Journal of Number Theory 157 (2015) 154–169

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Newman's conjecture in function fields ☆

Alan Chang [a], David Mehrle [b], Steven J. Miller [c,*], Tomer Reiter [b], Joseph Stahl [d], Dylan Yott [e]

[a] *Department of Mathematics, University of Chicago, Chicago, IL 60637, United States*
[b] *Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15289, United States*
[c] *Department of Mathematics and Statistics, Williams College, Williamstown, MA 01267, United States*
[d] *Department of Mathematics and Statistics, Boston University, Boston, MA 02215, United States*
[e] *Department of Mathematics, University of California, Berkeley, Berkeley, CA 94720, United States*

ARTICLE INFO

Article history:
Received 5 February 2015
Received in revised form 27 April 2015
Accepted 27 April 2015
Available online 26 June 2015
Communicated by David Goss

MSC:
11M20
11M26
11Y35
11Y60
14G10

Keywords:

ABSTRACT

Text. De Bruijn and Newman introduced a deformation of the completed Riemann zeta function ζ, and proved there is a real constant Λ which encodes the movement of the nontrivial zeros of ζ under the deformation. The Riemann hypothesis is equivalent to the assertion that $\Lambda \leq 0$. Newman, however, conjectured that $\Lambda \geq 0$, remarking, "the new conjecture is a quantitative version of the dictum that the Riemann hypothesis, if true, is only barely so". Andrade, Chang and Miller extended the machinery developed by Newman and Pólya to L-functions for function fields. In this setting we must consider a modified Newman's conjecture: $\sup_{f\in\mathcal{F}} \Lambda_f \geq 0$, for $\mathcal{F}$ a family of L-functions.

We extend their results by proving this modified Newman's conjecture for several families of L-functions. In contrast with

☆ This work was supported by NSF grants DMS-1347804, DMS-1265673, Williams College, and the PROMYS program. The authors thank Noam Elkies, David Geraghty, Rob Pollack, Glenn Stevens, and Keith Conrad for their insightful comments and support. We would also like to thank the referees for their careful reading of drafts and their helpful suggestions.

* Corresponding author.
E-mail addresses: ac@math.uchicago.edu (A. Chang), dmehrle@cmu.edu (D. Mehrle), sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu (S.J. Miller), treiter@andrew.cmu.edu (T. Reiter), jstahl@bu.edu (J. Stahl), dyott@math.berkeley.edu (D. Yott).

http://dx.doi.org/10.1016/j.jnt.2015.04.028

Newman's conjecture
Zeros of the L-functions
Function fields

previous work, we are able to exhibit specific L-functions for which $\Lambda_D = 0$, and thereby prove a stronger statement: $\max_{L\in\mathcal{F}} \Lambda_L = 0$. Using geometric techniques, we show a certain deformed L-function must have a double root, which implies $\Lambda = 0$. For a different family, we construct particular elliptic curves with $p+1$ points over $\mathbb{F}_p$. By the Weil conjectures, this has either the maximum or minimum possible number of points over $\mathbb{F}_{p^{2n}}$. The fact that $\#E(\mathbb{F}_{p^{2n}})$ attains the bound tells us that the associated L-function satisfies $\Lambda = 0$.

Video. For a video summary of this paper, please visit http://youtu.be/hM6-pjq7Gi0.

1. Introduction

Newman's conjecture, as originally formulated, is a statement about the zeros of a deformation of the completed Riemann zeta function. This deformation was introduced by Pólya to attack the Riemann hypothesis, but Newman's conjecture regarding this deformation is in fact an almost counter-conjecture to the Riemann hypothesis. The classical Newman's conjecture is explained below in Section 1.1.

1.1. The classical Newman's conjecture

Instead of working with the Riemann zeta function $\zeta(s)$ itself, define the completed Riemann zeta function

$$\xi(s) := \frac{s(s-1)}{2}\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s). \tag{1.1}$$

This has the effect of eliminating the trivial zeros of $\zeta(s)$, but keeping all of the nontrivial ones. Additionally, the functional equation for $\xi(s)$ is simpler than that for the Riemann zeta function: $\xi(s) = \xi(1-s)$. To simplify the analysis further, introduce

$$\Xi(x) := \xi\left(\frac{1}{2} + ix\right) \tag{1.2}$$

to shift the zeros of $\xi(s)$ to lie along the real line. Recall that because ξ is analytic and real valued on the real line, then $\xi(\overline{s}) = \overline{\xi(s)}$. Combining this fact and the functional equation for ξ, we have that $\Xi(x) \in \mathbb{R}$ whenever $x \in \mathbb{R}$. Now let $\Phi(u)$ denote the Fourier transform[1] of $\Xi(x)$. Because $\Xi(x)$ decays rapidly as $x \to \infty$, we may introduce a "time" parameter into the inverse Fourier transform.

[1] We normalize so that the Fourier transform of $f(x)$ is $\int_{-\infty}^{\infty} f(x)e^{-ixu}du$.

Definition 1.1. The *deformed Riemann zeta function* Ξ_t is

$$\Xi_t(x) := \int_0^\infty e^{tu^2} \Phi(u) \left(e^{iux} + e^{-iux}\right) du. \tag{1.3}$$

Note that $\Xi_0(x) = \Xi(x) = \xi(1/2 + ix)$ agrees with (1.2). This deformation $\Xi_t(s)$ is the function that Pólya hoped to use to attack the Riemann hypothesis, because the Riemann hypothesis is equivalent to the statement that all of the zeros of $\Xi_0(x)$ are real. De Bruijn managed to prove a related statement.

