Experimental Mathematics, 21(4):362–374, 2012

ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2012.671638

Taylor & Francis
Taylor & Francis Group

Experimental Data for Goldfeld's Conjecture over Function Fields

Salman Baig and Chris Hall

CONTENTS

This paper presents empirical evidence supporting Goldfeld's conjecture on the average analytic rank of a family of quadratic twists of a fixed elliptic curve in the function field setting. In particular, we consider representatives of the four classes of nonisogenous elliptic curves over $\mathbb{F}_q(t)$ with $(q, 6) = 1$ possessing two places of multiplicative reduction and one place of additive reduction. The case of $q = 5$ provides the largest data set as well as the most convincing evidence that the average analytic rank converges to $1/2$, which we also show is a lower bound following an argument of Kowalski. The data were generated via explicit computation of the L-function of these elliptic curves, and we present the key results necessary to implement an algorithm to efficiently compute the L-function of nonisotrivial elliptic curves over $\mathbb{F}_q(t)$ by realizing such a curve as a quadratic twist of a pullback of a "versal" elliptic curve. We also provide a reference for our open-source library ELLFF, which provides all the necessary functionality to compute such L-functions, and additional data on analytic rank distributions as they pertain to the density conjecture.

1. INTRODUCTION

Goldfeld's conjecture, in its original form, makes an assertion about a family of elliptic curves over a number field and some form of rank. For example, if we fix an elliptic curve $E/\mathbb{Q}$ and consider the set of its quadratic twists ordered by (increasing) discriminant of the twisting fields, then the conjecture asserts that the average rank of the first n curves tends to the limit $1/2$ as n tends to infinity. Recently, it was proved in [Bhargava and Shankar, forthcoming] that the average rank, if it exists, is less than 1.17, and in particular, a positive proportion of elliptic curves over $\mathbb{Q}$ have rank zero. This is essentially the best result we have thus far toward Golfdeld's conjecture over number fields.

In this paper, we will fix the rational function field $K = \mathbb{F}_q(t)$ as our base field and consider families of elliptic curves over K for which we can calculate each family member's analytic rank. Little theoretical progress has

2000 AMS Subject Classification: 11G05, 11G40, 11Y16, 11-04
Keywords: elliptic curves, function fields, L-functions, rank, Goldfeld's conjecture, Sage, ELLFF

been made when we consider the average rank of an "increasing" sequence of curves, and the genesis of this paper lies in a computational project to generate a rich data set of L-functions for studying the (empirical) averages.

In the bulk of this paper we focus on some algorithms of increasing complexity for explicitly calculating the L-function $L(E/K, s)$ for an elliptic curve E/K; the increasing complexity allows for increased speed but at the cost of increasing the disk and memory space requirements. In contrast to L-functions over number fields, these L-functions have the remarkable property that if we define a new variable T by $T = q^{-s}$, then we can represent the L-function as a polynomial $L(E/K, T) \in 1 + T \cdot \mathbb{Z}[T]$. The analytic rank of E/K is simply the order of vanishing at $s = 1$ $(T = 1/q)$, and hence the analytic Goldfeld's conjecture requires only a minuscule amount of the information present in each L-function.[1] However, there are many other questions one can ask about how $L(E/K, T)$ varies with E/K, so we hope that our database and algorithms will prove useful for others.

For the calculation of a single L-function, one can use the theory outlined in the first two subsections of Section 2. We follow the usual approach for calculating the L-function by expressing it as an Euler product; the terms of the product are indexed by valuations in K, i.e., by monic irreducibles in the polynomial ring $\mathbb{F}_q[t]$ and a point at infinity. The Euler product is infinite, but there is a finite collection of Euler factors that completely determine $L(E/K, T)$. To compute the L-function as efficiently as possible (in this approach), we want to minimize the size of this collection (e.g., by using a functional equation) and the cost of computing a single Euler factor.

Those who have experience computing quadratic twists know that the cost of computing an Euler factor for a twist is much cheaper if one knows the Euler factor for the original curve, the work being reduced to computing a Legendre symbol. A similar efficiency emerges when we consider pullbacks, i.e., when we replace K with a finite extension L/K: almost all of the Euler factors for $L(E/L, T)$ can be cheaply calculated from the Euler factors of $L(E/K, T)$. In fact, for each q, there is an elliptic curve E_0 over $F = \mathbb{F}_q(j)$ such that every E/K may be written as the combination of a pullback of E_0 to K (via the embedding $F \to K$ induced by $j \mapsto j(E)$) and a twist (by quadratic L/K). In particular, the Euler factors for $L(E/K, T)$ may be cheaply computed from the Euler factors of $L(E_0/F, T)$, and the second half of Section 2 explains this in detail.

The upshot is that whenever we construct a new curve E/K as a pullback or twist of another curve E_0/F, then the additional cost of computing $L(E/K, T)$ using a precomputed table of sufficiently many Euler factors for $L(E_0/F, T)$ is much cheaper than if we computed $L(E/K, T)$ from scratch. We have written a library for calculating L-functions whose core routines use the methods we outline in Section 2, and recently, we provided the wrapper routines for it to be used within Sage.[2] The library is called ELLFF (for elliptic L-functions over function fields), and we describe its basic structure in Section 3. We used our code to gather data to empirically study Goldfeld's conjecture in the function field setting, and we report a summary of these data and observations in Section 4.

2. THEORETICAL FRAMEWORK

2.1. Elliptic Curves

Fix a prime power q relatively prime to 6. Let $K = \mathbb{F}_q(t)$ be the function field of the curve $\mathbb{P}^1/\mathbb{F}_q$, $\mathcal{O}_K = \mathbb{F}_q[t]$ the affine coordinate ring of $\mathbb{P}^1 - \{\infty\}$, $\mathcal{O}_\infty = \mathbb{F}_q[u]$ the affine coordinate ring of $\mathbb{P}^1 - \{0\}$, and $u = 1/t \in K$. We identify the set of closed points $|\mathbb{P}^1| = \{\pi\}$ with the set formed by the closed point $\pi = \infty$ together with the monic irreducibles $\pi \in \mathbb{F}_q[t]$ of positive degree, and we write $\mathbb{F}_\pi$ for the residue field. For $\pi = \infty$ we identify $\mathbb{F}_\pi$ with the quotient field $\mathbb{F}_q[u]/u$, and otherwise we identify $\mathbb{F}_\pi$ with the quotient field $\mathbb{F}_q[t]/\pi$.

Let E/K be an elliptic curve. Up to a change of coordinates, we may represent our elliptic curve as the projective plane curve given by the affine curve $y^2 = x^3 + ax + b$, where $a, b \in K$, together with the point at infinity. The discriminant $\Delta = 4a^3 + 27b^2$ and j-invariant $j = 6912a^3/\Delta$ are rational functions in t, i.e., elements of K, and $\Delta \neq 0$.

Up to a change of coordinates $(x, y) \mapsto (x/g^2, y/g^3)$ with $g \in K^\times$, we may assume that $a, b \in \mathcal{O}_K$ and that $\deg_t(\Delta)$ is minimal, because $\mathcal{O}_K$ is a principal ideal domain, and we write $\Delta_\pi = \Delta$ for $\pi \neq \infty$. There is a unique integer e such that the substitution $(t, x, y) \mapsto (1/u, x/u^{2e}, y/u^{3e})$ yields a model of E over $\mathbb{F}_q[u]$ satisfying similar conditions, and we write Δ_∞ for the

[1] The Birch–Swinnerton-Dyer conjecture asserts that the algebraic (Mordell–Weil) and analytic ranks are the same, so someone who likes looking for points may want to comb our database for curves of rank preferably at least two and try their hand at producing points.

[2] Available at http://www.sagemath.org.

discriminant of this model. We glue the two models together over the annulus $\mathbb{P}^1 - \{0, \infty\}$ to form the so-called minimal Weierstrass model $\mathcal{E} \to \mathbb{P}^1$; it is the identity component of the so-called Néron model of E.

