Contemporary Mathematics
Volume **722**, 2019
https://doi.org/10.1090/conm/722/14532

Maps between curves and arithmetic obstructions

Andrew V. Sutherland and José Felipe Voloch

Abstract. Let X and Y be curves over a finite field. In this article we explore methods to determine whether there is a rational map from Y to X by considering L-functions of certain covers of X and Y and propose a specific family of covers to address the special case of determining when X and Y are isomorphic. We also discuss an application to factoring polynomials over finite fields.

1. Introduction

Given two algebraic curves X, Y of genus at least two over a finite field we would like to decide if there is a rational map from Y to X. Hess and Möhlmann [**7**, **12**] have given an algorithm to decide if such a map exists by performing an optimised search for the map up to a known bound; if the search is unsuccessful then no such map exists. This procedure works well when the map exists, but it may be very time consuming when it does not. The purpose of this paper is to investigate methods for deciding when there is no such map without performing an exhaustive search. We concentrate on the case of isomorphisms but briefly touch on the general case.

Our methods can also provide a short certificate of the non-existence of a rational map, a feature not available with existing algorithms.

A result of Poonen [**13**] extending an idea of Kayal shows that, given a one-parameter family of curves over a finite field with distinct L-polynomials for distinct values of the parameter and a suitable bound on the genus, one can construct a deterministic polynomial time algorithm for factoring polynomials over that field. Our investigations suggest some candidate families of such curves, but unfortunately we cannot prove that they work.

2. The fundamental group

Let X/K be a smooth geometrically connected variety over a field K. Let G_K be the absolute Galois group of K and $\bar{X}$ the base-change of X to an algebraic closure of K. We denote by $\pi_1(.)$ the algebraic fundamental group functor on (geometrically pointed) schemes and we omit base-points from the notation. We have the fundamental exact sequence

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to G_K \to 1. \tag{2.1}$$

2010 *Mathematics Subject Classification.* Primary 11T06, 14H25.

The map $p_X : \pi_1(X) \to G_K$ from the above sequence is obtained by functoriality from the structural morphism $X \to \operatorname{Spec} K$. Grothendieck's anabelian program is to specify a class of varieties, termed anabelian, for which the varieties and morphisms between them can be recovered from the corresponding fundamental groups together with the corresponding maps p_X when the ground field is finitely generated over $\mathbb{Q}$. There has been some work done over finite fields as well, although the anabelian program will not work in the same way (the analogue of the section conjecture is false, for example).

For the rest of the paper we restrict to the case where K is a finite field. As usual, $\mathbb{F}_q$ is the field of q elements and we denote by p its characteristic. Here is a positive result.

THEOREM 2.1. *(Mochizuki–Tamagawa) Let X, Y be smooth projective curves of genus at least two over a finite field $\mathbb{F}_q$. If there is an isomorphism from $\pi_1(X)$ to $\pi_1(Y)$ inducing the identity on $G_{\mathbb{F}_q}$ via p_X, p_Y, then X is isomorphic to Y.*

The fundamental group is a mysterious object. What kind of information can we extract from it? First of all, if J_X denotes the Jacobian of a curve X we have the fundamental exact sequence (2.1) for J_X also, and $\pi_1(\bar{J}_X)$ is the abelianisation of $\pi_1(\bar{X})$; thus the prime-to-p part of $\pi_1(\bar{J}_X)$ is the product of the Tate modules of J_X. The fundamental exact sequence describes the Galois action on the Tate module, so its description is equivalent to the L-function of X, which we can compute by counting points on X over suitable extensions of $\mathbb{F}_q$. But by the very nature of the fundamental group, we can count points on covers as well. Since knowing J_X alone up to isogeny is not enough to recover X, we need to pass to covers. According to J. Stix (personal communication) the proof of Theorem 2.1 requires only solvable covers. The most natural covers come from the Hilbert class field tower. Let $\mathrm{Fr} : J_X \to J_X$ denote the $\mathbb{F}_q$-Frobenius map. Define $H(X) := (I - \mathrm{Fr})^*(X) \subset J_X$; it is an unramified abelian cover of X with Galois group $J_X(\mathbb{F}_q)$, well defined up to a twist that corresponds to a choice of divisor of degree one embedding X into J_X. Define $H_0(X) := X$, $H_1(X) := H(X)$ and successively define $H_{n+1}(X) := H_n(H(X))$ for integers $n \geq 1$. These covers can be derived from $\pi_1(X)$ but are perhaps more computationally accessible.

