Recovering algebraic curves from L-functions of Hilbert class fields

Jeremy Booher and José Felipe Voloch

Abstract
In this paper, we prove that a smooth hyperbolic projective curve over a finite field can be recovered from L-functions associated to the Hilbert class field of the curve and its constant field extensions. As a consequence, we give a new proof of a result of Mochizuki and Tamagawa that two such curves with isomorphic fundamental groups are themselves isomorphic.

Keywords: L-functions, Curves over finite fields, Fundamental groups

1 Introduction
It has long been known that the zeta function of a global field does not determine the field uniquely (e.g. for function fields, take isogenous, but non-isomorphic, elliptic curves). Recently, there has been work done to recover a global field from more refined invariants of a similar nature. For example, [3] proves that a global field can be recovered from the collection of all its abelian L-functions. Another example is the conjecture [10, Conjecture 2.2] which predicts that the zeta functions of the Hilbert class field $H(C)$ and successive iterates $H(H(C)), \ldots$ determines an algebraic curve $C$ over a finite field up to Frobenius twist. These two approaches are naturally related to the classical work of Neukirch and Uchida of recovering global fields from their absolute Galois groups [12], and the more recent work of Mochizuki and Tamagawa (see [5, 11]) of recovering algebraic curves from their fundamental groups, respectively.

The purpose of this paper is twofold. First, we prove that a smooth proper curve of genus at least two (i.e. a proper hyperbolic curve) over a finite field can be recovered from L-functions associated to the Hilbert class field of the curve and its constant field extensions. Secondly, we show that two such curves with isomorphic fundamental groups are isomorphic. This gives a new proof of the weak isomorphism version of the theorem of Mochizuki and Tamagawa mentioned earlier.

Our approach crucially depends on the work of Zilber [13, 14], resolving a conjecture of Bogomolov et al. [2].

2 L-functions
Let $q = p^a$ be a prime power, and $C$ be a smooth, projective, irreducible curve over $\mathbb{F}_q$ of genus at least one. A divisor $D_1$ of degree one on $C$ gives an Abel–Jacobi embedding of $C$
into $f_C$ via $P \mapsto [P - D_1]$ on geometric points. Throughout, we fix a choice of degree one divisor and Abel–Jacobi embedding for each curve; a degree-one divisor exists exists by [7].

**Definition 2.1** Let $f_C$ be the Jacobian of $C$ and $\Phi : f_C \to f_C$ denote the $\mathbb{F}_q$-Frobenius map. A Hilbert class field of $C$, with respect to a fixed Abel–Jacobi embedding of $C$ into $f_C$, is defined to be $H(C) := (\Phi - \text{id})^*(C) \subset f_C$.

The function field of $H(C)$ is a Hilbert class field of the function field of $C$ in the sense of class field theory [1, VIII.3]. Thus we retain the name even though we are considering the smooth projective curve throughout. The curve $H(C)$ is an unramified abelian cover of $C$ with Galois group $f_C(\mathbb{F}_q) = (\ker(\Phi - \text{id})(\mathbb{F}_q))$. Note that changing $D_1$ twists $H(C)$. Let $S_C$ denote the set of places of $C$.

**Definition 2.2** Let $\chi : Gal(H(C)/C) = f_C(\mathbb{F}_q) \to \mathbb{C}^*$ be a character. For a place $P$ of $C$, let $\text{Frob}_P \in Gal(H(C)/C)$ denote the Frobenius at $P$. The $L$-series for $\chi$ is defined as

$$L(t, C, \chi) := \prod_{P \in S_C} (1 - \chi(\text{Frob}_P)T^{\deg P})^{-1}.$$ 

The following result is a special case of [9, VI §5 Theorem 2].

**Lemma 2.3** For $P \in S_C$, the Frobenius $\text{Frob}_P$ is $[P - \deg(P)D_1] \in f_C(\mathbb{F}_q) = Gal(H(C)/C)$, viewing $P$ as a divisor of degree $\deg(P)$.

We see that

$$L(t, C, \chi) = \sum_{D \geq 0} \chi([D - \deg(D)D_1])t^{\deg D}, \quad (2.1)$$

where the sum is over effective divisors on $C$ and $[\cdot]$ associates a divisor of degree zero to its divisor class in the Jacobian. Note that this again depends on the fixed choice of $D_1$.