For each π, we write $\mathcal{E}/\mathbb{F}_\pi$ for the fiber of $\mathcal{E} \to \mathbb{P}^1$ over π. If $\pi \neq \infty$, then it is the projective plane curve given by "reducing modulo π" the model for E over $\mathcal{O}_K$, while for $\pi = \infty$, we use the model for E over $\mathbb{F}_q[u]$. Then $\mathcal{E}/\mathbb{F}_\pi$ is a smooth curve if and only if the image of Δ_π in $\mathbb{F}_\pi$ is nonzero; otherwise, it has a unique singular point. We write M for the finite subset of π such that $\mathcal{E}/\mathbb{F}_\pi$ is singular with a node, A for the finite subset such that $\mathcal{E}/\mathbb{F}_\pi$ is singular with a cusp, and U for the open complement $\mathbb{P}^1 - M - A$; they are the loci of multiplicative, additive, and good reduction respectively of $\mathcal{E} \to \mathbb{P}^1$. We recall that if $\pi \neq \infty \in M \cup A$, then $\pi \in M$ if and only if the image of b in $\mathbb{F}_\pi$ is nonzero, and a similar criterion holds if $\pi = \infty \in M \cup A$.

We decompose M into the subset M^+ of π for which the slopes of the two branches through the node of $\mathcal{E}/\mathbb{F}_\pi$ are rational over $\mathbb{F}_\pi$ and the subset M^- for the complement $M - M^+$; they are the loci of split and nonsplit reduction respectively. The following lemma gives a criterion for deciding whether a given $\pi \neq \infty \in M$ lies in M^+ or M^-, while for $\pi = \infty$, one can use the model for E over $\mathbb{F}_q[u]$ to deduce a similar criterion.

Lemma 2.1. *If $\pi \neq \infty \in M$, then $\pi \in M^+$ if and only if the image of $6b$ in $\mathbb{F}_\pi$ is a square.*

Proof. Over $\mathbb{F}_\pi$, our affine model specializes to

$$y^2 = (x-c)^2(x+2c)$$

for some $c \neq 0 \in \overline{\mathbb{F}}_\pi$, and the node lies at $(x, y) = (c, 0)$. The substitution $y = s \cdot (x - c)$ and cancellation of $(x - c)^2$ leads to the curve $s^2 = x + 2c$, the blowup of our original curve at the node. The slopes of the two branches are the s-coordinates of the points $(x, s) = (c, s)$ that lie on this curve, whence $s = \pm\sqrt{3c}$. In particular, the slopes are rational over $\mathbb{F}_\pi$ if and only if $3c$ is a square in $\mathbb{F}_\pi$. In terms of the singular model, we see that the image of b in $\mathbb{F}_\pi$ is $2c^3$, whence $3c$ is a square in $\mathbb{F}_\pi$ if and only if $6b = 3c \cdot (2c)^2$ is. □

In the first three lines of Table 1, produced using [Silverman 86, Table 15.1], we give criteria for determining the type of additive reduction E has over $\pi \in A$. In the last line of the table we define a constant ϵ_π, which will be used in the next section.

Kodaira symbol	I_n^*	I_0^*	II	IV	IV*	II*	III	III*
$\mathrm{ord}_\pi(\Delta_\pi)$	$6+n$	6	2	4	8	10	3	9
$j \pmod{\pi}$	∞	$\not\equiv \infty$	0	0	0	0	1728	1728
ϵ_π	-1	-1	-1	-3	-3	-1	-2	-2

TABLE 1. Additive reduction information for E/K.

2.2. *L*-Functions

We keep the notation of the previous section and add the assumption that j is nonconstant, i.e., that it lies in the complement $K - \mathbb{F}_q$, and we remark that most of what follows extends to the case that Δ (but not necessarily j) is nonconstant.

For each $\pi \in |U|$ and $m \geq 1$, we write $\mathbb{F}_{\pi^m}$ for the unique extension of $\mathbb{F}_\pi$ of degree m, $\mathcal{E}(\mathbb{F}_{\pi^m})$ for the set of $\mathbb{F}_{\pi^m}$-rational points of $\mathcal{E}/\mathbb{F}_\pi$, and

$$a_{\pi^m} = q^{m \deg(\pi)} + 1 - \#\mathcal{E}(\mathbb{F}_{\pi^m}).$$

For each $\pi \in |U|$, the zeta function of $\mathcal{E}/\mathbb{F}_\pi$ is given by the exponential generating series

$$Z(T, \mathcal{E}/\mathbb{F}_\pi) = \exp\left(\sum_{m=1}^{\infty} \#\mathcal{E}(\mathbb{F}_{\pi^m}) \frac{T^m}{m}\right). \tag{2–1}$$

It is a rational function in $\mathbb{Q}(T)$ with denominator

$$(1-T)(1-q^{\deg(\pi)}T)$$

and numerator

$$L(T, \mathcal{E}/\mathbb{F}_\pi) = 1 - a_{\pi^1}T + q^{\deg(\pi)}T^2.$$

Because we assumed that j is nonconstant, the L-function $L(T, E/K)$ is a polynomial in $\mathbb{Z}[T]$ with constant coefficient 1 (cf. [Katz 02, bottom of p. 11]) and satisfies

$$\deg(L(T, E/K)) = \deg(M) + 2\deg(A) - 4.$$

It has an Euler product expansion

$$L(T, E/K) = \prod_{\pi \in |U|} L(T^{\deg(\pi)}, \mathcal{E}/\mathbb{F}_\pi)^{-1} \tag{2–2}$$
$$\times \prod_{\pi \in M^+} (1 - T^{\deg(\pi)})^{-1} \prod_{\pi \in M^-} (1 + T^{\deg(\pi)})^{-1}.$$

Using (2–1) and the formal identity

$$\frac{1}{1-\alpha T} = \exp\left(\sum_{n=1}^{\infty} (\alpha T)^n / n\right),$$

it is easy to show that

$$L(T^{\deg(\pi)}, \mathcal{E}/\mathbb{F}_\pi) = \exp\left(\sum_{n\geq 1, \deg(\pi)|n} \deg(\pi)\cdot a_{\pi^{n/\deg(\pi)}} \frac{T^n}{n}\right).$$

Therefore, if we define

$$b_n = \sum_{\substack{\pi\in|U|\\ \deg(\pi)|n}} \deg(\pi)\cdot a_{\pi^{n/\deg(\pi)}} + \sum_{\substack{\pi\in M^+\\ \deg(\pi)|n}} \deg(\pi) + \sum_{\substack{\pi\in M^-\\ \deg(\pi)|n}} \deg(\pi)(-1)^{n/\deg(\pi)},$$

then we can rewrite (2–2) as

$$L(T, E/K) = \exp\left(\sum_{n=1}^{\infty} b_n \frac{T^n}{n}\right). \tag{2–3}$$

If we truncate the formal series expansion of the right side of (2–3) by reducing modulo T^{N+1} for $N \geq 0$, then we obtain the congruence

$$L(T, E/K) \equiv \exp\left(\sum_{n=1}^{N} b_n \frac{T^n}{n}\right) \pmod{T^{N+1}}. \tag{2–4}$$

Thus $L(T, E/K) \pmod{T^{N+1}}$ is completely determined by $\{b_n : 1 \leq n \leq N\}$ for $N = \deg(L(T, E/K))$, and by definition, this set is determined by the Euler factors over $\pi \in |\mathbb{P}^1|$ satisfying $\deg(\pi) \leq N$. In fact, by taking the functional equation into consideration, as described below, it suffices to take $N = \lfloor \deg(L(T, E/K))/2 \rfloor$.

If we write

$$L(T, E/K) = \sum_{n=0}^{N} c_n T^n \quad \text{for} \quad N = \deg(L(T, E/K)),$$

then to recover $c_0, \ldots, c_N$ from (2–4), it suffices to apply the following lemma.

Lemma 2.2. *If $\{c_0 = 1\} \cup \{b_n, c_n : 1 \leq n \leq N\}$ are numbers satisfying*

$$\exp\left(\sum_{n=1}^{N} b_n \frac{T^n}{n}\right) \equiv \sum_{n=0}^{N} c_n T^n \pmod{T^{N+1}},$$

then they satisfy the recurrence relation

$$c_n = \frac{1}{n}\sum_{m=1}^{n} b_m \cdot c_{n-m}, \quad n \geq 1.$$

Proof. If we take the (formal) logarithmic derivative of both sides of the assumed relation between the b_n and c_n and clear denominators, then we obtain the relation

$$\left(\sum_{n=1}^{N} b_n T^n\right)\left(\sum_{n=0}^{N} c_n T^{n-1}\right) \equiv \sum_{n=1}^{N} n c_n T^{n-1} \pmod{T^{N+1}}.$$

The lemma follows by expanding the left side and comparing the coefficients on each side. □

As stated above, $L(T, E/K)$ satisfies a functional equation: there is $\varepsilon(E/K) \in \{\pm 1\}$ such that

$$L(T, E/K) = \varepsilon(E/K)\cdot (qT)^N \cdot L(1/(q^2T), E/K), \tag{2–5}$$

and hence we have the relation

$$c_n = \varepsilon(E/K)\cdot q^{2n-N}\cdot c_{N-n}, \quad 0 \leq n \leq N. \tag{2–6}$$

In the following lemma we write $(\frac{\epsilon_\pi}{\pi})$ for the Legendre symbol in $\mathbb{F}_\pi$ of ϵ_π, defined in Table 1, and give a formula for $\varepsilon(E/K)$ (cf. [Hall 06, Corollary 5]).

