A geometric interpretation of additive problems for primes

E. Kowalski

ETH Zürich

Berlin, May 2016

Additive questions with primes

Bizarre questions like Fermat's problem or problems on sums of prime numbers were elevated to supposedly central problems of mathematics. ("Why add prime numbers?" marvelled the great physicist Lev Landau. "Prime numbers are made to be multiplied, not added!")

V.I. Arnold, "*Will mathematics survive?*"
Math. Intelligencer, 1995

Classical additive problems

Problem (Prime Number Theorem)

How many prime numbers are there less than a given quantity?

Classical additive problems

Problem (Prime Number Theorem)

How many prime numbers are there less than a given quantity?

This was solved in 1896 by Hadamard and de la Vallée-Poussin: the number of primes $p \leq X$ is about $X/(\log X)$ as $X \to +\infty$.

Classical additive problems

Problem (Prime Number Theorem)

How many prime numbers are there less than a given quantity?

This was solved in 1896 by Hadamard and de la Vallée-Poussin: the number of primes $p \leq X$ is about $X/(\log X)$ as $X \to +\infty$.

Problem (Twin primes)

Do there exist infinitely many primes p such that $p+2$ is also prime?

Problem (Goldbach Problem)

If n is a large enough even integer, do there exist primes p and q such that $p+q=n$?

The Schinzel Hypothesis

Problem (Schinzel)

Let $F \in \mathbf{Z}[Y]$ be an irreducible polynomial. Assume that for all primes p, there exists some integer n with $p \nmid F(n)$. Is the set of integers n such that $F(n)$ is a prime (up to sign) infinite?

The Schinzel Hypothesis

Problem (Schinzel)

Let $F \in \mathbf{Z}[Y]$ be an irreducible polynomial. Assume that for all primes p, there exists some integer n with $p \nmid F(n)$. Is the set of integers n such that $F(n)$ is a prime (up to sign) infinite?

The answer is *expected* to be "Yes" (the *Schinzel Hypothesis*). It is *known* to be "Yes" if $\deg(F) = 1$ (Dirichlet). It is not known for any polynomial of degree ≥ 2.

The function field analogue

Number field	Function field
$\mathbf{Z}$	$A = \mathbf{F}_q[X]$
prime $\pm p \in \mathbf{Z}$	irreducible polynomial $\pi \in A$
polynomial $F \in \mathbf{Z}[Y]$	polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$
positive integers $n \leq N$	polynomials $f \in A$ of degree d
$N \to +\infty$	$d \to +\infty$

The function field analogue

Number field	Function field
$\mathbf{Z}$	$A = \mathbf{F}_q[X]$
prime $\pm p \in \mathbf{Z}$	irreducible polynomial $\pi \in A$
polynomial $F \in \mathbf{Z}[Y]$	polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$
positive integers $n \leq N$	polynomials $f \in A$ of degree d
$N \to +\infty$	$d \to +\infty$

Problem (Schinzel)

Let $A = \mathbf{F}_q[X]$. Let $F \in A[Y]$, irreducible. For $d \to +\infty$, how many polynomials $f \in A$ of degree d are there such that $F(f)$ is irreducible in A?

The function field analogue

Number field	Function field
$\mathbf{Z}$	$A = \mathbf{F}_q[X]$
prime $\pm p \in \mathbf{Z}$	irreducible polynomial $\pi \in A$
polynomial $F \in \mathbf{Z}[Y]$	polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$
positive integers $n \leq N$	polynomials $f \in A$ of degree d
$N \to +\infty$	$d \to +\infty$

Problem (Schinzel)

Let $A = \mathbf{F}_q[X]$. Let $F \in A[Y]$, irreducible. For $d \to +\infty$, how many polynomials $f \in A$ of degree d are there such that $F(f)$ is irreducible in A?

Example. $p = 17$, $F = Y^2 - (X^3 - X)$, $f = X^2 + 2$; then $F(f) = X^4 - X^3 + 4X^2 + X + 4$ is irreducible.

Features of the function field case

Features of the function field case

- New tools: for instance, $f \in A$ is squarefree if and only if $(f, f') = 1$; or the Frobenius (or Frobenii);

Features of the function field case

- New tools: for instance, $f \in A$ is squarefree if and only if $(f, f') = 1$; or the Frobenius (or Frobenii);
- New variables: instead of fixing g and letting d go to infinity, one can consider a fixed degree $d \geq 1$, and extend the base field $\mathbf{F}_q$ to $\mathbf{F}_{q^\nu}$ with $\nu \to +\infty$;

Features of the function field case

- New tools: for instance, $f \in A$ is squarefree if and only if $(f, f') = 1$; or the Frobenius (or Frobenii);
- New variables: instead of fixing g and letting d go to infinity, one can consider a fixed degree $d \geq 1$, and extend the base field $\mathbf{F}_q$ to $\mathbf{F}_{q^\nu}$ with $\nu \to +\infty$;
- **New points of view**: polynomials can be interpreted as *functions* on the affine line, and this leads to geometric intuition and ideas.

Group-theoretic interpretation of irreducibility

Group-theoretic interpretation of irreducibility

- Fix an algebraic closure $\bar{\mathbf{F}}_q$.

Group-theoretic interpretation of irreducibility

- Fix an algebraic closure $\bar{\mathbf{F}}_q$.
- Let $f \in A$ be a polynomial of degree $d \geq 1$.

Group-theoretic interpretation of irreducibility

- Fix an algebraic closure $\bar{\mathbf{F}}_q$.
- Let $f \in A$ be a polynomial of degree $d \geq 1$.
- The Frobenius automorphism $x \mapsto x^q$ permutes the set of roots of f in $\bar{\mathbf{F}}_q$.

Group-theoretic interpretation of irreducibility

- Fix an algebraic closure $\bar{\mathbf{F}}_q$.
- Let $f \in A$ be a polynomial of degree $d \geq 1$.
- The Frobenius automorphism $x \mapsto x^q$ permutes the set of roots of f in $\bar{\mathbf{F}}_q$.
- The polynomial f is irreducible in A if and only if this permutation Fr_f is a d-cycle.

Geometric interpretation of irreducibility of $F(f)$

We fix a (non-constant) irreducible polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$.

Let $f \in A$ be a polynomial of degree $d \geq 1$. Generically, the degree of $F(f)$ is fixed, say equal to n. Assume this is the case.

Geometric interpretation of irreducibility of $F(f)$

We fix a (non-constant) irreducible polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$.

Let $f \in A$ be a polynomial of degree $d \geq 1$. Generically, the degree of $F(f)$ is fixed, say equal to n. Assume this is the case.

- The polynomial $F(f)$ is irreducible if and only if $\mathrm{Fr}_{F(f)}$ acts on the roots of $F(f)$ like an n-cycle;

Geometric interpretation of irreducibility of $F(f)$

We fix a (non-constant) irreducible polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$.

