MÖBIUS CANCELLATION ON POLYNOMIAL SEQUENCES AND THE QUADRATIC BATEMAN-HORN CONJECTURE OVER FUNCTION FIELDS

WILL SAWIN AND MARK SHUSTERMAN

Abstract. We establish cancellation in short sums of certain special trace functions over $\mathbb{F}_q[u]$ below the Pólya-Vinogradov range, with savings approaching square-root cancellation as q grows. This is used to resolve the $\mathbb{F}_q[u]$-analog of Chowla's conjecture on cancellation in Möbius sums over polynomial sequences, and of the Bateman-Horn conjecture in degree 2, for some values of q. A final application is to sums of trace functions over primes in $\mathbb{F}_q[u]$.

Contents

W.S. served as a Clay Research Fellow, and, later, was supported by NSF grant DMS-2101491 while working on this paper.

1. Introduction

1.1. **Quadratic Bateman-Horn.** The history of interest in prime values of integral polynomials dates back at least to Euler, with early conjectural contributions also by Bunyakovsky, Landau, and Schinzel. Quantifying the existing qualitative predictions, Bateman and Horn conjectured that for every irreducible monic polynomial $F(T) \in \mathbb{Z}[T]$, we have

$$|\{X \leq n \leq 2X : F(n) \text{ is prime}\}| \sim \mathfrak{S}(F) \cdot \frac{X}{\log X} \tag{1.1}$$

where

$$\mathfrak{S}(F) = \frac{1}{\deg(F)} \prod_p \frac{1 - \frac{1}{p}|\{x \in \mathbb{Z}/p\mathbb{Z} : F(x) \equiv 0 \bmod p\}|}{1 - \frac{1}{p}}. \tag{1.2}$$

Even though the only completely resolved case is $\deg(F) = 1$, which is the prime number theorem, significant progress on this conjecture has been made in other cases as well. For example, it was shown by Iwaniec in [Iw78] that there are $\gg X/\log X$ integers $n \in [X, 2X]$ for which $n^2 + 1$ is a product of at most two primes. For an exposition of the proof of Iwaniec, a generalization to other quadratic polynomials, and a discussion of related results with $\deg(F) > 2$, we refer to [LO12].

Building and improving on a succession of previous works, Merikoski has shown in [Mer19] that there are infinitely many integers n with n^2+1 having a prime factor exceeding $n^{1.279}$ (or exceeding $n^{1.312}$ if Selberg's eigenvalue conjecture is assumed). Results in this vein have also been obtained in case $\deg(F) > 2$, see for instance [dlB15] and references therein.

Among results on multivariate analogs of the Bateman-Horn conjecture, we would like to mention the work [FI98] of Friedlander-Iwaniec obtaining an asymptotic for the number of primes of the form $n^2 + m^4$, the paper [HM04] by Heath-Brown–Moroz on counting primes represented by bivariate cubic polynomials, and the article [May20] of Maynard on incomplete norm forms. We also refer to [Yau19, BR20] and their references for results on the Bateman-Horn conjecture 'on average over the polynomial F'.

Here we are concerned with the function field analog of the Bateman-Horn conjecture. We fix throughout an odd prime number p and a power q of p. We denote by $\mathbb{F}_q$ the field with q elements. In this function field analogy, the ring $\mathbb{Z}$ is replaced by the univariate polynomial ring $\mathbb{F}_q[u]$. Throughout this work, we use π to denote a prime (monic irreducible) polynomial in $\mathbb{F}_q[u]$. One defines the norm of a nonzero polynomial $f \in \mathbb{F}_q[u]$ to be

$$|f| = q^{\deg(f)} = |\mathbb{F}_q[u]/(f)|, \tag{1.3}$$

where $\deg(f) = \deg_u(f)$ is the degree of f, and (f) is the ideal of $\mathbb{F}_q[u]$ generated by f. The degree of the zero polynomial is negative ∞, so we set its norm to be 0.

Conjecture 1.1. *Let $F(T) \in \mathbb{F}_q[u][T]$ be an irreducible separable monic polynomial with coefficients in $\mathbb{F}_q[u]$. Then we have*

$$|\{g \in \mathbb{F}_q[u] : |g| = X,\ g \textit{ is monic, } F(g) \textit{ is prime}\}| \sim \mathfrak{S}(F) \cdot \frac{X}{\log_q X} \tag{1.4}$$

as $X \to \infty$ through powers of q, and

$$\mathfrak{S}(F) = \frac{1}{\deg_T(F)} \prod_{\pi} \frac{1 - \frac{1}{|\pi|}\,|\{x \in \mathbb{F}_q[u]/(\pi) : F(x) \equiv 0 \bmod \pi\}|}{1 - \frac{1}{|\pi|}}. \tag{1.5}$$

Recall that a polynomial F in the variable T with coefficients from $\mathbb{F}_q[u]$ is *separable* if it is squarefree over an algebraic closure $\overline{\mathbb{F}_q(u)}$ of $\mathbb{F}_q(u)$. For an irreducible polynomial $F(T) \in \mathbb{F}_q[u][T]$ to be separable, it is necessary and sufficient that F is not a polynomial in T^p.

Conjecture 1.1 is a fairly straightforward adaptation of the Bateman-Horn conjecture to function fields, excluding inseparable polynomials over $\mathbb{F}_q[u]$, a family of polynomials that does not have a counterpart over $\mathbb{Z}$. The importance of singling out the inseparable case, which we do not study here, was first highlighted in the works of Conrad-Conrad-Gross who also put forth a version of Conjecture 1.1 for this case in [CCG08, Conjecture 6.2].

Apart from discussing the prior translation of existing results on the Bateman-Horn conjecture from $\mathbb{Z}$ to $\mathbb{F}_q[u]$, see [Pol06, Introduction], Pollack shows that for certain polynomials F in Conjecture 1.1 that do not depend on the variable u (namely $F \in \mathbb{F}_q[T]$), there exist infinitely many monic $g \in \mathbb{F}_q[u]$ for which $F(g)$ is prime. The polynomials g that Pollack substitutes into F are all monomials, so his method does not provide a lower bound that is comparable to the one in Conjecture 1.1.

The main result of this work is the resolution of the function field quadratic Bateman-Horn conjecture over certain finite fields.

Theorem 1.2. *Let p be an odd prime number, and let q be a power of p with $q > 2^{10}3^2e^2p^4$. Then Conjecture 1.1 holds in case $\deg_T(F) = 2$.*

We obtain the asymptotic in Conjecture 1.1 with a power saving error term. For somewhat larger (fixed) values of q, (the exponent of) this power saving is inversely proportional to p^2. We also have uniformity in the quadratic polynomial F, allowing the norm of its coefficients to grow almost as fast as X^2 when q is large, see Theorem 8.1 for a more detailed statement.

Bateman and Horn also made a conjecture for the 'reducible' or 'split' case, predicting simultaneous primality of the values of several irreducible polynomials, which in the case of linear polynomials specializes to the Hardy-Littlewood k-tuple conjecture. For some results in the direction of that conjecture see our previous work [SS19] (and references therein) on which this paper builds. In particular Theorem 1.2 is the nonsplit analog of the twin prime number theorem [SS19, Theorem 1.1], obtained therein under the assumption $q > 685090p^2$. The values of q satisfying Theorem 1.2 are somewhat smaller than those in [SS19, Theorem 1.1] for some very small primes p, but are otherwise larger. This is due to a new kind of difficulty appearing in one of the ranges in the proof of Theorem 1.2, as will be explained later.

One of the difficulties in making progress on the Bateman-Horn conjecture is the parity barrier, or in other words, producing many integers n with $F(n)$ having an odd number of prime factors. This is implicit for example in the aforementioned work [Iw78] whose strategy is sieve-theoretic. We shall now elaborate on this problem and on our resolution of a function field analog.

1.2. **Chowla's conjecture on polynomial sequences.**

In [Ch65, Eq. (341)] Chowla conjectured that for every (monic) squarefree polynomial $F \in \mathbb{Z}[T]$ one should have

$$\sum_{n \leq X} \mu(F(n)) = o(X). \tag{1.6}$$

As in the Bateman-Horn conjecture, the only resolved case is the linear one. For progress with multivariate polynomials F, we refer to works of Helfgott, Frantzikinakis–Host, and others. See [Hel06, FH17, La18] and references therein. Notable progress has also been made by Matomäki, Radziwiłł, Tao, Teräväinen, and many others, in case F splits as a product of linear factors, see [MRT19, Introduction].

Recall that the Möbius function of a polynomial $f \in \mathbb{F}_q[u]$ is 0 if f is divisible by a square of a nonconstant polynomial, and is otherwise given by $(-1)^r$ where r is the number of prime factors of f.

Theorem 1.3. *Fix an odd prime number p, an integer $k \geq 1$, and a power q of p satisfying $q > 4e^2k^2p^2$. Let $F(T) \in \mathbb{F}_q[u][T]$ be a separable polynomial of degree k in T. Then*

$$\sum_{\substack{f \in \mathbb{F}_q[u] \\ |f| \leq X}} \mu\left(F\left(f\right)\right) = o(X), \quad X \to \infty. \tag{1.7}$$

The result builds on and complements [CCG08] which deals with certain squarefree inseparable polynomials F, for which Eq. (1.7) is shown not to hold.

In fact, we obtain Eq. (1.7) with a power saving. This saving approaches $\frac{1}{2p}$ for fixed p and growing q. Moreover we can take the coefficients of F to be as large as any fixed power of X, by allowing some increase in q. An effective error term and wide uniformity in F are crucial (but not quite sufficient on their own) in our approach to establishing Theorem 1.2. We could likely obtain a similar cancellation in case the sum in Eq. (1.7) is restricted to prime polynomials $f \in \mathbb{F}_q[u]$, following [SS19, Corollary 6.1].

An analog of Conjecture 1.1 and Theorem 1.3, not considered in this work, is to fix X and let $q \to \infty$ (thus allowing F to change as well). Refining many previous works, Entin in [Ent16, Ent21] and then Kowalski in [Kow16] resolved the 'large finite field' variants of Conjecture 1.1 and Chowla's conjecture on polynomial sequences, obtaining an error term of size $O(q^{-\frac{1}{2}})$ with the implied constant depending on X. It is plausible that our arguments can be used to obtain superior error terms for certain special cases of these works.

Our proof of Theorem 1.3 also builds on and refines arguments from the proof of [SS19, Theorem 1.3] where F is assumed to be a product of (distinct) linear factors. The power savings and uniformity in F obtained here are similar to those in [SS19]. What follows is an overview of our proof of Theorem 1.3, which leads to the technical heart of our work - cancellation in short sums of trace functions.

We start, as in [SS19], by restricting in Eq. (5.11) to subsums over polynomials $f \in \mathbb{F}_q[u]$ sharing the same derivative, obtaining an equality of the form

$$\sum_{f} \mu(F(f)) = \sum_{r} \sum_{s} \mu(F(r + s^p))$$

with the goal of obtaining cancellation in the inner sum, for almost every r. Applying Pellet's formula from Eq. (4.85) to write the value of the Möbius function in Eq. (4.87) as a (quadratic) character of the resultant of the values at f of a pair of bivariate polynomials closely related to F and the aforementioned derivative. The outcome is an expression of the form

$$\sum_s \mu(F(r+s^p)) \approx \sum_s \chi_2(\mathrm{Resultant}(F(r+s^p), F_{\nabla r}(r+s^p)))$$

for the polynomial $F_{\nabla r}$ from Eq. (4.69) that depends on F and on the derivative ∇r of r.

This allows us to restate a good deal of the arithmetic problem in terms of the geometry of the two plane curves given by the vanishing loci of our pair $(F, F_{\nabla r})$ of bivariate polynomials, a strategy successfully employed in previous works on factorization statistics of polynomials over finite fields by Conrad-Conrad-Gross, Entin, Kowalski, and others.

Adapting a result from [CCG08], we obtain in Lemma 4.6 an expression for the above resultant in terms of the intersection numbers of our curves. We can then write in Proposition 4.9 a character of our resultant as a Jacobi symbol. To make matters more explicit (yet simplified), let us say that we find $W \in \mathbb{F}_q[u][T]$ and a squarefree $M \in \mathbb{F}_q[u]$ (depending on F and on r) such that

$$\sum_s \chi_2(\mathrm{Resultant}(F(r+s^p), F_{\nabla r}(r+s^p))) \approx \sum_s \left(\frac{W(s)}{M}\right).$$

Our problem becomes that of obtaining cancellation for very short sums in the étale $\mathbb{F}_q$-algebra $\mathbb{F}_q[u]/(M)$ of Jacobi symbols of the form

$$\sum_s \left(\frac{W(s)}{M}\right). \tag{1.8}$$

The problem of cancellation in short multiplicative character sums with W linear in s has been addressed in [SS19, Theorem 1.4], going below the Burgess range. The vanishing cycles argument used in the proof of that theorem, reducing the problem to bounds of Weil and Deligne, turns out to be insufficient for controlling Eq. (1.8) in part due to the lack of multiplicativity in s for a nonlinear polynomial W. Indeed, obtaining significant cancellation in Eq. (1.8) for general W remains out of our reach. We refer to [Saw20, Section 4, 4.3] for a further discussion of vanishing cycles in this context.

Sums as in Eq. (1.8) have been studied, over the integers, in several works of Burgess such as [Bur], and for multivariate integral polynomials W in [MC09]. Burgess works with prime M, and obtains stronger results under the assumption that W has a linear factor or even splits completely.

Although the arguments of Burgess are probably not directly applicable to getting cancellation in sums as short as ours, along analogous lines we are able, after making a linear change of variable in the original polynomial F, to show that the vast majority of our fixed derivative subsums give rise to short character sums with a prime factor of M mod which W is a power of a linear polynomial. This involves an application of a quantitative form of

Hilbert's irreducibility theorem due to S. D. Cohen from [Coh81] as adapted to a function field setting by Bary-Soroker and Entin in [BSE21].

The most novel part of our work is in establishing cancellation in sums satisfying this assumption on W and M, and more general short sums of certain special *trace functions* that arise in our approach to proving Theorem 1.2, which we now discuss.

1.3. **Strategy for proving the main result.** To prove Theorem 1.2, or rather its stronger form in Theorem 8.1, we use a convolution identity expressing the indicator of primes in terms of the Möbius function. As is often the case, it is more convenient to work with the von Mangoldt function

$$\Lambda(f) = \begin{cases} \deg(\pi), & f = \pi^m \text{ for some integer } m \geq 1 \text{ and prime } \pi \in \mathbb{F}_q[u] \\ 0, & \text{otherwise} \end{cases}$$

instead of the indicator function of primes. The aforementioned convolution identity gives something of the form

$$\sum_{|f|\sim X} \Lambda(F(f)) \approx \sum_{\substack{A \\ AB=F(f)}} \sum_{B} \mu(A)$$

the precise form appearing in Eq. (8.5).

Roughly speaking, this introduces three different ranges of summation. In the first range, where $|A| < X$, we manipulate with Euler products and use classical bounds for L-functions to single out and calculate the singular series main term of Theorem 1.2 - see the treatment of Eq. (8.21) in the proof of Theorem 8.1. For the second range, where $|A| > X^{1+\epsilon}$ for some fixed $\epsilon > 0$, a uniform version of Theorem 1.3 with a power saving cancellation is sufficient. (In fact, it would suffice to have aversion of Theorem 1.3 with logarithmic savings, as long as it holds uniformly for polynomials F with coefficients of size a reasonable power of X, but our methods naturally give a power savings.) This part of our approach is similar to arguments from [SS19], one difference is the need of a greater uniformity here.

A more significant difference is that in [SS19] the third range, where $X < |A| < X^{1+\epsilon}$ did not present substantial difficulties, because a similar problem has already been handled by Fouvry and Michel over $\mathbb{Z}$, see [FM98]. Here however, in the third range we need (roughly speaking) to count (with good savings) the number of values of a quadratic polynomial having a prime factor of size somewhat larger than their square root. This problem has not yet been resolved over $\mathbb{Z}$, and we refer to the aforementioned work [Mer19] for upper bounds and a discussion of the possibility of further progress.

In our solution of the problem over $\mathbb{F}_q[u]$, we first follow a strategy similar to some parts of [Mer19], applying Poisson summation, completion, and the theory of binary quadratic forms. This approach has its roots in the work [Hoo63] of Hooley. Due to the lack of an appropriate reference, and our desire to obtain Theorem 1.2 with significant uniformity, we develop for that matter the necessary parts of binary quadratic form theory over function fields. This allows us to reduce the problem in the third range to a version of Theorem 1.3 twisted by a Kloosterman fraction, see Theorem 5.1 for a more general twisted sum.

Our approach to proving Theorem 1.3 is also helpful for its twisted variants, leading again to short sums of trace functions. One difference is that in the twisted case the modulus of the resulting exponential sum is not squarefree, so we use a simple sieve in Corollary 5.3 to reduce to squarefree moduli.

1.4. **Trace functions.** In various works, Fouvry, Kowalski, and Michel highlighted the importance of *trace functions* to number theory over the integers, see for instance [FKMS19]. These are functions on the integers modulo a prime p, equivalently, functions on the integers that are periodic with period p, that arise from the trace of Frobenius on an ℓ-adic sheaf on the affine line over $\mathbb{F}_p$. Examples include multiplicative characters, additive characters, compositions of multiplicative characters or additive characters with rational functions, Kloosterman sums such as

$$t(x) = \frac{1}{\sqrt{p}} \sum_{\substack{a,b \in \mathbb{F}_p^\times \\ ab = x}} e\left(\frac{a+b}{p}\right), \quad e(y) = e^{2\pi i y}, \tag{1.9}$$

compositions of Kloosterman sums with rational functions, and products or sums of any of these functions. Despite this vast generality, it is possible to obtain nontrivial results for all (or almost all) trace functions.

More generally, as in [WX16], one can work with periodic functions with squarefree period, which are products of trace functions modulo distinct primes. These behave similarly to trace functions, although most results have not yet been proven at this level of generality.

We define trace functions over $\mathbb{F}_q[u]$ in an analogous way, as functions on $\mathbb{F}_q[u]/(\pi)$ for a prime $\pi \in \mathbb{F}_q[u]$ arising from sheaves on $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$, or products of these for distinct primes π.

Definition 1.4. Fix throughout an auxiliary prime number ℓ different from p and an embedding $\iota \colon \overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$. We work with the abelian category of constructible $\overline{\mathbb{Q}_\ell}$-sheaves on a variety in characteristic p, see [KR14, Part 2, Section 8], and call its objects simply 'sheaves'. Let $\pi \in \mathbb{F}_q[u]$ be a prime, and let $\mathcal{F}$ be a sheaf on $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$. We can think of any $x \in \mathbb{F}_q[u]/(\pi)$ as a point on $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$ and thus as a map

$$x \colon \operatorname{Spec}(\mathbb{F}_q[u]/(\pi)) \to \mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}. \tag{1.10}$$

For a geometric point $\overline{x}$ over x, the stalk $\mathcal{F}_{\overline{x}}$ of $\mathcal{F}$ at $\overline{x}$ is the underlying finite-dimensional vector space over $\overline{\mathbb{Q}_\ell}$ of the pullback $x^*\mathcal{F}$ of $\mathcal{F}$ to $\operatorname{Spec}(\mathbb{F}_q[u]/(\pi))$. This vector space is equipped with a linear action of $\mathrm{Frob}_{q^{\deg(\pi)}}$, so we can define

$$t \colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C}, \quad t(x) = \iota(\mathrm{tr}(\mathrm{Frob}_{q^{\deg(\pi)}}, \mathcal{F}_{\overline{x}})) \tag{1.11}$$

independently of the choice of $\overline{x}$.

A function t as above is called a *trace function*, and is sometimes denoted by $t_{\mathcal{F}}$ in order to emphasize that t arises from $\mathcal{F}$ via Eq. (1.11). On other occasions, we omit $\mathcal{F}$ when mentioning t, making the dependence of t on $\mathcal{F}$ implicit. There is usually an obvious choice of $\mathcal{F}$ for a given trace function t, so confusion is unlikely. It is at times convenient to think of t as a π-periodic function on $\mathbb{F}_q[u]$. In the sequel, abusing notation we drop ι from our formulas.

Note that the construction above suggests an extension of the function t to any finite field extension κ of $\mathbb{F}_q[u]/(\pi)$, by considering the action of $\mathrm{Frob}_{|\kappa|}$ on $\mathcal{F}_{\overline{x}}$ for every κ-valued point x of $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$. One says that $\mathcal{F}$ is punctually pure of weight $w \in \mathbb{R}$ if for every κ-valued point x of $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$, all the eigenvalues of $\mathrm{Frob}_{|\kappa|}$ on $\mathcal{F}_{\overline{x}}$ are of absolute value $|\kappa|^{\frac{w}{2}}$. The sheaf $\mathcal{F}$ is said to be mixed of nonpositive weights if there exist a nonnegative integer r, nonpositive real numbers $w_1, \dots, w_r$, and a filtration of $\mathcal{F}$ by subsheaves

$$0 = \mathcal{F}^{(0)} \subseteq \mathcal{F}^{(1)} \subseteq \cdots \subseteq \mathcal{F}^{(r)} = \mathcal{F} \tag{1.12}$$

such that the sheaf $\mathcal{F}^{(i)}/\mathcal{F}^{(i-1)}$ is punctually pure of weight w_i for every $1 \leq i \leq r$.

Set $\kappa = \mathbb{F}_q[u]/(\pi)$, let η be a generic point of $\mathbb{A}^1_\kappa$, and let

$$j \colon \mathrm{Spec}(\kappa(X)) \to \mathrm{Spec}(\kappa[X]) = \mathbb{A}^1_\kappa \tag{1.13}$$

be the map arising from the inclusion of $\kappa[X] \hookrightarrow \kappa(X)$. Then $j^*\mathcal{F}$ equips the stalk $\mathcal{F}_{\overline{\eta}}$ with the structure of a continuous finite-dimensional representation of $\mathrm{Gal}(\kappa(X)^{\mathrm{sep}}/\kappa(X))$ over $\overline{\mathbb{Q}_\ell}$. We call $\dim_{\overline{\mathbb{Q}_\ell}} \mathcal{F}_{\overline{\eta}}$ the (generic) rank of $\mathcal{F}$, or the rank of t, and denote it by either $\mathbf{r}(\mathcal{F})$ or $r(t)$.

Every closed point $x \in \mathbb{P}^1_\kappa$ defines a valuation on $\kappa(X)$, which we can extend (non-uniquely) to a valuation v_x on $\kappa(X)^{\mathrm{sep}}$. The closed subgroup

$$D_x = \{\sigma \in \mathrm{Gal}(\kappa(X)^{\mathrm{sep}}/\kappa(X)) : v_x \circ \sigma = v_x\} \tag{1.14}$$

fits into an exact sequence of profinite groups

$$1 \to I_x \to D_x \to \mathrm{Gal}(\overline{\kappa(x)}/\kappa(x)) \to 1. \tag{1.15}$$

We call I_x the inertia subgroup of $\mathrm{Gal}(\kappa(X)^{\mathrm{sep}}/\kappa(X))$ at x, and note that it is well-defined up to conjugation. We let P_x be a (unique) p-Sylow subgroup of I_x, and call it the wild inertia subgroup at x. We say that $\mathcal{F}$ is unramified (respectively, tamely ramified) at x if I_x (respectively, P_x) acts trivially on $\mathcal{F}_{\overline{\eta}}$. For $x \in \mathbb{P}^1_\kappa$, we denote by $\mathbf{sw}_x(\mathcal{F})$ the swan conductor of $\mathcal{F}$ at x, a nonnegative integer associated to the action of P_x on $\mathcal{F}_{\overline{\eta}}$. In particular, it is zero if and only if the action of P_x is trivial. For a thorough exposition of this notion see [KR14, Section 4].

We say that the trace function t (or the sheaf $\mathcal{F}$) is *infinitame* if $\mathcal{F}$ is tamely ramified at $\infty \in \mathbb{P}^1_\kappa$, mixed of nonpositive weights, and has no finitely supported sections. The latter condition means that for every étale map

$e\colon U \to \mathbb{A}^1_\kappa$, and every section s of $\mathcal{F}$ over U, the support of s

$$\operatorname{Supp}(s) = \{x \in U : s_{\overline{x}} \neq 0 \text{ in } \mathcal{F}_{\overline{x}}\} \tag{1.16}$$

is infinite. This is equivalent to the vanishing of the cohomology group $H^0_c(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{F})$, since any compactly supported global section can be decomposed into sections supported at individual points.

We define the conductor of an infinitame trace function t (or of the sheaf giving rise to it) to be the nonnegative integer

$$c(t) = c(\mathcal{F}) = \sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa](\mathbf{r}(\mathcal{F}) - \dim(\mathcal{F}_{\overline{x}}) + \mathbf{sw}_x(\mathcal{F})) \tag{1.17}$$

where the sum is taken over closed points, and the dimension is over $\overline{\mathbb{Q}_\ell}$.

Remark 1.5. The assumption that $\mathcal{F}$ is mixed of nonpositive weights is merely a normalization condition capable of capturing all of the examples that are of interest. It implies that $|t(x)| \leq r(t)$ for every $x \in \mathbb{F}_q[u]/(\pi)$. The technical assumption that $\mathcal{F}$ has no finitely supported sections guarantees that the conductor defined above has certain desirable properties. This assumption could easily be removed since the finitely supported sections of a sheaf contribute to only finitely many values of the trace function, and these values can be handled separately for most purposes, but it would make the formulas involving the conductor more complicated.

On the other hand, the assumption that $\mathcal{F}$ is tamely ramified at infinity is a substantive restriction necessitated by our methods of proof, and is (to some extent) suggested by the trace functions arising in the proofs of Theorem 1.2 and Theorem 1.3.

Remark 1.6. The definition of the conductor of t almost matches the logarithm to base $|\kappa|$ of the (global) Artin conductor of the Galois representation $\mathcal{F}_{\overline{\eta}}$, defined as

$$\prod_{x \in |\mathbb{A}^1_\kappa|} |\kappa(x)|^{\mathbf{r}(\mathcal{F}) - \dim(\mathcal{F}_{\overline{\eta}}^{I_x}) + \mathbf{sw}_x(\mathcal{F})}. \tag{1.18}$$

Note that there is a natural map $\mathcal{F}_{\overline{x}} \to \mathcal{F}_{\overline{\eta}}^{I_x}$ whose injectivity is equivalent to $\mathcal{F}$ having no sections supported at x. Hence, if $\mathcal{F}$ has no finitely supported sections, all these maps are injections. If $\mathcal{F}$ is moreover a middle extension sheaf, then these maps are isomorphisms. Hence the conductor of t is an adaptation of the Artin conductor to infinitame trace functions.

This notion differs from the complexity defined in [SFFK21] by $O(\mathbf{r}(\mathcal{F}))$, see [SFFK21, Theorem 7.3(2)]. This $O(\mathbf{r}(\mathcal{F}))$ factor is not greatly significant, and either definition of conductor/complexity could be used in this paper, but we chose a definition that is as easy as possible to use in our arguments and gives a reasonably good bound, since it can be detected by test-sheaves that are well suited to our inductive strategy in §3.2. It follows that our conductor differs at most quadratically from the conductor defined by Fouvry, Kowalski, and Michel in [FKM15, Definition 1.13], see [SFFK21, Corollary 7.4], so changing to that conductor would require squaring the conductor in the estimates.

Example 1.7. Let $\pi \in \mathbb{F}_q[u]$ be a prime, let

$$\chi\colon (\mathbb{F}_q[u]/(\pi))^\times \to \mathbb{C}^\times, \tag{1.19}$$

be a nonprincipal Dirichlet character, let $a \in (\mathbb{F}_q[u]/(\pi))^\times$ be a scalar, and let $b \in \mathbb{F}_q[u]/(\pi)$ be a shift. After constructing the Kummer sheaf

$$\mathcal{F} = \mathcal{L}_\chi(aT + b) \tag{1.20}$$

on $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$, we will see that the function

$$t\colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C}, \quad t(x) = \begin{cases} \chi(ax+b) & x \neq -ba^{-1} \\ 0 & x = -ba^{-1} \end{cases} \tag{1.21}$$

is an infinitame trace function with $r(t) = c(t) = 1$. We call t a *Dirichlet trace function.*

Definition 1.8. For a squarefree polynomial $g \in \mathbb{F}_q[u]$, we say that

$$t\colon \mathbb{F}_q[u]/(g) \to \mathbb{C} \tag{1.22}$$

is a (g-periodic) *trace function* if there exist trace functions

$$t_\pi\colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C} \tag{1.23}$$

for each prime factor π of g such that

$$t(x) = \prod_{\pi \mid g} t_\pi(x \bmod \pi), \quad x \in \mathbb{F}_q[u]/(g). \tag{1.24}$$

We say that t is *infinitame* if t_π is for each $\pi \mid g$, and define

$$r(t) = \max_{\pi \mid g}\{r(t_\pi)\}, \quad c(t) = \max_{\pi \mid g}\{c(t_\pi)\}. \tag{1.25}$$

We will use the notation $\mathcal{F}_\pi$ for a sheaf giving rise to the trace function t_π via Eq. (1.11). This means that $\mathcal{F}_\pi$ is a sheaf with $t_{\mathcal{F}_\pi} = t_\pi$.

The following trace functions appear in the proofs of Theorem 1.2 and Theorem 1.3.

Example 1.9. Let $g \in \mathbb{F}_q[u]$ be squarefree, let $\chi\colon (\mathbb{F}_q[u]/(g))^\times \to \mathbb{C}^\times$ be a multiplicative character, and let $\psi\colon \mathbb{F}_q[u]/(g) \to \mathbb{C}^\times$ be an additive character. Let $a(T)$ be a nonconstant polynomial with coefficients in $\mathbb{F}_q[u]/(g)$, and define

$$t\colon \mathbb{F}_q[u]/(g) \to \mathbb{C}, \quad t(x) = \begin{cases} 0 & a(x) \notin (\mathbb{F}_q[u]/(g))^\times \\ 0 & x \notin (\mathbb{F}_q[u]/(g))^\times \\ \chi(a(x))\psi\left(\frac{1}{x}\right) & \text{otherwise.} \end{cases}$$

The function t is an infinitame trace function with

$$r(t) = 1, \quad c(t) \leq \deg(a) + 2. \tag{1.26}$$

The first problem about trace functions one usually studies is that of obtaining cancellation in the complete sum

$$\sum_{x \in \mathbb{F}_q[u]/(\pi)} t(x) \tag{1.27}$$

for a trace function $t \colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C}$. For infinitame trace functions this is carried out, using standard tools, in Proposition 9.2.

The following is our main result on trace functions, a significant cancellation in very short sums of infinitame trace functions with a 'Dirichlet component'.

Theorem 1.10. *Let $g \in \mathbb{F}_q[u]$ be a squarefree polynomial, and let t be an infinitame g-periodic trace function. Suppose that there exists a prime $\pi \mid g$ for which t_π is a Dirichlet trace function. Then*

$$\sum_{\substack{f \in \mathbb{F}_q[u] \\ |f| < X}} t(f) \ll X^{\frac{1}{2}} |g|^{\log_q(2r(t)+c(t))}, \quad X, |g| \to \infty \tag{1.28}$$

with the implied constant depending only on q.

In applications, the quantities $r(t), c(t)$ are typically bounded, so for large (but fixed) q we get arbitrarily close to square-root cancellation in intervals as short as $X = |g|^\epsilon$, for any fixed $\epsilon > 0$. The reason for working with the kind of trace functions in Theorem 1.10 is that it seems to be the simplest family of functions to which we can reduce Eq. (1.8) (and its twisted variants) under the additional assumption on W and M discussed earlier. Indeed Theorem 1.10 is a crucial input to our proofs of Theorem 1.2 and Theorem 1.3. It would of course be desirable to treat trace functions of sheaves which are neither tamely ramified at infinity, nor necessarily related to Dirichlet characters.

A predecessor of Theorem 1.10 is [SS19, Theorem 2.1] proven under the assumption that t_π is a Dirichlet trace function for every $\pi \mid g$, namely that t is a shifted Dirichlet character. The vanishing cycles argument used to prove that result produces comparable bounds, but its application beyond the (shifted) multiplicative scenario remains challenging.

Over the integers, bounds for short sums of trace functions are in general not available beyond the Pólya-Vinogradov range $X \geq |g|^{\frac{1}{2}}$. We refer to [FKMRRS17] for recent developments in this direction. For the function field version of the Pólya-Vinogradov argument see Corollary 9.3.

We now give some examples demonstrating that, even though the assumptions in Theorem 1.10 are perhaps not strictly necessary, some restrictions on the trace functions are required.

Example 1.11. The constant function $t(x) = 1$ for $x \in \mathbb{F}_q[u]/(\pi)$ is an infinitame trace function of rank 1 and conductor 0, arising from the constant sheaves $\mathcal{F}_\pi = \overline{\mathbb{Q}_\ell}$. This is not a Dirichlet trace function, and the conclusion of Theorem 1.10 clearly fails in this case.

Example 1.12. We use here exponentiation on $\mathbb{F}_q(u)$ as reviewed in Section 2.4.1. Let $\tau, \pi \in \mathbb{F}_q[u]$ be distinct primes, and let $\chi\colon (\mathbb{F}_q[u]/(\tau))^\times \to \mathbb{C}^\times$ be a nontrivial character. Take $\overline{\pi} \in \mathbb{F}_q[u]$ satisfying $\pi\overline{\pi} \equiv 1 \mod \tau$, and define the trace function

$$t\colon \mathbb{F}_q[u]/(\tau\pi) \to \mathbb{C}, \quad t(x) = \chi(x) e\left(\frac{\pi\overline{\pi}-1}{\tau} \cdot \frac{x}{\pi}\right). \tag{1.29}$$

This trace function satisfies $r(t) = 1, c(t) = 1$, and all the assumptions of Theorem 1.10 except that $\mathcal{F}_\pi$ is not tamely ramified at infinity.

For X such that $|\tau| \le X \le \frac{|\tau\pi|}{q}$, we use properties of the exponential function to compute

$$\begin{aligned}\sum_{\substack{f\in\mathbb{F}_q[u]\\|f|<X}} t(f) &= \sum_{\substack{f\in\mathbb{F}_q[u]\\|f|<X}} \chi(f) e\left(\frac{\overline{\pi}f}{\tau} - \frac{f}{\tau\pi}\right) = \sum_{\substack{f\in\mathbb{F}_q[u]\\|f|<X}} \chi(f) e\left(\frac{\overline{\pi}f}{\tau}\right) e\left(-\frac{f}{\tau\pi}\right)\\ &= \sum_{\substack{f\in\mathbb{F}_q[u]\\|f|<X}} \chi(f) e\left(\frac{\overline{\pi}f}{\tau}\right) = \frac{X}{|\tau|} \sum_{x\in\mathbb{F}_q[u]/(\tau)} \chi(x) e\left(\frac{\overline{\pi}x}{\tau}\right).\end{aligned}$$

Since the Gauss sum appearing in the last formula has absolute value $|\tau|^{1/2}$, taking $|\tau|$ to be very small compared to $|\pi|$, we get barely any cancellation, so Eq. (1.28) does not hold.

1.4.1. *The geometric strategy.* Our proof of Theorem 1.10 relies on the theory of sheaves and trace functions on higher-dimensional varieties, see [IK04, 11.11] for an exposition covering applications to analytic number theory. We view the set of polynomials $f \in \mathbb{F}_q[u]$ with $|f| < X$ as the $\mathbb{F}_q$-points of an n-dimensional affine space, with one coordinate for each coefficient of the polynomial. We then construct in Corollary 3.14 a sheaf $\overline{\mathcal{F}}$ on this space whose trace of Frobenius at each point is $t(f)$. The construction uses the tensor direct image functor defined in [RL20].

Sheaves on higher-dimensional spaces are potentially much more complicated objects than the individual sheaves $\mathcal{F}_\pi$ (on $\mathbb{A}^1$) used to define t, but $\overline{\mathcal{F}}$ can be constructed from the base changes $\mathcal{F}_i$ of the $\mathcal{F}_\pi$ along $\mathbb{F}_q$-embeddings of $\mathbb{F}_{q^{\deg(\pi)}}$ into $\overline{\mathbb{F}_q}$, as a tensor product of pullbacks along (linear) evaluation maps $\{e_i\}_{i=1}^m$ at the roots $x_1, \dots, x_m$ of g in $\overline{\mathbb{F}_q}$. This tensor product decomposition, given in Eq. (3.85), is made possible by the factorizability into distinct linear factors $u - x_i$ over $\overline{\mathbb{F}_q}$ of the period g of the trace function t.

