COMPUTING ZETA FUNCTIONS OF KUMMER CURVES VIA MULTIPLICATIVE CHARACTERS

ALAN G.B. LAUDER

Abstract. We present a practical polynomial-time algorithm for computing the zeta function of a Kummer curve over a finite field of small characteristic. Such algorithms have recently been obtained using a method of Kedlaya based upon Monsky-Washnitzer cohomology, and are of interest in cryptography. We take a different approach. The problem is reduced to that of computing the L-function of a multiplicative character sum. This latter task is achieved via a cohomological formula based upon the work of Dwork and Reich. We show, however, that our method and that of Kedlaya are very closely related.

1. Introduction

Computing zeta functions of varieties over finite fields is one of the basic problems in algorithmic number theory. Over the last few decades this has attracted considerable attention, motivated mainly by applications in cryptography. In [19] Wan and the author showed that the problem always has a polynomial-time solution provided the characteristic of the field is small and the dimension is fixed. Our result was based on the p-adic methods in Dwork's proof of the rationality of these zeta functions. Unfortunately our algorithm is not really practical. Independently, Kedlaya presented a fast algorithm based upon Monsky-Washnitzer cohomology for hyperelliptic curves over finite fields of small odd characteristic [16]. This was of particular interest since such curves are useful in cryptography [18]. Gaudry and Gürel showed that Kedlaya's algorithm extends naturally to the so-called superelliptic curves [13]. In this article we shall call these Kummer curves. Neither of these algorithms were able to tackle hyperelliptic curves in characteristic 2, the case of greatest practical interest, the reason perhaps being that such curves are examples of Artin-Schreier curves, rather than Kummer curves. Wan and the author devised a fast method for a restricted class of Artin-Schreier curves, including elliptic and certain

Date: October 8, 2002.

Alan Lauder gratefully acknowledges the support of the EPSRC (Grant GR/N35366/01) and St John's College, Oxford, and thanks Frederik Vercauteren, Daqing Wan and the anonymous referees.

Mathematics Subject Classification 2000: 11T24, 11Y16, 14Q05 *Key words and phrases*: Multiplicative character, L-function, Kummer curve, zeta function, hyperelliptic, superelliptic, finite field, Kedlaya's algorithm, cryptography.

hyperelliptic curves in characteristic 2, based upon Dwork's ad hoc cohomology theory for one variable exponential sums [20]. (This method extends to all Artin-Schreier curves [21].) Subsequently, Denef and Vercauteren found a method for Artin-Schreier curves in characteristic 2, and were able to extend this to all hyperelliptic curves, using Monsky-Washnitzer cohomology [5, 29]. The purpose of the present article is to present a fast method for Kummer curves in small characteristic, based upon an ad hoc cohomology theory of Dwork-Reich for multiplicative character sums. The algorithm has the same complexity as those in [13, 16], and in fact in the final section we explain precisely how the two are related. As such, this article also gives a self-contained derivation of the algorithm of Kedlaya, which does not depend upon the machinery of Monsky-Washnitzer cohomology. Since our approach proceeds via character sums, we actually obtain a fast method for computing L-functions of multiplicative character sums.

Let p denote a prime number, and a a positive integer. Define $q = p^a$ and denote by $\mathbb{F}_q$ the finite field with q elements. Fix an algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$ and let $\mathbb{F}_{q^k}$ be the unique subfield of order q^k. We write $\bar{\mathbb{F}}_q^*$ for the set of non-zero elements in $\bar{\mathbb{F}}_q$. The Kummer curves over $\mathbb{F}_q$ we consider in this paper are defined by an equation of the form

$$Y^m = \bar{f}(X) \tag{1}$$

where $\bar{f} \in \mathbb{F}_q[X]$ is a polynomial of degree d. We shall assume throughout that $\bar{f}$ is squarefree with $\bar{f}(0) \neq 0$, $m > 1$ and is coprime to d, and m divides $p - 1$. (This final restriction is not needed in [13], and as such our result is actually slightly less general, although the complexity dependence on m is a little better.) Specifically, denote by $C_{\bar{f}}$ the curve embedded in $\{\bar{x} \in \bar{\mathbb{F}}_q \mid \bar{f}(\bar{x}) \neq 0\} \times \bar{\mathbb{F}}_q^*$ with equation (1) and let $\tilde{C}_{\bar{f}}$ be the unique smooth projective curve birational to $C_{\bar{f}}$.

Theorem 1. *The zeta function of the smooth projective curve $\tilde{C}_{\bar{f}}$ may be computed deterministically in $\tilde{\mathcal{O}}(pa^3d^4m^3)$ bit operations. Hence the order of the Jacobian of $\tilde{C}_{\bar{f}}$ may be found deterministically within this time bound.*

Here we use Soft-Oh notation $\tilde{\mathcal{O}}$ which ignores logarithmic factors, as in [19, Section 6.3].

Our approach yields as an intermediate result a method for computing the L-function of a multiplicative character sum defined in terms of $\bar{f}$. Specifically, let χ be a multiplicative character of order m defined on $\mathbb{F}_p^*$. Let χ_k denote the character on $\mathbb{F}_{q^k}^*$ comprising the Norm map followed by χ. Then the L-function $L(\bar{f}, \chi, T)$ is defined (as in Section 2) and we show that a p-adic embedding of it may be computed quickly.

We refer to the references in [2] for the large literature on point counting, including [9, 27], and the more recent work [5, 10, 11, 13, 14, 16, 22, 26, 29, 30, 31, 33].

Sections 2, 3, 4 and 5 lay the mathematical foundation of our algorithm: it is based mainly on a cohomological version of the Reich Trace Formula for one-variable character sums. To the author's knowledge, this version has previously only been worked out explicitly in [8, 25], and does not appear in the work of Reich [23, 24]. Since this formula is central to the algorithm we develop it in full detail. Our formula is very similar to the ones [8, 25], and in Note 17 we explain the precise relation. Section 6 contains a statement of the algorithm for Kummer curves and Section 7 describes exactly how to perform the main steps. Specifically, we present a reduction method and obtain bounds on the denominators introduced, allowing us to determine the required p-adic accuracy — this is the main original mathematical contribution of the article. The complexity analysis is tied up in Section 8, and the relation to Kedlaya's algorithm is explained in Section 9.

2. L-functions and Kummer curves

Let $\bar{\mathbb{Q}}$ denote an algebraic closure of the rationals $\mathbb{Q}$. Let $\chi : \mathbb{F}_p^* \to \bar{\mathbb{Q}}$ be a multiplicative character of order m, and $\mathrm{Nm}_k : \mathbb{F}_{q^k}^* \to \mathbb{F}_p^*$ the absolute Norm map. Notice that we have $m|p-1$. Let g be some generator of $\mathbb{F}_p^*$ and $\mu := \chi(g)$, a primitive mth root of unity. Define $\chi_k : \mathbb{F}_{q^k}^* \to \bar{\mathbb{Q}}$ to be the multiplicative character $\chi \circ \mathrm{Nm}_k$. For $1 \le j \le m-1$ we have that χ_k^j is a character of order $m/\gcd(j,m)$.

Let $\bar{f} \in \mathbb{F}_q[X]$ be the polynomial from Section 1. For $1 \le j \le m-1$ define

$$S_k^*(\bar{f},\chi^j) := \sum_{\bar{x}\in\mathbb{F}_{q^k}^*} \chi_k^j(\bar{f}(\bar{x})) \tag{2}$$

$$L^*(\bar{f},\chi^j,T) := \exp\left(\sum_{k=1}^{\infty} \frac{S_k^*(\bar{f},\chi^j)}{k} T^k\right) \tag{3}$$

where we use the convention that $\chi_k(0) = 0$. Let $S_k(\bar{f},\chi^j)$ and $L(\bar{f},\chi^j,T)$ denote the corresponding character sum and L-function over the affine line. When $j = 1$ we shall omit the χ in this notation. Let $C_{\bar{f}}$ be the curve embedded in $\{\bar{x} \in \bar{\mathbb{F}}_q \mid \bar{f}(\bar{x}) \neq 0\} \times \bar{\mathbb{F}}_q^*$ with equation

$$Y^m = \bar{f}(X).$$

Let $\tilde{C}_{\bar{f}}$ denote the unique smooth projective curve birational to $C_{\bar{f}}$.