Let $f \in A$ be a polynomial of degree $d \geq 1$. Generically, the degree of $F(f)$ is fixed, say equal to n. Assume this is the case.

- The polynomial $F(f)$ is irreducible if and only if $\mathrm{Fr}_{F(f)}$ acts on the roots of $F(f)$ like an n-cycle;
- The roots of $F(f)$ are the elements $x \in \bar{\mathbf{F}}_q$ such that

$$0 = F(f)(x) = F(x, f(x));$$

[e.g., $(f^2 - (X^3 - X))(x) = f(x)^2 - (x^3 - x)$.]

Geometric interpretation of irreducibility of $F(f)$

We fix a (non-constant) irreducible polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$.

Let $f \in A$ be a polynomial of degree $d \geq 1$. Generically, the degree of $F(f)$ is fixed, say equal to n. Assume this is the case.

- The polynomial $F(f)$ is irreducible if and only if $\mathrm{Fr}_{F(f)}$ acts on the roots of $F(f)$ like an n-cycle;
- The roots of $F(f)$ are the elements $x \in \bar{\mathbf{F}}_q$ such that

$$0 = F(f)(x) = F(x, f(x));$$

  [e.g., $(f^2 - (X^3 - X))(x) = f(x)^2 - (x^3 - x)$.]
- So the roots x of $F(f)$ are the abscissas of points $(x, y) \in \mathbf{A}^2$ such that $y = f(x)$ and $F(x, y) = 0$;

Geometric interpretation of irreducibility of $F(f)$

We fix a (non-constant) irreducible polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$.

Let $f \in A$ be a polynomial of degree $d \geq 1$. Generically, the degree of $F(f)$ is fixed, say equal to n. Assume this is the case.

- The polynomial $F(f)$ is irreducible if and only if $\mathrm{Fr}_{F(f)}$ acts on the roots of $F(f)$ like an n-cycle;
- The roots of $F(f)$ are the elements $x \in \bar{\mathbf{F}}_q$ such that

$$0 = F(f)(x) = F(x, f(x));$$

  [e.g., $(f^2 - (X^3 - X))(x) = f(x)^2 - (x^3 - x)$.]
- So the roots x of $F(f)$ are the abscissas of points $(x, y) \in \mathbf{A}^2$ such that $y = f(x)$ and $F(x, y) = 0$;
- In other words the abscissas of the points $(x, y) \in \Gamma_f \cap S \subset \mathbf{A}^2$, where Γ_f is the graph of f and S is the affine curve with equation $F(x, y) = 0$.

Geometric interpretation of irreducibility of $F(f)$

We fix a (non-constant) irreducible polynomial $F \in A[Y] = \mathbf{F}_q[X, Y]$.

Let $f \in A$ be a polynomial of degree $d \geq 1$. Generically, the degree of $F(f)$ is fixed, say equal to n. Assume this is the case.

- The polynomial $F(f)$ is irreducible if and only if $\mathrm{Fr}_{F(f)}$ acts on the roots of $F(f)$ like an n-cycle;
- The roots of $F(f)$ are the elements $x \in \bar{\mathbf{F}}_q$ such that

$$0 = F(f)(x) = F(x, f(x));$$

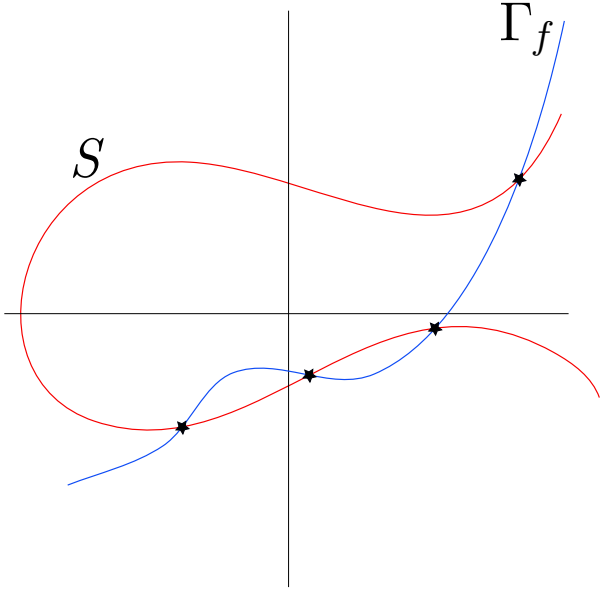
  [e.g., $(f^2 - (X^3 - X))(x) = f(x)^2 - (x^3 - x)$.]
- So the roots x of $F(f)$ are the abscissas of points $(x, y) \in \mathbf{A}^2$ such that $y = f(x)$ and $F(x, y) = 0$;
- In other words the abscissas of the points $(x, y) \in \Gamma_f \cap S \subset \mathbf{A}^2$, where Γ_f is the graph of f and S is the affine curve with equation $F(x, y) = 0$.
- And the Frobenius permutes the roots of $F(f)$ in the same way as it permutes the intersection $\Gamma_f \cap S$.

Good variations

Crucially, if we vary f in an *algebraic family*, the permutation $\mathrm{Fr}_{F(f)}$ of $\Gamma_f \cap S$ varies *algebraically*.

Good variations

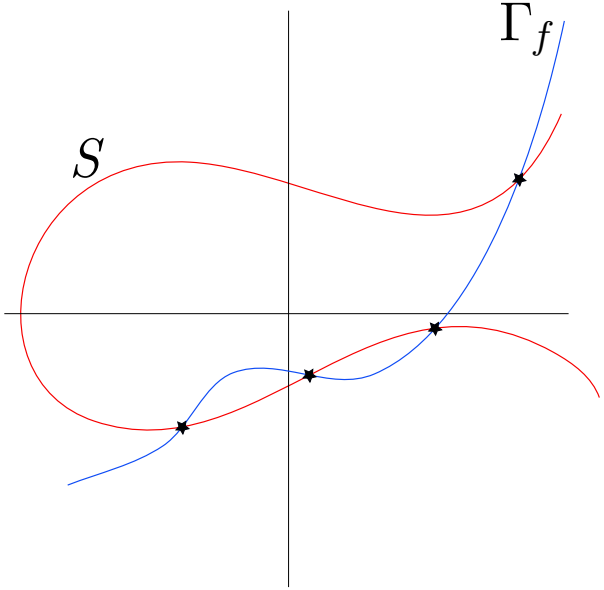
Crucially, if we vary f in an *algebraic family*, the permutation $\mathrm{Fr}_{F(f)}$ of $\Gamma_f \cap S$ varies *algebraically*.



Let $\mathcal{P} \subset \mathbf{A}^{d+1}$ denote the (dense open) space of squarefree polynomials of degree d such that $F(f)$ is squarefree of the generic degree n.

