

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

CRAG

The Weil Conjectures

D. Zack Garza

April 2020

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

Background: Generating Functions

Fix q a prime and $\mathbb{F} := \mathbb{F}_q$ the (unique) finite field with q elements, along with its (unique) degree n extensions

$$\mathbb{F}_{q^n} = \left\{ x \in \bar{\mathbb{F}}_q \mid x^{q^n} - x = 0 \right\} \quad \forall n \in \mathbb{Z}^{\geq 2}$$

Definition (Projective Algebraic Varieties)

Let $J = \langle f_1, \dots, f_M \rangle \trianglelefteq k[x_0, \dots, x_n]$ be an ideal, then a *projective algebraic variety* $X \subset \mathbb{P}_{\mathbb{F}}^n$ can be described as

$$X = V(J) = \left\{ \mathbf{x} \in \mathbb{P}_{\mathbb{F}}^n \mid f_1(\mathbf{x}) = \dots = f_M(\mathbf{x}) = \mathbf{0} \right\}$$

where J is generated by *homogeneous* polynomials in $n + 1$ variables, i.e. there is a fixed $d = \deg f_i \in \mathbb{Z}^{\geq 1}$ such that

$$f(\mathbf{x}) = \sum_{\substack{I=(i_1, \dots, i_n) \\ \sum_j i_j = d}} \alpha_I \cdot x_0^{i_1} \cdots x_n^{i_n} \quad \text{and} \quad f(\lambda \cdot \mathbf{x}) = \lambda^d f(\mathbf{x}), \lambda \in \mathbb{F}^\times.$$

Point Counts

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
n-space

Grassmannian

- For a fixed variety X , we can consider its \mathbb{F} -points $X(\mathbb{F})$.
 - Note that $\#X(\mathbb{F}) < \infty$ is an integer
- For any L/\mathbb{F} , we can also consider $X(L)$
 - In particular, we can consider $X(\mathbb{F}_{q^n})$ for any $n \geq 2$.
 - We again have $\#X(\mathbb{F}_{q^n}) < \infty$ and are integers for every such n .
- So we can consider the sequence

$$[N_1, N_2, \dots, N_n, \dots] := [\#X(\mathbb{F}), \#X(\mathbb{F}_{q^2}), \dots, \#X(\mathbb{F}_{q^n}), \dots].$$

- Idea: associate some generating function (a formal power series) encoding sequence, e.g.

$$F(z) = \sum_{n=1}^{\infty} N_n z^n = N_1 z + N_2 z^2 + \dots.$$

Why Generating Functions?

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Note that for such an ordinary generating functions, the coefficients are related to the real-analytic properties of F : we can easily recover the coefficients in the following way:

$$[z^n] \cdot F(z) = [z^n] \cdot T_{F,z=0}(z) = \frac{1}{n!} \left(\frac{\partial}{\partial z} \right)^n F(z) \Big|_{z=0} = N_n.$$

They are also related to the complex analytic properties: using the Residue theorem,

$$[z^n] \cdot F(z) := \frac{1}{2\pi i} \oint_{\mathbb{S}^1} \frac{F(z)}{z^{n+1}} dz = \frac{1}{2\pi i} \oint_{\mathbb{S}^1} \frac{N_n}{z} dz = N_n.$$

The latter form is very amenable to computer calculation.

Why Generating Functions?

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

An OGF is an infinite series, which we can interpret as an analytic function $\mathbb{C} \rightarrow \mathbb{C}$ – in nice situations, we can hope for a closed-form representation.

