CRAG

D. Zack Garza

Background Generating Functions

Zeta Functio

Example:

The Weil Conjecture

Weil for Elliptic Curves

Weil for Projective m-space

Grassmanniar

CRAG

The Weil Conjectures

D. Zack Garza

April 2020

CBAC

D. Zack Garza

Background Generating

Zeta Functions

Example

The Weil

Weil for Elliptic

Weil for Projective

Grassmanniar

Background: Generating Functions

Varieties

CRAG

D. Zack Garza

Background Generating Functions

Zeta Functi

Example

The Weil

Weil for Elliptic

Weil for

Grassma

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

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

Definition (Projective Algebraic Varieties)

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

$$X = V(J) = \left\{ \mathbf{x} \in \mathbb{P}_{\mathbb{F}}^{n} \mid f_{1}(\mathbf{x}) = \cdots = f_{M}(\mathbf{x}) = \mathbf{0} \right\}$$

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

$$f(\mathbf{x}) = \sum_{\substack{\mathbf{i} = (i_1, \cdots, i_n) \\ \sum_i i_i = d}} \alpha_{\mathbf{i}} \cdot x_0^{i_1} \cdots x_n^{i_n} \quad \text{ and } \quad f(\lambda \cdot \mathbf{x}) = \lambda^d f(\mathbf{x}), \lambda \in \mathbb{F}^{\times}.$$

Grassmar

- For a fixed variety X, we can consider its \mathbb{F} -points $X(\mathbb{F})$.
 - Note that $\#X(\mathbb{F})$ < ∞ 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

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

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

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

Why Generating Functions?

CRAG

D. Zac Garza

Background Generating Functions

Zeta Function

The Weil

Weil for Elliptic

Weil for Projectives

Grassman

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:

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

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

Background Generating Functions

Zeta

Example

The Weil

Weil for Elliptic Curves

Weil for Projective m-space

Grassman

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

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

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n \qquad (= 1 + z + z^2 + \cdots)$$

$$\implies \int \frac{1}{1-z} = \int \sum_{n=0}^{\infty} z^n$$

$$= \sum_{n=0}^{\infty} \int z^n \quad for|z| < 1 \quad \text{by uniform convergence}$$

$$= \sum_{n=0}^{\infty} \frac{1}{n+1} z^{n+1}$$

$$\implies -\log(1-z) = \sum_{n=0}^{\infty} \frac{z^n}{n} \qquad \left(= z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots\right).$$

For completeness, also recall that

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

CBAC

D. Zack Garza

Background: Generating Functions

Zeta Function

Examples

The Weil Conjecture

Weil for Elliptic Curves

Weil for Projective m-space

Grassmanniar

Zeta Functions

Definition: Local Zeta Function

CRAG

D. Zack Garza

ackgroun enerating

Zeta Functions

Example

The Weil

Weil for Elliptic Curves

Weil fo Project m-spac

Grassma

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:

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

Note that

$$z\left(\frac{\partial}{\partial z}\right)\log Z_X(z) = z\frac{\partial}{\partial z}\left(N_1z + N_2\frac{z^2}{2} + N_3\frac{z^3}{3} + \cdots\right)$$

$$= z\left(N_1 + N_2z + N_3z^2 + \cdots\right) \qquad \text{(unif. conv.)}$$

$$= N_1z + N_2z^2 + \cdots = \sum_{n=1}^{\infty} N_nz^n,$$

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

CBAC

D. Zack Garza

Background: Generating Functions

Zeta Functions

Examples

The Weil Conjecture

Weil for Elliptic

Weil for Projective

Grassmanniar

Examples

Example: A Point

CRAG

D. Zack Garza

Generating Functions

Zeta Functio

Examples

The Weil

Weil for

Weil for Projective

Grassmannia

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

and so

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

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

Example: The Affine Line

CRAG

D. Zack Garza

Backgroun Generating

Zeta Functio

Examples

The Weil

Weil for

Elliptic Curves

Projecti m-space

Grassman

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

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

:

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

Then

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

Example: Affine m-space

CRAG

D. Zack Garza

Backgroun Generating

Zeta

Examples

The Weil Conjecture

Weil for

Curves
Weil for

Grassman

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

$$\mathbb{A}^{m}(\mathbb{F}_{q^{n}}) = \left\{ \mathbf{x} = [x_{1}, \cdots, x_{m}] \mid x_{i} \in \mathbb{F}_{q^{n}} \right\}$$