Good variations

Crucially, if we vary f in an *algebraic family*, the permutation $\mathrm{Fr}_{F(f)}$ of $\Gamma_f \cap S$ varies *algebraically*.



Let $\mathcal{P} \subset \mathbf{A}^{d+1}$ denote the (dense open) space of squarefree polynomials of degree d such that $F(f)$ is squarefree of the generic degree n. There is an étale covering

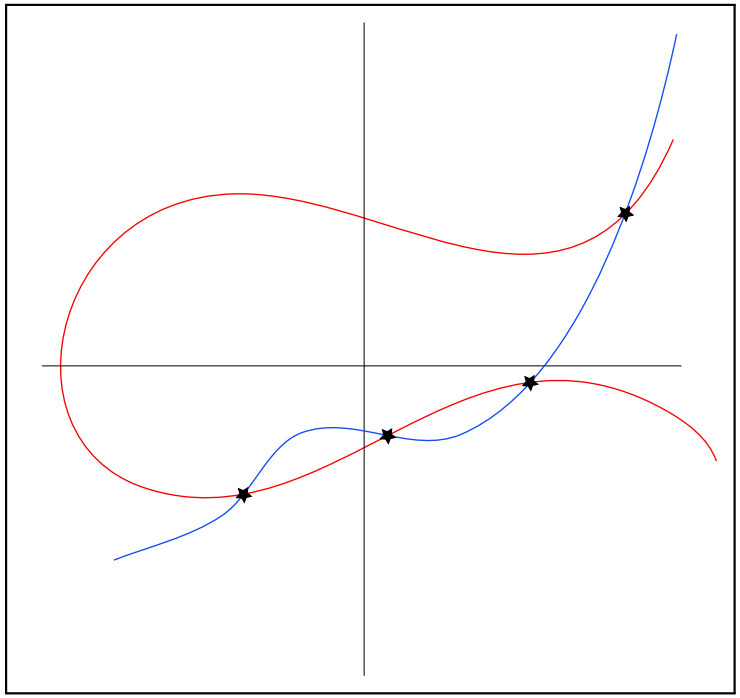
$$\mathcal{Z} = \{(f, x, y) \in \mathcal{P} \times S \mid f(x) = y\}$$
$$\downarrow$$
$$\mathcal{P}$$

of degree n, with fiber over $f \in \mathcal{P}$ equal to the intersection $\Gamma_f \cap S$.

Good variations

By covering theory, the étale covering $\mathcal{Z} \to \mathcal{P}$ induces a group homomorphism

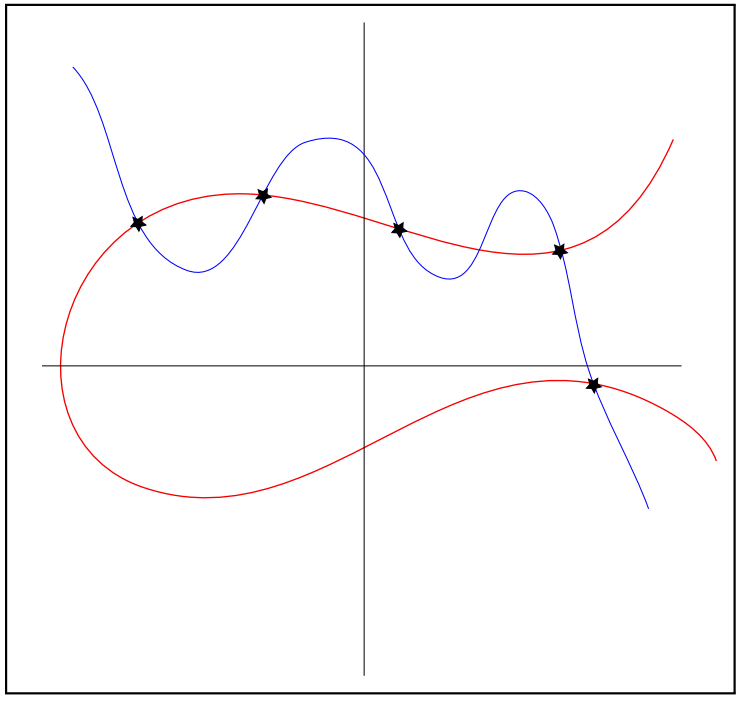
$$\rho\colon \pi_1(\mathcal{P}, \bar{\eta}) \to \mathfrak{S}_n.$$



Good variations

By covering theory, the étale covering $\mathcal{Z} \to \mathcal{P}$ induces a group homomorphism

$$\rho\colon \pi_1(\mathcal{P}, \bar{\eta}) \to \mathfrak{S}_n.$$

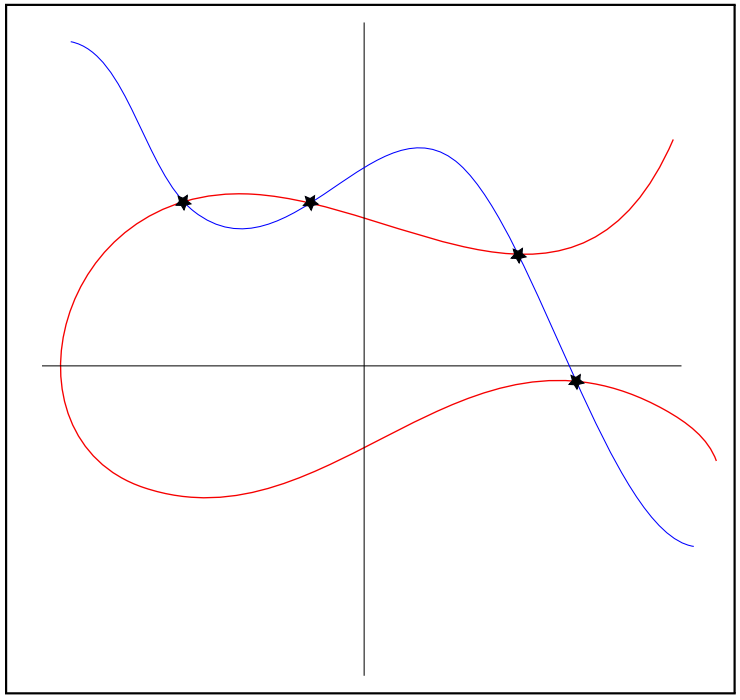


For any $f \in \mathcal{P}(\mathbf{F}_q)$, we obtain a Frobenius conjugacy $\mathrm{Fr}_{f,q}$ class at f by interpreting f as $\mathrm{Spec}(\mathbf{F}_q) \to \mathcal{P}$ and using functoriality of fundamental groups ($\pi_1(\mathrm{Spec}(\mathbf{F}_q)) \simeq \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$.)

