Cup products on curves over finite fields

Frauke Bleher

joint with Ted Chinburg

Maurice Auslander Distinguished Lectures

and International Conference

April 28, 2019

Notation and étale cohomology.

- $k = \mathbb{F}_q$ finite field with q elements.
- $C =$ smooth projective geometrically irreducible curve over k of genus $g \geq 1$.
- $\overline{k} =$ algebraic closure of k, and $\overline{C} = C \otimes_k \overline{k}$.
- $\ell =$ odd prime, $q \equiv 1 \mod \ell \rightsquigarrow k^* \supseteq \tilde{\mu}_\ell$ (ℓth roots of 1).

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

The étale fundamental group $\pi_1(X, \eta)$ 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, $\pi_1(X, \eta)$ 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 $r \geq 0$: $$\underbrace{\mathrm{H}^r(X, \mathbb{Z}/\ell)}_{\text{étale cohomology}} \cong \underbrace{\mathrm{H}^r(\pi_1(X,\eta), \mathbb{Z}/\ell)}_{\text{profinite group cohomology}}$$

Description of étale cohomology groups.

For $X \in \{C, \overline{C}\}$, let $\mathrm{Div}(X)$ be the divisor group of X, and let $\mathrm{Pic}(X) = \mathrm{Div}(X)/\mathrm{PrinDiv}(X)$ be the Picard group of X.

Assume: ℓ-torsion of the Jacobian of C over $\overline{k}$ is defined over k
$\rightsquigarrow \mathrm{Pic}(C)[\ell] = \mathrm{Pic}(\overline{C})[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

$1 \to k^* \to k(C)^* \xrightarrow{\mathrm{div}_C} \mathrm{Div}(C) \to \mathrm{Pic}(C) \to 0$ is exact.
Define $D(C) := \{a \in k(C)^* \mid \mathrm{div}_C(a) \in \ell\,\mathrm{Div}(C)\}$.

We have: ($\mu_\ell =$ sheaf of ℓth roots of unity)

$$\begin{aligned}
\mathrm{H}^1(C, \mathbb{Z}/\ell) &= \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell) &&\cong (\mathbb{Z}/\ell)^{2g+1},\\
\mathrm{H}^1(C, \mu_\ell) &= D(C)/(k(C)^*)^\ell &&\cong (\mathbb{Z}/\ell)^{2g+1},\\
\mathrm{H}^2(C, \mu_\ell) &= \mathrm{Pic}(C)/\ell\,\mathrm{Pic}(C) &&\rightsquigarrow \mathrm{H}^2(C, \mu_\ell^{\otimes 2}) = \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell,\\
\mathrm{H}^3(C, \mu_\ell) &= \mathbb{Z}/\ell &&\rightsquigarrow \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell.
\end{aligned}$$

$$\begin{aligned}
\mathrm{H}^1(\overline{C}, \mu_\ell) &= \mathrm{Pic}(\overline{C})[\ell] &&\cong (\mathbb{Z}/\ell)^{2g},\\
\mathrm{H}^2(\overline{C}, \mu_\ell) &= \mathbb{Z}/\ell &&\rightsquigarrow \mathrm{H}^2(\overline{C}, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell.
\end{aligned}$$

Triple cup products.

Assume: $q \equiv 1 \mod \ell$ and $\mathrm{Pic}(C)[\ell] = \mathrm{Pic}(\overline{C})[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

We consider the triple cup product of étale cohomology groups

$$F: \mathrm{H}^1(C, \mathbb{Z}/\ell) \times \mathrm{H}^1(C, \mu_\ell) \times \mathrm{H}^1(C, \mu_\ell) \xrightarrow{\cup} \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) \cong \tilde{\mu}_\ell.$$

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 by restricting to triples of cyclic groups of order ℓ to get a trilinear map (if this map is "cryptographic" it would be a big step forward in the security of intellectual property).