Lemma 1.2. *(See De Bruijn [4, Theorem 13].) If $t \in \mathbb{R}$ is such that Ξ_t has only real zeros, then for all $t' \geq t$, $\Xi_{t'}$ has only real zeros.*

Pólya wanted to show that Ξ_t has only real zeros for all $t \in \mathbb{R}$, which would imply the Riemann hypothesis. Unfortunately, this is not the case, as the next lemma shows.

Lemma 1.3. *There is some $t \in \mathbb{R}$ such that Ξ_t has a nonreal zero.*

Proof. The content of this lemma is implied by [11, Theorem 3]. See also the remark in [11] immediately preceding Theorem 1. □

However, it is possible to place bounds on this t; this is how Newman salvaged Pólya's strategy. By combining the previous two lemmas, we may define the De Bruijn–Newman constant.

Definition 1.4. (See Newman [11, Theorem 3].) The *De Bruijn–Newman Constant* $\Lambda \in \mathbb{R}$ is the value such that

- if $t \geq \Lambda$, then Ξ_t has only real zeros;
- if $t < \Lambda$, then Ξ_t has a non-real zero.

Such a constant exists because of Lemmas 1.2 and 1.3.

This allows us to rephrase the Riemann hypothesis yet again. The Riemann hypothesis is true if and only if $\Lambda \leq 0$, that is, if and only if Ξ_0 has only real zeros. On the other hand, Newman made the following conjecture.

Conjecture 1.5 *(Newman). (See [11, Remark 2].) Let Λ be the De Bruijn–Newman constant. Then $\Lambda \geq 0$.*

Note that if both Newman's Conjecture 1.5 and the Riemann hypothesis are true, then it must be the case that $\Lambda = 0$. On this, Newman remarked: "This new conjecture is a quantitative version of the dictum that the Riemann hypothesis, if true, is

only barely so" [11, Remark 2]. It is remarkable just how precise the bounds on Λ are: [12] achieved the current best-known bound of $\Lambda \geq -1.14541 \times 10^{-11}$. To find this bound, Saouter, Gourdon and Demichel build on the work of Csordas, Smith and Varga [6], who use differential equations describing the motion of the zeros under deformation to demonstrate that atypically close pairs of zeros yield lower bounds on Λ.

These ideas have since been translated to many different L-functions beyond the Riemann zeta function. Stopple [13] showed that there is a real constant Λ_{Kr} analogous to the De Bruijn–Newman constant for quadratic Dirichlet L-functions, and Andrade, Chang and Miller [1] expanded this to state a version of Newman's conjecture for automorphic L-functions. Stopple established bounds on Λ_{Kr} in the case of quadratic Dirichlet L-functions; in particular, for the L function corresponding to the quadratic character modulo $D = -175\,990\,483$, $\Lambda_{\mathrm{Kr}} > -1.13 \times 10^{-7}$. The results on lower bounds are extended to automorphic L-functions by [1]. Most recently, Andrade, Chang and Miller investigated in [1] the analogue of the De Bruijn–Newman constant for function field L-functions. This is the setting in which we work, so we describe the translation of this framework to the function field setting in Section 2.

1.2. This paper

In the function field setting, a similar setup is possible. We will work in this setting, which we develop in Section 2. It is in this setting that we resolve several versions of the generalized Newman's conjecture first considered by Andrade, Chang and Miller in [1]. We recall some of their work in Section 2.1. We then prove our main result 1.7 in Section 4, where this theorem is stated as Theorem 4.1.

Over function fields $\mathbb{F}_q[x]$, each quadratic Dirichlet L-function $L(s, \chi_D)$ also gives rise to a constant Λ_D. However, there is very different behavior in this case. For one, it is possible that $\Lambda_D = -\infty$, as in Remark 2.6. Therefore, we consider the supremum of the De Bruijn–Newman constants over a family of L-functions, so the appropriate analogue of Newman's conjecture becomes the following.

Conjecture 1.6 *(Newman's conjecture for function fields). (See [1, Conjecture 1.8].) Let $\mathcal{F}$ be a family of L-functions over a function field $\mathbb{F}_q[x]$. Then*

$$\sup_{D \in \mathcal{F}} \Lambda_D \;=\; 0. \tag{1.4}$$

Our main result resolves this conjecture for a wide class of families $\mathcal{F}$.

Theorem 1.7 *(Main result). Let $\mathcal{F}$ be a family of pairs of the form (D, q), where q is an odd prime power and $D \in \mathbb{F}_q[T]$ is monic squarefree polynomial of odd degree at least three. Suppose that for some odd prime power q', $(x^{q'} - x, q') \in \mathcal{F}$. Then if Λ_D is the De Bruijn–Newman constant associated to D,*

$$\sup_{(D,q)\in\mathcal{F}} \Lambda_D = \max_{(D,q)\in\mathcal{F}} \Lambda_D = 0. \tag{1.5}$$

Remark 1.8. Many times, the families of (D, q) in consideration will be constant in q; i.e., $q = q'$ for all $(D, q), (D', q') \in \mathcal{F}$. In these cases, to simplify notation we may omit q from the description and simply consider $\mathcal{F}$ to consist of only the D's rather than the pairs (D, q). We use the notation above to emphasize that the result also covers cases where q varies (for example, when the family $\mathcal{F}$ is obtained by reducing a fixed polynomial $D \in \mathcal{O}_K[T]$ modulo all primes $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K).

