MARSEILLE, 13 OCTOBER 2022

L.COLÒ I2M

THE WEIL BOUND & ITS FIRST REFINEMENT

LEONARDO COLÒ
Institut de Mathématiques de Marseille

Groupe de Travail ATI - Arithmétique et Théorie de l'Information

CURVES

Let X be a genus g curve over a finite field $\mathbb{F}_q$.

Frobenius

For any commutative $\mathbb{F}_q$-algebra R, the map $x \mapsto x^q$ is an $\mathbb{F}_q$-homomorphism from R to itself. For any scheme X over $\mathbb{F}_q$, this construction induces $F : X \to X$ called the Frobenius of X.
Let $\overline{X} = X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, then $\overline{X}$ is a smooth irreducible projective curve and

$$\begin{aligned} F : \overline{X} &\longrightarrow \overline{X} \\ (x_0 : \ldots : x_d) &\longmapsto (x_0^q : \ldots : x_d^q) \end{aligned}$$

has degree q.

$$X(\mathbb{F}_q) = \mathrm{Fix}\left(F, \overline{X}(\overline{\mathbb{F}}_q)\right)$$

WEIL AND HASSE BOUNDS

L.COLÒ I2M

Weil bound

Let X be a genus g curve over $\mathbb{F}_q$. We let $N(X) = \#X(\mathbb{F}_q)$. Then

$$|N(X) - (q+1)| \leq 2g\sqrt{q}$$

Hasse bound

Let E be an elliptic curve over $\mathbb{F}_q$. Then

$$|N(E) - (q+1)| \leq 2\sqrt{q}$$

HASSE BOUNDS - AN EXAMPLE

Consider the elliptic curve $E : y^2 = x^3 - x + 1$. Then

q	$N_q(E)$	$\lvert N(E) - (q+1)\rvert$	$2\sqrt{q}$
3	7	3	3.46
5	8	2	4.47
7	12	4	5.29
9	7	3	6
11	10	2	6.63
13	19	5	7.21
17	14	4	8.25
19	22	2	8.72
25	32	6	10
27	28	0	10.39
29	37	7	10.77
31	35	3	11.14
37	36	2	12.17
49	48	2	14

Hasse Bounds - Sketch of Proof

- The Frobenius endomorphism of E generates the Galois group $\mathcal{G}al(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.
- Then, for all $P \in E(\overline{\mathbb{F}}_q)$, we have

$$P \in E(\mathbb{F}_q) \quad \text{if and only if} \quad F(P) = P$$

- Thus, $E(\mathbb{F}_q) = \ker(1 - F)$
- In particular, as $1 - F$ is a separable isogeny, this implies

$$\#E(\mathbb{F}_q) = \#\ker(1 - F) = \deg(1 - F)$$

- Cauchy-Schwarz inequality gives

$$|\deg(1 - F) - \deg(F) - \deg(1)| \leq 2\sqrt{\deg(F)\deg(1)}$$

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

Silverman, J.H. *The arithmetic of elliptic curves*, Springer, 2009

Weil bounds - how to go about proving it

L.COLÒ I2M

There are many different approaches to the Weil bound.

- Cohomology
- Intersection theory on the self-product of the curve (Weil's second proof)
- Comparison of a curve with its Jacobian (Weil's original argument)
- Polynomial methods (Bombieri-Stepanov)

Hartshorne, R. *Algebraic Geometry*, Springer, 1977

Freitag, E. and Kiehl, R. *Etale cohomology and the Weil conjecture*, Springer, 1988

The idea is that counting fixed points of a self-map on a space should have something to do with computing traces of some associated linear map[1].

Example. If σ is a permutation of $\{1, \ldots, n\}$, then the number of fixed points of σ is equal to the trace of the permutation matrix associated to σ.

Example. [*Lefschetz trace formula*]. Let $T : S \to S$ be a continuous map of a topological space. Under suitable conditions, the quantity

$$\sum_i (-1)^i \operatorname{Trace}(T, H^i(S))$$

gives a weighted count of the fixed points of T; in particular, the nonvanishing of this quantity can be used to establish the existence of a fixed point of T.

[1] Kedlaya, K. *Course Math 206A - Topics in Algebraic Geometry: Weil cohomology in practice*

For some field K of characteristic zero, there is a series of contravariant "cohomological" functors

$$H^i : \{\text{algebraic varieties over } \mathbb{F}_q\} \longrightarrow \{\text{finite dimensional vector spaces over } K\}$$

satisfying the following formula: for $i = 0, \ldots, 2d = 2\dim(X)$

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d} (-1)^i \operatorname{Trace}(F^n, H^i(X))$$

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- $H^i(X)$ is a finite dimensional vector space over K and $H^i(X) = 0$ for $i > 2d$.

THE COHOMOLOGY APPROACH - CLASSICAL COHOMOLOGY

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- $H^i(X)$ is a finite dimensional vector space over K and $H^i(X) = 0$ for $i > 2d$.
- *Poincaré Duality*. There is a bilinear form $H^i(X) \times H^{2d-i} \to H^{2d} \simeq K$ allowing the identification

$$H^{2d-i}(X) \rightsquigarrow H_i(X) = \mathrm{Hom}(H^i(X), K)$$

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- $H^i(X)$ is a finite dimensional vector space over K and $H^i(X) = 0$ for $i > 2d$.
- *Poincaré Duality*. There is a bilinear form $H^i(X) \times H^{2d-i} \to H^{2d} \simeq K$ allowing the identification

$$H^{2d-i}(X) \rightsquigarrow H_i(X) = \mathrm{Hom}(H^i(X), K)$$

- *Künneth formula* $H^\bullet(X) \otimes H^\bullet(Y) \simeq H^\bullet(X \times Y)$

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- $H^i(X)$ is a finite dimensional vector space over K and $H^i(X) = 0$ for $i > 2d$.
- *Poincaré Duality*. There is a bilinear form $H^i(X) \times H^{2d-i} \to H^{2d} \simeq K$ allowing the identification

$$H^{2d-i}(X) \rightsquigarrow H_i(X) = \mathrm{Hom}(H^i(X), K)$$

- *Künneth formula* $H^\bullet(X) \otimes H^\bullet(Y) \simeq H^\bullet(X \times Y)$
- Any morphism $f : X \to X$ defines a linear map $f^{(i)} : H^i(X) \to H^i(X)$ such that the $f^{(i)}$ constitute a homomorphism of algebras $f^\bullet : H^\bullet(X) \to H^\bullet(X)$.