Our tensor product construction exhibits $\overline{\mathcal{F}}$ as a lisse sheaf on $\mathbb{A}^n_{\overline{\mathbb{F}_q}}$ away from the inverse images under the e_i of the finitely many points where each $\mathcal{F}_i$ is singular (namely, fails to be lisse). In other words, $\overline{\mathcal{F}}$ is lisse away from the arrangement of hyperplanes

$$\mathcal{A} = \bigcup_{i=1}^{m} \bigcup_{\substack{\alpha\in\overline{\mathbb{F}_q}\\ \mathcal{F}_i \text{ is singular at } \alpha}} \{f \in \overline{\mathbb{F}_q[u]} : \deg(f) < n,\ f(x_i) = \alpha\}$$

in n-dimensional affine space over $\overline{\mathbb{F}_q}$.

The bound in Theorem 1.10 follows from Corollary 3.7 - a strong cohomology vanishing result for $\overline{\mathcal{F}}$, which says that its étale cohomology with compact support vanishes in all degrees except for the middle degree and the next one, together with Lemma 3.13 - a bound for the dimensions of the potentially nonvanishing cohomology groups. These are proven by completely separate arguments.

The cohomology vanishing adapts a now-standard strategy to show vanishing for the cohomology of a sheaf on an affine variety by comparing its compactly supported cohomology, its usual cohomology, and the cohomology of a certain (derived) pushforward sheaf on the boundary of a well-chosen compactification of the affine variety. This comparison is made possible by the long excision exact sequence in Lemma 3.3.

By Artin's affine theorem, the cohomology of any sheaf on an affine variety vanishes in high degrees, and by duality, the cohomology with compact support of a sufficiently nice sheaf on an affine variety vanishes in low degrees The sufficiently nice sheaves are called, perversely, "perverse". The required perversity property of the sheaf $\overline{\mathcal{F}}$ is established in Lemma 3.6.

Thus, the more similar we can show the usual and compactly supported cohomologies are, the more vanishing we obtain, for both cohomology theories. The difference between the usual and compactly supported cohomology is controlled, unsurprisingly from the classical perspective, by the behavior "near infinity" or, more productively in our setting, by the behavior near the boundary of any given compactification. In our proof, this difference is captured by the third term in the exact sequence of Lemma 3.3.

The affine space $\mathbb{A}^n$ that $\overline{\mathcal{F}}$ lives on has a natural compactification, a projective space $\mathbb{P}^n$. However, the divisor at infinity, which we denote by H_∞, is unsuitable for our purposes. The étale-local behavior of the derived pushforward of $\overline{\mathcal{F}}$ from $\mathbb{A}^n$ to $\mathbb{P}^n$ near a point in H_∞ depends in a subtle way on the individual sheaves $\mathcal{F}_\pi$, making it hard to compute this pushforward.

We could pass to a different compactification, but no obvious alternative where this pushforward is easier to compute presents itself. Instead, we make a change of perspective – in concrete terms, a projective change of coordinate system - where we view the closure in $\mathbb{P}^n$ of one of the hyperplanes in $\mathcal{A}$, call it H_1, as the boundary, and $\mathbb{P}^n$ with H_1 removed as an affine variety. Now, instead of working with the sheaf $\overline{\mathcal{F}}$ on $\mathbb{A}^n$ which is $\mathbb{P}^n - H_\infty$, we are working with the sheaf $\overline{\mathcal{F}}^\circ$ on $\mathbb{P}^n - H_1$ obtained from $\overline{\mathcal{F}}$ in this change of coordinates, see Eq. (3.5). We relate the cohomology of $\overline{\mathcal{F}}$ to that of $\overline{\mathcal{F}}^\circ$ in Eq. (3.7). We denote by v the inclusion of $\mathbb{P}^n - H_1$ in $\mathbb{P}^n$.

We must carefully choose the hyperplane H_1 in order to make the derived pushforward $Rv_*\overline{\mathcal{F}}^\circ$ (appearing in Lemma 3.3) amenable to a local study. We choose H_1 to be the projective closure of the hyperplane of all $f \in \mathbb{A}^n$ with $f(x_1) = z$, where z is the singular point of the Dirichlet trace function $\chi(x - z)$ that we assumed appears as a t_π in Theorem 1.10, and $x_1 \in \overline{\mathbb{F}_q}$ is a root of π.

The sheaf $\mathcal{F}_1$ on $\mathbb{A}^1_{\overline{\mathbb{F}_q}}$, obtained by base changing the sheaf giving rise to the trace function $\chi(x-z)$, has a local monodromy representation around the point z which is one-dimensional and nontrivial. It follows that the pushforward of $\mathcal{F}_1$ from $\mathbb{A}^1 - \{z\}$ to $\mathbb{A}^1$, vanishes at the point z. We want to use this vanishing to deduce that the derived pushforward $Rv_*\overline{\mathcal{F}}^\circ$ of $\overline{\mathcal{F}}^\circ$ from $\mathbb{P}^n - H_1$ to $\mathbb{P}^n$ vanishes at all but finitely many points of H_1, namely it is supported at those finitely many points. This is achieved in Lemma 3.4 and Lemma 3.5. Using this general method, we can prove that the number of cohomology groups of $\overline{\mathcal{F}}$ that may be nonzero is equal to the dimension of the support of $Rv_*\overline{\mathcal{F}}^\circ$ plus two, so because we show the support of $Rv_*\overline{\mathcal{F}}^\circ$ is zero-dimensional, we can have nonzero cohomology only in two specific degrees.

In the proofs of Lemma 3.4 and Lemma 3.5, in order to upgrade the vanishing of the pushforward of $\mathcal{F}_1$ at $z \in \mathbb{A}^1$ to the vanishing of $Rv_*\overline{\mathcal{F}}^\circ$ at a point on H_1, we find local coordinates near each point of H_1, except finitely many, in which the sheaf $\overline{\mathcal{F}}$ splits as a tensor product of our well-understood sheaf $\mathcal{F}_1$ associated with with trace function $\chi(x-z)$, depending on one coordinate x, and another sheaf, which depends on all the remaining coordinates, and may do so in an arbitrarily complicated way, but does not depend on x. This allows us to compute the pushforward locally, and obtain the desired vanishing conclusion, by applying the Künneth formula.

One approach to the local tensor product decomposition would be to take one coordinate for each linear map e_i which we pull back a sheaf on, but the number of linear maps is $m = \deg(g)$, which is greater than the dimension $n = \log_q(X)$ of our variety, so this would be too many coordinates. Instead we must show that some of the sheaves $e_i^*\mathcal{F}_i$ are lisse (essentially, locally constant) and can be ignored in our local pushforward calculation. For points on our special hyperplane that do not lie on H_∞ (the original divisor $\mathbb{P}^n - \mathbb{A}^n$ at infinity), this requires controlling how many of the hyperplanes in $\mathcal{A}$ (where $\overline{\mathcal{F}}$ is not lisse) can intersect at a point on H_1, which reduces to some simple algebra performed in Lemma 3.4. For points on both H_1 and H_∞, this doesn't quite work, as all the sheaves $\mathcal{F}_1, \dots, \mathcal{F}_m$ can have singularities at infinity. Instead, we use in Lemma 3.5 our assumption that the local monodromy of these sheaves at infinity is tame, and employ properties of sheaves with tame ramification (ultimately, Abhyankar's Lemma) to separate variables locally.

The argument in Lemma 3.6 showing that $\overline{\mathcal{F}}$ has the necessary perversity property, requires a similar separation-of-variables argument but fewer explicit calculations. At this point we have all the local properties needed to complete the global argument in Corollary 3.7, which relies on the excision long exact sequence from Lemma 3.3 and properties of semiperverse sheaves.

The bound for dimensions of cohomology groups (that is, Betti numbers) in Lemma 3.13 follows a strategy loosely inspired by the Betti number bounds for cohomological transforms proved by Fouvry, Kowalski, and

Michel in [FKM21]. The basis of this strategy is to take as much advantage as possible of our understanding of Betti numbers of sheaves on curves, see for instance the proof of Lemma 3.11. This understanding comes from the facts that all but one cohomology group of a sheaf on a curve has a simple global representation-theoretic description, and this remaining group can be controlled in terms of the Euler characteristic which can be expressed via local representation-theoretic information using the Grothendieck-Ogg-Shafarevich formula in Lemma 2.9 and Lemma 2.10.

At the heart of our strategy lies a procedure, introduced in the proof of Lemma 3.13, that replaces a sheaf $\mathcal{F}_\pi$ in the construction of $\overline{\mathcal{F}}$ with much simpler sheaves - skyscraper sheaves and Artin-Schreier sheaves, whose trace functions are indicators and additive characters. We are able to bound the change in the sum of Betti numbers caused by such a replacement, in terms of the rank and conductor of $\mathcal{F}_\pi$. Applying this procedure to $\mathcal{F}_\pi$ for each prime π dividing g, we eventually arrive at a sheaf cohomology problem that corresponds to a (possibly shorter) additive character sum. Such sums can be evaluated explicitly, and indeed, we solve the corresponding sheaf cohomology problem by an explicit computation using Lemma 3.12.

The aforementioned procedure starts by applying the projection formula which expresses the cohomology of the tensor product $\overline{\mathcal{F}}$ of the pullback of m sheaves from m curves as the cohomology of one sheaf (in our case, $\mathcal{F}_\pi$) on one of these curves (in our case, $\mathbb{A}^1$) tensored with the pushforward to that curve of the tensor product (of the pullbacks) of the remaining sheaves. Our procedure then bounds in Lemma 3.11 the sum of Betti numbers for this tensor product in terms of the Betti numbers of the factors twisted by skyscraper and Artin-Schreier sheaves. This is done by calculating the tensor product sheaf cohomology on the curve in degrees 0 and 2 from the coinvariants of the global Galois representation associated to the sheaf, applying the Grothendieck-Ogg-Shafarevich formula, producing in Corollary 2.12 an upper bound for the Swan conductor of a tensor product in terms of information available from the factors in the product, and applying the Grothendieck-Ogg-Shafarevich formula once again in Lemma 3.10(5). The procedure culminates with invoking the projection formula as in the first step, and observing that the entire process is almost involutary in the sense that the final expression is reminiscent of the original one, with the sheaf $\mathcal{F}_\pi$ replaced by simpler sheaves.

Using this argument, we are able to obtain Betti number bounds that are almost as strong as those obtained by [SS19] in a much more specialized situation, namely the one where t_π is a Dirichlet trace function for *every* prime π dividing g.

Thanks to the power and generality of Deligne's Riemann hypothesis and theory of weights, the main difficulty left to convert these cohomology vanishing and Betti number bounds into a bound for the exponential sum is to verify that the trace function of the descent of the sheaf $\overline{\mathcal{F}}$ to $\mathbb{A}^n_{\mathbb{F}_q}$ agrees with the original function t, see Eq. (3.86). This can be done using the results of [RL20].

For the cohomology vanishing part of the argument, a strategy similar in some respects was taken by Cohen, Dimca, and Orlik in [CDO03]. They gave a general method to show cohomology vanishing for sheaves on projective space, lisse away from an arrangement of hyperplanes in characteristic zero. We adopt from them the strategy of choosing one of these hyperplanes to play the role of the hyperplane at infinity, and showing vanishing of the pushforward.

However, for them the greatest interest was to show vanishing of cohomology in every degree except the middle degree. For our purposes, it's just as good to show vanishing of cohomology in every degree except the middle two degrees. We could even allow more degrees, but this would not be helpful for the argument. This means that it is sufficient to show that the support of the pushforward is zero-dimensional, rather than empty as in [CDO03]. The pushforward having empty support is a stronger condition that would not hold in our setting without additional assumptions.

The second difference is that we work in characteristic p, where wild ramification can occur, while [CDO03] works in characteristic zero, where it does not. This is one reason why it is so helpful for us that the sheaf $\overline{\mathcal{F}}$ arises from a certain explicit construction with tensor products of sheaves pulled back from curves. This allows us to control what types of wild ramification occur. Unlike in the characteristic zero setting, it would be difficult to come up with a formulation of the cohomology vanishing statement that applies to an arbitrary lisse sheaf on the complement of a hyperplane arrangement and is suitable for our purpose.

The third, related, difference is that [CDO03] uses an explicit resolution of singularities - this is an iterated blow-up of the projective space such that the inverse image of $\mathcal{A}$ (the hyperplane arrangement in question) is a simple normal crossings divisor. This enables them to avoid working with perverse sheaves, because lisse sheaves with tame ramification on the complement of a normal crossings divisor have all the good properties of perverse sheaves (because they are, in fact, a special case of perverse sheaves). For sheaves with wild ramification, this description is not available, so we resort to the machinery of perverse sheaves.

We can also compare to the strategy of [SS19], where we proved our cohomology vanishing statement in the special case where all the sheaves $\mathcal{F}_\pi$ are shifts of character sheaves, instead of just one. In that work, we considered a family of hyperplane arrangements, and studied the support of the vanishing cycles sheaf, rather than fixing a hyperplane at infinity and studying the support of the pushforward. The arguments needed to calculate the vanishing cycles and the pushforward are closely related. In both cases, the problem is entirely local at a given point, and a key strategy to study a sheaf constructed in a certain way, is to find a simpler construction which produces an equivalent sheaf locally (but not globally).

The advantage of the pushforward over the vanishing cycles for our purposes is that we only need to do this local analysis for points on a single hyperplane. Namely we need to consider only points on H_1 and not every point in $\mathbb{P}^n$. Indeed, vanishing cycles could appear at any singular point, i.e. on any hyperplane, unless an étale local study of the family of sheaves (for which one takes the vanishing cycles) gives a compelling reason for the vanishing cycles not to appear. The fact that we only need to do difficult local calculations at a single hyperplane means that we need to make strong assumptions about only a single sheaf $\mathcal{F}_\pi$. However, abandoning the vanishing cycles method requires us to have an alternative strategy for Betti number bounds, because the same vanishing cycles method that proved cohomology vanishing statements in [SS19] was simultaneously used there to prove Betti number bounds. In this paper, it does not seem possible to derive Betti number bounds directly from considering the pushforward, so we instead obtain them from a separate argument.

1.4.2. *Trace functions vs Arithmetic functions.* Inspired by [FKM14] and other works on orthogonality of trace functions and arithmetic functions over the integers, we consider here the correlation between trace functions and von Mangoldt/Möbius functions over function fields. We shall use the notation

$$\mathcal{M}_n = \{f \in \mathbb{F}_q[u] : \deg(f) = n,\ f \text{ is monic}\} \tag{1.30}$$

where n is a nonnegative integer.

Theorem 1.13. *Let p be an odd prime, and let $q > 4e^2p^2$ be a power of p. For a prime $\pi \in \mathbb{F}_q[u]$, an infinitame trace function $t\colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C}$, and a nonnegative integer n we have*

$$\sum_{f \in \mathcal{M}_n} t(f)\mu(f) \ll |\mathcal{M}_n|^{1-\frac{1}{2p}+\frac{\log_q(2ep)}{p}} |\pi|^{\log_q\left(r(t)\left(1+\frac{1}{2p}\right)+\frac{c(t)}{2p}\right)} \tag{1.31}$$

as $n, |\pi| \to \infty$, with the implied constant depending only on q.

Theorem 1.13 improves on the savings obtained in [SS19, Theorem 1.8] for the Kloosterman fraction $t(f) = e(\overline{f}/\pi)$, in case p is small enough and q is large but fixed. For larger p, the savings here are smaller, but apply to lengths of summation as short as $|\mathcal{M}_n| \sim |\pi|^\epsilon$ for any $\epsilon > 0$, once q is chosen appropriately. As opposed to [SS19], here we do not pursue the possible applications of a bound as in Theorem 1.13 to the level of distribution of primes in arithmetic progressions. Over the integers, different arguments have been given to obtain cancellation for sums longer than $|\pi|^{\frac{1}{2}}$ for more general trace functions, see [FKM14, Theorem 1.7, Remark 1.9]. Using Theorem 1.13 we are able to prove the following.

Corollary 1.14. *Let p be an odd prime, let $q > 4e^2p^2$ be a power of p, let $\delta > 0$, and set*

$$\zeta = \frac{2\delta}{1+2\delta}\left(1+\frac{1}{2p}-\frac{\log_q(2ep)}{p}\right)^{-1}. \tag{1.32}$$

Take a prime $\pi \in \mathbb{F}_q[u]$, an integer $n \geq (\frac{1}{2}+\delta)\deg(\pi)$, and an infinitame trace function $t\colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C}$ arising from a sheaf $\mathcal{F}$ whose geometric monodromy representation does not admit the trivial representation $\overline{\mathbb{Q}_\ell}$ as a quotient. Then for any $\epsilon > 0$ we have

$$\sum_{f\in\mathcal{M}_n} t(f)\Lambda(f) = O\left(|\mathcal{M}_n|^{\frac{1}{1+2\delta}+\zeta+\epsilon}|\pi|^{\log_q\left(r(t)\left(1+\frac{1}{2p}\right)+\frac{c(t)}{2p}\right)} + (r(t)+c(t))\frac{|\mathcal{M}_n|^{1+\epsilon}}{|\pi|^{\frac{1}{2}}}\right)$$

with the implied constant depending only on q and ϵ.

This result gives very modest savings, and applies to fewer trace functions compared to [FKM14, Theorem 1.5]. Nevertheless, Corollary 1.14 guarantees cancellation in intervals shorter than those treated over the integers, see for instance [Irv14]. We obtain savings as long as $\deg(\pi) > \epsilon n$ and

$$\delta > \frac{(2p+1)\log\left(r(t)\left(1+\frac{1}{2p}\right)+\frac{c(t)}{2p}\right)}{\log\left(\frac{q}{4e^2p^2}\right)}, \tag{1.33}$$

so in particular we can take $\delta \to 0$ as $q \to \infty$ with fixed characteristic, rank, and conductor. The results of [FKM14], [Irv14] give savings only when (in our notation) $\delta > \frac{1}{4}$, though [Irv14] can handle any δ with an additional average over the modulus π.

We have another application for Theorem 1.13, concerning very short sums over primes of shifted multiplicative characters.

Corollary 1.15. *Let p be an odd prime, let $q > 4e^2p^2$ be a power of p, set*

$$\zeta = \left(1+\frac{1}{p}-\frac{\log_q(4e^2p^2)}{p}\right)^{-1} < 1, \tag{1.34}$$

and let $\epsilon > 0$. Then for a prime $\pi \in \mathbb{F}_q[u]$, a nontrivial Dirichlet character $\chi\colon (\mathbb{F}_q[u]/(\pi))^\times \to \mathbb{C}^\times$, a polynomial $h \in \mathbb{F}_q[u]$, and a nonnegative integer n we have

$$\sum_{f\in\mathcal{M}_n} \chi(f+h)\Lambda(f) = O\left(|\mathcal{M}_n|^{\frac{1+\zeta}{2}+\epsilon}|\pi|^{\log_q(3)} + |\mathcal{M}_n|^{1+\epsilon}|\pi|^{-1}\right) \tag{1.35}$$

as $|\pi|, n \to \infty$, with the implied constant depending only on q and ϵ.

As in Theorem 1.13, the strength of the result is in the shortness of the range of summation, the power saving being quite small. Corollary 1.15 provides savings as long as

$$\epsilon n < \deg(\pi) < \frac{\log_3\left(\frac{q}{4e^2p^2}\right)}{2p+2}n, \tag{1.36}$$

which as $q \to \infty$ with fixed p allows us to take $\deg(\pi)$ an arbitrarily large multiple of n. For the state of the art on the analogous problem over the integers we refer to [Rakh18] and references therein. In this result, and the previous two, we have worked for simplicity with trace functions to prime moduli only, but these results can be extended to trace functions (satisfying the assumptions in the previous three results) with an arbitrary squarefree period.

2. Sheaves

One can speak of sheaves and trace functions not only on $\mathbb{A}^1$, as we did so far, but also on other curves and on more general varieties. Most of the notions from Definition 1.4 admit natural generalizations to this setting. We start here by constructing the sheaves giving rise to the trace functions we have encountered, and their high-dimensional counterparts. These constructions are standard [SGA4$\frac{1}{2}$, Sommes trig.], but we provide here a detailed explanation including all the properties we need, for the reader's convenience.

2.1. **Kummer sheaves.**

Notation 2.1. Let κ be a finite field of characteristic p, let $\chi\colon \kappa^\times \to \overline{\mathbb{Q}_\ell}^\times$ be a multiplicative character, and let $w \in \kappa[T]$ be a nonzero polynomial. We extend χ to a function on κ by setting $\chi(0) = 0$, and construct a $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{L}_\chi(w)$, on the affine line $\mathbb{A}^1_\kappa = \operatorname{Spec} \kappa[T]$, whose trace function is χ, as follows.

Denote by $|\kappa|$ the number of elements in κ. Then the cover of $\mathbb{A}^1_\kappa$ defined by the equation

$$Y^{|\kappa|-1} = w(T) \tag{2.1}$$

is finite étale (see [Mil13, Example 2.5]) away from the set

$$S = \{z \in \mathbb{A}^1_\kappa : w(z) = 0\}. \tag{2.2}$$

The group $\kappa^\times$ acts on our cover (by automorphisms) via multiplication on Y, since every $\zeta \in \kappa^\times$ satisfies $\zeta^{|\kappa|-1} = 1$. As all $\zeta \in \overline{\kappa}$ with $\zeta^{|\kappa|-1} = 1$ lie in κ, we get a simply transitive action of $\kappa^\times$ on the (geometric) fiber of any geometric point $\overline{x}$ lying over a (not necessarily closed) point x of

$$U = \mathbb{A}^1_\kappa - S. \tag{2.3}$$

From the definition of the étale fundamental group as the automorphism group of the fiber functor (e.g. [Sz09, Theorem 5.4.2(2)]), we get a continuous action of $\pi_1^{\text{ét}}(U, \overline{x})$ on the fiber of $\overline{x}$ in our étale cover of U, commuting with the action of $\kappa^\times$. Since the latter acts simply transitively, by picking a point $\overline{t}$ in the fiber over $\overline{x}$, to each $g \in \pi_1^{\text{ét}}(U, \overline{x})$ we can associate a unique $\lambda \in \kappa^\times$ satisfying $\lambda(\overline{t}) = g(\overline{t})$. This association is a continuous homomorphism as, if to $g_1, g_2 \in \pi_1^{\text{ét}}(U, \overline{x})$ we have associated $\lambda_1, \lambda_2 \in \kappa^\times$, then

$$g_1g_2(\bar{t}) = g_1(g_2(\bar{t})) = g_1(\lambda_2(\bar{t})) = \lambda_2(g_1(\bar{t})) = \lambda_2(\lambda_1(\bar{t})) = \lambda_2\lambda_1(\bar{t}) = \lambda_1\lambda_2(\bar{t}).$$

Therefore, by composition with χ, we get a continuous homomorphism $\pi_1^{\text{ét}}(U, \overline{x}) \to \overline{\mathbb{Q}_\ell}^\times$. This gives rise to a continuous one-dimensional representation of $\pi_1^{\text{ét}}(U, \overline{x})$ over $\overline{\mathbb{Q}_\ell}$, hence a rank one lisse sheaf on U via the equivalence in [Ka88, 2.0.2]. We define $\mathcal{L}_\chi(w)$ to be the extension by zero of this lisse sheaf from U to $\mathbb{A}^1_\kappa$. We call $\mathcal{L}_\chi(w)$ a Kummer sheaf.

As suggested by the notation, the construction is independent of the choice of $\bar{t}$. Indeed if $\overline{h}$ is another geometric point in the fiber over $\overline{x}$, then by transitivity there exists $\gamma \in \kappa^\times$ with $\gamma(\bar{t}) = \overline{h}$, so we have

$$g(\overline{h}) = g(\gamma(\bar{t})) = \gamma(g(\bar{t})) = \gamma(\lambda(\bar{t})) = \gamma\lambda(\bar{t}) = \lambda\gamma(\bar{t}) = \lambda(\gamma(\bar{t})) = \lambda(\overline{h}),$$

where $\lambda \in \kappa^\times$ is associated to $g \in \pi_1^{\text{ét}}(U, \overline{x})$. Moreover, by [Sz09, Proposition 5.5.1] the fiber functors for different geometric points on the connected curve U are isomorphic, so our construction is also independent of the choice of the point $x \in U$ (or the geometric point above it).

In case $\overline{x}$ is a geometric generic point of U, its fiber can be identified with the set of all homomorphisms of $\kappa(T)$-algebras from $\kappa(T)[Y]/(Y^{|\kappa|-1} - w(T))$ to $\kappa(T)^{\text{sep}}$. The group $\pi_1^{\text{ét}}(\overline{x}) = \text{Gal}(\kappa(T)^{\text{sep}}/\kappa(T))$ acts on this set by postcomposition, and this action factors through the aforementioned action of $\pi_1^{\text{ét}}(U, \overline{x})$ on the fiber of $\overline{x}$ (via the map on fundamental groups induced from the inclusion of $\overline{x}$ in U).

In the following lemma, among other things, we will see that the trace function $t_{\mathcal{L}_\chi(w)}$ arising from the sheaf $\mathcal{L}_\chi(w)$ is infinitame, and calculate its invariants.

Lemma 2.2. *The sheaf $\mathcal{L}_\chi(w)$ on $\mathbb{A}^1_\kappa$ has the following properties.*

(1) *For every $x \in \kappa$ we have $t_{\mathcal{L}_\chi(w)}(x) = \chi(w(x))$;*
(2) *the sheaf $\mathcal{L}_\chi(w)$ is lisse on U, and vanishes on its complement S;*
(3) *the sheaf $\mathcal{L}_\chi(w)$ has tame local monodromy at every closed point $x \in \mathbb{P}^1_\kappa$, or in other words, it is tamely ramified (everywhere);*
(4) *the sheaf $\mathcal{L}_\chi(w)$ is mixed of nonpositive weights;*
(5) *the sheaf $\mathcal{L}_\chi(w)$ has no finitely supported sections;*
(6) *the rank and conductor are given by*

$$\mathbf{r}(\mathcal{L}_\chi(w)) = 1, \quad c(\mathcal{L}_\chi(w)) = |\{a \in \overline{\kappa} : w(a) = 0\}| \leq \deg(w);$$

(7) *the sheaf $\mathcal{L}_\chi(w)$ is the extension by zero to $\mathbb{A}^1_\kappa$ of some one-dimensional representation of the tame arithmetic fundamental group of $\mathbb{A}^1_\kappa - \{z\}$ for some $z \in \kappa$ if and only if there exists $c \in \kappa^\times$ and a positive integer d such that*

$$w(T) = c(T - z)^d.$$

If this is the case, let $v \geq 1$ be the (multiplicative) order of χ. Then the representation is trivial on the geometric fundamental group of $\mathbb{A}^1_\kappa - \{z\}$ if and only if v divides d.

Proof. Visibly, (2) is immediate from our construction.

To verify (1), first note that because the sheaf is zero on S, its trace function is zero, which matches our convention

$$\chi(w(x)) = \chi(0) = 0, \quad x \in S. \tag{2.4}$$

For $x \in \kappa \setminus S$, we get from Eq. (2.1) that $g = \mathrm{Frob}_{x,\kappa} \in \pi_1^{\text{ét}}(U, \overline{x})$ acts on the geometric fiber over x by

$$g(x,y) = (x^{|\kappa|}, y^{|\kappa|}) = (x, y^{|\kappa|}) = (x, w(x)y). \tag{2.5}$$

Hence, by our definition of the representation giving rise to the sheaf $\mathcal{L}_\chi(w)$, the element $\lambda = w(x) \in \kappa^\times$ is associated to g, so g is mapped to $\chi(w(x))$ as desired.

For (3), note that since the monodromy (i.e. image) of the representation giving rise to $\mathcal{L}_\chi(w)$ is isomorphic to a quotient of $\kappa^\times$, it has order prime to p. Therefore, by Lagrange's theorem, the image of an inertia group of any closed point $x \in \mathbb{P}^1_\kappa$ is of order prime to p as well. It follows that $\mathcal{L}_\chi(w)$ has tame local monodromy at x.

To get (4), note that for a closed point $x \in \mathbb{A}^1_\kappa$, every eigenvalue of $\mathrm{Frob}_{x,\kappa(x)}$ is a value of the finite order character χ, hence a root of unity whose norm is thus $1 = |\kappa(x)|^{0/2}$. This shows that $\mathcal{L}_\chi(w)$ is punctually pure of weight 0, so in particular it is mixed of nonpositive weights.

Observe that (5) is immediate from (2). Indeed, $\mathcal{L}_\chi(w)$ is lisse on U, so it has no finitely supported sections there, and it has no sections at all supported on S as all of its stalks vanish there.

To get the first part of (6), recall from (2) that $\mathcal{L}_\chi(w)$ is lisse on U, hence it is lisse at a geometric generic point $\overline{\eta}$ of U (and of $\mathbb{A}^1_\kappa$). Hence the dimension of $\mathcal{L}_\chi(w)_\eta$ is the rank of the representation giving rise to it, which is 1. For the second part of (6), we get from (3) that $\mathcal{L}_\chi(w)$ has tame ramification everywhere so all the Swan conductors vanish. By the definition in Eq. (1.17) we therefore have

$$\begin{aligned} c(\mathcal{L}_\chi(w)) &= \sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa](1 - \dim \mathcal{L}_\chi(w)_{\overline{x}}) \\ &= \sum_{x \in |U|} [\kappa(x) : \kappa](1-1) + \sum_{x \in |S|} [\kappa(x) : \kappa](1-0) = |\{a \in \overline{\kappa} : w(a) = 0\}| \end{aligned}$$

because the dimension of the stalk at every point where the sheaf is lisse equals the generic rank.

For (7), if $\mathcal{L}_\chi(w)$ is the extension by zero of a one-dimensional representation of $\pi_1^{\text{ét}}(\mathbb{A}^1_\kappa - \{z\})$, then it is lisse away from z and vanishes at z, making z the unique root of w by (2). The uniqueness of the root z allows us to write $w(T) = c(T-z)^d$ for a scalar $c \in \kappa^\times$ and a positive integer d. Conversely, if z is the unique root of w, then by construction $\mathcal{L}_\chi(w)$ is the extension by zero of a one-dimensional representation, which is tame by (3).

Our representation is geometrically trivial if and only if the image of the map from the geometric fundamental group to $\kappa^\times$ is contained in $\mathrm{Ker}(\chi)$. Since $\kappa^\times$ is cyclic of order $|\kappa|-1$, and χ is of order v, we see that

$$\mathrm{Ker}(\chi) = \{\zeta^v : \zeta \in \kappa^\times\} = \{\zeta \in \kappa^\times : \zeta^n = 1\}, \quad n = \frac{|\kappa|-1}{v}. \tag{2.6}$$

Therefore, the aforementioned image is contained in the kernel above if and only if the geometric fundamental group acts on the (geometric) generic fiber via multiplication by n-th roots of unity. This is equivalent to the geometric fundamental group acting trivially on the generic fiber of the finite étale subcover

$$\widetilde{Y}^v = w(T) = c(T-z)^d, \quad \widetilde{Y} = Y^n \tag{2.7}$$

of $\mathbb{A}^1_{\overline{\kappa}}$. Since the action of the fundamental group on the generic fiber is that of $\mathrm{Gal}(\overline{\kappa}(T)^{\mathrm{sep}}/\overline{\kappa}(T))$, the triviality of the action is tantamount to the existence of an v-th root for $w(T)$ in $\overline{\kappa}(T)$. Such a root exists if and only if d is a multiple of v, so we have finished the verification of (7). □

2.2. **Change of variable for sheaves.** For future use, we record some simple transformation rules of sheaves and their trace functions.

Proposition 2.3. *Let $g \in \mathbb{F}_q[u]$ be a squarefree polynomial, let*

$$t\colon \mathbb{F}_q[u]/(g) \to \mathbb{C} \tag{2.8}$$

be an infinitame trace function, and let $P, C \in \mathbb{F}_q[u]$. Then the function defined by

$$t'(x) = t(Px + C) \tag{2.9}$$

is an infinitame trace function with rank and conductor satisfying

$$r(t') \leq r(t), \quad c(t') \leq c(t). \tag{2.10}$$

Notation 2.4. For a finite field κ of characteristic p and $r \in \kappa$, we define the map

$$E_r\colon \mathbb{A}^1_\kappa \to \mathbb{A}^1_\kappa, \quad E_r(x) = r + x^p. \tag{2.11}$$

Proposition 2.5. *Let $\mathcal{F}$ be an infinitame sheaf on $\mathbb{A}^1_\kappa$. Then the sheaf $E_r^*\mathcal{F}$ and its trace function enjoy the following properties.*

1. *If $\mathcal{F}$ has no finitely supported sections, then neither does $E_r^*\mathcal{F}$.*
2. *If $\mathcal{F}$ is tamely ramified at infinity then so is $E_r^*\mathcal{F}$.*
3. *If $\mathcal{F}$ is mixed of nonpositive weights then so is $E_r^*\mathcal{F}$.*
4. *We have $c(E_r^*\mathcal{F}) = c(\mathcal{F})$ and $\mathbf{r}(E_r^*\mathcal{F}) = \mathbf{r}(\mathcal{F})$.*
5. *We have $t_{E_r^*\mathcal{F}}(x) = t_{\mathcal{F}}(r + x^p)$.*
6. *If $t_{\mathcal{F}}$ is a Dirichlet trace function then so is $t_{E_r^*\mathcal{F}}$.*

Proof. The map $x \mapsto r+x^p$ induces an autoequivalence of the étale site of $\mathbb{A}^1_\kappa$, hence pullback under it preserves étale topological invariants such as generic rank and conductor. This establishes (1) – (4), and (5) is a consequence of the fact that $(E_r^*\mathcal{F})_x \cong \mathcal{F}_{E_r(x)}$ for $x \in \mathbb{A}^1_\kappa$. For (6) we assume, following Example 1.7, that there exist $\chi\colon \kappa^\times \to \overline{\mathbb{Q}_\ell}^\times$, $a \in \kappa^\times$, and $b \in \kappa$ such that

$$t_{\mathcal{F}}(x) = \begin{cases} \chi(ax+b) & x \neq -ba^{-1} \\ 0 & x = -ba^{-1} \end{cases}$$

for every κ-valued point x on $\mathbb{A}^1_\kappa$. We then get from (5) and the multiplicativity of χ that

$$\begin{aligned} t_{E_r^*\mathcal{F}}(x) = t_{\mathcal{F}}(r+x^p) &= \begin{cases} \chi(ax^p+ar+b) & x^p \neq -ba^{-1}-r \\ 0 & x^p = -ba^{-1}-r \end{cases} \\ &= \begin{cases} \chi^p(a^{1/p}x+(ar+b)^{1/p}) & x \neq -(ar+b)^{1/p}a^{-1/p} \\ 0 & x = -(ar+b)^{1/p}a^{-1/p} \end{cases} \end{aligned}$$

where for $\lambda \in \kappa$ we denote by $\lambda^{1/p}$ the unique element of κ whose pth power is λ, and by $\lambda^{-1/p}$ the multiplicative inverse of that element. Since $\lambda \mapsto \lambda^{1/p}$ is an automorphism of κ, the equality above is justified. As χ^p is also a character of $\kappa^\times$, and $a^{1/p} \in \kappa^\times$, we conclude that $t_{E_r^*\mathcal{F}}(x)$ is a Dirichlet trace function as required for (6). □

2.3. **Local invariants.**

Here we take a closer look at the local invariants of a sheaf $\mathcal{F}$ on a curve C over a perfect field κ of characteristic p. Some of these invariants (and their analogs) were mentioned in passing earlier.

2.3.1. *Drop, Slope, Swan.*

Definition 2.6. For a sheaf $\mathcal{F}$ on a smooth curve C/κ and a closed point x of C, define the *drop*

$$\mathbf{d}_x(\mathcal{F}) = \mathbf{r}(\mathcal{F}) - \dim(\mathcal{F}_x). \tag{2.12}$$

This is the drop in the rank of $\mathcal{F}$ as we pass from a generic point to x. If $\mathcal{F}$ has no sections supported at x, then $\mathbf{d}_x(\mathcal{F}) \geq 0$. If $\mathcal{F}$ is a middle extension sheaf at x in the sense that $\mathcal{F}$ is the (non-derived) pushforward from $C - \{x\}$ to C of some sheaf, then $\mathcal{F}_x$ is equal to the invariants of $\mathcal{F}_\eta$ under the inertia group I_x, and then $\mathbf{d}_x(\mathcal{F})$ is the codimension of the inertia invariants.

Next we introduce the 'slope' of an irreducible inertia representation, which is sometimes also called 'break' or 'jump', see [Ka88, Chapter 1]. For that we use the upper numbering filtration on an inertia group I indexed by nonnegative real numbers. That is, for $s \geq 0$ we denote by I^s what is sometimes denoted by $\mathrm{Gal}(L^{\mathrm{sep}}/L)^s$, where L is the completion of the function field of C at x, see for instance [KR14, Definition 3.54].

