

CRAG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

# CRAG

## The Weil Conjectures

D. Zack Garza

April 2020

CRAG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

## 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

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

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

- 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?

CRAIG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

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

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

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

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

# 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

## Examples

## Example: A Point

CRAG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

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

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

CRAIG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

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

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

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

$$\vdots$$

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

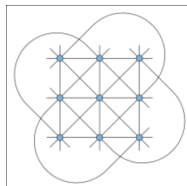


Figure:  $\mathbb{A}^2/\mathbb{F}_3$  ( $q = 3, m = 2, n = 1$ )

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

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

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

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

$$\vdots$$

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

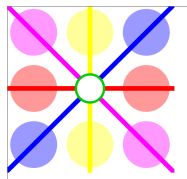


Figure:  $\mathbb{P}^1/\mathbb{F}_3$  ( $q = 3, n = 1$ )

Thus

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

# A Small Theorem

CRAG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

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

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

## Example: Projective m-space

CRAIG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

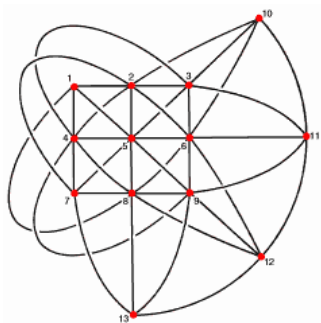
Examples

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!*

# Example: Projective m-space

CRAG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

To illustrate, this can be done combinatorially: identify  $\mathbb{P}_{\mathbb{F}}^m = \text{Gr}_{\mathbb{F}}(1, m)$  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  $q$ -binomial coefficient:*

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

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



## Example: Projective m-space

CRAG

D. Zack  
Garza

Background:  
Generating  
Functions

Zeta  
Functions

Examples

- 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

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

## Example: Projective m-space

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

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

$$\begin{bmatrix} m \\ 1 \end{bmatrix}_q = \frac{q^m - 1}{q - 1} = q^{m-1} + q^{m-2} + \cdots + q + 1 = \sum_{j=0}^{m-1} q^j.$$

Thus

$$\begin{aligned} X(\mathbb{F}) &= \sum_{j=0}^{m-1} q^j \\ X(\mathbb{F}_2) &= \sum_{j=0}^{m-1} (q^2)^j \\ &\vdots \\ X(\mathbb{F}_n) &= \sum_{j=0}^{m-1} (q^n)^j. \end{aligned}$$

So