$$\mathrm{Fix}(f, X) = \sum_{i=0}^{2d} (-1)^n \, \mathrm{Trace}(f^{(i)})$$

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- $H^i(X)$ is a finite dimensional vector space over K and $H^i(X) = 0$ for $i > 2d$.
- *Poincaré Duality*. There is a bilinear form $H^i(X) \times H^{2d-i} \to H^{2d} \simeq K$ allowing the identification

$$H^{2d-i}(X) \rightsquigarrow H_i(X) = \mathrm{Hom}(H^i(X), K)$$

- *Künneth formula* $H^\bullet(X) \otimes H^\bullet(Y) \simeq H^\bullet(X \times Y)$
- Any morphism $f : X \to X$ defines a linear map $f^{(i)} : H^i(X) \to H^i(X)$ such that the $f^{(i)}$ constitute a homomorphism of algebras $f^\bullet : H^\bullet(X) \to H^\bullet(X)$.

$$\mathrm{Fix}(f, X) = \sum_{i=0}^{2d} (-1)^n \,\mathrm{Trace}(f^{(i)})$$

- If Y is a nonsingular subvariety of X of dimension $d-1$ then there is a natural mapping $H^i(X) \to H^i(Y)$ which is bijective for $i \leq d-2$ and injective for $i = d-1$

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- Let $h \in H^2(X)$ and $L : a \to ah$ be the multiplication-by h map in $H^\bullet(X)$; then $L^{d-i} : H^i(X) \to H^{2d-i}(X)$ is an isomorphism for $i \leq d$.
  This implies that if we have a morphism $f : X \to X$ such that $f^{(2)}(h) = qh$ where $q > 0$ is a rational number, then $g_i = q^{-i/2} f^{(i)}$ is an automorphism of $H^i(X) \otimes_K \overline{K}$ and if $\alpha_{i,j}$ are the eigenvalues of $f^{(i)}$ in $\overline{K}$, then $\{q^{i/2}/\alpha_{i,j}\}_{i,j} = \{\alpha_{2d-i,j}/q^{d-(i/2)}\}$

$$H^\bullet(X) = \bigoplus_i H^i(X)$$

- Let $h \in H^2(X)$ and $L : a \to ah$ be the multiplication-by h map in $H^\bullet(X)$; then $L^{d-i} : H^i(X) \to H^{2d-i}(X)$ is an isomorphism for $i \leq d$.
  This implies that if we have a morphism $f : X \to X$ such that $f^{(2)}(h) = qh$ where $q > 0$ is a rational number, then $g_i = q^{-i/2} f^{(i)}$ is an automorphism of $H^i(X) \otimes_K \overline{K}$ and if $\alpha_{i,j}$ are the eigenvalues of $f^{(i)}$ in $\overline{K}$, then $\{q^{i/2}/\alpha_{i,j}\}_{i,j} = \{\alpha_{2d-i,j}/q^{d-(i/2)}\}$
- In each $H^i(X)$ for $i \leq d$ there is a subspace $A^i(X)$ stable under $f^{(i)}$ and on each $A^i(X)$, as v.s., there is a scalar product such that, if f verifies $f(h) = qh$, each g_i is a unitary mapping for that scalar product and all the $\alpha_{i,j}$ have absolute value $q^{i/2}$.

THE COHOMOLOGY APPROACH - A THEOREM OF SERRE

Theorem

There does not exist a cohomology theory for schemes over $\mathbb{F}_q$ with the following properties:

- Functorial
- Künneth formula
- $H^1(E) = \mathbb{Q}^2$

Fact

There's no cohomology theory with $\mathbb{Q}$-coefficients for schemes over $\mathbb{F}_q$.

THE COHOMOLOGY APPROACH - AN EXAMPLE OF SERRE

Let E be an elliptic curve.

Classical cohomology

For every coherent sheaf $\mathcal{F}$ on a proper scheme X

$$\chi(X) = \sum_i (-1)^i h^i(X, \mathcal{F})$$

- Since $\chi(E) = 2 - 2g = 0$ we have $H^1(E) = \mathbb{Q}^2$.
- There is a natural action of $\mathrm{End}(E)$ on $H^1(E)$ on the right.
- This action is compatible with products and sums (thanks to functoriality and Künneth formula).
- Thus, we have a representation of $\mathrm{End}(E)$ on $H^1(X)$ and also of $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$.
- But, if E is supersingular, then $\mathrm{End}^0(E)$ is of rank 4 and we cannot have a dimension 2 representation over $\mathbb{Q}$.
- This also excludes $K = \mathbb{Q}_p$ and $\mathbb{R}$ as $\mathrm{End}^0(E) \otimes \mathbb{Q}_p$ is still non-split.

There are essentially two known approaches to construct a Weil cohomology theory

- $K = \mathbb{Q}_\ell$, $\ell \neq p$; *Étale cohomology* developed by Grothendieck.
- $K = \overline{\mathbb{Q}}_p$; *Rigid cohomology*.

Definition

We say that a morphism of schemes $f : X \to Y$ is étale if it is

- Flat, i.e., $f_x^{\#} : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is flat for every x.
- Unramified, i.e., $\mathfrak{m}_{f(x)}\mathcal{O}_{X,x} = \mathfrak{m}_x$ and the extension $K(y) \to K(x)$ is separable.

For example, if L/K is a finite extension, then $\mathrm{Spec}(L) \to \mathrm{Spec}(K)$ is étale.

Also, if L/K is of number fields, $\mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_K)$ is flat and for all $\mathfrak{q} \subseteq \mathcal{O}_L$ above $\mathfrak{p} \subseteq \mathcal{O}_K$ we have $k(\mathfrak{q})/k(\mathfrak{p})$ separable.
Hence, $\mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_K)$ is unramified (and hence étale) at $\mathfrak{q} \subseteq \mathcal{O}_L$ if and only if $\mathfrak{q}(\mathcal{O}_L)_{\mathfrak{q}}$ is generated by $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, which is the usual definition of unramifiedness.

Properties

- Open immersions are étale.
- Compositions of étale morphisms are étale.
- Base change of étale is étale

THE COHOMOLOGY APPROACH - ÉTALE TOPOLOGY

One does not need to have a topological space to build up a sheaf theory (and a cohomology theory for sheaves). Indeed, let **C** be a category with, for each object $\mathcal{U}$ of **C** a distinguished set of families of maps $\{\mathcal{U}_i \to \mathcal{U}\}_{i\in I}$, called the *covering* of $\mathcal{U}$, that satisfy:

- For a covering $\{\mathcal{U}_i \to \mathcal{U}\}_{i\in I}$ of $\mathcal{U}$ and any morphism $\mathcal{V} \to \mathcal{U}$ in **C**, the fiber products $\{\mathcal{U}_i \times_{\mathcal{U}} \mathcal{V} \to \mathcal{V}\}_{i\in I}$ exist and form a covering of $\mathcal{V}$
- If $\{\mathcal{U}_i \to \mathcal{U}\}_{i\in I}$ is a covering of $\mathcal{U}$, and for each $i \in I$, $\{\mathcal{V}_{i,j} \to \mathcal{U}_i\}_{j\in J}$ is a covering of $\mathcal{U}_i$, then $\{\mathcal{V}_{i,j} \to \mathcal{U}\}_{i,j}$ is a covering of $\mathcal{U}$
- For all $\mathcal{U}$ in **C**, the family $\{\mathcal{U} \to \mathcal{U}\}$ is a covering of $\mathcal{U}$.