To prove this, we first note that $\Lambda_D = 0$ if and only if the L-function corresponding to D has a double root. Then we explicitly compute $L(s, \chi_D)$ for $D = x^q - x$ via ℓ-adic cohomology, the Weil conjectures, and a result of Katz [9]. The necessary background for the proof is recalled in Section 3.

Following from Theorem 1.7, the following conjectures (stated as Conjectures 2.8 and 2.9) of Andrade, Chang and Miller [1] are resolved.

Corollary 1.9. *Let $\mathcal{F}$ be one of the following families of L-functions. Then* $\sup_{D\in\mathcal{F}} \Lambda_D = 0$.

- $\mathcal{F} = \{D \in \mathbb{F}_q[T] \mid$ *squarefree, monic, odd degree* $\geq 3\}$;
- $\mathcal{F} = \{D \in \mathbb{F}_q[T] \mid \deg D = 2g + 1,\ 2g + 1 = p^k$ *for some prime* $p\}$.

2. Setup for a Newman's conjecture over function fields

In [1], the authors find many analogues between the number field and function field versions of Newman's conjecture. The appropriate replacement for $\mathbb{Z}$ is $\mathbb{F}_q[T]$, the ring of polynomials with coefficients in $\mathbb{F}_q$ (the finite field with q elements), where q is a power of a prime. We do not consider fields of characteristic two.

Definition 2.1. (See Andrade, Chang, Miller [1, Definition 3.1].) Let q be an odd prime power and let $D \in \mathbb{F}_q[T]$. We say that (D, q) is a *good pair* or simply that D is *good* (in the case that q is understood) if

(1) D is monic and square-free,
(2) $\deg D$ is odd, and
(3) $\deg D \geq 3$.

The rationale for these assumptions is elucidated in [1, Remark 3.2]. In short, we assume squarefree and monic because this corresponds to the fundamental discriminants in the number field setting, and we assume q is odd because we are not considering the characteristic 2 case, in which everything is a perfect square. Instead of the Riemann zeta function in this setting, we have the following.

Definition 2.2. Let D be good. We define the L-function associated to D to be

$$L(s, \chi_D) := \sum_{f \text{ monic}} \chi_D(f) N(f)^{-s}, \tag{2.1}$$

where $N(f)$ is the norm of f, $N(f) := q^{\deg f}$ and χ_D is quadratic character associated with D.

If we collect terms in (2.1), we have

$$L(s, \chi_D) = \sum_{n \geq 0} c_n \left(q^{-s}\right)^n, \tag{2.2}$$

where

$$c_n = \sum_{\substack{f \text{ monic} \\ \deg f = n}} \chi_D(f). \tag{2.3}$$

These coefficients vanish for $n \geq \deg D$, and $L(s, \chi_D)$ is a polynomial of degree exactly $\deg D - 1$ in q^{-s}. Setting g to be the genus of the hyperelliptic curve $y^2 = D(x)$ (so $g = (\deg D - 1)/2$), we complete $L(s, \chi_D)$ as we completed the Riemann zeta function in (1.1) in the classical setting. Set

$$\xi(s, \chi_D) := q^{gs} L(s, \chi_D), \tag{2.4}$$

so that $\xi(s, \chi_D)$ satisfies the nice functional equation $\xi(s, \chi_D) = \xi(1 - s, \chi_D)$. Then in analogy to (1.2), define

$$\Xi(s, \chi_D) := \xi\left(\frac{1}{2} + i\frac{x}{\log q}, \chi_D\right) = \Phi_0 + \sum_{n=1}^{g} \Phi_n (e^{inx} + e^{-inx}), \tag{2.5}$$

where $\Phi_n = c_{g-n} q^{n/2} = c_{g+n} q^{n/2}$. Note that Φ_n is the Fourier transform of Ξ_t in this case, which is a Fourier transform on the circle instead of the real line.

Definition 2.3. The *deformed L-function* $\Xi_t(x, \chi_D)$ is

$$\Xi_t(x, \chi_D) := \Phi_0 + \sum_{n=1}^{g} \Phi_n e^{tn^2} (e^{inx} + e^{-inx}). \tag{2.6}$$

Andrade, Chang and Miller established the existence of a De Bruijn–Newman constant Λ_D for each good $D \in \mathbb{F}_q[T]$ [1, Lemma 3.4]. The behavior of this constant Λ_D is in some ways similar to that of the classical De Bruijn–Newman constant, as the following lemma shows.

Lemma 2.4. *(See [1, Lemma 3.2].) Let (q, D) be a good pair. Let $t_0 \in \mathbb{R}$. If $\Xi_{t_0}(x, \chi_D)$ has a zero x_0 of order at least 2, then $t_0 \leq \Lambda_D$.*

However, there are differences between function and number fields. As there is a proof of the Riemann hypothesis in function fields, $\Lambda_D \leq 0$. Furthermore, for many D we can actually get the strict inequality $\Lambda_D < 0$ because of the existence of the following partial converse to Lemma 2.4 above.

Lemma 2.5. *If $\Xi_0(x, \chi_D)$ does not have a double zero, then $\Lambda_D < 0$.*

In fact, since there are L-functions $\Xi_0(x, \chi_D)$ with only real zeros, there is the possibility of $\Lambda_D = -\infty$, as in the following remark.