Definition 2.7. Let C be an open subset of a smooth proper curve $\overline{C}/\kappa$, let x be a closed point of $\overline{C}$. For an irreducible (finite-dimensional, continuous) representation V of I_x over $\overline{\mathbb{Q}_\ell}$ define

$$\mathrm{slope}(V) = \inf\{s \geq 0 : I_x^s \text{ acts trivially on } V\}. \tag{2.13}$$

Let V be a representation of I_x over $\overline{\mathbb{Q}_\ell}$, and let $V_1, \dots, V_n$ be the (irreducible) Jordan-Hölder factors of V, listed with multiplicity. One defines the Swan conductor of V by

$$\mathbf{sw}(V) = \sum_{i=1}^{n} \dim(V_i)\, \mathrm{slope}(V_i), \tag{2.14}$$

and the slopes of V to be

$$\mathrm{slopes}(V) = \{\mathrm{slope}(V_i) : 1 \leq i \leq n\}. \tag{2.15}$$

For a sheaf $\mathcal{F}$ on C, we can view the stalk $\mathcal{F}_\eta$ at the generic point as a representation of I_x, and define the Swan conductor of $\mathcal{F}$ at x by

$$\mathbf{sw}_x(\mathcal{F}) = \mathbf{sw}(\mathcal{F}_\eta) = \mathbf{sw}(I_x \curvearrowright \mathcal{F}_\eta). \tag{2.16}$$

Here $I_x \curvearrowright \mathcal{F}_\eta$ means that I_x acts on $\mathcal{F}_\eta$, namely we emphasize that $\mathcal{F}_\eta$ is viewed as a representation of I_x. Similarly, if I_x acts irreducibly on $\mathcal{F}_\eta$, we set

$$\mathrm{slope}_x(\mathcal{F}) = \mathrm{slope}(\mathcal{F}_\eta) = \mathrm{slope}(I_x \curvearrowright \mathcal{F}_\eta) \tag{2.17}$$

and in general

$$\mathrm{slopes}_x(\mathcal{F}) = \mathrm{slopes}(\mathcal{F}_\eta) = \mathrm{slopes}(I_x \curvearrowright \mathcal{F}_\eta). \tag{2.18}$$

We further define the local conductor of $\mathcal{F}$ at x as

$$\mathbf{c}_x(\mathcal{F}) = \mathbf{d}_x(\mathcal{F}) + \mathbf{sw}_x(\mathcal{F}). \tag{2.19}$$

Note that $\mathcal{F}$ is tamely ramified at x if and only if $\mathrm{slopes}_x(\mathcal{F}) = \{0\}$, or equivalently $\mathbf{sw}_x(\mathcal{F}) = 0$. By our earlier remarks, if $\mathcal{F}$ is a middle extension sheaf at x (pushforward of a sheaf from $C - \{x\}$ to C) then $\mathbf{c}_x(\mathcal{F})$ is the Swan conductor of the inertia representation of $\mathcal{F}$ at x plus the codimension of the inertia invariants. By definition, this is the Artin conductor of the inertia representation. Thus, $\mathbf{c}_x(\mathcal{F})$ is an adaptation of the Artin conductor to the setting of sheaves.

For an alternative definition of the Swan conductor see [KR14, Definition 4.72, Definition 4.82, Theorem 4.86].

2.3.2. *Euler characteristic.*

Definition 2.8. One defines the Euler characteristic of a sheaf $\mathcal{F}$ on a smooth curve $C/\overline{\kappa}$ by

$$\chi(C, \mathcal{F}) = \sum_{i=0}^{2} (-1)^i \dim H_c^i(C, \mathcal{F}). \tag{2.20}$$

For the constant sheaf on a proper smooth curve $C = \overline{C}$ of genus g we have

$$\chi(\overline{C}) = \chi(\overline{C}, \overline{\mathbb{Q}_\ell}) = \sum_{i=0}^{2} (-1)^i \dim H^i_c(\overline{C}, \overline{\mathbb{Q}_\ell}) = 1 - 2g + 1 = 2 - 2g, \tag{2.21}$$

while in the affine case $C \subsetneq \overline{C}$ we have

$$\begin{aligned}\chi(C) = \chi(C, \overline{\mathbb{Q}_\ell}) &= \dim H^2_c(C, \overline{\mathbb{Q}_\ell}) - \dim H^1_c(C, \overline{\mathbb{Q}_\ell}) \\ &= 1 - (2g + |\overline{C} - C| - 1) = \chi(\overline{C}) - |\overline{C} - C|.\end{aligned} \tag{2.22}$$

Lemma 2.9. *For a sheaf $\mathcal{F}$ on a proper smooth curve $\overline{C}/\overline{\kappa}$, we have*

$$\chi(\overline{C}, \mathcal{F}) = \chi(\overline{C}) \mathbf{r}(\mathcal{F}) - \sum_{x \in |\overline{C}|} \mathbf{c}_x(\mathcal{F}). \tag{2.23}$$

Note that $\mathbf{sw}_x(\mathcal{F})$ and $\mathbf{d}_x(\mathcal{F})$ both vanish at every point $x \in |\overline{C}|$ where $\mathcal{F}$ is lisse, so the sum above is finite.

Proof. This is the Grothendieck-Ogg-Shafarevich formula [SGA5, X, Theorem 7.1], specialized to the case of sheaves (instead of complexes of sheaves). □

Lemma 2.10. *For a sheaf $\mathcal{F}$ on an open subset C of a smooth proper curve $\overline{C}/\overline{\kappa}$, we have*

$$\chi(C, \mathcal{F}) = \chi(C) \mathbf{r}(\mathcal{F}) - \sum_{x \in |C|} \mathbf{c}_x(\mathcal{F}) - \sum_{x \in \overline{C} - C} \mathbf{sw}_x(\mathcal{F}) \tag{2.24}$$

Proof. Let $j \colon C \to \overline{C}$ be the open immersion. By Definition 2.8, Lemma 2.9, and the definition of compactly supported étale cohomology we have

$$\chi(C, \mathcal{F}) = \chi(\overline{C}, j_! \mathcal{F}) = \chi(\overline{C}) \mathbf{r}(j_! \mathcal{F}) - \sum_{x \in |\overline{C}|} \mathbf{c}_x(j_! \mathcal{F}). \tag{2.25}$$

Extension by zero preserves all local invariants at points of C, so we have

$$\mathbf{r}(j_! \mathcal{F}) = \mathbf{r}(\mathcal{F}), \quad \mathbf{c}_x(j_! \mathcal{F}) = \mathbf{c}_x(\mathcal{F}), \quad x \in |C|. \tag{2.26}$$

For $x \in \overline{C} - C$, we have $(j_! \mathcal{F})_x = 0$ so from Definition 2.6 we get

$$\mathbf{d}_x(j_! \mathcal{F}) = \mathbf{r}(j_! \mathcal{F}) - \dim (j_! \mathcal{F})_x = \mathbf{r}(\mathcal{F}) \tag{2.27}$$

and by Definition 2.7 we have

$$\mathbf{sw}_x(j_! \mathcal{F}) = \mathbf{sw}(j_! \mathcal{F})_\eta = \mathbf{sw}(\mathcal{F}_\eta) = \mathbf{sw}_x(\mathcal{F}) \tag{2.28}$$

so by definition of the local conductor in Eq. (2.19)

$$\mathbf{c}_x(j_! \mathcal{F}) = \mathbf{r}(\mathcal{F}) + \mathbf{sw}_x(\mathcal{F}). \tag{2.29}$$

Combining Eq. (2.22), Eq. (2.25), Eq. (2.26), and Eq. (2.29) we get

$$\begin{aligned}\chi(C,\mathcal{F}) &= \chi(\overline{C})\mathbf{r}(j_!\mathcal{F}) - \sum_{x\in|\overline{C}|}\mathbf{c}_x(j_!\mathcal{F})\\ &= (\chi(C)+|\overline{C}-C|)\mathbf{r}(\mathcal{F}) - \sum_{x\in|C|}\mathbf{c}_x(\mathcal{F}) - \sum_{x\in\overline{C}-C}(\mathbf{r}(\mathcal{F})+\mathbf{sw}_x(\mathcal{F}))\\ &= \chi(C)\mathbf{r}(\mathcal{F}) - \sum_{x\in|C|}\mathbf{c}_x(\mathcal{F}) - \sum_{x\in\overline{C}-C}\mathbf{sw}_x(\mathcal{F})\end{aligned}$$

as desired. □

2.3.3. *Local invariants of tensor products.*

Proposition 2.11. *For irreducible representations V_1, V_2 of an inertia group I we have*

$$\max\ \mathrm{slopes}(V_1\otimes V_2) \le \max\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\}. \tag{2.30}$$

Moreover, in case $\dim V_2 = 1$*, the representation $V_1\otimes V_2$ is irreducible, and*

$$\mathrm{slope}(V_1\otimes V_2) = \max\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\} \tag{2.31}$$

unless $\mathrm{slope}(V_1)=\mathrm{slope}(V_2)$ *and for every $g\in I^{\mathrm{slope}(V_1)}$ there exists $\lambda\in\overline{\mathbb{Q}_\ell}^\times$ such that for every $v_1\in V_1$ and $v_2\in V_2$ we have*

$$g(v_1)=\lambda v_1, \quad g(v_2)=\lambda^{-1}v_2. \tag{2.32}$$

Proof. In order to establish Eq. (2.30), take $s>\max\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\}$. By the definition in Eq. (2.13), the subgroup I^s acts trivially on both V_1 and V_2, so it acts trivially on $V_1\otimes V_2$, hence on all its Jordan-Hölder factors. It follows that $\max\mathrm{slopes}(V_1\otimes V_2)\le s$, therefore Eq. (2.30) holds.

That $V_1\otimes V_2$ is irreducible if $\dim V_2 = 1$ is a general fact about representations, because a subspace of $V_1\otimes V_2$ is invariant if and only if the corresponding subspace of V_1 is invariant.

For the proof of Eq. (2.31), assume first that $\mathrm{slope}(V_1)\neq\mathrm{slope}(V_2)$. For

$$\min\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\} < s < \max\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\}, \tag{2.33}$$

the subgroup I^s of I acts trivially on one of V_1, V_2 and nontrivially on the other, so it acts nontrivially on their tensor product. Since $I^s\subseteq I^{s'}$ if $s>s'$, we conclude that I^s acts nontrivially on $V_1\otimes V_2$ for any

$$s<\max\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\}, \tag{2.34}$$

hence $\mathrm{slope}(V_1\otimes V_2)\ge\max\{\mathrm{slope}(V_1),\mathrm{slope}(V_2)\}$. Using Eq. (2.30) and the irreducibility of $V_1\otimes V_2$, we arrive at Eq. (2.31).

Suppose now that $\mathrm{slope}(V_1)=\mathrm{slope}(V_2)=s$ but $\mathrm{slope}(V_1\otimes V_2)<s$, so I^s acts trivially on $V_1\otimes V_2$. As I^s acts by scalars on the one-dimensional representation V_2, it must act by the inverses of these scalars on V_1 for the action on $V_1\otimes V_2$ to be trivial. In other words, Eq. (2.32) holds. □

Corollary 2.12. *For representations V_1, V_2 of an inertia group we have*

$$\mathbf{sw}(V_1 \otimes V_2) \leq \mathbf{sw}(V_1)\dim(V_2) + \mathbf{sw}(V_2)\dim(V_1). \tag{2.35}$$

Proof. By Definition 2.7, the Swan conductor is additive in short exact sequences, so we are reduced to the case V_1 is irreducible, and then also to the case V_2 is irreducible. If $W_1, \dots W_n$ are the Jordan-Hölder factors of $V_1 \otimes V_2$, then by Proposition 2.11 we have

$$\begin{aligned}\mathbf{sw}(V_1 \otimes V_2) &= \sum_{i=1}^{n} \dim(W_i)\,\mathrm{slope}(W_i) \leq \sum_{i=1}^{n} \dim(W_i) \max\ \mathrm{slopes}(V_1 \otimes V_2) \\ &\leq \sum_{i=1}^{n} \dim(W_i) \max\{\mathrm{slope}(V_1), \mathrm{slope}(V_2)\} \\ &\leq (\mathrm{slope}(V_1) + \mathrm{slope}(V_2)) \dim(V_1 \otimes V_2) \\ &= \mathbf{sw}(V_1)\dim(V_2) + \mathbf{sw}(V_2)\dim(V_1)\end{aligned}$$

as required. □

Lemma 2.13. *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be sheaves on $\mathbb{A}^1_\kappa$. Then the tensor product $\mathcal{F}_1 \otimes \mathcal{F}_2$ has the following properties.*

1. *For every $x \in \kappa$ we have*
$$t_{\mathcal{F}_1 \otimes \mathcal{F}_2}(x) = t_{\mathcal{F}_1}(x) t_{\mathcal{F}_2}(x);$$
2. *if $\mathcal{F}_1$ and $\mathcal{F}_2$ have no finitely supported sections, then neither does $\mathcal{F}_1 \otimes \mathcal{F}_2$;*
3. *if $\mathcal{F}_1$ and $\mathcal{F}_2$ are tamely ramified at ∞, then so is $\mathcal{F}_1 \otimes \mathcal{F}_2$;*
4. *if $\mathcal{F}_1$ and $\mathcal{F}_2$ are mixed of nonpositive weights, then so is $\mathcal{F}_1 \otimes \mathcal{F}_2$;*
5. *the rank of the tensor product is given by $\mathbf{r}(\mathcal{F}_1 \otimes \mathcal{F}_2) = \mathbf{r}(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2)$;*
6. *if $\mathcal{F}_1$ and $\mathcal{F}_2$ are infinitame, then so is their tensor product, and its conductor satisfies*
$$c(\mathcal{F}_1 \otimes \mathcal{F}_2) \leq c(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2) + \mathbf{r}(\mathcal{F}_1)c(\mathcal{F}_2).$$

Proof. To verify (1), note that for every closed point $x \in \mathbb{A}^1_\kappa$ we have a $\mathrm{Frob}_{x,\kappa(x)}$-equivariant isomorphism

$$(\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{x}} \cong \mathcal{F}_{1,\overline{x}} \otimes \mathcal{F}_{2,\overline{x}} \tag{2.36}$$

so in case x is κ-valued, from Eq. (2.36) we get

$$\begin{aligned}t_{\mathcal{F}_1 \otimes \mathcal{F}_2}(x) &= \mathrm{tr}(\mathrm{Frob}_{x,\kappa}, (\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{x}}) = \mathrm{tr}(\mathrm{Frob}_{x,\kappa}, \mathcal{F}_{1,\overline{x}} \otimes \mathcal{F}_{2,\overline{x}}) \\ &= \mathrm{tr}(\mathrm{Frob}_{x,\kappa}, \mathcal{F}_{1,\overline{x}})\,\mathrm{tr}(\mathrm{Frob}_{x,\kappa}, \mathcal{F}_{2,\overline{x}}) = t_{\mathcal{F}_1}(x) t_{\mathcal{F}_2}(x)\end{aligned}$$

so (1) is established.

We further see from Eq. (2.36) that the eigenvalues of $\mathrm{Frob}_{x,\kappa(x)}$ on the stalk of the tensor product are products of the eigenvalues on $\mathcal{F}_{1,\overline{x}}$ and $\mathcal{F}_{2,\overline{x}}$. Since the product of complex numbers of norm at most $|\kappa|^{\frac{0}{2}}$ has norm at most $|\kappa|^{\frac{0}{2}}$, this verifies (4).

To check (3), let $\eta \in \mathbb{A}^1_\kappa$ be the generic point, and note that (as in Eq. (2.36)) we have an isomorphism

$$(\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{\eta}} \cong \mathcal{F}_{1,\overline{\eta}} \otimes \mathcal{F}_{2,\overline{\eta}} \tag{2.37}$$

of representations of $\mathrm{Gal}(\kappa(T)^{\mathrm{sep}}/\kappa(T))$. In particular this is an isomorphism of representations of the wild inertia subgroup P_∞. By the tameness assumption, the latter subgroup acts trivially on each of the factors in the right hand side of Eq. (2.37), so it acts trivially on their tensor product, hence it also acts trivially on the left hand side of Eq. (2.37). This triviality of the action of P_∞ is the desired tameness of the sheaf $\mathcal{F}_1 \otimes \mathcal{F}_2$ at ∞.

Let $i \in \{1, 2\}$. If $\mathcal{F}_i$ has no finitely supported sections, then the natural map $\mathcal{F}_{i,\overline{x}} \to \mathcal{F}_{i,\overline{\eta}}^{I_x}$ is injective for every closed point $x \in \mathbb{A}^1_\kappa$. Since the tensor product of two injective maps of vector spaces is injective, we get from Eq. (2.36) and Eq. (2.37) that the mappings

$$(\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{x}} \cong \mathcal{F}_{1,\overline{x}} \otimes \mathcal{F}_{2,\overline{x}} \to \mathcal{F}_{1,\overline{\eta}}^{I_x} \otimes \mathcal{F}_{2,\overline{\eta}}^{I_x} \to (\mathcal{F}_{1,\overline{\eta}} \otimes \mathcal{F}_{2,\overline{\eta}})^{I_x} \cong (\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{\eta}}^{I_x}$$

are all injective, hence $\mathcal{F}_1 \otimes \mathcal{F}_2$ has no finitely supported sections, so (2) is established.

For (5), we use Eq. (2.37) to conclude that

$$\begin{aligned}\mathbf{r}(\mathcal{F}_1 \otimes \mathcal{F}_2) &= \dim{(\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{\eta}}} = \dim(\mathcal{F}_{1,\overline{\eta}} \otimes \mathcal{F}_{2,\overline{\eta}}) \\ &= \dim(\mathcal{F}_{1,\overline{\eta}}) \dim(\mathcal{F}_{2,\overline{\eta}}) = \mathbf{r}(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2).\end{aligned} \tag{2.38}$$

Now we check (6). For any closed point $x \in \mathbb{A}^1_\kappa$, we have by Corollary 2.12

$$\mathbf{sw}_x(\mathcal{F}_1 \otimes \mathcal{F}_2) \leq \mathbf{sw}_x(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2) + \mathbf{r}(\mathcal{F}_1)\mathbf{sw}_x(\mathcal{F}_2). \tag{2.39}$$

By definition of the conductor in Eq. (1.17) we have

$$c(\mathcal{F}_1 \otimes \mathcal{F}_2) = \sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa](\mathbf{r}(\mathcal{F}_1 \otimes \mathcal{F}_2) - \dim(\mathcal{F}_1 \otimes \mathcal{F}_2)_{\overline{x}} \ + \mathbf{sw}_x(\mathcal{F}_1 \otimes \mathcal{F}_2))$$

which in view of Eq. (2.36), Eq. (2.38), and Eq. (2.39), is at most

$$\sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa](\mathbf{r}(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2) - \dim \mathcal{F}_{1,\overline{x}} \dim \mathcal{F}_{2,\overline{x}} + \mathbf{sw}_x(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2) + \mathbf{r}(\mathcal{F}_1)\mathbf{sw}_x(\mathcal{F}_2)). \tag{2.40}$$

On the other hand

$$c(\mathcal{F}_1)\mathbf{r}(\mathcal{F}_2) + \mathbf{r}(\mathcal{F}_1)c(\mathcal{F}_2) =$$

$$\sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa] \left((\mathbf{r}(\mathcal{F}_1) - \dim \mathcal{F}_{1,\overline{x}} + \mathbf{sw}_x(\mathcal{F}_1))\mathbf{r}(\mathcal{F}_2) + \mathbf{r}(\mathcal{F}_1)(\mathbf{r}(\mathcal{F}_2) - \dim \mathcal{F}_{2,\overline{x}} + \mathbf{sw}_x(\mathcal{F}_2))\right)$$

which comparing term-by-term, is larger than Eq. (2.40) by

$$\sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa](\mathbf{r}(\mathcal{F}_1) - \dim(\mathcal{F}_{1,x}))(\mathbf{r}(\mathcal{F}_2) - \dim(\mathcal{F}_{2,x})) \geq 0$$

since $\mathcal{F}_1$ and $\mathcal{F}_2$ have no finitely supported sections. □

2.4. **Artin-Schreier sheaves.**

2.4.1. *Residues, exponentiation, additive characters.* A variant of some of the material presented here can also be found in [Hay66].

Each rational function $a \in \mathbb{F}_q(u)$ has a unique expansion

$$a(u) = \sum_{i=-\infty}^{\infty} a_i \cdot \frac{1}{u^i} \tag{2.41}$$

as a Laurent series with $a_i \in \mathbb{F}_q$, such that $a_i = 0$ for all but finitely many negative $i \in \mathbb{Z}$. Using the $i = 1$ coefficient a_1, we set

$$e(a) = \exp\left(\frac{2\pi i \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a_1)}{p}\right) \tag{2.42}$$

where we have identified $\mathbb{F}_p$ with $\{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}$. An alternative definition of a_1 in terms of the residue at infinity is

$$a_1 = -\mathrm{Res}_{\infty}(a). \tag{2.43}$$

To get an explicit expression (or yet another equivalent definition) for a_1 write $a = M/N$ with $M, N \in \mathbb{F}_q[u]$, and let $\widetilde{M}$ be the reduction of M mod N (represented by a unique polynomial of degree less than $\deg(N)$). Then a_1 equals the coefficient of $u^{\deg(N)-1}$ in $\widetilde{M}$ (this is 0 if there is no such coefficient) divided by the leading coefficient of N. In particular, for a polynomial $a \in \mathbb{F}_q[u]$ we have $a_1 = 0$ and thus $e(a) = 1$. One also readily checks, either using Eq. (2.42) or the latter description, that

$$e(a + b) = e(a)e(b)$$

for any $a, b \in \mathbb{F}_q(u)$.

We say that a function $\psi\colon \mathbb{F}_q[u]/(N) \to \mathbb{C}^{\times}$ is an additive character if

$$\psi(f + g) = \psi(f)\psi(g), \quad f, g \in \mathbb{F}_q[u]/(N). \tag{2.44}$$

Using the nondegeneracy of the bilinear map $(x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xy)$, we see that the additive characters are given by

$$\psi_h(M) = e\left(\frac{hM}{N}\right), \quad h \in \mathbb{F}_q[u]/(N). \tag{2.45}$$

2.4.2. *Construction and Properties.* Our construction of Artin-Schreier sheaves will be analogous to that of Kummer sheaves. Both constructions are special cases of the Lang isogeny construction.

Notation 2.14. Let κ be a finite field of characteristic p, let $\psi\colon \kappa \to \overline{\mathbb{Q}_\ell}^{\times}$ be a nontrivial additive character, and let $w \in \kappa(X)$ be a rational function. We construct an ℓ-adic sheaf $\mathcal{L}_\psi(w)$, on the affine line $\mathbb{A}^1_\kappa = \mathrm{Spec}\ \kappa[X]$, as follows.

Write $w = \frac{a}{b}$ with $a, b \in \kappa[X]$ coprime, and $b \neq 0$. Let

$$U = \{x \in \mathbb{A}^1_\kappa : b(x) \neq 0\} \tag{2.46}$$

be the complement of the set S of poles of w, and consider the finite étale cover of U defined by the equation

$$Y^{|\kappa|} - Y = w(X). \tag{2.47}$$

The additive group of κ acts on our cover (by automorphisms) via translation on Y, since for every $\lambda \in \kappa$ we have $(Y+\lambda)^{|\kappa|} - (Y+\lambda) = Y^{|\kappa|} - Y$ in the polynomial ring $\kappa[Y]$. We thus get a simply transitive action of κ on the fiber of any geometric point $\overline{x}$ lying over any point $x \in U$.

Arguing as in the construction of Kummer sheaves, we get a continuous homomorphism $\pi_1^{\text{ét}}(U, \overline{x}) \to \kappa$, so composing with ψ gives rise to a lisse ℓ-adic sheaf of rank one on U. We define $\mathcal{L}_\psi(w)$ to be the extension by zero of this sheaf from U to $\mathbb{A}^1_\kappa$.

We shall now establish some properties of Artin-Schreier sheaves. For the study of local invariants, we will use not only the upper numbering ramification filtration used so far, but also the lower numbering filtration, as defined for instance in [KR14, Definition 3.31]. For a comparison of these filtrations see [KR14, Definition 3.52]

Lemma 2.15. *The sheaf $\mathcal{L}_\psi(w)$ on $\mathbb{A}^1_\kappa$ has the following properties.*

(1) *For every $x \in \kappa$ with $b(x) \neq 0$, we have $t_{\mathcal{L}_\psi(w)}(x) = \psi(w(x))$.*
(2) *The sheaf $\mathcal{L}_\psi(w)$ is lisse on U, and vanishes on $S = \mathbb{A}^1_\kappa - U$.*
(3) *Unless $\deg(a) - \deg(b)$ is a positive multiple of p, we have*

$$\mathrm{slope}_\infty(\mathcal{L}_\psi(w)) = \max\{\deg(a) - \deg(b), 0\}.$$

In particular, if $\deg(a) \leq \deg(b)$, then the sheaf $\mathcal{L}_\psi(w)$ is tamely ramified at ∞.
(4) *The sheaf $\mathcal{L}_\psi(w)$ is mixed of nonpositive weights.*
(5) *The sheaf $\mathcal{L}_\psi(w)$ has no finitely supported sections.*
(6) *We have $\mathbf{r}(\mathcal{L}_{\psi(w)}) = 1$. In case $\deg(a) \leq \deg(b)$ and the multiplicity of every root of b is prime to p, we also have*

$$c(\mathcal{L}_{\psi(w)}) = |\{x \in \overline{\kappa} : b(x) = 0\}| + \deg(b).$$

(7) *There exists a unique $\alpha \in \kappa$ such that $\psi(x^p) = \psi(\alpha x)$ for every $x \in \kappa$, and the sheaf $\mathcal{L}_\psi(w)$ is geometrically trivial on U if and only if there exists an $f \in \kappa(X)$ such that $w = f^p - \alpha f$.*

Proof. Property (2) is immediate from our construction. As in Lemma 2.2, (5) is immediate from (2).

To verify (1), note first that $x \in U$. We get from Eq. (2.47) that the Frobenius element $\mathrm{Frob}_{x,\kappa} \in \pi_1^{\text{ét}}(U, \overline{x})$ acts on the geometric fiber over x by

$$\mathrm{Frob}_{x,\kappa}(x,y) = (x^{|\kappa|}, y^{|\kappa|}) = (x, y^{|\kappa|}) = (x, w(x) + y). \tag{2.48}$$

Hence, by our definition of the representation giving rise to the sheaf $\mathcal{L}_\psi(w)$, the element $w(x) \in \kappa$ is associated to $\mathrm{Frob}_{x,\kappa}$, so $\mathrm{Frob}_{x,\kappa}$ is mapped to $\psi(w(x))$ as desired.

For (3), first consider the case when $\deg(a) \leq \deg(b)$. Then $w = \frac{a}{b}$ lies in the étale local ring of $\mathbb{P}^1$ at ∞, so by the Henselian property all roots of

$$Y^{|\kappa|} - Y = \frac{a(X)}{b(X)} \tag{2.49}$$

lie in that ring. Hence, the extension adjoining such a root is unramified, thus invariant under I_∞^s for all $s \geq 0$, and in particular has slope 0.

Next consider the case when $\deg(a) - \deg(b)$ is positive and prime to p, for which we use the argument of [La81, Example 1.1.7]. The completion at ∞ of the function field of $\mathbb{P}^1$ admits a valuation v satisfying

$$v(X) = -1, \quad v\left(\frac{a(X)}{b(X)}\right) = \deg(b) - \deg(a). \tag{2.50}$$

Adjoining a root y of Eq. (2.47), we can extend our valuation by setting

$$v(y) = \frac{\deg(b) - \deg(a)}{|\kappa|}. \tag{2.51}$$

Since $\deg(b) - \deg(a)$ is prime to $|\kappa|$, there exist integers j_1, j_2 such that

$$j_1 \frac{\deg(b) - \deg(a)}{|\kappa|} - j_2 = \frac{1}{|\kappa|}. \tag{2.52}$$

Consequently $v(y^{j_1} X^{j_2}) = \frac{1}{|\kappa|}$ so $y^{j_1} X^{j_2}$ is a uniformizer. Every nontrivial element σ of the Galois group G of our local extension sends y to $y + c$ for some $c \in \kappa^\times$ so

$$\sigma(y^{j_1} X^{j_2}) = (y + c)^{j_1} X^{j_2} = y^{j_1} X^{j_2} \left(1 + \sum_{m=1}^{j_1} \frac{c^m \binom{j_1}{m}}{y^m}\right). \tag{2.53}$$

Therefore

$$v(\sigma(y^{j_1} X^{j_2}) - y^{j_1} X^{j_2}) = v\left(y^{j_1} X^{j_2} \sum_{m=1}^{j_1} \frac{c^m \binom{j_1}{m}}{y^m}\right) = \frac{1}{|\kappa|} - \frac{\deg(b) - \deg(a)}{|\kappa|}$$

so by the definition of the lower numbering, σ lies in $G_{\deg(a) - \deg(b)}$ but not in $G_{\deg(a) - \deg(b) + 1}$. It follows that the slope is $\deg(a) - \deg(b)$.

To get (4), note that for a closed point $x \in U$, every eigenvalue of $\mathrm{Frob}_{x, \kappa(x)}$ is a value of the finite order character ψ, hence a root of unity whose norm is thus $1 = |\kappa(x)|^{0/2}$, and for $x \notin U$, there are no Frobenius eigenvalues at all. Hence $\mathcal{L}_\psi(w)$ is punctually pure of weight 0 and thus mixed of nonpositive weights.

To get the first part of (6), recall from (2) that $\mathcal{L}_\psi(w)$ is lisse on U, hence it is lisse at a geometric generic point $\overline{\eta}$ of U (and of $\mathbb{A}^1_\kappa$). Therefore the dimension of $\mathcal{L}_\psi(w)_{\overline{\eta}}$ is the rank of the representation giving rise to it, which is 1. For the second part of (6), because $\deg(a) \leq \deg(b)$, the sheaf $\mathcal{L}_\psi(w)$ is infinitame by (3), (4) and (5). Because $\mathcal{L}_\psi(w)$ has rank 1, its Swan conductor at each point is equal to its slope.

To calculate $\mathrm{slope}_x(\mathcal{L}_\psi(w))$ for a closed point $x \in \mathbb{A}^1_\kappa$, we choose a $\overline{\kappa}$-point $\overline{x}$ lying over x, and perform a change of variable that sends ∞ to $\overline{x}$, replacing X with $\overline{x} + \frac{1}{X}$. The degree in X of the rational function

$$\frac{a(\overline{x} + \frac{1}{X})}{b(\overline{x} + \frac{1}{X})} \tag{2.54}$$

is equal to the order of vanishing of b at $\overline{x}$ minus the order of vanishing of a at $\overline{x}$. By (3), the slope of $\mathcal{L}_\psi(w)$ at x is the maximum of this degree and 0, which is the order of vanishing of b at $\overline{x}$ since a and b are coprime.

By the definition in Eq. (1.17) we therefore have

$$\begin{aligned} c(\mathcal{L}_\psi(w)) &= \sum_{x \in |\mathbb{A}^1_\kappa|} [\kappa(x) : \kappa](1 - \dim \mathcal{L}_\chi(w)_{\overline{x}} + \mathrm{ord}_{\overline{x}}(b)) \\ &= \sum_{x \in |U|} [\kappa(x) : \kappa](1 - 1) + \sum_{x \in |S|} [\kappa(x) : \kappa](1 + \mathrm{ord}_{\overline{x}}(b)) \\ &= |\{\overline{x} \in \overline{\kappa} : b(\overline{x}) = 0\}| + \deg(b) \end{aligned} \tag{2.55}$$

where $\mathrm{ord}_{\overline{x}}(b)$ denotes the order of vanishing of b at $\overline{x}$. □

Notation 2.16. For a nonzero polynomial $g \in \mathbb{F}_q[u]$ and a polynomial x in $\mathbb{F}_q[u]$ coprime to g, we denote by $\overline{x} \in \mathbb{F}_q[u]$ the unique polynomial of degree less than $\deg(g)$ satisfying

$$x\overline{x} \equiv 1 \mod g. \tag{2.56}$$

Proposition 2.17. *Let $g \in \mathbb{F}_q[u]$ be squarefree, and let $h \in \mathbb{F}_q[u]$. Then there exists an infinitame g-periodic trace function $t\colon \mathbb{F}_q[u] \to \mathbb{C}$ with*

$$r(t) \leq 1, \quad c(t) \leq 2, \tag{2.57}$$

and

$$t(x) = e\left(\frac{h\overline{x}}{g}\right) \tag{2.58}$$

for every $x \in \mathbb{F}_q[u]$ that is coprime to g.

Proof. We induct on the number of distinct prime factors of g. In the base case, where g is prime, by Eq. (2.45) and Lemma 2.15(1) we have

$$e\left(\frac{h\overline{x}}{g}\right) = \psi_1(hx^{-1}) = t_{\mathcal{L}_{\psi_1}(hX^{-1})}(x). \tag{2.59}$$

The fact that this is an infinitame trace function, and the requisite bounds on the rank and conductor follow from Lemma 2.15(3,4,5,6).

Suppose now that $g = g_1 g_2$ is a nontrivial factorization. Since g is squarefree, the polynomials g_1, g_2 are coprime, so there exist $a, b \in \mathbb{F}_q[u]$ with

$$ag_1 + bg_2 = 1. \tag{2.60}$$

We then have

$$e\left(\frac{h\overline{x}}{g}\right) = e\left(\frac{h\overline{x}}{g_1 g_2}\right) = e\left(\frac{bh\overline{x}}{g_1} + \frac{ah\overline{x}}{g_2}\right) = e\left(\frac{bh\overline{x}}{g_1}\right) e\left(\frac{ah\overline{x}}{g_2}\right). \tag{2.61}$$

By the induction hypothesis, we have a product of an infinitame g_1-periodic trace function and an infinitame g_2-periodic trace function with ranks at most 1 and conductors at most 2. By Definition 1.8, we get an infinitame g-periodic trace function satisfying the rank and conductor bounds. □

2.5. **Abhyankar's Lemma.**

The following version of Abhyankar's lemma, which follows from [SGA1][XIII 5.2], will be of use to us.

Lemma 2.18. *Let X be a smooth scheme over an algebraically closed field κ of characteirstic p, let D be a smooth divisor on X, let $\mathcal{F}$ be a lisse sheaf on $X - D$ with tame monodromy around D, let $f \colon X \to \mathbb{A}^1$ be a map whose zero locus is D with restriction $f_0 \colon X - D \to \mathbb{G}_m$, and let $x \in D$. Suppose that f vanishes to order one on D.*

Then there exists a lisse sheaf $\mathcal{L}$ on $\mathbb{G}_m$ such that $\mathcal{F}$ and $f_0^* \mathcal{L}$ become isomorphic upon restriction to some punctured étale neighborhood of x (namely an étale neighborhood of x with the point over x removed).

Proof. Let R be the étale local ring of X at x, which contains the function f. We can pull $\mathcal{F}$ back to $\operatorname{Spec} R[f^{-1}]$, where it becomes a representation of the tame fundamental group of $\operatorname{Spec} R[f^{-1}]$. By [SGA1][XIII 5.3], the tame fundamental group of $\operatorname{Spec} R[f^{-1}]$ is $\prod_{\ell \neq p} \mathbb{Z}_\ell$, with the isomorphism obtained from the covers taking prime-to-p power roots of f. On the other hand, the tame fundamental group of $\mathbb{G}_m$ is also $\prod_{\ell \neq p} \mathbb{Z}_\ell$, with the isomorphism obtained from the covers taking prime-to-p power roots of the coordinate. So we can view this representation of $\prod_{\ell \neq p} \mathbb{Z}_\ell$ as a lisse sheaf $\mathcal{L}$ on $\mathbb{G}_m$, whose pullback to $\operatorname{Spec} R[f^{-1}]$ is isomorphic to the pullback of $\mathcal{F}$. This isomorphism must then be witnessed on some particular étale cover. □

3. Short sums of trace functions

This section is devoted to proving Theorem 1.10.

3.1. **Vanishing of cohomology.**

Here we obtain a vanishing of cohomology result, which is a key input to the Grothendieck-Lefschetz trace formula.

Notation 3.1. For a variety (that is, a separated geometrically integral scheme of finite type over a field) X we will be working with the bounded derived category $D_c^b(X, \overline{\mathbb{Q}_\ell})$. We use notation such as f_*, f^*, for the derived pushforward and pullback, never the operations on individual sheaves. This is to avoid continually writing $Rf_*, Rf^*, Rf_!$, etc. to refer to these operations.

Note that f^* always sends sheaves to sheaves, as does $\otimes$, and $f_!$ sends sheaves to sheaves if f is an open immersion, so when only these operations have been applied, we will be working with usual sheaves (as opposed to complexes). For brevity of notation, we also occasionally denote the stalk of a sheaf $\mathcal{F}$ at a geometric point $\overline{x}$ lying over a point x by $\mathcal{F}_x$.