Such a system of coverings is called a Grothendieck topology on **C** and **C** together with this topology is called a site.

Definition

We define the étale site of X (denoted X_{et}) as a category $\mathbb{E}\mathrm{t}_X$ with objects the étale morphisms $\mathcal{U} \to X$ and arrows the X-morphisms (the obvious commutative diagrams) $\phi : \mathcal{U} \to \mathcal{V}$.

A presheaf for the étale topology on X is a contravariant functor $\mathcal{F} : \mathbb{E}\mathrm{t}_X \to \mathbb{A}\mathrm{b}$ It is a sheaf if

$$\mathcal{F}(\mathcal{U}) \to \prod_{i \in I} \mathcal{F}(\mathcal{U}_i) \rightrightarrows \prod_{i,j} \mathcal{F}(\mathcal{U}_i \times_{\mathcal{U}} \mathcal{U}_j)$$

is exact for all étale coverings $\{\mathcal{U}_i \to \mathcal{U}\}_{i \in I}$

Constant sheaf. This takes any étale open set $(\mathcal{U} \to X)$ to a fixed abelian group A.

Sheaf of regular functions. This takes any étale open set $(\mathcal{U} \to X)$ of X to the space $\mathcal{O}(\mathcal{U})$ of regular functions of $\mathcal{U}$

Sheaf of invertible functions. It is denoted $\mathbb{G}_m$ and it takes any étale open set $(\mathcal{U} \to X)$ of X to $\mathcal{O}^\times(\mathcal{U})$, the units of the regular functions of $\mathcal{U}$.

Sheaf of n-th roots of unity. μ_n takes any étale open set $(\mathcal{U} \to X)$ of X to the n-th roots of unity in $\mathcal{O}(\mathcal{U})$.

The functor

$$\begin{aligned} \mathbb{S}\mathrm{h}(X_{et}) &\longrightarrow \mathbb{A}\mathrm{b} \\ \mathcal{F} &\longrightarrow \Gamma(X, \mathcal{F}) \end{aligned}$$

is left exact and we can define $H^r(X_{et}, -)$ as its r-th right derived functor. One then has the usual properties

- For any sheaf $\mathcal{F}$, $H^0_{et}(X, \mathcal{F}) = H^0(X_{et}, \mathcal{F}) = \Gamma(X, \mathcal{F})$.
- $H^r_{et}(X, \mathcal{I}) = 0$ for $r > 0$ if $\mathcal{I}$ is injective
- Functoriality; a short exact sequence of sheaves

$$0 \longrightarrow \mathcal{F}' \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}'' \longrightarrow 0$$

  gives rise to a long exact sequence in cohomology

$$0 \longrightarrow H^0_{et}(X, \mathcal{F}') \longrightarrow H^0_{et}(X, \mathcal{F}) \longrightarrow H^0_{et}(X, \mathcal{F}'') \longrightarrow H^1_{et}(X, \mathcal{F}') \longrightarrow \dots$$

Étale cohomology of a curve

Let X be a nonsingular projective curve over K. For n invertible in K

$$H^r_{et}(X, \mathbb{Z}/n\mathbb{Z}) = \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{if } r = 0 \\ (\mathbb{Z}/n\mathbb{Z})^{2g} & \text{if } r = 1 \\ \mathbb{Z}/n\mathbb{Z} & \text{if } r = 2 \end{cases}$$

Let X be a non-singular projective curve. We want to calculate $H^r_{et}(X, \mathbb{Z}/\ell^n\mathbb{Z})$
We define

$$H^r_{et}(X, \mathbb{Z}_\ell) = \varprojlim H^r_{et}(X, \mathbb{Z}/\ell^n\mathbb{Z}))$$

$$H^r_{et}(X, \mathbb{Q}_\ell) = H^r_{et}(X, \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell$$

Theorem

We have the Lefschetz formula

$$\#X(\mathbb{F}_q) = \sum_{i=0}^{2d} (-1)^n \operatorname{Trace}\left(F, H^r(X_{et}, \mathbb{Q}_\ell)\right)$$

Theorem

Weil proved that the eigenvalues π_i of F on $H^1(X_{et}, \mathbb{Q}_\ell)$ are algebraic integers with $|\pi_i| = q^{1/2}$.

Thus

$$|\#X(\mathbb{F}_q) - (q+1)| = \left|\operatorname{Trace}\left(F, H^1(X_{et}, \mathbb{Q}_\ell)\right)\right| \leq \sum_{i=1}^{2g} |\pi_i| \leq 2g\sqrt{q}$$

Let K be a field, and A a finitely generated K-algebra.

Definition

We define the module of Kähler differentials as

$$\Omega_{A/K} = \frac{\text{free module on formal symbols } dr \quad (r \in A)}{\langle dr \ (r \in K), d(r+s) - dr - ds, d(rs) - r\ ds - s\ dr \rangle}$$

We set $\Omega^i_{A/K} = \bigwedge^i \Omega_{A/K}$; there is a derivation map

$$\begin{aligned} d : \Omega^i_{A/K} &\longrightarrow \Omega^{i+1}_{A/K} \\ f_0\ df_1 \wedge \ldots \wedge df_i &\longrightarrow df_0 \wedge df_1 \wedge \ldots \wedge df_i \end{aligned}$$

We get the *de Rahm* complex $\Omega^\bullet_{A/K}$ and we define the de Rham cohomology of A as

$$H^i_{dR}(A/K) = H^i(\Omega^\bullet_{A/K})$$

If $X = \mathrm{Spec}(A)$, then $H^i_{dR}(X/K) = H^i_{dR}(A/K)$.

Let $\mathrm{char}(k) = p$. We set R to be the Witt vectors of k. We have $R/pR = k$. We set $K = \mathrm{Frac}(R)$.

Elkik-Arabia Theorem

There is a unique (up to isomorphism) R algebra $\hat{A}$ complete w.r.t. the p-adic topology, flat over R, such that

$$\hat{A} \otimes_R k = A$$

For $A = k[x]$ this is

$$\hat{A} = R\langle x\rangle = \left\{ \sum_{n=0}^{+\infty} a_n x^n \,\middle|\, |a_n|_p \to 0 \right\}$$

Problem

If we try to mimic the de Rahm construction we get infinite dimensional objects

Let $\mathrm{char}(k) = p$. We set R to be the Witt vectors of k. We have $R/pR = k$. We set $K = \mathrm{Frac}(R)$.