A useful example: by integrating a geometric series we can derive

$$\begin{aligned}\frac{1}{1-z} &= \sum_{n=0}^{\infty} z^n && (= 1 + z + z^2 + \cdots) \\ \Rightarrow \int \frac{1}{1-z} &= \int \sum_{n=0}^{\infty} z^n \\ &= \sum_{n=0}^{\infty} \int z^n && \text{for } |z| < 1 \text{ by uniform convergence} \\ &= \sum_{n=0}^{\infty} \frac{1}{n+1} z^{n+1} \\ \Rightarrow -\log(1-z) &= \sum_{n=1}^{\infty} \frac{z^n}{n} && \left(= z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots \right).\end{aligned}$$

For completeness, also recall that

$$\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

CRAG

D. Zack
Garza

Background:
Generating
Functions

**Zeta
Functions**

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

Zeta Functions

Definition: Local Zeta Function

Problem: count points of a (smooth?) projective variety X/\mathbb{F} in all (finite) degree n extensions of \mathbb{F} .

Definition (Local Zeta Function)

The *local zeta function* of an algebraic variety X is the following formal power series:

$$Z_X(z) = \exp \left(\sum_{n=1}^{\infty} N_n \frac{z^n}{n} \right) \in \mathbb{Q}[[z]] \quad \text{where} \quad N_n := \#X(\mathbb{F}_n).$$

Note that

$$\begin{aligned} z \left(\frac{\partial}{\partial z} \right) \log Z_X(z) &= z \frac{\partial}{\partial z} \left(N_1 z + N_2 \frac{z^2}{2} + N_3 \frac{z^3}{3} + \cdots \right) \\ &= z (N_1 + N_2 z + N_3 z^2 + \cdots) \quad (\text{unif. conv.}) \\ &= N_1 z + N_2 z^2 + \cdots = \sum_{n=1}^{\infty} N_n z^n, \end{aligned}$$

which is an *ordinary* generating function for the sequence (N_n) .

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

Examples

Example: A Point

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Take $X = \{\text{pt}\} = V(\{f(x) = 0\})/\mathbb{F}$ a single point over \mathbb{F} , then

$$\#X(\mathbb{F}_q) := N_1 = 1$$

$$\#X(\mathbb{F}_{q^2}) := N_2 = 1$$

$$\vdots$$

$$\#X(\mathbb{F}_{q^n}) := N_n = 1$$

$$\vdots$$

and so

$$\begin{aligned} Z_{\{\text{pt}\}}(z) &= \exp\left(1 \cdot z + 1 \cdot \frac{z^2}{2} + 1 \cdot \frac{z^3}{3} + \cdots\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{z^n}{n}\right) \\ &= \exp(-\log(1-z)) \\ &= \frac{1}{1-z}. \end{aligned}$$

*Notice: Z admits a closed form **and** is a rational function.*

Example: The Affine Line

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
n-space

Grassmannian

Take $X = \mathbb{A}^1/\mathbb{F}$ the affine line over \mathbb{F} , then We can write

$$\mathbb{A}^1(\mathbb{F}_{q^n}) = \left\{ \mathbf{x} = [x_1] \mid x_1 \in \mathbb{F}_{q^n} \right\}$$

as the set of one-component vectors with entries in \mathbb{F}_n , so

$$X(\mathbb{F}_q) = q$$

$$X(\mathbb{F}_{q^2}) = q^2$$

$$\vdots$$

$$X(\mathbb{F}_{q^n}) = q^n.$$

Then

$$\begin{aligned} Z_X(z) &= \exp \left(\sum_{n=1}^{\infty} q^n \frac{z^n}{n} \right) \\ &= \exp \left(\sum_{n=1}^{\infty} \frac{(qz)^n}{n} \right) \\ &= \exp(-\log(1 - qz)) \\ &= \frac{1}{1 - qz}. \end{aligned}$$