Good variations

By covering theory, the étale covering $\mathcal{Z} \to \mathcal{P}$ induces a group homomorphism

$$\rho\colon \pi_1(\mathcal{P}, \bar{\eta}) \to \mathfrak{S}_n.$$



For any $f \in \mathcal{P}(\mathbf{F}_q)$, we obtain a Frobenius conjugacy $\mathrm{Fr}_{f,q}$ class at f by interpreting f as $\mathrm{Spec}(\mathbf{F}_q) \to \mathcal{P}$ and using functoriality of fundamental groups ($\pi_1(\mathrm{Spec}(\mathbf{F}_q)) \simeq \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$.)

The element $\rho(\mathrm{Fr}_{f,q})$ is in the same conjugacy class of $\mathfrak{S}_n$ as $\mathrm{Fr}_{F(f)}$.

Chebotarev density theorem

The Chebotarev density theorem leads in principle to a solution of the Schinzel Problem for F, in the large finite field limit.

Chebotarev density theorem

The Chebotarev density theorem leads in principle to a solution of the Schinzel Problem for F, in the large finite field limit.

Let G be the Galois group of the Galois closure $\tilde{\mathcal{Z}} \to \mathcal{P}$ of the covering $\mathcal{Z} \to \mathcal{P}$ (i.e., the image of $\rho\colon \pi_1(\mathcal{P}, \bar{\eta}) \to \mathfrak{S}_n$). We then have

$$\frac{1}{q^{(d+1)\nu}} |\{f \in \mathcal{P}(\mathbf{F}_{q^\nu}) \mid F(f) \text{ irreducible}\}| \to \mu$$

as $\nu \to +\infty$ (under a mild technical assumption) where

$$\mu = \frac{1}{|G|} |\{\sigma \in G \subset \mathfrak{S}_n \mid \sigma \text{ is conjugated to an } n\text{-cycle}\}|.$$

If $G = \mathfrak{S}_n$, then $\mu = 1/n$.

Chebotarev density theorem

The Chebotarev density theorem leads in principle to a solution of the Schinzel Problem for F, in the large finite field limit.

Let G be the Galois group of the Galois closure $\tilde{\mathcal{Z}} \to \mathcal{P}$ of the covering $\mathcal{Z} \to \mathcal{P}$ (i.e., the image of $\rho\colon \pi_1(\mathcal{P}, \bar{\eta}) \to \mathfrak{S}_n$). We then have

$$\frac{1}{q^{(d+1)\nu}} |\{f \in \mathcal{P}(\mathbf{F}_{q^\nu}) \mid F(f) \text{ irreducible}\}| \to \mu$$

as $\nu \to +\infty$ (under a mild technical assumption) where

$$\mu = \frac{1}{|G|} |\{\sigma \in G \subset \mathfrak{S}_n \mid \sigma \text{ is conjugated to an } n\text{-cycle}\}|.$$

If $G = \mathfrak{S}_n$, then $\mu = 1/n$.

The Schinzel problem becomes: *compute* G, given F and d.

The geometric Schinzel problem

General case

Classical case

The geometric Schinzel problem

General case	Classical case
▶ k arbitrary field;	▶ $k = \mathbf{F}_q$;

The geometric Schinzel problem

General case	Classical case
▶ k arbitrary field;	▶ $k = \mathbf{F}_q$;
▶ C/k smooth projective geometrically connected curve, genus g;	▶ $C = \mathbf{P}^1$, $g = 0$;

The geometric Schinzel problem

General case	Classical case
▶ k arbitrary field;	▶ $k = \mathbf{F}_q$;
▶ C/k smooth projective geometrically connected curve, genus g;	▶ $C = \mathbf{P}^1$, $g = 0$;
▶ D effective divisor on C of degree $d \geq 1$;	▶ $D = d(\infty)$;

The geometric Schinzel problem

General case	Classical case
▶ k arbitrary field;	▶ $k = \mathbf{F}_q$;
▶ C/k smooth projective geometrically connected curve, genus g;	▶ $C = \mathbf{P}^1$, $g = 0$;
▶ D effective divisor on C of degree $d \geq 1$;	▶ $D = d(\infty)$;
▶ $U = C - \mathrm{Supp}(D)$ an affine curve;	▶ $U = \mathbf{A}^1$;

The geometric Schinzel problem

General case	Classical case
▶ k arbitrary field;	▶ $k = \mathbf{F}_q$;
▶ C/k smooth projective geometrically connected curve, genus g;	▶ $C = \mathbf{P}^1$, $g = 0$;
▶ D effective divisor on C of degree $d \geq 1$;	▶ $D = d(\infty)$;
▶ $U = C - \mathrm{Supp}(D)$ an affine curve;	▶ $U = \mathbf{A}^1$;
▶ $S \subset U \times \mathbf{A}^1$ smooth curve, dominant over U;	▶ $S\colon F(x, y) = 0$;

The geometric Schinzel problem

General case	Classical case
▶ k arbitrary field;	▶ $k = \mathbf{F}_q$;
▶ C/k smooth projective geometrically connected curve, genus g;	▶ $C = \mathbf{P}^1$, $g = 0$;
▶ D effective divisor on C of degree $d \geq 1$;	▶ $D = d(\infty)$;
▶ $U = C - \mathrm{Supp}(D)$ an affine curve;	▶ $U = \mathbf{A}^1$;
▶ $S \subset U \times \mathbf{A}^1$ smooth curve, dominant over U;	▶ $S\colon F(x, y) = 0$;
▶ $\mathcal{H}/k$ parameterizing the functions on C with polar divisor D and $d = \deg(D)$ distinct zeros in U; $\dim \mathcal{H} = \deg(D) + 1 - g$.	▶ Squarefree polynomials of degree $d \geq 1$; dimension $d + 1$.

The Schinzel covering

We want to study the variation of the intersection

$$\Gamma_f \cap S \subset U \times S$$

as f varies in $\mathcal{H}(k)$.

The Schinzel covering

We want to study the variation of the intersection

$$\Gamma_f \cap S \subset U \times S$$

as f varies in $\mathcal{H}(k)$.

The first question is to compute the Galois group of the *Schinzel covering*

$$\mathcal{Z} \to \mathcal{H}$$

where

$$\mathcal{Z} = \{(f, x, y) \in \mathcal{H} \times S \mid f(x) = y\}.$$

This is étale of some degree $n \geq 1$ over the dense open subset $\mathcal{H}'$ of $\mathcal{H}$ where the intersection $\Gamma_f \cap S$ is transverse.

Computation of the Galois group

Theorem 1 (K.)

Suppose $\deg(D) \geq 2g+3$, *where* g *is the genus of* C. *If* k *has characteristic* 0, *or under some restrictions*[1] *if* k *has positive characteristic, the Galois group of the Schinzel covering is* $\mathfrak{S}_n$.

Earlier results (for $C = \mathbf{P}^1$, $D = d(\infty)$): (Cohen), Hall, Pollack, Bary-Soroker, Entin.