Monsky-Washnitzer

We can consider a subring

$$A^\dagger = \left\{ \sum_{n=0}^{+\infty} a_n x^n \;\middle|\; \lim_{n\to\infty} |a_n|\rho^n = 0 \;\text{ some } \rho > 1 \right\}$$

Elements of $\hat{A}$ are functions on the closed unit disc. $A^\dagger$ consists of functions on the closed unit disc which in fact converge on some bigger disc.

Monsky-Washnitzer cohomology

We define

$$H^i_{MW}(A/K) = H^i(\Omega^\bullet_{A^\dagger/K})$$

- Suppose X is an hyperelliptic curve $y^2 = P(x)$ of genus $g = (\deg(P) - 1)/2$
- Its coordinate ring is $A = \frac{K[x,y,z]}{(y^2 - P(X), yz-1)} = \frac{K[x,y,y^{-1}]}{(y^2 - P(X))}$
- Construct A^∞, the $\mathfrak{p}$-adic completion of A.
- Consider the weak completion of A:

$$A^\dagger = \left\{ \sum_{n=-\infty}^{+\infty} \frac{B_n(x)}{y^n} \,\middle|\, B_n \in K[x], \;\deg B_n \leq 2g \right\}$$

  with the further condition that $\nu_p(B_n(x))$ grows faster than some linear function of $|n|$ as $|n| \to \pm\infty$.
- The only non-trivial MW cohomology groups are H^0 and H^1.
- The first cohomology group splits into two eigenspaces under the hyperelliptic involution

$$H^1_{MW}(X/K)^+ \;\text{ with basis }\; \left\{x^i dx/y^2\right\}_{0 \leq i \leq 2g}$$

$$H^1_{MW}(X/K)^- \;\text{ with basis }\; \left\{x^i dx/2y\right\}_{0 \leq i \leq 2g-1}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X}/\mathrm{K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = (F_K(P)(x^p))^{1/2}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X}/\mathrm{K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = \left(F_K(F)(x^p) - P(x)^p + P(x)^p\right)^{1/2}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF^{-1}}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X/K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = P(x)^{p/2}\left(1 + \frac{F_K(P)(x^p) - P(x)^p}{P(x)^p}\right)^{1/2}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X/K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = y^p \left(1 + \frac{F_K(P)(x^p) - P(x)^p}{P(x)^p}\right)^{1/2}$$

L.COLÒ I2M

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X}/\mathrm{K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(F_K(P)(x^p) - P(x)^p)^i}{y^{2ip}}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{q}\mathrm{F}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X}/\mathrm{K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(F_K(P)(x^p) - P(x)^p)^i}{y^{2ip}}$$

- Now we apply it to $\mathrm{H}^1_{\mathrm{MW}}(X')$:

$$F^*\omega_i = \frac{x^{ip} d(x^p)}{2F(y)}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{q}\mathrm{F}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X}/\mathrm{K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(F_K(P)(x^p) - P(x)^p)^i}{y^{2ip}}$$

- Now we apply it to $\mathrm{H}^1_{\mathrm{MW}}(X')$:

$$F^*\omega_i = px^{ip+p-1}\frac{dx}{2F(y)}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X}/\mathrm{K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(F_K(P)(x^p) - P(x)^p)^i}{y^{2ip}}$$

- Now we apply it to $\mathrm{H}^1_{\mathrm{MW}}(X')$:

$$F^*\omega_i = px^{ip+p-1} \frac{y}{F(y)} \frac{dx}{2y}$$

Lefschetz formula

$$\#X(\mathbb{F}_{q^r}) = q^r - \mathrm{Trace}(\mathrm{qF}^{-1}, \mathrm{H}^1_{\mathrm{MW}}(\mathrm{X/K}))$$

- K is an unramified extension of $\mathbb{Q}_p$. Thus, we have a unique automorphism F_K lifting the Frobenius of $\mathbb{F}_q$. Let F denote a p-power Frobenius lift on $A^\dagger$:

$$F(x) = x^p$$

$$F(y) = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(F_K(P)(x^p) - P(x)^p)^i}{y^{2ip}}$$

- Now we apply it to $\mathrm{H}^1_{\mathrm{MW}}(X')$:

$$F^*\omega_i = px^{ip+p-1}y \left(y^{-p} \sum_{k=0}^{+\infty} \binom{-1/2}{i} \frac{(F_K(P)(x^p) - P(x)^p)^i}{y^{2pk}} \right) \frac{dx}{2y}$$

INTERSECTION THEORY - SURFACES

By surface, we refer to a smooth projective variety of dimension 2 over an algebraically closed field k. By a curve on a surface, we mean an effective divisor on the surface. We say that two curves C and D meet transversely if, for every common point P, their local defining equations f and g generate the maximal ideal of the local ring $\mathcal{O}_{P,X}$.

We would like to define a bilinear form

$$\mathrm{Div}(X) \times \mathrm{Div}(X) \to \mathbb{Z} \qquad (C, D) \mapsto C.D$$

that expresses the intersection number of two curves on a surface.

- If C and D meet transversely at d points, then $C.D = d$
- $C.D = D.C$ and $(C_1 + C_2).D = C_1.D + C_2.D$
- The intersection number depends only on linear equivalence classes

$$C.D = \sum_{P \in C \cap D} \mathrm{len}\left(\mathcal{O}_{P,X}/(f, g)\right)$$

Lemma (Adjunction formula)

Let C be nonsingular curve on X of genus g. Then the following holds:

$$g = \frac{C.(C + K_X)}{2} + 1$$

Riemann-Roch

Let X be a surface and D a divisor on X. Let K_X be the canonical class, $\ell(D) = \dim_k H^0(X, \mathcal{O}_X)$ and $s(D) = \dim_k H^1(X, \mathcal{O}_X)$ and the arithmetic genus of X, $\rho_a = \chi(\mathcal{O}_X) - 1$. Then,

$$\ell(D) - s(D) + \ell(K_X - D) = \frac{1}{2}\left(D.(D - K_X)\right) + \chi(\mathcal{O}_X)$$

Let H be a very ample divisor on a surface X. Then for a curve C on X, the degree of C under the embedding given by H into $\mathbb{P}^n$ coincides with $C.H$.

Lemma

Let H be an ample divisor on X, and let D be a divisor such that $D.H > 0$ and $D^2 > 0$. Then for all $n \gg 0$, nD is linearly equivalent to an effective divisor.

Hodge Index Theorem

Let H be an ample divisor on the surface X and let D be a non zero divisor with $D.H = 0$. Then $D^2 < 0$.

Nakai-Moishezon criterion

A divisor D on a surface X is ample if and only if $D^2 > 0$ and $D.C > 0$ for all irreducible curves C in X.

The idea is to use the intersection theory on the surface $\overline{X} \times_{\overline{\mathbb{F}}_q} \overline{X}$.