Lemma 2.3.

$$\varepsilon(E/K) = (-1)^{\#M^+}\cdot \prod_{\pi\in A}\left(\frac{\epsilon_\pi}{\pi}\right).$$

Proof. This follows from calculations in [Rohrlich 96], where the sign is the global root number of E/K and is given by a product of local root numbers. If $\pi \in |U|$, then the local root number is trivial by [Rohrlich 96, Proposition 8] with $\tau = 1$. If $\pi \in M \cup A$, then we apply [Rohrlich 96, Theorem 2 (ii), (iii)] with $\tau = 1$ for the remaining cases. Note that if π is in A and does not have Kodaira symbol I_n^* with $n > 0$, then we need the assumption that q is not divisible by 2 or 3. □

We observe that the recurrence relation given by Lemma 2.2 enables us to perform a consistency check when trying to compute $L(T, E/K)$: the b_m and c_m are integers, so for each $n \geq 1$, the integer $\sum_{m=1}^{n} b_m \cdot c_{n-m}$ must be divisible by n. A second consistency check is to compute c_n for one or more $n > \lfloor N/2 \rfloor$ using the same method as for smaller n and then to verify that (2–6) holds. While one would not want to use the latter check when computing large data sets, it is very useful for making sure that the calculations are correct, because one can use it to test a small subset of data.

2.3. Quadratic Twists

We continue the notation of the previous sections. Thus we fix an elliptic curve E/K and a minimal Weierstrass model $y^2 = x^3 + ax + b$ of E over $\mathcal{O}_K$. For each $f \in K^\times$, we define E_f/K to be the elliptic curve with affine model $y^2 = x^3 + f^2ax + f^3b$.

Lemma 2.4. *Suppose L/K is an extension. If an elliptic curve over K is L-isomorphic to E, then it is K-isomorphic to some E_f, and $\sqrt{f} \in L$. Conversely, if $\sqrt{f} \in L$, then E and E_f are L-isomorphic.*

Proof. If $y^2 = x^3 + a'x + b'$ is an affine model for an elliptic curve E'/K, then an L-isomorphism $E \to E'$ must take the form $(x, y) \mapsto (x/c^2, y/c^3)$ for some $c \in L^\times$ (see [Silverman 86, p. 50]); recall that j is nonconstant, hence neither 0 nor 1728. In particular, $a' = c^4 a$ and $b' = c^6 b$, so $f = c^2 = b'/a'$ lies in $K^\times$ and $E' = E_f$. Conversely, if $c = \pm\sqrt{f} \in L$, then $(x, y) \mapsto (x/c^2, y/c^3)$ is an L-isomorphism $E \to E_f$. □

The lemma implies that $L = K(\sqrt{f})$ is the smallest extension over which E, E_f are L-isomorphic. Hence if f lies in the complement $K^\times - (K^\times)^2$, then E_f/K is a so-called quadratic twist of E/K.

Lemma 2.5. *E_f, E_g are K-isomorphic if and only if $f = gc^2$ for some $c \in K^\times$.*

Proof. Replace E/K by E_g/K and apply the previous lemma with $L = K$. □

We define the family of polynomials

$$\mathcal{F} = \{f \in \mathcal{O}_K : f \text{ is monic, square-free, prime to } \Delta\}$$

and write $\mathcal{F}_d \subset \mathcal{F}$ for the subset of f satisfying $\deg(f) = d$. The previous lemma implies that the E_f are mutually non-K-isomorphic for $f \in \mathcal{F}$, while for a fixed d, we will see that $\deg(L(T, E_f/K))$ is independent of $f \in \mathcal{F}_d$. The latter fact would not be true if we dropped the condition that f be relatively prime to Δ. As we will see, if $\alpha \in \mathbb{F}_q^\times$ is a nonsquare, then $L(T, E_{\alpha f}/K) = L(-T, E_f/K)$, which is why we restrict to monic f.

If $f \in \mathcal{F}$, then one can easily verify that $y^2 = x^3 + f^2 ax + f^3 b$ is a minimal Weierstrass model for E_f over $\mathcal{O}_K$ with discriminant $f^6 \cdot \Delta$. There is a unique integer e such that the substitution $(t, x, y) \mapsto (1/u, x/u^e, y/u^e)$ yields a minimal Weierstrass model for E_f over $\mathbb{F}_q[u]$, and we glue the models together over $\mathbb{P}^1 - \{0, \infty\}$ to construct the minimal Weierstrass model $\mathcal{E}_f \to \mathbb{P}^1$. We write M_f and A_f respectively for the divisors of multiplicative and additive reduction of $\mathcal{E}_f \to \mathbb{P}^1$.

We write $\mathbb{A}^1$ for the complement $\mathbb{P}^1 - \{\infty\}$. If $\pi \in |\mathbb{A}^1|$, then one can easily verify that

$$M_f \cap \mathbb{A}^1 = M \cap \mathbb{A}^1$$

and

$$A_f \cap \mathbb{A}^1 = (A \cap \mathbb{A}^1) \cup \{\pi \in |\mathbb{A}^1| : \pi | f\}.$$

If $\pi \in M_f \cap \mathbb{A}^1$, then one can also easily verify that $\mathcal{E}_f/\mathbb{F}_\pi$ has the same splitting behavior as $\mathcal{E}/\mathbb{F}_\pi$ if and only if the image of f is a square in $\mathbb{F}_\pi$, and otherwise it has the opposite splitting behavior; that is,

$$M_f^\pm \cap \mathbb{A}^1 = \left\{\pi \in M^\pm \cap \mathbb{A}^1 : \left(\frac{f}{\pi}\right) = \pm 1\right\} \cup \left\{\pi \in M^\mp \cap \mathbb{A}^1 : \left(\frac{f}{\pi}\right) = \mp 1\right\}.$$

If $f \in \mathcal{F}_d$ and d is even, then $\mathcal{E}$ and $\mathcal{E}_f$ are isomorphic over $\mathbb{F}_\infty$. On the other hand, if d is odd, then the Kodaira symbols of $\mathcal{E}/\mathbb{F}_\infty$ and $\mathcal{E}_f/\mathbb{F}_\infty$ form an unordered pair $\{S, S^*\}$, where $S \in \{\mathrm{I}_n, \mathrm{II}, \mathrm{III}, \mathrm{IV}\}$.

If we fix a nonsquare $\alpha \in \mathbb{F}_q^\times$ and $f \in \mathcal{F}$, then a similar calculation for $E_{\alpha f}$ shows that the Kodaira symbols for $\mathcal{E}_f$ and $\mathcal{E}_{\alpha f}$ are the same for all $\pi \in |\mathbb{P}^1|$, so $M_{\alpha f} = M_f$ and $A_{\alpha f} = A_f$. If $\pi \in A_f$, then $\mathcal{E}_f$ and $\mathcal{E}_{\alpha f}$ are isomorphic over $\mathbb{F}_\pi$. On the other hand, for every $\pi \in |\mathbb{P}^1 - A_f|$, there is a unique quadratic twist of $\mathcal{E}_f/\mathbb{F}_\pi$, which we call the scalar twist, and it is easy to show that $\mathcal{E}_{\alpha f}/\mathbb{F}_\pi$ is isomorphic to $\mathcal{E}_f/\mathbb{F}_\pi$ if $\deg(\pi) = [\mathbb{F}_\pi : \mathbb{F}_q]$ is even; otherwise, it is the scalar twist. We call $E_{\alpha f}$ the scalar twist of E_f.