CONJECTURE 2.2. *Let X, Y be smooth projective curves of genus at least two over a finite field $\mathbb{F}_q$. If, for each n, there are choices of twists such that the L-function of $H_n(X)$ is equal to the L-function of $H_n(Y)$ for all $n \geq 0$, then X is isomorphic to an $\mathbb{F}_q/\mathbb{F}_p$ conjugate of Y.*

Up to isomorphism there are exactly 8 smooth projective curves of positive genus over finite fields for which $H(X) = X$, equivalently, curves whose function fields have class number one [**10**, **16**], of which 5 have genus at least two. We have verified that Conjecture 2.2 holds when X and Y are among these 5 curves, and it therefore holds if either $H(X) = X$ or $H(Y) = Y$. We may thus assume henceforth that X and Y have non-trivial Hilbert class field towers.

The basis for our heuristic is the following consequence of the usual calculation leading to the birthday paradox. If $\mathcal{M}$ and $\mathcal{I}$ are finite sets with cardinalities M and I respectively, then for $I \preceq M^2$ the probability that a random map $\mathcal{M} \to \mathcal{I}$ is non-injective is bounded above zero, but for I asymptotically larger than M^2 this probability decays rapidly to zero. Explicitly, this probability is

$$1 - \prod_{j=0}^{M-1}(1 - j/I) \sim 1 - e^{-M(M-1)/2I}.$$

We first apply this to the set $\mathcal{M}$ of isomorphism classes of curves of some fixed genus $g > 1$ over a finite field $\mathbb{F}_q$ and the set $\mathcal{I}$ of isogeny classes of abelian varieties of dimension g over a finite field $\mathbb{F}_q$. For fixed g and large q we have $M \sim q^{3g-3}$ and $I \sim q^{g(g+1)/4}$, hence it is reasonable to expect that there will be distinct curves with isogenous Jacobians when $6g - 6 \leq g(g+1)/4$, that is, $g \leq 22$ (see [**3**] and [**15**] where this kind of question is discussed in more detail). For larger genus one expects this to be very rare, but we note a result of Mestre [**11**] that allows one to construct, for every $g > 1$, pairs of non-isomorphic genus g curves with isogenous Jacobians (over sufficiently large finite fields).

Provided $H(X) \neq X$ (as we now assume), passing from X to $H(X)$ increases the genus and thus makes it more likely that we can use isogeny invariants to distinguish non-isomorphic curves. For large q and g, the genus of $H(X)$ is much larger than the genus g of X; indeed, it is on the order of gq^g. However, the Jacobian of $H(X)$ is not an arbitrary abelian variety of this dimension; it decomposes up to isogeny as a product of abelian varieties of smaller dimension. The precise shape of the decomposition depends on the group structure of $J(\mathbb{F}_q)$ but it falls into a small set of possibilities. Thus, given its huge dimension, barring any additional constraints, the isogeny class of the Jacobian of $H(X)$ still varies in a huge space. So, on probabilistic grounds, it is still likely that the map $X \mapsto L(H(X), T)$ is injective when g and q are large. This makes it plausible that, up to a finite set of exceptions, Conjecture 2.2 holds even when we restrict to $n \leq 1$. The set of exceptions is non-empty as the examples in the next section show.

In addition to $H(X)$, we can also consider the cover of X obtained by pulling back via multiplication by 2 on the Jacobian (assuming the characteristic is not 2). This gives a cover of X of degree 2^{2g}. Note that, over the ground field this cover is not abelian, but it is abelian after base change to the algebraic closure. In general, this cover is not a subcover of the $H_n(X)$ considered above. Its Jacobian $J_{X^{(2)}}$ is not a random abelian variety of its dimension, since it decomposes (after base change to the algebraic closure of the ground field) up to isogeny into a product of the Jacobian J_X of X and $2^{2g} - 1$ abelian varieties of dimension $g - 1$, the Prym varieties of X. Typically, these Prym varieties are not defined over the ground field, only those coming from the rational 2-torsion of the Jacobian are. Even in the case of full rational 2-torsion, if we assume that the isogeny classes of these factors are random, we are picking them out of a set of size $\sim q^{(2^{2g}-1)g(g-1)/4}$ which is much smaller than if we regarded $J_{X^{(2)}}$ as random, but still very large. If we iterate this construction, as we did with $H(X)$, we quickly reach a point where the corresponding 2-torsion is not rational, hence this construction gives information which is different from what comes from $H(X)$ and its iterates. On the other hand we should note that the construction of Mestre [**11**] mentioned above produces curves that not only have isogenous Jacobians, but a few of their Prym varieties (which are defined over the ground field) will also be isogenous.