We let $\text{Frob}$ denote the $q$th power map. We refer to the $q^m$-th power map $\text{Frob}^m$ as the $\mathbb{F}_q^m$-Frobenius, and refer to an arbitrary element of $Gal(\mathbb{F}_q^m/\mathbb{F}_q)$ as a generalized Frobenius. These field automorphisms induce isomorphisms of schemes over $\mathbb{F}_q$, and in particular on the base change to $\mathbb{F}_q$ of schemes over $\mathbb{F}_q$. If $C$ is a curve defined over $\mathbb{F}_q$, then the Frobenius twist $\text{Frob}^m(C)$ and the curve $C$ are isomorphic as schemes (via the map induced by the field automorphism $\text{Frob}^m$), but not as $\mathbb{F}_q$-schemes.

Zilber [13,14] resolved a conjecture of Bogomolov et al. [2].

**Theorem 2.4** [14, Theorem 1.3] Let $C$ and $C'$ be smooth, projective, irreducible curves over $\mathbb{F}_q$ of genus at least two. If $\psi : f_C(\mathbb{F}_q) \to f_C(\mathbb{F}_q)$ is a group isomorphism such that $\psi(C(\mathbb{F}_q)) = C'(\mathbb{F}_q)$ (with respect to the fixed Abel–Jacobi embeddings), then $\psi$ arises from a morphism of curves composed with a lift of Frobenius maps.

More precisely, there exists an integer $m$, an isomorphism $\alpha : \text{Frob}^m(C) \simeq C'$, and a generalized Frobenius $\beta : \mathbb{F}_q \to \mathbb{F}_q$ restricting to $\text{Frob}^{-m}$ on $\mathbb{F}_q$ such that $\psi$ is the map on Jacobians induced by $\alpha \circ \beta : C \to C'$.

We use this to prove our first main result.
Theorem 2.5 Let $C, C'$ be smooth projective curves of genus at least two over a finite field $\mathbb{F}_q$. Suppose $\psi : J_C(\mathbb{F}_q) \to J_{C'}(\mathbb{F}_q)$ is a set-theoretic map inducing an isomorphism of groups between $J_C(\mathbb{F}_q^n)$ and $J_{C'}(\mathbb{F}_q^n)$ for every $n \geq 1$. If

$$L(t, C \otimes \mathbb{F}_q^n, \chi) = L(t, C' \otimes \mathbb{F}_q^n, \chi \circ \psi|_{J_C(\mathbb{F}_q^n)})$$

for all $n$ and all characters $\chi$ of $J_C(\mathbb{F}_q^n)$, then $C$ and $C'$ are Frobenius twists of each other.

Proof We show that $\psi(C(\mathbb{F}_q^n)) = C'(\mathbb{F}_q^n)$ for all $n \geq 1$ under our hypotheses, in order to apply Zilber’s theorem. It suffices to treat the case $n = 1$ as the same arguments applied to $C \otimes \mathbb{F}_q^n$ and $C' \otimes \mathbb{F}_q^n$ yield the general result. Using (2.1) we write

$$L(t, C, \chi) = \sum_{x \in J_C(\mathbb{F}_q^n)} \chi(x) \left( \sum_{d=0}^{\infty} \{D \geq 0 : D \sim x + dD_1\}t^d. \right)$$

Knowledge of all these $L$-functions for all characters $\chi$ gives us the values of $\#\{D \geq 0 : D \sim x + dD_1\}$ for each $x \in J_C(\mathbb{F}_q)$, $d \geq 0$. Finally $x + D_1 \sim P, P \in C(\mathbb{F}_q)$ if and only if $\#\{D \geq 0 : D \sim x + dD_1\} = 1$. Indeed, if $x + D_1$ is not linearly equivalent to a point then $\#\{D \geq 0 : D \sim x + dD_1\} = 0$ and if it is, then $\#\{D \geq 0 : D \sim x + dD_1\} = 1$ since the curve has positive genus so distinct points are not linearly equivalent. This shows that $\psi(C(\mathbb{F}_q^n)) = C'(\mathbb{F}_q^n)$; applying Theorem 2.4 completes the proof. □

