Cup products and Frobenius operators

Frauke Bleher

joint with Ted Chinburg

BIRS workshop “Multivariable Spectral Theory and Representation Theory”

April 1, 2019

Notation and Frobenius operator.

- $k = \mathbb{F}_q$ finite field with q elements, $\mathrm{char}(k) = p$, $q = p^f$.
- $\overline{k} =$ fixed algebraic closure of k.
- $C =$ smooth projective geometrically irreducible curve over k.
- $\overline{C} = C \otimes_k \overline{k}$ (base change).

Frobenius operator $\Phi = \Phi_k$: $(q = \#k)$
induced by the qth power map on $\overline{k}$.

Φ acts on $\overline{C} = C \otimes_k \overline{k}$ as $\Phi_{C/k} \otimes 1$ (geometric Frobenius)
where $\Phi_{C/k}$ is the k-morphism $C \to C$ that is the identity map on the underlying topological space and is the qth power map on $\mathcal{O}_C$.

$\rightsquigarrow$ Φ acts on $\overline{C}(\overline{k})$ by raising the coordinates of any point to the qth power.

Spectrum of Φ determines zeta function of C.

$$Z(C,t) := \exp\left(\sum_{m=1}^{\infty} (\#C(\mathbb{F}_{q^m}))\,\frac{t^m}{m}\right)$$

where $\#C(\mathbb{F}_{q^m}) = \#(\text{points of } C \text{ with coordinates in } \mathbb{F}_{q^m})$.

Note: $Z(C,t)$ determines $\#C(\mathbb{F}_{q^m})$ for $m \geq 1$:

$$\#C(\mathbb{F}_{q^m}) = \frac{1}{(m-1)!}\,\frac{d^m}{dt^m}\log Z(C,t)\Big|_{t=0}.$$

Example: $C = \mathbb{P}^1$ over $k = \mathbb{F}_q$.

$\rightsquigarrow \#C(\mathbb{F}_{q^m}) = 1 + q^m$.

$\rightsquigarrow \log Z(C,t) = \sum_{m=1}^{\infty}(1+q^m)\frac{t^m}{m} = -\log(1-t) - \log(1-qt)$.

$\rightsquigarrow Z(\mathbb{P}^1,t) = \dfrac{1}{(1-t)(1-qt)}$.

Connection to spectrum of Φ: $\ell =$ odd prime, $\ell \nmid q$.

By the Grothendieck-Lefschetz trace formula, we have

$$\#C(\mathbb{F}_{q^m}) = \sum_{r=0}^{2} (-1)^r \operatorname{Tr}\left(\Phi^m \mid \mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)\right).$$

We obtain:

$$\begin{aligned} \log Z(C,t) &= \sum_{m=1}^{\infty} (\#C(\mathbb{F}_{q^m})) \frac{t^m}{m} \\ &= \sum_{r=0}^{2} (-1)^r \sum_{m=1}^{\infty} \operatorname{Tr}\left(\Phi^m \mid \mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)\right) \frac{t^m}{m} \\ &= \sum_{r=0}^{2} (-1)^{r+1} \log\left(\det\left(1 - \Phi t \mid \mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)\right)\right). \end{aligned}$$

Therefore, $\quad Z(C,t) = \prod_{r=0}^{2} \det\left(1 - \Phi t \mid \mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)\right)^{(-1)^{r+1}}.$

$$Z(C,t) = \prod_{r=0}^{2} \det\left(1 - \Phi t \mid \mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)\right)^{(-1)^{r+1}}$$

$$= \frac{P_1(C,t)}{P_0(C,t)\, P_2(C,t)} \quad \text{where } P_r(C,t) = \det\left(1 - \Phi t \mid \mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)\right).$$

ℓ-adic cohomology:

$$\mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell) \stackrel{\text{def}}{=} \mathrm{H}^r(\overline{C}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \stackrel{\text{def}}{=} \varprojlim_n \underbrace{\mathrm{H}^r(\overline{C}, \mathbb{Z}/\ell^n\mathbb{Z})}_{\text{étale cohomology}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Note:

- $\mathrm{H}^0(\overline{C}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ and Φ acts as identity $\rightsquigarrow P_0(C,t) = 1 - t$.
- $\mathrm{H}^2(\overline{C}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ and Φ acts as multiplication by $\deg(\Phi) = q$ $\rightsquigarrow P_2(C,t) = 1 - qt$.
- $\mathrm{H}^1(\overline{C}, \mathbb{Q}_\ell) = (\mathbb{Q}_\ell)^{2g}$, where $g = \mathrm{genus}(C)$, on which Φ acts $\rightsquigarrow P_1(C,t) = \prod_{i=1}^{2g}(1 - \omega_i t)$ where $\{\omega_i\}_{i=1}^{2g}$ are the eigenvalues of Φ acting on $\mathrm{H}^1(\overline{C}, \mathbb{Q}_\ell)$.