Everett Howe provided us with the following family of examples:

$$X(t)\colon y^2 = (x^3 - 1/t^3)(x^3 - t^3).$$

This is a one parameter family of genus 2 curves with geometrically split Jacobians having full rational 2-torsion over $\mathbb{F}_q$ for $q \equiv 1 \bmod 3$. Among elements of this family, for many values of q one can find distinct values of t for which the curves $X(t)$ are geometrically non-isomorphic and the L-functions of $X^{(2)}(t)$ coincide (as do those of $X(t)$). For example, one can take $t = 3, 13$ in $\mathbb{F}_{97}$, or $t = 3, 11$ in $\mathbb{F}_{127}$.

Similar examples can be obtained using

$$X(t)\colon y^2 = x(x-1)(x-t)(x-1/(1-t))(x-(t-1)/t)$$

over any finite field $\mathbb{F}_q$. Here one can take $t = 4, 5$ in $\mathbb{F}_{31}$, or $t = 4, 13$ or $t = 6, 12$ in $\mathbb{F}_{41}$, for example. The fact that these curves have split Jacobian increases the chances of instances where the L-functions of $X^{(2)}(t)$ coincide. In our computations of these examples, we noticed that these coincidences were more common than expected. We do not have an explanation for this. But we have not found any examples of genus larger than two.

QUESTION 2.3. *Are there non-isomorphic curves X, Y over $\mathbb{F}_q$ of genus at least three and $p \neq 2$ with $J_{X^{(2)}}, J_{Y^{(2)}}$ isogenous?*

For maps between curves of different genera, it is less clear what to expect. In particular, we do not have a result generalizing Theorem 2.1. But one can consider the following:

QUESTION 2.4. *Let X, Y be smooth projective curves of genus at least two over a finite field $\mathbb{F}_q$, with $H(X) \neq X$ and $H(Y) \neq Y$. Suppose the L-function of $H_n(X)$ divides the L-function of $H_n(Y)$ for all $n \geq 0$. Does this imply the existence of a dominant map $Y \to X$?*

As shown by an example of Brendan Creutz, the answer to Question 2.4 is no if we allow $H(X) = X$. A generalization of his idea (which is the case $n = 0$) is as follows. Start with X such that $X(\mathbb{F}_q) = \emptyset$. Consider the Jacobian J of $H_n(X)$ and by slicing with suitable hypersurfaces, construct a smooth curve $D \subset J$ with $0 \in D$, hence in particular $D(\mathbb{F}_q) \neq \emptyset$. This D cannot map to X (as $X(\mathbb{F}_q) = \emptyset$) but $L(H_n(X), T) | L(D, T) | L(H_n(D), T)$ by construction. So the n in Question 2.4 cannot be uniformly bounded.

3. Certifying non-isomorphism

If two curves can be distinguished by the L-polynomials of low degree covers then a succinct certificate can be given in the form of a prime ℓ for which the corresponding two L-polynomials are distinct modulo ℓ, together with the calculation of these polynomials; note that we can assume $\ell = O(g \log q)$, since otherwise the L-polynomials must coincide. For fixed g the Schoof-Pila algorithm can be used to determine ℓ and compute the L-polynomials modulo ℓ with a running time that is polynomial in $\log q$, but exponential in g. When g is large relative to $\log p$, where p is the characteristic of $\mathbb{F}_q$, one is better off using algorithms based on p-adic cohomology to compute the L-polynomials over $\mathbb{Z}$ and then reduce modulo a suitable prime ℓ. The complexity of the p-adic approach is polynomial in g but exponential in $\log p$. The most general algorithm of this type is due to Tuitman [**17**], and is applicable to all curves that admit a suitable lift to characteristic zero; its complexity is quasi-linear in p and polynomial in g. When $q = p$ is prime one can instead apply Harvey's result for arithmetic schemes [**4**], which improves the dependence on p to $O(p^{1/2+o(1)})$. At present there is no algorithm known with a running time that is polynomial in both g and $\log q$, thus in general, it may be costly to verify this certificate. But typically the degrees of the covers and the value of ℓ will be quite small (much smaller than $g \log q$), in which case computing the L-polynomials modulo ℓ (or even just enough terms to distinguish them) may be feasible.