Example: Affine m-space

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Take $X = \mathbb{A}^m/\mathbb{F}$ the affine line over \mathbb{F} , then We can write

$$\mathbb{A}^m(\mathbb{F}_{q^n}) = \left\{ \mathbf{x} = [x_1, \dots, x_m] \mid x_i \in \mathbb{F}_{q^n} \right\}$$

as the set of one-component vectors with entries in \mathbb{F}_n , so

$$X(\mathbb{F}_q) = q^m$$

$$X(\mathbb{F}_{q^2}) = (q^2)^m$$

$$\vdots$$

$$X(\mathbb{F}_{q^n}) = q^{nm}.$$

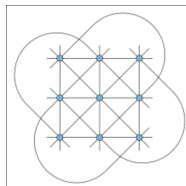


Figure: $\mathbb{A}^2/\mathbb{F}_3$ ($q = 3, m = 2, n = 1$)

Then

$$\begin{aligned} Z_X(z) &= \exp \left(\sum_{n=1}^{\infty} q^{nm} \frac{z^n}{n} \right) = \exp \left(\sum_{n=1}^{\infty} \frac{(q^m z)^n}{n} \right) \\ &= \exp(-\log(1 - q^m z)) \\ &= \frac{1}{1 - q^m z}. \end{aligned}$$

Example: Projective Line

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Take $X = \mathbb{P}^1/\mathbb{F}$, we can still count by enumerating coordinates:

$$\mathbb{P}^1(\mathbb{F}_{q^n}) = \left\{ [x_1 : x_2] \mid x_1, x_2 \neq 0 \in \mathbb{F}_{q^n} \right\} / \sim = \left\{ [x_1 : 1] \mid x_1 \in \mathbb{F}_{q^n} \right\} \coprod \{[1 : 0]\}.$$

Thus

$$X(\mathbb{F}_q) = q + 1$$

$$X(\mathbb{F}_{q^2}) = q^2 + 1$$

$$\vdots$$

$$X(\mathbb{F}_{q^n}) = q^n + 1.$$

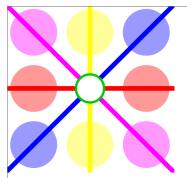


Figure: $\mathbb{P}^1/\mathbb{F}_3$ ($q = 3, n = 1$)

Thus

$$\begin{aligned} Z_X(z) &= \exp \left(\sum_{n=1}^{\infty} (q^n + 1) \frac{z^n}{n} \right) \\ &= \exp \left(\sum_{n=1}^{\infty} q^n \frac{z^n}{n} + \sum_{n=1}^{\infty} 1 \cdot \frac{z^n}{n} \right) \\ &= \frac{1}{(1 - qz)(1 - z)}. \end{aligned}$$

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

The Weil Conjectures

(Weil 1949)

Let X be a smooth projective variety of dimension N over \mathbb{F}_q for q a prime, let $Z_X(z)$ be its zeta function, and define $\zeta_X(s) = Z_X(q^{-s})$.

1 (Rationality)

$Z_X(z)$ is a rational function:

$$Z_X(z) = \frac{p_1(z) \cdot p_3(z) \cdots p_{2N-1}(z)}{p_0(z) \cdot p_2(z) \cdots p_{2N}(z)} \in \mathbb{Q}(z), \quad \text{i.e.} \quad p_i(z) \in \mathbb{Z}[z]$$

$$P_0(z) = 1 - z$$

$$P_{2N}(z) = 1 - q^N z$$

$$P_j(z) = \prod_{i=1}^{\beta_j} (1 - a_{j,i} z) \quad \text{for some reciprocal roots } a_{j,i} \in \mathbb{C}$$

where we've factored each P_i using its reciprocal roots a_{ij} .

In particular, this implies the existence of a meromorphic continuation of the associated function $\zeta_X(s)$, which a priori only converges for $\Re(s) \gg 0$. This also implies that for n large enough, N_n satisfies a linear recurrence relation.