Lemma 2. *For each $\bar{x} \in \mathbb{F}_{q^k}$ with $\bar{f}(\bar{x}) \neq 0$ there are exactly $n_{\bar{x}}$ points of the form $(\bar{x},\bar{y}) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}^*$ on $C_{\bar{f}}$ where*

$$n_{\bar{x}} = \begin{cases} m & \text{if } \chi(\mathrm{Nm}_k(\bar{f}(\bar{x}))) = 1 \\ 0 & \text{if } \chi(\mathrm{Nm}_k(\bar{f}(\bar{x}))) \neq 1 \end{cases}$$

Proof. We have $n_{\bar{x}} = m$ when $\bar{f}(\bar{x})$ is an mth power in $\mathbb{F}_{q^k}$ and $n_{\bar{x}} = 0$ otherwise. This first condition is equivalent to $\mathrm{Nm}_k(\bar{f}(\bar{x}))$ an mth power in $\mathbb{F}_p^*$, and the result follows. □

Denote by $C_{\bar{f}}(\mathbb{F}_{q^k})$ the set of $\mathbb{F}_{q^k}$-rational points on $C_{\bar{f}}$. From Lemma 2 one deduces

$$\sum_{j=1}^{m-1} \sum_{\bar{x} \in \mathbb{F}_{q^k}} \chi_k^j(\bar{f}(\bar{x})) = (-1)(R_k - \frac{N_k}{m}) + \frac{(m-1)N_k}{m}.$$

Here $N_k := \#(C_{\bar{f}}(\mathbb{F}_{q^k}))$ and

$$R_k := \#\{\bar{x} \in \mathbb{F}_{q^k} \,|\, \bar{f}(\bar{x}) \neq 0\} =: q^k - r_k$$

and we use the fact that $\sum_{j=1}^{m-1}(\mu^i)^j = -1$ for $1 \leq i \leq m-1$. It follows that

$$\#(C_{\bar{f}}(\mathbb{F}_{q^k})) = \sum_{j=1}^{m-1} S_k(\bar{f}, \chi^j) + (q^k - r_k).$$

Letting $Z(C_{\bar{f}}, T)$ denote the zeta function of $C_{\bar{f}}$ we find

$$Z(C_{\bar{f}}, T) = \frac{\prod_{j=1}^{m-1} L(\bar{f}, \chi^j, T)}{1 - qT} R(T)$$

where $R(T)$ is the reciprocal of the zeta function of the zero dimensional variety defined by the vanishing of $\bar{f}$ i.e. a polynomial with unit root factors. By Weil we know that

$$Z(\tilde{C}_{\bar{f}}, T) = \frac{P(T)}{(1-T)(1-qT)}$$

where $P(T)$ is a polynomial of degree twice the genus g of $\tilde{C}_{\bar{f}}$ with reciprocal roots of complex absolute value $q^{1/2}$. Again by Weil [15, Section 1] we know that $L(\bar{f}, \chi^j, T)$ is a polynomial of degree $d-1$ with reciprocal roots of complex absolute value $q^{1/2}$. (Here we use the fact that since $\gcd(m, d) = 1$ and $m > 1$, the order of the character χ^j does not divide d.) Since $C_{\bar{f}}$ and $\tilde{C}_{\bar{f}}$ differ in only finitely many points their zeta functions differ by a unit root factor. It follows that

$$P(T) = \prod_{j=1}^{m-1} L(\bar{f}, \chi^j, T) \tag{4}$$

and thus $g = (m-1)(d-1)/2$. Note that for m prime this is the product of the Galois conjugates of $L(\bar{f}, T)$ over the mth cyclotomic field. In general it equals $\prod_{1 \neq e | m} \prod_{\theta \in G_e} \theta(L(\bar{f}, \chi^{m/e}, T))$ where G_e is the Galois group of the eth cyclotomic field, although we shall not use this formulation. In Sections 3, 4 and 5 we focus on computing $L(\bar{f}, T)$, indicating the minor changes required for the other factors in (4) in Section 7.4.

3. Analytic representation of multiplicative characters

3.1. p-Adic rings.

Let $\mathbb{Q}_p$ denote the p-adic numbers with ring of integers $\mathbb{Z}_p$. Fix Ω the completion of an algebraic closure of $\mathbb{Q}_p$. Let K denote the unramified extension of $\mathbb{Q}_p$ of degree a, where $q = p^a$, and A the ring of integers of K. Let ord(.) denote the p-adic valuation on Ω normalised so that $\mathrm{ord}(p) = 1$, $|.|$ the corresponding p-adic norm, and τ the Frobenius automorphism of K [19, Section 3].

Let $f \in A[X]$ be the following lifting of the polynomial $\bar{f} \in \mathbb{F}_q[X]$: Write $\bar{f} = \prod_{i=0}^{d-1}(X - \bar{r}_i)$ and define $f(X) = \prod_{i=0}^{d-1}(X - r_i)$ where r_i is the Teichmuller lifting of $\bar{r}_i$. This special lifting is not essential for the theory, but we do have the nice property that $\tau(r_i) = r_i^p$, which is of help in Section 7.3.

Let $K[X, 1/f]$ be the ring of polynomials in X and $1/f$ over K and $K[[X, 1/f]]$ (respectively $A[[X, 1/f]]$) be the space of formal power series in X and $1/f$ over K (over A). Explicitly, $K[[X, 1/f]]$ is the K-space of formal sums $\sum_{i,j} a_{ij}X^i f^j$ where the summation is over $0 \le i < d$ and $j \in \mathbb{Z}$ and each $a_{ij} \in K$. For each rational number $\Delta, \epsilon \ge 0$ denote by $L_{f,\Delta,\epsilon} \subset K[[X, 1/f]]$ the p-adic Banach space [28, Section 1] consisting of all elements

$$\sum_{i,j} a_{ij}X^i f^j$$

where the summation is over $0 \le i < d$, and $j \in \mathbb{Z}$, and we have $a_{ij} \in K$ with (compare [24, pages 843-844])

$$\mathrm{ord}(a_{ij}) + \epsilon j \to \infty \text{ as } j \to -\infty, \tag{5}$$

$$\mathrm{ord}(a_{ij}) - jd\Delta \to \infty \text{ as } j \to +\infty. \tag{6}$$

Note that each $L_{f,\Delta,\epsilon}$ has the structure of a ring, via the usual multiplication and addition rules for power series. Define

$$D_{f,\Delta,\epsilon} := \{x \in \Omega \,|\, \mathrm{ord}(x) \ge -\Delta, \mathrm{ord}(f(x)) \le \epsilon\}.$$

Lemma 3. *The space $L_{f,\Delta,\epsilon}$ is precisely the ring of all power series in $K[[X, 1/f]]$ which converge on the disk $D_{f,\Delta,\epsilon}$.*

Proof. Let $g \in K[[X, 1/f]]$ with $g = \sum a_{ij}X^i f^j$. For $\xi \in D_{f,\Delta,\epsilon}$ we have that g converges at ξ if and only if for every real number $\delta > 0$ there exists only finitely many pairs (i, j) such that $|a_{ij}\xi^i f(\xi)^j| > \delta$. This is true if and only if $|a_{ij}\xi^i f(\xi)^j| \to 0$ as $j \to \infty$ and as $j \to -\infty$. When $\Delta > 0$, picking $\xi \in \Omega$ with $\mathrm{ord}(\xi) = -\Delta$, and thus $\mathrm{ord}(f(\xi)) = -d\Delta$, shows that a_{ij} must satisfy (6). When $\Delta = 0$, choosing ξ with $\mathrm{ord}(\xi) = 0$ and $\mathrm{ord}(f(\xi)) = 0$ again shows that a_{ij} must satisfy (6). Picking $\xi \in \Omega$ with $\mathrm{ord}(f(\xi)) = \epsilon$ and $\mathrm{ord}(\xi) = 0$ shows that a_{ij} must satisfy (5). Thus $g \in L_{f,\Delta,\epsilon}$. Conversely, for $g \in L_{f,\Delta,\epsilon}$ write $g = g^- + g^+$ where the former contains the negative powers of f and the latter the non-negative. Then (6) ensures g^+ converges for any x with $\mathrm{ord}(x) \ge -\Delta$, and (5) ensures g^- converges for any x with $\mathrm{ord}(f(x)) \le \epsilon$. Thus g converges on $D_{f,\Delta,\epsilon}$ as required. □

3.2. **The multiplicative character.** Recall that $m|p-1$ and so in particular m is coprime to p.

Definition 4. *Let* Teich *be the Teichmuller map from* $\mathbb{F}_p^*$ *to* A *and write* $(p-1) = mm'$. *Let* $\chi := \mathrm{Teich}^{m'}$. *So* χ *is a multiplicative character of order* m *on* $\mathbb{F}_p^*$. *Denote by* $\chi_k := \chi \circ \mathrm{Nm}_k$ *the corresponding character on* $\mathbb{F}_{q^k}^*$ *obtained by composing with the norm map.*

The next step is to construct an analytic representation of the map $\chi_k(\bar{f}(\bar{x}))$ on the set $\{\bar{x} \in \mathbb{F}_{q^k} \,|\, \bar{f}(\bar{x}) \neq 0\}$.

Definition 5. *Define the power series* $F, F^{(a)} \in A[[X, 1/f]]$ *as follows:*

$$F(X) := \left(\frac{\tau(f(X^p))}{f(X)}\right)^{\frac{m'}{p-1}} = f(X)^{m'}\left(1 + p\frac{g(X)}{f(X)^p}\right)^{\frac{1}{m}} \tag{7}$$

$$F^{(a)}(X) := \left(\frac{f(X^q)}{f(X)}\right)^{\frac{m'}{p-1}} = f(X)^{m'(q-1)/(p-1)}\left(1 + p\frac{h(X)}{f(X)^q}\right)^{\frac{1}{m}}. \tag{8}$$

Here $\tau(f(X^p)) = f(X)^p + pg(X)$ *and* $f(X^q) = f(X)^q + ph(X)$ *where* $g, h \in A[X]$. *Also, we choose the* m*th root of the rational function so that* $F, F^{(a)} \equiv 1 \bmod p$.

Lemma 6. *We have* $F \in L_{f,\Delta,\epsilon}$ *for any* $\epsilon, \Delta \geq 0$ *with* $\epsilon < 1/p$.