Key sharing for 4 persons.

Restrict the triple cup product F to

$$f: \quad G_1 \times G_2 \times G_3 \;\rightarrow\; H = \tilde{\mu}_\ell$$

where G_i is identified with a cyclic group G of order ℓ $(i = 1, 2, 3)$. Then f is trilinear in the sense that

$$f(g^{\alpha_1}, g^{\alpha_2}, g^{\alpha_3}) = f(g, g, g)^{\alpha_1 \alpha_2 \alpha_3}$$

when $G = \langle g \rangle$ and $\alpha_i \in \mathbb{Z}$.

Public information: generators g of G and h of H, and map f.

Secrets: jth person $(j = 1, \ldots, 4)$ picks secret $c_j \in (\mathbb{Z}/\ell)^*$ and posts g^{c_j}.

Decode: each of the 4 persons can compute $f(g, g, g)^{c_1 c_2 c_3 c_4}$: e.g., 4th person can compute $f(g^{c_1}, g^{c_2}, g^{c_3})^{c_4}$.

f is "cryptographic" if f is "easy to compute" and "hard to break" (this can be made precise in computer science terms).

Theorem: (B-Chinburg) Assume $q \equiv 1 \mod \ell$ and $\mathrm{Pic}(C)[\ell] = \mathrm{Pic}(\overline{C})[\ell]$.

The trilinear map given by the triple cup product

$$F: \quad \mathrm{H}^1(C, \mathbb{Z}/\ell) \times \mathrm{H}^1(C, \mu_\ell) \times \mathrm{H}^1(C, \mu_\ell) \xrightarrow{\cup} \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell$$

is non-trivial. The total number of triples $\mathcal{G} = (G_1, G_2, G_3)$ *of subgroups of order* ℓ *in* $\mathrm{H}^1(C, \mathbb{Z}/\ell)$, $\mathrm{H}^1(C, \mu_\ell)$ *and* $\mathrm{H}^1(C, \mu_\ell)$, *respectively, is* $N = \left(\frac{\ell^{2g+1} - 1}{\ell - 1}\right)^3$.

The number $N(C)$ *of triples* $\mathcal{G}$ *for which the restriction* $F_{\mathcal{G}}$ *is non-degenerate satisfies* $N(C) \geq N \cdot (1 - \ell^{-1})^2$. *More precisely,*

$$\frac{\ell^{4g-1}(\ell^3 - 1)(\ell^{2g} - 1)}{(\ell - 1)^2} \leq N(C) \leq \frac{\ell^{2g+1}(\ell^{2g+1} - 1)(\ell^{2g} - 1)}{(\ell - 1)^2}.$$

If k' *is the extension of degree* ℓ *of* k *in* $\overline{k}$, *then*

$$N(C \otimes_k k') = \frac{\ell^{4g-1}(\ell^3 - 1)(\ell^{2g} - 1)}{(\ell - 1)^2}.$$

Example: elliptic curves.

Let C be an elliptic curve. On choosing an isomorphism between $\mathbb{Z}/\ell$ and $\tilde{\mu}_\ell$, the previous theorem shows that the cup product

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)\times\mathrm{H}^1(C,\mathbb{Z}/\ell)\times\mathrm{H}^1(C,\mathbb{Z}/\ell)\xrightarrow{\cup}\mathrm{H}^3(C,(\mathbb{Z}/\ell)^{\otimes 3})=\mathbb{Z}/\ell$$

is non-trivial. Since this cup product is alternating and $\mathrm{H}^1(C,\mathbb{Z}/\ell)$ has dimension 3 over $\mathbb{Z}/\ell$, this trilinear map is, up to multiplication by a non-zero scalar, the unique non-trivial alternating form of degree three on $\mathrm{H}^1(C,\mathbb{Z}/\ell)$.