Remark 2.6 The proof actually gives more. The proof only uses that the derivatives of $L(t, C \otimes \mathbb{F}_q^n, \chi)$ and of $L(t, C' \otimes \mathbb{F}_q^n, \chi \circ \psi|_{J_C(\mathbb{F}_q^n)})$ at $t = 0$ are equal for all $n$ and $\chi$. Secondly, the proof shows there is an integer $m$, an isomorphism $\alpha : \text{Frob}^m(C) \to C'$, and a generalized Frobenius $\beta : \mathbb{F}_q \to \mathbb{F}_q$ restricting to $\text{Frob}^{-m}$ on $\mathbb{F}_q$ such that $\psi$ is the composition

$$J_C(\mathbb{F}_q) \xrightarrow{\beta} J_{\text{Frob}^m(C)}(\mathbb{F}_q) \xrightarrow{\alpha} J_{C'}(\mathbb{F}_q).$$

Remark 2.7 The theorem fails for curves of genus one. In this case, for any non-trivial character $\chi$ we have $L(t, C \otimes \mathbb{F}_q^n, \chi) = 1$, and for the trivial character one gets the zeta function of $C \otimes \mathbb{F}_q^n$, which only detects the isogeny class of $C$. If we have two elliptic curves with isomorphic endomorphism rings (which exist if the class number of the ring is at least two), then results of Kohel [4, Propositions 21 and 22] imply the existence of two isogenies of coprime orders between the elliptic curves (which are their own Jacobians) and, in particular we have an isomorphism of groups between $C(\mathbb{F}_q^n)$ and $C'(\mathbb{F}_q^n)$ for every $n \geq 1$ inducing equality of all corresponding $L$-functions.

Remark 2.8 It is not generally enough to have $J_C(\mathbb{F}_q)$ and $J_{C'}(\mathbb{F}_q)$ isomorphic and the corresponding $L$-functions matching (i.e. the conditions only for $n = 1$). To see this, let $C/\mathbb{F}_3$ be a curve of genus two with non-constant map of degree two $\pi : C \to \mathbb{P}^1$ such that:

- $C$ has no rational or quadratic Weierstrass points,
- only one rational point of $\mathbb{P}^1$ splits in $C$ under $\pi$,
- $J_C(\mathbb{F}_3)$ has order 5.

[10, Example 4.1] provides two non-isomorphic curves satisfying these conditions. But these conditions will determine $L(t, C, \chi)$ for each character $\chi : J_C(\mathbb{F}_3) \to \mathbb{C}^*$, providing the desired example.
The conditions imply one fiber of $\pi$ consists of rational points and the other three fibers of $\pi$ consist of pairs of quadratic points. Let $C(\mathbb{F}_3) = \{P, Q\}$. The fibers give linearly equivalent effective divisors of degree two. The divisors $2P, 2Q$ are also effective divisors of degree two but are not equivalent to the fibers or to each other. As $JC(\mathbb{F}_3)$ has order 5 there are two more classes of divisors of degree two, each represented by a single effective divisor consisting of conjugate quadratic points. So $#C(\mathbb{F}_3) = 2, #C(\mathbb{F}_9) = 12$ and the zeta function of $C$ (which is the $L$-function with trivial character) is determined.

We use $D_1 = P$ as the divisor of degree 1 embedding $C$ in $JC$. For divisors of degree one, $P \mapsto 0$ and $Q \mapsto Q - P$; notice the latter generates $JC(\mathbb{F}_3)$. For divisors of degree 2, we have $D \mapsto D - 2P$. Thus $P + Q \mapsto Q - P$ and likewise for the other fibers of $\pi$ as they are linearly equivalent. Furthermore $2P \mapsto 0$ and $2Q \mapsto 2(Q - P)$. The two other effective divisors of degree 2 map to $3(Q - P), 4(Q - P)$ respectively. Since we know that $L(t, C, \chi)$ is a quadratic polynomial, if $\chi \neq 1$ this is enough information to compute it. In particular, if $\chi(Q - P) = \zeta$ then using (2.1) we have

$$L(t, C, \chi) = 1 + (1 + \zeta)t + (4\zeta + 1 + \zeta^2 + \zeta^3 + \zeta^4)t^2 = 1 + (1 + \zeta)t + 3\zeta t^2.$$