[1] For instance, if the genus of the projective model of S is ≥ 1 and the characteristic does not divide n.

Arithmetic application, 1

In the context of the classical case, for $k = \mathbf{F}_q$, we obtain:

Corollary

For $\nu \geq 1$, we have

$$\frac{1}{q^{(d+1)\nu}} |\{f \in \mathcal{P}(\mathbf{F}_{q^\nu}) \mid F(f) \text{ irreducible}\}| = \frac{1}{n} + O(Eq^{-\nu/2}),$$

where

$$E = 3 \cdot 2^{5+2n} \cdot (3 + (4+2n)(2n-1)\deg(F))^{d+2n+6} \cdot n^{-1}.$$

This uses an effective version of the Chebotarev Density Theorem based on the general form of the Riemann Hypothesis over finite fields of Deligne, and bounds for Betti numbers due to Bombieri and Katz.

Arithmetic application, 2

The simplest special case of the general problem is

$$S = U \times \{0\} \subset U \times \mathbf{A}^1,$$

which means that we consider the variation of the *zero divisor* of $f \in \mathcal{H}$ (in the classical case, the zeros of a polynomial of degree d). We then have $n = d$.

Arithmetic application, 2

The simplest special case of the general problem is

$$S = U \times \{0\} \subset U \times \mathbf{A}^1,$$

which means that we consider the variation of the *zero divisor* of $f \in \mathcal{H}$ (in the classical case, the zeros of a polynomial of degree d). We then have $n = d$.

It turns out that, in this case, Theorem 1 was proved by Katz under the sole condition $\deg(D) \geq 2g + 1$: the Galois group is $\mathfrak{S}_d$.

Arithmetic application, 2

The simplest special case of the general problem is

$$S = U \times \{0\} \subset U \times \mathbf{A}^1,$$

which means that we consider the variation of the *zero divisor* of $f \in \mathcal{H}$ (in the classical case, the zeros of a polynomial of degree d). We then have $n = d$.

It turns out that, in this case, Theorem 1 was proved by Katz under the sole condition $\deg(D) \geq 2g + 1$: the Galois group is $\mathfrak{S}_d$.

This is particularly interesting when k is a number field, where a corollary is that for a "generic" $f \in \mathcal{H}(k)$, the splitting field of the zero divisor has Galois group $\mathfrak{S}_d$ over k. This can be made quantitative (large sieve, Hilbert Irreducibility Theorem).

Galois computations

What methods do we know to compute Galois groups, or more generally monodromy groups (of ℓ-adic sheaves, or of local systems on manifolds)?

Galois computations

What methods do we know to compute Galois groups, or more generally monodromy groups (of ℓ-adic sheaves, or of local systems on manifolds)? In other words, we have a representation

$$\rho\colon \pi_1(\mathcal{X}, \bar{\eta}) \to \mathrm{GL}_n(K)$$

where the images of the Frobenius classes have some arithmetic meaning, and we wish to compute the image G of ρ, or its Zariski closure.

Galois computations

What methods do we know to compute Galois groups, or more generally monodromy groups (of ℓ-adic sheaves, or of local systems on manifolds)? In other words, we have a representation

$$\rho\colon \pi_1(\mathcal{X}, \bar{\eta}) \to \mathrm{GL}_n(K)$$

where the images of the Frobenius classes have some arithmetic meaning, and we wish to compute the image G of ρ, or its Zariski closure.

"Nature" helps by (often) following the group-theoretic Occam razor: the Galois group is (often) the largest possible group compatible with the natural symmetries of the problem.

Galois computations

What methods do we know to compute Galois groups, or more generally monodromy groups (of ℓ-adic sheaves, or of local systems on manifolds)? In other words, we have a representation

$$\rho\colon \pi_1(\mathcal{X}, \bar{\eta}) \to \mathrm{GL}_n(K)$$

where the images of the Frobenius classes have some arithmetic meaning, and we wish to compute the image G of ρ, or its Zariski closure.

"Nature" helps by (often) following the group-theoretic Occam razor: the Galois group is (often) the largest possible group compatible with the natural symmetries of the problem.

For instance, we might know that the group G is a subgroup of GL_n, but with trivial determinant, hence a subgroup of SL_n; or that G leaves a symplectic pairing invariant (e.g., from Poincaré duality).

Local method

Restrict to an open curve $V \subset \mathcal{X}$ in the parameter space, and use *local monodromy* around singularities to get special elements of the group (for instance, transvections or transpositions) using the composition

$$\pi_1(V, \bar{\eta}) \to \pi_1(\mathcal{X}, \bar{\eta}) \xrightarrow{\rho} \mathrm{GL}_n(K);$$

Local method

Restrict to an open curve $V \subset \mathcal{X}$ in the parameter space, and use *local monodromy* around singularities to get special elements of the group (for instance, transvections or transpositions) using the composition

$$\pi_1(V, \bar{\eta}) \to \pi_1(\mathcal{X}, \bar{\eta}) \xrightarrow{\rho} \mathrm{GL}_n(K);$$

prove then that only the maximal group has these special elements (using maybe a little "global" information, e.g., that G acts irreducibly in some representation).

Local method

Restrict to an open curve $V \subset \mathcal{X}$ in the parameter space, and use *local monodromy* around singularities to get special elements of the group (for instance, transvections or transpositions) using the composition

$$\pi_1(V, \bar{\eta}) \to \pi_1(\mathcal{X}, \bar{\eta}) \xrightarrow{\rho} \mathrm{GL}_n(K);$$

prove then that only the maximal group has these special elements (using maybe a little "global" information, e.g., that G acts irreducibly in some representation).

Example. (1) [Kazhdan–Margulis] A subgroup of $\mathrm{Sp}_{2g}(\mathbf{C})$ acting irreducibly on $\mathbf{C}^{2g}$ and generated by transvections is Zariski-dense in $\mathrm{Sp}_{2g}(\mathbf{C})$.

(2) [Jordan] A subgroup of $\mathfrak{S}_n$ acting transitively and generated by transpositions is $\mathfrak{S}_n$.

Global method

Use arithmetic properties of the problem (and many dimensions of $\mathcal{X}$) to determine global invariants of the group (such as the dimension of invariant vectors in some natural representations);

Global method

Use arithmetic properties of the problem (and many dimensions of $\mathcal{X}$) to determine global invariants of the group (such as the dimension of invariant vectors in some natural representations); prove that the maximal group is characterized by these global invariants (using maybe a little "local" information; e.g., local monodromy to check that a subgroup of an orthogonal group is not contained in SO).

Global method

Use arithmetic properties of the problem (and many dimensions of $\mathcal{X}$) to determine global invariants of the group (such as the dimension of invariant vectors in some natural representations); prove that the maximal group is characterized by these global invariants (using maybe a little "local" information; e.g., local monodromy to check that a subgroup of an orthogonal group is not contained in SO).

