Cup products on curves over finite fields

Ted Chinburg
joint with Frauke Bleher

Hawaii AMS meeting
March 2019
Let $C$ be an elliptic curve over a finite field $k$ of order $q$ and let $\overline{C} = \overline{k} \otimes C$ be the base change of $C$ to an algebraic closure $\overline{k}$ of $k$. Suppose $\ell$ is a prime with $q \equiv 1 \mod \ell$.

**Miller’s algorithm** gives a polynomial time algorithm for computing the Weil pairing

$$\langle \ , \rangle_{\text{Weil}} : \overline{C}[\ell] \times \overline{C}[\ell] \to \tilde{\mu}_\ell.$$

This pairing is the same as the étale cup product

$$H^1(\overline{C}, \mu_\ell) \times H^1(\overline{C}, \mu_\ell) \to H^2(\overline{C}, \mu_\ell \otimes 2) = \tilde{\mu}_\ell.$$
Cup products over $C$ are harder to compute. We will compare the complexity of computing specializations of the pairing

$$H^1(C, \mathbb{Z}/\ell) \times H^1(C, \mu_\ell) \rightarrow H^2(C, \mu_\ell) = \text{Pic}(C)/\ell \quad (1)$$

with that of Inverting the Weil pairing. One reason for studying this is to consider the cryptographic use of the trilinear map

$$H^1(C, \mathbb{Z}/\ell) \times H^1(C, \mu_\ell) \times H^1(C, \mu_\ell) \rightarrow H^3(C, \mu_\ell \otimes 2) = \tilde{\mu}_\ell$$

which comes about from composing (1) with the class field theory isomorphism

$$H^1(C, \mu_\ell) = \text{Hom}(	ext{Pic}(C), \tilde{\mu}_\ell).$$
Inverting the Weil pairing

The problem of inverting the Weil pairing has to do with making explicit the isomorphism

$$\text{Hom}(\overline{C}[\ell], \tilde{\mu}_\ell) \to \overline{C}[\ell]$$

induced by the Weil pairing. For some history of work on this, see the blog post “Recent work on pairing inversion” by S. Galbraith.

Here is a more specific formulation:

**Problem:** Suppose one is given the projective coordinates of generators $Q_1$ and $Q_2$ for $\overline{C}[\ell]$ as well as elements $\zeta_1, \zeta_2 \in \tilde{\mu}_\ell$. Find the projective coordinates of the unique $Q \in \overline{C}[\ell]$ such that

$$\langle Q, Q_1 \rangle_{\text{Weil}} = \zeta_1 \quad \text{and} \quad \langle Q, Q_2 \rangle_{\text{Weil}} = \zeta_2.$$
Cup products for curves over finite fields

We will consider two different specializations of the pairing

\[ H^1(C, \mathbb{Z}/\ell) \times H^1(C, \mu_\ell) \to H^2(C, \mu_\ell) = \text{Pic}(C)/\ell. \]  

(2)
Specializing elements of $H^1(C, \mathbb{Z}/\ell)$

There is a diagram

$$
\begin{array}{ccc}
H^1(C, \mathbb{Z}/\ell) & \times & H^1(C, \mu_\ell) \\
\uparrow & & \downarrow \\
\text{Hom}(\text{Gal}(N/k), \mathbb{Z}/\ell) & \times & C[\ell](k) \\
\downarrow & & \longrightarrow \\
& & C[\ell](k)
\end{array}
\rightarrow H^2(C, \mu_\ell) = \text{Pic}(C)/\ell
$$

of the following kind. Let $N/k$ be the unique cyclic degree $\ell$ extension. The left vertical homomorphism arises from

$$H^1(C, \mathbb{Z}/\ell) = \text{Hom}(\pi_1(C), \mathbb{Z}/\ell)$$

and the natural surjection $\pi_1(C) \to \text{Gal}(N/k)$. The next vertical homomorphism is from the Kummer sequence and

$C[\ell](k) = H^1(C, \mathbb{G}_m)[\ell]$. The right vertical homomorphism is from the natural inclusion $C[\ell](k) = \text{Pic}(C)[\ell] \to \text{Pic}(C)$. 

Ted Chinburg

Cup products on curves over finite fields
Complexity of this specialization

The bottom row of the previous diagram is a pairing

$$\langle , \rangle_1 : \text{Hom}(\text{Gal}(N/k), \mathbb{Z}/\ell) \times C[\ell](k) \to C[\ell](k).$$

**Problem 1:** Let $h$ be the element of $\text{Hom}(\text{Gal}(N/k), \mathbb{Z}/\ell)$ sending the Frobenius automorphism $\Phi_k$ to 1 mod $\ell$. Suppose $Q \in C[\ell](k)$ is given in projective coordinates for $C$. Calculate the projective coordinates of a representative in $C(k)$ for $\langle h, Q \rangle_1$.