4. Examples

The simplest case to consider in Conjecture 2.2 is when $g = 2$ and $q = 2$; in this case there are 20 isomorphism classes of curves, all of which have distinct L-functions, so one could take $n = 0$ in Conjecture 2.2. The next simplest case is $g = 2$ and $q = 3$; now there are 69 isomorphism classes of curves, but only 50 isogeny classes of Jacobians. Of the 50 isogeny classes of Jacobians, 31 contain a unique Jacobian, while 19 contain a pair of Jacobians of non-isomorphic curves. Among these 19 all but 4 pairs are distinguished by considering the L-functions of $H_1(X)$. These 4 pairs are considered in the first 3 examples below, each of which demonstrates that Conjecture 2.2 does not hold if we restrict to $n \leq 1$.

Example 4.1. The genus two curves:

$$C_1 \colon y^2 = 2x^6 + 2x^4 + 2x^3 + 2, \qquad C_2 \colon y^2 = 2x^6 + 2x^5 + x^4 + x^2 + 2x + 2$$

over $\mathbb{F}_3$ are non-isomorphic, but they have isogenous Jacobians J_1, J_2 with L-polynomial:

$$9T^4 - 6T^3 + 3T^2 - 2T + 1.$$

The corresponding Hilbert class fields have degree $\#J_1(\mathbb{F}_3) = \#J_2(\mathbb{F}_3) = 5$, and the Riemann-Hurwitz theorem implies that the curves $H_1(C_1)$, $H_1(C_2)$ both have genus 6. The function fields of $H_1(C_1)$ and $H_1(C_2)$ both have exactly the same number of degree $1, 2, 3, 4, 5, 6$ places (the counts are $5, 0, 10, 15, 60, 140$, respectively, as computed using the function `NumberOfPlacesOfDegree`, which is implemented in Magma [**1**], along with the function `HilbertClassField` which we used to compute $H_1(C_1)$ and $H_1(C_2)$), which implies that their L-polynomials coincide. The computation of $H_2(C_i)$ seems out of reach so we cannot verify whether these distinguish the two curves. Instead we look at 2-power covers in the setting of Question 2.3.

The polynomial $f_1(x)$ in the equation $y^2 = f_1(x)$ for C_1 is irreducible over $\mathbb{F}_3$, while the polynomial $f_2(x)$ in the equation $y^2 = f_2(x)$ for C_2 splits into irreducible cubic factors; this implies that the Jacobian J_2 has full 2-torsion over $\mathbb{F}_{27}$, while J_1 does not. This is already enough to show that the two Jacobians J_1 and J_2 (and therefore the curves C_1 and C_2) are non-isomorphic, but this does not immediately fit our approach of computing L-polynomials.

However, by taking double covers over $\mathbb{F}_{27}$ and looking at the corresponding elliptic curves, (see Example 4.5 below for a similar calculation), we get elliptic curves with 2-torsion for the second genus 2 curve but not for the first, so the isomorphism classes of C_1 and C_2 are distinguished by the L-functions of these double covers.

Example 4.2. The genus two curves:

$$C_1 \colon y^2 = x^5 + x^4 + 2x + 1, \qquad C_2 \colon y^2 = x^5 + x^3 + x^2 + 2x + 2$$

over $\mathbb{F}_3$ both have L-polynomial $L(T) = 9T^4 - 3T^3 + T^2 - T + 1$, and the curves $H_1(C_1)$, $H_1(C_2)$ of genus 8 also have equal L-polynomials.

This example is particularly interesting, in that the corresponding Jacobians J_1 and J_2 are isomorphic; indeed, after a linear change of variable this is precisely the example given by Howe in [**8**].