Example. [Larsen alternative] If $g \geq 2$, a semisimple algebraic subgroup of $\mathrm{Sp}_{2g}(\mathbf{C})$ whose invariant space in $\mathrm{End}(\mathrm{End}(\mathbf{C}^{2g}))$ has dimension 3 is either finite or equal to $\mathrm{Sp}_{2g}(\mathbf{C})$.

Entin's argument

In the special case $C = \mathbf{P}^1$ over $k = \mathbf{F}_q$, Entin gives a beautiful global argument for $G = \mathfrak{S}_n$:

Entin's argument

In the special case $C = \mathbf{P}^1$ over $k = \mathbf{F}_q$, Entin gives a beautiful global argument for $G = \mathfrak{S}_n$:

- G acts on the generic fiber

$$Z = \{x_1, \ldots, x_n\} = \{ \text{ roots of } F(f) \text{ for "generic" } f \ \};$$

Entin's argument

In the special case $C = \mathbf{P}^1$ over $k = \mathbf{F}_q$, Entin gives a beautiful global argument for $G = \mathfrak{S}_n$:

- G acts on the generic fiber

$$Z = \{x_1, \ldots, x_n\} = \{ \text{ roots of } F(f) \text{ for "generic" } f \ \};$$

- Using the Chebotarev density theorem and the arithmetic definition of G, one can compute the number of orbits of G acting on Z^k for suitable integers k;

Entin's argument

In the special case $C = \mathbf{P}^1$ over $k = \mathbf{F}_q$, Entin gives a beautiful global argument for $G = \mathfrak{S}_n$:

- G acts on the generic fiber

$$Z = \{x_1, \ldots, x_n\} = \{ \text{ roots of } F(f) \text{ for "generic" } f \ \};$$

- Using the Chebotarev density theorem and the arithmetic definition of G, one can compute the number of orbits of G acting on Z^k for suitable integers k;
- This reveals by elementary group theory that the action of G on Z is k-transitive for $k = 6$;

Entin's argument

In the special case $C = \mathbf{P}^1$ over $k = \mathbf{F}_q$, Entin gives a beautiful global argument for $G = \mathfrak{S}_n$:

- G acts on the generic fiber

$$Z = \{x_1, \ldots, x_n\} = \{ \text{ roots of } F(f) \text{ for "generic" } f \ \};$$

- Using the Chebotarev density theorem and the arithmetic definition of G, one can compute the number of orbits of G acting on Z^k for suitable integers k;
- This reveals by elementary group theory that the action of G on Z is k-transitive for $k = 6$;
- The Classification of Finite Simple Groups implies that G contains the alternating group A_n;

Entin's argument

In the special case $C = \mathbf{P}^1$ over $k = \mathbf{F}_q$, Entin gives a beautiful global argument for $G = \mathfrak{S}_n$:

- G acts on the generic fiber

$$Z = \{x_1, \ldots, x_n\} = \{ \text{ roots of } F(f) \text{ for "generic" } f \ \};$$

- Using the Chebotarev density theorem and the arithmetic definition of G, one can compute the number of orbits of G acting on Z^k for suitable integers k;
- This reveals by elementary group theory that the action of G on Z is k-transitive for $k = 6$;
- The Classification of Finite Simple Groups implies that G contains the alternating group A_n;
- A separate local argument "finds" an odd element of G, so $G = \mathfrak{S}_n$.

Idea of the proof of Theorem 1

We build on Katz's (implicit) local proof in the case $S = U \times \{0\}$. We may assume that k is algebraically closed (since extending the base field could only make G smaller).

Idea of the proof of Theorem 1

We build on Katz's (implicit) local proof in the case $S = U \times \{0\}$. We may assume that k is algebraically closed (since extending the base field could only make G smaller).
We then consider one-parameter families of functions. The simplest are given by

$$f_t = f + t$$

where $f \in \mathcal{H}$ is fixed and t varies in $\mathbf{A}^1$.

Idea of the proof of Theorem 1

We build on Katz's (implicit) local proof in the case $S = U \times \{0\}$. We may assume that k is algebraically closed (since extending the base field could only make G smaller).
We then consider one-parameter families of functions. The simplest are given by

$$f_t = f + t$$

where $f \in \mathcal{H}$ is fixed and t varies in $\mathbf{A}^1$.
The fiber of $\mathcal{Z} \to \mathcal{H}$ over f_t is the set of points (x, y) in S with

$$y = f_t(x) = f(x) + t,$$

Idea of the proof of Theorem 1

We build on Katz's (implicit) local proof in the case $S = U \times \{0\}$. We may assume that k is algebraically closed (since extending the base field could only make G smaller).
We then consider one-parameter families of functions. The simplest are given by

$$f_t = f + t$$

where $f \in \mathcal{H}$ is fixed and t varies in $\mathbf{A}^1$.
The fiber of $\mathcal{Z} \to \mathcal{H}$ over f_t is the set of points (x, y) in S with

$$y = f_t(x) = f(x) + t,$$

or in other words the set of solutions $(x, y) \in S$ of the equation $g(x, y) = t$, where g is the function *on* S defined by

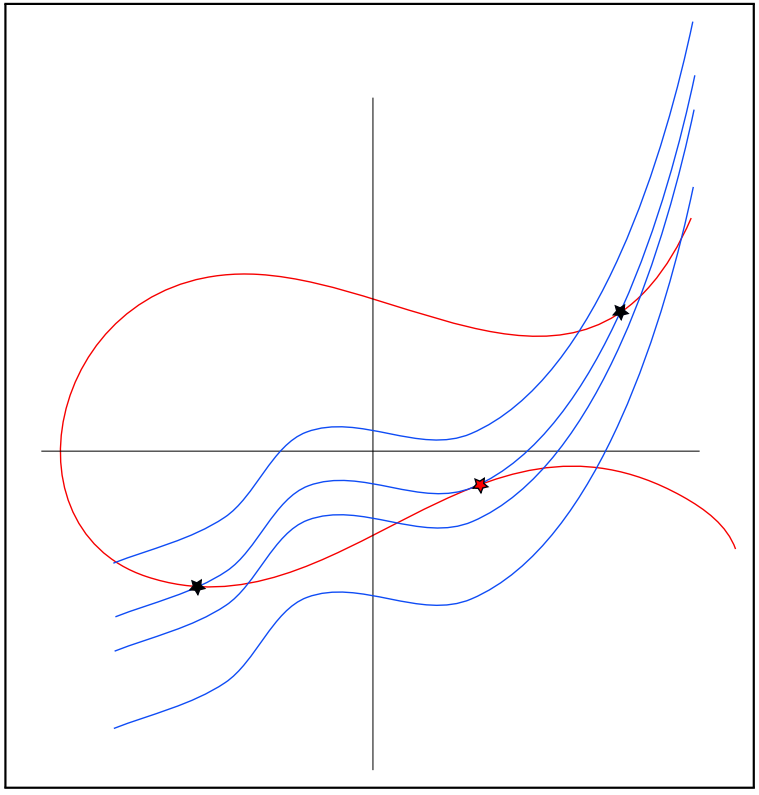
$$g(x, y) = y - f(x).$$

Lefschetz pencils

In much greater generality, given a morphism $h\colon \mathcal{X} \to \mathbf{P}^1$ on an algebraic variety, the variation with $t \in \mathbf{P}^1$ of the solutions of $h(x) = t$ is the *very* classical topic of *hyperplane sections* of an algebraic variety. In particular, if h defines a *Lefschetz pencil*, then one knows a lot about this problem.