2.4. *L*-Functions of Quadratic Twists

We continue the notation of the previous section and fix an elliptic curve E/K and a quadratic twist E_f/K. If U_f, M_f, and A_f are the primes over which E_f has good, multiplicative, and additive reduction respectively, then we can use the results of Section 2.2 to infer that the L-function $L(T, E_f/K)$ has Euler product expansion

$$L(T, E_f/K) = \prod_{\pi \in |U_f|} L(T^{\deg(\pi)}, \mathcal{E}_f/\mathbb{F}_\pi)^{-1} \times \prod_{\pi \in M_f^+} (1 - T^{\deg(\pi)})^{-1} \times \prod_{\pi \in M_f^-} (1 + T^{\deg(\pi)})^{-1}.$$

There is an important observation that relates this to the Euler product expansion in (2–2) of $L(T, E/K)$: if π lies in $U \cap U_f$ and if $\chi_\pi(f) \in \{\pm 1\}$ denotes the Legendre symbol of $f \pmod{\pi}$, then

$$L(T, \mathcal{E}_f/\mathbb{F}_\pi) = L(\chi_\pi(f)T, \mathcal{E}/\mathbb{F}_\pi).$$

In particular, if one has precomputed sufficiently many Euler factors for $L(T, E/K)$, then for most of the Euler factors of $L(T, E_f/K)$, the cost of computing the factor is essentially the cost of computing $\chi_\pi(f)$.

2.5. Pullbacks

We continue the notation of previous sections and fix an elliptic curve E/K and a minimal Weierstrass model $y^2 = x^3 + ax + b$ of E over $\mathcal{O}_K$. We write M, A respectively for the subsets of primes in K over which E has multiplicative and additive reduction respectively.

We fix a rational function field $L = \mathbb{F}_q(w)$ and a nonconstant element $\theta \in L$, and we write $\theta^* : K \to L$ for the embedding induced by sending t to θ. Let $\mathcal{O}_L \subset L$ be the integral closure of $\mathcal{O}_K$, and let $\mathcal{O}_\infty \subset L$ be the integral closure of $\mathcal{O}_\infty \subset K$. We call the primes of $\mathcal{O}_L$ the finite primes of L, and the primes of $\mathcal{O}_\infty$ the infinite primes of L. In general, $\mathcal{O}_L$ is not $\mathbb{F}_q[w]$ and $\mathcal{O}_\infty$ is not the local ring with uniformizer $1/w$, but rather, the infinite primes are the poles of θ. If π is a prime (finite or infinite) in L, we write $\theta(\pi)$ for the corresponding prime in K, f_π for the degree of inertia of π over $\theta(\pi)$, and e_π for the ramification degree.

We write E_L for the elliptic curve over L (eliding the dependence on the choice of θ) with affine model $y^2 = x^3 + \theta^*(a)x + \theta^*(b)$, and thus the coefficients of the model are rational functions in w when a, b are viewed as elements of L via θ^*. A priori, this model is not a minimal Weierstrass model of E_L over $\mathcal{O}_L$, but if π is a finite prime that is unramified in L or if $\theta(\pi)$ does not lie in A, then the model is a minimal Weierstrass model over the local ring $\mathcal{O}_\pi$. Similarly, if $\pi \in \mathcal{O}_\infty$ is an infinite prime, then a minimal Weierstrass model for E over $\mathcal{O}_\infty$ is guaranteed to be a minimal Weierstrass model over $\mathcal{O}_\pi$ only if π is unramified over $\theta(\pi)$ or if ∞ does not lie in A.

Now suppose that π is a prime of L such that π is ramified over $\theta(\pi)$ and E has bad reduction over $\theta(\pi)$, and let $y^2 = x^3 + a_\pi x + b_\pi$ be a minimal Weierstrass model of E over $\mathcal{O}_{\theta(\pi)}$ and let $\Delta_{\theta(\pi)}$ be the discriminant of this model. If E has Kodaira type I_n over $\theta(\pi)$ and if $e = e_\pi$ (e being the unique integer used to obtain a model for E over $\mathbb{F}_q[u]$), then $y^2 = x^3 + \theta^*(a_\pi)x + \theta^*(b_\pi)$ is a minimal Weierstrass model of E_L over $\mathcal{O}_\pi$ with discriminant $\Delta_\pi = \theta^*(\Delta_{\theta(\pi)})$ and E_L has Kodaira type I_{en} over π. On the other hand, if $\theta(\pi)$ lies in A, then the Kodaira type of E_L over π may differ from the Kodaira type of E over $\theta(\pi)$ depending on $e = e_\pi$. More precisely, if E has Kodaira type I_n^* over $\theta(\pi)$, then E_L has Kodaira type I_{en} or I_{en}^* over π if e is even or odd respectively. Otherwise, the discriminant Δ_π for a minimal Weierstrass model of E_L over $\mathcal{O}_\pi$ satisfies $\mathrm{ord}_\pi(\Delta_\pi) \equiv e \cdot \mathrm{ord}_{\theta(\pi)}(\Delta_{\theta(\pi)}) \pmod{12}$. Hence the Kodaira type of E_L over π is completely determined by the Kodaira type of E over $\theta(\pi)$ and Table 1.

Aside from the fact that one can use pullbacks to generate new elliptic surfaces from old, the other important role they play lies in the fact that every elliptic curve over L with nonconstant j-invariant can be written as a quadratic twist of the pullback of the "versal" elliptic curve E/K with affine model

$$y^2 = x^3 - \frac{108t}{t - 1728}x + \frac{432t}{t - 1728}.$$

One can easily verify that this elliptic curve has j-invariant t. Hence for an elliptic curve over L, one can take θ to be the j-invariant and use Lemma 2.5 to infer that an appropriate quadratic twist of the pullback will be the original elliptic curve over L. We remark that if $\sqrt{2} \notin \mathbb{F}_q$, this model is the twist of the model in [Silverman 86, proof of Proposition III.1.4] by the quadratic extension $K(\sqrt{2})/K$. The latter model has split-multiplicative reduction at $t = \infty$, while our model forces $\varepsilon(E/K) = -1$. In both cases, the L-function has degree 1, and thus in our model, we have $L(T, E/K) = 1 - qT$. One can verify that the point $P = (4, 8)$ lies on E and has height $1/2$, and thus the Mordell–Weil and analytic ranks of E are both equal to 1.

2.6. L-Functions of Pullbacks

We continue the notation of the previous section and fix an elliptic curve E/K and a pullback E_L/L. If U_L, M_L, and A_L are the primes over which E_L has good, multiplicative, and additive reduction respectively, then the L-function $L(T, E_L/L)$ has Euler product expansion

$$L(T, E_L/L) = \prod_{\pi \in |U_L|} L(T^{\deg(\pi)}, \mathcal{E}_L/\mathbb{F}_\pi)^{-1} \times \prod_{\pi \in M_L^+} (1 - T^{\deg(\pi)})^{-1} \times \prod_{\pi \in M_L^-} (1 + T^{\deg(\pi)})^{-1}.$$

As in the case of quadratic twists, if one has computed enough information for E/K, then it is relatively cheap to compute most of the Euler factors of $L(T, E_L/L)$. More precisely, if E_L has good reduction over π and if E has good reduction over $\mathfrak{p} = \theta(\pi)$, then

$$L(T, \mathcal{E}_L/\mathbb{F}_\pi) = 1 - a_{\mathfrak{p}^f} T + q^{\deg(\pi)} T^2,$$

where f_π is the degree of inertia of π over $\mathfrak{p}$ and $a_{\mathfrak{p}^{f_\pi}}$ can be determined by the expansion (2–1). In practice, it is easier to keep track of $a_{\mathfrak{p}^n}$ for several n than to use (2–1) directly, because among other reasons, it is difficult to compare elements of $\mathbb{F}_\mathfrak{p}$ with the corresponding subfield of $\mathbb{F}_\pi = \mathbb{F}_{\mathfrak{p}^{f_\pi}}$. Nonetheless, the amount of additional work one must do is small, since "most" elements of $\mathbb{F}_{q^n}$ have degree n over $\mathbb{F}_q$, and the upshot is that most of

the work of computing b_n in the corresponding expansion (2–3) for $L(T, E_L/L)$ is the cost of explicitly evaluating the map $\theta : \mathbb{P}^1(\mathbb{F}_{q^n}) \to \mathbb{P}^1(\mathbb{F}_{q^n})$ for all elements in the domain.