**Hypothesis:** Assume from now on that

$$\#C[\ell](k) = \#C[\ell^2](k) = \ell^2.$$  

**Theorem (B - C):** Problem 1 can be solved in a polynomial in the run time of any algorithm which inverts the Weil pairing.

We do not know if Problem 1 is equal in difficulty to inverting the Weil pairing.
Specializing elements of $H^1(C, \mu_\ell)$

There is a diagram

$$
\begin{array}{c}
H^1(C, \mathbb{Z}/\ell) \times H^1(C, \mu_\ell) \longrightarrow H^2(C, \mu_\ell) = \text{Pic}(C)/\ell \\
\downarrow \downarrow \\
\text{Hom}(C[\ell](k), \mathbb{Z}/\ell) \times k^*/(k^*)^\ell \longrightarrow C(k)/\ell
\end{array}
$$

of the following kind. The left vertical homomorphism arises from the inclusion $\pi_1(\overline{C}) \to \pi_1(C)$ and $\pi_1(\overline{C})^{ab}/\ell = C[\ell](k) = C[\ell](k)$. The next vertical homomorphism is the inflation map $H^1(k, \mu_\ell) = k^*/(k^*)^\ell \to H^1(C, \mu_\ell)$. The right vertical homomorphism is from the natural inclusion

$$
C(k) = \text{Pic}^0(C) \to \text{Pic}(C).
$$
Complexity of this specialization

The bottom row of the previous diagram is a pairing

$$\langle , \rangle_2 : \text{Hom}(C[\ell](k), \mathbb{Z}/\ell) \times k^*/(k^*)^\ell \rightarrow C(k)/\ell.$$ 

Problem 2: As input, give the projective coordinates of generators $Q_1$ and $Q_2$ for $C[\ell](k)$, an element $\beta \in k^*$ and elements $a_1, a_2 \in \mathbb{Z}/\ell$. Let $f$ be the element of $\text{Hom}(C[\ell](k), \mathbb{Z}/\ell)$ for which $f(Q_1) = a_1$ and $f(Q_2) = a_2$. Let $[\beta] \in k^*/(k^*)^\ell$ be the class represented by $\beta$. Calculate the projective coordinates of a representative for $\langle f, [\beta] \rangle_2$ in $C(k)$.

Theorem (B - C): The complexity of inverting the Weil pairing and of Problem 2 are equivalent, in the sense that either can be solved in a polynomial in the run time of any algorithm giving a solution of the other.
Some ideas from the proofs

The main tools are counterparts over global function fields of formulas McCallum and Sharifi proved for étale cup products over number fields. Here is one example.

Define an arithmetic derivative of the Frobenius $\Phi_k$ on $C[\ell](k)$ by the formula

$$d\Phi_k(\lambda) = (\Phi_k - 1)(\frac{1}{\ell} \lambda)$$

for $\lambda \in C[\ell](k)$, where $\frac{1}{\ell} \lambda$ is any $\ell$-th root of $\lambda$ in $C[\ell^2](\overline{k})$. The resulting map $d\Phi_k : C[\ell](k) \to C[\ell](k)$ is an automorphism under our hypotheses. The derivative of the Legendre transform of Frobenius is defined to be the inverse

$$d\Phi_k^{-1} : C[\ell](k) \to C[\ell](k)$$

of the isomorphism $d\Phi_k$. 
Theorem: The pairing

\[ \langle , \rangle_1 : \text{Hom}(\text{Gal}(N/k), \mathbb{Z}/\ell) \times C[\ell](k) \to C[\ell](k). \]

arising in Problem 1 satisfies

\[ \langle h, Q \rangle_1 = d\Phi_k^{-1}Q. \]

where \( h \) sends the Frobenius of \( \text{Gal}(N/k) \) to 1 and \( Q \in C[\ell](k) \).
The Tate-Lichtenbaum pairing

$$\tau : (C(k)/\ell) \times C[\ell](k) \to k^*/(k^*)^\ell$$ (3)

has the property that

$$\tau(P, Q)^{q-1 \over \ell} = \langle d\Phi_k P, Q \rangle_{\text{Weil}}$$ (4)

if $P$ comes from a point in $C[\ell](k)$.

A key step in the proof of the first Theorem is that Miller’s algorithm gives a polynomial time algorithm for computing values of the Tate-Lichtenbaum pairing.

We then show

$$\langle d\Phi_k^{-1} Q, P \rangle_{\text{Weil}} = (\langle d\Phi_k P, Q \rangle_{\text{Weil}})^{-\left(\#C(k)/\ell^2\right)}$$ (5)

where $\#C(k)/\ell^2$ can be computed by Schoof’s algorithm. Given an algorithm for inverting the Weil pairing, we use (5) to calculate $d\Phi_k^{-1} Q = \langle h, Q \rangle_1$ from $Q$. 