Proof. Expanding (7) using the binomial series we have that

$$F(X) = f(X)^{m'} \sum_{j=0}^{\infty} a_j p^j \left(\frac{g(X)}{f(X)^p}\right)^j$$

where $a_j = \binom{1/m}{j} \in \mathbb{Z}_p$ (since $1/m \in \mathbb{Z}_p$). Writing $F = F^- + F^+$ we see that F^+ is simply a polynomial and so satisfies condition (6) for any choice of $\Delta \geq 0$. The power series F^- satisfies condition (5) for any $\epsilon < 1/p$. □

By Lemma 3, $F(X)$ converges at the Teichmuller lifting x of a point $\bar{x}$ with $\bar{f}(\bar{x}) \neq 0$ (for then $\mathrm{ord}(x) \geq 0$ and $\mathrm{ord}(f(x)) = 0 < 1/p$). One may check that $F^{(a)} = \prod_{i=0}^{a-1} \tau^i(F(X^{p^i}))$, and thus $F^{(a)}$ also converges at these points.

Lemma 7. *For* $\bar{x} \in \mathbb{F}_{q^k}$ *with* $\bar{f}(\bar{x}) \neq 0$ *we have that*

$$\chi_k(\bar{f}(\bar{x})) = F^{(a)}(x)F^{(a)}(x^q)\ldots F^{(a)}(x^{q^{k-1}}).$$

Here $\chi_k = \chi \circ \mathrm{Nm}_k$ *where* χ *is the character of order* m *defined in terms of the Teichmuller map, and* $x := \mathrm{Teich}(\bar{x})$.

Proof. Since $F^{(a)} = (f(X^q)/f(X))^{1/m}$ it follows that

$$\left(F^{(a)}(X)F^{(a)}(X^q)\ldots F^{(a)}(X^{q^{k-1}})\right)^m = f(X^{q^k})/f(X). \tag{9}$$

Let $\bar{x} \in \mathbb{F}_{q^k}$ with $\bar{f}(\bar{x}) \neq 0$ and put $X = x$ where $x := \mathrm{Teich}(\bar{x})$. The bracketted product on the lefthand side of (9) is then an mth root of unity, since $x^{q^k} = x$. Moreover, this bracketted product is equivalent modulo p to

$$f(x)^{m'(q-1)(1+q+\ldots+q^{k-1})/(p-1)} \equiv \mathrm{Teich}^{m'}(\mathrm{Nm}_k(\bar{f}(\bar{x}))) \bmod p$$

and the result follows. □

Corollary 8. *With $F^{(a)}$ as given in Definition 5 and χ_k as in Definition 4 we have*

$$\sum_{\bar{x}\in\mathbb{F}^*_{q^k}} \chi_k(\bar{f}(\bar{x})) = \sum_{x^{q^k-1}=1} F^{(a)}(x)F^{(a)}(x^q)\ldots F^{(a)}(x^{q^{k-1}})$$

where both summations are over points with $\bar{f}(\bar{x}) \neq 0$.

4. The Reich Trace Formula

Definition 9. *Let $\Delta \geq 0$ and $0 \leq \epsilon \leq 1$. Define $L_{\tau(f),\Delta,\epsilon}$ and $D_{\tau(f),\Delta,\epsilon}$ to be usual sets, but with f replaced by $\tau(f)$. For $G \in L_{f,\Delta/p,\epsilon/p}$ let $\tilde{\psi}_p(G)$ be the function on the set $D_{\tau(f),\Delta,\epsilon}$ defined by*

$$\tilde{\psi}_p(G)(x) := \frac{1}{p}\sum_{y^p=x} G(y).$$

Here $\tilde{\psi}_p$ is a linear map. Define $\psi_p := \tau^{-1} \circ \tilde{\psi}_p$, a τ^{-1}-linear map from $L_{f,\Delta/p,\epsilon/p}$ to $L_{f,\Delta,\epsilon}$, and let $\psi_q := \psi_p^a$ a linear map from $L_{f,\Delta/q,\epsilon/q}$ to $L_{f,\Delta,\epsilon}$.

We first prove that the properties claimed in the definition actually hold.

Lemma 10. *First, for $G \in L_{f,\Delta/p,\epsilon/p}$ and $x \in D_{\tau(f),\Delta,\epsilon}$ the function $\tilde{\psi}_p(G)$ converges at x. Thus $\tilde{\psi}_p$ has image in $L_{\tau(f),\Delta,\epsilon}$. Second, $\tilde{\psi}_p$ is a linear map, ψ_p is τ^{-1}-linear and ψ_q is linear, with range as claimed in the definition.*

Proof. Let $y \in \Omega$ with $y^p = x$. Then $\mathrm{ord}(y) \geq -\Delta/p$. First assume that $\mathrm{ord}(y) \geq 0$. Then $f^\tau(x) = f^\tau(y^p) \equiv (f(y))^p \bmod p$ where the superscript notation emphasises that τ acts only on coefficients of $f(X)$. Since $\epsilon \leq 1$ we see that $\mathrm{ord}(f^\tau(x)) \leq 1$ and thus $\mathrm{ord}(f(y)) = \mathrm{ord}(f^\tau(x))/p \leq \epsilon/p$. For $\mathrm{ord}(y) < 0$ we always have that $\mathrm{ord}(f(y)) = d\mathrm{ord}(y) < 0 \leq \epsilon/p$. Thus G converges at y, and the mapping $\tilde{\psi}_p(G)$ is therefore defined at x i.e. $\tilde{\psi}_p(G)$ is a mapping on $D_{\tau(f),\Delta,\epsilon}$. By the explicit method for computing $\tilde{\psi}_p$ in Section 7.3 (see also [21, Lemma 6] and [1, Lemma 1]), the function $\tilde{\psi}_p(G)$ may be identified with a power series in $K[[X, 1/\tau(f)]]$. Therefore by Lemma 3 the map $\tilde{\psi}_p$ has image in $L_{\tau(f),\Delta,\epsilon}$. The linearity for $\tilde{\psi}_p$ claim follows directly from the definition, and the similar claims for ψ_p and ψ_q are immediate (recall τ^{-a} is the identity on K). □

We shall also need the following properties.

Lemma 11. *First, for any $H, G \in L_{f,\Delta,\epsilon}$, where $\Delta \geq 0$, $0 \leq \epsilon \leq 1$, we have*

$$\tilde{\psi}_p(H(X^p)G(X)) = H(X)\tilde{\psi}_p(G(X))$$

and thus

$$\psi_q(H(X^q)G(X)) = H(X)\psi_q(H(X)).$$

Second, the map $\tilde{\psi}_p$ acts on monomials in $L_{f,\Delta,\epsilon}$ as follows:

$$\tilde{\psi}_p(X^u) = \begin{cases} X^{u/p} & \text{if } p|u \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Follows directly from the definitions. □

Theorem 12 (Reich Trace Formula). *For $G \in L_{f,0,0}$ let $\psi_q \circ G$ denote the map composed of multiplication by G followed by the map ψ_q on the p-adic Banach space $L_{f,0,0}$. For $k \geq 1$ let $\mathrm{Tr}((\psi_q \circ G)^k)$ denote the trace of the map $(\psi_q \circ G)^k$ with respect to the orthonormal basis $\{X^i f^j\}$ where $0 \leq i < d$ and $j \in \mathbb{Z}$. Then*

$$(q^k - 1)\mathrm{Tr}((\psi_q \circ G)^k) = \sum G(x)G(x^q)\dots G(x^{q^{k-1}})$$

where the sum is over those $x \in A$ with $x^{q^k-1} = 1$ and $\mathrm{ord}(f(x)) = 0$.

Proof. (We follow the proof of the related theorem given in [3, Section 5].) Using the identity

$$(\psi_q \circ G)^k = \psi_q^k \circ G(X)G(X^q)\dots G(X^{q^{k-1}})$$

we can reduce to the case $k = 1$ (by changing q to q^k and G to the product on the righthand side). By linearity of the trace map we can reduce to the case $G = X^i f^j$ for $0 \leq i < d$ and $j \in \mathbb{Z}$. Let r be a non-negative integer such that $p^r(q-1)+j \geq 0$. Then $f^{p^r(q-1)}G \in A[[X]]$. Define $\beta_r := \psi_q \circ f^{p^r(q-1)}G$ and let β_r' denote this map restricted to $A[[X]]$. By the Dwork Trace Formula [6, Lemma 2]

$$(q-1)\mathrm{Tr}(\beta_r') = \sum_{x^{q-1}=1} f(x)^{p^r(q-1)}G(x) \tag{10}$$

where the trace is with respect to the basis $X^i f^j$ ($0 \leq i < d$, $0 \leq j < \infty$) for $A[[X]]$. Now

$$f(X)^{qp^r} \equiv f(X^q)^{p^r} \bmod p^{r+1}. \tag{11}$$

Define

$$\gamma_r := \psi_q \circ G\left(\frac{f(X^q)}{f(X)}\right)^{p^r} = f(X)^{p^r} \circ \beta \circ \frac{1}{f(X)^{p^r}} \tag{12}$$

where $\beta := \psi_q \circ G$. The second equality follows from Lemma 11. Define $b_{ij} := X^i f^j$ for $0 \leq i < d$ and $j \in \mathbb{Z}$. In what follows below all summations are for $0 \leq k, i < d$ and $l, j \in \mathbb{Z}$ (except when we further insist $j \geq 0$). Write

$$\begin{array}{rcl} \beta_r(b_{ij}) & = & \sum_{k,l} A^{(r)}_{i,j;k,l} b_{kl} \\ \beta(b_{ij}) & = & \sum_{k,l} A_{i,j;k,l} b_{kl}. \end{array}$$