Remark 2.6. In the function field setting, we may have that $\Lambda_D = -\infty$. Indeed, [1, Remark 3.10] supplies a counterexample: $D = T^3 + T \in \mathbb{F}_3[T]$ has $\Lambda_D = -\infty$.

In light of this remark, we can see that Newman's conjecture, if directly translated to the function field setting, is false. Thus, different versions of Newman's conjecture are necessary. Most generally, the modified Newman's conjecture is the following.

Conjecture 2.7 *(Newman's conjecture for function fields). (See [1, Conjecture 1.8].) Let $\mathcal{F}$ be a family of L functions over a function field $\mathbb{F}_q[x]$. Then*

$$\sup_{D \in \mathcal{F}} \Lambda_D = 0. \tag{2.7}$$

Regarding the De Bruijn–Newman constant in the function field setting, Andrade, Chang and Miller made the following conjectures for specific families.

Conjecture 2.8. *(See Andrade, Chang, Miller [1, Conjecture 3.14].) Fix q a power of an odd prime. Then*

$$\sup_{(D,q) \text{ good}} \Lambda_D \geq 0. \tag{2.8}$$

Conjecture 2.9. *(See Andrade, Chang, Miller [1, Conjecture 3.15].) Fix g a positive integer. Then*

$$\sup_{\substack{\deg D = 2g+1 \\ (D,q) \text{ good}}} \Lambda_D \geq 0. \tag{2.9}$$

Conjecture 2.10. *(See Andrade, Chang, Miller [1, Conjecture 3.16].) Fix $D \in \mathbb{Z}[T]$ square-free. For each prime p, let $D_p \in \mathbb{F}_p[T]$ be the polynomial obtained from reducing $D \pmod p$. Then*

$$\sup_{(D_p,p)\ \text{good}} \Lambda_{D_p} \geq 0. \tag{2.10}$$

The last of these three conjectures, Conjecture 2.10, was resolved in [1, Theorem 3.19] for the case where $\deg D = 3$. This result is briefly reviewed in the following subsection.

2.1. Previous results

In this section, the work of Andrade, Chang and Miller in [1] to prove Newman's conjecture for families given by elliptic curves is described. Fix a square-free polynomial $\mathcal{D} \in \mathbb{Z}[T]$ of degree 3 and for each prime p, let $D_p \in \mathbb{F}_p[T]$ be the polynomial obtained by reducing $D \pmod p$. In [1] Newman's conjecture is proved for the family $\mathcal{F} = \{D_p\}$.

Theorem 2.11. *(See [1, Theorem 3.19].) For $\mathcal{F}$ defined above, $\sup_{D\in\mathcal{F}} \Lambda_D = 0$.*

The proof uses the fact that

$$\Xi_t(x, \chi_{D_p}) \;=\; -a_p(\mathcal{D}) + 2\sqrt{p}e^t \cos x, \tag{2.11}$$

where $a_p(\mathcal{D})$ is the trace of Frobenius of the elliptic curve $y^2 = \mathcal{D}(T)$. From this, we can deduce

$$\Lambda_{D_p} \;=\; \log \frac{|a_p(\mathcal{D})|}{2\sqrt{p}}. \tag{2.12}$$

Finally, the recent proof of Sato–Tate for elliptic curves without complex multiplication [5,8,14,3] implies that there exists a sequence of primes $p_1, p_2, \ldots$ such that

$$\lim_{n\to\infty} \frac{a_{p_n}(\mathcal{D})}{2\sqrt{p_n}} \;\to\; 1. \tag{2.13}$$

Hence $\Lambda_{D_{p_n}} \to 0$.

Remark 2.12. It should be noted that (2.12) holds not only for p prime, but also when p is replaced by a prime power q. We make use of this more general explicit form of Λ later on.

Remark 2.13. The proof relied on the fact that Λ_{D_p} could be computed explicitly, which is made possible by the fact that D has genus $g = 1$, so there are only two terms to consider when computing (2.6). When $g \geq 2$, then Ξ_t contains multiple e^t terms and

therefore multiple $\cos nx$ terms, making it much harder to find the explicit expression of Λ_{D_p}.

Remark 2.14. We are not aware of any proof of the existences of a sequence of primes for which (2.13) holds without appealing to proven Sato–Tate laws; it would be interesting to have an elementary proof of such a statement.

The previous two remarks above suggest that it would be difficult to prove results for $\deg \mathcal{D} \geq 5$ using the same methods.

3. The Hasse–Weil zeta function and the Weil conjectures

Let $X/\mathbb{F}_q$ be a curve, q a power of a prime p as always.

Definition 3.1. Let $N_m := \#X(\mathbb{F}_{q^m})$. The *Hasse–Weil zeta function* of the curve X is defined by the formal power series

$$Z(X,s) \ := \ \exp\left(\sum_{m\geq 1} \frac{N_m}{m}\left(q^{-s}\right)^m\right). \tag{3.1}$$

Remark 3.2. Most of the definitions and results in this section hold in much greater generality than stated here, but for ease of exposition we will only state results in the generality required for our applications.

It isn't immediately clear from the definition that these zeta functions are useful objects to consider, but the following canonical example illustrates that in fact the zeta function contains information about the geometry of X.

