A variety with many points over a finite field

Jared Weinstein (joint with Mitya Boyarchenko)

January 13, 2012

Varieties over finite fields: Rationality of the zeta function

Let $X/\mathbf{F}_q$ be a variety.

Varieties over finite fields: Rationality of the zeta function

Let $X/\mathbf{F}_q$ be a variety.
How do the numbers $\#X(\mathbf{F}_q), \#X(\mathbf{F}_{q^2}), \ldots$ behave?

Varieties over finite fields: Rationality of the zeta function

Let $X/\mathbf{F}_q$ be a variety.
How do the numbers $\#X(\mathbf{F}_q), \#X(\mathbf{F}_{q^2}), \ldots$ behave?
By the rationality of the zeta function, there exist $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_s$ in $\mathbf{C}^\times$ with

$$\#X(\mathbf{F}_{q^n}) = \sum_i \alpha_i^n - \sum_i \beta_i^n.$$

Varieties over finite fields: Rationality of the zeta function

Let $X/\mathbf{F}_q$ be a variety.
How do the numbers $\#X(\mathbf{F}_q), \#X(\mathbf{F}_{q^2}), \ldots$ behave?
By the rationality of the zeta function, there exist $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_s$ in $\mathbf{C}^\times$ with

$$\#X(\mathbf{F}_{q^n}) = \sum_i \alpha_i^n - \sum_i \beta_i^n.$$

The α_i and β_i are the inverse poles and roots of the zeta function $Z_{\mathbf{F}_q}(X, T)$.

The case of curves

If X is a geometrically connected nonsingular projective curve over $\mathbf{F}_q$, then

$$\#X(\mathbf{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \beta_i^n$$

where g is the genus of X.

The case of curves

If X is a geometrically connected nonsingular projective curve over $\mathbf{F}_q$, then

$$\#X(\mathbf{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \beta_i^n$$

where g is the genus of X. The numbers β_i have absolute value $\sqrt{q}$.

The case of curves

If X is a geometrically connected nonsingular projective curve over $\mathbf{F}_q$, then

$$\#X(\mathbf{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \beta_i^n$$

where g is the genus of X. The numbers β_i have absolute value $\sqrt{q}$. Therefore X satisfies the Hasse-Weil bound

$$\#X(\mathbf{F}_q) \leq q + 1 + 2g\sqrt{q}$$

Maximal Curves

A curve X is *maximal* if it achieves the Hasse-Weil bound:

$$\#X(\mathbf{F}_q) = q + 1 + 2g\sqrt{q}.$$

Maximal Curves

A curve X is *maximal* if it achieves the Hasse-Weil bound:

$$\#X(\mathbf{F}_q) = q + 1 + 2g\sqrt{q}.$$

(So q will have to be a square.)

Maximal Curves

A curve X is *maximal* if it achieves the Hasse-Weil bound:

$$\#X(\mathbf{F}_q) = q + 1 + 2g\sqrt{q}.$$

(So q will have to be a square.) For instance, the Hermitian curve has affine part

$$y^q + y = x^{q+1}$$

over $\mathbf{F}_{q^2}$. We have $g = q(q-1)/2$ and

$$\#X(\mathbf{F}_{q^2}) = q^3 + 1 = q^2 + 1 + 2gq.$$

Maximal Curves

A curve X is *maximal* if it achieves the Hasse-Weil bound:

$$\#X(\mathbf{F}_q) = q + 1 + 2g\sqrt{q}.$$

(So q will have to be a square.) For instance, the Hermitian curve has affine part

$$y^q + y = x^{q+1}$$

over $\mathbf{F}_{q^2}$. We have $g = q(q-1)/2$ and

$$\#X(\mathbf{F}_{q^2}) = q^3 + 1 = q^2 + 1 + 2gq.$$

Maximal curves tend to have large automorphism groups. The Hermitian curve has on the order of q^3 automorphisms.

Varieties over finite fields: Cohomological interpretation

The number $\#X(\mathbf{F}_q)$ is the number of closed fixed points of the Frobenius endomorphism $\mathrm{Frob}_q \colon X \to X$.