- For every morphism of curves $f : X \to Y$, we have a prime correspondence

$$\Gamma_f := (Id_X \times f)(X) \subset X \times Y$$

  called the graph of f.
- We let Δ be the graph of the identity morphism $Id_X : X \to X$, also called the diagonal correspondence
- We let $\Gamma = \Gamma_F$ be the graph of Frobenius given by the image of the closed immersion

$$\overline{X} \to \overline{X} \times \overline{X} \qquad x \mapsto (x, F(x))$$

  Notice that this is a prime correspondence, and therefore a curve of genus $g = g(X)$.
- Since Γ and Δ intersect transversely at all points where they intersect

$$N(X) = \#\mathrm{Fix}(F, \overline{X}) = \Gamma.\Delta$$

INTERSECTION THEORY - PROVING THE WEIL BOUND

- We have $\Delta^2 = 2 - 2g$ as Δ^2 is the degree of the normal bundle to the diagonal embedding $\overline{X} \to \overline{X} \times \overline{X}$; this is the tangent bundle to $\overline{X}$, which has degree $2 - 2g$.
- To compute Γ^2 we note that Γ^2

$$2g - 2 = \Gamma^2 + \Gamma.K_{\overline{X}\times\overline{X}}$$

We can express $K_{\overline{X}\times\overline{X}}$ as the sum of the pullbacks $\pi_1 * K_{\overline{X}} + \pi_2^* K_{\overline{X}}$. Now Γ intersects $\overline{X} \times \{*\}$ and $\{*\} \times \overline{X}$ with multiplicity 1 and q. Since $\deg K_{\overline{X}} = 2g - 2$, this gives $\Gamma^2 = 2g - 2 - (q+1)(2g-2) = q(2-2g)$.

Proposition

Let D be any divisor on $\overline{X} \times \overline{X}$ with $a = D.(\overline{X} \times \{*\})$ and $b = D.(\{*\} \times \overline{X})$. Then

$$|D.\Delta - (a+b)| \leq \sqrt{2g(2ab - D^2)}$$

- The Weil bound follows by taking $D = \Gamma$ for which $a = 1$ and $b = q$.

WEIL BOUND - A FIRST REFINEMENT

L.COLÒ 1 2 M

Theorem

We have

$$|N-(q+1)| \leq g\left[2q^{1/2}\right]$$

We have seen

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

Proposition

One can order the π_i in such a way that $\pi_{g+1}, \ldots, \pi_{2g}$ are equal to $\overline{\pi}_1, \ldots, \overline{\pi}_g$ respectively.

- It suffices to show that if $q = q_0^2$ then q_0 and $-q_0$ both occur with even multiplicity.
- all the other cases follow by the stability under $\mathcal{G}a\ell(\overline{\mathbb{Q}}/\mathbb{Q})$).

PROOF OF THE REFINED WEIL BOUND

- $N(X) - (q+1) = -\sum_{i=1}^{2g} \pi_i = -\sum_{i=1}^{g} x_i$ where $x_i = \pi_i + \overline{\pi}_i$
- Let $m = \lfloor 2q^{1/2} \rfloor$, then $|x_i| < m+1$ for every i.
- Let $y_i = m + 1 + x_i$, then $y_i > 0$.
- The y_i's are stable under Galois conjugation and thus they are algebraic integers. Hence their product is a natural number.
- The arithmetic-geometric mean inequality gives

$$\frac{y_1 + \ldots + y_g}{g} \geq (y_1 \cdots y_g)^{1/g} \geq 1$$

Thus

$$\frac{y_1 + \ldots + y_g}{g} = m + 1 + \frac{1}{g} \sum_{i=1}^{g} x_i \geq 1$$

- This gives the inequality $\mathrm{Trace}(F) \geq -gm$. For the other inequality, one applies the same proof to the opposite of the Frobenius.

REFINED WEIL BOUND - AN EXAMPLE

```
sage: p = 101
....: prec = 10
....: R.<x> = QQ['x']
....: A,forms=monsky_washnitzer.matrix_of_frobenius_hyperelliptic(x^5 + 2*x^2 + x+1,p,prec);
[sage: EQ=HyperellipticCurve(x^5+2*x^2+x+1)
....: K=Qp(p,prec)
....: E=EQ.change_ring(K)
....: M=A.change_ring(ZZ); M
[ 5649321321572464 7323  9122165197272078 9035 10946751237347895 6972  3109667909971050 1963]
```

```
sage: p = 101
....: prec = 10
....: R.<x> = QQ['x']
....: A,forms=monsky_washnitzer.matrix_of_frobenius_hyperelliptic(x^5 + 2*x^2 + x+1,p,prec);
[sage: EQ=HyperellipticCurve(x^5+2*x^2+x+1)
....: K=Qp(p,prec)
....: E=EQ.change_ring(K)
....: M=A.change_ring(ZZ); M
[ 56493213215724647323  91221651972720789035 109467512373478956972  31096679099710501963]
```

```
sage: p = 101
....: prec = 10
....: R.<x> = QQ['x']
....: A,forms=monsky_washnitzer.matrix_of_frobenius_hyperelliptic(x^5 + 2*x^2 + x+1,p,prec);
[sage: EQ=HyperellipticCurve(x^5+2*x^2+x+1)
....: K=Qp(p,prec)
....: E=EQ.change_ring(K)
....: M=A.change_ring(ZZ); M
[ 56493213215724647323  91221651972720789035 10946751237347895697 2  31096679099710501963]
```

```
sage: p = 101
....: prec = 10
....: R.<x> = QQ['x']
....: A,forms=monsky_washnitzer.matrix_of_frobenius_hyperelliptic(x^5 + 2*x^2 + x+1,p,prec);
[sage: EQ=HyperellipticCurve(x^5+2*x^2+x+1)
....: K=Qp(p,prec)
....: E=EQ.change_ring(K)
....: M=A.change_ring(ZZ); M
[ 56493213215724647323  91221651972720789035 109467512373478956972  31096679099710501963]
[ 30588000606515507587  85600942703587230697  68841142676393372694  13975965182916593107]
[ 69060715659998179697 103331531349894232384  27136296461538705801  78187521694516401570]
[ 12771691150105329442  47970135072000782451  95042490856601645827  51693972701390318174]
[sage: P=A.charpoly();P;
[sage: P
(1 + O(101^10))*x^4 + (7 + O(101^10))*x^3 + (66 + 101 + O(101^10))*x^2 + (7*101 + O(101^10))*x + 101^2 + O(101^10)
[sage: R=P.roots();
[sage: R
[(20 + 93*101 + 67*101^2 + 57*101^3 + 101^4 + 63*101^5 + 10*101^6 + 13*101^7 + 45*101^8 + 99*101^9 + O(101^10),
  1),
 (74 + 27*101 + 18*101^2 + 64*101^3 + 5*101^5 + 64*101^6 + 65*101^7 + 3*101^8 + 57*101^9 + O(101^10),
  1),
 (96*101 + 93*101^2 + 89*101^3 + 43*101^4 + 65*101^5 + 30*101^6 + 28*101^7 + 83*101^8 + 24*101^9 + O(101^10),
  1),
 (86*101 + 21*101^2 + 91*101^3 + 54*101^4 + 68*101^5 + 96*101^6 + 94*101^7 + 69*101^8 + 20*101^9 + O(101^10),
  1)]
[sage: -(R[0][0]+R[1][0]+R[2][0]+R[3][0])
7 + O(101^10)
[sage: R[0][0]*R[2][0]
101 + 47*101^9 + O(101^10)
[sage: R[1][0]*R[3][0]
101 + 18*101^9 + O(101^10)
sage: K = GF(101)
....: PR.<t> = PolynomialRing(K)
....: EH = HyperellipticCurve(t^5 + 2*t^2 + t + 1)
....: EH.cardinality()
109
sage:
```

More on the refined Weil bound

Theorem

If $\mathrm{Trace}(F) = \pm gm$, then the x_i's are equal to $\pm m$.