As in the previous example, verifying Conjecture 2.2 seems to be computationally out of reach, but we can distinguish them by taking double covers. We need

to work over $\mathbb{F}_{3^5}$ and each curve has 15 étale double covers lying in 3 orbits of 5 curves under Frobenius. The Jacobians of the double covers have an additional elliptic curve factor and we get, as trace of Frobenius for these factors, the values (up to sign) of: $28, 28, 8$ for the first curve and $28, 20, 8$ for the second. The appearance of the 20 shows these elliptic curve factors are not isogenous, so the curves are not isomorphic.

A similar example is the pair of curves $C_1\colon y^2 = 2x^6+x^4+x^3+1$ and $C_2\colon y^2 = x^6+x^4+x^3+2$ over $\mathbb{F}_3$, with L-polynomial $L(T) = 9T^4-3T^3+3T^2-T+1$. Traces of Frobenius for the elliptic curve factors are $4, 16, 28$ for first curve and $4, 4, 16$ for the second.

Example 4.3. The fourth and final example for $g = 2$ and $q = 3$ is the pair of curves

$$C_1\colon y^2 = x^5 - 1, \qquad C_2\colon y^2 = x^5 + 1,$$

which are non-isomorphic quadratic twists. Their Jacobians are both supersingular with L-polynomial $9T^4+1$, and the genus 11 curves $H_1(C_1)$, $H_1(C_2)$ have the same L-polynomial.

The curves C_1 and C_2 both have 4 points over $\mathbb{F}_3$ and admit a unique (up to twist) unramified double cover. We pin down the double cover by insisting that it have 6 points over $\mathbb{F}_3$ (the other twist has 2 points). Then we look at an unramified triple cover of the double cover, of which there are three, all twists of each other. Finally, we see how the 6 points split on these covers and use this information to distinguish the curves.

We have double covers $X_1\colon w^2 = x^4+x^3+x^2+x+1$ and $X_2\colon w^2 = x^4-x^3+x^2-x+1$ of C_1 and C_2 respectively. Here and below, we just present the equation defining the cover, so the full equation of the curve includes the previous equations as well. The polynomials in x defining the covers are factors of the corresponding polynomials in the definition of the curves, as required to get unramified covers. To get the triple covers below we follow the classical method of Hasse and Witt.

Triple covers of X_1 are given by $Y_{1,a}: z^3 - z = (x+1)w + a$, for $a = 0, 1, 2$.

Triple covers of X_2 are given by $Y_{2,a}: z^3 - z = (x-1)w + a$, for $a = 0, 1, 2$.

The distinguishing feature is that while all the $Y_{1,a}$ have $\mathbb{F}_3$-points $(12, 3, 3,$ respectively), $Y_{2,0}$ is pointless (the curves $Y_{2,1}$ and $Y_{2,2}$ both have 9 $\mathbb{F}_3$-points). This implies that the L-polynomials of $H_2(C_1)$, $H_2(C_2)$ differ and confirms Conjecture 2.2 in this case.

Example 4.4. We did an exhaustive search over $\mathbb{F}_2$ and found that there is exactly one pair of non-isomorphic smooth plane quartics C_1, C_2 over $\mathbb{F}_2$ with the same L-polynomial for which $H_1(C_1), H_1(C_2)$ also have the same L-polynomial:

$$C_1\colon x^3z + xyz^2 + y^4 + y^2z^2 + yz^3, \qquad C_2\colon x^3z + xy^2z + y^4 + y^2z^2 + yz^3.$$

Both curves have L-polynomial $8T^6 - 4T^5 + 2T^3 - T + 1$, with 6 rational points on their Jacobians, and the Hilbert class curves $H_1(C_1)$, $H_1(C_2)$ have genus 13.

The curves C_1, C_2 both have a unique (up to twist) quadratic unramified cover, say D_1, D_2 of genus 5. By the Deuring-Shafarevich formula, D_1, D_2 themselves have a unique (up to twist) quadratic unramified cover, and they have distinct L-polynomials, even up to quartic twists, which is enough to show C_1, C_2 are non-isomorphic and distinguished by the L-polynomials of $H_2(C_1)$, $H_2(C_2)$, confirming Conjecture 2.2 for this example.