Varieties over finite fields: Cohomological interpretation

The number $\#X(\mathbf{F}_q)$ is the number of closed fixed points of the Frobenius endomorphism $\mathrm{Frob}_q : X \to X$.
Accordingly there's a Lefschetz fixed point theorem:

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

Varieties over finite fields: Cohomological interpretation

The number $\#X(\mathbf{F}_q)$ is the number of closed fixed points of the Frobenius endomorphism $\mathrm{Frob}_q : X \to X$.
Accordingly there's a Lefschetz fixed point theorem:

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

Here $H^i(X)$ is shorthand for $H^i_{\text{ét}}(X \otimes \overline{\mathbf{F}}_q, \overline{\mathbf{Q}}_\ell)$, for a prime $\ell \nmid p$.

Varieties over finite fields: Cohomological interpretation

The number $\#X(\mathbf{F}_q)$ is the number of closed fixed points of the Frobenius endomorphism $\mathrm{Frob}_q : X \to X$.
Accordingly there's a Lefschetz fixed point theorem:

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

Here $H^i(X)$ is shorthand for $H^i_{\text{ét}}(X \otimes \overline{\mathbf{F}}_q, \overline{\mathbf{Q}}_\ell)$, for a prime $\ell \nmid p$.
The α_i and β_i are the eigenvalues of Frob_q on $H^i(X)$ for i even and odd, respectively.

Varieties over finite fields: Cohomological interpretation

The number $\#X(\mathbf{F}_q)$ is the number of closed fixed points of the Frobenius endomorphism $\mathrm{Frob}_q : X \to X$.
Accordingly there's a Lefschetz fixed point theorem:

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

Here $H^i(X)$ is shorthand for $H^i_{\text{ét}}(X \otimes \overline{\mathbf{F}}_q, \overline{\mathbf{Q}}_\ell)$, for a prime $\ell \nmid p$.
The α_i and β_i are the eigenvalues of Frob_q on $H^i(X)$ for i even and odd, respectively.
Deligne: The eigenvalues on $H^i(X)$ have absolute value $\leq q^{i/2}$.

Varieties over finite fields: Cohomological interpretation

The number $\#X(\mathbf{F}_q)$ is the number of closed fixed points of the Frobenius endomorphism $\mathrm{Frob}_q : X \to X$.
Accordingly there's a Lefschetz fixed point theorem:

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

Here $H^i(X)$ is shorthand for $H^i_{\text{ét}}(X \otimes \overline{\mathbf{F}}_q, \overline{\mathbf{Q}}_\ell)$, for a prime $\ell \nmid p$.
The α_i and β_i are the eigenvalues of Frob_q on $H^i(X)$ for i even and odd, respectively.
Deligne: The eigenvalues on $H^i(X)$ have absolute value $\leq q^{i/2}$.
There is equality if X is nonsingular and projective. This is the Riemann Hypothesis for X.

Maximal varieties: definition

Let q be a prime power.

Maximal varieties: definition

Let q be a prime power.
Let's call a variety $X/\mathbf{F}_q$ *maximal* if Frob_q acts upon $H^i(X)$ as the scalar $(-1)^i q^{i/2}$.

Maximal varieties: definition

Let q be a prime power.
Let's call a variety $X/\mathbf{F}_q$ *maximal* if Frob_q acts upon $H^i(X)$ as the scalar $(-1)^i q^{i/2}$.
This ensures that

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

is the maximum possible with respect to the Riemann Hypothesis.

Maximal varieties: definition

Let q be a prime power.
Let's call a variety $X/\mathbf{F}_q$ *maximal* if Frob_q acts upon $H^i(X)$ as the scalar $(-1)^i q^{i/2}$.
This ensures that

$$\#X(\mathbf{F}_q) = \sum_i (-1)^i \mathrm{tr}(\mathrm{Frob}_q | H^i(X))$$

is the maximum possible with respect to the Riemann Hypothesis.
We construct an interesting maximal variety for every dimension and field of scalars.

Context

Shimura varieties link automorphic forms and Galois representations.

Context

Shimura varieties link automorphic forms and Galois representations.
A "piece" of a certain Shimura variety reduces modulo p to a variety X defined over a finite field.

Context

Shimura varieties link automorphic forms and Galois representations.
A "piece" of a certain Shimura variety reduces modulo p to a variety X defined over a finite field.
It turns out that this X is maximal, has a huge automorphism group, and exhibits interesting representation theory in its cohomology.