Hence the number $N(C)$ of triples $\mathcal{G}$ for which the restriction $F_{\mathcal{G}}$ is non-degenerate is therefore

$$N(C)=\frac{\#\mathrm{GL}_3(\mathbb{Z}/\ell)}{(\ell-1)^3}=\frac{\ell^{4g-1}(\ell^3-1)(\ell^{2g}-1)}{(\ell-1)^2}$$

when $g=1$.

A formula for the triple cup product

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)\times \mathrm{H}^1(C,\mu_\ell)\times \mathrm{H}^1(C,\mu_\ell)\xrightarrow{\cup} \mathrm{H}^3(C,\mu_\ell^{\otimes 2})\cong \tilde{\mu}_\ell.$$

Assumptions: $q\equiv 1 \mod \ell$ and $\mathrm{Pic}(C)[\ell]=\mathrm{Pic}(\overline{C})[\ell]$.

Recall: $1\to k^*\to k(C)^*\xrightarrow{\mathrm{div}_C}\mathrm{Div}(C)\to \mathrm{Pic}(C)\to 0$ is exact.

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

We have:

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

Theorem: (B-Chinburg) Assume $q \equiv 1 \mod \ell$ and $\mathrm{Pic}(C)[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

Suppose $a, b \in D(C)$ define non-trivial classes $[a], [b] \in \mathrm{H}^1(C, \mu_\ell)$. Choose $\alpha \in k(C)^{\mathrm{sep}}$ with $\alpha^\ell = a$. Then $L = k(C)(\alpha)$ is the function field of an irreducible smooth projective curve C' over k. There is an element $\gamma \in L$ such that $b = \mathrm{Norm}_{L/k(C)}(\gamma)$. Write $\mathfrak{b} = \mathrm{div}_C(b)/\ell \in \mathrm{Div}(C)$, and let $\mathrm{Gal}(L/k(C)) = \langle\sigma\rangle$. Then there is a divisor $\mathfrak{c} \in \mathrm{Div}(C')$ such that

$$(1-\sigma)\cdot\mathfrak{c} = \mathrm{div}_{C'}(\gamma) - \pi^*\mathfrak{b}$$

where $\pi : C' \to C$ is the morphism associated with $k(C) \hookrightarrow L$. We have $\xi = \sigma(\alpha)/\alpha \in \tilde{\mu}_\ell$. We obtain

$$[a] \cup [b] = [\mathrm{Norm}_{C'/C}(\mathfrak{c})] \otimes \xi \qquad \in \mathrm{Pic}(C) \otimes \tilde{\mu}_\ell = \mathrm{H}^2(C, \mu_\ell^{\otimes 2})$$

where $[\mathfrak{d}]$ is the class in $\mathrm{Pic}(C)$ of a divisor $\mathfrak{d}$.

If $t \in \mathrm{H}^1(C, \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell)$, then

$$[t] \cup [a] \cup [b] = \xi^{t([\mathrm{Norm}_{C'/C}(\mathfrak{c})])} \qquad \in \tilde{\mu}_\ell = \mathrm{H}^3(C, \mu_\ell^{\otimes 2}).$$

Computability and restriction.

- This formula is based on a formula by McCallum-Sharifi for a cup product used in the context of Iwasawa theory.
- We do not know if this formula can in general be computed in polynomial time.

We now consider the restriction of the cup product

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)\times \mathrm{H}^1(C,\mu_\ell)\times \mathrm{H}^1(C,\mu_\ell)\xrightarrow{\cup}\mathrm{H}^3(C,\mu_\ell^{\otimes 2})\cong\tilde{\mu}_\ell$$

such that the third argument comes from $\mathrm{H}^1(k,\mu_\ell)$.