3. THE LIBRARY ELLFF

The discussion in Section 2.2 above naturally leads to a naive algorithm to compute the L-function of a non-isotrivial elliptic curve defined over a function field via counting points on a finite number of its fibers. Moreover, if sufficiently many Euler factors have been computed for the versal elliptic curve, one can realize a given elliptic curve as a pullback and quadratic twist and use the results of Sections 2.3–2.6 to significantly reduce the number of fibers on which one needs to count points. The authors have written a standalone C++ library called ELLFF built on Shoup's number theory library [Shoup 09], which can be added as a module to the free open-source mathematics software system Sage. The package allows anyone to efficiently compute these L-functions on their own.[3]

Internally, the library uses tables, computed on demand, to represent Euler factors. If one asks for the L-function of a curve, then the library demands the minimal number of tables necessary. One may also demand and manipulate the tables directly, e.g., in order to study how the sizes of special fibers vary. The library uses a database in order to reduce the complexity of computing a table, e.g., by returning a previously calculated copy of the table or twisting a table for another curve with the same j-invariant. A user whose database has the appropriate tables for the versal curve will benefit from such reductions, and thus we have made available a modest collection for download. Users may also save their own tables in the database in order to facilitate calculating tables for families of curves. For more information and setup instructions, see http://ellff.sagemath.org.

4. COMPUTATIONS

Using the discussion from Section 2, a database of L-functions was amassed for the family of quadratic twists of the following four elliptic curves (with notation consistent with that found in [Miranda and Persson 86]):

$$X_{222} : y^2 = x^3 - 27(t^4 - t^3 + t^2)x + 27(2t^6 - 3t^5 - 3t^4 + 2t^3), \tag{4–1}$$

$$X_{211} : y^2 = x^3 - 27t^4x + 54t^5(t-2), \tag{4–2}$$

$$X_{321} : y^2 = x^3 - 108t^3(4t-3)x + 432t^5(8t-9), \tag{4–3}$$

$$X_{431} : y^2 = x^3 - t^3(27t-24)x + t^4(54t^2 - 72t + 16). \tag{4–4}$$

These are the only elliptic curves, up to isogeny, over $\mathbb{F}_q(t)$ with $(q, 6) = 1$ such that $\#M = 2$ and $\#A = 1$. They are normalized so that $\infty \in M^+$, $t \in A$, and $t - 1 \in M$, forcing the L-function to be trivial for each of the curves. Note that the first curve is the Legendre curve,[4] given by the alternative model

$$X_{222} : y^2 = x(x+t)\left(x+t^2\right).$$

For each of these curves, we considered all prime $q \in \mathcal{Q} = \{5, 7, \ldots, 29\}$ and computed the L-functions of all the twists with bounded degree. The bound on the degree was determined by considerations of computational feasibility and depended on the size of the field of constants. Table 2 lists the number of twists over $\mathbb{F}_q$ of degree d in each family $\mathcal{F}_d$. This number does not depend on which of the four curves above one considers. A blank entry in the table denotes that the L-functions for all twists for the given d and q were not determined due to the computation requiring an excessive amount of time.

4.1. Goldfeld's Conjecture

In 1979, Goldfeld conjectured an average value for the analytic rank of a family of quadratic twists of a fixed elliptic curve $E/\mathbb{Q}$:

Conjecture 4.1. [Goldfeld 79] *For D a discriminant,*

$$\lim_{D\to\infty} \frac{\sum_{|d|<D} r(E_d)}{\#\{d : |d| < D\}} = \frac{1}{2}, \tag{4–5}$$

where $r(E_d)$ is the order of vanishing at $s = 1$ of the L-function of the quadratic twist $E_d/\mathbb{Q}$.

Goldfeld's conjecture concerns the analytic rank of an elliptic curve, though it is important to note that many authors replace the analytic rank with the algebraic rank (i.e., the rank, as a free $\mathbb{Z}$-module, of the group $E(K)$ of K-rational points on E modulo torsion), invoking the Birch–Swinnerton-Dyer conjecture if

[3] The library currently allows for only characteristic not 2 or 3, though handling these cases is straightforward and will be addressed in a future release.

[4] Strictly speaking, X_{222} is a twist by $-t$ of the usual Legendre curve model $y^2 = x(x-1)(x-t)$.

	5	7	11	13	17	19	23	29
$\#\mathcal{F}_1$	3	5	9	11	15	17	21	27
$\#\mathcal{F}_2$	13	31	91	133	241	307	463	757
$\#\mathcal{F}_3$	71	227	1019	1751	4127	5867	10691	22007
$\#\mathcal{F}_4$	345	1573	11181	22729	70113	111421	213762	638121
$\#\mathcal{F}_5$	1739	11033	123029	295523				
$\#\mathcal{F}_6$	8677	77203						
$\#\mathcal{F}_7$	43407							
$\#\mathcal{F}_8$	217009							
$\#\mathcal{F}_9$	1085075							
All	1356339	90072	135329	320147	74496	117612	224937	660912

TABLE 2. Number of twists in $\mathcal{F}_d$ for $q \in \mathcal{Q}$.

needed. For a survey of results on the average value and variation of the (algebraic) ranks of elliptic curves in a family of quadratic twists in the number field setting, see [Rubin and Silverberg 02]. A more recent paper [Bektemirov et al. 07] provides data for the average value and distribution of the analytic ranks of elliptic curves over $\mathbb{Q}$ ordered by conductor. Thus the reader should be wary of concluding that the data presented therein either support or undermine Goldfeld's conjecture, which considers the family of quadratic twists of a fixed elliptic curve and not all elliptic curves with bounded conductor.

Goldfeld's conjecture has a direct analogue in the function field setting: for an elliptic curve E over K, we set its analytic rank r to be the order of vanishing of $L(T, E/K)$ at $T = 1/q$. Instead of considering all twists by d with $|d| < D$, we consider those twists in $\mathcal{F}_D^* = \bigcup_{d \le D} \mathcal{F}_d$ and let D grow to infinity as before:

Conjecture 4.2. *For D a positive number,*

$$\lim_{D\to\infty} \frac{\sum_{f\in\mathcal{F}_D^*} r(E_f)}{\#\mathcal{F}_D^*} = \frac{1}{2}, \tag{4–6}$$

where $r(E_f)$ is the order of vanishing at $s = 1$ of the L-function of the quadratic twist $E_f/\mathbb{F}_q(t)$.

One would like a lower bound on the average analytic rank over the family of interest $\mathcal{F}_d$ analogous to that found in [Goldfeld 79, Proposition 1, p. 114]. In contrast to that proposition, where the average is taken over all discriminants, here determining the average over $\mathcal{F}_d$ is nontrivial. But using the functional equation, it is clear that if in the limit, the average of the sign of the functional equation over $\mathcal{F}_d$ is 0, then the average analytic rank over $\mathcal{F}_d$ is at least $1/2$. We next prove such a lower bound using this line of argument.

We begin by letting $M \cap \mathbb{A}^1 = \{\pi_1, \dots, \pi_r\}$ be the finite primes where E/K has multiplicative reduction and setting $N = \pi_1 \cdots \pi_r$.

Proposition 4.3. *There exists $\varepsilon_d \in \{\pm 1\}$ such that for all $f \in \mathcal{F}_d$,*

$$\varepsilon(E_f/K) = \varepsilon_d \cdot \varepsilon(E/K) \cdot \left(\frac{f}{N}\right), \tag{4–7}$$

where $\left(\frac{\cdot}{N}\right)$ is the Jacobi symbol of N.

Proof. We proceed by examining the contribution to the sign from the places of bad reduction.

Case 1: If $\pi \in A_1 \cap \mathbb{A}^1$, then E/K and E_f/K have the same Kodaira type at π. Thus there is no change to the local contribution from $\varepsilon(E/K)$ to $\varepsilon(E_f/K)$ for such π.

Case 2: If π is a finite prime that divides f, then E_f has reduction of type I_0^* over π. Thus the contribution to the sign in this case is given by

$$\left(\frac{\epsilon_{\pi,f}}{\pi}\right) = \left(\frac{-1}{\pi}\right) \equiv q^{\deg \pi} \pmod 4,$$

implying that the total contribution ϵ_f to the sign coming from those $\pi \in A_f - A$ satisfies

$$\epsilon_f \equiv q^d \pmod 4.$$

Thus the change in the local contribution from $\varepsilon(E/K)$ to $\varepsilon(E_f/K)$ from these primes depends only on d.

Case 3: For $\pi \in M_f \cap \mathbb{A}^1 = M \cap \mathbb{A}^1$, the splitness at π changes if and only if $(\frac{f}{\pi}) = -1$. Thus the total change in the local contribution from $\varepsilon(E/K)$ to $\varepsilon(E_f/K)$ is $(\frac{f}{N})$.