Notation 3.2. Let κ be an algebraically closed field of characteristic p. Let $g \in \kappa[u]$ be a squarefree polynomial of degree $m \geq 1$, and let $x_1, \dots, x_m \in \kappa$ be the roots of g. For each $1 \leq i \leq m$, let $\mathcal{F}_i$ be a sheaf on $\mathbb{A}^1 = \mathbb{A}^1_\kappa$. Our interest here is in infinitame trace functions, so we assume for all i that

- the sheaf $\mathcal{F}_i$ has no finitely supported sections;
- the sheaf $\mathcal{F}_i$ has tame local monodromy at ∞, or in other words, it is tamely ramified at infinity.

For one of the sheaves, say $\mathcal{F}_1$, we make a more stringent assumption. Assume that $\mathcal{F}_1$ is the extension by zero of some nontrivial (continuous) one-dimensional $\overline{\mathbb{Q}_\ell}$-representation of the tame étale fundamental group

$$\pi_1^{\text{tame}}\left(\mathbb{A}^1 - \{z\}\right) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell \tag{3.1}$$

for some $z \in \kappa$. This is a geometric form of the assumption in Theorem 1.10 that for some prime we have a Dirichlet trace function. The formulation of this assumption is motivated in part by Lemma 2.2(7).

Let $n \leq m$ be a nonnegative integer, view $\mathbb{A}^n = \mathbb{A}^n_\kappa$ as the space of polynomials over κ of degree less than n, and for every $1 \leq i \leq m$ let

$$e_i \colon \mathbb{A}^n \to \mathbb{A}^1, \qquad e_i(a_0, \dots, a_{n-1}) = a_0 + a_1 x_i + \dots + a_{n-1} x_i^{n-1}, \tag{3.2}$$

be the (linear) map that evaluates a polynomial at x_i. We set

$$\overline{\mathcal{F}} = \bigotimes_{i=1}^{m} e_i^* \mathcal{F}_i$$

and for a subset $S \subseteq \{1, \dots, m\}$ we use the notation

$$\overline{\mathcal{F}}_S = \bigotimes_{i \in S} e_i^* \mathcal{F}_i, \quad \overline{\mathcal{F}}_{\not S} = \bigotimes_{\substack{1 \leq i \leq m \\ i \notin S}} e_i^* \mathcal{F}_i.$$

Our first goal is to prove (in Corollary 3.7) a vanishing statement for the compactly supported cohomology groups $H^j_c\left(\mathbb{A}^n, \overline{\mathcal{F}}\right)$. To do this, view $\mathbb{A}^n$ as the complement of a hyperplane H_∞ in $\mathbb{P}^n = \mathbb{P}^n_\kappa$. Let H_1 be the hyperplane in $\mathbb{P}^n$ obtained as the closure of the hyperplane $e_1^{-1}(z)$ in $\mathbb{A}^n$. Let

$$\begin{gathered} w \colon \mathbb{P}^n - (H_1 \cup H_\infty) \to \mathbb{P}^n - H_\infty = \mathbb{A}^n, \quad v \colon \mathbb{P}^n - H_1 \to \mathbb{P}^n \\ u \colon \mathbb{P}^n - (H_1 \cup H_\infty) \to \mathbb{P}^n - H_1 \end{gathered} \tag{3.3}$$

be the natural open immersions and

$$d \colon H_1 \to \mathbb{P}^n \tag{3.4}$$

the closed immersion.

Finally we put

$$\overline{\mathcal{F}}^\circ = u_! w^* \overline{\mathcal{F}}. \tag{3.5}$$

Since $\mathcal{F}_1$ is an extension by zero from $\mathbb{A}^1 - \{z\}$, its stalk at z vanishes, so the stalk of $e_1^*\mathcal{F}_1$ vanishes for every $x \in e_1^{-1}(z) \subseteq \mathbb{A}^n$. Hence

$$\overline{\mathcal{F}} = w_! w^* \overline{\mathcal{F}}. \tag{3.6}$$

The above implies that for every nonnegative integer j we have

$$H_c^j\Big(\mathbb{A}^n, \overline{\mathcal{F}}\Big) = H_c^j\Big(\mathbb{P}^n - (H_1 \cup H_\infty), w^*\overline{\mathcal{F}}\Big) = H_c^j\Big(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ\Big). \tag{3.7}$$

Our strategy will be focused on the following excision long exact sequence.

Lemma 3.3. *We have the following long exact sequence indexed by $j \in \mathbb{Z}$.*

$$\cdots \to H_c^j\Big(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ\Big) \to H^j\Big(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ\Big) \to H^j\Big(H_1, d^* v_* \overline{\mathcal{F}}^\circ\Big) \to \dots$$

Proof. By [SGA4-3, XVII, (5.1.16.2)] we have a long exact sequence

$$\cdots \to H^*\Big(\mathbb{P}^n, v_! v^* v_* \overline{\mathcal{F}}^\circ\Big) \to H^*\Big(\mathbb{P}^n, v_* \overline{\mathcal{F}}^\circ\Big) \to H^*\Big(\mathbb{P}^n, d_* d^* v_* \overline{\mathcal{F}}^\circ\Big) \to \dots. \tag{3.8}$$

Each term can be simplified in this special case. For the first term, we use the identity $v^* v_* = \mathrm{id}$, and then functoriality of compactly supported pushforward in the derived category tells us that

$$H^*(\mathbb{P}^n, v_! \overline{\mathcal{F}}^\circ) = H_c^*(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ).$$

For the second identity, we use functoriality of pushforward in the derived category to obtain $H^*(\mathbb{P}^n, v_* \overline{\mathcal{F}}^\circ) = H^*(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ)$. For the third identity, we use functoriality of pushforward in the derived category to get $H^*(\mathbb{P}^n, d_* d^* v_* \overline{\mathcal{F}}^\circ) = H^*(H_1, d^* v_* \overline{\mathcal{F}}^\circ)$. □

In order to gain an insight into the cohomology groups in the exact sequence above, our first order of business will be understanding the complex $d^* v_* \overline{\mathcal{F}}^\circ$ of sheaves on H_1.

Given a sheaf $\mathcal{F}$ on a variety X, and a point $x \in X$, we say that $\mathcal{F}$ is lisse at x if there is a neighborhood N of x such that the restriction $\mathcal{F}|_N$ is a lisse sheaf. If $\mathcal{F}$ is not lisse at x, we say that x is a singular point of $\mathcal{F}$.

Lemma 3.4. *Let $Z \subseteq \mathbb{A}^n$ be the set of those polynomials f for which*

$$|\{1 \leq i \leq m : f(x_i) \text{ is a singular point of } \mathcal{F}_i\}| > n. \tag{3.9}$$

The set Z is finite, and the restriction of the complex $v_* \overline{\mathcal{F}}^\circ$ to $H_1 - (H_\infty \cap H_1)$ vanishes away from Z.

Proof. There are only finitely many subsets of $\{1, \dots, m\}$ of size at least n, and for each subset, only finitely many choices of a singular point of each $\mathcal{F}_i$. Since there is at most one polynomial of degree less than n that takes prescribed values for (at least) n given points $x_i \in \kappa$, it follows that the set Z is finite.

Let $j\colon \mathbb{P}^n - H_\infty \to \mathbb{P}^n$ be the open immersion. The Cartesian square

$$\begin{tikzcd}
\mathbb{P}^n - (H_1 \cup H_\infty) \arrow[r, "w"] \arrow[d, "u"] & \mathbb{P}^n - H_\infty \arrow[d, "j"] \\
\mathbb{P}^n - H_1 \arrow[r, "v"] & \mathbb{P}^n
\end{tikzcd}$$

gives $j^* v_* = w_* u^*$ by the base change theorem [SGA4$\frac{1}{2}$, Exp. V, Theorem 3.2] for the smooth morphism j, and u is an open immersion so $u^* u_!$ is the identity, therefore

$$j^* v_* u_! w^* = w_* u^* u_! w^* = w_* w^*. \tag{3.10}$$

Thus it suffices to show that the stalk of the complex $w_* w^* \overline{\mathcal{F}}$ vanishes for every point in H_1 which is neither in H_∞ nor in Z.

Fix a point $f_0 \in H_1$ which is not in H_∞ and not in Z. Since $f_0 \notin H_\infty$, we have $f_0 \in \mathbb{P}^n - H_\infty = \mathbb{A}^n$, and $f_0(x_1) = z$ as $f_0 \in H_1$. Since $f_0 \notin Z$, the set

$$S = \{1 \leq i \leq m : f_0(x_i) \text{ is a singular point of } \mathcal{F}_i\} \tag{3.11}$$

satisfies $|S| \leq n$. We show that the stalk of the complex $w_* w^* \overline{\mathcal{F}}$ at f_0 vanishes. For each $1 \leq i \leq m$ that is not in S, the sheaf $\mathcal{F}_i$ is lisse in a neighborhood of the point $f_0(x_i) = e_i(f_0) \in \mathbb{A}^1$, so the sheaf $e_i^* \mathcal{F}_i$ is lisse in a neighborhood of f_0. Because the pushforward and pullback along an open immersion can be computed locally, and both commute with tensoring by a lisse sheaf, it suffices to prove that the complex

$$w_* w^* \overline{\mathcal{F}}_S = w_* w^* \bigotimes_{i \in S} e_i^* \mathcal{F}_i \tag{3.12}$$

vanishes at f_0.

Since $|S| \leq n$, the maps $\{e_i\}_{i \in S}$ are linearly independent, so we can identify $\mathbb{A}^n$ with $\mathbb{A}^{|S|} \times \mathbb{A}^{n-|S|}$ by using the $\{f(x_i)\}_{i \in S}$ as the coordinates of $\mathbb{A}^{|S|}$. Using this identification we can write

$$\overline{\mathcal{F}}_S \cong \left(\boxtimes_{i \in S} \mathcal{F}_i\right) \boxtimes \overline{\mathbb{Q}_\ell} \tag{3.13}$$

where $\overline{\mathbb{Q}_\ell}$ stands for a constant rank one sheaf on $\mathbb{A}^{n-|S|}$. It follows from our assumptions that $1 \in S$, so we make a further identification of $\mathbb{A}^n$ with $\mathbb{A}^1 \times \mathbb{A}^{|S|-1} \times \mathbb{A}^{n-|S|}$, giving

$$\overline{\mathcal{F}}_S \cong \mathcal{F}_1 \boxtimes \left(\boxtimes_{i \in S \setminus \{1\}} \mathcal{F}_i\right) \boxtimes \overline{\mathbb{Q}_\ell}. \tag{3.14}$$

Taking $\overline{w}\colon \mathbb{A}^1 - \{z\} \to \mathbb{A}^1$ to be the open immersion, our identifications give $w = \overline{w} \times \mathrm{id}^{S \setminus \{1\}} \times \mathrm{id}$, so by Eq. (3.14), the complex from Eq. (3.12) can be expressed as

$$w_* w^* \overline{\mathcal{F}}_S \cong \left(\overline{w} \times \mathrm{id}^{S\setminus\{1\}} \times \mathrm{id}\right)_* \left(\overline{w} \times \mathrm{id}^{S\setminus\{1\}} \times \mathrm{id}\right)^* \left(F_1 \boxtimes \left(\boxtimes_{i \in S \setminus \{1\}} \mathcal{F}_i\right) \boxtimes \overline{\mathbb{Q}_\ell}\right). \tag{3.15}$$

By the Künneth formula, the above equals

$$\left(\overline{w} \times \mathrm{id}^{S\setminus\{1\}} \times \mathrm{id}\right)_* \left(\overline{w}^*\mathcal{F}_1 \boxtimes \left(\boxtimes_{i\in S\setminus\{1\}}\mathcal{F}_i\right) \boxtimes \overline{\mathbb{Q}_\ell}\right) = \overline{w}_*\overline{w}^*\mathcal{F}_1 \boxtimes \left(\boxtimes_{i\in S\setminus\{1\}}\mathcal{F}_i\right) \boxtimes \overline{\mathbb{Q}_\ell}.$$

As $\mathcal{F}_1$ has rank one with nontrivial monodromy around z, the stalk of $\overline{w}_*\overline{w}^*\mathcal{F}_1$ vanishes at z, so the stalk of our external tensor product vanishes at any $f \in \mathbb{A}^n$ with $f(x_1) = z$. In particular, it vanishes at f_0, so the stalk of $w_*w^*\overline{\mathcal{F}}_S$ also vanishes at f_0, as required. □

Lemma 3.5. *The restriction of the complex $v_*\overline{\mathcal{F}}^\circ$ to $H_\infty \cap H_1$ vanishes.*

Proof. We view the points of $\mathbb{P}^n$ as pairs $(f : t)$ of a polynomial f over κ of degree less than n and a scalar $t \in \kappa$, not both zero, up to scaling. Then

$$H_\infty = \{(f : t) \in \mathbb{P}^n \mid t = 0\}, \quad H_1 = \{(f, t) : f(x_1) - zt = 0\}, \tag{3.16}$$

and the map e_i is given by the formula

$$e_i(f : t) = \frac{f(x_i)}{t}, \quad t \neq 0. \tag{3.17}$$

Let $(f_0 : 0) \in H_\infty \cap H_1$, put

$$S = \{1 \leq i \leq m \mid f_0(x_i) = 0\}, \tag{3.18}$$

note that $1 \in S$, and that $|S| < n$ since $f_0 \neq 0$.

Since our goal is to establish the vanishing of the stalk of the complex $v_*\overline{\mathcal{F}}^\circ$ at $(f_0, 0)$, we are free to restrict to an étale neighborhood of $(f_0, 0)$. We will first restrict to a Zariski open neighborhood with a convenient coordinate system, and then further restrict to an étale neighborhood where the sheaves $e_i^*\mathcal{F}_i$ for $i \notin S$ become simpler.

Since $n \leq m$ there exists a subset

$$S \subsetneq T \subseteq \{1, \ldots, m\}, \quad |T| = n. \tag{3.19}$$

Any polynomial of degree less than n is uniquely determined by its values at n distinct points. More precisely, Lagrange's interpolation (or the nonsingularity of the Vandermonde matrix) allows us to write the coefficients of a polynomial f of degree less than n as an invertible linear transformation of the values $\{f(x_i)\}_{i\in T}$. Therefore, the set $\{f(x_i)\}_{i\in T} \cup \{t\}$ forms a projective coordinate system for $\mathbb{P}^n$.

Fix $j \in T \setminus S$, and define the coordinates

$$c_1 = \frac{f(x_1) - zt}{f(x_j)}, \; c_j = \frac{t}{f(x_j)}, \; c_i = \frac{f(x_i)}{f(x_j)}, \; i \in T \setminus \{1, j\}. \tag{3.20}$$

This system of coordinates is obtained from the previous one by dividing all the coordinates by the coordinate $f(x_j)$ and then applying the linear translation $c_1 \mapsto c_1 - zc_j$. Since $f_0(x_j) \neq 0$, it follows that $\{c_i\}_{i\in T}$ forms a coordinate system for the affine neighborhood

$$U = \{(f : t) \in \mathbb{P}^n \mid f(x_j) \neq 0\} \tag{3.21}$$

of $(f_0, 0)$ in $\mathbb{P}^n$. We let $\nu \colon U \to \mathbb{P}^n$ be the open immersion.

In our new coordinates,

$$e_1 = \frac{c_1}{c_j} + z, \quad e_i = \frac{c_i}{c_j},\ i \in T \setminus \{1, j\}. \tag{3.22}$$

Let $U_{1,j}$ be the locus in U where c_1 and c_j are nonzero, and let

$$\xi \colon U_{1,j} \to \mathbb{P}^n - (H_1 \cup H_\infty) \tag{3.23}$$

be the open immersion, well-defined because $\nu^{-1}(H_1)$ is the vanishing locus of c_1 and $\nu^{-1}(H_\infty)$ is the vanishing locus of c_j. We can write

$$U_{1,j} = (\mathbb{A}^1 - \{0\}) \times (\mathbb{A}^{n-1} - \mathbb{A}^{n-2}) \subseteq U \cong \mathbb{A}^n \tag{3.24}$$

where the coordinate in the first factor is c_1, and the coordinates in the second factor are $\{c_i\}_{i \in T \setminus \{1\}}$. We will now express the restriction of the sheaf $\xi^* w^* \overline{\mathcal{F}}$ to a certain punctured étale neighborhood of $(f_0 : 0)$ as the restriction to that neighborhood of the external tensor product of sheaves on each of the two factors of $U_{1,j}$ in Eq. (3.24), see Eq. (3.37) for this expression. We do this for each $1 \leq i \leq m$ separately, distinguishing between the three cases $i \in S \setminus \{1\}$, $i \notin S$, and $i = 1$.

In the first case, following Eq. (3.22), for $i \in S \setminus \{1\}$ we define the (restricted) map

$$\overline{e_i} \colon \mathbb{A}^{n-1} - \mathbb{A}^{n-2} \to \mathbb{A}^1, \quad \overline{e_i}\left((c_k)_{k \in T \setminus \{1\}}\right) = \frac{c_i}{c_j}, \tag{3.25}$$

so that we have

$$\xi^* w^* e_i^* \mathcal{F}_i \cong \overline{\mathbb{Q}_\ell} \boxtimes \overline{e}_i^* \mathcal{F}_i, \quad i \in S \setminus \{1\}. \tag{3.26}$$

In the second case, we take $1 \leq i \leq m$ which is not in S. Let Z_i be the intersection of H_∞ with the vanishing locus of $f(x_i)$. Then, following Eq. (3.17) we can extend e_i to a map

$$\widehat{e_i} \colon \mathbb{P}^n - Z_i \to \mathbb{P}^1, \quad \widehat{e_i}(f : t) = \frac{f(x_i)}{t}. \tag{3.27}$$

Geometrically, we can see that H_∞ is a pole of $\widehat{e_i}$, the vanishing locus of $f(x_i)$ is the zero locus of $\widehat{e_i}$, and the intersection Z_i is the indeterminacy locus.

By our definition of S and choice of i, the point $(f_0 : 0) \in \mathbb{P}^n - Z_i$ lies in the pole and not in the indeterminacy locus, so the map $\widehat{e_i}$ is defined at that point, and we have $\widehat{e_i}(f_0 : 0) = \infty \in \mathbb{P}^1$. On some punctured Zariski neighborhood of ∞ in $\mathbb{P}^1$ the sheaf $\mathcal{F}_i$ is lisse and tamely ramified around ∞, so it follows that there exists a Zariski open neighborhood $U^* \subseteq U$ of $(f_0, 0)$ in $\mathbb{P}^n$ such that on the punctured Zariski open neighborhood

$$U' = U^* - (U^* \cap \widehat{e_i}^{-1}(\infty)) = U^* - (U^* \cap H_\infty)$$

of $(f_0, 0)$ in $\mathbb{P}^n$ the sheaf $e_i^* \mathcal{F}_i$ is lisse and tamely ramified along H_∞. Therefore, on the punctured neighborhood U' of $(f_0, 0)$ in $\mathbb{P}^n$ the sheaf

$$\overline{\mathcal{F}}_{\not{S}} = \bigotimes_{i \notin S} e_i^* \mathcal{F}_i \tag{3.28}$$

is lisse and tamely ramified at H_∞.

We let $\alpha\colon U' \to \mathbb{P}^n - H_\infty$ be the inclusion, let $\delta\colon U^* \to \mathbb{A}^1$ be the restriction of c_j to U^*, and let $\delta_0 : U' \to \mathbb{G}_m$ be the restriction of c_j to U'. Note that $U^* \cap H_\infty$ is a smooth divisor where δ vanishes to order one. We now apply Abhyankar's lemma, as stated in Lemma 2.18, to the scheme U^*, the divisor $U^* \cap H_\infty$, the sheaf $\alpha^* \overline{\mathcal{F}}_{\not g}$ on U', and the map δ. We conclude that there exists an étale neighborhood $V \to U^*$ of $(f_0, 0)$, giving rise to a map $\beta\colon V \times_{U^*} U' \to U'$, and a lisse sheaf $\mathcal{L}_{\not g}$ on $\mathbb{G}_m$, such that

$$\beta^* \alpha^* \overline{\mathcal{F}}_{\not g} \cong \beta^* \delta_0^* \mathcal{L}_{\not g}. \tag{3.29}$$

Let $\tau\colon V \to U$ be the map induced by the composition $V \to U^* \to U$, and let

$$\zeta\colon V \times_U U_{1,j} \to U_{1,j}, \quad \gamma\colon V \times_U U_{1,j} \to V \times_U (U - H_\infty) = V \times_{U^*} U' \tag{3.30}$$

be maps obtained via projections from the fibered product, and via the natural open immersion of $U_{1,j}$ into $U - H_\infty$. We then have

$$\gamma^* \beta^* \alpha^* \overline{\mathcal{F}}_{\not g} \cong \gamma^* \beta^* \delta_0^* \mathcal{L}_{\not g} \tag{3.31}$$

and

$$w \circ \xi \circ \zeta = \alpha \circ \beta \circ \gamma. \tag{3.32}$$

We further define

$$\pi\colon \mathbb{A}^{n-1} - \mathbb{A}^{n-2} \to \mathbb{G}_m = \mathbb{A}^1 - \{0\}, \quad \pi\left((c_i)_{i \in T \setminus \{1\}}\right) = c_j, \tag{3.33}$$

and let $\mathrm{pr}_2\colon U_{1,j} \to \mathbb{A}^{n-1} - \mathbb{A}^{n-2}$ be the projection on the second factor in Eq. (3.24). Then

$$\delta_0 \circ \beta \circ \gamma = \pi \circ \mathrm{pr}_2 \circ \zeta \tag{3.34}$$

because both compositions are given by the coordinate c_j. It follows from Eq. (3.28), Eq. (3.32), Eq. (3.31), and Eq. (3.34) that

$$\zeta^* \xi^* w^* \overline{\mathcal{F}}_{\not g} = \gamma^* \beta^* \alpha^* \overline{\mathcal{F}}_{\not g} \cong \gamma^* \beta^* \delta_0^* \mathcal{L}_{\not g} \cong \zeta^* \mathrm{pr}_2^* \pi^* \mathcal{L}_{\not g} \cong \zeta^* (\overline{\mathbb{Q}_\ell} \boxtimes \pi^* \mathcal{L}_{\not g}). \tag{3.35}$$

We turn now to the third case, namely $i = 1$. Let $\mathcal{L}_\chi$ be the sheaf on $\mathbb{G}_m$ obtained by translating $\mathcal{F}_1$ by z. Then the sheaf $\xi^* w^* e_1^* \mathcal{F}_1$ is the pullback of $\mathcal{L}_\chi$ by the map $\frac{c_1}{c_j}$. By the multiplicative properties of tame rank one lisse sheaves on $\mathbb{G}_m$, this is the tensor product of the pullback of $\mathcal{L}_\chi$ by c_1 with the pullback of its dual $\mathcal{L}_\chi^\vee$ by c_j, so

$$\xi^* w^* e_1^* \mathcal{F}_1 \cong \mathcal{L}_\chi \boxtimes \pi^* \mathcal{L}_\chi^\vee. \tag{3.36}$$

Combining Eq. (3.35), and ζ^* applied to Eq. (3.26) and Eq. (3.36), we see that

(3.37)
$$\begin{aligned}\zeta^*\xi^*w^*\overline{\mathcal{F}} &\cong \zeta^*\left(\overline{\mathbb{Q}_\ell}\boxtimes\bigotimes_{i\in S\backslash\{1\}}\overline{e}_i^*\mathcal{F}_i\right)\otimes\zeta^*(\overline{\mathbb{Q}_\ell}\boxtimes\pi^*\mathcal{L}_{\not g})\otimes\zeta^*(\mathcal{L}_\chi\boxtimes\pi^*\mathcal{L}_\chi^\vee)\\ &\cong \zeta^*\left(\mathcal{L}_\chi\boxtimes\left(\pi^*\mathcal{L}_\chi^\vee\otimes\pi^*\mathcal{L}_{\not g}\otimes\bigotimes_{i\in S\backslash\{1\}}\overline{e}_i^*\mathcal{F}_i\right)\right).\end{aligned}$$

Let

$$\overline{v}\colon \mathbb{A}^1-\{0\}\to\mathbb{A}^1,\quad \overline{u}\colon \mathbb{A}^{n-1}-\mathbb{A}^{n-2}\to\mathbb{A}^{n-1} \tag{3.38}$$

be the inclusions of the locus where c_1, respectively c_j, does not vanish. We have the commutative diagram

$$\begin{tikzcd}
\mathbb{P}^n-H_\infty & \mathbb{P}^n-(H_1\cup H_\infty) \arrow[l, "w"'] \arrow[r, "u"] & \mathbb{P}^n-H_1 \arrow[r, "v"] & \mathbb{P}^n \\
 & (\mathbb{A}^1-\{0\})\times(\mathbb{A}^{n-1}-\mathbb{A}^{n-2}) \arrow[u, "\xi"'] \arrow[r, "\mathrm{id}\times\overline{u}"] & (\mathbb{A}^1-\{0\})\times\mathbb{A}^{n-1} \arrow[u] \arrow[r, "\overline{v}\times\mathrm{id}"] & \mathbb{A}^1\times\mathbb{A}^{n-1} \arrow[u, "\nu"'] \\
 & V\times_U U_{1,j} \arrow[u, "\zeta"'] \arrow[r, "\tilde{u}"] & V\times_U(U-\nu^{-1}H_1) \arrow[u] \arrow[r, "\tilde{v}"] & V \arrow[u, "\tau"']
\end{tikzcd}$$

where all morphisms are étale (hence smooth) and all squares are Cartesian.

We claim that we can make the following series of identifications

$$\begin{gathered}\tau^*\nu^*v_*\overline{\mathcal{F}}^\circ=\tau^*\nu^*v_*u_!w^*\bigotimes_{i=1}^m e_i^*\mathcal{F}_i=\tilde{v}_*\tilde{u}_!\zeta^*\xi^*w^*\bigotimes_{i=1}^m e_i^*\mathcal{F}_i=\\ \tilde{v}_*\tilde{u}_!\zeta^*\Big(\mathcal{L}_\chi\boxtimes\Big(\pi^*\mathcal{L}_\chi^\vee\otimes\pi^*\mathcal{L}_{\not g}\otimes\bigotimes_{i\in S\backslash\{1\}}\overline{e}_i^*\mathcal{F}_i\Big)\Big)=\\ \tau^*(\overline{v}\times\mathrm{id})_*(\mathrm{id}\times\overline{u})_!\Big(\mathcal{L}_\chi\boxtimes\Big(\pi^*\mathcal{L}_\chi^\vee\otimes\pi^*\mathcal{L}_{\not g}\otimes\bigotimes_{i\in S\backslash\{1\}}\overline{e}_i^*\mathcal{F}_i\Big)\Big).\end{gathered}\tag{3.39}$$

The second equality requires base change over all four squares of the above commutative diagram. For the top-right and bottom-right squares, we are base-changing a pushforward by a smooth map, and so we may apply the smooth base change theorem. For the top-left and bottom-left, we are base-chaning a compactly supported pushforward (also by a smooth map), and so we may apply the proper base change theorem. The third equality follows from Eq. (3.37). The fourth equality requires base change along the bottom-left and bottom-right squares, which again uses the smooth and proper base change theorems.

Since the pullbacks τ^* and ν^* are compatible with stalks, it follows from Eq. (3.39) that the stalk of $v_* \overline{\mathcal{F}}^{\circ}$ at $(f_0, 0)$ is isomorphic to the stalk of

$$(\overline{v} \times \mathrm{id})_* (\mathrm{id} \times \overline{u})_! \Big(\mathcal{L}_\chi \boxtimes \Big(\pi^* \mathcal{L}_\chi^\vee \otimes \pi^* \mathcal{L}_{\not{g}} \otimes \bigotimes_{i \in S \setminus \{1\}} \overline{e}_i^* \mathcal{F}_i \Big) \Big) \tag{3.40}$$

at $(f_0, 0)$. To show that the latter stalk vanishes, we invoke the Künneth formula to get

$$\begin{aligned}
&(\overline{v} \times \mathrm{id})_* (\mathrm{id} \times \overline{u})_! \Big(\mathcal{L}_\chi \boxtimes \Big(\pi^* \mathcal{L}_\chi^\vee \otimes \pi^* \mathcal{L}_{\not{g}} \otimes \bigotimes_{i \in S \setminus \{1\}} \overline{e}_i^* \mathcal{F}_i \Big) \Big) = \\
&(\overline{v} \times \mathrm{id})_* \Big(\mathcal{L}_\chi \boxtimes \overline{u}_! \Big(\pi^* \mathcal{L}_\chi^\vee \otimes \pi^* \mathcal{L}_{\not{g}} \otimes \bigotimes_{i \in S \setminus \{1\}} \overline{e}_i^* \mathcal{F}_i \Big) \Big) = \\
&\overline{v}_* \mathcal{L}_\chi \boxtimes \overline{u}_! \Big(\pi^* \mathcal{L}_\chi^\vee \otimes \pi^* \mathcal{L}_{\not{g}} \otimes \bigotimes_{i \in S \setminus \{1\}} \overline{e}_i^* \mathcal{F}_i \Big).
\end{aligned} \tag{3.41}$$

Since we assumed that $\mathcal{F}_1$ has nontrivial local monodromy at z, the rank one sheaf $\mathcal{L}_\chi$ has nontrivial local monodromy at 0, so the stalk of $\overline{v}_* \mathcal{L}_\chi$ at 0 vanishes. We conclude that the stalk of the external tensor product above vanishes at every point U with $c_1 = 0$. In particular, it vanishes at $(f_0 : 0)$. □

Lemma 3.6. *The shifted sheaf* $\overline{\mathcal{F}}[n]$ *is a perverse sheaf.*

Proof. Perversity is an étale-local condition, so it suffices to show that each polynomial $f \in \mathbb{A}^n$ has an étale neighborhood $\nu \colon U \to \mathbb{A}^n$ such that $(\nu^* \overline{\mathcal{F}})[n]$ is perverse. For each $1 \leq i \leq m$, we will choose a suitable étale neighborhood U_i of $e_i(f)$ in $\mathbb{A}^1$ and then take

$$U = (((\mathbb{A}^n \times_{\mathbb{A}^1} U_1) \times_{\mathbb{A}^1} U_2) \dots) \times_{\mathbb{A}^1} U_m, \tag{3.42}$$

which will be an étale neighborhood of f.

Fix $1 \leq i \leq m$. By definition, every section of the stalk of $\mathcal{F}_i$ at $e_i(f)$ is defined over an étale neighborhood of $e_i(f) \in \mathbb{A}^1$. By constructibility,

$$r_i = \dim(\mathcal{F}_i)_{e_i(f)} < \infty \tag{3.43}$$

so there exists an étale neighborhood U_i' of $e_i(f)$ in $\mathbb{A}^1$ over which all the sections of $\mathcal{F}_i$ at $e_i(f)$ are defined. We then have a natural map

$$\psi \colon \overline{\mathbb{Q}_\ell}^{r_i} \to \mathcal{F}_i \mid_{U_i'} \tag{3.44}$$

from a constant sheaf on U_i' of some rank r_i inducing an isomorphism on the stalks at $e_i(f)$. We denote the cokernel of ψ by $\mathcal{Q}_i$, and note that its stalk at $e_i(f)$ vanishes.

Observe that ψ is injective. Indeed if any nontrivial section of $\overline{\mathbb{Q}_\ell}^{r_i}$ has image vanishing on some Zariski open set containing $e_i(f)$, then the corresponding nontrivial section of $\mathcal{F}_i$ is supported in the finite complement of that open set, contradicting the assumption that $\mathcal{F}_i$ has no finitely supported sections. It follows that the restriction of $\mathcal{F}_i$ to U_i' is an extension of $\mathcal{Q}_i$ by $\overline{\mathbb{Q}_\ell}^{r_i}$.

Let U_i be the union with $\{e_i(f)\}$ of the largest open subset of U_i' where $\mathcal{Q}_i$ is lisse. Restricted to U_i, the sheaf $\mathcal{Q}_i$ is lisse on $U_i - \{e_i(f)\}$ and extended by zero to U_i. We define U using Eq. (3.42), and let $\widetilde{e_i}\colon U \to U_i$ for $1 \le i \le m$ and $\nu\colon U \to \mathbb{A}^n$ be the projections.

As $\mathcal{F}_i$ restricted to U_i is an extension of $\mathcal{Q}_i$ by $\overline{\mathbb{Q}_\ell}^{r_i}$, the sheaf $\nu^*\overline{\mathcal{F}}$ is an iterated extension of 2^m sheaves, each of the form

$$\bigotimes_{i\notin S} \widetilde{e_i}^*\overline{\mathbb{Q}_\ell}^{r_i} \otimes \bigotimes_{i\in S} \widetilde{e_i}^*\mathcal{Q}_i, \quad S \subseteq \{1,\dots,m\}. \tag{3.45}$$

Since an extension of perverse sheaves is perverse, it suffices to prove that

$$\left(\bigotimes_{i\notin S} \widetilde{e_i}^*\overline{\mathbb{Q}_\ell}^{r_i} \otimes \bigotimes_{i\in S} \widetilde{e_i}^*\mathcal{Q}_i\right)[n] \tag{3.46}$$

is perverse for any $S \subseteq \{1,\dots,m\}$. Tensoring a sheaf M with the pullback of $\overline{\mathbb{Q}_\ell}^{r_i}$ is equivalent to taking a direct sum of r_i copies of M, so it suffices to show that

$$\left(\bigotimes_{i\in S} \widetilde{e_i}^*\mathcal{Q}_i\right)[n] \tag{3.47}$$

is perverse.

Since each $\mathcal{Q}_i$ is the extension by zero from $U_i - \{e_i(f)\}$ to U_i of a lisse sheaf, the sheaf $\widetilde{e_i}^*\mathcal{Q}_i$ is the extension by zero from $U - \widetilde{e_i}^{-1}\{e_i(f)\}$ to U of a lisse sheaf, and thus the sheaf

$$\bigotimes_{i\in S} \widetilde{e_i}^*\mathcal{Q}_i \tag{3.48}$$

is the extension by zero of a lisse sheaf from the complement in U of

$$D = \bigcup_{i\in S} \widetilde{e_i}^{-1}\{e_i(f)\} \tag{3.49}$$

to U.

We claim that the inclusion of the complement of D in U is an affine open immersion. Since $U_1,\dots,U_m$ are affine schemes, U is affine as well, so it suffices to show that the complement of $\widetilde{e_i}^{-1}\{e_i(f)\}$ is affine as the intersection of affine open subsets of U is an open affine set. Since U_i is étale over $\mathbb{A}^1$, it is a curve so the complement in U_i of (the point over) $e_i(f)$ is affine. The map $\widetilde{e_i}$ is affine, so the inverse image of the aforementioned affine complement is affine, hence our claim is established.

Lisse sheaves shifted by $\dim(U) = \dim(\mathbb{A}^n) = n$ are perverse, and by [BBD82, Corollary 4.1.3], extensions by zero along affine open immersions of perverse sheaves are perverse, so indeed the complex in Eq. (3.47) is perverse. We can thus conclude that $\overline{\mathcal{F}}[n]$ is perverse. □

Corollary 3.7. *We have*

$$H^j_c(\mathbb{A}^n, \overline{\mathcal{F}}) = 0 \tag{3.50}$$

for every integer $j \notin \{n, n+1\}$.

Proof. The vanishing for $j < n$ follows from Artin's affine theorem [BBD82, Corollaire 4.1.2] and the fact, from Lemma 3.6, that $\overline{\mathcal{F}}[n]$ is perverse.

By the excision long exact sequence

$$\dots \to H^j_c\left(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ\right) \to H^j\left(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ\right) \to H^j\left(H_1, d^* v_* \overline{\mathcal{F}}^\circ\right) \to \dots$$

from Lemma 3.3, and Eq. (3.7), to prove vanishing for $j > n+1$, it suffices to show that for $j > n$ we have

$$H^j\left(\mathbb{P}^n - H_1, \overline{\mathcal{F}}^\circ\right) = 0, \quad H^j\left(H_1, d^* v_* \overline{\mathcal{F}}^\circ\right) = 0. \tag{3.51}$$

For the first, note that $\mathbb{P}^n - H_1$ is an affine variety of dimension n, and $\overline{\mathcal{F}}^\circ$ is a sheaf, so we can invoke Artin's affine theorem again.

We shall now prove the second vanishing statement in Eq. (3.51). Since $\overline{\mathcal{F}}^\circ$ is a sheaf on an n-dimensional variety, the complex $\overline{\mathcal{F}}^\circ[n]$ is semiperverse, so $(v_* \overline{\mathcal{F}}^\circ)[n]$ is semiperverse by [BBD82, Corollaire 4.1.3] as v is affine, and

$$\left(d^* v_* \overline{\mathcal{F}}^\circ\right)[n] \tag{3.52}$$

is semiperverse by [BBD82, 4.2.4] because d is a closed immersion. It follows that the stalks of this complex are supported in nonpositive degrees, hence the stalks of the complex $d^* v_* \overline{\mathcal{F}}^\circ$ are supported in degrees not exceeding n.