**Remark 2.9** All of the $L$-functions appearing in the theorem can be realized as (non-abelian) $L$-functions over the base field up to a harmless change of variable. Recall that for a Galois extension of global fields $L/K$ with Galois group $G$, a subgroup $H \subset G$ with $K' = L^H$, and a representation $\rho$ of $H$, we have that (note the change of variable to $s$, such that $t = q^{-s}$ in the function field case)

$$L(s, L/K', \rho) = L(s, L/K, \text{Ind}_H^G(\rho)).$$

Let $K = \mathbb{F}_q(C)$ and $L$ be the function field of the cover of $C$ corresponding to the cover of $JC$ given by $(\text{Frob}^n - \text{id})^*$; note this cover includes an extension of the constant field when $n > 1$. We see that for a character $\chi$ of $JC(\mathbb{F}_q^n)$,

$$L(t^n, C \otimes \mathbb{F}_q^n, \chi) = L(t, C, \text{Ind}_{JC(\mathbb{F}_q^n)}^{\text{Gal}(L/K)}(\chi)).$$

The equality of $L$-functions in Theorem 2.5 can be checked after the change of variable $t \mapsto t^n$, so can be checked using $L$-functions over the base field.

### 3 Fundamental groups

Recall the fundamental exact sequence of étale fundamental groups

$$1 \to \pi_1(\overline{C}) \to \pi_1(C) \to G_{\mathbb{F}_q} \to 1, \quad (3.1)$$

where $\overline{C} = C \otimes \mathbb{F}_q$ and $G_{\mathbb{F}_q}$ is the absolute Galois group of $\mathbb{F}_q$. We use the notation $pc : \pi_1(C) \to G_{\mathbb{F}_q}$ for the right map in the above sequence.

As mentioned in the introduction, we give a new proof of the following theorem.

**Theorem 3.1** (Mochizuki–Tamagawa) Let $C, C'$ be smooth projective curves of genus at least two over a finite field $\mathbb{F}_q$. If there is an isomorphism $\pi_1(C) \simeq \pi_1(C')$ of groups then $C$ is isomorphic to $C'$ as schemes.

**Proof** First, it is already known that $\pi_1(C)$ group-theoretically determines the Frobenius element in $G_{\mathbb{F}_q}$ [11, Proposition 3.4]. Thus the isomorphism $\pi_1(C) \simeq \pi_1(C')$ induces the
identity on $G_{\mathbb{F}_q}$ via $p_C$ and $p_{C'}$ and induces isomorphisms $\pi_1(C \otimes \mathbb{F}_{q^n}) \simeq \pi_1(C' \otimes \mathbb{F}_{q^n})$ for each $n \geq 1$.

Next, for $n \geq 1$ there is a short exact sequence

$$0 \to J_C(\mathbb{F}_{q^n}) \to \text{Pic}_C(\mathbb{F}_{q^n}) \to \widehat{\mathbb{Z}} \to 0.$$  \hspace{1cm} (3.2)

obtained by taking the profinite completion of the short exact sequence arising from the degree map $\text{Pic}_C(\mathbb{F}_{q^n}) \to \mathbb{Z}$. Class field theory identifies $\text{Pic}_C(\mathbb{F}_{q^n})$ with $\pi_1(C \otimes \mathbb{F}_{q^n})^{\text{ab}}$ and the degree map with $p_{C \otimes \mathbb{F}_{q^n}}$. It follows that $\pi_1(C \otimes \mathbb{F}_{q^n})^{\text{ab,tor}}$ is identified with $J_C(\mathbb{F}_{q^n})$. The (group-theoretic) transfer map $\pi_1(C)^{\text{ab}} \to \pi_1(C \otimes \mathbb{F}_{q^n})^{\text{ab}}$ is compatible with the Artin map, and induces the inclusion map $J_C(\mathbb{F}_{q^n}) \to J_C(\mathbb{F}_{q^n})$ [8, VII.8]. Therefore the isomorphism $\pi_1(C) \simeq \pi_1(C')$ determines isomorphisms $\pi_1(C \otimes \mathbb{F}_{q^n}) \simeq \pi_1(C' \otimes \mathbb{F}_{q^n})$ and hence isomorphisms $\psi_n : J_C(\mathbb{F}_{q^n}) \simeq J_C'(\mathbb{F}_{q^n})$. For $m \geq 1$, $\psi_n$ and $\psi_{nm}$ are compatible with the inclusion maps $J_C(\mathbb{F}_{q^n}) \to J_C(\mathbb{F}_{q^{nm}})$ and $J_C'(\mathbb{F}_{q^n}) \to J_C'(\mathbb{F}_{q^{nm}})$, and hence we obtain a bijection $\psi : J_C(\mathbb{F}_{q^n}) \to J_C'(\mathbb{F}_{q^n})$ as in Theorem 2.5.