Case 4: For $\pi = \infty$, the reductions of E/K and E_f/K are the same if d is even by the discussion in Section

2.3. If d is odd, then the reduction depends only on the leading coefficient of f. Thus the local contribution to the sign is independent of $f \in \mathcal{F}_d$, so the change in the local contribution from $\varepsilon(E/K)$ to $\varepsilon(E_f/K)$ for $\pi = \infty$ depends only on d.

These cases exhaust all possible changes to the sign of the functional equation introduced by twisting, yielding equation (4–7). □

Corollary 4.4.

$$\frac{1}{\#\mathcal{F}_d}\sum_{f\in\mathcal{F}_d}\varepsilon(E_f/K) = \frac{\varepsilon_d\cdot\varepsilon(E/K)}{\#\mathcal{F}_d}\sum_{f\in\mathcal{F}_d}\left(\frac{f}{N}\right).$$

Corollary 4.4 reduces the average of the sign of the functional equation to the average of the Jacobi symbol over $\mathcal{F}_d$. The following proposition is due to private correspondence with E. Kowalski:

Proposition 4.5. (Kowalski.) *With notation as above, we have*

$$\lim_{d\to\infty}\frac{\sum_{f\in\mathcal{F}_d}(\frac{f}{N})}{\#\mathcal{F}_d} = 0.$$

Proof. Unless stated otherwise, we write $f, g, h \in \mathbb{F}_q[t]$ for arbitrary monic polynomials. Write $\Delta = NN'$ and let $\chi_\Delta(f)$ be the characteristic function of those f that are square-free and coprime to Δ. Setting

$$A_d = \sum_{f\in\mathcal{F}_d}\left(\frac{f}{N}\right),$$

we then have

$$A_d = \sum_{\deg(f)=d}\chi_\Delta(f)\left(\frac{f}{N}\right)$$

and

$$\#\mathcal{F}_d = \sum_{\deg(f)=d}\chi_\Delta(f).$$

Let $\mu(\cdot)$ be the Möbius function for polynomials. If $\deg(g) > 0$, then $\sum_{h|g}\mu(h) = 0$, and otherwise, $\sum_{h|g}\mu(h) = 1$. Thus

$$f \mapsto \sum_{g^2|f}\mu(g) \quad\text{and}\quad f \mapsto \sum_{h|(\Delta,f)}\mu(h)$$

are the characteristic functions for square-free polynomials and polynomials coprime to Δ respectively, and hence

$$\chi_\Delta(f) = \sum_{g^2|f}\mu(g)\sum_{h|(\Delta,f)}\mu(h).$$

Note that if $(g,\Delta) \neq 1$, then the right-hand sum over h vanishes, and hence we can restrict to g such that $(g,\Delta) = 1$. In particular, if we substitute into the above expression for A_d and rearrange terms, we have

$$A_d = \sum_{h|\Delta}\mu(h)\sum_{\substack{\deg(g)\le\frac{d}{2}\\(g,\Delta)=1}}\mu(g)\sum_{\substack{g^2h|f\\\deg(f)=d}}\left(\frac{f}{N}\right).$$

If we write $f = f_1g^2h$ in the innermost sum, then we have

$$A_d = \sum_{h|\Delta}\mu(h)\left(\frac{h}{N}\right)\sum_{\substack{\deg(g)\le\frac{d}{2}\\(g,\Delta)=1}}\mu(g)\sum_{\deg(f_1)=e}\left(\frac{f_1}{N}\right),$$

where $e = d - 2\deg(g) - \deg(h)$. Moreover, if we write B_e for the sum $B_e = \sum_{\deg(f)=e}(\frac{f}{N})$ and if we suppose $e \ge \deg(N)$, then

$$\begin{aligned}B_e &= \sum_{\alpha\in\mathbb{F}_q[t]/(N)}\left(\frac{\alpha}{N}\right)\sum_{\substack{\deg(f)=e\\f\equiv\alpha\,(\mathrm{mod}\ N)}}1\\ &= \sum_{\alpha\in\mathbb{F}_q[t]/(N)}\left(\frac{\alpha}{N}\right)q^{e-\deg(N)} = 0\end{aligned}$$

(because the last sum is a complete character sum). Therefore, if we write $e = d - 2\delta - \deg(h)$ $e' = \frac{1}{2}(d - \deg(N) - \deg(h)$, and suppose $e < \deg(N)$, we then have

$$A_d = \sum_{h|\Delta}\mu(h)\left(\frac{h}{N}\right)\sum_{e'\le\delta\le\frac{d}{2}}\sum_{\substack{\deg(g)=\delta\\(g,\Delta)=1}}\mu(g)B_{d-2\delta-\deg(h)},$$

where here e' denotes $\frac{1}{2}(d - \deg(N) - \deg(h))$. Observe that for all $e, \delta \ge 0$, we have $|B_e| \le q^e$ and $(\sum_{\deg(g)=\delta}1) \le q^\delta$. Thus for $d \ge 1$,

$$\begin{aligned}|A_d| &\le \sum_{h|\Delta}\mu(h)\sum_\delta q^{d-2\delta-\deg(h)}\sum_{\substack{\deg(g)=\delta\\(g,\Delta)=1}}1\\ &\le \sum_{h|\Delta}\mu(h)\sum_\delta q^{\deg(N)}q^{d/2} \ll q^{\deg(N)+d/2},\end{aligned}$$

where $\sum_\delta$ means summation over $\frac{1}{2}(d - \deg(N) - \deg(h)) \le \delta \le \frac{d}{2}$ and where the implied constant depends on Δ and N. On the other hand, $\#\mathcal{F}_d \gg q^d$, so

$$\lim_{d\to\infty}\frac{|A_d|}{\#\mathcal{F}_d} \ll \lim_{d\to\infty}q^{\deg(N)-d/2} = 0,$$

proving the proposition. □

This proposition then leads to the desired corollary:

Corollary 4.6. *With notation as above, we have*

$$\lim_{D\to\infty}\frac{\sum_{f\in\mathcal{F}_D^*}r(E_f)}{\#\mathcal{F}_D^*} \ge \frac{1}{2}.$$

D	5	7	11	13	17	19	23	29
1	1.000	0.400	0.667	0.636	0.733	0.588	0.571	0.704
2	0.688	0.667	0.680	0.674	0.668	0.679	0.661	0.652
3	0.644	0.669	0.622	0.629	0.610	0.607	0.588	0.576
4	0.653	0.659	0.638	0.620	0.605	0.599	0.588	0.575
5	0.666	0.633	0.590	0.581				
6	0.628	0.609						
7	0.623							
8	0.592							
9	0.582							

TABLE 3. $\mu(X_{222}, D)$ for $q \in \mathcal{Q}$.

D	5	7	11	13	17	19	23	29
1	0.333	0.400	0.444	0.636	0.600	0.471	0.571	0.481
2	0.562	0.556	0.540	0.618	0.590	0.580	0.587	0.585
3	0.690	0.570	0.577	0.605	0.583	0.565	0.552	0.558
4	0.625	0.609	0.569	0.574	0.559	0.555	0.551	0.543
5	0.618	0.571	0.553	0.554				
6	0.602	0.569						
7	0.587							
8	0.568							
9	0.556							

TABLE 5. $\mu(X_{321}, D)$ for $q \in \mathcal{Q}$.

4.2. Average Analytic Rank Data

We define

$$\mu(E, D) = \frac{\sum_{f \in \mathcal{F}_D^*} r(E_f)}{\#\mathcal{F}_D^*}$$

to be the average rank of the family of quadratic twists of E up to degree D. This value was calculated for the four elliptic curves discussed above with increasing D, and the data are presented in Tables 3 through 6, where the dependence of the average rank on D is made explicit. As in the case of Table 2, an empty entry denotes that those computations were not done.

Considering each table separately, we note that the individual columns present the data pertaining to Goldfeld's conjecture. In particular, for the largest data sets with $q = 5$, there is a slow convergence to the conjecture value of $1/2$. On the other hand, each row of a table presents data relevant to [Katz and Sarnak 99], where one lets q grow to infinity to determine that the conjugacy classes of the Frobenius automorphism are equidistributed in the special orthogonal group of $N \times N$ matrices with respect to Haar measure, where N is the degree of the L-function.

We can also consider how the average rank varies among each of the four curves for a fixed q, as presented in Figures 1 and 2. Recall that the four curves are not isogenous but have nearly the same reduction types. Even for the smallest data sets ($q \in \{17, 19, 23, 29\}$), there is good numerical evidence that the average ranks for each of the four curves are converging to the same value for any given q. Again, $q = 5$ provides the strongest evidence that this value is $1/2$. Note also that in general, the average rank of the Legendre curve X_{222} dominates the rank of the other three curves.