Then from (12)

$$\gamma_r(b_{ij}) = \sum_{k,l} A_{i,j-p^r;k,l-p^r} b_{kl}.$$

From (11) we see that

$$\mathrm{ord}\{(\beta_r - \gamma_r)(b_{ij})\} \geq r+1$$

and so

$$\mathrm{ord}(A^{(r)}_{i,j;k,l} - A_{i,j-p^r;k,l-p^r}) \geq r+1. \tag{13}$$

Now $\{b_{i,j}\}_{0\leq i<d, j\geq 0}$ is a basis for $A[[X]]$ and

$$\mathrm{Tr}(\beta'_r) = \sum_{i,j\geq 0} A^{(r)}_{i,j;i,j}.$$

By (13)

$$\mathrm{ord}(\mathrm{Tr}(\beta'_r) - \sum_{i,j\geq 0} A_{i,j-p^r;i,j-p^r}) \geq r+1.$$

Now

$$\lim_{r\to\infty} \sum_{i,j\geq 0} A_{i,j-p^r;i,j-p^r} = \sum_{i,j} A_{i,j;i,j} = \mathrm{Tr}(\beta). \tag{14}$$

To compute the limit of $\mathrm{Tr}(\beta'_r)$ use the righthand side of (10) and the fact that

$$\lim_{r\to\infty} f(x)^{p^r(q-1)} = \begin{cases} 1 & \text{if } \mathrm{ord}(f(x)) = 0 \\ 0 & \text{if } \mathrm{ord}(f(x)) > 0. \end{cases}$$

The result now follows from (13) and (14). □

Theorem 13. *Let $\Delta \geq 0$ and $0 \leq \epsilon < 1$. Then $\alpha_a := \psi_q \circ F^{(a)}$ and $\alpha := \psi_p \circ F$ are linear and τ^{-1}-linear maps on the ring $L_{f,\Delta,\epsilon}$. Moreover, $\alpha_a = \alpha^a$ and we have*

$$\sum_{\bar{x}\in\mathbb{F}^*_{q^k}} \chi(\bar{f}(\bar{x})) = (q^k - 1)\mathrm{Tr}(\alpha^k_a),$$

and thus

$$L^*(f,T) = \frac{\det(1 - T\alpha_a \,|\, L_{f,\Delta,\epsilon})}{\det(1 - Tq\alpha_a \,|\, L_{f,\Delta,\epsilon})}.$$

Here the trace and determinant are defined via matrices for the maps with respect to an orthonormal basis of $L_{f,\Delta,\epsilon}$. (More simply, one can use the "formal basis" $X^i f^j$ for $j \in \mathbb{Z}, 0 \leq i < d$, see [32, Section 2] *for the definition.)*

Proof. Certainly α and α_a are τ^{-1}-linear and linear respectively, the key point being to show that for $\Delta \geq 0$ and $0 \leq \epsilon < 1$ they are stable on the required space. Since $L_{f,\Delta,\epsilon/p}$ is a ring containing F (Lemma 6) and $L_{f,\Delta,\epsilon}$ we see that the map multiplication by F sends $L_{f,\Delta,\epsilon}$ to $L_{f,\Delta,\epsilon/p}$. The map ψ_p sends $L_{f,\Delta,\epsilon/p}$ to $L_{f,p\Delta,\epsilon} \subset L_{f,\Delta,\epsilon}$ (Lemma 10). Thus the composite map $\psi_p \circ F$ sends $L_{f,\Delta,\epsilon}$ to $L_{f,\Delta,\epsilon}$ as required. The claim on α_a now follows from the identity $\alpha_a = \alpha^a$. The proof that $\alpha_a = \alpha^a$ itself follows from the relation $F^{(a)} = \prod_{i=0}^{a-1} \tau^i(F(X^{p^i}))$ and the fact $\psi_p(H(X^p)G(X)) = \tau^{-1}(H(X))\psi_p(G(X))$ for any $H, G \in L_{f,\Delta,\epsilon}$ (Lemma 11). The final statement follows from Theorem 12 and Corollary 8. □

Define

$$XL_{f,\Delta,\epsilon} := \{Xg \mid g \in L_{f,\Delta,\epsilon}\}.$$

This is precisely the ideal of functions which vanish at $X = 0$. In particular, for G in this space we have that $F^{(a)}G$ vanishes at $X = 0$. From the definition of ψ_q it is immediate that $\psi_q(F^{(a)}G)$ vanishes at 0. Hence α_a is stable on $XL_{f,\Delta,\epsilon}$. Certainly $1 \notin XL_{f,\Delta,\epsilon}$ and any function $G \in XL_{f,\Delta,\epsilon}$ can be written uniquely as $G = G(0).1 + H$ where H vanishes at $X = 0$. Thus we have the direct sum decomposition of vector spaces

$$L_{f,\Delta,\epsilon} = \langle 1 \rangle \oplus XL_{f,\Delta,\epsilon}.$$

With respect to this decomposition, the matrix for α_a has a lower (say) triangular block decomposition. From this it follows that

$$\det(1 - T\alpha_a \mid L_{f,\Delta,\epsilon}) = (1 - F^{(a)}(0)T)\det(1 - T\alpha_a \mid XL_{f,\Delta,\epsilon})$$

and we have from Lemma 7 that $F^{(a)}(0) = \chi(\mathrm{Nm}_1(f(0)))$, since $f(0) \neq 0$. Now with $L(\bar{f}, T)$ as in Section 2 we find that $L(\bar{f}, T) = L^*(\bar{f}, T)(1 - \chi(\mathrm{Nm}_1(f(0)))T)^{-1}$ and thus

Theorem 14. *Let $L(\bar{f}, T)$ be the character sum over the affine line from Section 2. Then for any $\Delta \geq 0$ and $0 \leq \epsilon < 1$ we have*

$$L(\bar{f}, T) = \frac{\det(1 - T\alpha_a \mid XL_{f,\Delta,\epsilon})}{\det(1 - Tq\alpha_a \mid L_{f,\Delta,\epsilon})}.$$

This theorem should be compared with [20, Theorem 19].

5. Reich Cohomology

Unfortunately to derive cohomological formulae the spaces $L_{f,\Delta,\epsilon}$ are not quite large enough. Instead we shall work in the "overconvergent" ring

$$L_f^\dagger := \cup_{\Delta>0,\epsilon>0} L_{f,\Delta,\epsilon}.$$

By Theorem 13 the maps α and α_a are stable on this space. Define

$$XL_f^\dagger := \{Xg \mid g \in L_f^\dagger\}.$$

Note that these are no longer p-adic Banach spaces, but the determinants and traces of certain maps may still be defined in terms of the formal bases and the chain level determinantal formula in Theorem 14 still holds with $L_{f,\Delta,\epsilon}$ replaced by $L_f^\dagger$.

Define the operator D on $K[[X,1/f]]$ as

$$D=\frac{d}{dX}-\frac{1}{m}\frac{f'(X)}{f(X)}\ \left(=f^{1/m}\circ\frac{d}{dX}\circ f^{-1/m}\right).$$

The motivation for the introduction of this operator is similar to [20, Note 20], and explained in [8, Appendix, Eqns (24),(25)]. Notice that d/dX is stable on $L_f^\dagger$, and $-f'/mf\in L_f^\dagger$ and so the operator D is stable on $L_f^\dagger$. Thus $XD:=X\circ D$ maps $L_f^\dagger$ to the ideal $XL_f^\dagger$ of functions which vanish at $X=0$.

Let $\mathcal{L}_f$ be the complex of K-vector spaces

$$\begin{tikzcd} 0 \arrow[r] & L_f^\dagger \arrow[r, "XD"] & XL_f^\dagger \arrow[r] & 0. \end{tikzcd}$$

Denote by H_1 and H_0 the kernel and co-kernel of the map XD.

Proposition 15. *The map XD is injective and so $H_1=0$. Moreover, H_0 is a finite K-vector space of dimension $d-1$. A basis for H_0 may be taken as the set*

$$\{X/f,\dots,X^{d-1}/f\}.$$

Proof. Over the algebraic closure of $K[X,1/f]$ the formal solutions of the first order linear differential equation $XD=0$ is the one-dimensional subspace generated by $f(X)^{1/m}$. But $f(X)^{1/m}\not\in L_f^\dagger$ since $\bar{f}(X)$ is not the mth power of a polynomial over $\mathbb{F}_q$ (it is squarefree). This shows that the restriction of the operator XD to L_f is injective. The second part of the proposition follows from the normal form computations in section 7. □

As in [8, Appendix, Eqn (26)] we have

$$(XD)\circ q\alpha_a=\alpha_a\circ(XD).$$

Thus the map α_a defines a chain map on $\mathcal{L}_f$:

$$\begin{tikzcd} 0 \arrow[r] & L_f^\dagger \arrow[r, "XD"] \arrow[d, "q\alpha_a"] & XL_f^\dagger \arrow[r] \arrow[d, "\alpha_a"] & 0 \\ 0 \arrow[r] & L_f^\dagger \arrow[r, "XD"] & XL_f^\dagger \arrow[r] & 0. \end{tikzcd}$$

Denote by $H_0(\alpha_a)$ and $H_1(q\alpha_a)$ the maps induced on the homology H_0 and H_1 by this chain map, and $\det(1-H_0(\alpha_a)T)$, $\det(1-H_1(q\alpha_a)T)$ the corresponding determinants.