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

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

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

$$\vdots$$

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

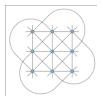


Figure:
$$\mathbb{A}^2/\mathbb{F}_3$$
 ($q = 3, m = 2, n = 1$)

Then

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

Example: Projective Line

CBAG

D. Zack Garza

ckground:

Functions

Examples

Lxampic

Conjecture

Weil for Elliptic Curves

Weil for Projective m-space

Grassmanniar

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

$$\mathbb{P}^{1}(\mathbb{F}_{q^{n}}) = \left\{ [x_{1} : x_{2}] \mid x_{1}, x_{2} \neq 0 \in \mathbb{F}_{q^{n}} \right\} / \sim = \left\{ [x_{1} : 1] \mid x_{1} \in \mathbb{F}_{q^{n}} \right\} \coprod \left\{ [1 : 0] \right\}.$$

Thus

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

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

$$\vdots$$

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

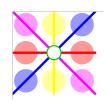


Figure: $\mathbb{P}^1/\mathbb{F}_3$ (q=3, n=1)

Thus

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

CDAG

D. Zack Garza

Background: Generating Functions

Zeta Functions

Examples

The Weil

Weil for Elliptic Curves

Weil for Projective

Grassmanniar

The Weil Conjectures

CRAC

D. Zacl Garza

Generating Functions

Zeta Functio

Exampl

The Weil Conjectures

Weil for Elliptic Curves

Weil for Projection m-space

Grassmar

(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 $\zeta_X(s) = Z_X(q^{-s})$.

(Rationality)

 $Z_X(z)$ is a rational function:

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

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

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

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

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:

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

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

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

$$\alpha_{i,k} \iff \alpha_{2N-i,k}$$

which sends roots of p_i to roots of p_{2N-i} .

CRAG

D. Zack Garza

Generatin Functions

Zeta Functi

Exampl

The Weil Conjectures

Weil for Elliptic Curves

Weil fo Project m-spac

Grassma

(Riemann Hypothesis)

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

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

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"?

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 $\widehat{\zeta}(s)$, there are three relevant properties

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

The Weil Conjectures

Why is (3) called the "Riemann Hypothesis"?

CRAG

D. Zack Garza

Generating Functions

Functio

Th - 14/-:1

The Weil Conjectures

Weil for Elliptic

Weil for Projective m-space

Grassmanniar

Suppose it holds. We can use the facts that

- $|\exp(z)| = \exp(\Re(z))$ 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

CRAG

D. Zack Garza

Backgrour Generating Functions

Zeta

Example

The Weil Conjectures

Weil for Elliptic Curves

Weil for Projective m-space

Grassmannia

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

$$L_{j}(s_{0}) = 0$$

$$\iff q^{-s_{0}} = \frac{1}{\alpha_{j,k}} \quad \text{for some} \quad k$$

$$\implies |q^{-s_{0}}| = \left| \frac{1}{\alpha_{j,k}} \right| \qquad \stackrel{\text{by assumption}}{=} q^{-\frac{j}{2}}$$

$$\implies q^{-\frac{j}{2}} \stackrel{\text{(a)}}{=} \exp\left(-\frac{j}{2} \cdot \operatorname{Log}(q)\right) = |\exp\left(-s_{0} \cdot \operatorname{Log}(q)\right)|$$

$$\stackrel{\text{(b)}}{=} |\exp\left(-(\Re(s_{0}) + i \cdot \Im(s_{0})) \cdot \operatorname{Log}(q)\right)|$$

$$\stackrel{\text{(a)}}{=} \exp\left(-(\Re(s_{0})) \cdot \operatorname{Log}(q)\right)$$

$$\implies -\frac{j}{2} \cdot \operatorname{Log}(q) = -\Re(s_{0}) \cdot \operatorname{Log}(q) \quad \text{by injectivity}$$

$$\implies \Re(s_{0}) = \frac{j}{2}.$$

Analogy with Riemann Hypothesis

CDAC

D. Zack Garza 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.

CRAG

Backgrou Generatin Functions

Zeta

Example

The Weil Conjectures

Weil for Elliptic Curves

Weil for Projective m-space

Grassilia

Precise Relation

CRAG

Garza

Generating Functions

Zeta Functio

The Weil

The Weil Conjectures

Weil for

Weil for Projective

Grassman

- Difficult to find in the literature! Idea: make a similar definition for schemes, then take $X = \operatorname{Spec} \mathbb{Z}$.