We know from Lemma 3.4 and Lemma 3.5 that the complex $d^* v_* \overline{\mathcal{F}}^\circ$ is supported at only finitely many points, so its cohomology is simply the direct sum of its stalks. We have seen that these stalks are supported in degrees not exceeding n, so the cohomology indeed vanishes in degrees greater than n, as required for the second part of Eq. (3.51). □

3.2. **Betti numbers bound.**

Here we bound the dimension of the cohomology groups that are not known to vanish by our previous arguments. We let κ be a perfect field of characteristic p.

Definition 3.8. For $K \in D^b_c(\mathbb{A}^1_\kappa, \overline{\mathbb{Q}_\ell})$ define the *rank*

$$\mathbf{r}(K) = \sum_{j=-\infty}^{\infty} \dim \mathcal{H}^j(K)_\eta \tag{3.53}$$

where η is a geometric generic point of $\mathbb{A}^1$, and the *Fourier conductor*

$$c_F(K) = \sum_{j=-\infty}^{\infty} \dim H^j_c(\mathbb{A}^1_{\overline{\kappa(\alpha)}}, K \otimes \mathcal{L}_\psi(\alpha x)) \tag{3.54}$$

where $\kappa(\alpha)$ is the field of rational functions over κ in a variable α, ψ is an additive character of $\mathbb{F}_p$, and $\mathcal{L}_\psi(\alpha x)$ is the Artin-Schreier sheaf.

Note that the rank agrees with the usual notion of the generic rank when K is a sheaf or a perverse sheaf. We call c_F the Fourier conductor because it is equal (by the proper base change theorem) to the rank of the Fourier transform [KL85, Definition 2.1.1]. However, we will not use the characterization in terms of Fourier transform here. The Fourier conductor can also be expressed in terms of local invariants, see Lemma 3.10(5). In order to write this expression, we need the following ad-hoc modification of the Swan conductor.

Definition 3.9. As in Definition 2.7, let V be a representation of an inertia group over $\overline{\mathbb{Q}_\ell}$, and let $V_1, \dots, V_n$ be the Jordan-Hölder factors of V. We set

$$\mathbf{sw}'(V) = \sum_{i=1}^{n} \max\{\mathbf{sw}(V_i) - \dim V_i, 0\} = \sum_{i=1}^{n} \max\{\mathrm{slope}(V_i) - 1, 0\} \dim V_i.$$

For a sheaf $\mathcal{F}$ on an open subset C of a proper curve $\overline{C}/\kappa$ and a closed point x of $\overline{C}$, put

$$\mathbf{sw}'_x(\mathcal{F}) = \mathbf{sw}'(\mathcal{F}_\eta) \tag{3.55}$$

with $\mathcal{F}_\eta$ viewed as a representation of I_x.

Every complex $K \in D_c^b(\mathbb{A}^1_\kappa, \overline{\mathbb{Q}_\ell})$ has a filtration into its truncations $\tau^{\leq p}K$ taken with respect to the perverse t-structure [BBD82, Proposition 1.3.3(i)1], whose associated graded objects are shifts of $\{{}^p\mathcal{H}^j(K)\}_{j\in\mathbb{Z}}$, which are perverse sheaves. We call this the perverse filtration.

Lemma 3.10. (1) *For $K \in D_c^b(\mathbb{A}^1_\kappa, \overline{\mathbb{Q}_\ell})$ we have*

$$\mathbf{r}(K) = \sum_{j=-\infty}^{\infty} \mathbf{r}({}^p\mathcal{H}^j(K)), \quad c_F(K) = \sum_{j=-\infty}^{\infty} c_F({}^p\mathcal{H}^j(K)).$$

(2) *For a short exact sequence of perverse sheaves*

$$0 \to P_1 \to P_2 \to P_3 \to 0,$$

on $\mathbb{A}^1_\kappa$, we have

$$\mathbf{r}(P_2) = \mathbf{r}(P_1) + \mathbf{r}(P_3), \quad c_F(P_2) = c_F(P_1) + c_F(P_3).$$

(3) *For a skyscraper sheaf K on $\mathbb{A}^1_\kappa$, we have*

$$\mathbf{r}(K) = 0, \quad c_F(K) = 1.$$

(4) *For any $\beta \in \overline{\kappa}$, we have*

$$\mathbf{r}(\mathcal{L}_\psi(\beta x)) = 1, \quad c_F(\mathcal{L}_\psi(\beta x)) = 0.$$

(5) *For a sheaf $\mathcal{F}$ on $\mathbb{A}^1_\kappa$ with no finitely supported sections, we have*

$$c_F(\mathcal{F}) = \sum_{x\in|\mathbb{A}^1_\kappa|} \mathbf{c}_x(\mathcal{F}) + \mathbf{sw}'_\infty(\mathcal{F}).$$

(6) *Suppose that κ is finite. Then for an infinitame sheaf $\mathcal{F}$ on $\mathbb{A}^1_\kappa$ we have $c_F(\mathcal{F}) = c(\mathcal{F})$.*

Proof. For (1) and (2), the key point will be that for a perverse sheaf P on $\mathbb{A}^1_\kappa$, the stalk $\mathcal{H}^i(P)_\eta$ vanishes for $i \neq -1$ and

$$H^i_c\left(\mathbb{A}^1_{\overline{\kappa(\alpha)}}, P \otimes \mathcal{L}_\psi(\alpha x)\right) = 0, \quad i \neq 0. \tag{3.56}$$

The vanishing of $\mathcal{H}^i(P)_\eta$ is due to the fact that perverse sheaves on a curve are lisse and supported in degree -1 on an open set. The vanishing in Eq. (3.56) follows from the fact that $P \otimes \mathcal{L}_\psi(\alpha x)$ is perverse on a curve, hence has compactly-supported cohomology in degrees 0 and 1 only, and the cohomology in degree 1 equals the monodromy coinvariants, which vanish for α generic since the representation $\mathcal{L}_\psi(\alpha x)^\vee = \mathcal{L}_\psi(-\alpha x)$ can occur as a quotient of the monodromy representation of P for only finitely many specializations of α.

Write $P_j = {}^p\mathcal{H}^j(K)$. Associated to the perverse filtration, there is a spectral sequence whose first page is

$$E_1^{p,q} = \mathcal{H}^{2p+q}(P_{-p})_\eta$$

converging to $\mathcal{H}^{p+q}(K)_\eta$. Similarly, there is a spectral sequence whose first page is $E_1^{p,q} = H_c^{2p+q}(\mathbb{A}^1_{\overline{\kappa(\alpha)}}, P_{-p} \otimes \mathcal{L}_\psi(\alpha x))$ converging to

$$H_c^{p+q}(\mathbb{A}^1_{\overline{\kappa(\alpha)}}, K \otimes \mathcal{L}_\psi(\alpha x)).$$

Because of the vanishing above, in both spectral sequences we have $E_1^{p,q} = 0$ unless $q = -2p$. Since the differential on the rth page sends $E^{p,q}$ to $E^{p+r,q+1-r}$ and $1 - r = -2r$ only if $r = -1$, the differentials on the rth page for every $r \geq 1$ vanish, and so the spectral sequence degenerates on the first page, giving (1).

We also deduce from the vanishing above that the functors on perverse sheaves $P \mapsto \mathcal{H}^{-1}(P)_\eta$ and $P \mapsto H_c^0(\mathbb{A}^1_{\overline{\kappa(\alpha)}}, P \otimes \mathcal{L}_\psi(\alpha x))$ are exact, and that composing these functors with dimension gives $\mathbf{r}(P)$ and $c_F(P)$ respectively. This proves (2).

For a skyscraper sheaf, its stalk at the generic point vanishes, while its twist by an Artin-Schreier sheaf is again a skyscraper sheaf, so has one-dimensional cohomology in degree zero and no cohomology in all other degrees, verifying (3).

For an Artin-Schreier sheaf, its stalk at the generic point has rank one in degree 0 and none in all other degrees, while its cohomology twisted by any Artin-Schreier sheaf but its dual vanishes, verifying (4).

Now we check (5). Certainly the stalk of $\mathcal{F}$ at the generic point has rank $\mathbf{r}(\mathcal{F})$ in degree 0 and rank zero in other degrees. Since $\mathcal{F}$ has no finitely supported sections, we get that $\mathcal{F}[1]$ is perverse, so $\mathcal{F} \otimes \mathcal{L}_\psi(\alpha x)$ has no cohomology in degrees other than 1, hence

$$c_F(\mathcal{F}) = -\chi(\mathbb{A}^1_{\overline{\kappa(\alpha)}}, \mathcal{F} \otimes \mathcal{L}_\psi(\alpha x)). \tag{3.57}$$

From Lemma 2.10 we get that

$$\chi(\mathbb{A}^1_{\kappa(\alpha)}, \mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) = \chi(\mathbb{A}^1)\mathbf{r}(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) - \sum_{y\in|\mathbb{A}^1_{\kappa(\alpha)}|} \mathbf{c}_y(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) - \mathbf{sw}_\infty(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x))$$

so to establish (5), it suffices to check that for all $y \in \left|\mathbb{A}^1_{\kappa(\alpha)}\right|$, we have

$$\mathbf{c}_y(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) = \mathbf{c}_y(\mathcal{F}) \tag{3.58}$$

and that

$$\mathbf{sw}_\infty(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) - \chi(\mathbb{A}^1)\mathbf{r}(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) = \mathbf{sw}'_\infty(\mathcal{F}). \tag{3.59}$$

Eq. (3.58) is straightforward from Eq. (2.19) since neither the Swan conductor at y nor the drop at y can be changed by tensoring with a lisse sheaf of rank one in a neighborhood of y.

For Eq. (3.59) note that $\chi(\mathbb{A}^1) = 1$ by Eq. (2.22), and that tensoring with a lisse sheaf of rank one does not affect the rank, so it suffices to prove that

$$\mathbf{sw}_\infty(\mathcal{F}\otimes\mathcal{L}_\psi(\alpha x)) - \mathbf{r}(\mathcal{F}) = \mathbf{sw}'_\infty(\mathcal{F}). \tag{3.60}$$

Every term above can be expressed in terms of the representation $V = \mathcal{F}_\eta$ of I_∞, so it suffices to show that

$$\mathbf{sw}(V\otimes\mathcal{L}_\psi(\alpha x)) - \dim(V) = \mathbf{sw}'(V) \tag{3.61}$$

where we have abused notation by using $\mathcal{L}_\psi(\alpha x)$ for both a sheaf and its inertia representation at ∞.

Since all terms above are additive in extensions of irreducible representations, we may assume V is irreducible, in which case it suffices by Definition 2.7 and Definition 3.9 to prove that

$$\operatorname{slope}(V\otimes\mathcal{L}_\psi(\alpha x))\dim(V) - \dim(V) = \max\{\operatorname{slope}(V)-1, 0\}\dim(V) \tag{3.62}$$

or, equivalently, that

$$\operatorname{slope}(V\otimes\mathcal{L}_\psi(\alpha x)) = \max\{\operatorname{slope}(V), 1\}. \tag{3.63}$$

The above follows from Proposition 2.11 once we check that I^1_∞ does not act on V by scalars via the character $\mathcal{L}_\psi(-\alpha x)$. If it were to act by scalars, the character defined by those scalars would be unique, but $\mathcal{L}_\psi(-\alpha x)$ gives distinct characters of I^1_∞ for different specializations of α, so such an action by scalars is impossible for generic α.

At last we deduce (6) from (5). Since $\mathcal{F}$ has no finitely supported sections and is tamely ramified at infinity, it follows from (5), Definition 3.9, Definition 2.7, Definition 2.6, and the definition in Eq. (1.17) that

$$c_F(\mathcal{F}) = \sum_{x\in|\mathbb{A}^1_\kappa|} \mathbf{c}_x(\mathcal{F}) = \sum_{x\in|\mathbb{A}^1_\kappa|} [\kappa(x):\kappa](\mathbf{d}_x(\mathcal{F}) + \mathbf{sw}_x(\mathcal{F})) = c(\mathcal{F}) \tag{3.64}$$

as required for (6). □

3.2.1. *Betti bounds for tensor products.*

Lemma 3.11. *For $K_1 \in D_c^b(\mathbb{A}^1_\kappa, \overline{\mathbb{Q}_\ell})$ and a sheaf K_2 on $\mathbb{A}^1_\kappa$ with no finitely supported sections, we have*

$$\sum_{j=-\infty}^{\infty} \dim H_c^j(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) \leq c_F(K_1)\mathbf{r}(K_2) + \mathbf{r}(K_1)c_F(K_2) + \mathbf{r}(K_1)\mathbf{r}(K_2). \tag{3.65}$$

Proof. First, let us reduce to the case when K_1 is perverse. The perverse filtration on K_1, whose jth associated graded by definition is ${}^p\mathcal{H}^j(K_1)$, induces a filtration on $K_1 \otimes K_2$ whose jth associated graded is ${}^p\mathcal{H}^j(K_1) \otimes K_2$ and thus a filtration on $H^*(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2)$ whose jth associated graded is $H_c^*(\mathbb{A}^1_{\overline{\kappa}}, {}^p\mathcal{H}^j(K_1) \otimes K_2)$. The spectral sequence associated to this filtration converges to $H_c^{p+q}(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2)$ with first page $H_c^{2p+q}(\mathbb{A}^1_{\overline{\kappa}}, {}^p\mathcal{H}^{-p}(K_1) \otimes K_2)$. This spectral sequence gives the inequality

$$\dim H_c^n(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) \leq \sum_{j=-\infty}^{\infty} \dim H_c^{n-j}(\mathbb{A}^1_{\overline{\kappa}}, {}^p\mathcal{H}^j(K_1) \otimes K_2) \tag{3.66}$$

which implies

$$\sum_{i=-\infty}^{\infty} \dim H_c^i(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) \leq \sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty} \dim H_c^i(\mathbb{A}^1_{\overline{\kappa}}, {}^p\mathcal{H}^j(K_1) \otimes K_2). \tag{3.67}$$

Thus the left hand side of Eq. (3.65) is subadditive when we pass to perverse cohomology. By Lemma 3.10(1), the right hand side of Eq. (3.65) is additive when we pass to perverse cohomology. It is therefore sufficient to handle the case when K_1 is perverse. By the same argument, except using Lemma 3.10(2), it suffices to handle the case when K_1 is an irreducible perverse sheaf.

As K_1 is an irreducible perverse sheaf, it is either a skyscraper sheaf or the shift of a middle extension sheaf [BBD82, 5.2.2 (a),(b)], which in particular will have no finitely supported sections. Since both sides of Eq. (3.65) are invariant under shifts, it suffices to handle the case when K_1 is either a skyscraper sheaf or a sheaf with no finitely supported sections.

If $K_1 = \delta_x$ for some $x \in \mathbb{A}^1_\kappa$ is a skyscraper sheaf then by Lemma 3.10(3) we have $c_F(K_1) = 1$ and

$$H_c^i(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) = \mathcal{H}^i(K_2)_x = \begin{cases} K_{2,x} & i = 0 \\ 0 & i \neq 0 \end{cases} \tag{3.68}$$

so since K_2 has no finitely supported sections, we get

$$\sum_{i=-\infty}^{\infty} H_c^i(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) = \dim K_{2,x} \leq \mathbf{r}(K_2) = c_F(K_1)\mathbf{r}(K_2) \tag{3.69}$$

so the required inequality in Eq. (3.65) is satisfied.

Finally, we must check the case when K_1 and K_2 are sheaves with no finitely supported sections. Thus $K_1 \otimes K_2$ has no finitely supported sections either, so $H^0_c(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) = 0$. Hence we have

$$\sum_{i=-\infty}^{\infty} \dim H^i_c(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) = \dim H^1_c(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) + \dim H^2_c(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2)$$

$$= 2 \dim H^2_c(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) - \chi(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2).$$

By [Ka88, 2.0.6], we can identify $H^2_c(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2)$ with the coinvariants of $K_{1,\eta} \otimes K_{2,\eta}$ under the action of $\pi_1^{\text{ét}}(U)$, for some open U in $\mathbb{A}^1_{\overline{\kappa}}$ where K_1, K_2 are lisse. By Lemma 2.10 we have

$$\chi(\mathbb{A}^1_{\overline{\kappa}}, K_1 \otimes K_2) =$$

$$\mathbf{r}(K_1 \otimes K_2) - \sum_{x \in |\mathbb{A}^1_{\overline{\kappa}}|} (\mathbf{r}(K_1 \otimes K_2) - \dim(K_1 \otimes K_2)_x + \mathbf{sw}_x(K_1 \otimes K_2)) - \mathbf{sw}_\infty(K_1 \otimes K_2).$$

We will check that

$$\mathbf{r}(K_1 \otimes K_2) - \dim(K_1 \otimes K_2)_x + \mathbf{sw}_x(K_1 \otimes K_2) \le \mathbf{c}_x(K_1)\mathbf{r}(K_2) + \mathbf{r}(K_1)\mathbf{c}_x(K_2) \tag{3.70}$$

for every $x \in |\mathbb{A}^1_{\overline{\kappa}}|$, and that

$$\begin{aligned} &\mathbf{sw}_\infty(K_1 \otimes K_2) - \mathbf{r}(K_1 \otimes K_2) + 2 \dim(K_{1,\eta} \otimes K_{2,\eta})_{\pi_1^{\text{ét}}(U)} \le \\ &\mathbf{sw}'_\infty(K_1)\mathbf{r}(K_2) + \mathbf{r}(K_1)\mathbf{sw}'_\infty(K_2) + \mathbf{r}(K_1)\mathbf{r}(K_2). \end{aligned} \tag{3.71}$$

The bound in Eq. (3.65) will then follow upon summing Eq. (3.70) over all $x \in |\mathbb{A}^1_{\overline{\kappa}}|$, adding Eq. (3.71), and using Lemma 3.10(5).

For Eq. (3.70), first observe that

$$\dim(K_1 \otimes K_2)_x = \dim(K_{1,x} \otimes K_{2,x}) = \dim(K_{1,x}) \dim(K_{2,x}) \tag{3.72}$$

so that

$$\mathbf{r}(K_1 \otimes K_2) - \dim(K_1 \otimes K_2)_x = \mathbf{r}(K_1)\mathbf{r}(K_2) - \dim(K_{1,x}) \dim(K_{2,x}) \le$$
$$\mathbf{r}(K_1)\mathbf{r}(K_2) - \dim(K_{1,x}) \dim(K_{2,x}) + (\mathbf{r}(K_1) - \dim(K_{1,x}))(\mathbf{r}(K_2) - \dim(K_{2,x})) =$$
$$\mathbf{r}(K_1)(\mathbf{r}(K_2) - \dim(K_{2,x})) + (\mathbf{r}(K_1) - \dim(K_{1,x}))\mathbf{r}(K_2).$$

Next we apply Corollary 2.12 to obtain

$$\mathbf{sw}_x(K_1 \otimes K_2) \le \mathbf{sw}_x(K_1)\mathbf{r}(K_2) + \mathbf{r}(K_1)\mathbf{sw}_x(K_2). \tag{3.73}$$

Eq. (3.70) now follows from the definition of $\mathbf{c}_x(K_1)$ and $\mathbf{c}_x(K_2)$.

We turn to Eq. (3.71). As every global monodromy coinvariant is a coinvariant of the local monodromy at ∞, it suffices to prove that

$$\mathbf{sw}_\infty(K_1 \otimes K_2) + 2 \dim(K_{1,\eta} \otimes K_{2,\eta})_{I_\infty} \le \mathbf{sw}'_\infty(K_1)\mathbf{r}(K_2) + \mathbf{r}(K_1)\mathbf{sw}'_\infty(K_2) + 2\mathbf{r}(K_1)\mathbf{r}(K_2).$$

Both sides above depend only on $V_1 = K_{1,\eta}$ and $V_2 = K_{2,\eta}$ viewed as representations of I_∞. Writing V_1 and V_2 as iterated extensions of irreducible representations, the swan conductor, rank, and $\mathbf{sw}'$ are all additive, while the dimension of the inertia coinvariants is subadditive, so it suffices to handle the case when V_1 and V_2 are irreducible.

In case V_1 and V_2 are irreducible, by Definition 3.9, we must prove that

$$\mathbf{sw}(V_1 \otimes V_2) + 2\dim(V_1 \otimes V_2)_{I_\infty} \leq$$
$$\dim(V_1)\dim(V_2)(\max\{\mathrm{slope}(V_1) - 1, 0\} + \max\{\mathrm{slope}(V_2) - 1, 0\} + 2).$$

Since trivial representations have Swan conductor zero, and

$$\dim(V_1 \otimes V_2)_{I_\infty} = \dim \mathrm{Hom}_{I_\infty}(V_1 \otimes V_2, \overline{\mathbb{Q}_\ell}) = \dim \mathrm{Hom}_{I_\infty}(V_1, V_2^\vee) \leq 1$$

in view of irreducibility, it follows from Proposition 2.11(1) that

$$\begin{aligned}\mathbf{sw}(V_1 \otimes V_2) &\leq (\dim(V_1)\dim(V_2) - \dim(V_1 \otimes V_2)_{I_\infty}) \max\{\mathrm{slope}(V_1), \mathrm{slope}(V_2)\} \\ &\leq (\dim(V_1)\dim(V_2) - \dim(V_1 \otimes V_2)_{I_\infty}) \max\{\mathrm{slope}(V_1), \mathrm{slope}(V_2), 2\} \\ &\leq \dim(V_1)\dim(V_2)\max\{\mathrm{slope}(V_1), \mathrm{slope}(V_2), 2\} - 2\dim(V_1 \otimes V_2)_{I_\infty}\end{aligned}$$

and this is at most

$$\dim(V_1)\dim(V_2)(\max\{\mathrm{slope}(V_1)-1, 0\}+\max\{\mathrm{slope}(V_2)-1, 0\}+2)-2\dim(V_1\otimes V_2)_{I_\infty}$$

so Eq. (3.71) is established. □

We shall need an auxiliary vanishing statement for the cohomology of Artin-Schreier sheaves.

Lemma 3.12. *Let n, m be a positive integers, let $\mathbb{A}^n$ be the affine space over κ, let $e_1, \dots, e_m \colon \mathbb{A}^n \to \mathbb{A}^1$ be affine maps, and let $\alpha_1, \dots, \alpha_m \in \kappa$ be scalars such that the map*

$$e = \sum_{i=1}^{m} \alpha_i e_i \tag{3.74}$$

is nonconstant. Then

$$H_c^*\left(\mathbb{A}^n_{\overline{\kappa}}, \bigotimes_{i=1}^{m} e_i^* \mathcal{L}_\psi(\alpha_i x)\right) = 0. \tag{3.75}$$

Proof. We start with the special case $n = m = 1$, $\alpha_1 = 1$, $e_1 = \mathrm{id}$, where we need to show that

$$H_c^0(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) = H_c^1(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) = H_c^2(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) = 0. \tag{3.76}$$

Vanishing in degree 0 follows from Lemma 2.15(5). For degree 2 we have

$$H_c^2(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) = (\mathcal{L}_\psi(x)_{\overline{\eta}})_{\pi_1^{\text{ét}}(U)} \tag{3.77}$$

for some open $U \subseteq \mathbb{A}^1_{\overline{\kappa}}$ where $\mathcal{L}_\psi(x)$ is lisse as in Lemma 2.15(2). Since $\dim \mathcal{L}_\psi(x)_{\overline{\eta}} = 1$ by Lemma 2.15(6) and $\pi_1^{\text{ét}}(U)$ acts nontrivially, the dimension of the coinvariants is less than 1, so we have the desired vanishing of cohomology in degree 2. In view of the vanishing in degrees 0 and 2, we get from Lemma 2.10, Lemma 2.15(2,6), and Eq. (2.22) that

$$\begin{aligned}\dim H_c^1(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) = -\chi(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) &= \mathbf{sw}_\infty \mathcal{L}_\psi(x) - \chi(\mathbb{A}^1_{\overline{\kappa}})\mathbf{r}(\mathcal{L}_\psi(x)) \\ &= 1 \cdot 1 - 1 = 0.\end{aligned}$$

For the general case, we shall begin by checking that

$$\bigotimes_{i=1}^{m} e_i^* \mathcal{L}_\psi(\alpha_i x) \cong e^* \mathcal{L}_\psi(x). \tag{3.78}$$

Both sheaves are lisse of rank 1 on $\mathbb{A}^n$, so it suffices to check that each σ in $\pi_1^{\text{ét}}(\mathbb{A}^n_\kappa)$ acts on their generic fibers by the same scalar. For each $1 \leq i \leq m$, the action of σ on the generic fiber of $e_i^* \mathcal{L}_\psi(\alpha_i x)$ arises from its action on the finite étale cover $y_i^p - y_i = \alpha_i e_i$ of $\mathbb{A}^n$ (by translation on y_i) composed with ψ, so the action of σ on the generic fiber of the tensor product arises from its action on the product of all these covers, composed with ψ, and multiplying. That is, σ acts by the scalar

$$\prod_{i=1}^{m} \psi(\sigma(y_i) - y_i) = \psi\left(\sum_{i=1}^{m} (\sigma(y_i) - y_i)\right) = \psi\left(\sigma\left(\sum_{i=1}^{m} y_i\right) - \sum_{i=1}^{m} y_i\right).$$

Setting $y = \sum_{i=1}^m y_i$, we see that

$$y^p - y = \sum_{i=1}^{m} y_i^p - \sum_{i=1}^{m} y_i = \sum_{i=1}^{m} \alpha_i e_i = e, \tag{3.79}$$

so σ acts by the same scalar on the generic fiber of $e^* \mathcal{L}_\psi(x)$.

If e is nonconstant, we can use it as a coordinate of $\mathbb{A}^n$, namely write $\mathbb{A}^n = \mathbb{A}^1 \times \mathbb{A}^{n-1}$ with e projecting onto the first factor. From the Künneth formula and Eq. (3.76) we get that

$$\begin{aligned} H_c^*\left(\mathbb{A}^n_{\overline{\kappa}}, \bigotimes_{i=1}^{m} e_i^* \mathcal{L}_\psi(\alpha_i x)\right) &= H_c^*(\mathbb{A}^n_{\overline{\kappa}}, e^* \mathcal{L}_\psi(x)) = H_c^*(\mathbb{A}^1_{\overline{\kappa}} \times \mathbb{A}^{n-1}_{\overline{\kappa}}, \mathcal{L}_\psi(x) \boxtimes \overline{\mathbb{Q}_\ell}) \\ &= H_c^*(\mathbb{A}^1_{\overline{\kappa}}, \mathcal{L}_\psi(x)) \otimes H_c^*(\mathbb{A}^{n-1}_{\overline{\kappa}}, \overline{\mathbb{Q}_\ell}) \\ &= 0 \otimes H_c^*(\mathbb{A}^{n-1}_{\overline{\kappa}}, \overline{\mathbb{Q}_\ell}) = 0. \end{aligned}$$

□

Lemma 3.13. *Let κ be an algebraically closed field of characteristic p, let $x_1, \dots, x_m \in \kappa$ be distinct elements, and let $K_1, \dots, K_m$ be sheaves on $\mathbb{A}^1_\kappa$ with no finitely supported sections. For a nonnegative integer $n \leq m$, view $\mathbb{A}^n_\kappa$ as the space of polynomials of degree less than n, and for $1 \leq i \leq m$ let $e_i \colon \mathbb{A}^n \to \mathbb{A}^1$ be the map that evaluates a polynomial at x_i. We then have*

$$\sum_{j=-\infty}^{\infty} \dim H_c^j\Big(\mathbb{A}^n, \bigotimes_{i=1}^{m} e_i^* K_i\Big) \leq \Big(\prod_{i=1}^{m} (\mathbf{r}(K_i)(1+Z) + c_F(K_i) Z)\Big)[Z^n] \tag{3.80}$$

where Z is a formal variable and $[Z^n]$ is the operator extracting the coefficient of Z^n from a polynomial.

Proof. We will prove this by inductively replacing each K_i with either a skyscraper sheaf δ_{α_i} or an Artin-Schreier sheaf $\mathcal{L}_\psi(\alpha_i x)$. To that end, let us formulate a more general statement, depending on a parameter d, which we will prove by induction.

Fix $0 \leq d \leq m$. Let $\kappa(\alpha_{d+1}, \dots, \alpha_m)$ be the field of rational functions in $m-d$ variables. Let $S \subseteq \{d+1, \dots, m\}$ be a subset, and denote its complement by S^c. Our more general statement is that

$$\sum_{j=-\infty}^{\infty} \dim H_c^j \Big(\mathbb{A}^n_{\overline{\kappa(\alpha_{d+1}, \dots, \alpha_m)}}, \Big(\bigotimes_{i=1}^{d} e_i^* K_i \Big) \otimes \Big(\bigotimes_{i \in S} e_i^* \delta_{\alpha_i} \Big) \otimes \Big(\bigotimes_{i \in S^c} e_i^* \mathcal{L}_\psi(\alpha_i x) \Big) \Big)$$

is at most

$$\Big(Z^{|S|} \prod_{i=1}^{d} (\mathbf{r}(K_i)(1+Z) + c_F(K_i)Z) \Big) [Z^n]. \tag{3.81}$$

Our lemma follows by taking $d = m$.

We prove the above by induction on d. Let us first check the base case, when $d = 0$, so no K_i appear, and Eq. (3.81) is simply 1 if $|S| = n$ and 0 otherwise. In this case, observe that $\bigotimes_{i \in S} e_i^* \delta_{\alpha_i}$ is the constant sheaf on

$$L = \{ f \in \mathbb{A}^n : f(x_i) = \alpha_i, \ i \in S \}. \tag{3.82}$$

As the α_i are independent transcendentals, L is empty in case $|S| > n$, and then the sheaf $\bigotimes_{i \in S} e_i^* \delta_{\alpha_i}$ is zero, so the cohomology is vanishing in all degrees hence the zero bound in Eq. (3.81) is confirmed. In case $|S| \leq n$, the locus L is an affine space of dimension $n - |S|$. By Lemma 3.12, the cohomology of this affine space with coefficients in $\bigotimes_{i \in S^c} e_i^* \mathcal{L}_\psi(\alpha_i x)$ vanishes as long as $\sum_{i \in S^c} \alpha_i e_i$ is nonconstant. Since the α_i are independent transcendentals this sum is nonconstant as soon as one of the e_i (i.e. $f \mapsto f(\alpha_i)$) is nonconstant on L. If $|S| < n$ then all of these forms are nonconstant on L, and because $n \leq m$ by assumption, the set S^c parametrizing these forms is nonempty, so indeed at least one is nonconstant, and the zero bound in Eq. (3.81) is valid also in case $|S| < n$. If $|S| = n$, we are taking the cohomology of a point with coefficients in a (constant) sheaf of rank 1, hence the cohomology is 1-dimensional (concentrated in degree $j = 0$). This verifies the base case.

For the induction step, we first introduce the simplifying notation

$$\kappa_d = \overline{\kappa(\alpha_{d+1}, \dots, \alpha_m)}, \ \overline{K}_d = \bigotimes_{i=1}^{d} e_i^* K_i, \ \overline{\Delta}_S = \bigotimes_{i \in S} e_i^* \delta_{\alpha_i}, \ \overline{A}_{S^c} = \bigotimes_{i \in S^c} e_i^* \mathcal{L}_\psi(\alpha_i x).$$

In this notation, the inductive statement is that

$$\sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^n_{\kappa_d}, \overline{K}_d \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c} \right)$$

is bounded by Eq. (3.81). We assume that the statement is known for $d-1$; we will verify it for d. By the projection formula and the definition of $\overline{K}_d$, for every integer j we have

$$H_c^j \left(\mathbb{A}^n_{\kappa_d}, \overline{K}_d \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c} \right) = H_c^j \left(\mathbb{A}^1_{\kappa_d}, K_d \otimes e_{d,!} \left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c} \right) \right).$$

It follows from Lemma 3.11 that

$$\sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^n_{\kappa_d}, \overline{K}_d \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right) \leq$$
$$\mathbf{r}(K_d) c_F \left(e_{d,!}\left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right)\right) + (\mathbf{r}(K_d) + c_F(K_d))\mathbf{r}\left(e_{d,!}\left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right)\right).$$

Using the fact that κ_{d-1} is an algebraic closure of $\kappa_d(\alpha_d)$, we get from Definition 3.8, the projection formula, and the inductive hypothesis that

$$c_F\left(e_{d,!}\left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right)\right) =$$
$$\sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^1_{\kappa_{d-1}}, \mathcal{L}_\psi(\alpha_d x) \otimes e_{d,!}\left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right)\right) =$$
$$\sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^n_{\kappa_{d-1}}, \overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c \cup \{d\}}\right) \leq$$
$$\left(Z^{|S|} \prod_{i=1}^{d-1} (\mathbf{r}(K_i)(1+Z) + c_F(K_i)Z)\right)[Z^n].$$

We make a similar argument for the rank. To do so, observe that taking the stalk at the generic point is equivalent to taking the stalk, over the field extension of the base field adjoining a new variable α_d, at the point α_d, and this is equivalent to taking the tensor product with the skyscraper sheaf δ_{α_d} and taking cohomology in degree zero. This gives

$$\mathbf{r}\left(e_{d,!}\left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right)\right) = \sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^1_{\kappa_{d-1}}, \delta_{\alpha_d} \otimes e_{d,!}\left(\overline{K}_{d-1} \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right)\right) =$$
$$\sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^n_{\kappa_{d-1}}, \overline{K}_{d-1} \otimes \overline{\Delta}_{S \cup \{d\}} \otimes \overline{A}_{S^c}\right) \leq$$
$$\left(Z^{|S|+1} \prod_{i=1}^{d-1} (\mathbf{r}(K_i)(1+Z) + c_F(K_i)Z)\right)[Z^n].$$

Combining all the bounds above, we obtain

$$\sum_{j=-\infty}^{\infty} \dim H_c^j \left(\mathbb{A}^n_{\kappa_d}, \overline{K}_d \otimes \overline{\Delta}_S \otimes \overline{A}_{S^c}\right) \leq$$
$$\left(Z^{|S|}(\mathbf{r}(K_d) + (\mathbf{r}(K_d) + c_F(K_d))Z) \prod_{i=1}^{d-1} (\mathbf{r}(K_i)(1+Z) + c_F(K_i)Z)\right)[Z^n] =$$
$$\left(Z^{|S|} \prod_{i=1}^{d} (\mathbf{r}(K_i)(1+Z) + c_F(K_i)Z)\right)[Z^n],$$

completing the induction step. □

3.2.2. *Short trace sum bound.*

Corollary 3.14. *Let m be a positive integer, let $g \in \mathbb{F}_q[u]$ be a squarefree polynomial of degree m, and let*

$$t\colon \mathbb{F}_q[u]/(g) \to \mathbb{C} \tag{3.83}$$

be an infinitame trace function, such that for some prime factor τ of g, the function t_τ is a Dirichlet trace function. Then for $n < m$ we have

$$\Big|\sum_{\substack{f\in\mathbb{F}_q[u]\\ \deg(f)<n}} t(f)\Big| \leq q^{\frac{n}{2}+\frac{1}{2}}\Big(\prod_{\pi|g}(r(t_\pi)(1+Z)+c(t_\pi)Z)^{\deg(\pi)}\Big)[Z^n]$$

while for $n \geq m$ we have

$$\sum_{\substack{f\in\mathbb{F}_q[u]\\ \deg(f)<n}} t(f) = 0.$$

Proof. Suppose first that $n < m$.

Let $x_1, \ldots, x_m \in \overline{\mathbb{F}_q}$ be the roots of g ordered in such a way that $\tau(x_1) = 0$. For each prime factor π of g, let $\mathcal{F}_\pi$ be a sheaf on $\mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$ giving rise to the trace function t_π.

Since t_τ is a Dirichlet trace function, in view of Example 1.7 and Notation 2.1, we can take

$$\mathcal{F}_\tau = \mathcal{L}_\chi(c(T-z)) \tag{3.84}$$

where $c \in (\mathbb{F}_q[u]/(\tau))^\times$, $z \in \mathbb{F}_q[u]/(\tau)$, and $\chi\colon (\mathbb{F}_q[u]/(\tau))^\times \to \mathbb{C}^\times$ is a character of order greater than 1.

Fix $1 \leq i \leq m$. Since g is squarefree, there exists a unique prime factor π of g such that $\pi(x_i) = 0$. We define a sheaf $\mathcal{F}_i$ on $\mathbb{A}^1_{\overline{\mathbb{F}_q}}$ to be the base change of $\mathcal{F}_\pi$ along the embedding $\mathbb{F}_q[u]/(\pi) \hookrightarrow \overline{\mathbb{F}_q}$ mapping u to x_i. Since $\tau(x_1) = 0$, for the case $i = 1$ we have $\pi = \tau$, hence $\mathcal{F}_1$ is geometrically isomorphic to the Kummer sheaf $\mathcal{L}_\chi(c(T-z))$, so we conclude from Lemma 2.2(7), that all the assumptions made in Notation 3.2 are satisfied here. From that notation we borrow the evaluation maps $e_i\colon \mathbb{A}^n \to \mathbb{A}^1$ defined in Eq. (3.2).