Now let $J_X$ be the Jacobian of a curve $X$ defined over a finite field $k$ with fixed Abel–Jacobi embedding. Analogously to (3.1), there is a fundamental exact sequence

$$1 \to \pi_1(J_X) \to \pi_1(J_X) \otimes \mathbb{G}_m \to G_k \to 1.$$  \hspace{1cm} (3.3)

Furthermore $\pi_1(J_X)$ is the abelianisation of $\pi_1(X)$. Thus the prime-to-$p$ part of $\pi_1(J_X)$ is the product of the Tate modules of $J_X$. The fundamental exact sequence describes the Galois action on the Tate module, and so the Tate module with its Galois action is determined by $\pi_1(J_X)$ (equivalently by $\pi_1(X)^{\text{ab}}$ using the fixed Abel–Jacobi embedding).

We apply this with $k = \mathbb{F}_q$ and $X := X_n = H(C \otimes \mathbb{F}_{q^n})$. Let $\Phi$ denote the $\mathbb{F}_q$-Frobenius on $J_C$. For characters $\chi$ of $J_C(\mathbb{F}_{q^n})$, the $L(t, C \otimes \mathbb{F}_{q^n}, \chi)$ are the characteristic polynomials of $\Phi^t$ in the $\chi$-eigencomponent of the Tate module of $J_X_n$. Notice that $\pi_1(X_n)$ is determined group-theoretically by $\pi_1(C)$ as it is the kernel of the morphism $\pi_1(C \otimes \mathbb{F}_{q^n}) \to \pi_1(C \otimes \mathbb{F}_{q^n})^{\text{ab,tor}} = J_C(\mathbb{F}_{q^n})$ and we already know that $\pi_1(C \otimes \mathbb{F}_{q^n})$ is determined group-theoretically. Then the previous paragraph applies, showing that the Tate modules and hence $L$-functions for $C$ and $C'$ agree. Theorem 2.5 shows that $C$ and $C'$ are Frobenius twists, and hence are isomorphic as schemes.

\[\square\]

Remark 3.2 Theorem 3.1 shows how to recover projective curves from their fundamental groups. It is known to experts that the affine case follows relatively easily. Historically the argument went in the other direction; Mochizuki proved the projective case building on work of Tamagawa which treated affine curves [5, 11].

Remark 3.3 We do not need the full data of an isomorphism $\pi_1(C) \simeq \pi_1(C')$ in order to apply Theorem 2.5. In particular, we only need two pieces of information for each $n \geq 1$:

- an isomorphism $\pi_1(C \otimes \mathbb{F}_{q^n})^{\text{ab}} \simeq \pi_1(C' \otimes \mathbb{F}_{q^n})^{\text{ab}}$;
- isomorphisms $\pi_1(X_{n, \mathbb{F}_q})^{\text{ab}} \simeq \pi_1(X'_{n, \mathbb{F}_q})^{\text{ab}}$ that are compatible with the action by the Frobenius and actions by $J_C(\mathbb{F}_{q^n})$ and $J_C'(\mathbb{F}_{q^n})$.

The first identifies $J_C(\mathbb{F}_{q^n}) \simeq J_C'(\mathbb{F}_{q^n})$ and similarly for geometric points. The latter isomorphisms, or even just an isomorphism of the abelian pro-$\ell$ fundamental groups for any prime $\ell \neq p$, suffices to identify the $L$-functions. In particular, it identifies
$H^1(X_{n,F_q}, \mathbb{Q}_\ell) \simeq H^1(X'_{n,F_q}, \mathbb{Q}_\ell)$ with an action of $J_C(F_{q^n}) \simeq \text{Gal}(X_n / C \otimes F_{q^n})$ and of Frobenius. The $L$-function is the characteristic polynomial of the $F_{q^n}$-Frobenius on the $X$-component of the cohomology $H^1(X_{n,F_q}, \mathbb{Q}_\ell)$. In particular, an isomorphism between the “geometrically abelian by abelian pro-$\ell$” fundamental groups suffices. The required actions on $\pi_1(X_{n,F_q})^{ab}$ are encoded in this group via conjugation by lifts of Frobenius and by lifts of elements of $J_C(F_{q^n})$.