EXAMPLE 4.5. Another example is the pair of genus two curves

$$C_1\colon y^2 = x^6 + 3x^2 + 4, \qquad C_2\colon y^2 = x^6 + 5x^4 + 5x^2 + 1$$

over $\mathbb{F}_7$, which have the same L-function. To show that they are not isomorphic one can look at the respective double covers and show, by counting points, that there cannot be a matching between the double covers of the two curves. Specifically, both curves have three unramified double covers defined over $\mathbb{F}_7$. The Jacobians of these covers split as the product of the Jacobian of the original curve with an additional elliptic curve. For the first curve, all three of these elliptic curves have trace of Frobenius -4. For the second curve, the elliptic curve obtained from the cover $z^2 = x^2 + 1$ has trace of Frobenius 0.

5. Factoring polynomials over finite fields

As mentioned in the introduction, the existence of a one-parameter family X_t of curves of genus g over $\mathbb{F}_p(t)$ with g bounded (or growing very slowly with p) such that the L-polynomials $L(X_t, T)$ are all distinct (or the number of collisions is bounded independent of p) for varying $t \in \mathbb{F}_p$ (excluding the t of bad reduction, those for which X_t is singular) leads to a deterministic polynomial-time algorithm for factoring polynomials in $\mathbb{F}_p[t]$. There are well-known randomized algorithms to solve this problem whose expected running times are polynomially-bounded that are quite fast in practice, so this question is primarily of theoretical interest. But even for polynomials of degree two, no deterministic polynomial-time algorithm is known, unless one assumes the Generalized Riemann Hypothesis (GRH), and for general polynomials the question remains open even under GRH.

Using the same heuristic as in section 2.1, there are p choices of t and $p^{g(g+1)/4}$ possible values for the L-polynomial so one would expect this to hold for "most" families as soon as $g > 2$, since $p^2 < p^{g(g+1)/4}$. Buium [**2**] has shown that most families (in a differential algebraic sense) in characteristic zero have finitely many isogeny correspondences, however, even if this result extends to characteristic p, it does not rule out sporadic isogenies. Conjecture 2.2 does not give the result either, as the genus of the resulting covers grows too quickly.

We first considered the family $y^2 = x^7 + (t-1)x^3 + tx^2 + (t+1)x + 1$ of curves of genus 3. One expects the number of isogeny classes of 3-dimensional abelian varieties over $\mathbb{F}_p$ to be about p^3. So under our probabilistic heuristic, a one parameter family of curves (with about p elements) has a probability of about $1/(2p)$ of containing isogenous Jacobians. Using the algorithms in [**5**, **6**, **9**] we have verified that for all primes $p \leq 10000$ the L-polynomials in this family are distinct for all t of good reduction (for each p, at most 9 values of $t \in \mathbb{F}_p$ yield singular curves). Now $\sum 1/(2p) = O(\log\log p)$ diverges (albeit slowly), so one might expect a collision of L-polynomials to occur in this family for some $p > 10^5$ (but one would expect the number of collisions for each p to be bounded by a constant).

To obtain a more compelling example, we instead consider the genus 4 hyperelliptic family:

$$X_t\colon y^2 = x^9 + (t-1)x^3 + tx^2 + (t+1)x + 1.$$

Now the number of isogeny classes is on the order of p^5, and our heuristic model predicts a probability of roughly $1/(2p^3)$ that two L-polynomials $L(X_t, T)$ in our family coincide for some pair of $t \in \mathbb{F}_p$. The sum $\sum 1/(2p^3)$ now converges.

We have verified that for primes $p \le 2^{17}$ the L-polynomials arising in this family are distinct for all t of good reduction (now at most 11 values of $t \in \mathbb{F}_p$ yield singular X_t), and it seems quite likely that the L-polynomials $L(X_t, T)$ arising in the family are distinct for all primes p. Indeed, if $\pi(t) = t/\log(t) + \varepsilon(t)$ denotes the prime counting function, we can bound the tail of our sum $\sum 1/(2p^3)$ using

$$\sum_{p>2^{17}} \frac{1}{2p^3} = \int_{2^{17}}^{\infty} \frac{d\pi(t)}{2t^3} = \int_{2^{17}}^{\infty} \frac{dt}{2t^3 \log t} + \frac{\varepsilon(t)}{2t^3}\Big|_{2^{17}}^{\infty} + \int_{2^{17}}^{\infty} \frac{3\varepsilon(t)dt}{2t^4},$$

and applying the bound $\varepsilon(t) \le (3t)/(2\log(t)^2)$ (valid for $t \ge 59$) from [**14**] yields

$$\sum_{p>2^{17}} \frac{1}{2p^3} < 1.187 \times 10^{-12} + 4.36 \times 10^{-13} + 3.15 \times 10^{-13} < 2 \times 10^{-12}.$$

Thus under our heuristic model, the probability that the L-polynomials $L(X_t, T)$ at good values of t are not all distinct for every prime p is less than 2×10^{-12}.