2 (Functional Equation and Poincare Duality)

Let $\chi(X)$ be the Euler characteristic of X , i.e. the self-intersection number of the diagonal embedding $\Delta \hookrightarrow X \times X$; then $Z_X(z)$ satisfies the following *functional equation*:

$$Z_X\left(\frac{1}{q^N z}\right) = \pm \left(q^{\frac{N}{2}} z\right)^{\chi(X)} Z_X(z).$$

Equivalently,

$$\zeta_X(N-s) = \pm \left(q^{\frac{N}{2}-s}\right)^{\chi(X)} \zeta_X(s)$$

Note that when $N = 1$, e.g. for a curve, this relates $\zeta_X(s)$ to $\zeta_X(1-s)$.

Equivalently, there is an involutive map on the (reciprocal) roots

$$z \longleftrightarrow \frac{q^N}{z}$$

$$\alpha_{j,k} \longleftrightarrow \alpha_{2N-j,k}$$

which sends roots of p_j to roots of p_{2N-j} .

3 (Riemann Hypothesis)

The reciprocal roots $a_{j,k}$ are *algebraic* integers (roots of some monic $p \in \mathbb{Z}[x]$) which satisfy

$$|a_{j,k}|_{\mathbb{C}} = q^{\frac{j}{2}}, \quad 1 \leq j \leq 2N - 1, \quad \forall k.$$

4 (Betti Numbers)

If X is a “good reduction mod q ” of a nonsingular projective variety \tilde{X} in characteristic zero, then the $\beta_i = \deg p_i(z)$ are the Betti numbers of the topological space $\tilde{X}(\mathbb{C})$.

Moral:

- The Diophantine properties of a variety’s zeta function are governed by its (algebraic) topology.
- Conversely, the analytic properties of encode a lot of geometric/topological/algebraic information.
- Langland’s: similarly asks for every L function arising from an automorphic representation to satisfy Weil 2 and 3.

Why is (3) called the “Riemann Hypothesis”?

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Recall the Riemann zeta function is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

After modifying ζ to make it symmetric about $\Re(s) = \frac{1}{2}$ and eliminate the trivial zeros to obtain $\hat{\zeta}(s)$, there are three relevant properties

- “Rationality”: $\hat{\zeta}(s)$ has a meromorphic continuation to \mathbb{C} with simple poles at $s = 0, 1$.
- “Functional equation”: $\hat{\zeta}(1 - s) = \hat{\zeta}(s)$
- “Riemann Hypothesis”: The only zeros of $\hat{\zeta}$ have $\Re(s) = \frac{1}{2}$.

Why is (3) called the “Riemann Hypothesis”?

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Suppose it holds. We can use the facts that

a. $|\exp(z)| = \exp(\Re(z))$ and

b. $a^z := \exp(z \operatorname{Log}(a)),$

and to replace the polynomials P_i with

$$L_j(s) := P_j(q^{-s}) = \prod_{k=1}^{\beta_j} (1 - \alpha_{j,k} q^{-s}).$$

Analogy to Riemann Hypothesis

CRAIG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Now consider the roots of $L_j(s)$: we have

$$L_j(s_0) = 0$$

$$\iff q^{-s_0} = \frac{1}{\alpha_{j,k}} \quad \text{for some } k$$

$$\implies |q^{-s_0}| = \left| \frac{1}{\alpha_{j,k}} \right| \quad \text{by assumption } q^{-\frac{j}{2}}$$

$$\implies q^{-\frac{j}{2}} \stackrel{(a)}{=} \exp\left(-\frac{j}{2} \cdot \text{Log}(q)\right) = |\exp(-s_0 \cdot \text{Log}(q))|$$

$$\stackrel{(b)}{=} |\exp(-(\Re(s_0) + i \cdot \Im(s_0)) \cdot \text{Log}(q))|$$

$$\stackrel{(a)}{=} \exp(-(\Re(s_0)) \cdot \text{Log}(q))$$

$$\implies -\frac{j}{2} \cdot \text{Log}(q) = -\Re(s_0) \cdot \text{Log}(q) \quad \text{by injectivity}$$