Theorem 16. *The L-function from Theorem 14 satisfies*

$$L(\bar{f},T)=\det(1-H_0(\alpha_a)T).$$

Proof. Exactly as in [20, Theorem 22] using Theorem 14. □

Note 17 Theorem 16 is essentially [8, Eqn (28)] with two minor changes: First, the second module in the complex [8, Eqn (27)] is our $L_f^\dagger$ rather than $XL_f^\dagger$. The extra X just ensures we obtain the L-function over the affine line, rather than over the torus. Second, the polynomial "f" in [8] is actually our $\bar{f}^{(q-1)/m}$, since Adolphson considers a character of order $q-1$. The relation to the equation on [25, Line 10] is similar: in [25] take "g" our $\bar{f}$, "h" to be our $\bar{f}^{(q-1)/m}$, and "f" equals 0. Robba actually assumes "$g(0) = 0$" [25, page 230], but again this is a minor change which just ensures, in our notation, $L(\bar{f}, T) = L^*(\bar{f}, T)$, and so Robba does not need the extra factor X to account for the origin. (Note that we assume $f(0) \neq 0$, so that we can handle the origin in a uniform, if different, way.) One final observation is that in the original work of Reich, slightly smaller spaces were used: essentially power series with "overconvergent" growth at least $\Delta, \epsilon > 1/(p-1)$. This makes the proof of finite dimensionality for H_0 easier, as one can use naive bounds on the denominators introduced in the reduction process (based on [4, Eqn (14)]). Unfortunately, with this approach the factor ϵ from Section 7.2 must be taken to be $\mathrm{ord}(\prod_{i=0}^{\lfloor d/m \rfloor}(i-(d/m)))$, and this impacts on the complexity analysis. As such, we use a more involved approach to bound the denominators (Lemmas 20,21), and may as well then just use the full overconvergent space.

The strategy of the algorithm is to compute the determinant of the map $H_0(\alpha_a)$ on the zeroth homology H_0, up to a suitable modular precision. (This yields the first factor in (4) and the others may be found using a similar approach with minor modifications.) This may be done efficiently via the following lemma, which is an immediate consequence of the identity $\alpha_a = \alpha^a$ from Theorem 13.

Lemma 18. *Let $H_0(\alpha)$ denote the map induced on H_0 by α. Then $H_0(\alpha_a) = H_0(\alpha)^a$.*

It will be enough to compute the p-adic integer coefficients of $\det(1 - H_0(\alpha_a)T)$ modulo p^N for

$$N = \lfloor (m-1)(d-1)(1+a/2) + 1 \rfloor.$$

This follows since the L-function of the exponential sum $L(\bar{f}, \chi^j, T)$ has reciprocal roots whose complex absolute values are $\sqrt{q}$. Thus the coefficient of T^k in the polynomial $\prod_{j=1}^{m-1} L(\bar{f}, \chi^j, T)$ are integers of absolute value at most $\binom{2g}{k} p^{ak/2} \leq 2^{2g} p^{ak/2}$. Since the polynomial $\prod_{j=1}^{m-1} L(\bar{f}, \chi^j, T)$ has degree $2g = (m-1)(d-1)$, it follows that determining the coefficients modulo p^N for $N > (m-1)(d-1)(1+a/2)$ is sufficient. (This choice can be about halved using the functional equation, as in [20, Note 26].)

6. The Algorithm

(For $k \in K$ by "computing k with coefficients determined modulo p^*" we mean finding the coefficients of p^i in its p-adic expansion for $i < *$.)

Algorithm 19 [Kummer Curves]
Input: An equation $Y^m = \bar{f}(X)$ over $\mathbb{F}_q$ where $q = p^a$. We assume that $\bar{f}(0) \neq 0$, $\bar{f}$ is squarefree, m is coprime to $d := \deg(\bar{f})$, and m does divide $p-1$. (In particular this implies $m > 1$ and thus $p \neq 2$.)
Output: The zeta function $Z(\tilde{C}_{\bar{f}}, T)$ of the unique smooth projective curve birational to the affine curve with this equation.

Step 0: Set $N := \lfloor (m-1)(d-1)(1+a/2)+1 \rfloor$, where d is the degree of $\bar{f}$, and define $\tilde{N} := 2(N + \epsilon a d)$ where $\epsilon := \lfloor \log_p(d) \rfloor$.

Step 1: Compute the power series $\tau^{-1}(F)$, where F is given in Definition 5, with coefficients determined modulo $p^{\tilde{N}}$. Let α be the map from on the ring $L_f^\dagger$ (Section 3) defined as $\alpha = \psi_p \circ F = \tilde{\psi}_p \circ \tau^{-1}(F) \circ \tau^{-1}$ (Theorem 13). Let $H_0(\alpha)$ be the map induced on the zeroth homology H_0 of the complex $\mathcal{L}_f$ by α (Section 5).

Step 2: Let $X/f, X^2/f, \ldots, X^{d-1}/f$ be the basis for the zeroth homology H_0. For each basis element e, compute the image $H_0(\alpha)(e) \in H_0$ with coefficients determined modulo $p^{N+\epsilon a(d-1)}$. Construct M, defined as the matrix representing the map $H_0(\alpha)$ with respect to the basis, with coefficients determined modulo $p^{N+\epsilon a(d-1)}$. Specifically, $M = (m_{ij})$ where i is the row index, and j the column index, and $H_0(\alpha)(X^j/f) = \sum_{i=1}^{d-1} m_{ij}(X^i/f) \bmod p^N$ for $1 \leq j \leq d-1$.

Step 3: Compute

$$M_a := M\tau^{-1}(M)\tau^{-2}(M)\ldots\tau^{-(a-1)}(M)$$

modulo $p^{N+\epsilon a(d-1)}$, where the map τ is the lifting of Frobenius to K. Thus M_a is a matrix for the map $H_0(\alpha_a)$. Compute $L(\bar{f}, \chi, T) := \det(1 - M_a T)$ modulo p^N.

Step 4: Repeat steps 1-3 replacing F by F^j and modifying the reduction formulae as explained in Section 7.4 to computed $L(\bar{f}, \chi^j, T)$ for $j = 2, \ldots, m-1$. Output the rational function

$$Z(\tilde{C}_{\bar{f}}, T) := \frac{\prod_{j=1}^{m-1} L(\bar{f}, \chi^j, T)}{(1-T)(1-qT)}.$$

The correctness of the algorithm follows from Equation (4), Theorem 16 and Lemma 18. In Section 7 we will describe exactly how the cohomological reduction in Step 2 is computed, and shall justify the choice of $\tilde{N}$, allowing us to give a complexity analysis of the algorithm in Section 8. This will complete the proof of Theorem 1.

7. Required subroutines

7.1. **Normal Form Computations.** We first consider the space $L_f := K[X, 1/f]$ and the operator D. We shall find a basis for the "algebraic cohomology" $L_f/D(L_f)$ and show that it in fact forms a basis for the "analytic cohomology" $L_f^\dagger/D(L_f^\dagger)$. Finally, the isomorphism $L_f^\dagger/D(L_f^\dagger) \cong XL_f^\dagger/XD(L_f^\dagger)$ is applied.

We first explain how to reduce the function $B(X)/f^k$ where $B(X)$ is a polynomial of degree less than d, and $k > 1$. (In the following paragraph, we mimic the notation in [16, Section 3] to emphasise the parallel.) Since f is squarefree we may write $B(X) = R(X)f(X) + S(X)f'(X)$. Here $\deg(R) \leq \deg(B) + d - 2 \leq 2d - 3$ and $\deg(S) \leq \deg(B) + d - 1 \leq 2d - 2$. Since $k > 1$ we have

$$\frac{B(X)}{f^k} = \frac{R}{f^{k-1}} + \frac{Sf'}{f^k}. \tag{15}$$

Now for any $l \geq 0$

$$0 \equiv D(X^l/f^{k-1}) = \frac{lX^{l-1}}{f^{k-1}} + \left((1-k) - \frac{1}{m}\right)\frac{X^l f'}{f^k}$$

and so

$$\frac{X^l f'}{f^k} = c_k^{-1}\frac{lX^{l-1}}{f^{k-1}} - D(c_k^{-1}X^l/f^{k-1}) \tag{16}$$

where $c_k := ((k-1) + (1/m)) \neq 0$ (since $m > 1$). Using (15) and (16) we find that for $k > 1$

$$\frac{B(X)}{f^k} = \frac{R(X) + c_k^{-1}S'(X)}{f^{k-1}} - D(c_k^{-1}S(X)/f^{k-1}). \tag{17}$$

We have reduced B/f^k to a linear combination of X^i/f^j for $0 \leq i < d$ and $j = k-1$, and $0 \leq i < d-2$ with $j = k-2$. Applying this reduction repeatedly we can reduce all elements $\sum_{k=0}^{L} B_k(X)/f^k$, where $\deg(B_k) < d$ to a linear combination of the terms $X^{d-3}, X^{d-4}, \ldots, X, 1, 1/f, X/f, \ldots, X^{d-1}/f$.