Definition of X

Let $\mathbf{U}$ be the group over $\mathbf{F}_q$ whose points over an $\mathbf{F}_q$-algebra R are expressions

$$1 + a_1\tau + \cdots + a_n\tau^n,\ a_i \in R$$

Definition of X

Let $\mathbf{U}$ be the group over $\mathbf{F}_q$ whose points over an $\mathbf{F}_q$-algebra R are expressions

$$1 + a_1\tau + \cdots + a_n\tau^n,\ a_i \in R$$

Multiplication in $\mathbf{U}$ is determined by the rules

$$\tau^{n+1} = 0,\ \tau a = a^q\tau.$$

Definition of X

Let $\mathbf{U}$ be the group over $\mathbf{F}_q$ whose points over an $\mathbf{F}_q$-algebra R are expressions

$$1 + a_1\tau + \cdots + a_n\tau^n,\ a_i \in R$$

Multiplication in $\mathbf{U}$ is determined by the rules

$$\tau^{n+1} = 0,\ \tau a = a^q\tau.$$

Let $X \subset \mathbf{U}$ be

$$\{g \in \mathbf{U} \mid \mathrm{Frob}_{q^n}(g)g^{-1} \text{ has no coeff. of } \tau^n\}$$

Definition of X

Let $\mathbf{U}$ be the group over $\mathbf{F}_q$ whose points over an $\mathbf{F}_q$-algebra R are expressions

$$1 + a_1\tau + \cdots + a_n\tau^n,\ a_i \in R$$

Multiplication in $\mathbf{U}$ is determined by the rules

$$\tau^{n+1} = 0,\ \tau a = a^q\tau.$$

Let $X \subset \mathbf{U}$ be

$$\{g \in \mathbf{U} \mid \mathrm{Frob}_{q^n}(g)g^{-1} \text{ has no coeff. of } \tau^n\}$$

Then X has a right action of $U = \mathbf{U}(\mathbf{F}_{q^n})$, a nonabelian group of order q^{n^2}.

Equation for X

X is an affine hypersurface over $\mathbf{F}_q$ of dimension $n-1$.

Equation for X

X is an affine hypersurface over $\mathbf{F}_q$ of dimension $n-1$.
The equation for X is

$$\det \begin{pmatrix} a_1^{q^n} - a_1 & a_2^{q^n} - a_2 & a_3^{q^n} - a_3 & \cdots & a_{n-1}^{q^n} - a_{n-1} & a_n^{q^n} - a_n \\ 1 & a_1^q & a_2^q & \cdots & a_{n-2}^q & a_{n-1}^q \\ 0 & 1 & a_1^{q^2} & \cdots & a_{n-3}^{q^2} & a_{n-2}^{q^2} \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_1^{q^{n-1}} \end{pmatrix} = 0.$$

Then $\#X(\mathbf{F}_{q^n}) = \#\mathbf{A}^n(\mathbf{F}_{q^n}) = q^{n^2}$.

Theorem

X is maximal over $\mathbf{F}_{q^n}$.

Representation-theoretic complements

How does U act on the spaces $H^i(X)$?

Representation-theoretic complements

How does U act on the spaces $H^i(X)$?
Let $H = \bigoplus_i H^i(X)$.
The center of U is a group Z, isomorphic to $\mathbf{F}_{q^n}$.

Theorem

Let ψ be a character of Z. Then $H[\psi]$ is an irreducible representation of U.

Representation-theoretic complements

How does U act on the spaces $H^i(X)$?
Let $H = \bigoplus_i H^i(X)$.
The center of U is a group Z, isomorphic to $\mathbf{F}_{q^n}$.

Theorem

Let ψ be a character of Z. Then $H[\psi]$ is an irreducible representation of U.

Thus H is a direct sum of irreducible representations of U, each appearing with multiplicity 1!

Representation-theoretic complements

How does U act on the spaces $H^i(X)$?
Let $H = \bigoplus_i H^i(X)$.
The center of U is a group Z, isomorphic to $\mathbf{F}_{q^n}$.

Theorem

Let ψ be a character of Z. Then $H[\psi]$ is an irreducible representation of U.

Thus H is a direct sum of irreducible representations of U, each appearing with multiplicity 1!
This is a microcosm of the world of Shimura varieties, whose cohomology has nice representation-theoretic properties.