Example 3.3. Let $X = \mathbb{P}^1(\mathbb{F}_q)$. It follows that $N_m = q^m + 1$, so we obtain the following expression for the zeta function after setting $T = q^{-s}$:

$$Z(X,s) \ = \ \frac{1}{(1-T)(1-qT)}. \tag{3.2}$$

The two terms linear in T in the denominator reflect the fact that $H^0_{\acute{e}t}(\mathbb{P}^1, \mathbb{Q}_\ell)$ and $H^2_{\acute{e}t}(\mathbb{P}^1, \mathbb{Q}_\ell)$ are one-dimensional. The lack of a linear term in the numerator reflects the fact that $H^1_{\acute{e}t}(\mathbb{P}^1, \mathbb{Q}_\ell) = 0$.

Henceforth, we set $T = q^{-s}$ unless stated otherwise. There is a collection of theorems called the Weil conjectures (although they have now been proven) which make more precise the relationship between the geometry of X and its zeta function. The Weil conjectures were first stated for algebraic curves by Artin, and were proven later by Dwork and Deligne. We now state the subset of the Weil conjectures relevant for this paper.

Theorem 3.4. *Let $X/\mathbb{F}_q$ be a nonsingular projective curve. Then the Hasse–Weil zeta function $Z(X,s)$ of X has the form*

$$Z(X,s) = \frac{P(T)}{(1-T)(1-qT)}, \qquad P \in \mathbb{Z}[T]. \tag{3.3}$$

Moreover,

(1) $\deg P = 2g$, *where g is the genus of the curve X, and*
(2) P *factors as* $\prod_{i=1}^{2g}(1-\alpha_i T)$. *For all i,* $|\alpha_i| = q^{1/2}$.

By putting these results together and unwinding the definition of $Z(X,s)$ as a generating function, we obtain the following useful result.

Corollary 3.5. *Let X be a nonsingular projective curve of genus g. Then the numbers $\alpha_1, \ldots, \alpha_{2g}$ coming from the zeta function satisfy*

$$\#X(\mathbb{F}_q^m) = 1 + q^m - \sum_{i}^{2g} \alpha_i^m. \tag{3.4}$$

Remark 3.6. We have the following useful application of Corollary 3.5. Let $E/\mathbb{F}_p$ be an elliptic curve such that $\#E(\mathbb{F}_p) = p+1$. Recall that elliptic curves have genus 1. By (3.4) we have $\alpha_1 + \alpha_2 = 0$. We also have $P(T) = (1-\alpha_1 T)(1-\alpha_2 T) \in \mathbb{Z}[T]$, so that $\alpha_1\alpha_2 \in \mathbb{Z}$. Since $|\alpha_i| = \sqrt{p}$, we have $\alpha_1\alpha_2 = \pm p$. However, the first condition implies that we must have (after possibly reordering) $\alpha_1 = i\sqrt{p}$, $\alpha_2 = -i\sqrt{p}$. Now we compute

$$\#E(\mathbb{F}_p^2) = p^2 + 1 - (i\sqrt{p})^2 - (-i\sqrt{p})^2 = p^2 + 2p + 1. \tag{3.5}$$

The computation in Remark 3.6 and generalizations thereof will be very important later for proving particular cases of Newman's conjecture in families by constructing particular elliptic curves $E/\mathbb{F}_p$ with $p+1$ points. The condition of having p^2+2p+1 points over $\mathbb{F}_{p^2}$ is significant because Corollary 3.5 implies that this number is as large as possible for a curve of genus 1 over $\mathbb{F}_q$.

Definition 3.7. We say a curve X with $q + 2\sqrt{q} + 1$ points over $\mathbb{F}_q$ is *maximal* over $\mathbb{F}_q$. Similarly, X is *minimal* if it has $q - 2\sqrt{q} + 1$ points over $\mathbb{F}_q$.

Remark 3.8. It is clear that a curve can only be maximal (or minimal) over $\mathbb{F}_q$ when q is a square. This will be important for proving cases of Newman's conjecture in families.

Corollary 3.5 allows us to prove a special case of Newman's conjecture using the explicit formula for Λ_D found in [1], when $y^2 = D(x)$ is an elliptic curve. We prove this result by explicitly relating our L-function $L(s,\chi_D)$ to the zeta function of the curve $y^2 = D(x)$, in a result known to Artin [2].

Proposition 3.9. *(See [2, Equation (3) on page 209].)* $L(s, \chi_D)$ *is the numerator of the zeta function* $Z(X, s)$*, where* X *is the curve defined by* $y^2 = D(x)$*. More precisely,* $Z(X, s) = Z(\mathbb{P}^1, s)L(s, \chi_D)$*.*

Now that we can realize our L-function $L(s, \chi_D)$ as part of the zeta function $Z(X, s)$, the Weil conjectures tell us valuable information about the behavior of the roots of L. In particular, we will be able to prove that certain curves have a double root (in fact, a root of multiplicity g).

4. Families of curves satisfying Newman's conjecture

We are now ready to prove our main result, Theorem 1.7. It is restated below as Theorem 4.1. Throughout this section we assume familiarity with the theory of étale cohomology (specifically ℓ-adic cohomology) of projective curves; development of this subject can be found in J.S. Milne's book [10].

Theorem 4.1. *Let* $\mathcal{F}$ *be a family of pairs of the form* (D, q)*, where* $D \in \mathbb{F}_q[T]$ *is monic squarefree polynomial of odd degree at least three, and* $(x^q - x, q) \in \mathcal{F}$*. Then*

$$\sup_{(D,q)\in\mathcal{F}} \Lambda_D = \max_{(D,q)\in\mathcal{F}} \Lambda_D = 0. \tag{4.1}$$

To prove this theorem, we need the following key lemma.