Let

$$\overline{\mathcal{F}} = \bigotimes_{i=1}^{m} e_i^*\mathcal{F}_i. \tag{3.85}$$

We will construct a sheaf $\mathcal{F}$ on $\mathbb{A}^n_{\mathbb{F}_q}$ such that for every $f \in \mathbb{F}_q[u]$ with $\deg(f) < n$ we have

$$t_{\mathcal{F}}(f) = t(f) \tag{3.86}$$

and the base change of $\mathcal{F}$ to $\mathbb{A}^n_{\overline{\mathbb{F}_q}}$ is isomorphic to $\overline{\mathcal{F}}$.

To do this, fix a prime factor π of g. Let $e_\pi\colon \mathbb{A}^n_{\mathbb{F}_q[u]/(\pi)} \to \mathbb{A}^1_{\mathbb{F}_q[u]/(\pi)}$ be the map sending a polynomial f of degree less than n to $f(u)$ mod π. Let $\delta^\pi\colon \mathbb{A}^n_{\mathbb{F}_q[u]/(\pi)} \to \mathbb{A}^n_{\mathbb{F}_q}$ be the map arising from the field embedding

$\mathbb{F}_q \to \mathbb{F}_q[u]/(\pi)$. The map δ^π is a finite étale Galois cover. Antonio Rojas-León has associated to such a cover in [RL20] a tensor direct image functor $\delta^\pi_{\otimes *}$ from sheaves on the source to sheaves on the target. Using this, we take

$$\mathcal{F} = \bigotimes_{\pi | g} \delta^\pi_{\otimes *} e_\pi^* \mathcal{F}_\pi.$$

To prove Eq. (3.86), we note that

$$t_{\mathcal{F}}(f) = \operatorname{tr}(\mathrm{Frob}_q, \mathcal{F}_f) = \operatorname{tr}\Big(\mathrm{Frob}_q, \bigotimes_{\pi|g} \left(\delta^\pi_{\otimes *} e_\pi^* \mathcal{F}_\pi\right)_f\Big) = \prod_{\pi|g} \operatorname{tr}\left(\mathrm{Frob}_q, \left(\delta^\pi_{\otimes *} e_\pi^* \mathcal{F}_\pi\right)_f\right)$$

$$= \prod_{\pi|g} \operatorname{tr}\left(\mathrm{Frob}_{q^{\deg \pi}}, (e_\pi^* \mathcal{F}_\pi)_f\right) = \prod_{\pi|g} \operatorname{tr}\left(\mathrm{Frob}_{q^{\deg \pi}}, (\mathcal{F}_\pi)_{e_\pi(f)}\right) = \prod_{\pi|g} t_\pi(f) = t(f).$$

Here the first two equalities are by definition of $t_{\mathcal{F}}$ and $\mathcal{F}$, the third is a basic property of tensor products, the key fourth equality is a consequence of [RL20, Proposition 7], the fifth is a basic property of stalks, and the last two are by definition of $\mathcal{F}_\pi$ and t.

We now prove that the base change of $\mathcal{F}$ to $\mathbb{A}^n_{\overline{\mathbb{F}_q}}$ is isomorphic to $\overline{\mathcal{F}}$. It follows from [RL20, Definition 1] that the pullback of $\delta^\pi_{\otimes *} e_\pi^* \mathcal{F}_\pi$ to $\mathbb{A}^n_{\mathbb{F}_q[u]/(\pi)}$ under δ^π is

$$\bigotimes_{\tau \in \mathrm{Gal}(\mathbb{F}_{q[u]/(\pi)}/\mathbb{F}_q)} \tau^* e_\pi^* \mathcal{F}_\pi. \tag{3.87}$$

After making a further pullback (of the sheaf above) to $\overline{\mathbb{F}_q}$, each choice of $\tau \in \mathrm{Gal}(\mathbb{F}_{q[u]/(\pi)}/\mathbb{F}_q)$ induces a different embedding $\iota_\tau \colon \mathbb{F}_q[u]/(\pi) \to \overline{\mathbb{F}_q}$. The pullback of $e_\pi^* \mathcal{F}_\pi$ along such an embedding ι_τ is the pullback of $\iota_\tau^* \mathcal{F}_\pi$ along the map obtained from e_π by applying ι_τ to its coordinates.

For each embedding ι_τ, the element $\iota_\tau(u)$ is the root x_{i_τ} of π for some $1 \le i_\tau \le m$. Since e_π sends f to $f(u)$ and ι_τ sends u to x_{i_τ}, the map obtained from e_π by applying ι_τ to its coordinates sends f to $f(x_{i_\tau})$, namely this map is e_{i_τ}. Similarly, since τ is the embedding $\mathbb{F}_q[u]/(\pi) \to \overline{\mathbb{F}_q}$ sending u to x_{i_τ}, the sheaf $\iota_\tau^* \mathcal{F}_\pi$ is by definition $\mathcal{F}_{i_\tau}$.

It follows that the base change of $\delta^\pi_{\otimes *} e_\pi^* \mathcal{F}_\pi$, or equivalently of the sheaf in Eq. (3.87), to $\mathbb{A}^n_{\overline{\mathbb{F}_q}}$ is

$$\bigotimes_{\tau \in \mathrm{Gal}(\mathbb{F}_{q[u]/(\pi)}/\mathbb{F}_q)} e_{i_\tau}^* \mathcal{F}_{i_\tau} = \bigotimes_{\substack{1 \le i \le m \\ \pi(x_i) = 0}} e_i^* \mathcal{F}_i.$$

Taking the tensor product over all primes π dividing g, we conclude from the definitions of $\mathcal{F}$ and $\overline{\mathcal{F}}$ that the base change of $\mathcal{F}$ to $\mathbb{A}^n_{\overline{\mathbb{F}_q}}$ is indeed isomorphic to $\overline{\mathcal{F}}$.

Since $\mathcal{F}_\pi$ is mixed of nonpositive weights, a property that is preserved under pullback and tensor product, the sheaf in Eq. (3.87) is mixed of nonpositive weights. Thus $\delta^\pi_{\otimes *} e_\pi^* \mathcal{F}_\pi$ is mixed of nonpositive weights, and hence $\mathcal{F}$ is mixed of nonpositive weights.

It follows from Eq. (3.86) and the Grothendieck-Lefschetz trace formula that

$$\left|\sum_{\substack{f\in\mathbb{F}_q[u]\\ \deg f<n}} t(f)\right| = \left|\sum_{x\in\mathbb{A}^n(\mathbb{F}_q)} t_{\mathcal{F}}(x)\right| \leq \sum_{j=-\infty}^{\infty}\left|\operatorname{tr}(\mathrm{Frob}_q, H^j_c(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \overline{\mathcal{F}}))\right|. \tag{3.88}$$

Since $\mathcal{F}$ is mixed of nonpositive weights, Deligne's Riemann Hypothesis and Eq. (3.85) bound the above by

$$\sum_{j=-\infty}^{\infty} q^{j/2}\dim H^j_c\Big(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \bigotimes_{i=1}^m e_i^*\mathcal{F}_i\Big). \tag{3.89}$$

Corollary 3.7 allows us to bound the sum above by

$$q^{\frac{n+1}{2}}\dim H^n_c\Big(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \bigotimes_{i=1}^m e_i^*\mathcal{F}_i\Big) + q^{\frac{n+1}{2}}\dim H^{n+1}_c\Big(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \bigotimes_{i=1}^m e_i^*\mathcal{F}_i\Big). \tag{3.90}$$

Since the sheaves $\mathcal{F}_i$ have no finitely supported sections, and $n \leq m$, we get from Lemma 3.13 that the above is at most

$$q^{\frac{n+1}{2}}\left(\prod_{i=1}^m (\mathbf{r}(\mathcal{F}_i)(1+Z) + c_F(\mathcal{F}_i)Z)\right)[Z^n] \tag{3.91}$$

and since each $\mathcal{F}_\pi$ occurs with multiplicity $\deg(\pi)$ among the $\mathcal{F}_i$, we get

$$q^{\frac{n}{2}+\frac{1}{2}}\left(\prod_{\pi|g} (\mathbf{r}(\mathcal{F}_\pi)(1+Z) + c_F(\mathcal{F}_\pi)Z)^{\deg(\pi)}\right)[Z^n]. \tag{3.92}$$

By Definition 1.4 we have $\mathbf{r}(\mathcal{F}_\pi) = r(t_\pi)$, and since the sheaves $\mathcal{F}_\pi$ are infinitame, we get from Lemma 3.10(6) and Eq. (1.17) that $c_F(\mathcal{F}_\pi) = c(t_\pi)$, so the above equals

$$q^{\frac{n}{2}+\frac{1}{2}}\left(\prod_{\pi|g} (r(t_\pi)(1+Z) + c(t_\pi)Z)^{\deg(\pi)}\right)[Z^n] \tag{3.93}$$

as required.

Suppose now that $n \geq m$. By the Chinese Remainder Theorem, and the fact that each residue class mod g contains q^{n-m} polynomials of degree less than n, we have

$$\sum_{\substack{f\in\mathbb{F}_q[u]\\ \deg(f)<n}} t(f) = q^{n-m}\sum_{f\in\mathbb{F}_q[u]/(g)}\prod_{\pi|g} t_\pi(f) = q^{n-m}\prod_{\pi|g}\sum_{f\in\mathbb{F}_q[u]/(\pi)} t_\pi(f).$$

For $\pi = \tau$ we are summing a Dirichlet trace function over all residue classes, so this sum vanishes, hence the product is zero. □

We deduce Theorem 1.10. Namely for a squarefree $g \in \mathbb{F}_q[u]$, and an infinitame g-periodic trace function t for which there exists a prime $\pi \mid g$ with t_π a Dirichlet trace function, we show that

$$\sum_{\substack{f \in \mathbb{F}_q[u] \\ |f| < X}} t(f) \ll X^{\frac{1}{2}} |g|^{\log_q(2r(t)+c(t))}.$$

Proof of Theorem 1.10. Applying Corollary 3.14 with $n = \lceil \log_q(X) \rceil$, and recalling Definition 1.8, we get the bound

$$\begin{aligned} \sum_{\substack{f \in \mathbb{F}_q[u] \\ |f| < X}} t(f) &\ll q^{\frac{n}{2}+\frac{1}{2}} \left(\prod_{\pi \mid g} (\mathbf{r}(t_\pi)(1+Z) + c_F(t_\pi)Z)^{\deg(\pi)} \right) [Z^n] \\ &\ll X^{\frac{1}{2}} \left(\prod_{\pi \mid g} (r(t)(1+Z) + c(t)Z)^{\deg(\pi)} \right) [Z^n]. \end{aligned} \tag{3.94}$$

The coefficients of the polynomial above are nonnegative, so the coefficient of Z^n is bounded by the sum of all the coefficients. This sum is the value of the polynomial at $Z = 1$ which equals

$$\begin{aligned} \prod_{\pi \mid g} (2r(t) + c(t))^{\deg(\pi)} &= (2r(t) + c(t))^{\sum_{\pi \mid g} \deg(\pi)} \\ &= (2r(t) + c(t))^{\deg(g)} = |g|^{\log_q(2r(t)+c(t))} \end{aligned}$$

so we get the result after multiplying by the factor $X^{\frac{1}{2}}$ from Eq. (3.94). □

4. Möbius function, discriminants, resultants

Notation 4.1. Define an interval $\mathcal{I}$ in $\mathbb{F}_q[u]$ to be a set of the form

$$\mathcal{I}_{f,d} = \{f + g : g \in \mathbb{F}_q[u], \deg(g) < d\} \tag{4.1}$$

for some $f \in \mathbb{F}_q[u]$ and some nonnegative integer d. Define the dimension, length, and degree of the interval $\mathcal{I} = \mathcal{I}_{f,d}$ to be

$$\dim(\mathcal{I}) = d, \quad \operatorname{len}(\mathcal{I}) = q^d, \quad \deg(\mathcal{I}) = \max\{d, \deg(f)\}. \tag{4.2}$$

While f is not uniquely determined by the interval $\mathcal{I}$, it is easy to see that the dimension, length, and degree are.

As an example, the set of monic polynomials of degree d is an interval of dimension d, which we can see by taking $f = u^d$.

Associated to an interval $\mathcal{I} = \mathcal{I}_{f,d}$, we have the subset $\mathcal{I}_{\overline{\mathbb{F}_q}}$ of $\overline{\mathbb{F}_q}[u]$, similarly defined as

$$\mathcal{I}_{\overline{\mathbb{F}_q}} = \{f + g : g \in \overline{\mathbb{F}_q}[u], \deg(g) < d\}. \tag{4.3}$$

For $f + g \in \mathcal{I}_{\overline{\mathbb{F}_q}}$, let $\theta_i(f + g)$ be the coefficient of u^i in $f + g$. Then writing $f = \tau_0 u^0 + \cdots + \tau_{\deg(f)} u^{\deg(f)}$, we get that

$$f + g = \sum_{i=0}^{d-1} \theta_i u^i + \sum_{j=d}^{\deg(f)} \tau_j u^j, \tag{4.4}$$

and so g is uniquely determined by $\theta_0, \dots, \theta_{d-1}$. We say that $\{\theta_i\}_{i=0}^{d-1}$ are the coordinates of $\mathcal{I}_{\overline{\mathbb{F}_q}}$. We call θ_0 the lowest coordinate of $\mathcal{I}_{\overline{\mathbb{F}_q}}$. Note that the number of coordinates of $\mathcal{I}_{\overline{\mathbb{F}_q}}$ is $\dim(\mathcal{I})$.

We say an interval $\mathcal{I}$ is F-adapted for $F \in \mathbb{F}_q[u, T]$ if the degree of $F(u, g(u))$ is independent of $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$ and nonnegative. For an F-adapted interval $\mathcal{I}$, call the degree of $F(u, g(u))$ for $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$ the F-degree.

The next proposition shows that F-adapted intervals satisfy a property that is seemingly slightly stronger.

Proposition 4.2. *Keep Notation 4.1 and Notation 4.11. Let $\mathcal{I}$ be an F-adapted interval in $\mathbb{F}_q[u]$. Then the leading term of $F(u, g(u))$ is also independent of $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$.*

Proof. The coefficient of the highest power u^d of u in $F(u, g(u))$ is a polynomial function P of the coordinates of $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$. Since the degree d of $F(u, g(u))$ is independent of $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$, this polynomial function P vanishes nowhere, so by the Nullstellensatz, it is constant. □

4.1. **Relating the Möbius function to Dirichlet characters.**

The main goal of this section, generalizing [SS19, Section 3], is to prove Corollary 4.12, which gives a formula for the quantity $\mu(F(u, f(u))$ from Theorem 1.3, when restricted to special subsets of the form $f(u) = r(u) + s(u)^p$ for fixed $r(u)$ and varying $s(u)$. Later, we will use this to control the average of $\mu(F(u, f(u)))$ by averaging over each special subset separately.

4.1.1. *Zeuthen's rule.*

We recall Zeuthen's rule from [CCG08, Lemma 4.6] in a slightly generalized form.

Notation 4.3. Let $f_1(u, T)$ and $f_2(u, T)$ be two polynomials in $\mathbb{F}_q[u, T]$. Set

$$Z_{f_i} = \{(a, b) \in \overline{\mathbb{F}_q}^2 : f_i(a, b) = 0\}, \quad i \in \{1, 2\}. \tag{4.5}$$

In case $Z_{f_1} \cap Z_{f_2}$ is finite, for any

$$x = (u_x, t_x) \in \overline{\mathbb{F}_q}^2 \tag{4.6}$$

we denote by

$$i_x(Z_{f_1}, Z_{f_2}) = \dim_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}[u, T]_{(u-u_x, T-t_x)}/(f_1, f_2) \tag{4.7}$$

the intersection number of Z_{f_1} and Z_{f_2} at x. One readily checks that the quantity above is positive if and only if $x \in Z_{f_1} \cap Z_{f_2}$.

Let d, d' be nonnegative integers. As in [CCG08, Section 3], we denote by

$$R_{d,d'}(\alpha(u), \beta(u)) \in \mathbb{F}_q \tag{4.8}$$

the resultant defined by the universal formula for a polynomial $\alpha(u) \in \mathbb{F}_q[u]$ of degree at most d, and a polynomial $\beta(u) \in \mathbb{F}_q[u]$ of degree at most d' in terms of the coefficients of these polynomials (this universal formula is the determinant of the Sylvester matrix associated to α and β). Omitting d, d' we set

$$R(\alpha(u), \beta(u)) = R_{\deg(\alpha),\deg(\beta)}(\alpha(u), \beta(u)). \tag{4.9}$$

In this work, every time we write $R_{d,d'}(\alpha(u), \beta(u))$ we will in fact have $d = \deg(\alpha)$, in which case [CCG08, (3.2)] says that

$$R_{d,d'}(\alpha(u), \beta(u)) = \alpha_d^{d'-\deg(\beta)} R(\alpha(u), \beta(u)) \tag{4.10}$$

where α_d is the coefficient of u^d in $\alpha(u)$. We conclude that

$$R_{d,d''}(\alpha(u), \beta(u)) = \alpha_d^{d''-d'} R_{d,d'}(\alpha(u), \beta(u)) \tag{4.11}$$

for any integer $d'' \geq \deg(\beta)$. We also recall from [CCG08, (3.1)] that

$$R(\alpha(u), \beta(u)) = \alpha_d^{\deg(\beta)} \prod_{\substack{z \in \overline{\mathbb{F}_q} \\ \alpha(z)=0}} \beta(z). \tag{4.12}$$

Occasionally, we will think of $f_1, f_2 \in \mathbb{F}_q[u][T]$ as polynomials in T with coefficients from $\mathbb{F}_q[u]$. For example, the leading coefficient of f_1 is the coefficient of the highest power of T. Moreover, we use the notation $R(f_1, f_2)$ for the resultant of f_1 and f_2, always to be taken with respect to the variable T, producing a polynomial in $\mathbb{F}_q[u]$.

For $\gamma \in \overline{\mathbb{F}_q}[u]$ and $u_0 \in \overline{\mathbb{F}_q}$, we denote by

$$\mathrm{ord}_{u=u_0}\gamma(u) = \sup\{m \geq 0 : (u-u_0)^m \mid \gamma(u)\} \tag{4.13}$$

the order of vanishing of $\gamma(u)$ at $u = u_0$. All of the above is in fact valid for an arbitrary field in place of $\mathbb{F}_q$.

Lemma 4.4. *Keep Notation 4.3, and suppose that $Z_{f_1} \cap Z_{f_2}$ is finite. Then*

$$\mathrm{ord}_{u=u_0} R(f_1, f_2) \geq \sum_{c \in \overline{\mathbb{F}_q}} i_{(u_0,c)}(f_1, f_2) \tag{4.14}$$

for every $u_0 \in \overline{\mathbb{F}_q}$, with equality if the leading coefficient of one of the polynomials f_1, f_2 does not vanish at u_0.

Proof. The case where one leading coefficient does not vanish is [CCG08, Lemma 4.6], so we only prove the inequality above.

Since $Z_{f_1} \cap Z_{f_2}$ is finite, we can find $\lambda \in \overline{\mathbb{F}_q}$ with $(u_0, \lambda) \notin Z_{f_1} \cap Z_{f_2}$. Making the change of variable $T \mapsto T + \lambda$, which preserves both sides of the inequality above, we can assume that $(u_0, 0) \notin Z_{f_1} \cap Z_{f_2}$. In other words, the constant term of one of the polynomials f_1, f_2 does not vanish at u_0.

Let d_1 and d_2 be the degrees of f_1 and f_2 respectively, and set

$$f_1'(u,T) = f_1(u,T^{-1})T^{d_1}, \quad f_2'(u,T) = f_2(u,T^{-1})T^{d_2} \tag{4.15}$$

exchanging the constant and leading terms. Then

$$R(f_1',f_2') = (-1)^{d_1 d_2} R(f_1,f_2) \tag{4.16}$$

so

$$\operatorname{ord}_{u=u_0} R(f_1,f_2) = \operatorname{ord}_{u=u_0} R(f_1',f_2'). \tag{4.17}$$

Since the leading coefficient of one of the polynomials f_1', f_2' does not vanish at u_0, by the previous case we have equality in Eq. (4.14), namely

$$\operatorname{ord}_{u=u_0} R(f_1',f_2') = \sum_{c\in\overline{\mathbb{F}_q}} i_{(u_0,c)}(f_1',f_2'). \tag{4.18}$$

Removing $c=0$, we get

$$\sum_{c\in\overline{\mathbb{F}_q}} i_{(u_0,c)}(f_1',f_2') \geq \sum_{c\in\overline{\mathbb{F}_q}^\times} i_{(u_0,c)}(f_1',f_2'). \tag{4.19}$$

For every $c \in \overline{\mathbb{F}_q}^\times$, mapping T to Y^{-1} induces an isomorphism

$$\overline{\mathbb{F}_q}[u,T]_{(u-u_0,T-c^{-1})} \cong \overline{\mathbb{F}_q}[u,Y]_{(u-u_0,Y-c)} \tag{4.20}$$

hence also the isomorphisms

$$\begin{aligned} &\overline{\mathbb{F}_q}[u,T]_{(u-u_0,T-c^{-1})}/(f_1(u,T),f_2(u,T)) \cong \\ &\overline{\mathbb{F}_q}[u,T]_{(u-u_0,T-c)}/(f_1(u,T^{-1}),f_2(u,T^{-1})) \cong \\ &\overline{\mathbb{F}_q}[u,T]_{(u-u_0,T-c)}/(f_1'(u,T),f_2'(u,T)). \end{aligned} \tag{4.21}$$

Therefore, by definition of intersection numbers in Eq. (4.7), we get

$$i_{(u_0,c^{-1})}(f_1,f_2) = i_{(u_0,c)}(f_1',f_2'). \tag{4.22}$$

Inverting $c \in \overline{\mathbb{F}_q}^\times$, we get

$$\sum_{c\in\overline{\mathbb{F}_q}^\times} i_{(u_0,c)}(f_1',f_2') = \sum_{c\in\overline{\mathbb{F}_q}^\times} i_{(u_0,c)}(f_1,f_2) = \sum_{c\in\overline{\mathbb{F}_q}} i_{(u_0,c)}(f_1,f_2) \tag{4.23}$$

where the last equality holds because the constant term of one of the polynomials f_1, f_2 does not vanish at u_0 so $i_{(u_0,0)}(f_1,f_2)$ vanishes. Combining Eqs. (4.17) to (4.19) and (4.23), we get Eq. (4.14). □

Remark 4.5. The proof above is valid for every algebraically closed field in place of $\overline{\mathbb{F}_q}$.

4.1.2. *Resultant formula.* Using Zeuthen's rule, we prove a formula for a resultant, which we later apply to the resultant of a polynomial and its derivative, namely the discriminant. The latter is related to the value of Möbius by Pellet's formula. Our formula is a variant of [CCG08, Theorem 4.5], with our condition on the interval $\mathcal{I}$ replacing the assumption on the degree therein.

Lemma 4.6. *Keep Notation 4.1 and Notation 4.3. Suppose that $Z_{f_1} \cap Z_{f_2}$ is finite, and let $\mathcal{I}$ be an f_1-adapted interval in $\mathbb{F}_q[u]$. Let d be the f_1-degree of $\mathcal{I}$, and let d' be an integer satisfying*

$$\deg(f_2(u, g(u))) \leq d' \tag{4.24}$$

for $g \in \mathcal{I}_{\overline{\mathbb{F}_q}}$. Then there exists $c \in \mathbb{F}_q^\times$ (depending on $\mathcal{I}, f_1, f_2$) such that

$$R_{d,d'}(f_1(u, g(u)), f_2(u, g(u))) = c \prod_{x \in Z_{f_1} \cap Z_{f_2}} (g(u_x) - t_x)^{i_x(Z_{f_1}, Z_{f_2})} \tag{4.25}$$

for any $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$, using the convention $x = (u_x, t_x)$ from Notation 4.3.

Proof. We assume first that $\dim(\mathcal{I}) \geq 2$, namely that $\mathcal{I}_{\overline{\mathbb{F}_q}}$ has at least two coordinates θ_0, θ_1.

As in the proof of [CCG08, Theorem 4.5], the first step is to prove that there exists $c \in \mathbb{F}_q^\times$ and an assignment of a positive integer e_x to each $x \in Z_{f_1} \cap Z_{f_2}$ such that

$$R_{d,d'}(f_1(u, g), f_2(u, g)) = c \prod_{x \in Z_{f_1} \cap Z_{f_2}} (g(u_x) - t_x)^{e_x} \tag{4.26}$$

for every $g \in \mathcal{I}_{\overline{\mathbb{F}_q}}$. In the proof of this factorization we essentially follow the proof of [CCG08, Lemma 4.4], and the first paragraph in the proof of [CCG08, Theorem 4.5], with some modifications to account for the fact that we range over all polynomials g in a base-changed interval (over $\overline{\mathbb{F}_q}$) rather than over all monic polynomials of a given degree.

Note that the left hand side of Eq. (4.26) is a polynomial in the coordinates of g, and that for every $x \in Z_{f_1} \cap Z_{f_2}$, the polynomial $g(u_x) - t_x$ is linear in the coordinates of g, and thus geometrically irreducible. Moreover, using our assumption that g has at least two coordinates, one readily checks that for any $y \in Z_{f_1} \cap Z_{f_2}$ different from x, the polynomial $g(u_y) - t_y$ in the coordinates of g, is not a multiple of $g(u_x) - t_x$ by a scalar from $\overline{\mathbb{F}_q}$. Hence, by the Nullstellensatz, in order to establish Eq. (4.26) with some $c \in \overline{\mathbb{F}_q}^\times$, it suffices to show that our resultant $R_{d,d'}(f_1(u, g), f_2(u, g))$ vanishes if and only if

$$g(u_x) - t_x = 0 \tag{4.27}$$

for some $x \in Z_{f_1} \cap Z_{f_2}$.

Our resultant vanishes if and only if $f_1(u, g(u))$ and $f_2(u, g(u)))$ share a root $u_0 \in \overline{\mathbb{F}_q}$, or the coefficients of u^d in $f_1(u, g(u))$ and of $u^{d'}$ in $f_2(u, g(u))$

both vanish. The latter possibility is excluded by our definition of d, and the former is equivalent to the existence of an

$$x = (u_0, g(u_0)) \in Z_{f_1} \cap Z_{f_2} \tag{4.28}$$

for which Eq. (4.27) is satisfied. Hence, Eq. (4.26) is established with $c \in \overline{\mathbb{F}_q}^{\times}$.

To check that c is in $\mathbb{F}_q^{\times}$ (and not merely in $\overline{\mathbb{F}_q}^{\times}$), we note that (each linear factor, and thus) the product on the right hand side of Eq. (4.26) is monic when viewed as a polynomial in the lowest coordinate θ_0 of g, so c is a coefficient of the polynomial on the left hand side of Eq. (4.26). The latter is clearly a polynomial over $\mathbb{F}_q$, so indeed $c \in \mathbb{F}_q^{\times}$.

Next, in order to establish Eq. (4.25), we fix $y \in Z_{f_1} \cap Z_{f_2}$, and check that $e_y = i_y(Z_{f_1}, Z_{f_2})$. Since $\dim(\mathcal{I}) \geq 2$, we can find $g_0 \in \mathcal{I}_{\overline{\mathbb{F}_q}}$ such that

$$\{x \in Z_{f_1} \cap Z_{f_2} : g_0(u_x) = t_x\} = \{y\}. \tag{4.29}$$

This choice of g_0 is such that

$$\operatorname{ord}_{z=0}(g_0(u_x) + z - t_x)^{e_x} = \begin{cases} e_y, & x = y \\ 0, & x \neq y \end{cases} \tag{4.30}$$

for any $x \in Z_{f_1} \cap Z_{f_2}$. We conclude from Eq. (4.26) and Eq. (4.30) that

$$\operatorname{ord}_{z=0} R_{d,d'}(f_1(u, g_0 + z), f_2(u, g_0 + z)) = e_y \tag{4.31}$$

and set

$$\widetilde{f_1}(u, z) = f_1(u, g_0 + z), \quad \widetilde{f_2}(u, z) = f_2(u, g_0 + z). \tag{4.32}$$

Since the degree d of $f_1(u, g)$ is independent of $g \in \mathcal{I}_{\overline{\mathbb{F}_q}}$ by the f_1-adaptedness assumption, we see that the coefficient of u^d in $\widetilde{f_1}$ does not vanish for any $z \in \overline{\mathbb{F}_q}$, in particular for $z = 0$. We therefore get from Eq. (4.10) that

$$\operatorname{ord}_{z=0} R_{d,d'}\left(\widetilde{f_1}(u, z), \widetilde{f_2}(u, z)\right) = \operatorname{ord}_{z=0} R\left(\widetilde{f_1}(u, z), \widetilde{f_2}(u, z)\right). \tag{4.33}$$

We apply the case of equality in Lemma 4.4 to the above. This requires checking that

$$\left|Z_{\widetilde{f_1}} \cap Z_{\widetilde{f_2}}\right| < \infty, \tag{4.34}$$

and that the coefficients of the highest powers of u in $\widetilde{f_1}$ and $\widetilde{f_2}$ do not have a common zero at $z = 0$. The former follows from our assumption that $Z_{f_1} \cap Z_{f_2}$ is finite, and the latter was deduced above from our assumption that the degree $f_1(u, g)$ is independent of g. It then follows from Lemma 4.4, Eq. (4.31), and Eq. (4.33) that

$$e_y = \sum_{\lambda \in \overline{\mathbb{F}_q}} i_{(\lambda,0)}(Z_{\widetilde{f_1}}, Z_{\widetilde{f_2}}). \tag{4.35}$$

Using the definition of $\widetilde{f}_1, \widetilde{f}_2$ in Eq. (4.32) we get from the above that

$$e_y = \sum_{\lambda \in \overline{\mathbb{F}_q}} i_{(\lambda, g_0(\lambda))}(Z_{f_1}, Z_{f_2}). \tag{4.36}$$

By construction of g_0 in Eq. (4.29), the summands with $(\lambda, g_0(\lambda)) \neq y$ vanish, so our sum reduces to $i_y(Z_{f_1}, Z_{f_2})$, and it follows that $e_y = i_y(Z_{f_1}, Z_{f_2})$ as required.

Assume now that $\dim(\mathcal{I}) = 1$, so that there exists some $h \in \mathbb{F}_q[u]$ such that

$$\mathcal{I}_{\overline{\mathbb{F}_q}} = \{h + z : z \in \overline{\mathbb{F}_q}\}. \tag{4.37}$$

Recall that we need to establish Eq. (4.25), which in this case can be rewritten as

$$R_{d,d'}(f_1(u, h(u) + z), f_2(u, h(u) + z)) = c \prod_{\alpha \in \overline{\mathbb{F}_q}} (z - \alpha)^{m_\alpha} \tag{4.38}$$

where

$$m_\alpha = \sum_{\substack{x \in Z_{f_1} \cap Z_{f_2} \\ t_x - h(u_x) = \alpha}} i_x(Z_{f_1}, Z_{f_2}). \tag{4.39}$$

As in the previous case, applying Eq. (4.10) and Lemma 4.4 we get that

$$\operatorname{ord}_{z=\alpha} \; R_{d,d'}(f_1(u, h + z), f_2(u, h + z)) \tag{4.40}$$

equals

$$\begin{aligned} \operatorname{ord}_{z=\alpha} \; R(f_1(u, h+z), f_2(u, h+z)) &= \sum_{\lambda \in \overline{\mathbb{F}_q}} i_{(\lambda, \alpha)} \left(Z_{f_1(u,h+z)}, Z_{f_2(u,h+z)}\right) \\ &= \sum_{\lambda \in \overline{\mathbb{F}_q}} i_{(\lambda, \alpha + h(\lambda))} \left(Z_{f_1}, Z_{f_2}\right). \end{aligned}$$

We can restrict the sum above to those $\lambda \in \overline{\mathbb{F}_q}$ with

$$(\lambda, \alpha + h(\lambda)) = (u_x, t_x) \tag{4.41}$$

for some $x \in Z_{f_1} \cap Z_{f_2}$, since the other terms vanish. We then see that our sum equals m_α, so Eq. (4.38) holds with some $c \in \overline{\mathbb{F}_q}^\times$. To show that in fact $c \in \mathbb{F}_q^\times$, one can argue as in the previous case.

Suppose at last that $\dim(\mathcal{I}) = 0$, or equivalently that $\operatorname{len}(\mathcal{I}) = 1$. Note that the left hand side of Eq. (4.25) is in $\mathbb{F}_q$, and by invariance under the action of $\operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, the same is true for the product on the right hand side of Eq. (4.25). Hence, Eq. (4.25) boils down to the fact, proven earlier, that our resultant vanishes if and only if $g(u_x) - t_x = 0$ for some $x \in Z_{f_1} \cap Z_{f_2}$. □

Remark 4.7. It is possible to extract from the proof an explicit expression for the constant c.

Notation 4.8. Keep Notation 4.3. Define the polynomial

$$R^\flat(f_1, f_2) = \mathrm{rad}(R(f_1, f_2)) = \prod_{\pi | R(f_1,f_2)} \pi \tag{4.42}$$

in $\mathbb{F}_q[u]$, and let

$$L(f_1, f_2) \in \mathbb{F}_q[u] \tag{4.43}$$

be the greatest common divisor of the leading coefficients of f_1 and f_2.

Assume from now on that q is odd, and denote the unique multiplicative quadratic character of $\mathbb{F}_q$ by χ_2. For every $x \in \mathbb{F}_q$ we have

$$\chi_2(x) = \begin{cases} 1 & x \in \mathbb{F}_q^{\times 2} \\ -1 & x \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2} \\ 0 & x = 0. \end{cases} \tag{4.44}$$

For $a \in \mathbb{F}_q[u]$ and a nonzero $b \in \mathbb{F}_q[u]$ we denote by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)_2 \tag{4.45}$$

the Jacobi symbol (quadratic residue symbol) in $\mathbb{F}_q[u]$, studied for instance in [Ros02, Chapter 3]. For a nonzero $M \in \mathbb{F}_q[u]$, we denote by

$$N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(M)} \colon \mathbb{F}_q[u]/(M) \to \mathbb{F}_q \tag{4.46}$$

the norm map defined by

$$N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(M)}(f) = \prod_{\substack{a \in \overline{\mathbb{F}_q} \\ M(a)=0}} f(a) \tag{4.47}$$

where $f(a)$ stands for the image of $f \in \mathbb{F}_q[u]/(M)$ in $\overline{\mathbb{F}_q}$ under the map sending u to a. This map is surjective, and we have

$$\chi_2\left(N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(M)}(f)\right) = \left(\frac{f}{M}\right). \tag{4.48}$$

The following proposition, whose proof builds on Lemma 4.6, is the key to deducing Corollary 4.12. It is the generalization of [SS19, Lemma 3.1] needed here.

Proposition 4.9. *Keep Notation 4.8, and the assumptions of Lemma 4.6. Suppose that* $\deg_T(f_1) \geq 1$. *Then there exists a polynomial*

$$W(u, T) \in (\mathbb{F}_q[u]/(R^\flat(f_1, f_2)))[T] \tag{4.49}$$

that satisfies the following two properties.

- *For each root* $a \in \overline{\mathbb{F}_q}$ *of* $R^\flat(f_1, f_2)$, *the image* $W(a, T)$ *of* $W(u, T)$ *in* $\overline{\mathbb{F}_q}[T]$ *under the map sending* u *to* a *satisfies*

$$\mathrm{ord}_{T=b} W(a, T) = i_{(a,b)}(Z_{f_1}, Z_{f_2}) \tag{4.50}$$

for every $b \in \overline{\mathbb{F}_q}$;

- *for all $g \in \mathcal{I}$ we have*

$$\chi_2(R_{d,d'}(f_1(u,g(u)), f_2(u,g(u)))) = \left(\frac{W(u,g)}{R^\flat(f_1,f_2)}\right) \tag{4.51}$$

the right hand side being the Jacobi symbol.

Remark 4.10. The first property above satisfied by $W(u,T)$ determines it up to multiplication by an element of $(\mathbb{F}_q[u]/(R^\flat(f_1,f_2)))^\times$.

Proof. Fix a prime $\pi \mid R^\flat(f_1,f_2)$. For a root $a \in \overline{\mathbb{F}_q}$ of π define the polynomial

$$W^{(\pi,a)}(T) = \prod_{\substack{x \in \overline{\mathbb{F}_q}^2 \\ u_x = a}} (T - t_x)^{i_x(Z_{f_1}, Z_{f_2})} \in \overline{\mathbb{F}_q}[T]. \tag{4.52}$$

That the above is indeed a polynomial follows from the assumption, made in Lemma 4.6, that $Z_{f_1} \cap Z_{f_2}$ is finite.