Introducing more operators.

Let G be a finite group of k-automorphisms of C.

$\rightsquigarrow$ G acts on $\overline{C}$, and the actions of $\sigma \in G$ and Φ on $\overline{C}$ commute!

One can show:

$$Z(C,t) = Z(C/G,t) \cdot \prod_{\rho} L(C,\rho,t)^{\dim_{D_\rho} V_\rho}$$

where

- ρ ranges over all non-trivial irreducible representations of G over $\mathbb{Q}_\ell$, with underlying $\mathbb{Q}_\ell$-vector space V_ρ,
- $D_\rho = \mathrm{End}_{\mathbb{Q}_\ell G}(V_\rho)$, and
- $L(C,\rho,t) = \det\left(1 - \Phi t \mid \mathrm{H}^1(\overline{C},\mathbb{Q}_\ell)^\rho\right)$ where

$$\begin{aligned} \mathrm{H}^1(\overline{C},\mathbb{Q}_\ell)^\rho &= \left(\mathrm{H}^1(\overline{C},\mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} {V_\rho}^*\right)^G \\ &= \mathrm{Hom}_{\mathbb{Q}_\ell G}(V_\rho, \mathrm{H}^1(\overline{C},\mathbb{Q}_\ell)). \end{aligned}$$

More on ℓ-adic and étale cohomology: $k = \mathbb{F}_q$.

Let ℓ be an odd prime number with $\ell \not| \, q$. Recall:

$$\underbrace{\mathrm{H}^r(\overline{C}, \mathbb{Q}_\ell)}_{\ell\text{-adic cohom.}} = \mathrm{H}^r(\overline{C}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \varprojlim_n \underbrace{\mathrm{H}^r(\overline{C}, \mathbb{Z}/\ell^n\mathbb{Z})}_{\text{étale cohom.}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Let $X \in \{\overline{C}, C\}$, and let $\overline{x}$ be a geometric point on X, corresp. to an algebraic closure $\overline{k(X)}$ of the function field $k(X)$. Let $k(X)^{\mathrm{sep}}$ be the separable closure of $k(X)$ inside $\overline{k(X)}$.

The étale fundamental group $\pi_1(X, \overline{x})$ is the quotient group of $\mathrm{Gal}(k(X)^{\mathrm{sep}}/k(X))$ modulo the subgroup generated by all inertia groups associated to closed points of X. In other words, $\pi_1(X, \overline{x})$ is the profinite group that is the inverse limit of the Galois groups of all finite Galois covers of X that are flat and unramified (i.e. étale).

For all $r \geq 0$, we have

$$\underbrace{\mathrm{H}^r(X, \mathbb{Z}/\ell^n\mathbb{Z})}_{\text{étale cohomology}} \cong \underbrace{\mathrm{H}^r(\pi_1(X, \overline{x}), \mathbb{Z}/\ell^n\mathbb{Z})}_{\text{profinite group cohomology}} .$$

Elliptic curves.

From now on, I will make the following assumptions:

- C is an elliptic curve over $k = \mathbb{F}_q$.
- $\overline{C} = C \otimes_k \overline{k}$ (base change to fixed algebraic closure $\overline{k}$).
- $\ell =$ odd prime number, $q \equiv 1 \mod \ell \rightsquigarrow \mu_\ell \subseteq k^*$.

ℓ-adic Tate module $T_\ell(C)$:

$$\begin{aligned} T_\ell(C) &= \varprojlim_n \overline{C}[\ell^n](\overline{k}) \qquad (\overline{C}[\ell^n](\overline{k}) = \ell^n \text{ torsion points of } \overline{C} \text{ over } \overline{k}) \\ &= \varprojlim_n ((\mathbb{Z}/\ell^n\mathbb{Z}) \oplus (\mathbb{Z}/\ell^n\mathbb{Z})) = \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell. \end{aligned}$$

Note: $\mathrm{H}^1(\overline{C}, \mathbb{Z}_\ell) = \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(C), \mathbb{Z}_\ell) = \mathbb{Z}_\ell$-dual of $T_\ell(C)$.