Lemma 4.2. $L(s, \chi_D)$ *has a double root if and only if* $\Lambda_D = 0$*.*

Proof. If $L(s, \chi_D)$ has a double root, then the fact that $\Lambda_D = 0$ follows from [1, Lemma 3.22, Remark 3.23]. The converse is a consequence of [1, Lemma 3.11]. □

The immediate consequence of this lemma is the following.

Corollary 4.3. *If* $L(s, \chi_D)$ *has a double zero, then Newman's conjecture is true for any family* $\mathcal{F}$ *containing* D*.*

To show that $\sup_{(D,q)\in\mathcal{F}} \Lambda_D = 0$, it suffices to find D such that $L(s, \chi_D)$ has a double root. In this case, $\Lambda_D = 0$, so the supremum is actually a maximum.

Proposition 4.4. *Let* $D \in \mathbb{F}_q[x]$ *be given by* $D(x) = x^q - x$*. Then* $L(s, \chi_D)$ *has a double root.*

Remark 4.5. In fact, $L(s, \chi_D)$ has a root of order g, and $L(s, \chi_D)$ is explicitly given by $L(s, \chi_D) = (T^2 q \pm 1)^g$.

Proof of Proposition 4.4. The curve $X : y^2 = x^q - x$ carries an action of $G = \mathbb{F}_q$ by $\mathbb{F}_q$-linear automorphisms. That is, the action of $\mathbb{F}_q$ commutes with the Frobenius map. For $a \in \mathbb{F}_q$, the action is defined by

$$a \cdot (x, y) \;=\; (x + a, y). \tag{4.2}$$

By functoriality, the cohomology groups $H^i_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ carry an action of G as well. In certain nice cases, $H^*_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ splits up into distinct irreducible representations of G (i.e., is multiplicity free). In this case, this means $H^*_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ is a sum of characters of G. Since the action of Frobenius commutes with the action of G, we have a well-defined action of Frobenius on $H^*_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})[\chi]$, the χ-isotypic component for χ a character of G. Assuming the multiplicity-free hypothesis, these spaces are 1-dimensional and Frobenius acts as a scalar, which is therefore a Frobenius eigenvalue. Since the only information needed to construct the zeta function are the Frobenius eigenvalues, we can construct the zeta function if we can understand $H^*_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ as a representation of G and how Frobenius acts. It is a result of Nick Katz (restated below as Theorem 4.6) that gives conditions for the above to be true and also gives the Frobenius eigenvalues explicitly as Gauss sums. The following theorem gives us the decomposition of $H^*_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ and the Frobenius eigenvalues, which finishes the proof. □

Theorem 4.6. *(See Katz [9].) Let $X/\mathbb{F}_q$ be projective and smooth, and G a finite group acting on X by $\mathbb{F}_q$-linear automorphisms, and ρ an irreducible complex (or ℓ-adic) representation of G. Define*

$$S(X/\mathbb{F}_q, \rho, n) \;:=\; \frac{1}{\#G} \sum_{g \in G} \mathrm{Tr}(\rho(g))\, \#\mathrm{Fix}(\mathrm{Frob}_p \circ g^{-1}). \tag{4.3}$$

Then the following are equivalent.

(1) *The multiplicity of ρ is one in $H^{i_0}_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ and zero in $H^i_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ for $i \neq i_0$.*
(2) *For all $n \geq 1$, we have*

$$|S(X/F_q, \rho, n)| \;=\; (\sqrt{q})^{i_0 n}. \tag{4.4}$$

(3) Frob *acts on $H^i_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell})$ by the scalar $(-1)^{i_0} S(X/\mathbb{F}_q, \rho, 1)$.*

Now we compute the sums $S(X/\mathbb{F}_q, \chi, n)$ as χ ranges over the characters of $G = \mathbb{F}_q$ (since G is abelian its irreducible representations are characters). The characters of $\mathbb{F}_q$ are parametrized by $\mathbb{F}_q$ itself, as they take the form χ_a where $\chi_a(b) = \zeta_p^{\mathrm{Tr}(ab)}$, where ζ_p is a primitive pth root of unity.

Theorem 4.7. *The conditions in Theorem 4.6 hold for $X : y^2 = x^q - x/\mathbb{F}_q$. Let $q = p^r$ and $p^* = \left(\frac{-1}{p}\right) p$. As a representation of $G = \mathbb{F}_q$*

$$H^1_{\acute{e}t}(X, \overline{\mathbb{Q}_\ell}) \;=\; \sum_{\chi \text{ nontrivial}} \chi. \tag{4.5}$$

The Frobenius eigenvalues are $(\sqrt{p^*})^r$ *and* $-(\sqrt{p^*})^r$*, both with multiplicity* $\frac{q-1}{2}$*.*

Proof. Our projectivized curve X is given by $y^2 z^{q-2} = x^q - xz^{q-1}$, which is easily checked to be smooth. We have the following equality:

$$S(X, \chi, n) \;=\; \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi(a) \#\mathrm{Fix}(\mathrm{Frob}_q^n \circ [-a]). \tag{4.6}$$