Corollary

If $N = 1 + q + 2m$, then the eigenvalues of the Frobenius are equal to $(-m \pm \sqrt{m^2 - 4q})/2$ (g times each).

Trace of algebraic integers - a theorem of Smyth

Let A be a g-dimensional abelian variety over $\mathbb{F}_q$.

- If $\mathrm{Trace}(F) = \pm gm$ (defect 0 case) then $(x_1, \ldots, x_g) = \pm(m, \ldots, m)$.
- If $\mathrm{Trace}(F) = \pm(gm - 1)$ (defect 1 case) there are two possibilities for $(x_1, \ldots, x_g)$. Namely,

$$\pm(\underbrace{m, m, \ldots, m}_{g-1}, m-1) \quad \text{and} \quad \pm\left(\underbrace{m, m, \ldots, m}_{g-2}, m + \frac{-1 \pm \sqrt{5}}{2}\right)$$

- If $\mathrm{Trace}(F) = \pm(gm - 2)$ (defect 2) there are 7 possibilities for $(x_1, \ldots, x_g)$.

$$\begin{cases} \pm(m, m, \ldots, m, m-2) & (g \geq 1) \\ \pm(m, \ldots, m, m-1, m-1) & (g \geq 2) \\ \pm\left(m, \ldots, m, m+\sqrt{2}-1, m-\sqrt{2}-1\right) & (g \geq 2) \\ \pm\left(m, \ldots, m, m+\sqrt{3}-1, m-\sqrt{3}-1\right) & (g \geq 2) \\ \pm\left(m, \ldots, m, m-1, m+(-1\pm\sqrt{5})/2\right) & (g \geq 3) \\ \pm\left(m, \ldots, m, m+(-1\pm\sqrt{5})/2, m+(-1\pm\sqrt{5})/2\right) & (g \geq 4) \\ \pm\left(m, \ldots, m, m+1-4\cos^2(a\pi/7)\right), \quad a = 1, 2, 3 & (g \geq 3) \end{cases}$$

Theorem

Let α be a totally positive algebraic integer of degree $\deg(\alpha)$. If α is neither 1 nor $(3 \pm \sqrt{5})/2$ then

$$\mathrm{Trace}(\alpha) > \frac{3}{2}\deg(\alpha)$$

- If $\alpha = 1$, then $\mathrm{Trace}(\alpha)/\deg(\alpha) = 1$.
- If $\alpha = (3 \pm \sqrt{5})/2$, then $\mathrm{Trace}(\alpha)/\deg(\alpha) = 3/2$.
- If $\alpha \neq 1, (3 \pm \sqrt{5})/2$ then Smyth proved $\mathrm{Trace}(\alpha)/\deg(\alpha) \geq 5/3$.

Corollary

Let $k(\alpha) = \mathrm{Trace}(\alpha) - \deg(\alpha)$. Then:

- If $k(\alpha) = 0$, then $\alpha = 1$.
- If $k(\alpha) = 1$, then $\alpha = 2$ or $\alpha = (3 \pm \sqrt{5})/2$.
- If $k(\alpha) = 2$, then $\alpha = 3$ or $\alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$ or α is one of the conjugates of $4\cos^2(\pi/7)$

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.

TRACE OF ALGEBRAIC INTEGERS - PROOF OF THE COROLLARY

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$
  - $\deg(\alpha) = 2$ gives $\mathrm{Trace}(\alpha) = 4$ and α is root of $x^2 - 4x + n$ with all conjugates (roots) positive. Then $n = 1, 2, 3$ and $\alpha = 3, \alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$
  - $\deg(\alpha) = 2$ gives $\mathrm{Trace}(\alpha) = 4$ and α is root of $x^2 - 4x + n$ with all conjugates (roots) positive. Then $n = 1, 2, 3$ and $\alpha = 3, \alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$
  - $\deg(\alpha) = 3$ gives the roots of a cubic polynomial $P(x) = x^3 - 5x^2 + px + q$ with positive roots.

TRACE OF ALGEBRAIC INTEGERS - PROOF OF THE COROLLARY

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$
  - $\deg(\alpha) = 2$ gives $\mathrm{Trace}(\alpha) = 4$ and α is root of $x^2 - 4x + n$ with all conjugates (roots) positive. Then $n = 1, 2, 3$ and $\alpha = 3, \alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$
  - $\deg(\alpha) = 3$ gives the roots of a cubic polynomial $P(x) = x^3 - 5x^2 + px + q$ with positive roots.

    $1 \leq p \leq 8$ since the derivative must have 2 positive roots;

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$
  - $\deg(\alpha) = 2$ gives $\mathrm{Trace}(\alpha) = 4$ and α is root of $x^2 - 4x + n$ with all conjugates (roots) positive. Then $n = 1, 2, 3$ and $\alpha = 3, \alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$
  - $\deg(\alpha) = 3$ gives the roots of a cubic polynomial $P(x) = x^3 - 5x^2 + px + q$ with positive roots.

    $1 \leq p \leq 8$ since the derivative must have 2 positive roots;

    $1 \leq q \leq 4$ by the arithmetic-geometric mean inequality;

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$
  - $\deg(\alpha) = 2$ gives $\mathrm{Trace}(\alpha) = 4$ and α is root of $x^2 - 4x + n$ with all conjugates (roots) positive. Then $n = 1, 2, 3$ and $\alpha = 3, \alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$
  - $\deg(\alpha) = 3$ gives the roots of a cubic polynomial $P(x) = x^3 - 5x^2 + px + q$ with positive roots.