Rational functions B/f with $\deg(B) \geq d-1$ can be reduced to a linear combination of $1/f, X/f, \ldots, X^{d-2}/f$ as follows: For $n \geq 1$ the relation $D(X^n) \equiv 0$ and the fact $n - (d/m) \neq 0$ (since $\gcd(m,d) = 1$ and $m > 1$) is used to reduce $X^{d+(n-1)}/f$. From the relation $D(1) \equiv 0$ we deduce $f'/f \equiv 0$ allowing one to reduce X^{d-1}/f.

We now examine the denominators which occur in this reduction process, using a similar method to [16, Lemma 2]

Lemma 20. *Let $B(X)$ be a polynomial over A of degree at most $d-1$. Then for $k \geq 2$ the reduction of $B(X)/f^k$ becomes integral upon multiplication by $n := p^{\lfloor \log_p(k)+1 \rfloor}$.*

Proof. First note that $n(-k+i-(1/m)) \in A$ for any $1 \leq i \leq k-1$, since $m < p$. Let $C(X)/f$ be the reduction of $B(X)/f^k$ and g the function such that $D(g) = B/f^k - C/f$ with $\deg(C) \leq d-1$. We have

$$D = (d/dX) - (f'/mf) = f^{1/m} \circ (d/dX) \circ f^{-1/m}.$$

It is evident from the first expression for D that $g = \sum_{i=1}^{k-1} g_i(X)/f^i$ for some polynomials $g_i(X)$ with $\deg(g_i) < \deg(f)$. Let a be any root of the polynomial f. We shall take local expansions at the prime $T := (X-a)$. Assuming that $b(\neq a \bmod p)$ is a unit we have $(X-b)^{-1/m} = \sum_{i=0}^{\infty} *T^i$ where each $*$ indicates a p-adic integer, and the coefficient of T^0 is a p-adic unit. Thus $(f/(X-a))^{-1/m} = \sum_{i=0}^{\infty} *T^i$ where each $*$ is a p-adic integer, and the coefficient of T^0, u say, is a unit. Since $d/dX = d/dT$ from the equation $D(g) = B/f^k - C/f$ we deduce

$$T^{\frac{1}{m}} \left(\sum_{i=0}^{\infty} *T^i \right)^{-1} \circ \frac{d}{dT} \circ T^{-\frac{1}{m}} \sum_{i=0}^{\infty} *T^i \left(T^{-(k-1)} \sum_{i=0}^{\infty} g_{a,i} T^i \right)$$

$$= T^{-k} \sum_{i=0}^{\infty} B_{a,i} T^i - T^{-1} \sum_{i=0}^{\infty} C_{a,i} T^i.$$

Here $B_{a,i}$ are p-adic integers since they are just the coefficients in the local expansion of B/f^k at T. Also, the operand on the lefthand side is the local expansion of g, and the final summand on the righthand side that of C/f. Multiplying both sides by an obvious factor we find

$$\frac{d}{dT} \left(T^{-k+1-\frac{1}{m}} \sum_{i=0}^{\infty} *T^i \sum_{i=0}^{\infty} g_{a,i} T^i \right) = \tag{18}$$

$$T^{-k-\frac{1}{m}} \sum_{i=0}^{\infty} *T^i \sum_{i=0}^{\infty} B_{a,i} T^i - T^{-1-\frac{1}{m}} \sum_{i=0}^{\infty} *T^i \sum_{i=0}^{\infty} C_{a,i} T^i. \tag{19}$$

Since no power on the righthand side equals -1, we can integrate this side termwise. We compare the coefficient of $T^{-k+1-\frac{1}{m}}$ on both sides of the integrated equation "$\int (18) dT = \int (19) dT$". We find that $u g_{a,0}$ equals $u B_{a,0}/(-k+1-(1/m))$. Since $B_{a,0}$ is a p-adic integer $n g_{a,0}$ is a p-adic integer for n as in the statement of the lemma. Now $g_{a,0}$ is just the function $g_{k-1}/(f/(X-a))^{k-1}$ evaluated at a, and thus $n g_{k-1}(a)$ is integral. Since this is true for all d roots a of f, by the degree bound on g_{k-1} we must have $n g_{k-1}(X)$ a polynomial over A. Now move the contribution from the term g_{k-1}/f^{k-1} to the righthand side of the integrated equation and compare coefficients of $T^{-k+2-\frac{1}{m}}$ on both sides. We find $u g_{k-2}(a) = u B_{a,1}/(-k+2-(1/m)) + *B_{a,0}/(-k+1-(1/m)) + */n$ where the final $*$ is a p-adic integer coming from the new term $-g_{k-1}/f^{k-1}$ on the righthand side. Once again we see $ng_{k-2}(X)$ is a polynomial over A. Continuing in this way we find $ng_i(X) \in A[X]$ for $i = k-3, k-4, \dots, -1$. Note that since $-k + (k-1) - (1/m) < -1/m$ the possibly non-integral coefficients $C_{a,i}$ never come into play. Thus $ng(X)$ has coefficients in A, as therefore does $nD(g(X)) = B/f^k - C/f$, which completes the proof. □

Lemma 21. *For $B(X) \in A[X]$ of degree l the reduction of $B(X)$ becomes integral upon multiplication by p^r where $r := \max(\lfloor \log_p(d) \rfloor, \lfloor \log_p(l+1) \rfloor)$.*

Proof. As in [16, Lemma 3] we use local expansions at the prime X^{-1}. Specifically, letting C/f be the reduced function and $D(g) = B - (C/f)$ we find using similar notation to before

$$\frac{d}{dX}\left(X^{-\frac{d}{m}} \sum_{i=0}^{\infty} *X^{-i} \sum_{i=0}^{l+1} g_i X^i \right) = X^{-\frac{d}{m}} \sum_{i=0}^{\infty} *X^{-i} \left(\sum_{i=0}^{\infty} B_{l-i} X^{l-i} - \sum_{i=2}^{\infty} C_{-i} X^{-i} \right).$$

Integrating we once again find that all coefficients g_i are integral upon multiplication by n. Therefore so are $g(X)$ and C/f. □

Thus we have shown that $L_f^\dagger / D(L_f^\dagger)$ is isomorphic to the K-vector space spanned by $1/f, X/f, \dots, X^{d-2}/f$. It follows that $XL_f^\dagger / XD(L_f^\dagger)$ is isomorphic to the K-vector space spanned by $X/f, X^2/f, \dots, X^{d-1}/f$.

7.2. **Loss of p-adic accuracy.** Write

$$(\psi_p \circ F)(X^i/f) = \psi_p(X^i f^{m'-1}(1 + (pg/f^p))^{1/m}) = \psi_p(G(X)) + \psi_p(H(X))$$

where $G(X) \in A[X]$ and $H(X) = \sum_{i,j} a_{ij} X^i / f^j$ with $0 \le j < \infty$ and $0 \le i < d$. We have $\mathrm{ord}(a_{ij}) \ge \lceil (j + m' - 1)/p \rceil$. Using [1, Lemma 1] we see that $\psi_p(H(X)) = \sum b_{ij} X^i / f^j$ with $\mathrm{ord}(b_{ij}) \ge j$. (The key estimate one must use is $\lceil (j + m' - 1)/p \rceil \ge \lfloor (j-1)/p \rfloor + 1$.) It follows from Lemma 20 that the reduction of $\psi_p(H(X))$ has integral coefficients. Now $G(X)$ has degree $i + (((p-1)/m) - 1)d$ and so $\psi_p(G(X))$ has degree bound by d/m. From Lemma 21 the reduction of $\psi_p(G(X))$ has coefficients of order at worst $-\epsilon$ where $\epsilon := \lfloor \log_p(d) \rfloor$. Because of this small denominator, to compute the coefficients of the L-function modulo p^N, we need to know the entries in M modulo $p^{N + \epsilon a(d-1)}$. To determine these coefficients it is enough by Lemma 20 to compute F with coefficients determined modulo $\tilde{N}$ where

$$\tilde{N} - \log_p(\tilde{N}) \ge N + \epsilon a(d-1).$$

Taking $\tilde{N} := 2(N + \epsilon a d)$ is sufficient.