$$\implies \Re(s_0) = \frac{j}{2}.$$

Analogy with Riemann Hypothesis

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

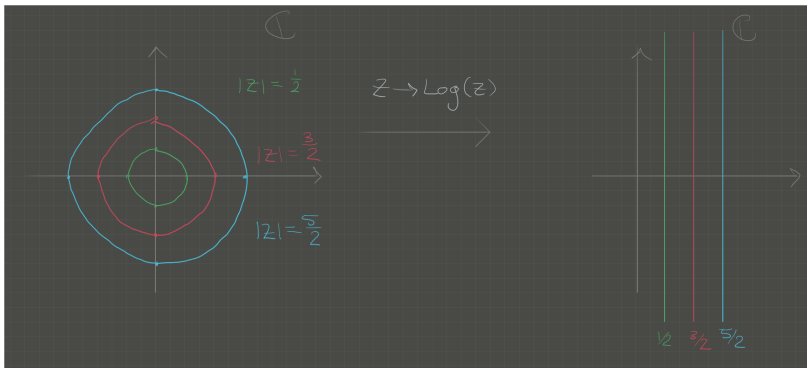
The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Roughly speaking, realizing that we would need to apply a logarithm (a conformal map) to send the $\alpha_{j,k}$ to zeros of the L_j , this says that the zeros all must lie on the “critical lines” $\frac{j}{2}$.



In particular, the zeros of L_1 have real part $\frac{1}{2}$, analogous to the classical Riemann hypothesis.

Precise Relation

CRAIG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

- Difficult to find in the literature! Idea: make a similar definition for schemes, then take $X = \text{Spec } \mathbb{Z}$.
- Define the “reductions mod q ” X_q for closed points q .
- Define the *local* zeta functions $\zeta_{X_p}(s) = Z_{X_p}(q^{-s})$.
- (Potentially incorrect) Evaluate to find $Z_{X_p}(z) = \frac{1}{1-z}$.
- Take a product over all closed points to define

$$\begin{aligned} L_X(s) &= \prod_{p \text{ prime}} \zeta_{X_p}(p^{-s}) \\ &= \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}} \right) \\ &= \zeta(s), \end{aligned}$$

which is the Euler product expansion of the classical Riemann Zeta function.

If anyone knows a reference for this, let me know!

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

Weil for Elliptic Curves

Example: An Elliptic Curve

CRAIG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

The Weyl conjectures take on a particularly nice form for curves. Let X/\mathbb{F} be a smooth projective curve of genus g , then

1 (Rationality)

$$\zeta_X(z) = \frac{p(z)}{(1-z)(1-qz)}$$

2 (Functional Equation)

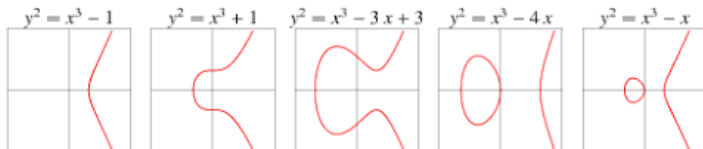
$$\zeta_X\left(\frac{1}{qz}\right) = q^{1-g} z^{2-2g} \zeta_X(z)$$

3 (Riemann Hypothesis)

$$p(t) = \prod_{i=1}^{2g} (q - a_i z) \quad \text{where} \quad |a_i| = \frac{1}{\sqrt{q}}$$

Take $X = E/\mathbb{F}$.