    $1 \leq p \leq 8$ since the derivative must have 2 positive roots;

    $1 \leq q \leq 4$ by the arithmetic-geometric mean inequality;

    $p \geq 3q^{2/3} \geq 3$ by the arithmetic-geometric mean inequality;

Suppose α is not in the list. Then by Siegel's theorem $k(\alpha)/\deg(\alpha) > 1/2$, i.e., $\deg(\alpha) < 2k(\alpha)$

- If $k(\alpha) < 2$, then $\deg(\alpha) = 1$ and $\alpha = 1, 2$.
- If $k(\alpha) = 2$, then $\deg(\alpha) < 4$
  - $\deg(\alpha) = 1$ gives $\alpha = 3$
  - $\deg(\alpha) = 2$ gives $\mathrm{Trace}(\alpha) = 4$ and α is root of $x^2 - 4x + n$ with all conjugates (roots) positive. Then $n = 1, 2, 3$ and $\alpha = 3, \alpha = 2 \pm \sqrt{2}$ or $2 \pm \sqrt{3}$
  - $\deg(\alpha) = 3$ gives the roots of a cubic polynomial $P(x) = x^3 - 5x^2 + px + q$ with positive roots.
    $1 \leq p \leq 8$ since the derivative must have 2 positive roots;
    $1 \leq q \leq 4$ by the arithmetic-geometric mean inequality;
    $p \geq 3q^{2/3} \geq 3$ by the arithmetic-geometric mean inequality;
    Since we need real roots (positive discriminant) we remain with 4 possibilities
    $(p, q) \in \{\underbrace{(6, 2), (5, 1), (7, 2)}_{\text{reducible polynomials}}, (6, 1)\}$

- Let $P(X) = X^g - a_1 X^{g-1} + \dots$ be the polynomial $\prod_i (X - m - 1 + x_i)$.

- Let $P(X) = X^g - a_1 X^{g-1} + \dots$ be the polynomial $\prod_i (X - m - 1 + x_i)$.
- Its coefficients are in $\mathbb{Z}$, its roots are real and positive, and its coefficient a_1 is equal to $gm + g - \mathrm{Trace}(F)$.

- Let $P(X) = X^g - a_1 X^{g-1} + \dots$ be the polynomial $\prod_i (X - m - 1 + x_i)$.
- Its coefficients are in $\mathbb{Z}$, its roots are real and positive, and its coefficient a_1 is equal to $gm + g - \mathrm{Trace}(F)$.
- The defect of P is $k(P) = a_1 - g = gm - \mathrm{Trace}(F)$ and we assumed it $= 0, 1, 2$.

- Let $P(X) = X^g - a_1 X^{g-1} + \ldots$ be the polynomial $\prod_i (X - m - 1 + x_i)$.
- Its coefficients are in $\mathbb{Z}$, its roots are real and positive, and its coefficient a_1 is equal to $gm + g - \mathrm{Trace}(F)$.
- The defect of P is $k(P) = a_1 - g = gm - \mathrm{Trace}(F)$ and we assumed it $= 0, 1, 2$.
- We write P as the product of irreducible polynomials Q_λ. The sum of the defects of the Q_λ is $0, 1$ or 2. Thus their roots (and therefore those of P) belong to the set described before

$$\{1, 2, 3, (3 \pm \sqrt{5})/2, 2 \pm \sqrt{2}, 2 \pm \sqrt{3}, 4\cos^2(a\pi/7)\ a = 1, 2, 3\}$$

For a real t, we denote by $\{t\} = t - [t]$ the fractional part of t. We have $2q^{1/2} = m + \{2q^{1/2}\}$.

Proposition

The second defect 1 case

$$\pm\left(\underbrace{m, m, \ldots, m}_{g-2}, m + \frac{-1 \pm \sqrt{5}}{2}\right)$$

can only occur if $\{2q^{1/2}\} > (\sqrt{5} - 1)/2 = 0.6180$

Proposition

The third, fourth, fifth, sixth and seventh defect 2 cases can only occur if $\{2q^{1/2}\}$ is greater than

$$0.4142\ldots \qquad 0,7320\ldots \qquad 0.6180\ldots \qquad 0.6180\ldots \qquad 0.8019\ldots$$

respectively.

Let $\{P_\lambda\}_{\lambda\in\Lambda}$ be a finite family of monic polynomials with all roots real and positive, and coefficients in $\mathbb{Z}$.

Let $(c_\lambda)_{\lambda\in\Lambda}$ be positive real numbers. For $x > 0$ such that $P_\lambda(x) \neq 0$ for every λ, let $g(x) = x - \sum_\lambda c_\lambda \log|P_\lambda(x)|$ and let $\min(g) = \min_{x\geq 0} g(x)$

Theorem

Let α be a totally positive algebraic integer of degree d which is not a root of any P_λ. Then

$$\mathrm{Trace}(\alpha)/\deg(\alpha) \geq \min(g)$$

- Let $d = \deg(\alpha)$ and $\alpha_1, \ldots, \alpha_d$ its conjugates.

Trace of algebraic integers - Proof of Siegel theorem

Let $\{P_\lambda\}_{\lambda\in\Lambda}$ be a finite family of monic polynomials with all roots real and positive, and coefficients in $\mathbb{Z}$.

Let $(c_\lambda)_{\lambda\in\Lambda}$ be positive real numbers. For $x > 0$ such that $P_\lambda(x) \neq 0$ for every λ, let $g(x) = x - \sum_\lambda c_\lambda \log|P_\lambda(x)|$ and let $\min(g) = \min_{x\geq 0} g(x)$

Theorem

Let α be a totally positive algebraic integer of degree d which is not a root of any P_λ. Then

$$\mathrm{Trace}(\alpha)/\deg(\alpha) \geq \min(g)$$

- Let $d = \deg(\alpha)$ and $\alpha_1, \dots, \alpha_d$ its conjugates.
- $\alpha_i > 0$ for all i. Up to sign, the resultant of P_λ and the minimal polynomial of α is $P_\lambda(\alpha_1)\cdot P_\lambda(\alpha_2)\cdots P_\lambda(\alpha_d)$, hence lies in $\mathbb{Z}\setminus\{0\}$. Thus

$$|P_\lambda(\alpha_1)\cdot P_\lambda(\alpha_2)\cdots P_\lambda(\alpha_d)| \geq 1 \implies \sum_{i=1}^{d} \log(|P_\lambda|) \geq 0$$

TRACE OF ALGEBRAIC INTEGERS - PROOF OF SIEGEL THEOREM

Let $\{P_\lambda\}_{\lambda\in\Lambda}$ be a finite family of monic polynomials with all roots real and positive, and coefficients in $\mathbb{Z}$.