Φ induces an automorphism of $T_\ell(C)$ given by raising the coordinates of each point to the qth power (geometric Frobenius).

Frobenius derivative.

Assumption: $C[\ell](k) = C[\ell^2](k) \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$.

Proposition: (B-Chinburg)

There exists an automorphism A of $T_\ell(C)$ such that $\Phi = 1 + \ell A$.

Corollary:

We can define a derivative of Φ on $C[\ell](k)$ by

$$d\Phi(\lambda) = (\Phi - 1)\left(\frac{1}{\ell}\lambda\right) = A\lambda$$

for $\lambda \in C[\ell](k)$, where $\frac{1}{\ell}\lambda$ is any ℓth root of λ in $C[\ell^2](\overline{k})$. This definition is independent of the choice of $\frac{1}{\ell}\lambda$.

The resulting map $d\Phi : C[\ell](k) \to C[\ell](k)$ is an automorphism.

Goal: Use $d\Phi$ and its inverse $(d\Phi)^{-1}$ to study triple cup products.

Triple cup products.

We consider the triple cup product of étale cohomology groups

$$F:\ \mathrm{H}^1(C,\mathbb{Z}/\ell\mathbb{Z})\times \mathrm{H}^1(C,\mu_\ell)\times \mathrm{H}^1(C,\mu_\ell)\to \mathrm{H}^3(C,\mu_\ell^{\otimes 2}).$$

Significance of F:

- useful to get an explicit description of certain profinite groups (ℓ-adic completions of the étale fundamental group of C) as quotients of pro-free groups modulo relations;
- potentially useful for cryptographic applications (on restricting to triples of cyclic groups of order ℓ, we get a trilinear map - if it is "cryptographic" it would be a big step forward in security of intellectual property).

Description of certain étale cohomology groups for C.

Assumption: $C[\ell](k) = C[\ell^2](k) \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$.

- $\mathrm{Div}(C)$ = divisor group of $C \supseteq \mathrm{Div}^0(C)$ (degree 0 divisors).
- $\mathrm{Pic}(C)$ = Picard group = $\mathrm{Div}(C)/\mathrm{PrinDiv}(C) \supseteq \mathrm{Pic}^0(C)$.
- There is an exact sequence of groups

  $$1 \to k^* \to k(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \xrightarrow{\mathrm{sum}} C(k) \to 0$$

  $\rightsquigarrow \mathrm{Pic}^0(C) = C(k)$.
- Define $D(C) := \{a \in k(C)^* \mid \mathrm{div}(a) \in \ell\,\mathrm{Div}^0(C)\}$.

One can show:

- $\mathrm{H}^1(C, \mathbb{Z}/\ell\mathbb{Z}) = \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell\mathbb{Z})$.
- $\mathrm{H}^1(C, \mu_\ell) = D(C)/(k(C)^*)^\ell$.
- $\mathrm{H}^2(C, \mu_\ell) = \mathrm{Pic}(C)/\ell\,\mathrm{Pic}(C) \rightsquigarrow \mathrm{H}^2(C, \mu_\ell^{\otimes 2}) = \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \mu_\ell$.
- $\mathrm{H}^3(C, \mu_\ell) = \mathbb{Z}/\ell\mathbb{Z} \rightsquigarrow \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) = \mu_\ell$.

Results on cup products.

$$\begin{array}{ccccccc} \mathrm{H}^1(C,\mathbb{Z}/\ell\mathbb{Z}) & \times & \mathrm{H}^1(C,\mu_\ell) & \times & \mathrm{H}^1(C,\mu_\ell) & \xrightarrow{F} & \mathrm{H}^3(C,\mu_\ell^{\otimes 2}) \\ \| & & \| & & \| & & \| \\ \mathrm{Hom}(\mathrm{Pic}(C),\mathbb{Z}/\ell\mathbb{Z}) & & D(C)/(k(C)^*)^\ell & & D(C)/(k(C)^*)^\ell & & \mu_\ell \end{array}$$