Now we must determine when a point (x, y) is fixed by $\mathrm{Frob}_q^n \circ [-a]$. This is when $y^{q^n} = y$ and $x^{q^n} - x = a$. That means $y \in \mathbb{F}_{q^n}$ and $\mathrm{Tr}(x^q - x) = a$, where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is the field theoretic trace. For a fixed $y \in \mathbb{F}_{q^n}$, when $\mathrm{Tr}(y^2) = a$, we have q fixed points corresponding to the q distinct solutions to $x^q - x = a$, otherwise we have 0 fixed points. Define

$$I(y, a) \;=\; \begin{cases} 1 & \text{if } \mathrm{Tr}(y) = a; \\ 0 & \text{otherwise.} \end{cases} \tag{4.7}$$

Then we have

$$\begin{aligned} S(X, \chi, n) \;&=\; \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi(a) \sum_{y \in \mathbb{F}_{q^n}} qI(y, a) \\ &=\; \sum_{y \in \mathbb{F}_{q^n}} \sum_{a \in \mathbb{F}_q} \chi(a) I(y, a) \\ &=\; \sum_{y \in \mathbb{F}_{q^n}} \chi(\mathrm{Tr}(y^2)) \\ &=\; \sum_{y \in \mathbb{F}_{q^n}} \chi(\mathrm{Tr}(y)) \left(\frac{N_m(y)}{q} \right). \end{aligned} \tag{4.8}$$

Note here $\left(\frac{\cdot}{q}\right)$ is the $\mathbb{F}_q$-Legendre symbol. Now we apply the Hasse–Davenport relation which says precisely that the above "Gauss sums" are (up to sign) just powers of Gauss sums over $\mathbb{F}_q$. More precisely, it tells us that

$$|S(X, \chi, n)| \;=\; \left| \sum_{y \in \mathbb{F}_q} \chi(y) \left(\frac{y}{q} \right) \right|^n. \tag{4.9}$$

If χ is nontrivial, it is a well-known result that the inner sum has magnitude $\sqrt{q}$. That is,

$$|S(X,\chi,n)| \;=\; \begin{cases} (\sqrt{q})^n & \text{if } \chi \text{ is trivial;} \\ q^n & \text{otherwise.} \end{cases} \tag{4.10}$$

By Theorem 4.6 that means that

$$H^1_{\acute{e}t}(X,\overline{\mathbb{Q}_\ell}) \;=\; \sum_{\chi \text{ nontrivial}} \chi,\; H^2_{\acute{e}t}(X,\overline{\mathbb{Q}_\ell}) \;=\; \chi_{\text{triv}} \tag{4.11}$$

as representations of $\mathbb{F}_q$. The reason $H^0_{\acute{e}t}(X,\overline{\mathbb{Q}_\ell})$ doesn't appear is because in order for our results to be true, we must take compactly supported cohomology, which forces $H^0_{\acute{e}t}(X,\overline{\mathbb{Q}_\ell}) = 0$, since X isn't compact. By the equivalent condition of Theorem 4.6, we know that the Frobenius eigenvalues on $H^1_{\acute{e}t}(X,\overline{\mathbb{Q}_\ell})$ are the sums $(-1)S(X,\chi,1)$. We also immediately verify that Frobenius acts on $H^2_{\acute{e}t}(X,\overline{\mathbb{Q}_\ell})$ by the scalar q in accordance with the Weil conjectures. To compute $S(X,\chi,1)$, we write $q = p^r$, and $\chi = \chi_a$ for some $a \in \mathbb{F}_q$. Applying the Hasse–Davenport relation again and using the computation of the standard quadratic Gauss sum over $\mathbb{F}_p$ gives

$$S(X,\chi_a,1) \;=\; \begin{cases} (-1)^{r+1}(\sqrt{p^*})^r & \text{if } a \text{ is a quadratic residue;} \\ (-1)^r(\sqrt{p^*})^r & \text{otherwise.} \end{cases} \tag{4.12}$$

□

Corollary 4.8. *Let $\mathcal{F} = \{D \in \mathbb{F}_q[T] \mid D \text{ monic, squarefree, of odd degree} \geq 3\}$. Then*

$$\sup_{D\in\mathcal{F}} \Lambda_D = 0. \tag{4.13}$$

Corollary 4.9. *Let $\mathcal{F} = \{D \mid \deg D = 2g+1, 2g+1 = p^k \text{ for some prime } p\}$. Then*

$$\sup_{D\in\mathcal{F}} \Lambda_D = 0. \tag{4.14}$$

In addition to the above two corollaries, we can also show that the following family satisfies Newman's conjecture.

Theorem 4.10. *Let $D \in \mathbb{Z}[T]$ be a square-free monic cubic polynomial. Then there exists a number field $K/\mathbb{Q}$ such that*

$$\sup_{\mathfrak{p}\subseteq\mathcal{O}_K} \Lambda_{D_\mathfrak{p}} = 0, \tag{4.15}$$

where $D_\mathfrak{p}$ denotes the reduction of D modulo the prime ideal $\mathfrak{p}$.

Proof. It suffices to produce a single prime π so that $a_\pi(D) = 2\sqrt{p^2}$, so that $\Lambda_{D_\pi} = 0$ by the previous lemma. If we can find $p \in \mathbb{Z}$ inert in K with $a_p(D) = 0$, then for $\pi = p\mathcal{O}_K$ we have $a_\pi(D) = 2\sqrt{p^2}$ by the Weil conjectures. Thus $\Lambda_{D_\pi} = 0$, which gives the result. It is important to note that we don't need to take the supremum over all π, since any π as constructed above attains the supremum.