Figure: Some Elliptic Curves



- The number of points is given by

$$N_n := X(\mathbb{F}_n) = (q^n + 1) - (\alpha^n + \bar{\alpha}^n) \quad \text{where} \quad |\alpha| = |\bar{\alpha}| = \sqrt{q}$$

- Proof: Unsure! Maybe someone can point me to a reference. Involves trace (or eigenvalues?) of Frobenius.
- The Poincare polynomial is given by $P(x) = \sum \beta_i x^i = 1 + 2x + x^2$.
- The dimension of X over \mathbb{C} is $N = 1$,

The WC say we should be able to write as

$$Z_E(z) = \frac{p_1(z)}{p_0(z)p_2(z)} = \frac{p_1(z)}{(1-z)(1-qz)} = \frac{(1-\alpha_{1,1}z)(1-\alpha_{1,2}z)}{(1-z)(1-qz)}.$$

Since we know the number of points, we can compute

$$\begin{aligned}
 \zeta_X(z) &= \exp \sum_{n=1}^{\infty} \#X(\mathbb{F}_n) \frac{z^n}{n} \\
 &= \exp \sum_{n=1}^{\infty} (q^n + 1 - (\alpha^n + \bar{\alpha}^n)) \frac{z^n}{n} \\
 &= \exp \left(\sum_{n=1}^{\infty} q^n \cdot \frac{z^n}{n} \right) \exp \left(\sum_{n=1}^{\infty} 1 \cdot \frac{z^n}{n} \right) \exp \left(\sum_{n=1}^{\infty} -\alpha^n \cdot \frac{z^n}{n} \right) \exp \left(\sum_{n=1}^{\infty} -\bar{\alpha}^n \cdot \frac{z^n}{n} \right) \\
 &= \exp(-\log(1 - qz)) \exp(-\log(1 - z)) \exp(\log(1 - \alpha z)) \exp(\log(1 - \bar{\alpha} z)) \\
 &= \frac{(1 - \alpha z)(1 - \bar{\alpha} z)}{(1 - z)(1 - qz)} \in \mathbb{Q}(z),
 \end{aligned}$$

which is indeed a rational function.

Then

$$\zeta_X(t) = \frac{(1 - aq^{-t})(1 - \bar{a}q^{-t})}{(1 - q^{-t})(1 - q^{1-t})}.$$

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Weil for Projective m-space

Setup

CRAIG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

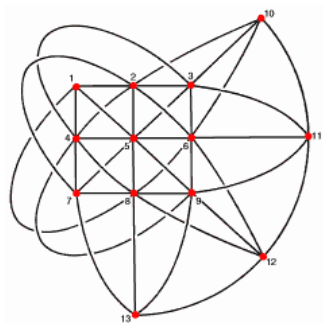
Grassmannian

Take $X = \mathbb{P}^m/\mathbb{F}$ We can write

$$\mathbb{P}^m(\mathbb{F}_{q^n}) = \mathbb{A}^{m+1}(\mathbb{F}_{q^n}) \setminus \{\mathbf{0}\} / \sim = \left\{ \mathbf{x} = [x_0, \dots, x_m] \mid x_i \in \mathbb{F}_{q^n} \right\} / \sim$$

But how many points are actually in this space?

Figure: Points and Lines in $\mathbb{P}^2/\mathbb{F}_3$



A nontrivial combinatorial problem!

q-Analogs and Grassmannians

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

To illustrate, this can be done combinatorially: identify $\mathbb{P}_{\mathbb{F}}^m = \text{Gr}_{\mathbb{F}}(1, m+1)$ as the space of lines in $\mathbb{A}_{\mathbb{F}}^{m+1}$.

Theorem

The number of k -dimensional subspaces of $\mathbb{A}_{\mathbb{F}_q}^N$ is the q -analog of the binomial coefficient:

$$\begin{bmatrix} N \\ k \end{bmatrix}_q := \frac{(q^N - 1)(q^{N-1} - 1) \cdots (q^{N-(k-1)} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

Remark: Note $\lim_{q \rightarrow 1} \begin{bmatrix} N \\ k \end{bmatrix}_q = \binom{N}{k}$, the usual binomial coefficient.