Theorem: (B-Chinburg)

Let $a \in k^* \subset D(C)$ and $b \in D(C)$ with non-trivial classes $[a],[b] \in \mathrm{H}^1(C,\mu_\ell) = D(C)/(k(C)^*)^\ell$. Let $B = \mathrm{div}(b)/\ell$ with class $[B] \in \mathrm{Pic}^0(C)[\ell] = C[\ell](k)$. Under the cup product

$$\mathrm{H}^1(C,\mu_\ell) \times \mathrm{H}^1(C,\mu_\ell) \xrightarrow{\cup} \mathrm{H}^2(C,\mu_\ell^{\otimes 2}) = \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \mu_\ell$$

we have $\quad [a] \cup [b] = (d\Phi)^{-1}[B] \otimes a^{(q-1)/\ell}.$

Corollary:

Let $t \in \mathrm{H}^1(C,\mathbb{Z}/\ell\mathbb{Z}) = \mathrm{Hom}(\mathrm{Pic}(C),\mathbb{Z}/\ell\mathbb{Z})$. With a, b, B as in the theorem, the triple cup product F gives

$$[t] \cup [a] \cup [b] = a^{t((d\Phi)^{-1}[B]) \cdot (q-1)/\ell}.$$

Consequence.

This result shows that $[t] \cup [a] \cup [b]$ depends only on the restriction of t to $\mathrm{Pic}^0(C) = C(k)$. Since $C(k)$ has no points of order ℓ^2, restriction defines isomorphisms

$$\mathrm{Hom}(\mathrm{Pic}^0(C), \mathbb{Z}/\ell\mathbb{Z}) = \mathrm{Hom}(C(k), \mathbb{Z}/\ell\mathbb{Z}) = \mathrm{Hom}(C[\ell](k), \mathbb{Z}/\ell\mathbb{Z}).$$

We can specify an element $\tilde{t} \in \mathrm{Hom}(C[\ell](k), \mathbb{Z}/\ell\mathbb{Z})$ by giving two points $Q_1, Q_2 \in C[\ell](k)$ with non-trivial Weil pairing. One lets $\tilde{t}$ be the unique homomorphism with $\tilde{t}(Q_1) = 0$ and $\tilde{t}(Q_2) = 1$.

Weil pairing: This is the non-degenerate cup product pairing

$$\begin{array}{cccccc} \langle\ ,\ \rangle_{\mathrm{Weil}} : & \mathrm{H}^1(\overline{C}, \mu_\ell) & \times & \mathrm{H}^1(\overline{C}, \mu_\ell) & \xrightarrow{\cup} & \mathrm{H}^2(\overline{C}, \mu_\ell^{\otimes 2}) \\ & \| & & \| & & \| \\ & \overline{C}[\ell](\overline{k}) & & \overline{C}[\ell](\overline{k}) & & \mu_\ell \end{array}$$

where, by our assumptions, $\overline{C}[\ell](\overline{k}) = C[\ell](k)$.

Miller's algorithm computes the Weil pairing in polynomial time.

Question.

As before, let $a \in k^* \subset D(C)$, $b \in D(C)$ such that the classes $[a], [b] \in \mathrm{H}^1(C, \mu_\ell) = D(C)/(k(C)^*)^\ell$ are non-trivial.
Let $B = \mathrm{div}(b)/\ell$ with $[B] \in \mathrm{Pic}^0(C)[\ell] = C[\ell](k)$.
Let $t \in \mathrm{H}^1(C, \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell\mathbb{Z})$ with restriction $\tilde{t} \in \mathrm{Hom}(C[\ell](k), \mathbb{Z}/\ell\mathbb{Z})$ given by two points $Q_1, Q_2 \in C[\ell](k)$ with non-trivial Weil pairing such that $\tilde{t}(Q_1) = 0$ and $\tilde{t}(Q_2) = 1$.

A basic question is whether there is a polynomial time algorithm for computing the triple cup product

$$[t] \cup [a] \cup [b] = a^{\tilde{t}((d\Phi)^{-1}[B]) \cdot (q-1)/\ell}.$$

One can certainly do this if one can compute $\tilde{t}((d\Phi)^{-1}[B])$ quickly.

We do not know if an algorithm for computing the triple cup product quickly would lead to one for computing $\tilde{t}((d\Phi)^{-1}[B])$ quickly.