- 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

$$L_X(s) = \prod_{p \text{ prime}} \zeta_{X_p}(p^{-s})$$

$$= \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}}\right)$$

$$= \zeta(s),$$

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

Examples

The Weil Conjecture

Weil for Elliptic Curves

Weil for Projective m-space

Grassmanniar

Weil for Elliptic Curves

Example: An Elliptic Curve

CRAG

D. Zack Garza

Backgrour Generating

Zeta

Example

The Weil

Weil for Elliptic Curves

Weil for Projectiv m-space

Grassmar

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

(Rationality)

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

(Functional Equation)

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

3 (Riemann Hypothesis)

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

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

Consider the curve E defined by the following equation

CRAG

D. Zack Garza

Background: Generating Functions

Zeta Function

Examples

The Weil Conjecture

Weil for

Weil for Projective m-space

Grassmanniar

Weil for Projective m-space

Setup

CRAG

D. Zack Garza

ground:

Functions

Example

The Weil

Weil for

Weil for Projective m-space

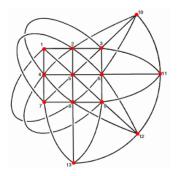
Grassmannia

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

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

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

Generation Function

Fxample

The Weil

Conjectur
Weil for

Weil for Projective m-space

Grassma

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

Theorem

The number of k-dimensional subspaces of $\mathbb{A}^N_{\mathbb{F}_q}$ 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 $\lim_{q \to 1} {N \brack k}_q = {N \choose k}$, the usual binomial coefficient.

Proof: To choose a *k*-dimensional subspace,

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

Grassmar

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

 $-\cdots$ until \mathbf{v}_k is chosen in

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

#subspaces =
$$\frac{(q^N - 1)(q^N - q)(q^N - q^2) \cdots (q^N - q^{k-1})}{(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})}$$

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

Counting Points

CRAG

D. Zack Garza

Backgrour Generating

Function Zeta

Example

The Weil

Weil for Elliptic Curves

Weil for Projective m-space

Grassmannia

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

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

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

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

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

CRAG

D. Zack Garza

Backgrou Generatin Functions

Zeta

Exampl

The Weil

Weil for

Weil for Projective m-space

Grassmanniar

So

$$Z_X(z) = \exp\left(\sum_{n=1}^{\infty} \sum_{j=0}^{m} (q^n)^j \frac{z^n}{n}\right)$$

$$= \exp\left(\sum_{n=1}^{\infty} \sum_{j=0}^{m} \frac{(q^j z)^n}{n}\right)$$

$$= \exp\left(\sum_{j=0}^{m} \sum_{n=1}^{\infty} \frac{(q^j z)^n}{n}\right)$$

$$= \exp\left(\sum_{j=0}^{m-1} -\log(1-q^j z)\right)$$

$$= \prod_{j=0}^{m} \left(1-q^j z\right)^{-1}$$

$$= \left(\frac{1}{1-z}\right) \left(\frac{1}{1-qz}\right) \left(\frac{1}{1-q^2 z}\right) \cdots \left(\frac{1}{1-q^m z}\right),$$

Miraculously, still a rational function!

An Easier Proof

CRAG

D. Zack Garza

Backgroun Generating Functions

Function: Zeta

Example

The Weil

Weil for Elliptic Curves

Weil for Projective m-space

Grassma

Quick recap:

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

Note that $\mathbb{P}^1 = \mathbb{A}^1 \coprod \{\infty\}$ 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

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

A Easier Proof

CRAG

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

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

and recalling that

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

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 PP^m/\mathbb{F}_q can be though of as a mod q reduction of \mathbb{RP}^m or \mathbb{CP}^m , and somehow Z "sees" its dimension.

Functions

Examples
The Weil

Conjecture
Weil for

Curves
Weil for
Projective
m-space

Grassman

CRAG

D. Zack Garza

Background: Generating Functions

Zeta Functions

Examples

The Weil Conjecture

Weil for Elliptic Curves

Projective m-space

Grassmanniai

Grassmannian

CRAG

D. Zacl Garza

Backgrour Generating Functions

Functio

Examp

The Weil

Weil for

Curves
Weil for

Grassmannia

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

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

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

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

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