4.3. Rank Distributions

Combining Goldfeld's conjecture with the parity conjecture leads to a conjecture on the density of ranks in a family of quadratic twists (for details of the formulation, see [Rubin and Silverberg 02, Section 7.6]):

Conjecture 4.7. *With notation as in Conjecture 4.2,*

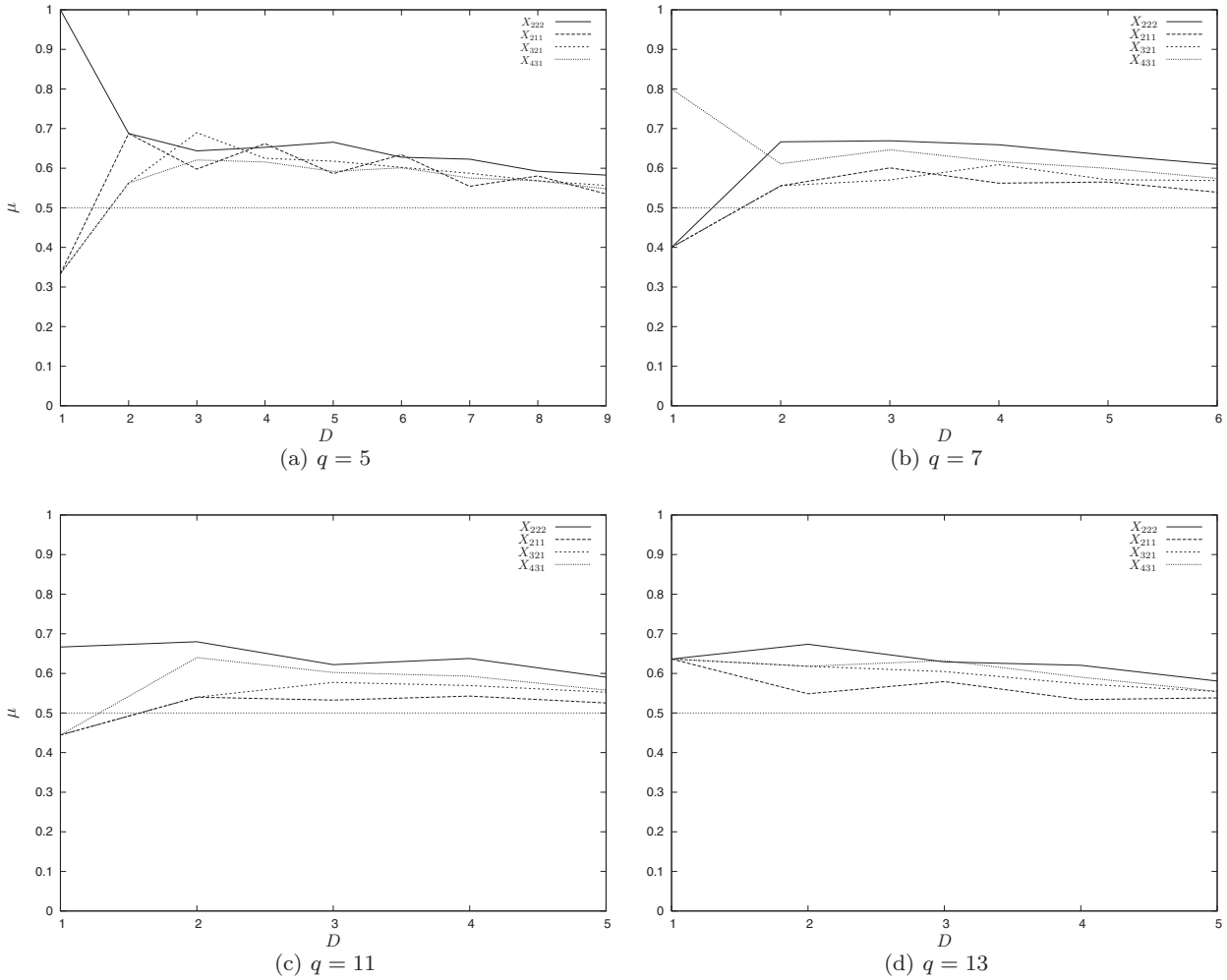
$$\lim_{D\to\infty} \frac{\#\{f \in \mathcal{F}_D^* : r(E_f) = 0\}}{\#\mathcal{F}_D^*} = \lim_{D\to\infty} \frac{\#\{f \in \mathcal{F}_D^* : r(E_f) = 1\}}{\#\mathcal{F}_D^*} = \frac{1}{2},$$

D	5	7	11	13	17	19	23	29
1	0.333	0.400	0.444	0.636	0.467	0.588	0.571	0.481
2	0.688	0.556	0.540	0.549	0.527	0.568	0.562	0.545
3	0.598	0.601	0.533	0.579	0.536	0.562	0.526	0.524
4	0.662	0.562	0.543	0.534	0.529	0.532	0.525	0.521
5	0.586	0.565	0.525	0.538				
6	0.634	0.539						
7	0.554							
8	0.581							
9	0.535							

TABLE 4. $\mu(X_{211}, D)$ for $q \in \mathcal{Q}$.

D	5	7	11	13	17	19	23	29
1	0.333	0.800	0.444	0.636	0.467	0.588	0.571	0.556
2	0.562	0.611	0.640	0.618	0.613	0.611	0.616	0.614
3	0.621	0.646	0.602	0.632	0.580	0.594	0.567	0.557
4	0.616	0.617	0.593	0.590	0.576	0.575	0.562	0.553
5	0.592	0.600	0.558	0.555				
6	0.601	0.574						
7	0.575							
8	0.568							
9	0.548							

TABLE 6. $\mu(X_{431}, D)$ for $q \in \mathcal{Q}$.



(a) $q = 5$ (b) $q = 7$

(c) $q = 11$ (d) $q = 13$

FIGURE 1. Variation of $\mu(X_i, D)$ as q varies.

whereas

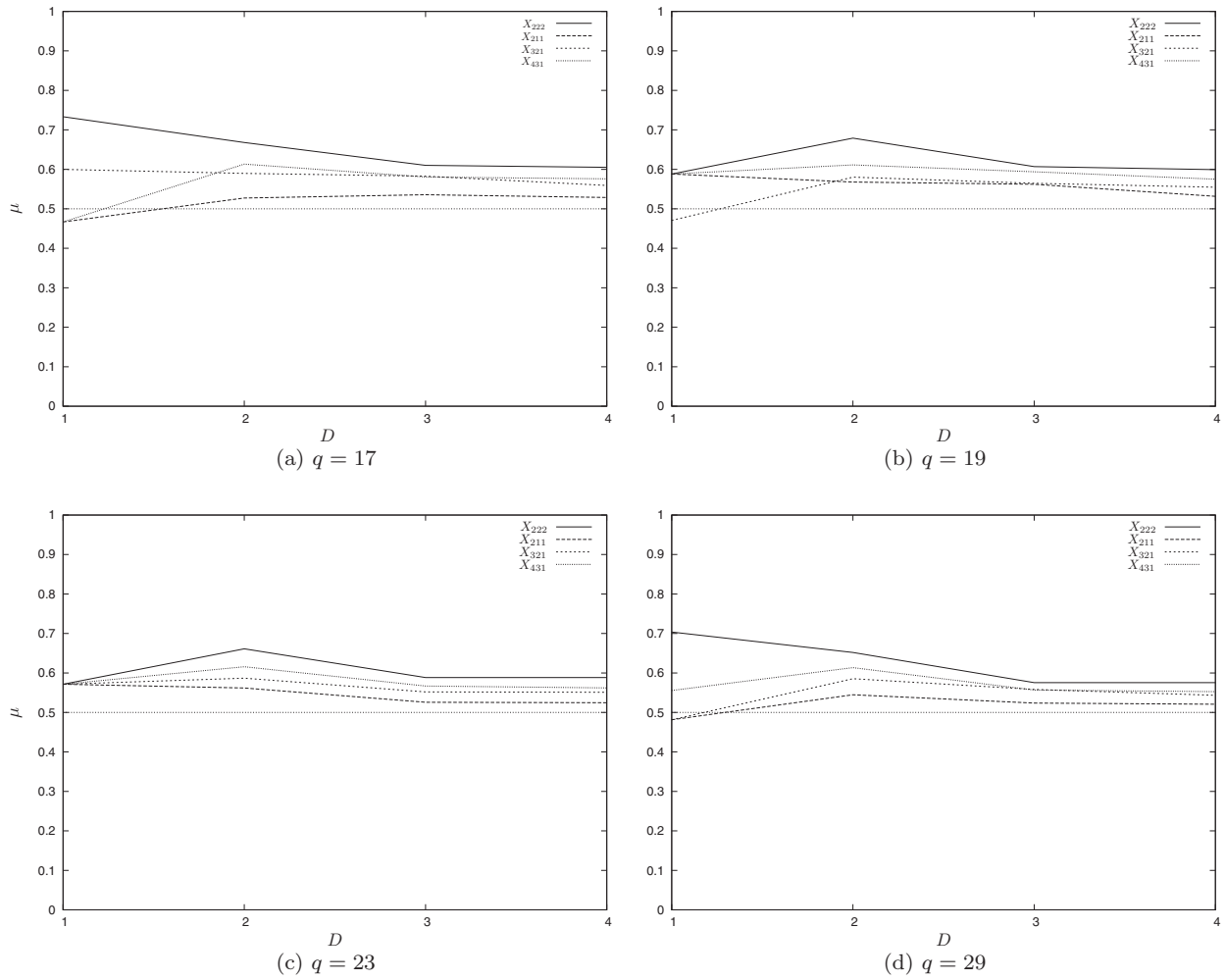
$$\lim_{D\to\infty} \frac{\#\{f \in \mathcal{F}_D^* : r(E_f) \geq 2\}}{\#\mathcal{F}_D^*} = 0.$$