We claim that $W^{(\pi,a)}(T)$ belongs to $\mathbb{F}_{q^{\deg(\pi)}}[T]$, and that its pullback

$$W_0^{(\pi,a)}(u,T) \in (\mathbb{F}_q[u]/(\pi))[T] \tag{4.53}$$

under the isomorphism from $\mathbb{F}_q[u]/(\pi)$ to $\mathbb{F}_{q^{\deg(\pi)}}$ sending u to a, is independent of the root a.

To prove the claim, note that the function $x \mapsto i_x(Z_{f_1}, Z_{f_2})$ is constant on each orbit of the natural action

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \curvearrowright \overline{\mathbb{F}_q}^2, \tag{4.54}$$

so it is also constant on orbits of the stabilizer of a in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, namely the subgroup

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q(a)) = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^{\deg(\pi)}}). \tag{4.55}$$

It follows that $W^{(\pi,a)}(T)$ is invariant under $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^{\deg(\pi)}})$, hence

$$W^{(\pi,a)}(T) \in \mathbb{F}_{q^{\deg(\pi)}}[T]. \tag{4.56}$$

We also conclude that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ we have

$$\sigma\left(W^{(\pi,a)}(T)\right) = W^{(\pi,\sigma(a))}(T). \tag{4.57}$$

Since the isomorphism from $\mathbb{F}_q[u]/(\pi)$ to $\mathbb{F}_{q^{\deg(\pi)}}$ sending u to $\sigma(a)$ is the composition of σ with the isomorphism sending u to a, we get that $W_0^{(\pi,a)}(u,T)$ is indeed independent of the chosen root a of π. We denote this polynomial by $W_0^{(\pi)}(u,T)$, and use the Chinese Remainder Theorem to define a polynomial

$$W_0(u,T) \in (\mathbb{F}_q[u]/(R^\flat(f_1,f_2)))[T] \tag{4.58}$$

that reduces mod π to $W_0^{(\pi)}(u,T)$ for every $\pi \mid R^\flat(f_1,f_2)$.

Next we claim that

$$N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(R^\flat(f_1,f_2))}(W_0(u,g)) = \prod_{x\in Z_{f_1}\cap Z_{f_2}} (g(u_x)-t_x)^{i_x(Z_{f_1},Z_{f_2})} \tag{4.59}$$

for any $g \in \mathcal{I}$. By definition of the norm map from Eq. (4.47), we have

$$N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(R^\flat(f_1,f_2))}(W_0(u,g)) = \prod_{\substack{a\in\overline{\mathbb{F}_q}\\ R^\flat(f_1,f_2)(a)=0}} W_0(a,g(a)). \tag{4.60}$$

By definition of $W_0(u,T)$, and independence of a, the above equals

$$\prod_{\pi|R^\flat(f_1,f_2)} \prod_{\substack{a\in\overline{\mathbb{F}_q}\\ \pi(a)=0}} W_0^{(\pi,a)}(a,g(a)) = \prod_{\pi|R^\flat(f_1,f_2)} \prod_{\substack{a\in\overline{\mathbb{F}_q}\\ \pi(a)=0}} W^{(\pi,a)}(g(a)). \tag{4.61}$$

From the definition of $W^{(\pi,a)}(T)$ in Eq. (4.52), we get

$$N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(R^\flat(f_1,f_2))}(W_0(u,g)) = \prod_{\substack{x\in Z_{f_1}\cap Z_{f_2}\\ R^\flat(f_1,f_2)(u_x)=0}} (g(u_x)-t_x)^{i_x(Z_{f_1},Z_{f_2})}. \tag{4.62}$$

For every $x \in Z_{f_1}\cap Z_{f_2}$, the polynomials $f_1(u_x,T), f_2(u_x,T)$ vanish at t_x. Hence $R(f_1(u_x,T), f_2(u_x,T)) = 0$, so $R(f_1,f_2)$ vanishes at u_x. From the definition of $R^\flat(f_1,f_2)$ in Eq. (4.42) we conclude that $R^\flat(f_1,f_2)(u_x)=0$, so Eq. (4.62) coincides with the right hand side of Eq. (4.59) as required for our claim.

Finally, we take $c \in \mathbb{F}_q^\times$ from Lemma 4.6 that satisfies

$$c\prod_{x\in Z_{f_1}\cap Z_{f_2}} (g(u_x)-t_x)^{i_x(Z_{f_1},Z_{f_2})} = R_{d,d'}(f_1(u,g(u)), f_2(u,g(u))) \tag{4.63}$$

and choose $c' \in (\mathbb{F}_q[u]/(R^\flat(f_1,f_2)))^\times$ such that $N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/(R^\flat(f_1,f_2))}(c') = c$. Define $W(u,T) = c'W_0(u,T)$, so that from Eq. (4.59) and Eq. (4.63) we get

$$N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/R^\flat(f_1,f_2)}(W(u,g)) = R_{d,d'}(f_1(u,g(u)), f_2(u,g(u))). \tag{4.64}$$

Applying χ_2 to the above, it follows from Eq. (4.48) that

$$\left(\frac{W(u,g)}{R^\flat(f_1,f_2)}\right) = \chi_2\left(N^{\mathbb{F}_q}_{\mathbb{F}_q[u]/R^\flat(f_1,f_2)}(W(u,g))\right) = \chi_2(R_{d,d'}(f_1(u,g),f_2(u,g)))$$

so Eq. (4.51) holds. For $a,b\in\overline{\mathbb{F}_q}$ we have

$$\begin{aligned}\operatorname{ord}_{T=b}W(a,T) &= \operatorname{ord}_{T=b}W_0(a,T) = \operatorname{ord}_{T=b}W_0^{(\pi)}(a,T)\\ &= \operatorname{ord}_{T=b}W_0^{(\pi,a)}(a,T) = \operatorname{ord}_{T=b}W^{(\pi,a)}(T) = i_{(a,b)}(Z_{f_1},Z_{f_2})\end{aligned}$$

so Eq. (4.50) holds. □

4.1.3. *Möbius function formula.* We set up much of the notation needed to state, prove, and apply Corollary 4.12.

Notation 4.11. Keep Notation 4.8. Let $k \geq 1$ be an integer, let

$$F(u,T) = \sum_{i=0}^{k} a_i(u)T^i \in \mathbb{F}_q[u,T], \quad a_k(u) \neq 0, \tag{4.65}$$

and let $c_1, c_2 \in \mathbb{R}$ such that

$$c_1 \geq 0, \quad c_2 \leq 0, \quad \deg(a_i(u)) \leq c_1 + c_2 i, \quad 0 \leq i \leq k. \tag{4.66}$$

We introduce the auxiliary function

$$E(c_1, c_2, x) = 2kc_1 + k\max\{0, c_2 + x\} - k + c_2k^2, \quad x \in \mathbb{R}. \tag{4.67}$$

Let $\overline{\mathbb{F}_q(u)}$ be an algebraic closure of $\mathbb{F}_q(u)$, and let $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{F}_q(u)}$ be such that

$$F(u,T) = a_k \prod_{i=1}^{k} (T - \alpha_i). \tag{4.68}$$

We assume that F is separable as a polynomial in T, namely that the roots $\alpha_1, \ldots, \alpha_k$ are distinct. Equivalently the derivative $\frac{\partial F}{\partial T}$ of F with respect to the variable T, which we also denote by $\partial_T F$, does not vanish at $T = \alpha_i$ for any $1 \leq i \leq k$.

Set

$$F_v = \partial_u F + v\partial_T F \in \mathbb{F}_q[u,T,v]. \tag{4.69}$$

For a polynomial $r \in \mathbb{F}_q[u]$ we denote its derivative by ∇r, and put

$$F_{\nabla r} = \sum_{j=0}^{k} b_j(u)T^j \in \mathbb{F}_q[u,T] \tag{4.70}$$

where

$$b_j = \nabla a_j + (j+1)a_{j+1}\nabla r, \quad 1 \leq j \leq k-1, \quad b_k = \nabla a_k. \tag{4.71}$$

Following Eq. (4.43), in case $F_{\nabla r} \neq 0$, we further set

$$k' = \deg_T(F_{\nabla r}),\ L_{F,r} = L(F, F_{\nabla r}) = \gcd(a_k, b_{k'}) \in \mathbb{F}_q[u]. \tag{4.72}$$

Denote by

$$R(F, F_v) \in \mathbb{F}_q[u,v], \quad R(F, F_{\nabla r}) \in \mathbb{F}_q[u] \tag{4.73}$$

the resultants in the variable T. By Eq. (4.12) and Eq. (4.69), we have

$$\begin{aligned} R(F,F_v) &= a_k^{\deg_T F_v} \prod_{i=1}^{k} F_v(u,\alpha_i) \\ &= a_k^{\deg_T F_v} \prod_{i=1}^{k} \left(\partial_u F(u,\alpha_i) + v\partial_T F(u,\alpha_i)\right). \end{aligned} \tag{4.74}$$

Following Eq. (4.42), define

$$M_{F,r} = R^\flat(F, F_{\nabla r}) = \mathrm{rad}(R(F, F_{\nabla r})) = \prod_{\pi \mid R(F,F_{\nabla r})} \pi. \tag{4.75}$$

Let $\mathcal{I}$ be an interval in $\mathbb{F}_q[u]$ such that for some $r \in \mathcal{I}$ the assumptions of Proposition 4.9 are satisfied for $f_1 = F,\ f_2 = F_{\nabla r}$, with d' the least even integer satisfying Eq. (4.24). We can then fix a polynomial

$$W_{F,r}(u,T) \in (\mathbb{F}_q[u]/(M_{F,r}))[T] \tag{4.76}$$

such that for each root $a \in \overline{\mathbb{F}_q}$ of $M_{F,r}$ and $b \in \overline{\mathbb{F}_q}$ we have

$$\mathrm{ord}_{T=b} W_{F,r}(a,T) = i_{(a,b)}(Z_F, Z_{F_{\nabla r}}), \tag{4.77}$$

and for all $g \in \mathcal{I}$ we have

$$\chi_2(R_{d,d'}(F(u,g), F_{\nabla r}(u,g))) = \left(\frac{W_{F,r}(u,g)}{M_{F,r}}\right). \tag{4.78}$$

For a prime $\pi \mid M_{F,r}$, we denote by

$$W_{F,r}^{(\pi)}(T) \in (\mathbb{F}_q[u]/(\pi))[T] \tag{4.79}$$

the reduction of $W_{F,r}$ mod π.

For a polynomial $f \in \mathbb{F}_q[u]$ we define its discriminant, following [CCG08, (2.3)], to be

$$\Delta(f) = \prod_{i<j} (\gamma_i - \gamma_j)^2. \tag{4.80}$$

where $\gamma_1, \dots, \gamma_{\deg(f)}$ are the roots of f in $\overline{\mathbb{F}_q}$. Denoting the leading coefficient of f by f_0, and the degree of f by d, we learn from [CCG08, (3.3)] that

$$\Delta(f) = \frac{(-1)^{\frac{d(d-1)}{2}} R_{d,d-1}(f, \nabla f)}{f_0^{2d-1}}. \tag{4.81}$$

If we want to emphasize that the discriminant is taken with respect to the variable u, we write $\Delta_u(f)$. For instance,

$$\Delta_v(R(F, F_v)) \in \mathbb{F}_q[u] \tag{4.82}$$

stands for the discriminant with respect to v of the resultant in the variable T of the polynomials F and F_v as above.

The following corollary is the generalization of [SS19, Lemma 3.2] needed to prove Theorem 1.3. The proof mainly rests on Proposition 4.9 and Pellet's formula

$$\mu(f) = (-1)^{\deg(f)} \chi_2(\Delta(f)), \quad f \in \mathbb{F}_q[u] \tag{4.83}$$

as given in [CCG08, (2.5)].

Corollary 4.12. *Keep Notation 4.1 and Notation 4.11. Let $\mathcal{I}$ be an F-adapted interval in $\mathbb{F}_q[u]$, and fix $r \in \mathcal{I}$. Suppose that $Z_F \cap Z_{F_{\nabla r}}$ is finite. Then for any $s \in \mathbb{F}_q[u]$ with $\deg(s) < \frac{\dim(\mathcal{I})}{p}$ we have*

$$\mu(F(u, r + s^p)) = (-1)^d \chi_2(-1)^{\frac{d(d-1)}{2}} \chi_2(a)^d \left(\frac{W_{F,r}(u, r + s^p)}{M_{F,r}} \right). \tag{4.84}$$

Proof. By Proposition 4.2, the leading term of $F(u, g(u))$ is independent of $g(u) \in \mathcal{I}_{\overline{\mathbb{F}_q}}$. Let au^d be this fixed leading term.

By Pellet's formula above, we have

$$\mu(F(u, r + s^p)) = (-1)^d \chi_2(\Delta(F(u, r + s^p))), \tag{4.85}$$

so applying Eq. (4.81), we see that the above equals

$$(-1)^d \chi_2(-1)^{\frac{d(d-1)}{2}} \chi_2(a) \chi_2 \left(R_{d,d-1} \left(F(u, r + s^p), \nabla F(u, r + s^p) \right) \right).$$

Using the Leibniz derivative product rule, the chain rule, and the fact that derivatives of p-th powers vanish, we arrive at

$$(-1)^d \chi_2(-1)^{\frac{d(d-1)}{2}} \chi_2(a) \chi_2 \left(R_{d,d-1} \left(F(u, r + s^p), F_{\nabla r}(u, r + s^p) \right) \right). \tag{4.86}$$

Applying Eq. (4.11), the above becomes

$$(-1)^d \chi_2(-1)^{\frac{d(d-1)}{2}} \chi_2(a)^{d-d'} \chi_2 \left(R_{d,d'} \left(F(u, r + s^p), F_{\nabla r}(u, r + s^p) \right) \right) \tag{4.87}$$

with d' defined in Notation 4.11, so using Eq. (4.78) we get

$$(-1)^d \chi_2(-1)^{\frac{d(d-1)}{2}} \chi_2(a)^{d-d'} \left(\frac{W(u, r + s^p)}{M_{F,r}} \right). \tag{4.88}$$

Since d' is even we have $\chi_2(a)^{d-d'} = \chi_2(a)^d$, so we arrive at the right hand side of Eq. (4.84). □

4.2. **Tools for applying the Möbius function formula.** Here we prove several claims that help verify the hypotheses of Corollary 4.12, deal with the cases when these fail, make the application of Corollary 4.12 more effective, and relate it to the trace function bounds we proved earlier.

4.2.1. *Infinite intersection.* We show that on special subsets for which the finite intersection condition in Corollary 4.12 fails, the Möbius function vanishes almost everywhere.

Proposition 4.13. *Keep Notation 4.11. Let $r \in \mathbb{F}_q[u]$ for which $Z_F \cap Z_{F_{\nabla r}}$ is infinite. Then*

$$|\{s \in \mathbb{F}_q[u] : \mu(F(u, r + s^p)) \neq 0\}| \leq k(q - 1). \tag{4.89}$$

Proof. Since the two zero loci have infinite intersection, it follows from Bezout's Theorem that F and $F_{\nabla r}$ share a common irreducible factor $P(u, T)$. From the chain rule, and the fact that derivatives of pth powers vanish in characteristic p, we get that

$$F_{\nabla r}(u, r + s^p) = \nabla F(u, r + s^p). \tag{4.90}$$

We conclude that both $F(u, r + s^p)$ and its derivative $\nabla F(u, r + s^p)$ are divisible by $P(u, r + s^p)$, hence $\mu(F(u, r + s^p)) = 0$ once $P(u, r + s^p) \notin \mathbb{F}_q^\times$. Because $P(u, r + s^p)$ is a polynomial in s^p of degree at most k, there are at most $(q - 1)k$ choices of $s^p \in \mathbb{F}_q(u)$ for which

$$P(u, r + s^p) \in \mathbb{F}_q^\times. \tag{4.91}$$

The proposition follows since in a field of characteristic p, the map $s \mapsto s^p$ is injective. □

4.2.2. *Partitioning an interval.* In order to prove (a generalized form of) Theorem 1.3 we need to control suns of the form $\sum_{g \in \mathcal{I}} \mu(F(u, g))$. For the Möbius function formula from Corollary 4.12 to apply, we need the leading term of $F(u, g)$ to be independent of g. Since this is not always the case, we introduce the following lemma partitioning $\mathcal{I}$ into well-behaved subintervals. This will allow us to avoid unnecessary monicity conditions and certain inequalities on degrees as in [SS19, Theorem 4.5].

Lemma 4.14. *Keep Notation 4.1 and Notation 4.11. For every interval $\mathcal{I}$ in $\mathbb{F}_q[u]$, there exists a collection $\mathcal{P}$ of intervals in $\mathbb{F}_q[u]$ such that*

1. *every $\mathcal{J} \in \mathcal{P}$ is contained in $\mathcal{I}$.*
2. *for every $f \in \mathcal{I}$ there exists $\mathcal{J} \in \mathcal{P}$ with $f \in \mathcal{J}$;*
3. *for every two distinct intervals $\mathcal{J}, \mathcal{K} \in \mathcal{P}$ we have $\mathcal{J} \cap \mathcal{K} = \emptyset$;*
4. *Each $\mathcal{J} \in \mathcal{P}$, is either F-adapted or has length 1.*
5. *for each $0 \leq j \leq \dim(\mathcal{I}) - 1$, we have $|\{\mathcal{J} \in \mathcal{P} : \dim(\mathcal{J}) = j\}| \leq kq$.*

Proof. Fix an extension $z \mapsto |z|$ of the norm on $\mathbb{F}_q[u]$ to $\overline{\mathbb{F}_q(u)}$, and denote by

$$\omega(z) = -\log_q |z| \tag{4.92}$$

the associated valuation of $z \in \overline{\mathbb{F}_q(u)}$. Note that if $z \in \overline{\mathbb{F}_q}[u]$, then

$$\omega(z) = -\deg(z). \tag{4.93}$$

For $f \in \mathcal{I}$, if $f \notin \{\alpha_1, \dots, \alpha_k\}$, let

$$\mathcal{J}_f = \left\{ z \in \mathcal{I} : |z - f| < \min_{1 \leq i \leq k} |f - \alpha_i| \right\}, \tag{4.94}$$

and for $f \in \mathcal{I} \cap \{\alpha_1, \dots, \alpha_k\}$ set $\mathcal{J}_f = \{f\}$. Put

$$\mathcal{P} = \{\mathcal{J}_f : f \in \mathcal{I}\}, \tag{4.95}$$

and note that (1) and (2) above are satisfied.

To check (3), suppose that $\mathcal{J}_f \cap \mathcal{J}_g \neq \emptyset$ for some $f, g \in \mathcal{I}$. Since our intervals are nonarchimedean, this implies (without loss of generality) that $\mathcal{J}_g \subseteq \mathcal{J}_f$, so in particular $g \in \mathcal{J}_f$. If $g \in \{\alpha_1, \dots, \alpha_k\}$, we see from Eq. (4.94) that $g \in \mathcal{J}_f$ implies $f \in \{\alpha_1, \dots, \alpha_k\}$. It follows that $\operatorname{len}(\mathcal{J}_g) = \operatorname{len}(\mathcal{J}_f) = 1$ and thus that $\mathcal{J}_g = \mathcal{J}_f$ as required. If $g \notin \{\alpha_1, \dots, \alpha_k\}$, then this is also the case for f, so from Eq. (4.94) we get that $|g - f| < |f - \alpha_i|$ for all $1 \leq i \leq k$.

Our norm is nonarchimedean, so $|g-\alpha_i| = |f-\alpha_i|$ by the above. It follows from Eq. (4.94) that $\dim \mathcal{J}_g = \dim \mathcal{J}_f$ so $\mathcal{J}_g = \mathcal{J}_f$ as required.

To check (4) for some $\mathcal{J} \in \mathcal{P}$, by definition, it suffices to check that $\deg(F(u,g(u)))$ is independent of $g(u) \in \mathcal{J}_{\overline{\mathbb{F}_q}}$, since $\deg(F(u,g(u))$ can be negative for only finitely many values of g. Equivalently, by Eq. (4.93), we need to check the independence of $\omega(F(u,g))$ on $g \in \mathcal{J}_{\overline{\mathbb{F}_q}}$. For that, pick an $f \in \mathcal{I} \setminus \{\alpha_1, \dots, \alpha_k\}$ with $\mathcal{J} = \mathcal{J}_f$. For $g \in \mathcal{J}_{\overline{\mathbb{F}_q}}$ we get as in the above paragraph that $\omega(g-\alpha_i) = \omega(f-\alpha_i)$ so Eq. (4.68) implies that

$$\omega(F(u,g)) = \omega(a_k) + \sum_{i=1}^{k} \omega(g-\alpha_i) = \omega(a_k) + \sum_{i=1}^{k} \omega(f-\alpha_i) \tag{4.96}$$

is indeed independent of g.

At last we check (5). For that, fix $0 \le j \le \dim(\mathcal{I}) - 1$, and let $f \in \mathcal{I}$ with $\dim(\mathcal{J}_f) = j$. It follows from our definition of $\mathcal{J}_f$ that there exists some $1 \le i \le k$ such that $\omega(f-\alpha_i) \ge -j$. Therefore, it suffices to check that for a given i we have

$$|\{\mathcal{J}_g : g \in \mathcal{I},\ \dim(\mathcal{J}_g) = j,\ \omega(g-\alpha_i) \ge -j\}| \le q. \tag{4.97}$$

To establish the above inequality we show that $\mathcal{J}_g$ (as in Eq. (4.97)) is determined by the coefficient of u^j in g. Let $\mathcal{J}_g, \mathcal{J}_{g'}$ be two intervals from the set in Eq. (4.97). We have $\omega(g-\alpha_i), \omega(g'-\alpha_i) \ge -j$, so we get from Eq. (4.93) that

$$\deg(g-g') = -\omega(g-g') \le j \tag{4.98}$$

since ω is nonarchimedean. Hence, if the coefficient of u^j in g coincides with the coefficient of u^j in g', we get that $\deg(g-g') \le j-1$ and thus $\mathcal{J}_g = \mathcal{J}_{g'}$ since $\dim(\mathcal{J}_g) = \dim(\mathcal{J}_{g'}) = j$. □

4.2.3. *Sheaf-theoretic setup.* We set up some of the notation needed to prove Theorem 1.3 and to state its ‘trace-twisted’ variant.

Notation 4.15. Keep Notation 4.11, Notation 2.1, and Notation 2.4. Let $r \in \mathbb{F}_q[u]$ be a polynomial for which $Z_F \cap Z_{F_{\nabla r}}$ is finite. Let $g \in \mathbb{F}_q[u]$ be a squarefree polynomial, let

$$t \colon \mathbb{F}_q[u]/(g) \to \mathbb{C} \tag{4.99}$$

be an infinitame trace function, let $\mathcal{F}_\pi$ be a sheaf giving rise to the trace function t_π, and set

$$g_{F,r} = \operatorname{lcm}(g, M_{F,r}). \tag{4.100}$$

Fix a prime factor π of $g_{F,r}$, let $\kappa = \mathbb{F}_q[u]/(\pi)$, and let $\chi \colon \kappa^\times \to \overline{\mathbb{Q}_\ell}^\times$ be the unique quadratic character. In other words, the character χ is the Legendre symbol mod π, that is

$$\chi(f) = \left(\frac{f}{\pi}\right), \quad f \in \kappa^\times = (\mathbb{F}_q[u]/(\pi))^\times. \tag{4.101}$$

We reduce r mod π, and recall from Notation 2.4 the map

$$E_r\colon \mathbb{A}^1_\kappa \to \mathbb{A}^1_\kappa, \quad E_r(x) = r + x^p. \tag{4.102}$$

Using this map, we define a sheaf on $\mathbb{A}^1_\kappa$ by

$$\mathcal{F}_{F,r,\pi} = E_r^* \begin{cases} \mathcal{L}_\chi\left(W^{(\pi)}_{F,r}\right) & \pi \nmid g, \ \pi \mid M_{F,r} \\ \mathcal{F}_\pi & \pi \mid g, \ \pi \nmid M_{F,r} \\ \mathcal{L}_\chi\left(W^{(\pi)}_{F,r}\right) \otimes \mathcal{F}_\pi & \pi \mid g, \ \pi \mid M_{F,r} \end{cases} \tag{4.103}$$

and use the shorthand notation $t_{F,r,\pi}$ for the associated trace function $t_{\mathcal{F}_{F,r,\pi}}$. At last, define the trace function

$$t_{F,r} = \prod_{\pi \mid g_{F,r}} t_{F,r,\pi}. \tag{4.104}$$

By Lemma 2.2 and Lemma 2.13(6), this is an infinitame trace function.

For a positive $\gamma \in \mathbb{R}$, we set

$$B(t;\gamma) = \prod_{\pi \mid g} (r(t_\pi)(1+\gamma) + c(t_\pi)\gamma)^{\deg(\pi)}$$

so in particular we have

$$B(t_{F,r};\gamma) = \prod_{\pi \mid g_{F,r}} (r(t_{F,r,\pi})(1+\gamma) + c(t_{F,r,\pi})\gamma)^{\deg(\pi)}.$$

In the proof of Theorem 1.3 and its variants, we will be tasked with applying Corollary 3.14 to $g_{F,r}$ and $t_{F,r}$. In order to make Corollary 3.14 a useful bound, we need to have some control on the rank and conductor. The notation $B(t;\gamma)$ will help with keeping track of an upper bound for the coefficient of the polynomial of Corollary 3.14 given as a product.

4.2.4. *Bounding rank and conductor.* In order to control $|M_{F,r}|$ and $|g_{F,r}|$, we recall from Eq. (4.75) that $|M_{F,r}|$ is bounded by $|R(F, F_{\nabla r})|$, so it suffices to control the latter. The following is the variant of [SS19, (4.24)] needed here.

Proposition 4.16. *Keep Notation 4.11. For $r \in \mathbb{F}_q[u]$ we have*

$$\deg(R(F, F_{\nabla r})) \le E(c_1, c_2, \deg(r)). \tag{4.105}$$

Proof. The quasi-homogeneity of the resultant from [GKZ08, p. 399, (1.6)], and Sylvester's formula as given in [GKZ08, p. 400, (1.12)], imply that $R(F, F_{\nabla r})$ is a linear combination (over $\mathbb{F}_q$) of subproducts of

$$a_{i_1}(u)\dots a_{i_k}(u) b_{j_1}(u)\dots b_{j_k}(u), \quad i_1 + \dots + i_k + j_1 + \dots + j_k = k^2. \tag{4.106}$$

By Eq. (4.71), we have the bound

$$\begin{aligned} \deg(b_i) &\le \max\{\deg(a_i) - 1, \deg(r) + \deg(a_{i+1}) - 1\} \\ &\le \max\{c_1 - 1 + c_2 i, \deg(r) - 1 + c_1 + c_2(i+1)\} \\ &= \max\{0, c_2 + \deg(r)\} + c_1 - 1 + c_2 i \end{aligned} \tag{4.107}$$

for the degrees of the coefficients of $F_{\nabla r}$. As a result we get that

$$\begin{aligned} \deg(R(F,F_{\nabla r})) &\leq \max_{i_1+\dots+i_k+j_1+\dots+j_k=k^2} \deg(a_{i_1}\dots a_{i_k}b_{j_1}\dots b_{j_k}) \\ &= \max_{i_1+\dots+i_k+j_1+\dots+j_k=k^2} \sum_{\ell=1}^{k} (\deg(a_{i_\ell})+\deg(b_{j_\ell})) . \end{aligned} \tag{4.108}$$

Using Eq. (4.66) and Eq. (4.107) we see that the above is at most

$$2kc_1+k\max\{0,c_2+\deg(r)\}-k+\max_{i_1+\dots+i_k+j_1+\dots+j_k=k^2} \sum_{\ell=1}^{k} c_2(i_\ell+j_\ell) \tag{4.109}$$

which evaluates to

$$2kc_1+k\max\{0,c_2+\deg(r)\}-k+c_2k^2. \tag{4.110}$$

By the notation in Eq. (4.67), the above equals $E(c_1,c_2,\deg(r))$. □

Proposition 4.17. *Keep Notation 4.15. For any positive $\gamma \in \mathbb{R}$ we have*

$$B(t_{F,r};\gamma) \leq (1+2\gamma)^{E(c_1,c_2,\deg(r))} B(t;\gamma).$$

Proof. Let π be a prime dividing $g_{F,r}$. In case π divides g and does not divide $M_{F,r}$, from the definition of $\mathcal{F}_{F,r,\pi}$ in Eq. (4.103)(2), and the invariance of rank and conductor in Proposition 2.5(4), we get

$$\begin{aligned} \mathbf{r}(\mathcal{F}_{F,r,\pi})(1+\gamma)+c(\mathcal{F}_{F,r,\pi})\gamma &= \mathbf{r}(E_r^*\mathcal{F}_\pi)(1+\gamma)+c(E_r^*\mathcal{F}_\pi)\gamma \\ &= \mathbf{r}(\mathcal{F}_\pi)(1+\gamma)+c(\mathcal{F}_\pi)\gamma. \end{aligned} \tag{4.111}$$

In case π divides both g and $M_{F,r}$, from Eq. (4.103)(3), Proposition 2.5(4), and Lemma 2.13(5) we get

$$\mathbf{r}(\mathcal{F}_{F,r,\pi}) = \mathbf{r}\left(E_r^*\left(\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\otimes\mathcal{F}_\pi\right)\right) = \mathbf{r}\left(\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\otimes\mathcal{F}_\pi\right) = \mathbf{r}(\mathcal{F}_\pi). \tag{4.112}$$

Similarly, by Eq. (4.103)(3), Proposition 2.5(4), Lemma 2.13(6), and Lemma 2.2(6), we have

$$\begin{aligned} c(\mathcal{F}_{F,r,\pi}) &= c\left(E_r^*\left(\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\otimes\mathcal{F}_\pi\right)\right) = c\left(\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\otimes\mathcal{F}_\pi\right) \\ &\leq c(\mathcal{F}_\pi)+c\left(\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\right)\mathbf{r}(\mathcal{F}_\pi) \leq c(\mathcal{F}_\pi)+\deg\left(W_{F,r}^{(\pi)}\right)\mathbf{r}(\mathcal{F}_\pi). \end{aligned} \tag{4.113}$$

Let $a \in \overline{\mathbb{F}_q}$ be a root of π. From the definition of $W_{F,r}^{(\pi)}$ after Eq. (4.79), the information on multiplicities in Eq. (4.77), and Lemma 4.4 we obtain

$$\begin{aligned} \deg\left(W_{F,r}^{(\pi)}\right) &= \deg(W_{F,r}(a,T)) = \sum_{b\in\overline{\mathbb{F}_q}} \operatorname{ord}_{T=b} W_{F,r}(a,T) \\ &= \sum_{\substack{x\in Z_F\cap Z_{F_{\nabla r}} \\ u_x=a}} i_x(Z_F,Z_{F_{\nabla r}}) \leq \operatorname{ord}_{u=a} R(F,F_{\nabla r}) = v_\pi(R(F,F_{\nabla r})) \end{aligned} \tag{4.114}$$

where v_π is the π-adic valuation on $\mathbb{F}_q[u]$. From Eq. (4.113) and Eq. (4.114) we conclude that

$$c(\mathcal{F}_{F,r,\pi}) \leq c(\mathcal{F}_\pi) + v_\pi(R(F, F_{\nabla r}))\mathbf{r}(\mathcal{F}_\pi). \tag{4.115}$$

Combining Eq. (4.112) with Eq. (4.115), and using Bernoulli's inequality, we get

$$\begin{aligned} \mathbf{r}(\mathcal{F}_{F,r,\pi})(1+\gamma) + c(\mathcal{F}_{F,r,\pi})\gamma &\leq \mathbf{r}(\mathcal{F}_\pi)(1+\gamma) + c(\mathcal{F}_\pi)\gamma + v_\pi(R(F, F_{\nabla r}))\mathbf{r}(\mathcal{F}_\pi)\gamma \\ &\leq (1 + v_\pi(R(F, F_{\nabla r}))\gamma)(\mathbf{r}(\mathcal{F}_\pi)(1+\gamma) + c(\mathcal{F}_\pi)\gamma) \\ &\leq (1+\gamma)^{v_\pi(R(F,F_{\nabla r}))}(\mathbf{r}(\mathcal{F}_\pi)(1+\gamma) + c(\mathcal{F}_\pi)\gamma). \end{aligned} \tag{4.116}$$

In case π divides $M_{F,r}$ and does not divide g, by Eq. (4.103)(1), Proposition 2.5(4), and Lemma 2.2(6) we have

$$\mathbf{r}(\mathcal{F}_{F,r,\pi}) = \mathbf{r}(E_r^* \mathcal{L}_\chi(W_{F,r}^{(\pi)})) = \mathbf{r}(\mathcal{L}_\chi(W_{F,r}^{(\pi)})) = 1. \tag{4.117}$$

Similarly, from Eq. (4.103)(1), Proposition 2.5(4), Lemma 2.2(6), and Eq. (4.114) we get

$$\begin{aligned} c(\mathcal{F}_{F,r,\pi}) &= c\left(E_r^* \mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\right) \\ &= c\left(\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)\right) \leq \deg\left(W_{F,r}^{(\pi)}\right) \leq v_\pi(R(F, F_{\nabla r})). \end{aligned} \tag{4.118}$$

Since π divides $M_{F,r}$, it follows from the definition of the latter in Eq. (4.75) that π divides $R(F, F_{\nabla r})$, or equivalently $v_\pi(R(F, F_{\nabla r})) \geq 1$. Therefore, from Eq. (4.117), Eq. (4.118), and Bernoulli's inequality we have

$$\begin{aligned} \mathbf{r}(\mathcal{F}_{F,r,\pi})(1+\gamma) + c(\mathcal{F}_{F,r,\pi})\gamma &\leq 1 + \gamma + v_\pi(R(F, F_{\nabla r}))\gamma \\ &\leq 1 + 2v_\pi(R(F, F_{\nabla r}))\gamma \leq (1+2\gamma)^{v_\pi(R(F,F_{\nabla r}))}. \end{aligned} \tag{4.119}$$

At last, combining Definition 1.4, Eq. (4.119), Eq. (4.111), Eq. (4.116), and Proposition 4.16 we get

$$\begin{aligned} B(t_{F,r};\gamma) &= \prod_{\pi \mid g_{F,r}} (\mathbf{r}(\mathcal{F}_{F,r,\pi})(1+\gamma) + c(\mathcal{F}_{F,r,\pi})\gamma)^{\deg(\pi)} \\ &= \prod_{\substack{\pi \mid M_{F,r} \\ \pi \nmid g}} (\mathbf{r}(\mathcal{F}_{F,r,\pi})(1+\gamma) + c(\mathcal{F}_{F,r,\pi})\gamma)^{\deg(\pi)} \prod_{\pi \mid g} (\mathbf{r}(\mathcal{F}_{F,r,\pi})(1+\gamma) + c(\mathcal{F}_{F,r,\pi})\gamma)^{\deg(\pi)} \\ &\leq B(t;\gamma) \prod_{\substack{\pi \mid M_{F,r} \\ \pi \nmid g}} (1+2\gamma)^{\deg(\pi) v_\pi(R(F,F_{\nabla r}))} \prod_{\pi \mid g} (1+2\gamma)^{\deg(\pi) v_\pi(R(F,F_{\nabla r}))} \\ &= B(t;\gamma) \prod_{\pi \mid M_{F,r}} (1+2\gamma)^{\deg(\pi) v_\pi(R(F,F_{\nabla r}))} = B(t;\gamma)(1+2\gamma)^{\sum_{\pi \mid M_{F,r}} \deg(\pi) v_\pi(R(F,F_{\nabla r}))} \\ &= B(t;\gamma)(1+2\gamma)^{\deg(R(F,F_{\nabla r}))} \leq B(t;\gamma)(1+2\gamma)^{E(c_1,c_2,\deg(r))}. \end{aligned}$$

□

4.2.5. *Finding a good prime.* Our goal here is to give a sufficient condition for the existence of a prime τ as in Corollary 3.14 for the trace function $t_{F,r}$ from Notation 4.15.

Proposition 4.18. *Keep Notation 4.11. Suppose that $a \in \overline{\mathbb{F}_q}$ is not a root of the polynomial*

$$\Delta_v(R(F, F_v)) \tag{4.120}$$

introduced in Eq. (4.82). Then for any $r \in \mathbb{F}_q[u]$ for which $Z_F \cap Z_{F_{\nabla r}}$ is finite, there exists at most one $b \in \overline{\mathbb{F}_q}$ such that $(a, b) \in Z_F \cap Z_{F_{\nabla r}}$.

Proof. Suppose toward a contradiction that there exist distinct $b_1, b_2 \in \overline{\mathbb{F}_q}$ with $(a, b_1), (a, b_2) \in Z_F \cap Z_{F_{\nabla r}}$ and let $\pi \in \mathbb{F}_q[u]$ be the minimal polynomial of a over $\mathbb{F}_q$. We will arrive at a contradiction to a not being a root of $\Delta_v(R(F, F_v))$ by showing that π divides $\Delta_v(R(F, F_v))$ in the ring $\mathbb{F}_q[u]$.