These two families were chosen essentially at random by writing a plausible family with no specializations having the same L-polynomial for small primes. We note that the similar looking families $y^2 = x^7 + (t-1)x^3 + (t+1)x + 1, y^2 = x^9 + (t-1)x^3 + (t+1)x + 1$ have specializations with the same L-polynomial for some small primes.

Acknowledgements: Both authors would like to thank Kiran Kedlaya for mentioning the results of [**13**] at AGCT, and Bjorn Poonen for writing up that account at our instigation, as well as Brendan Creutz, Noam Elkies, and Jakob Stix for helpful discussions, and the organizers of AGCT. We also thank Everett Howe for his feedback on an early draft of this article. The first author thanks the National Science Foundation for financial support under grant DMS-152256 and the Simons Foundation for financial support under grant #550033, and the second author thanks the Simons Foundation for financial support under grant #234591 .

References

[1] W. Bosma, J.J. Cannon, C. Fieker, and A. Steel (Eds.), *Handbook of Magma functions*, v2.23, 2017. 171

[2] A. Buium, *A finiteness theorem for isogeny correspondences*, Astérisque **218** (1993), 35–60. Journées de Géométrie Algébrique d'Orsay (Orsay, 1992). MR1265308 ↑173

[3] S. A. DiPippo and E. W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory **73** (1998), no. 2, 426–450, DOI 10.1006/jnth.1998.2302. MR1657992 ↑169

[4] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 6, 1379–1401, DOI 10.1112/plms/pdv056. MR3447797 ↑170

[5] D. Harvey and A. V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273, DOI 10.1112/S1461157014000187. MR3240808 ↑173

[6] D. Harvey and A. V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147, DOI 10.1090/conm/663/13352. MR3502941 ↑173

[7] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 263–271, DOI 10.1007/978-3-540-24847-7_19. MR2137359 ↑167

[8] E. W. Howe, *Constructing distinct curves with isomorphic Jacobians*, J. Number Theory **56** (1996), no. 2, 381–390, DOI 10.1006/jnth.1996.0026. MR1373560 ↑171

[9] K. S. Kedlaya and A. V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 312–326, DOI 10.1007/978-3-540-79456-1_21. MR2467855 ↑173
[10] P. Mercuri and C. Stirpe, *Classification of algebraic function fields with class number one*, J. Number Theory **154** (2015), 365–374, DOI 10.1016/j.jnt.2015.02.008. MR3339577 ↑168
[11] J.-F. Mestre, *Couples de jacobiennes isogènes de courbes hyperelliptiques de genre arbitraire* arxiv 0902.3470 169
[12] G. Möhlmann, *Einbettungen globaler Funktionenkörper* Diplomarbeit TU Berlin 2008 167
[13] B. Poonen, *Using zeta functions to factor polynomials over finite fields*, Arithmetic Geometry: Computation and Applications, Contemp. Math., vol. 722, Amer. Math. Soc., Providence, RI, 2019. 167, 174
[14] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR0137689 ↑174
[15] A. S. Shankar and J. Tsimerman, *Unlikely intersections in finite characteristic* arxiv 1610.03552 169
[16] Q. Shen and S. Shi, *Function fields of class number one*, J. Number Theory **154** (2015), 375–379, DOI 10.1016/j.jnt.2015.02.005. MR3339578 ↑168
[17] J. Tuitman, *Counting points on curves using a map to* $\mathbf{P}^1$*, II*, Finite Fields Appl. **45** (2017), 301–322, DOI 10.1016/j.ffa.2016.12.008. MR3631366 ↑170

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139
Email address: drew@math.mit.edu
URL: http://math.mit.edu/~drew

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand
Email address: felipe.voloch@canterbury.ac.nz
URL: http://www.math.canterbury.ac.nz/~f.voloch