ell) \cong 0$ for $i = 1, 3, 5, 7$,

(b) $H^i_{\text{ét}}(E, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ for $i = 0, 2, 6, 8$,

(c) $\dim(H^4_{\text{ét}}(E, \mathbb{Q}_\ell)) = 23$

(d) $(1 - 4T)$ always divides $\det(\mathbb{1} - T\phi^* | H^4_{\text{ét}}(X, \mathbb{Q}_\ell))$

For more information on this, see [1, Section 4.1,4.4]. Since all the odd cohomology groups are trivial, we have that

$$P_1(T) = \cdots = P_7(T) = 1$$

so the numerator of our zeta function will always be 1. Further, since the even cohomology (besides 4) are 1-dimensional, and we know their roots lie on a unit circle of radius $2^{-\frac{i}{2}}$, we have that

$$P_0(T) = (1-T),\ P_2(T) = (1-2T),\ P_6(T) = (1-8T), \text{ and } P_8(T) = (1-16T)$$

Then we are only left to solve for $P_4(T)$, but note that since $(1-4T)$ always divides $P_4(T)$, we can always pull out this factor and we are left with an unknown polynomial $P(T)$ with degree 22. With this, the zeta function of our general cubic fourfold looks like

$$Z(E,T) = \frac{1}{(1-T)(1-2T)(1-4T)(1-8T)(1-16T)P(T)}.$$

For more information, see [1, Section 4.1,4.4]. Then to solve for such a zeta function we need at most $\deg(P(T)) = 22$ point counts of our cubic fourfold. However, the functional equation tells us that the point counts will be symmetric (up to a change of sign), so in most cases, we can compute 11 point counts and deduce the sign of the functional equation by trying both signs and seeing if one of the signs does not satisfy the property that the roots of $P_4(T)$ lie along the complex circle of radius $\frac{1}{4}$. In certain cases, both may satisfy this property, in which case, either 22 point counts must be performed, or, more efficiently, one can deduce the sign of the functional equation from the discriminant of the variety (see [1, Theorem 4.1]). To actually count points one could simply enumerate points over each $\mathbb{F}_{2^i}$ and check if they satisfy the defining equation but as i will ultimately reach 11, such a computation

strategy is infeasible if we desire quick enumeration. Instead we use a faster method in our actual computation involving the algebraic blowup of the variety on a line - a topic not discussed in this paper. For our purposes, it is sufficient to note that we were able to compute these point counts and thus quickly compute zeta functions for each variety in our census. In this way, we are now equipped to compute and understand these zeta functions.

Chapter 3

Results

All results for this section can also be found at [1].

3.0.1. Filtration of Cubic Fourfolds

Using the methods and knowledge of the previous chapters, we can now perform a census of cubic fourfolds and their zeta functions. Let us first understand the scope of this enumeration problem.

Let $V = \mathbb{F}_2[x_0, \ldots, x_5]_3$ be the space of cubic fourfolds over $\mathbb{F}_2$. As an $\mathbb{F}_2$ vector space, this has dimension

$$\binom{5+3}{3} = 56.$$

Then there are in total $2^{56} - 1$ (or roughly 70 quadrillion) cubic fourfolds. A complete enumeration of these is intractable so we will instead consider these cubic fourfolds up to linear isomorphim, that is, mod the action induced by $G = \mathrm{GL}_6(\mathbb{F}_2)$. This is because two cubic fourfolds are isomorphic if and only if they projectively equivalent. Applying Burnside's lemma, we find that there are

$$|V/G| = 3,718,649$$

cubic fourfolds in distinct, non-zero orbits.

To find and populate these orbits with naive enumeration or union-find would take unreasonably long on most personal computers. In the case of union-find, our earlier runtime analysis tells us that computing such a census would have roughly

$$\begin{aligned}|V/G||G| &= (3718649) \cdot |\operatorname{GL}_6(\mathbb{F}_2)| = (3718649) \cdot \left(\prod_{i=0}^{5} 2^6 - 2^i\right) \\ &= (3718649) \cdot (20158709760) = 74963165890314240\end{aligned}$$

steps. Then given the (extremely generous) assumption that each step takes one clock cycle, then on a 4 GHz processor we can expect that this will take

$$\frac{1}{4 * 10^9} \cdot 74963165890314240 \text{ sec } = \sim 18740791 \text{ sec } = \sim 216.9 \text{ days.}$$