7.3. **Computation of the map ψ_p.** Recall that $\psi_p = \tau^{-1} \circ \tilde{\psi}_p$ where $\tilde{\psi}_p$ is a linear map from L_f to $L_{\tau(f)}$. We will see that it is a little time consuming to compute τ^{-1} on large degree rational functions. For this reason, we rewrite $\psi_p = \tilde{\psi}_p \circ \tau^{-1}$ where the former map $\tilde{\psi}_p$ is from $L_{\tau^{-1}(f)}$ to L_f. We explain how to compute this former map on rational functions in $K[X, 1/\tau^{-1}(f)]$, based upon a suggestion of Daqing Wan. Let

$$G := \sum_{i, -L \le j \le L} a_{ij} \frac{X^i}{\tau^{-1}(f)^j} = \frac{h(X)}{\tau^{-1}(f(X))^L}$$

where in the latter we have put everything over a common denominator, and so $h(X)$ is a polynomial of degree $2dL - 1$. We write this as

$$G = \frac{h(X)}{\tau^{-1}(f(X))^L} . \frac{f(X^p)^L}{f(X^p)^L} .$$

Using the property of $\tilde{\psi}_p$ from the first part of Lemma 11 we see that

$$\tilde{\psi}_p(G) = \frac{1}{f(X)^L} \tilde{\psi}_p \left\{ h(X) \left(\frac{f(X^p)}{\tau^{-1}(f(X))} \right)^L \right\} .$$

Factoring $f(X) = \prod_{i=1}^{d-1}(X - r_i)$ we find

$$\frac{f(X^p)}{\tau^{-1}(f(X))} = \prod_{i=0}^{d-1} \frac{X^p - r_i}{X - \tau^{-1}(r_i)} = \prod_{i=0}^{d-1} (X^{p-1} + \tau^{-1}(r_i) X^{p-2} + \ldots + \tau^{-1}(r_i)^{p-1})$$

which is a polynomial, $k(X)$ say, of degree $(p-1)d$ with coefficients in A itself. Here we use the fact that the lifting of $\bar{f}$ was chosen so that $\tau^{-1}(r_i)^p = r_i$ i.e. $\tau(r_i) = r_i^p$. Thus we have

$$\tilde{\psi}_p(G) = \frac{1}{f(X)^L} \tilde{\psi}_p(h(X) k(X)^L).$$

Now we can expand $h(X)k(X)^L$ into a polynomial of degree $2dL - 1 + L(p-1)d$ and compute $\tilde{\psi}_p$ on this polynomial using the second part of Lemma 11.

7.4. **Performing the main steps.** We now describe how to perform the main steps of the algorithms. First, one computes $\tau^{-1}(F)$ with the coefficients determined modulo $p^{\tilde{N}}$ directly from the formula in Definition 5 using the binomial expansion and an iterative formula similar to [16, Section 4]. Specifically, we have the formula

$$\tau^{-1}(F(X)) = \tau^{-1}(f(X))^{m'} \left(1 + p \frac{\tau^{-1}(g(X))}{\tau^{-1}(f(X))^p} \right)^{1/m} .$$

Let $s^{1/m}$ be the second factor. We use [12, Algorithm 9.22] to expand this. In their notation we take "R" equal to $L_{\tau^{-1}(f), *, 1/p}$ (the choice of Δ is not important), the prime "p" equal to our p, "ϕ" the polynomial $Y^m - s$, and initial value "g_0" equals 1. Working with coefficients modulo $p^{\tilde{N}}$, for each basis element e the rational function $G := \psi_p \circ F(e) \bmod p^{\tilde{N}}$ may be constructed. Precisely, we compute it as $\tilde{\psi}_p(\tau^{-1}(F)\tau^{-1}(e))$ where $\tau^{-1}(e) = e$. The reduction method of Section 7.1 is then used to write G as a linear combination of the basis elements $X/f, \ldots, X^{d-1}/f$. Precisely, compute $X^{-1}G$ modulo $p^{\tilde{N}}$ as follows: write $G = G_1 + G_2$ where

$G_1 \in XA[X]$ and $G_2 = * + \sum_{i,j\geq 1} p^j * X^i/f^j$ with the $*$'s p-adic integers. Then $G_2 = a(X)/f^{\tilde{N}-1} + p^{\tilde{N}}*$ where here $*$ indicates a power series with p-adic integer coefficients and $a(X) \in A[X]$. Since $G(0) = 0$, evaluating G, G_1 and G_2 at zero we find that $a(0) \equiv 0 \bmod p^{\tilde{N}}$. Thus $X^{-1}G = X^{-1}G_1 + (X^{-1}a(X))/f^{\tilde{N}} + p^{\tilde{N}}*$. Now reduce $X^{-1}G$ modulo D and multiply the answer by X. In this way the matrix M is found with coefficients determined modulo $p^{N+\epsilon a(d-1)}$. Next, M_a may be computed and the characteristic polynomial found modulo p^N in exactly the same way as in, for example, [20, Section 7.4]. We compute the remaining $L(\bar{f}, \chi^j, T)$ as follows: Modify Steps 0-3, replacing F by F^j and the operator $D = d/dX - f'/mf$ by $d/dX - jf'/mf$. In Equation (16) one must use $c_k := ((k-1)+(j/m))$, with a similar minor change for reducing polynomials. (When reducing polynomials the coefficients $n-(jd/m)$ are non-zero by our assumption $\gcd(m, d) = 1$ and $m > 1$.) Since $\mathrm{ord}(j) = 0$ these changes do not affect any of the estimates. (For m prime direct computation of the conjugates would seem more sensible, but I do not know how to do this.)

8. Complexity Analysis

We assume that all arithmetic operations on rational functions over "truncated" p-adic fields can be performed in soft-Oh linear time in the input size. (By truncated p-adic fields we mean that we disregard the coefficients of suitably large powers of p in the p-adic expansions of elements in K.) First we compute $\tau^{-1}(F)$ with coefficients determined modulo $p^{\tilde{N}}$ using a quadratic Newton iteration, reducing the numerator at each step so the rational function is expressed with respect to the basis $X^i\tau^{-1}(f)^j$, in $\tilde{\mathcal{O}}((pd\tilde{N})(a\tilde{N}))$ bit operations. Second, finding $\psi_p \circ F(e)$ for one basis monomial requires one multiplication, followed by the map $\tilde{\psi}_p$. This latter step may be done in soft-Oh linear time, using the approach of Section 7.3 along with a soft-Oh linear time algorithm for converting between X-adic and f-adic representations (also $\tau^{-1}(f)$-adic representations) of polynomials. (One may do this using a straightforward divide-and-conquer approach, using a fast method for multiplication and division by powers of f [12, Section 9.2].) Thus the complexity of computing $\psi_p \circ F(e)$ for all $d-1$ basis elements is $\tilde{\mathcal{O}}((pd^2\tilde{N})(a\tilde{N}))$ bit operations. Each application of a reduction formula (17) requires $\tilde{\mathcal{O}}(da\tilde{N})$ bit operations (as in [16, Section 5]), and it must be applied $\mathcal{O}(\tilde{N})$ times for each rational function $\psi_p \circ F(e)$. Since there are $d-1$ such functions, the total cost for this is $\tilde{\mathcal{O}}(ad^2\tilde{N}^2)$ bit operations. Finally, to compute M_a from M we can just use ordinary matrix multiplication, combined with a fast "exponentiation" routine, and complete this in $\tilde{\mathcal{O}}(d^3a(N+\epsilon ad))$ bit operations. The determinant may be computed as in [5, Section 4] using a deterministic algorithm based upon the Hessenberg form in $\tilde{\mathcal{O}}(d^3(N+\epsilon ad))$ bit operations. Putting $N = \mathcal{O}(mda), \tilde{N} = \tilde{\mathcal{O}}(mda)$ we get $\tilde{\mathcal{O}}(pa^3d^4m^2)$ bit operations to compute the L-function $L(\bar{f}, T)$. The whole algorithm is repeated $m-2$

times, with minor changes, to find the other L-functions $L(\bar{f}, \chi^j, T)$). This gives a total time of $\tilde{\mathcal{O}}(pa^3d^4m^3)$ bit operations with space complexity in bits $\mathcal{O}(pa^3d^3m^2)$. (For m prime the dependence on m could be reduced to m^2 by computing conjugates directly.)

In the above estimate we have ignored the contributions from the computation of the map τ^{-1}. By the method in [16, Section 5], this may be done on $A/(p^*)$ in $\tilde{\mathcal{O}}(a(a*))$ bit operations, for any positive integer $*$. In the computation of M_a from M, we require $\mathcal{O}(\log(a))$ applications of τ^{-1} to a matrix of side $\mathcal{O}(d)$ whose entries are in K "modulo" $p^{N+\epsilon a(d-1)}$ with p-adic order at least $-\epsilon a$. One may check that this is absorbed in the final bit estimate above. To compute $\psi_p \circ F(e)$ for each basis element e, we just need $\tau^{-1}(F)$ and $\tau^{-1}(e)$. The latter is just e. The only application of τ^{-1} in the former comes from finding $\tau^{-1}(f)$ and $\tau^{-1}(g)$ in the Newton iteration formula. These operations are again absorbed in the above estimate. (Notice that computing τ^{-1} directly on $\tilde{\psi_p} \circ F(e)$ would increase the complexity dependence on a to fourth power.)

9. Relation to Monsky-Washnitzer cohomology

In this section we describe the relation between our approach based upon the Reich Trace Formula and a multiplicative character $\chi(\bar{f}(X))$, and the method of Kedlaya based upon the Monsky-Washnitzer cohomology of the affine curve $Y^m = \bar{f}(X)$ with the divisor of Y removed. We restrict to the case $m = 2$; for $m > 2$ the algorithm in [13] is related in a similar way using our assumption $p \equiv 1 \bmod m$.