Proof: To choose a k -dimensional subspace,

- Choose a nonzero vector $\mathbf{v}_1 \in \mathbb{A}_{\mathbb{F}}^n$ in $q^N - 1$ ways.
 - For next step, note that $\#\text{span}\{\mathbf{v}_1\} = \#\left\{\lambda \mathbf{v}_1 \mid \lambda \in \mathbb{F}_q\right\} = \#\mathbb{F}_q = q$.
- Choose a nonzero vector \mathbf{v}_2 *not* in the span of \mathbf{v}_1 in $q^N - q$ ways.
 - Now note $\#\text{span}\{\mathbf{v}_1, \mathbf{v}_2\} = \#\left\{\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 \mid \lambda_i \in \mathbb{F}\right\} = q \cdot q = q^2$.

Proof continued

CRAG

- Choose a nonzero vector \mathbf{v}_3 *not* in the span of $\mathbf{v}_1, \mathbf{v}_2$ in $q^N - q^2$ ways.
- \dots until \mathbf{v}_k is chosen in

$$(q^N - 1)(q^N - q) \cdots (q^N - q^{k-1}) \quad \text{ways}$$

- This yields a k -tuple of linearly independent vectors spanning a k -dimensional subspace V_k
- This overcounts because many linearly independent sets span V_k , we need to divide out by the number of ways to choose a basis inside of V_k .
- By the same argument, this is given by

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$$

Thus

$$\begin{aligned} \# \text{subspaces} &= \frac{(q^N - 1)(q^N - q)(q^N - q^2) \cdots (q^N - q^{k-1})}{(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})} \\ &= \frac{q^N - 1}{q^k - 1} \cdot \left(\frac{q}{q^k - 1}\right) \frac{q^{N-1} - 1}{q^{k-1} - 1} \cdot \left(\frac{q^2}{q^k - 1}\right) \frac{q^{N-2} - 1}{q^{k-2} - 1} \cdots \left(\frac{q^{k-1}}{q^k - 1}\right) \frac{q^{N-(k-1)} - 1}{q^{k-(k-1)-1}} \\ &= \frac{(q^N - 1)(q^{N-1} - 1) \cdots (q^{N-(k-1)} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}. \end{aligned}$$

Counting Points

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Note that we've actually computed the number of points in any Grassmannian.

Identify $\mathbb{P}_{\mathbb{F}}^m = \text{Gr}_{\mathbb{F}}(1, m+1)$ as the space of lines in $\mathbb{A}_{\mathbb{F}}^{m+1}$.

We obtain a nice simplification for the number of lines corresponding to setting $k = 1$:

$$\begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q = \frac{q^{m+1} - 1}{q - 1} = q^m + q^{m-1} + \cdots + q + 1 = \sum_{j=0}^m q^j.$$

Thus

$$X(\mathbb{F}_q) = \sum_{j=0}^m q^j$$

$$X(\mathbb{F}_{q^2}) = \sum_{j=0}^m (q^2)^j$$

$$\vdots$$

$$X(\mathbb{F}_{q^n}) = \sum_{j=0}^m (q^n)^j.$$

Computing the Zeta Function

So

$$\begin{aligned}Z_X(z) &= \exp \left(\sum_{n=1}^{\infty} \sum_{j=0}^m (q^n)^j \frac{z^n}{n} \right) \\&= \exp \left(\sum_{n=1}^{\infty} \sum_{j=0}^m \frac{(q^j z)^n}{n} \right) \\&= \exp \left(\sum_{j=0}^m \sum_{n=1}^{\infty} \frac{(q^j z)^n}{n} \right) \\&= \exp \left(\sum_{j=0}^{m-1} -\log(1 - q^j z) \right) \\&= \prod_{j=0}^m (1 - q^j z)^{-1} \\&= \left(\frac{1}{1 - z} \right) \left(\frac{1}{1 - qz} \right) \left(\frac{1}{1 - q^2 z} \right) \cdots \left(\frac{1}{1 - q^m z} \right),\end{aligned}$$

Miraculously, still a rational function!