Note: The group $\mathrm{H}^1(k,\mu_\ell)=k^*/(k^*)^\ell$ has order ℓ and is the kernel of the surjective restriction map

$$r:\quad \begin{array}{ccc} \mathrm{H}^1(C,\mu_\ell) & \longrightarrow & \mathrm{H}^1(\overline{C},\mu_\ell) \\ \| & & \| \\ \mathrm{Hom}(\mathrm{Pic}(C),\tilde{\mu}_\ell) & & \mathrm{Hom}(\mathrm{Pic}(\overline{C}),\tilde{\mu}_\ell) \end{array}$$

Formula of the restriction of the triple cup product.

As above, $r : \mathrm{H}^1(C, \mu_\ell) \to \mathrm{H}^1(\overline{C}, \mu_\ell)$ is the surjective restriction map with kernel $\mathrm{H}^1(k, \mu_\ell) = k^*/(k^*)^\ell$.

Theorem: (B-Chinburg) Assume $q \equiv 1 \mod \ell$ and $\mathrm{Pic}(C)[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.
Suppose $a, b \in D(C)$ define non-trivial classes $[a], [b] \in \mathrm{H}^1(C, \mu_\ell)$, and suppose $b \in k^*$. Let $t \in \mathrm{H}^1(C, \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell)$.

Then $b^{(q-1)/\ell} \in \tilde{\mu}_\ell$
and $w = t \otimes b^{(q-1)/\ell} \in \mathrm{H}^1(C, \mathbb{Z}/\ell) \otimes \tilde{\mu}_\ell = \mathrm{H}^1(C, \mu_\ell)$.

One has

$$[t] \cup [a] \cup [b] = \langle r(w), r([a]) \rangle_{\mathrm{Weil}} \quad \in \; \mathrm{H}^2(\overline{C}, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell$$

where

$$\langle \; , \; \rangle_{\mathrm{Weil}} : \; \mathrm{H}^1(\overline{C}, \mu_\ell) \times \mathrm{H}^1(\overline{C}, \mu_\ell) \; \to \; \mathrm{H}^2(\overline{C}, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell$$

is the Weil pairing, i.e. the non-degenerate cup product pairing associated to $\overline{C}$.

More precise connection to the (inverse) Weil pairing.

$$\begin{array}{ccccc} \langle\ ,\ \rangle_{\mathrm{Weil}} : \mathrm{H}^1(\overline{C}, \mu_\ell) & \times & \mathrm{H}^1(\overline{C}, \mu_\ell) & \longrightarrow & \mathrm{H}^2(\overline{C}, \mu_\ell^{\otimes 2}) \\ \| & & \| & & \| \\ \mathrm{Pic}(\overline{C})[\ell] & & \mathrm{Pic}(\overline{C})[\ell] & & \tilde{\mu}_\ell \end{array}$$ non-degenerate

where, by our assumptions, $\mathrm{Pic}(C)[\ell] = \mathrm{Pic}(\overline{C})[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

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

Given $w \in \mathrm{H}^1(C, \mu_\ell) = \mathrm{Hom}(\mathrm{Pic}(C), \tilde{\mu}_\ell)$, then $r(w) \in \mathrm{H}^1(\overline{C}, \mu_\ell)$ is produced using the so-called inverse Weil identifications

$$\mathrm{Pic}(\overline{C})[\ell] = \mathrm{H}^1(\overline{C}, \mu_\ell) = \mathrm{Hom}(\mathrm{Pic}(\overline{C})[\ell], \tilde{\mu}_\ell).$$

Concretely, suppose $r(w)$ is identified as a homomorphism to $\tilde{\mu}_\ell$ by giving its values on generators of $\mathrm{Pic}(C)[\ell] = \mathrm{Pic}(\overline{C})[\ell]$ as specified by $w : \mathrm{Pic}(C) \to \tilde{\mu}_\ell$. Then realizing $r(w)$ as an element of $\mathrm{H}^1(\overline{C}, \mu_\ell) = \mathrm{Pic}(\overline{C})[\ell]$ amounts to inverting the Weil pairing.

Issue: No polynomial time algorithm is known for inverting the Weil pairing.