The essence of Kedlaya's algorithm is to compute the action of the pth power Frobenius map "$p^{-1}\sigma$" on the "negative eigenspace" of the first Monsky-Washnitzer cohomology group "$H^1(\bar{A}; K)$". Concretely, this group is the spanned by differential forms $\omega_i := X^i dX/Y$ for $i = 0, \ldots, d-2$. The pth power map "$p^{-1}\sigma$" acts on such a form as

$$\frac{X^i dX}{Y} \mapsto \frac{X^{pi+(p-1)}}{Y^p}\left(1 + p\frac{g(X)}{Y^{2p}}\right)^{-1/2} dX.$$

Here $pg(X) = \tau(f(X^p)) - f(X)^p$. This is then reduced to an element in the negative eigenspace using the reduction relations for $k \geq 2$

$$\frac{B(X)dX}{Y^{2k-1}} \equiv \frac{R(X) + (S'(X)/(k-(3/2)))}{Y^{2k-3}} dX \tag{20}$$

where $B(X) = R(X)f(X) + S(X)f'(X)$. The relation $d(X^kY) \equiv 0$ is used to reduce forms $G(X)dX/Y$ with $\deg(G) \geq d-1$. Let M denote the matrix for the map "$p^{-1}\sigma$" with respect to the basis ω_i. (Kedlaya computes σ itself, and so an extra factor of p arises. In fact, in the trace formula of Monsky-Washnitzer it is the inverse map $p\sigma^{-1}$ which appears [16, Theorem 1].)

Returning to our own approach, let inv denote the map on the roots of unity in Ω which sends an element to its inverse. Then the power series

F^{-1} gives an analytic representation of the character $\chi^{-1} := \mathrm{inv} \circ \chi$ of order m, and the theory developed in this paper holds with F replaced by F^{-1}. The map $\alpha := \psi_p \circ F^{-1}$ has a one-sided inverse $\beta := F \circ \phi_p$, where $\phi_p : G(X) \mapsto \tau(G(X^p))$. Precisely, $(\psi_p \circ F^{-1}) \circ (F \circ \phi_p)$ is the identity map on L_f. This induces a one-sided inverse $H_0(\beta)$ to $H_0(\alpha)$ on the cohomology space H_0. Since this is finite dimensional we must also have $H_0(\beta) \circ H_0(\alpha)$ the identity, that is, we have an inverse. Thus $\det(I - H_0(\alpha)T) = \det(H_0(\beta) - T)$, and so we may compute the numerator of the zeta function of $Y^m = \bar{f}(X)$ using β instead of α. Taking $m = 2$ we find that β maps a basis monomial $X^i/f(X)$ for $i = 1, \ldots, d-1$ to

$$\frac{X^{pi}}{\tau(f(X^p))} f(X)^{(p-1)/2} \left(1 + p\frac{g(X)}{f(X)^p}\right)^{1/2} = \frac{X.X^{p(i-1)+(p-1)}}{f(X)^{(p+1)/2}} \left(1 + p\frac{g(X)}{f(X)^p}\right)^{-1/2}.$$

Writing $\tilde{\omega}_i := X^i/f$ for $0 \leq i \leq d-2$ we see that $\beta(X\tilde{\omega}_i) = b_i + XD(c_i)$ where XD is the operator $X(d/dX + f'/mf)$, and b_i is a sum of the $X\tilde{\omega}_j$. Thus $X^{-1} \circ \beta \circ X(\tilde{\omega}_i) = X^{-1}b_i + D(c_i)$ where $X^{-1}b_i$ is a sum of the $\tilde{\omega}_j$. By a trivial adaptation of Section 7.1, reduction via the operator D is performed using the relations for $k \geq 2$

$$\frac{B(X)}{f(X)^k} \equiv \frac{R(X) + (S'(X)/(k - (3/2)))}{f(X)^{k-1}}.$$

(Here the change from F to F^{-1} switches the sign of $1/m$ in the relations in Section 7.1.) This is just Equation (20), only with the denominator terms Y^{2*-1} replaced by $f(X)^*$. Also, the relation $D(X^i) \equiv 0$ can be used to reduce all forms $G(X)/f(X)$ with $\deg(G(X)) \geq d-1$. Letting $\tilde{M}$ denote the matrix for the map β with respect to the basis $X\tilde{\omega}_i$ one can now see that $\tilde{M} = M$. Thus our algorithm and Kedlaya's only really differ in that we essentially compute the inverse map to Kedlaya's twisted in some sense by the operator multiplication by X.

References

[1] A. Adolphson and S. Sperber, Exponential sums on the complement of a hypersurface, Amer. J. Math., **102** No.3, (1980), 461-487.

[2] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, LMS Lecture Note Series 265, Cambridge University Press, 1999.

[3] M. Boyarsky, The Reich Trace Formula, Sociétié Mathématique de France, Astérisque **119-120**, (1984), 129-150.

[4] D.N. Clark, A note on the p-adic convergence of solutions of linear differential equations, Proc. Amer. Math. Soc. **17** (1966), 262-269.

[5] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2, in C. Fieker and D.R. Kohel (eds), ANTS-V, Lecture Notes in Computer Science 2369, Springer-Verlag, (2002), 308-323.

[6] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math., **82**, (1960), 631-648.

[7] B. Dwork, On the zeta function of a hypersurface, Pub. Math. IHES **12**, 1962.

[8] B. Dwork, Lectures on p-Adic Differential Equations, Appendix (by A. Adolphson) L-functions, Springer-Verlag, 1982.

[9] N. Elkies, Elliptic and modular curves over finite fields and related computational issues, in "*Computational perspectives in number theory: Proceedings of a conference in honour of A.O.L. Atkin*" , (D.A. Buell and J.T. Teitelbaum), American Mathematical Society International Press 7, 1998, 21-76.

[10] M. Fouquet, P. Gaudry and R. Harley, An extension of Satoh's algorithm and its implementation, J. Ramanujan Math. Soc. **15**, (2000), 281-318.

[11] M. Fouquet, P. Gaudry and R. Harley, Finding secure curves with the Satoh-FGH algorithm and an early abort strategy, in B. Pfitzmann (ed), Advances in Cryptology - EUROCRYPT 2001, Lecture Notes in Computer Science 2045, Springer-Verlag, (2001), 14-29.

[12] J. von zur Gathen and J. Gerhard, Modern Computer Algebra, Cambridge University Press, 1999.

[13] P. Gaudry and N. Gürel, An extension of Kedlaya's point-counting algorithm to superelliptic curves, in C. Boyd (ed), Advances in Cryptology - ASIACRYPT 2001, Lecture note in Computer Science 2248, Springer-Verlag, (2001), 480-494.

[14] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields, in B. Preneel (ed), Advances in Cryptology - EUROCRYPT 2000, Lecture notes in Computer Science 1807, Springer-Verlag, (2000), 19-34.

[15] N.M. Katz, Estimates for "non-singular" multiplicative character sums, preprint 2001, available at http://www.math.princeton.edu/∼nmk/

[16] K.S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, J. Ramanujan Math. Soc. **16**, (2001), 323-338.
preprint available at http://www.math.berkeley.edu/∼kedlaya/math/index.html

[17] N. Koblitz, p-Adic Numbers, p-Adic Analysis and Zeta Functions, 2nd Edition, Springer, 1984.

[18] N. Koblitz, Hyperelliptic cryptosystems, J. of Cryptology **1**, (1989), 139-150.

[19] A.G.B. Lauder and D. Wan, Counting points on varieties over finite fields of small characteristic, preprint 2001,
available at http://web.comlab.ox.ac.uk/oucl/work/alan.lauder/

[20] A.G.B. Lauder and D. Wan, Computing zeta functions of Artin-Schreier curves over finite fields, London Math. Soc. JCM **5**, (2002), 34-55.

[21] A.G.B. Lauder and D. Wan, Computing zeta functions of Artin-Schreier curves over finite fields II, preprint 2002.
available at http://web.comlab.ox.ac.uk/oucl/work/alan.lauder/

[22] B. Poonen, Computational aspects of curves of genus at least 2, in "*Algorithmic Number Theory II*" (H. Cohen), Lecture Notes in Computer Science 1122, Springer, 1996, 283-306.

[23] D. Reich, p-Adic function spaces and the theory of the zeta function, Princeton University Ph.D. Thesis, 1966.

[24] D. Reich, A p-adic fixed point formula, Amer. J. Math., **91**, (1969), 835-850.

[25] P. Robba, Index of p-adic differential operators III. Applications to twisted exponential sums, Astérique **119-120** (1984), 191-266.

[26] T. Satoh, The canonical lift of an ordinary elliptic curve over a finite fields and its points counting, J. Ramanujan Math. Soc. **15**, (2000), 247-270.

[27] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. **44**, no. 170, (1985), 483-494.

[28] J.-P. Serre, Endomorphisms complètement continus des espaces de Banach p-adique, Pub. Math. IHES **12**, (1962), 69-85.

[29] F. Vercauteren, Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2, in M. Yung (ed), Advances in Cryptology - CRYPTO 2002, Lecture Notes in Computer Science 2442, Springer-Verlag, (2002), 369-384.

[30] F. Vercauteren, B. Preneel and J. Vandewalle, A memory efficient version of Satoh's algorithm, in B. Pfitzmann (ed) Advances in Cryptology - EUROCRYPT 2001, Lecture Notes in Computer Science 2045, Springer-Verlag, (2001), 1-13.

[31] D. Wan, Computing zeta functions over finite fields, Contemporary Mathematics, 225 (1999), 131-141.

[32] D. Wan, Dwork's conjecture on unit root zeta functions, Ann. Math., **150** (1999), 867-927.

[33] D. Wan, Algorithmic theory of zeta functions over finite fields, preprint 2001, available at www.math.uci.edu/∼dwan/preprint.html

Computing Laboratory, Oxford University, Oxford OX1 3QD, UK *E-mail address*: `alan.lauder@comlab.ox.ac.uk`