CRAIG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

An Easier Proof

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Quick recap:

$$Z_{\{\text{pt}\}} = \frac{1}{1-z} \quad Z_{\mathbb{P}^1}(z) = \frac{1}{1-qz} \quad Z_{\mathbb{A}^1}(z) = \frac{1}{(1-z)(1-qz)}.$$

Note that $\mathbb{P}^1 = \mathbb{A}^1 \amalg \{\infty\}$ and correspondingly $Z_{\mathbb{P}^1}(z) = Z_{\mathbb{A}^1}(z) \cdot Z_{\{\text{pt}\}}(z)$.
This works in general:

Lemma (Excision)

*If $Y/\mathbb{F}_q \subset X/\mathbb{F}_q$ is a closed subvariety, for $U = X \setminus Y$,
 $Z_X(z) = Z_Y(z) \cdot Z_U(z)$.*

Proof: Let $N_n = \#Y(\mathbb{F}_{q^n})$ and $M_n = \#U(\mathbb{F}_{q^n})$, then

$$\begin{aligned} \zeta_X(z) &= \exp \left(\sum_{n=1}^{\infty} (N_n + M_n) \frac{z^n}{n} \right) \\ &= \exp \left(\sum_{n=1}^{\infty} N_n \cdot \frac{z^n}{n} + \sum_{n=1}^{\infty} M_n \cdot \frac{z^n}{n} \right) \\ &= \exp \left(\sum_{n=1}^{\infty} N_n \cdot \frac{z^n}{n} \right) \cdot \exp \left(\sum_{n=1}^{\infty} M_n \cdot \frac{z^n}{n} \right) = \zeta_Y(z) \cdot \zeta_U(z). \end{aligned}$$

A Easier Proof

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
m-space

Grassmannian

Note that geometry can help us here: we have a stratification $\mathbb{P}^n = \mathbb{P}^{n-1} \amalg \mathbb{A}^n$, and so inductively

$$\mathbb{P}^m = \coprod_{j=0}^m \mathbb{A}^j = \mathbb{A}^0 \amalg \mathbb{A}^1 \amalg \cdots \amalg \mathbb{A}^m,$$

and recalling that

$$Z_{X \amalg Y}(z) = Z_X(z) \cdot Z_Y(z)$$

and $Z_{\mathbb{A}^j}(z) = \frac{1}{1-q^j z}$ we have

$$Z_{\mathbb{P}^m}(z) = \prod_{j=0}^m Z_{\mathbb{A}^j}(z) = \prod_{j=0}^m \frac{1}{1-q^j z}.$$

Notice that the highest degree is exactly m , and there is exactly one factor for each $j \leq m$. Note that $\mathbb{P}^m/\mathbb{F}_q$ can be thought of as a mod q reduction of $\mathbb{R}P^m$ or $\mathbb{C}P^m$, and somehow Z “sees” its dimension.

CRAG

D. Zack
Garza

Background:
Generating
Functions

Zeta
Functions

Examples

The Weil
Conjectures

Weil for
Elliptic
Curves

Weil for
Projective
 m -space

Grassmannian

Grassmannian

Consider now $X = \text{Gr}(k, m)/\mathbb{F}$ – by the previous computation, we know

$$X(\mathbb{F}_{q^n}) = \left[\begin{matrix} m \\ k \end{matrix} \right]_{q^n} := \frac{(q^{nm} - 1)(q^{nm-1} - 1) \cdots (q^{nm-n(k-1)} - 1)}{(q^{nk} - 1)(q^{n(k-1)} - 1) \cdots (q^n - 1)}$$

but the corresponding Zeta function is much more complicated than the previous examples:

$$Z_X(z) = \exp \left(\sum_{n=1}^{\infty} \left[\begin{matrix} m \\ k \end{matrix} \right]_{q^n} \frac{z^n}{n} \right) = \cdots?.$$

Note that $\dim_{\mathbb{R}} \text{Gr}_{\mathbb{R}}(k, m) = k(m - k)$ as a real manifold, so