In reality this will likely take hundreds of clock cycles even in well optimized code. That is to say, on a personal computer such a computation could take *years*. Instead we can consider the following sequence of G-invariant subspaces of V:

$$0 \subseteq W_1 \subseteq W_2 \subseteq V$$

where

$$\begin{aligned}W_1 &= \operatorname{span}\{l^3 \mid l \in \mathbb{F}_2[x_0, \ldots, x_5]_1\} \\ W_2 &= \operatorname{span}\{l_1 \cdot l_2^2 \mid l_1, l_2 \in \mathbb{F}_2[x_0, \ldots, x_5]_1\}.\end{aligned}$$

Here, $\mathbb{F}_2[x_0, \ldots, x_5]_1$ denotes the space of all linear polynomials of 6 variables over $\mathbb{F}_2$. Using this sequence of inclusions, we were able to apply the filtration method to compute a list of all representatives of this group action in roughly *an hour and a*

half on a personal computer with a 1.1 GHz processor.

3.0.2. Census Results

These results are based on *A Census of Cubic Fourfolds over* $\mathbb{F}_2$ by Asher Auel, Avinash Kulkarni, Jack Petok, and Jonah Weinbaum [1] - whose theoretical underpinnings are explained in this thesis. The github repository of code used for the project can be found at https://github.com/JonahWeinbaum/cubic-fourfolds. Using our database of representatives, along with code written in the Magma computer algebra programming language [2], we were able to compute:

Theorem 3.1. *Of the* $3,718,649$ *isomorphism classes of cubic fourfolds over* $\mathbb{F}_2$*, exactly* $1,069,562$ *(*$\sim 29\%$*) are smooth.*

Furthermore, we computed all the zeta functions of these smooth cubic fourfolds.

Theorem 3.2. *There are* $86,472$ *distinct zeta functions realized amongst the* $1,069,562$ *isomorphism classes of smooth cubic fourfolds over* $\mathbb{F}_2$*.*

With our census we can examine some of these zeta functions:

Example 3.3. Let

$$R(T) = \frac{1}{(1-T)(1-2T)(1-4T)(1-8T)(1-16T)}.$$

Then,

(a) $Z(V(x_0^3 + \cdots + x_5^3), T)$
$= R(T) \cdot (-17592186044416T^{22} + 12094627905536T^{20} - 3779571220480T^{18} + 708669603840T^{16} - 88583700480T^{14} + 7751073792T^{12} - 484442112T^{10} + 21626880T^8 - 675840T^6 + 14080T^4 - 176T^2 + 1)^{-1}$

(b) $Z(V(x_0x_5^2 + x_1x_4^2 + x_2x_3^2 + x_3x_2^2 + x_4x_1^2 + x_5x_0^2), T)$
$= R(T) \cdot ((1-T)^{15} \cdot (1+T)^7)^{-1}$

In addition to these results, a number of statistics on cubic fourfolds are also presented in the paper, including:

(a) Counts of linear subspaces contained in each cubic

(b) Ranks of groups of algebraic cycles

(c) Newton polygons

We anticipate that the database will be attached to the Arxiv posting of the paper [1]. We hope that the reader will find the database, and the methods used to generate it, of use for further research and future applications.

Bibliography

[1] Asher Auel, Avinash Kulkarni, Jack Petok, and Jonah Weinbaum, *A census of cubic fourfolds over* $\mathbb{F}_2$, 2023, Arxiv preprint forthcoming.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[3] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR 2286236

[4] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 0463157

[5] Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid. MR 1011461

[6] James S. Milne, *Lectures on etale cohomology (v2.21)*, 2013, Available at www.jmilne.org/math/, p. 202.

[7] ———, *Algebraic geometry*, 2017, Available at www.jmilne.org/math/, p. 221.

[8] Michael Spivak, *Calculus on manifolds. A modern approach to classical theorems of advanced calculus*, W. A. Benjamin, Inc., New York-Amsterdam, 1965. MR 0209411

[9] The Stacks Project Authors, *Stacks Project*, https://stacks.math.columbia.edu, 2018.

[10] Richard P. Stanley, *Enumerative combinatorics. Volume 1*, second ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012. MR 2868112

[11] Ravi Vakil, *The rising sea: Foundations of algebraic geometry*, preprint (2017).

[12] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324