Remark 3.4 Jakob Stix suggested an alternative way to deduce Theorem 3.1 from Zilber’s theorem without going through Theorem 2.5. As in the proof of Theorem 3.1, construct the map $\psi$ between the points of the respective Jacobians. To prove that $\psi$ induces a bijection between the points of the respective curves, Stix uses Tamagawa’s [11, Proposition 0.7] characterization of those sections of the fundamental exact sequence that come from rational points on the curve. He shows that the composition of a section $G_{F_q} \rightarrow \pi_1(C)$ coming from a point with the isomorphism $\pi_1(C) \rightarrow \pi_1(C')$, yields a section $G_{F_q} \rightarrow \pi_1(C')$ also coming from a point and similarly over $F_{q^n}$. Moreover, the resulting map $C(F_{q^n}) \rightarrow C'(F_{q^n})$ is compatible with the map $J_C(F_q) \rightarrow J_C'(F_q)$, at which point Zilber’s theorem applies.

Acknowledgements

The authors were supported by the Marsden Fund Council administered by the Royal Society of New Zealand. They would also like to thank Jakob Stix and the referees for many helpful comments.

Received: 11 May 2020 Accepted: 6 October 2020 Published online: 20 October 2020

References

1. Artin, E., Tate, J.: Class Field Theory. AMS Chelsea Publishing, Providence (2009). Reprinted with corrections from the 1967 original
2. Bogomolov, F., Korotiaev, M., Tschinkel, Y.: A Torelli theorem for curves over finite fields. Pure Appl. Math. Q. 6, no. 1, Special Issue: In honor of John Tate, 245–294 (2010)
3. Cornelissen, G., de Smit, B., Li, X., Marcolli, M., Smit, H.: Characterization of global fields by Dirichlet $L$-series. Res. Number Theory 5 (2019), no. 1, Art. 7, 15
4. Kohel, D.R.: Endomorphism rings of elliptic curves over finite fields, ProQuest LLC, Ann Arbor, MI, Thesis (Ph.D.), University of California, Berkeley (1996)
5. Mochizuki, S.: Absolute anabelian cuspidalizations of proper hyperbolic curves. J. Math. Kyoto Univ. 47(3), 451–539 (2007)
6. Saidi, M., Tamagawa, A.: On the anabelian geometry of hyperbolic curves over finite fields, Algebraic number theory and related topics: RIMS Kôkyûroku Bessatsu, B12, Res. Inst. Math. Sci. (RIMS), Kyoto 2009, 67–89 (2007)
7. Schmidt, F.K.: Analytische Zahlentheorie in Körperrn der Charakteristik $p$. Math. Z. 33, 1–32 (1931)
8. Serre, J.-P.: Local Fields, Graduate Texts in Mathematics, vol. 67. Springer, New York, Berlin, Translated from the French by Marvin Jay Greenberg (1979)
9. Serre, J.-P.: Algebraic Groups and Class Fields, Graduate Texts in Mathematics, vol. 117. Springer, New York (1988)
10. Sutherland, A.V., Voloch, J.F.: Maps between curves and arithmetic obstructions. preprint, arxiv:1709.05734. Proceedings of AGCT 16, AMS Contemporary Mathematics, to appear
11. Tamagawa, A.: The Grothendieck conjecture for affine curves. Compos. Math. 109(2), 135–194 (1997)
12. Uchida, K.: Isomorphisms of Galois groups of algebraic function fields. Ann. Math. 106(3), 589–598 (1977)
13. Zilber, B.: A curve and its abstract Jacobian. Int. Math. Res. Notices 5, 1425–1439 (2014)
14. Zilber, B.: A curve and its abstract Jacobian (2017). Corrected version of [Zil14], preprint, http://people.maths.ox.ac.uk/zilber/JacobianCor.pdf

Publisher’s Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.