Lefschetz pencils

In much greater generality, given a morphism $h\colon \mathcal{X} \to \mathbf{P}^1$ on an algebraic variety, the variation with $t \in \mathbf{P}^1$ of the solutions of $h(x) = t$ is the *very* classical topic of *hyperplane sections* of an algebraic variety. In particular, if h defines a *Lefschetz pencil*, then one knows a lot about this problem.



In our case, $g = Y - f(X)$ defines a Lefschetz pencil on S if

1. there are finitely many "singularities" $t \in \mathbf{A}^1$ where $g = t$ has less than n roots;
2. for such t we have a single double root;
3. and g separates these singular points.

If $\deg(D) \geq 2g + 1$, a "generic" f has these properties (Katz).

Characteristic 0 case

In characteristic 0, the existence of an f such that $g(x, y) = f(x) - y$ defines a Lefschetz pencil is enough to compute the Galois group because of:

Theorem 2 (Folklore?)

Assume k is algebraically closed of characteristic 0. Let $g\colon \tilde{S} \to \mathbf{P}^1$ be a function on a smooth projective connected curve $\tilde{S}/k$ which defines a Lefschetz pencil. Then over a dense open set where g is étale of degree n, the Galois group of the covering g is $\mathfrak{S}_n$.

Characteristic 0 case

In characteristic 0, the existence of an f such that $g(x, y) = f(x) - y$ defines a Lefschetz pencil is enough to compute the Galois group because of:

Theorem 2 (Folklore?)

Assume k is algebraically closed of characteristic 0. Let $g\colon \tilde{S} \to \mathbf{P}^1$ be a function on a smooth projective connected curve $\tilde{S}/k$ which defines a Lefschetz pencil. Then over a dense open set where g is étale of degree n, the Galois group of the covering g is $\mathfrak{S}_n$.

Why?

Characteristic 0 case

In characteristic 0, the existence of an f such that $g(x, y) = f(x) - y$ defines a Lefschetz pencil is enough to compute the Galois group because of:

Theorem 2 (Folklore?)

Assume k is algebraically closed of characteristic 0. Let $g\colon \tilde{S} \to \mathbf{P}^1$ be a function on a smooth projective connected curve $\tilde{S}/k$ which defines a Lefschetz pencil. Then over a dense open set where g is étale of degree n, the Galois group of the covering g is $\mathfrak{S}_n$.

Why?

- The Galois group G is transitive (because $\tilde{S}$ is connected);

Characteristic 0 case

In characteristic 0, the existence of an f such that $g(x, y) = f(x) - y$ defines a Lefschetz pencil is enough to compute the Galois group because of:

Theorem 2 (Folklore?)

Assume k is algebraically closed of characteristic 0. Let $g\colon \tilde{S} \to \mathbf{P}^1$ be a function on a smooth projective connected curve $\tilde{S}/k$ which defines a Lefschetz pencil. Then over a dense open set where g is étale of degree n, the Galois group of the covering g is $\mathfrak{S}_n$.

Why?

- The Galois group G is transitive (because $\tilde{S}$ is connected);
- The Galois group G is generated by transpositions (coming from the inertia action at the *finite* singularities, which generate G because $\mathbf{A}^1$ is simply connected in characteristic 0);

Characteristic 0 case

In characteristic 0, the existence of an f such that $g(x, y) = f(x) - y$ defines a Lefschetz pencil is enough to compute the Galois group because of:

Theorem 2 (Folklore?)

Assume k is algebraically closed of characteristic 0. Let $g\colon \tilde{S} \to \mathbf{P}^1$ be a function on a smooth projective connected curve $\tilde{S}/k$ which defines a Lefschetz pencil. Then over a dense open set where g is étale of degree n, the Galois group of the covering g is $\mathfrak{S}_n$.

Why?

- The Galois group G is transitive (because $\tilde{S}$ is connected);
- The Galois group G is generated by transpositions (coming from the inertia action at the *finite* singularities, which generate G because $\mathbf{A}^1$ is simply connected in characteristic 0);
- Jordan's elementary group-theory criterion.

Positive characteristic

In characteristic $p > 0$, the affine line is far from being (algebraically) simply connected.

Katz and Rains extended Theorem 2 to functions g which define a Lefschetz pencil *and* satisfy an additional property, related to poles of the differential dg.

Positive characteristic

In characteristic $p > 0$, the affine line is far from being (algebraically) simply connected.

Katz and Rains extended Theorem 2 to functions g which define a Lefschetz pencil *and* satisfy an additional property, related to poles of the differential dg.

- If g has a pole of order k coprime to p at some point $x \in S$, then dg has always a pole of order $k+1$ at x;

Positive characteristic

In characteristic $p > 0$, the affine line is far from being (algebraically) simply connected.

Katz and Rains extended Theorem 2 to functions g which define a Lefschetz pencil *and* satisfy an additional property, related to poles of the differential dg.

- If g has a pole of order k coprime to p at some point $x \in S$, then dg has always a pole of order $k+1$ at x;
- but if k is divisible by p, the differential dg might even have no pole at x!

Positive characteristic

In characteristic $p > 0$, the affine line is far from being (algebraically) simply connected.

Katz and Rains extended Theorem 2 to functions g which define a Lefschetz pencil *and* satisfy an additional property, related to poles of the differential dg.

- If g has a pole of order k coprime to p at some point $x \in S$, then dg has always a pole of order $k+1$ at x;
- but if k is divisible by p, the differential dg might even have no pole at x!
- In this case, Katz and Rains show that for a generic function g, the order of the pole is k: only the coefficient of $\pi^{-(k+1)}$ of dg is zero;

Positive characteristic

In characteristic $p > 0$, the affine line is far from being (algebraically) simply connected.

Katz and Rains extended Theorem 2 to functions g which define a Lefschetz pencil *and* satisfy an additional property, related to poles of the differential dg.

- If g has a pole of order k coprime to p at some point $x \in S$, then dg has always a pole of order $k+1$ at x;
- but if k is divisible by p, the differential dg might even have no pole at x!
- In this case, Katz and Rains show that for a generic function g, the order of the pole is k: only the coefficient of $\pi^{-(k+1)}$ of dg is zero;
- Then they show that Theorem 2 holds for such generic functions (criterion: a primitive subgroup of $\mathfrak{S}_n$ containing a transposition is $\mathfrak{S}_n$).