Let $(c_\lambda)_{\lambda\in\Lambda}$ be positive real numbers. For $x > 0$ such that $P_\lambda(x) \neq 0$ for every λ, let $g(x) = x - \sum_\lambda c_\lambda \log|P_\lambda(x)|$ and let $\min(g) = \min_{x\geq 0} g(x)$

Theorem

Let α be a totally positive algebraic integer of degree d which is not a root of any P_λ. Then

$$\mathrm{Trace}(\alpha)/\deg(\alpha) \geq \min(g)$$

- Let $d = \deg(\alpha)$ and $\alpha_1, \ldots, \alpha_d$ its conjugates.
- $\alpha_i > 0$ for all i. Up to sign, the resultant of P_λ and the minimal polynomial of α is $P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \cdots P_\lambda(\alpha_d)$, hence lies in $\mathbb{Z} \setminus \{0\}$. Thus

$$|P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \cdots P_\lambda(\alpha_d)| \geq 1 \implies \sum_{i=1}^{d} \log(|P_\lambda|) \geq 0$$

- We get

$$\frac{\mathrm{Trace}(\alpha)}{\deg(\alpha)} = \frac{1}{d}\sum_{i=1}^{d} \alpha_i$$

TRACE OF ALGEBRAIC INTEGERS - PROOF OF SIEGEL THEOREM

Let $\{P_\lambda\}_{\lambda\in\Lambda}$ be a finite family of monic polynomials with all roots real and positive, and coefficients in $\mathbb{Z}$.

Let $(c_\lambda)_{\lambda\in\Lambda}$ be positive real numbers. For $x > 0$ such that $P_\lambda(x) \neq 0$ for every λ, let $g(x) = x - \sum_\lambda c_\lambda \log|P_\lambda(x)|$ and let $\min(g) = \min_{x\geq 0} g(x)$

Theorem

Let α be a totally positive algebraic integer of degree d which is not a root of any P_λ. Then

$$\mathrm{Trace}(\alpha)/\deg(\alpha) \geq \min(g)$$

- Let $d = \deg(\alpha)$ and $\alpha_1, \ldots, \alpha_d$ its conjugates.
- $\alpha_i > 0$ for all i. Up to sign, the resultant of P_λ and the minimal polynomial of α is $P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \cdots P_\lambda(\alpha_d)$, hence lies in $\mathbb{Z} \setminus \{0\}$. Thus

$$|P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \cdots P_\lambda(\alpha_d)| \geq 1 \implies \sum_{i=1}^{d} \log(|P_\lambda|) \geq 0$$

- We get

$$\frac{\mathrm{Trace}(\alpha)}{\deg(\alpha)} = \frac{1}{d}\sum_{i=1}^{d} g(\alpha_i) + \frac{1}{d}\sum_{\lambda\in\Lambda}\sum_{i=1}^{d} c_\lambda \log(|P_\lambda|)$$

TRACE OF ALGEBRAIC INTEGERS - PROOF OF SIEGEL THEOREM

Let $\{P_\lambda\}_{\lambda\in\Lambda}$ be a finite family of monic polynomials with all roots real and positive, and coefficients in $\mathbb{Z}$.
Let $(c_\lambda)_{\lambda\in\Lambda}$ be positive real numbers. For $x > 0$ such that $P_\lambda(x) \neq 0$ for every λ, let $g(x) = x - \sum_\lambda c_\lambda \log|P_\lambda(x)|$ and let $\min(g) = \min_{x\geq 0} g(x)$

Theorem

Let α be a totally positive algebraic integer of degree d which is not a root of any P_λ. Then

$$\mathrm{Trace}(\alpha)/\deg(\alpha) \geq \min(g)$$

- Let $d = \deg(\alpha)$ and $\alpha_1, \ldots, \alpha_d$ its conjugates.
- $\alpha_i > 0$ for all i. Up to sign, the resultant of P_λ and the minimal polynomial of α is $P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \cdots P_\lambda(\alpha_d)$, hence lies in $\mathbb{Z} \setminus \{0\}$. Thus

$$|P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \cdots P_\lambda(\alpha_d)| \geq 1 \implies \sum_{i=1}^{d} \log\left(|P_\lambda|\right) \geq 0$$

- We get

$$\frac{\mathrm{Trace}(\alpha)}{\deg(\alpha)} \geq \frac{1}{d}\sum_{i=1}^{d} g(\alpha_i)$$

TRACE OF ALGEBRAIC INTEGERS - PROOF OF SIEGEL THEOREM

Let $\{P_\lambda\}_{\lambda\in\Lambda}$ be a finite family of monic polynomials with all roots real and positive, and coefficients in $\mathbb{Z}$.

Let $(c_\lambda)_{\lambda\in\Lambda}$ be positive real numbers. For $x > 0$ such that $P_\lambda(x) \neq 0$ for every λ, let $g(x) = x - \sum_\lambda c_\lambda \log|P_\lambda(x)|$ and let $\min(g) = \min_{x\geq 0} g(x)$

Theorem

Let α be a totally positive algebraic integer of degree d which is not a root of any P_λ. Then

$$\mathrm{Trace}(\alpha)/\deg(\alpha) \geq \min(g)$$

- Let $d = \deg(\alpha)$ and $\alpha_1, \ldots, \alpha_d$ its conjugates.
- $\alpha_i > 0$ for all i. Up to sign, the resultant of P_λ and the minimal polynomial of α is $P_\lambda(\alpha_1)\cdot P_\lambda(\alpha_2)\cdots P_\lambda(\alpha_d)$, hence lies in $\mathbb{Z}\setminus\{0\}$. Thus

$$|P_\lambda(\alpha_1)\cdot P_\lambda(\alpha_2)\cdots P_\lambda(\alpha_d)| \geq 1 \implies \sum_{i=1}^{d} \log\left(|P_\lambda|\right) \geq 0$$

- We get

$$\frac{\mathrm{Trace}(\alpha)}{\deg(\alpha)} \geq \min(g)$$

TRACE OF ALGEBRAIC INTEGERS - SIEGEL BOUND

To obtain Siegel's bound, we need to exclude $x = 1$ and $x = (3 \pm \sqrt{5})/2$ which are roots of $x^2 - 3x + 1$. We take

$$g(x) = x - a\log|x| - b\log|x1| - clog|x^2 - 3x + 1|$$

with $a, b, c > 0$.
If we choose $a = 0.574$, $b = 0.879$ and $c = 0.374$ we find

$$\min(g) > 1.59$$

Hence

$$\frac{\mathrm{Trace}(\alpha)}{\deg(\alpha)} > 1.59$$

QUESTIONS?

References

- Hartshorne, R. *Algebraic Geometry*, Springer, 1977
- Freitag, E. and Kiehl, R. *Etale cohomology and the Weil conjecture*, Springer, 1988
- Kedlaya, K., *Course Math 206A - Topics in Algebraic Geometry: Weil cohomology in practice* `https://kskedlaya.org/papers/weil_cohomology_in_practice.pdf`
- Kedlaya, K., *Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology* `https://arxiv.org/abs/math/0105031`
- Venkatesh, S., *Étale cohomology of curves* `https://math.mit.edu/~sidnv/Cohomology_of_Curves.pdf`
- Borcheerds, R.E., *Weil conjectures playlist on YouTube* `https://www.youtube.com/watch?v=2n8xpH5enDg`