As the data on average rank above suggest, the distribution of analytic ranks for our four families is close to that predicted by the density conjecture with a nontrivial number of twists with rank greater than or equal to two.[5] We present the relevant data in Table 7, where we have removed the dependence of the distribution on the degree of the twisting polynomials and instead consider all the L-functions we were able to compute given some q. For the dependence of the rank distribution on the degree, see the tables at http://ellff.sagemath.org.

[5]The largest rank discovered was a rank-5 curve, a twist of $X_{222}/\mathbb{F}_5(t)$ by $f = t^7 + 2t^6 + t^5 + 4t^4 + 4t^3 + t^2 + 2t + 1$.

5. CONCLUSION

The remarkable property that the L-function of a nonisotrivial elliptic curve over a function field is a polynomial yields an effective algorithm to determine its coefficients by computing the number of points on a finite number of fibers. These fibers precisely correspond to the Euler factors that determine $L(E/K, T)$, and by realizing a given curve as a quadratic twist or pullback of another curve, the number of Euler factors that need to be computed can be minimized. In particular, the versal elliptic curve provides a (noncanonical) choice for an elliptic curve from which one can pull back and twist to recover any given elliptic curve, allowing for the efficient computation of the given curve's L-function, provided sufficiently many Euler factors have been precomputed. These algorithms have been incorporated into ELLFF, a software library for the open-source mathematical



(a) $q = 17$ (b) $q = 19$

(c) $q = 23$ (d) $q = 29$

FIGURE 2. Variation of $\mu(X_i, D)$ as q varies.

software system Sage, allowing anyone to quickly compute such L-functions.

Experimentally, we computed the L-functions of four different families of quadratic twists in order to examine their analytic ranks for numerical evidence pertaining to Goldfeld's conjecture. Using an elementary argument, we know that the asymptotic average rank over our family of quadratic twists is at least $1/2$ as the degree of the twisting polynomial becomes arbitrarily large. In contrast to the situation in number fields, the case of function fields provides strong evidence, especially for the largest data sets, that this average is indeed $1/2$, thus supporting the validity of Goldfeld's conjecture in the function field case. Moreover, the experimental data also suggest that the analytic ranks are distributed closely with the density conjecture's prediction. Nonetheless, the presence of a nontrivial number of curves of rank at least 2 in even the largest data sets may suggest that the convergence to this distribution is rather slow.

This work is part of a small but growing body of computational number theory directly focused on function fields. Historically, computational number theorists have primarily worked over number fields, in particular $\mathbb{Q}$. This (understandable) bias has produced a dearth of algorithms and data for the function field setting, despite the fact that many of the ideas from number fields can be formulated more generally for any global field. There is much work left to be done—both theoretical and computational—for the case of function fields, but we believe that the example of L-functions of elliptic curves indicates that the effort is worthwhile and yields interesting mathematics.

q	5				7				11				13			
Rank	0	1	2	≥ 3	0	1	2	≥ 3	0	1	2	≥ 3	0	1	2	≥ 3
X_{222}	0.461	0.498	0.039	0.002	0.447	0.499	0.053	0.002	0.457	0.498	0.043	0.002	0.462	0.498	0.038	0.002
X_{211}	0.483	0.500	0.018	0.000	0.481	0.500	0.019	0.001	0.488	0.500	0.012	0.000	0.481	0.500	0.019	0.000
X_{321}	0.473	0.499	0.027	0.001	0.468	0.497	0.031	0.003	0.474	0.500	0.026	0.000	0.474	0.499	0.026	0.000
X_{431}	0.477	0.499	0.023	0.001	0.464	0.499	0.036	0.001	0.471	0.500	0.029	0.000	0.474	0.499	0.026	0.001

q	17				19				23				29			
Rank	0	1	2	≥ 3	0	1	2	≥ 3	0	1	2	≥ 3	0	1	2	≥ 3
X_{222}	0.450	0.498	0.059	0.002	0.452	0.498	0.048	0.002	0.458	0.498	0.042	0.002	0.463	0.499	0.036	0.001
X_{211}	0.485	0.500	0.014	0.000	0.484	0.500	0.016	0.000	0.488	0.500	0.012	0.000	0.490	0.500	0.010	0.000
X_{321}	0.471	0.500	0.029	0.000	0.473	0.500	0.027	0.001	0.475	0.500	0.025	0.000	0.479	0.500	0.021	0.000
X_{431}	0.463	0.499	0.037	0.000	0.463	0.499	0.036	0.001	0.470	0.499	0.030	0.001	0.474	0.499	0.026	0.001

TABLE 7. Rank distributions for all curves over all d and $q \in \mathcal{Q}$.

REFERENCES

[Bektemirov et al. 07] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins. "Average Ranks of Elliptic Curves: Tension between Data and Conjecture." *Bull. Amer. Math. Soc. (N.S.)* 44:2 (2007), 233–254.

[Bhargava and Shankar, forthcoming] M. Bhargava and A. Shankar. "Ternary Cubic Forms Having Bounded Invariants, and the Existence of a Positive Proportion of Elliptic Curves Having Rank 0." Available at http://arxiv.org/abs/1007.0052, forthcoming.

[Goldfeld 79] D. Goldfeld. "Conjectures on Elliptic Curves over Quadratic Fields." In *Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979*, Lecture Notes in Math. 751, pp. 108–118. Springer, 1979.

[Hall 06] C. Hall. "L-Functions of Twisted Legendre Curves." *J. of Number Theory* 119:1 (2006), 128–147.

[Katz 02] N. M. Katz. *Twisted L-Functions and Monodromy*, Annals of Mathematics Studies 150. Princeton University Press, 2002.

[Katz and Sarnak 99] N. M. Katz and P. Sarnak. "Zeroes of Zeta Functions and Symmetry." *Bull. Amer. Math. Soc. (N.S.)* 36:1 (1999), 1–26.

[Miranda and Persson 86]R. Miranda and U. Persson, "On Extremal Rational Elliptic Surfaces." *Math. Z.* 193:4 (1986), 537–558.

[Rohrlich 96] D. Rohrlich. "Galois Theory, Elliptic Curves, and Root Numbers." *Compositio Math.* 100:3 (1996), 311–349.

[Rubin and Silverberg 02] K. Rubin and A. Silverberg. "Ranks of Elliptic Curves." *Bull. Amer. Math. Soc. (N.S.)* 39:4 (2002), 455–474.

[Shoup 09] V. Shoup. *NTL: A Library for Doing Number Theory*. Available at http://www.shoup.net/ntl/, 2009.

[Silverman 86] J. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106. Springer, 1986.

Salman Baig, Department of Mathematics, University of Washington, Seattle, WA 98195 (salmanhb@math.washington.edu)

Chris Hall, Department of Mathematics, University of Wyoming, Ross Hall, Laramie, WY 82071 (chall14@uwyo.edu)