"Strong" Lefschetz functions

However, the functions $g(x, y) = y - f(x)$ that we use are *not* generic in this sense! The order of the pole of dg will usually "drop" by more than one.

"Strong" Lefschetz functions

However, the functions $g(x, y) = y - f(x)$ that we use are *not* generic in this sense! The order of the pole of dg will usually "drop" by more than one.

We can extend the result of Katz and Rains if $p \neq 2$, S has genus ≥ 1, and either $p \nmid n$, or n is a prime; we show that it holds under these assumptions when dg has a pole *of some order* at all poles of g.

"Strong" Lefschetz functions

However, the functions $g(x, y) = y - f(x)$ that we use are *not* generic in this sense! The order of the pole of dg will usually "drop" by more than one.

We can extend the result of Katz and Rains if $p \neq 2$, S has genus ≥ 1, and either $p \nmid n$, or n is a prime; we show that it holds under these assumptions when dg has a pole *of some order* at all poles of g.

This assumption holds for $g = Y - f(X)$ for generic $f \in \mathcal{H}'$.

The genuine Schinzel problem

The real goal is to study the Schinzel problem for a fixed finite field k and a fixed curve S, for a sequence of divisors with $\deg(D) \to +\infty$, for instance $D = d(\infty)$ on $\mathbf{P}^1$.

The genuine Schinzel problem

The real goal is to study the Schinzel problem for a fixed finite field k and a fixed curve S, for a sequence of divisors with $\deg(D) \to +\infty$, for instance $D = d(\infty)$ on $\mathbf{P}^1$.

In principle, the Grothendieck–Lefschetz trace formula reduces to problem to understanding the Frobenius action on the étale cohomology groups

$$H_c^i(\mathcal{H}_D \times \bar{k}, \mathcal{F}_\pi)$$

where π runs over the irreducible representations of $\mathfrak{S}_n$ that occur in the decomposition of the characteristic function of n-cycles (known since Frobenius), and $\mathcal{F}_\pi$ is the lisse ℓ-adic sheaf corresponding to

$$\rho\colon \pi_1(\mathcal{H}_D, \bar{\eta}) \to \mathfrak{S}_n \to \mathrm{GL}(V_\pi).$$

The genuine Schinzel problem

The real goal is to study the Schinzel problem for a fixed finite field k and a fixed curve S, for a sequence of divisors with $\deg(D) \to +\infty$, for instance $D = d(\infty)$ on $\mathbf{P}^1$.

In principle, the Grothendieck–Lefschetz trace formula reduces to problem to understanding the Frobenius action on the étale cohomology groups

$$H_c^i(\mathcal{H}_D \times \bar{k}, \mathcal{F}_\pi)$$

where π runs over the irreducible representations of $\mathfrak{S}_n$ that occur in the decomposition of the characteristic function of n-cycles (known since Frobenius), and $\mathcal{F}_\pi$ is the lisse ℓ-adic sheaf corresponding to

$$\rho\colon \pi_1(\mathcal{H}_D, \bar{\eta}) \to \mathfrak{S}_n \to \mathrm{GL}(V_\pi).$$

In other words, one has to understand the cohomology groups $H_c^i(\tilde{\mathcal{Z}}_D \times \bar{k}, \bar{\mathbf{Q}}_\ell)$ as $\mathfrak{S}_n$-representations, where $\tilde{\mathcal{Z}}_D \to \mathcal{H}_D$ is the Galois closure of the Schinzel covering.

The simplest case

Let $C = \mathbf{P}^1$ and $D = d(\infty)$. Take $S = \mathbf{A}^1 \times \{0\}$. The space $\mathcal{H}_D$ is the space of squarefree polynomials of degree d. The covering $\tilde{\mathcal{Z}}_D \to \mathcal{H}_D$ can be identified with

$$\{(a, a_1, \ldots, a_d) \in \mathbf{G}_m \times \mathbf{A}^d \mid a_i \neq a_j \text{ if } i \neq j\} \to \mathcal{H}_D$$

given by $(a, a_1, \ldots, a_d) \mapsto a(X - a_1) \cdots (X - a_d)$.

The simplest case

Let $C = \mathbf{P}^1$ and $D = d(\infty)$. Take $S = \mathbf{A}^1 \times \{0\}$. The space $\mathcal{H}_D$ is the space of squarefree polynomials of degree d. The covering $\tilde{\mathcal{Z}}_D \to \mathcal{H}_D$ can be identified with

$$\{(a, a_1, \ldots, a_d) \in \mathbf{G}_m \times \mathbf{A}^d \mid a_i \neq a_j \text{ if } i \neq j\} \to \mathcal{H}_D$$

given by $(a, a_1, \ldots, a_d) \mapsto a(X - a_1) \cdots (X - a_d)$.

So $\tilde{\mathcal{Z}}_D/\mathbf{G}_m$ is the ordered configuration space of d points on $\mathbf{A}^1$, and $\mathcal{H}_D/\mathbf{G}_m$ is the unordered configuration space, whose cohomology was first famously computed by Arnold.

The simplest case

Lehrer and Solomon determined the $\mathfrak{S}_n$-representation on the cohomology of $\tilde{\mathcal{Z}}_D$. Using this, the Grothendieck–Lefschetz trace formula approach has been implemented by Church, Ellenberg and Farb in this case.

The simplest case

Lehrer and Solomon determined the $\mathfrak{S}_n$-representation on the cohomology of $\tilde{\mathcal{Z}}_D$. Using this, the Grothendieck–Lefschetz trace formula approach has been implemented by Church, Ellenberg and Farb in this case.

They recover "topologically" the formula

$$|\mathcal{H}_D(\mathbf{F}_q)| = (q-1)(q^d - q^{d-1}),$$

and also the formula of Gauss for the number of irreducible polynomials of degree d in $\mathbf{F}_q[X]$, hence in particular the (elementary!) Prime Number Theorem for $\mathbf{F}_q[X]$.

Going further?

- For general C and $S = U \times \{0\}$, the issue is to understand the cohomology (even with trivial coefficients) of a configuration space of distinct points on C whose sum in the Jacobian is fixed.

Going further?

- For general C and $S = U \times \{0\}$, the issue is to understand the cohomology (even with trivial coefficients) of a configuration space of distinct points on C whose sum in the Jacobian is fixed.
- For $C = \mathbf{P}^1$ and $D = d(\infty)$ with general S, the degree n depends stably on d as $n = ad + b$ where a and b depend on S; this gives sequences of configuration spaces where the number of points changes by the addition of a new points when d increases by 1. What kind of algebraic/topological structure encodes this type of variation?