For all but finitely many p, we can reduce $y^2 = D(x) \bmod p$ and thereby obtain an elliptic curve over $\mathbb{F}_p$. For these p, the condition that $a_p(D) = p+1$ can be rephrased as saying that p is a supersingular prime for E (as long as $p > 5$). It is a theorem of Noam Elkies [7, Theorem 1] that for $E/\mathbb{Q}$ an elliptic curve, and any finite set of primes S, we can find a supersingular prime for E outside of S. This result uses the theory of complex multiplication of elliptic curves. Now we need only choose $d \in \mathbb{Z}$ and p a supersingular prime so that $\left(\frac{d}{p}\right) = -1$, which is easily accomplished since we are free to choose d squarefree belonging to a class which is a quadratic non-residue mod p. Thus p is inert in K, and the proof is complete. □

Remark 4.11. Since we can find a supersingular prime of E outside of any finite set, we might hope to prove something stronger, namely, we might want to fix K beforehand and hope that the collection of supersingular primes of E contains a prime inert in K. Unfortunately, this statement can fail for K quadratic.

The following counterexample was suggested to us in correspondence with Noam Elkies.

Example 4.12 *(Elkies).* Consider $X_0(11)$, an elliptic curve over $\mathbb{Q}$ with 5-torsion and good reduction away from 11. For $p \neq 11$, the 5-torsion points remain distinct mod p, giving

$$\#X_0(11)(\mathbb{F}_p) \equiv 0 \pmod 5. \tag{4.16}$$

Thus if p is supersingular for $X_0(11)$, we must have $p \equiv 4 \pmod 5$, which forces p to split in $K = \mathbb{Q}(\sqrt{5})$. Thus, since supersingularity is equivalent to $a_p = p+1$ only for $p > 5$, we check $p = 2$, 3 and 5 separately and see that $a_p \neq 0$. Thus we've shown that for $E = X_0(11)$ and $K = \mathbb{Q}(\sqrt{5})$, we cannot find a prime $\pi \subset \mathcal{O}_K$ so that $\Lambda_{D_\pi} = 0$.

Remark 4.13. For a representation theoretic explanation of this counterexample, recall that for elliptic curves $E/\mathbb{Q}$, and primes ℓ not dividing the conductor of E we can consider the mod ℓ representation attached to E:

$$\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_\ell). \tag{4.17}$$

For $q \nmid \ell$ and the conductor of E, we have that $\mathrm{Tr}(\overline{\rho_{E,\ell}}(\mathrm{Frob}_q)) \equiv a_q \pmod \ell$. When we're in the case that the mod ℓ representation is surjective, we can find q so that $a_q \equiv 0 \pmod \ell$, which is necessary but not sufficient for $a_q = 0$, which we want in order to construct maximal curves. In the case of $E = X_0(11)$, we can compute using SAGE that the mod 5 representation is not surjective, which helps explain why $a_p \equiv 0 \pmod 5$ can't be attained. It follows from Serre's open image theorem that the mod ℓ representation is surjective. One avenue for future research is to use surjectivity of the mod ℓ representation to strengthen the above theorem as much as possible.

References

[1] J. Andrade, A. Chang, S.J. Miller, Newman's conjecture in various settings, J. Number Theory 144 (2013) 70–91.
[2] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. II, Math. Z. 19 (1) (1924) 207–246.
[3] T. Barnet-Lamb, D. Geraghty, M. Harris, R. Taylor, A family of Calabi–Yau varieties and potential automorphy II, Publ. Res. Inst. Math. Sci. 47 (1) (2011) 29–98.
[4] N.G. De Bruijn, The roots of trigonometric integrals, Duke Math. J. 17 (3) (1950) 197–226.
[5] L. Clozel, M. Harris, R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations, Publ. Math. Inst. Hautes Études Sci. 108 (2008) 1–181, with Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.
[6] G. Csordas, W. Smith, R.S. Varga, Lehmer pairs of zeros, the De Bruijn–Newman constant Λ, and the Riemann hypothesis, Constr. Approx. 10 (1) (1994) 107–129.
[7] N.D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, Invent. Math. 89 (3) (1987) 561–567.
[8] M. Harris, N. Shepherd-Barron, R. Taylor, A family of Calabi–Yau varieties and potential automorphy, Ann. of Math. (2) 171 (2) (2011) 779–813.
[9] N.M. Katz, Crystalline cohomology, Dieudonné modules, and Jacobi sums, in: Automorphic Forms, Representation Theory and Arithmetic, Springer, Berlin, Heidelberg, 1981, pp. 165–246.
[10] J. Milne, Étale Cohomology, Princeton University Press, Princeton, NJ, 1980.
[11] C.M. Newman, Fourier transforms with only real zeros, Proc. Amer. Math. Soc. 61 (2) (1976) 245–251.
[12] Y. Saouter, X. Gourdon, P. Demichel, An improved lower bound for the De Bruijn–Newman constant, Math. Comp. 80 (276) (2011) 2281–2287.
[13] J. Stopple, Notes on low discriminants and the generalized Newman conjecture, Funct. Approx. Comment. Math. 51 (1) (2013) 23–41.
[14] R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations. II, Publ. Math. Inst. Hautes Études Sci. 108 (2008) 183–239.