Denote by v_0 the residue class of ∇r in $\mathbb{F}_q[u]/(\pi)$. To check that

$$\Delta_v(R(F, F_v)) \equiv 0 \mod \pi, \tag{4.121}$$

it suffices to prove that

$$\mathrm{ord}_{v=v_0}\left(R(F, F_v) \bmod \pi\right) \geq 2. \tag{4.122}$$

By Eq. (4.74), we have

$$R(F, F_v) = a_k^{\deg_T F_v} \prod_{i=1}^{k} \left(\partial_u F(u, \alpha_i) + v \partial_T F(u, \alpha_i)\right). \tag{4.123}$$

Suppose first that $\deg_T(F_v) = 0$. Then

$$\deg_T(F_{\nabla r} \bmod \pi) \leq \deg_T(F_{\nabla r}) \leq \deg_T(F_v) = 0, \tag{4.124}$$

and since $\pi(a) = 0$, the polynomial $F_{\nabla r} \bmod \pi$ has a zero, so it is the zero polynomial. It follows from finiteness of $Z_F \cap Z_{F_{\nabla r}}$ that $F \bmod \pi$ is not zero, and since $\pi(a) = 0$, we conclude that $F \bmod \pi$ has at least two zeros so

$$k = \deg_T(F) \geq \deg_T(F \bmod \pi) \geq 2. \tag{4.125}$$

Our assumption that F_v is constant as a polynomial in T, the separability of F which implies that $\deg_v(F_v) = 1$, and the fact that $k \geq 2$ established above, imply that

$$\Delta_v(R(F, F_v)) = \Delta_v(F_v^k) = 0 \tag{4.126}$$

so Eq. (4.121) holds in this case.

Suppose now that $\deg_T(F_v) \geq 1$. We see from Eq. (4.123) that if $\pi \mid a_k$ then Eq. (4.121) is satisfied, so we assume from now on that $\pi \nmid a_k$. Since the α_i are roots of a polynomial with leading coefficient not divisible by π, we can reduce Eq. (4.123) mod a prime of (the ring of $\mathbb{F}_q[u]$-integral elements of) $\overline{\mathbb{F}_q(u)}$ lying over π. Since $\pi(a) = 0$, it follows that after the reduction, at least two of the factors on the right hand side of Eq. (4.123) vanish at $v = v_0$. Hence, Eq. (4.122) holds. □

The following is the generalization of [SS19, Remark 3.3] needed here.

Proposition 4.19. *Keep Notation 4.15. Suppose that $R(F, F_{\nabla r})$ is not of the form A^2B for any $A \in \mathbb{F}_q[u]$ and any $B \in \mathbb{F}_q[u]$ that divides the polynomial*

$$g \cdot a_k \cdot \Delta_v(R(F, F_v)) \in \mathbb{F}_q[u]. \tag{4.127}$$

Then there exists a prime $\pi \in \mathbb{F}_q[u]$ dividing $g_{F,r}$ such that $t_{F,r,\pi}$ is a Dirichlet trace function.

Proof. Our assumption on $R(F, F_{\nabla r})$ is equivalent to the existence of a prime π not dividing the polynomial in Eq. (4.127) such that $v_\pi(R(F, F_{\nabla r}))$ is odd. Since the latter valuation is nonzero, our prime π divides $R(F, F_{\nabla r})$, so by the definition in Eq. (4.75), π divides $M_{F,r}$. We conclude from the definition of $g_{F,r}$ in Eq. (4.100), and from Eq. (4.127), that π divides $g_{F,r}$ and does not divide g. By Eq. (4.103)(1) we have

$$\mathcal{F}_{F,r,\pi} = E_r^* \mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right). \tag{4.128}$$

In order to show that the associated trace function $t_{F,r,\pi}$ is a Dirichlet trace function, by the permanence property in Proposition 2.5(6), it suffices to show that the function

$$t_{\mathcal{L}_\chi\left(W_{F,r}^{(\pi)}\right)}(x) = \chi\left(W_{F,r}^{(\pi)}(x)\right), \quad x \in \mathbb{F}_q[u]/(\pi), \tag{4.129}$$

is a Dirichlet trace function. Recall from Eq. (4.101) that the character χ is quadratic, so by the definition in Eq. (1.21) it is enough to show that $W_{F,r}^{(\pi)}$ is an odd power of a monic linear polynomial, up to a constant from $(\mathbb{F}_q[u]/(\pi))^\times$. In other words, we want to show that $W_{F,r}^{(\pi)}$ vanishes at no more than one point in $\overline{\mathbb{F}_q[u]/(\pi)}$, and its order of vanishing there is odd.

Fix a root $a \in \overline{\mathbb{F}_q}$ of π. We are tasked with showing that $W_{F,r}(a, T)$ has a unique zero in $\overline{\mathbb{F}_q}$, and the multiplicity of this zero is odd. Since π does not divide the polynomial in Eq. (4.127), it does not divide $\Delta_v(R(F, F_v))$, so $\Delta_v(R(F, F_v))(a) \neq 0$. The desired uniqueness of the zero of $W_{F,r}(a, T)$ follows from Eq. (4.77) and Proposition 4.18. From Eq. (4.77) we moreover conclude that the order of vanishing of $W_{F,r}(a, T)$ at its unique vanishing point is

$$\sum_{b \in \overline{\mathbb{F}_q}} i_{(a,b)}(Z_F, Z_{F_{\nabla r}}). \tag{4.130}$$

Since π does not divide the polynomial in Eq. (4.127), it does not divide the leading coefficient of F. In other words, the leading coefficient of F does not vanish at a, so by Lemma 4.4 the sum above equals

$$\operatorname{ord}_{u=a} R(F, F_{\nabla r}). \tag{4.131}$$

This order of vanishing equals $v_\pi(R(F, F_{\nabla r}))$ which is odd by assumption. □

Proposition 4.19 is not useful in case $\Delta_v(R(F,F_v))=0$. The next proposition characterizes the cases in which this vanishing occurs. The condition that arises is our generalization of the 'distinct derivatives' assumption in [SS19, Proposition 4.3].

Proposition 4.20. *Keep Notation 4.11. In $\overline{\mathbb{F}_q(u)}$ we have*

$$\frac{\partial_u F}{\partial_T F}(u,\alpha_i)\neq\frac{\partial_u F}{\partial_T F}(u,\alpha_j),\quad 1\leq i<j\leq k, \tag{4.132}$$

if and only if $\Delta_v(R(F,F_v))$ is not the zero polynomial.

Proof. Our discriminant is nonzero if and only if $R(F,F_v)$ does not have a double root in $\overline{\mathbb{F}_q(u)}$ as a polynomial in v. By Eq. (4.74), we have

$$R(F,F_v)=a_k^{\deg_T F_v}\prod_{i=1}^{k}\left(\partial_u F(u,\alpha_i)+v\partial_T F(u,\alpha_i)\right) \tag{4.133}$$

so the nonexistence of a double root among the k roots

$$v_i=-\frac{\partial_u F}{\partial_T F}(u,\alpha_i),\quad 1\leq i\leq k, \tag{4.134}$$

of $R(F,F_v)$ in $\overline{\mathbb{F}_q(u)}$ is equivalent to our assumption in Eq. (4.132). □

Using Proposition 4.20, we show in the next proposition that we can always arrive at a situation where $\Delta_v(R(F,F_v))\neq 0$ by performing a linear change of variable. This is our generalization of the main argument in the proof of [SS19, Theorem 4.5].

Proposition 4.21. *Keep Notation 4.11. There exists a monic polynomial $P(u)\in\mathbb{F}_q[u]$ with $|P(u)|\leq q\binom{k}{2}$ such that for all $c(u)\in\mathbb{F}_q[u]$, the polynomial*

$$G(u,T)=F(u,P(u)T+c(u)) \tag{4.135}$$

is separable in T and satisfies

$$\Delta_v(R(G,G_v))\neq 0. \tag{4.136}$$

Proof. In view of Eq. (4.68), for any choice of a monic $P(u)\in\mathbb{F}_q[u]$ we have

$$G\left(u,\frac{\alpha_i-c(u)}{P(u)}\right)=0,\quad 1\leq i\leq k, \tag{4.137}$$

so these are all the roots of G in $\overline{\mathbb{F}_q(u)}$ since $\deg_T(G)=\deg_T(F)=k$. By Proposition 4.20, it suffices to choose $P(u)$ in such a way that

$$\frac{\partial_u G}{\partial_T G}\left(u,\frac{\alpha_i-c(u)}{P(u)}\right)\neq\frac{\partial_u G}{\partial_T G}\left(u,\frac{\alpha_j-c(u)}{P(u)}\right),\quad 1\leq i<j\leq k. \tag{4.138}$$

Using the chain rule, we get

$$\frac{\partial_u G}{\partial_T G}\left(u, \frac{\alpha_i - c(u)}{P(u)}\right) = \frac{\partial_u F(u,\alpha_i) + \frac{\alpha_i - c(u)}{P(u)} \cdot \nabla P \cdot \partial_T F(u,\alpha_i) + \nabla c \cdot \partial_T F(u,\alpha_i)}{P(u)\partial_T F(u,\alpha_i)}$$
$$= \frac{\partial_u F(u,\alpha_i)}{P(u)\partial_T F(u,\alpha_i)} + \frac{(\alpha_i - c(u))\nabla P}{P(u)^2} + \frac{\nabla c}{P(u)}.$$

Hence, Eq. (4.138) holds unless for some $1 \leq i < j \leq k$ we have

$$\frac{\partial_u F}{\partial_T F}(u,\alpha_i) + \frac{(\alpha_i - c(u))\nabla P}{P(u)} = \frac{\partial_u F}{\partial_T F}(u,\alpha_j) + \frac{(\alpha_j - c(u))\nabla P}{P(u)}. \tag{4.139}$$

Since $\alpha_i - \alpha_j \neq 0$ by separability, the above is equivalent to

$$\frac{\nabla P}{P(u)} = \frac{\frac{\partial_u F}{\partial_T F}(u,\alpha_j) - \frac{\partial_u F}{\partial_T F}(u,\alpha_i)}{\alpha_i - \alpha_j} \tag{4.140}$$

so Eq. (4.138) holds if (and only if)

$$\frac{\nabla P}{P(u)} \tag{4.141}$$

does not belong to a specific set of at most $\binom{k}{2}$ elements of $\overline{\mathbb{F}_q(u)}$.

The 'logarithmic derivation' map

$$P \mapsto \frac{\nabla P}{P}, \quad P \in \mathbb{F}_q[u], \tag{4.142}$$

sends monic polynomials P, Q to the same rational function if and only if their quotient $\frac{P}{Q}$ is a p-th power in $\mathbb{F}_q(u)$. In particular, the restriction of the logarithmic derivation map to monic squarefree polynomials is injective. By [Ros02, Proposition 2.3], and the formula for the sum of a geometric progression, the number of such polynomials of degree at most d exceeds q^d, so we need that $q^d \geq \binom{k}{2}$. We thus take

$$d = \left\lceil \log_q \binom{k}{2} \right\rceil \leq \log_q \binom{k}{2} + 1 \tag{4.143}$$

so we can choose P satisfying Eq. (4.138) with $|P| \leq q^d \leq q\binom{k}{2}$. □

In order to bound the number of possible B in Proposition 4.19, we bound the degree of the polynomial $\Delta_v(R(F, F_v))$.

Proposition 4.22. *Keep Notation 4.11. Then*

$$\deg(\Delta_v(R(F, F_v))) \leq 4k(k-1)(c_1 + k \max\{c_2, 0\}). \tag{4.144}$$

Proof. Since $\deg_T(F), \deg_T(F_v) \leq k$, it follows from Sylvester's formula as given in [GKZ08, p. 400, (1.12)] that $R(F, F_v)$ is a linear combination (over $\mathbb{F}_q$) of products of at most k coefficients of F and at most k coefficients of F_v. By Eq. (4.66), the degree of every coefficient a_i of F is at most

$$c_1 + c_2 i \leq c_1 + k \max\{c_2, 0\} \tag{4.145}$$

thus the degree in u of (every coefficient of) F_v is also bounded by the right hand side of Eq. (4.145). We conclude that

$$\deg_u(R(F,F_v)) \leq 2k(c_1 + k\max\{c_2,0\}). \tag{4.146}$$

Since F is separable in T, it follows from Eq. (4.74) that

$$\deg_v(R(F,F_v))) = k. \tag{4.147}$$

We then infer from [GKZ08, p. 404] that $\Delta_v(R(F,F_v))$ is a linear combination (over $\mathbb{F}_q$) of products of $2(k-1)$ coefficients of $R(F,F_v)$. Using the bound on the degree of a coefficient from Eq. (4.146), we get that

$$\deg(\Delta_v(R(F,F_v))) \leq 2(k-1)\cdot 2k(c_1 + k\max\{c_2,0\}) \tag{4.148}$$

and the right hand side above matches the right hand side of Eq. (4.144), which gives the desired result. □

Now that we have control over the number of possible B, we need to know how often $R(F,F_{\nabla r}) = A^2B$ for a particular B. For that, we have the following lemma which is a consequence of Cohen's quantitative Hilbert's irreducibility theorem as stated in [Coh81, Theorem 2.3]. We refer to [BSE21] of Bary-Soroker–Entin extending Cohen's work to function fields.

Lemma 4.23. *Let $H(u,v) \in \mathbb{F}_q[u][v]$ be a polynomial which is not a perfect square in $\overline{\mathbb{F}_q(u)}[v]$, and let $B \in \mathbb{F}_q[u]$. Then for $X \geq \max\{\deg_u(H),\deg(B)\}^4$ we have*

$$|\{g \in \mathbb{F}_q[u] : |g| < X,\ H(u,g(u)) = B\cdot\square\}| \ll \sqrt{X}\log X \tag{4.149}$$

as $X \to \infty$, with the implied constant depending only on $\deg_v(H)$. Here the symbol $\square$ stands for the square of a polynomial in $\mathbb{F}_q[u]$.

The lemma above is the generalization of [SS19, Proposition 4.2] needed here. A proof can also be obtained by a standard sieve theoretic argument, as in Heath-Brown's square sieve for example. More specifically, we need the following corollary.

Corollary 4.24. *Keep Notation 4.1, Notation 4.11, and suppose that*

$$\Delta_v(R(F,F_v)) \neq 0. \tag{4.150}$$

Let $B \in \mathbb{F}_q[u]$, and let $\mathcal{I}$ be an interval in $\mathbb{F}_q[u]$ with

$$\operatorname{len}(\mathcal{I}) \geq \max\{E(c_1,c_2,\deg(\mathcal{I})),\deg(a_k^kB)\}^4. \tag{4.151}$$

Take $\mathcal{R} \subseteq \mathcal{I}$ such that for every $f \in \mathcal{I}$ there exists a unique $r \in \mathcal{R}$ with

$$\nabla f = \nabla r. \tag{4.152}$$

Then as $\operatorname{len}(\mathcal{I}) \to \infty$ we have

$$|\{r \in \mathcal{R} : R(F,F_{\nabla r}) = B\cdot\square\}| \ll \sqrt{\operatorname{len}(\mathcal{I})}\log\operatorname{len}(\mathcal{I}) \tag{4.153}$$

with the implied constant depending only on k.

Proof. Fix $f \in \mathcal{I}$, and note that

$$\begin{aligned}|\{r \in \mathcal{R} : R(F, F_{\nabla r}) = B \cdot \square\}| &= |\{g \in \mathbb{F}_q[u] : |g| < \operatorname{len}(\mathcal{I}),\ R(F, F_{\nabla f + \nabla g}) = B \cdot \square\}| \\ &\leq |\{g \in \mathbb{F}_q[u] : |g| < \operatorname{len}(\mathcal{I}),\ R(F, F_{\nabla f + g}) = B \cdot \square\}|.\end{aligned}$$

Put $j = \deg_T(F_{\nabla f + v})$. By Eq. (4.10), the above is at most

$$\left|\bigcup_{i=0}^{j} \{g \in \mathbb{F}_q[u] : |g| < \operatorname{len}(\mathcal{I}),\ R_{k,j}(F, F_{\nabla f + g}) = a_k^i B \cdot \square\}\right|$$

so setting

$$H(u, v) = R_{k,j}(F, F_{\nabla f + v}), \tag{4.154}$$

and noting that $j \leq k$, we get the bound

$$\sum_{i=0}^{k} |\{g \in \mathbb{F}_q[u] : |g| < \operatorname{len}(\mathcal{I}),\ H(u, g) = a_k^i B \cdot \square\}|. \tag{4.155}$$

Therefore, in order to conclude by applying Lemma 4.23, one thing we need to check is that $\operatorname{len}(\mathcal{I}) \geq \max\{\deg_u(H), \deg(a_k^k B)\}^4$. By our assumption in Eq. (4.151), this amounts to showing that

$$\deg_u(H) \leq E(c_1, c_2, \deg(\mathcal{I})). \tag{4.156}$$

We claim that there exists $\lambda \in \overline{\mathbb{F}_q}$ for which

$$\deg_u(H) = \deg R(F, F_{\nabla(f + \lambda u)}). \tag{4.157}$$

Since F is separable, the coefficient of the highest power of u in $H(u, v)$ is a nonzero polynomial $P \in \mathbb{F}_q[v]$, and the coefficient of the highest power of T in $F_{\nabla f + v}$ is a nonzero polynomial $Q \in \mathbb{F}_q[u, v]$. Hence, there exists $\lambda \in \overline{\mathbb{F}_q}$ such that $P(\lambda) \neq 0$ and $Q(u, \lambda) \neq 0$. It follows that

$$\deg_u(H(u, v)) = \deg(H(u, \lambda)) = \deg(R_{k,j}(F, F_{\nabla f + \lambda})) = \deg R(F, F_{\nabla(f + \lambda u)})$$

so our claim from Eq. (4.157) is established. From Proposition 4.16, Notation 4.1, and the fact that $\operatorname{len}(\mathcal{I}) > 1$, we get that

$$\deg(R(F, F_{\nabla(f + \lambda u)})) \leq E(c_1, c_2, \deg(f + \lambda u)) \leq E(c_1, c_2, \deg(\mathcal{I})) \tag{4.158}$$

so the two equations above imply Eq. (4.156).

The other thing we need to check is that $R_{k,j}(F, F_{\nabla f + v})$ is not a perfect square in $\overline{\mathbb{F}_q(u)}[v]$. For that we use Eq. (4.74) to write

$$R_{k,j}(F, F_{\nabla f + v}) = a_k^j \prod_{i=1}^{k} \left(\partial_u F(u, \alpha_i) + (\nabla f + v)\, \partial_T F(u, \alpha_i)\right).$$

Viewed as a polynomial in v, the roots in $\overline{\mathbb{F}_q(u)}$ of the polynomial above are

$$v_i = -\frac{\partial_u F}{\partial_T F}(u, \alpha_i) - \nabla f, \quad 1 \leq i \leq k. \tag{4.159}$$

Since $\Delta_v(R(F, F_v)) \neq 0$ by assumption, it follows from Proposition 4.20 that the roots above are pairwise distinct, so $R_{k,j}(F, F_{\nabla f+v})$ is not a square of a polynomial in v over $\overline{\mathbb{F}_q(u)}$. □

5. Trace functions vs Möbius function

This section is devoted to proving Theorem 1.3 and its twisted variants. The most general form is the following theorem. We give an essentially self-contained statement, recalling some of Notation 4.11 and Notation 4.15.

Theorem 5.1. *Fix an odd prime p, a power q of p, and a positive integer k. Let $0 < \gamma \leq 1$ and*

$$0 < \alpha < \frac{1}{2p} + \frac{\log_q \gamma}{p} - k \log_q(1 + 2\gamma) \tag{5.1}$$

be real numbers, and set $\beta = (1 + 2\gamma)^k$. Take a separable polynomial

$$F(u, T) = \sum_{i=0}^{k} a_i(u) T^i \in \mathbb{F}_q[u, T] \tag{5.2}$$

of degree k in T. Pick $c_1, c_2 \in \mathbb{R}$ with $c_1 \geq 0 \geq c_2$ such that

$$\deg(a_i(u)) \leq c_1 + c_2 i, \quad 0 \leq i \leq k. \tag{5.3}$$

Let $g \in \mathbb{F}_q[u]$ be a squarefree polynomial, let t be an infinitame g-periodic trace function, and let $\mathcal{I}$ be an interval in $\mathbb{F}_q[u]$ as in Notation 4.1. Then

$$\sum_{f \in \mathcal{I}} \mu(F(u, f)) t(f) \ll q^{\dim(\mathcal{I})(1-\alpha)} \beta^{2c_1 + (k+1)c_2} \left(\beta^{-c_2 - \dim(\mathcal{I})} + \beta^{\deg(\mathcal{I}) - \dim(\mathcal{I})} \right) \prod_{\pi | g} (r(t_\pi)(1 + \gamma) + c(t_\pi)\gamma)^{\deg(\pi)} \tag{5.4}$$

as $\dim(\mathcal{I}) \to \infty$, with the implied constant depending only on q, k, α, γ.

The trivial bound here is $q^{\dim(\mathcal{I})} \prod_{\pi|g} r(t_\pi)$, where $q^{\dim(\mathcal{I})} = \text{len}(\mathcal{I})$ is the length of the sum and $\prod_{\pi|g} r(t_\pi)$ is a bound for each term. If we think of c_1, c_2, t, and $\deg(\mathcal{I}) - \dim(\mathcal{I})$ as fixed, then the bound in the theorem describes a power savings of α, with the other terms describing the quality of the uniformity in F, t and $\mathcal{I}$. Our proof builds on the strategy of proving [SS19, Proposition 4.3]. The statement could be simplified by restricting to the case $c_2 = 0$, in which case c_1 would be $\deg_u(F)$, but this would lead some of our later results, including Bateman-Horn, to be valid for larger values of q only.

Proof. We first reduce to the case of a polynomial F with

$$\Delta_v(R(F, F_v)) \neq 0. \tag{5.5}$$

By Proposition 4.21, there exists a (nonzero) polynomial $P \in \mathbb{F}_q[u]$ with $|P| \ll 1$ such that for every $c \in \mathbb{F}_q[u]$ with $\deg(c) < \deg(P)$ the polynomial $G(u,T) = F(u, PT + c)$ is separable in T, and satisfies

$$\Delta_v(R(G, G_v)) \neq 0. \tag{5.6}$$

Define the intervals

$$\mathcal{I}_c = \left\{ \frac{f-c}{P} : f \in \mathcal{I},\ f \equiv c \bmod P \right\}, \quad c \in \mathbb{F}_q[u],\ \deg(c) < \deg(P), \tag{5.7}$$

and note that

$$\begin{aligned} \sum_{f \in \mathcal{I}} \mu(F(u,f))t(f) &= \sum_{\substack{c \in \mathbb{F}_q[u] \\ \deg(c) < \deg(P)}} \sum_{h \in \mathcal{I}_c} \mu(G(u,h))t(Ph + c) \\ &\ll |P| \left| \sum_{h \in \mathcal{J}} \mu(G(u,h))t(Ph + c) \right| \end{aligned} \tag{5.8}$$

where $\mathcal{J} = \mathcal{I}_c$ for some c as above (for which the maximum is achieved). In view of Proposition 2.3, the change of the trace function increases neither $r(t_\pi)$ nor $c(t_\pi)$, and the change of the polynomial F can be handled by increasing c_1 by $k \deg(P)$. The overall loss in the change of variable $T \mapsto PT + c$ is therefore a factor of $O(1)$, so we can assume throughout that Eq. (5.5) is satisfied.

By Lemma 4.14 there exists a partition $\mathcal{P}$ of $\mathcal{I}$ into subintervals $\mathcal{J}$ which are F-adapted (except possibly for those of dimension 0) and the number of $\mathcal{J} \in \mathcal{P}$ of any given dimension is $O(1)$. As a result, for

$$\xi = 4 \log_q \max\{E(c_1, c_2, \deg(\mathcal{I})), \deg(g \cdot a_k^{k+1} \cdot \Delta_v(R(F, F_v)))\} \tag{5.9}$$

we have

$$\begin{aligned} \sum_{f \in \mathcal{I}} \mu(F(u,f))t(f) &= \sum_{\mathcal{J} \in \mathcal{P}} \sum_{f \in \mathcal{J}} \mu(F(u,f))t(f) \\ &= \sum_{\substack{\mathcal{J} \in \mathcal{P} \\ \dim(\mathcal{J}) \geq \xi}} \sum_{f \in \mathcal{J}} \mu(F(u,f))t(f) + O\left(q^\xi \prod_{\pi | g} r(t_\pi)\right). \end{aligned} \tag{5.10}$$

We will check later (around Eq. (5.37)) that the contribution of the error term $O(q^\xi \prod_{\pi|g} r(t_\pi))$ in Eq. (5.10) is indeed dominated by our final bound from Eq. (5.4). Similarly, we will defer a few other elementary computations comparing two different bounds until we have completed the more fundamental work of splitting the sum into different ranges and explaining the bound we will use for each range.

Fix an interval $\mathcal{J} \in \mathcal{P}$ with $\dim(\mathcal{J}) \geq \xi$, and set $n = \frac{\dim(\mathcal{J})}{p}$. Pick a subset $\mathcal{R} \subseteq \mathcal{J}$ in a way that for every $f \in \mathcal{J}$ there exists a unique $r \in \mathcal{R}$

and a unique $s \in \mathbb{F}_q[u]$ with $\deg(s) < n$ such that $f = r + s^p$. We can then write

$$\sum_{f \in \mathcal{J}} \mu(F(u,f))t(f) = \sum_{r \in \mathcal{R}} \sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \mu(F(u, r+s^p))t(r+s^p). \tag{5.11}$$

Our choice of $\mathcal{R}$ is such that for each $f \in \mathcal{J}$ there is a unique $r \in \mathcal{R}$ with

$$\nabla f = \nabla r. \tag{5.12}$$

Fix $r \in \mathcal{R}$, and suppose first that $Z_F \cap Z_{F_{\nabla r}}$ is infinite. Then from Proposition 4.13 we get that

$$\sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \mu(F(u, r+s^p))t(r+s^p) \ll \prod_{\pi | g} r(t_\pi). \tag{5.13}$$

Therefore, the contribution of such r to Eq. (5.11) is

$$\ll |\mathcal{R}| \prod_{\pi | g} r(t_\pi) \ll q^{\dim(\mathcal{J})(1-\frac{1}{p})} \prod_{\pi | g} r(t_\pi). \tag{5.14}$$

We will check later (around Eq. (5.25)) that the contribution of Eq. (5.14) to Eq. (5.10) is bounded by Eq. (5.4).

From now on we assume that $Z_F \cap Z_{F_{\nabla r}}$ is finite, so that we can use Notation 4.15. By Corollary 4.12 we have

$$\sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \mu(F(u, r+s^p))t(r+s^p) \ll \left| \sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \left(\frac{W_{F,r}(u, r+s^p)}{M_{F,r}} \right) t(r+s^p) \right|.$$

By definition of the Jacobi symbol, and the definition of a trace function in Eq. (1.24), the above equals

$$\sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \prod_{\pi | M_{F,r}} \left(\frac{W_{F,r}^{(\pi)}(r+s^p)}{\pi} \right) \prod_{\pi' | g} t_{\pi'}(r+s^p). \tag{5.15}$$

Using Proposition 2.5(5) and Lemma 2.2(1) we can rewrite the above as

$$\sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \prod_{\pi | M_{F,r}} t_{E_r^* \mathcal{L}_\chi \left(W_{F,r}^{(\pi)} \right)}(s) \prod_{\pi' | g} t_{E_r^* \mathcal{F}_{\pi'}}(s). \tag{5.16}$$

With Lemma 2.13(1), the notation of Eq. (4.103), and Eq. (4.104) we arrive at

$$\sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} \prod_{\pi | g_{F,r}} t_{F,r,\pi}(s) = \sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s)<n}} t_{F,r}(s). \tag{5.17}$$

For all those $r \in \mathcal{R}$ for which $t_{F,r,\pi}$ is not a Dirichlet trace function for any $\pi \mid g_{F,r}$, we bound the sum above trivially. Since $Z_F \cap Z_{F_{\nabla r}}$ is finite, Proposition 4.19 tells us that for every such r there exist $A, B \in \mathbb{F}_q[u]$ such that

$$R(F, F_{\nabla r}) = A^2 B, \quad B \mid g \cdot a_k \cdot \Delta_v(R(F, F_v)). \tag{5.18}$$

Let us now check that Corollary 4.24 applies here.

First, recall that we have $\Delta_v(R(F,F_v)) \neq 0$. Second, we use Notation 4.1, Eq. (5.9), and Eq. (5.18) to get that that

$$\begin{aligned}\mathrm{len}(\mathcal{J}) = q^{\dim(\mathcal{J})} \geq q^{\xi} &= \max\{E(c_1, c_2, \deg(\mathcal{I})), \deg(a_k^k \cdot g \cdot a_k \cdot \Delta_v(R(F, F_v)))\}^4 \\ &\geq \max\{E(c_1, c_2, \deg(\mathcal{J})), \deg(a_k^k B)\}^4.\end{aligned}$$

This verifies the assumption made in Eq. (4.151), so we can indeed invoke Corollary 4.24.

It follows from Corollary 4.24 applied to each B in Eq. (5.18), and the function field version of the divisor bound in [IK04, Eq. (1.81)] that the number of $r \in \mathcal{R}$ for which $t_{F,r,\pi}$ is not a Dirichlet trace function for any $\pi \mid g_{F,r}$ is

$$\ll \mathrm{len}(\mathcal{J})^{\frac{1}{2}+\epsilon} |g \cdot a_k \cdot \Delta_v(R(F, F_v))|^{\epsilon} \tag{5.19}$$

for any $\epsilon > 0$. Now we use Proposition 4.22, and conclude that the contribution of these r to Eq. (5.17) is

$$\ll \mathrm{len}(\mathcal{J})^{\frac{1}{2}+\epsilon} |g|^{\epsilon} \cdot |a_k|^{\epsilon} \cdot q^{4\epsilon k(k-1)(c_1 + k \max\{c_2, 0\}) + n} \cdot \prod_{\pi \mid g_{F,r}} r(t_{F,r,\pi}). \tag{5.20}$$

For all those $r \in \mathcal{R}$ for which there exists a prime τ dividing $g_{F,r}$ such that $t_{F,r,\tau}$ is a Dirichlet trace function, we bound the sum on the right hand side of Eq. (5.17) by invoking Corollary 3.14 and get

$$\sum_{\substack{s \in \mathbb{F}_q[u] \\ \deg(s) < n}} t_{F,r}(s) \ll q^{\frac{n}{2}} \left(\prod_{\pi \mid g_{F,r}} (r(t_{F,r,\pi})(1+Z) + c(t_{F,r,\pi})Z)^{\deg(\pi)} \right) [Z^n].$$

As the coefficients of powers of Z in the polynomial above are nonnegative, for any $\gamma > 0$ the coefficient of Z^n is at most

$$q^{\frac{n}{2}} \gamma^{-n} \left(\prod_{\pi \mid g_{F,r}} (r(t_{F,r,\pi})(1+\gamma) + c(t_{F,r,\pi})\gamma)^{\deg(\pi)} \right) = q^{\frac{n}{2}} \gamma^{-n} B(t_{F,r}; \gamma) \tag{5.21}$$

which, by Proposition 4.17, is bounded from above by

$$q^{\frac{n}{2}} \gamma^{-n} (1 + 2\gamma)^{E(c_1, c_2, \deg(r))} B(t; \gamma). \tag{5.22}$$

Using the definition of E in Eq. (4.67), and the inequalities

$$\deg(r) \leq \deg(\mathcal{J}) \leq \deg(\mathcal{I}), \tag{5.23}$$

we see that Eq. (5.22) is at most

$$q^{\frac{n}{2}}\gamma^{-n}(1+2\gamma)^{2kc_1+k\max\{0,c_2+\deg(\mathcal{I})\}-k+c_2k^2}B(t;\gamma).$$

We can ignore the factor $(1+2\gamma)^{-k}$ as it is at most 1. Summing trivially over $\mathcal{R}$ in Eq. (5.11), the above is multiplied by $|\mathcal{R}| \ll q^{\dim(\mathcal{J})-n}$, so recalling that $n = \frac{\dim(\mathcal{J})}{p}$, we obtain

$$q^{\dim(\mathcal{J})\left(1-\frac{1}{2p}\right)}\gamma^{-\frac{\dim(\mathcal{J})}{p}}(1+2\gamma)^{2kc_1+k\max\{0,c_2+\deg(\mathcal{I})\}+c_2k^2}B(t;\gamma). \tag{5.24}$$

This is the main contribution to the error term and responsible for the form of Eq. (5.4). All other contributions (we shall soon see), are secondary, and our estimates for them can be somewhat wasteful.

We are now ready to show that each of the four contributions Eq. (5.14), Eq. (5.20), Eq. (5.24), and the error term in Eq. (5.10), are each bounded by the right side of Eq. (5.4), proving Eq. (5.4).

First, we show that the contribution of those r for which $Z_F \cap Z_{F_{\nabla r}}$ is infinite, bounded in Eq. (5.14) by $q^{\dim(\mathcal{J})(1-\frac{1}{p})}\prod_{\pi|g} r(t_\pi)$ for each interval $\mathcal{K} \in \mathcal{P}$, is dominated by Eq. (5.4).

Summing $q^{\dim(\mathcal{J})(1-\frac{1}{p})}\prod_{\pi|g} r(t_\pi)$ over the intervals $\mathcal{J}$ that partition $\mathcal{I}$, we get a contribution of

$$\ll q^{\dim(\mathcal{I})(1-\frac{1}{p})}\prod_{\pi|g} r(t_\pi). \tag{5.25}$$

Using our assumption that $0 < \gamma \leq 1$, we get that

$$\alpha < \frac{1}{2p} + \frac{\log_q \gamma}{p} - k\log_q(1+2\gamma) \leq \frac{1}{2p} < \frac{1}{p} \tag{5.26}$$

and that $\beta = (1+2\gamma)^k \geq 1$. From Notation 4.1 we recall that $\deg(\mathcal{I})$ is at least $\dim(\mathcal{I})$, and from Eq. (5.3) we deduce that

$$2c_1 + (k+1)c_2 = (c_1+c_2) + (c_1+kc_2) \geq \deg(a_1) + \deg(a_k) \geq 0. \tag{5.27}$$

It is now visible that the quantity in Eq. (5.25) is smaller than the right hand side of Eq. (5.4).

We next handle the terms described in Eq. (5.20) and Eq. (5.24), by first checking that the contribution from Eq. (5.20) is smaller than that of Eq. (5.24), and then bounding Eq. (5.24). For the first step, observe that Eq. (5.24) is at least

$$q^{\dim(\mathcal{J})\left(1-\frac{1}{2p}\right)}(1+2\gamma)^{2kc_1+k(c_2+\deg(\mathcal{I}))+c_2k^2}\prod_{\pi|g}(r(t_\pi)(1+\gamma))^{\deg(\pi)} \tag{5.28}$$

since conductors are nonnegative, and $\gamma \leq 1$. As g is squarefree, its degree is the sum of the degrees of its prime factors, so the above is at least

$$q^{\dim(\mathcal{J})\left(1-\frac{1}{2p}\right)}(1+2\gamma)^{2kc_1+\left(k-\frac{1}{p}\right)\deg(\mathcal{I})+c_2k(k+1)}(1+\gamma)^{\deg(g)}\prod_{\pi|g} r(t_\pi)^{\deg(\pi)}.$$

Since $\deg(\pi) \geq 1$ and $n = \frac{\dim(\mathcal{J})}{p}$, the above is at least

$$\left(q^{\frac{1}{2}\dim(\mathcal{J})+n}\prod_{\pi|g} r(t_\pi)\right)\cdot\left(q^{\dim(\mathcal{J})\left(\frac{p-3}{2p}\right)}(1+2\gamma)^{2kc_1+\left(k-\frac{1}{p}\right)\deg(\mathcal{I})+c_2k(k+1)}(1+\gamma)^{\deg(g)}\right).$$

By Eq. (4.103), Lemma 2.2(6), Lemma 2.13(5), and Proposition 2.5(4), for primes π dividing $g_{F,r}$ but not dividing g, we have $r(t_{F,r,\pi}) = 1$, and for primes $\pi \mid g$ we have $r(t_{F,r,\pi}) = r(t_\pi)$. Therefore, Eq. (5.20) equals

$$\left(q^{\frac{1}{2}\dim(\mathcal{J})+n}\prod_{\pi|g} r(t_\pi)\right)\cdot\left(\operatorname{len}(\mathcal{J})|g||a_k|q^{4k(k-1)(c_1+k\max\{c_2,0\})}\right)^{\epsilon} \tag{5.29}$$

so it suffices to show that

$$\left(\operatorname{len}(\mathcal{J})|g||a_k|q^{4k(k-1)(c_1+k\max\{c_2,0\})}\right)^{\epsilon} \leq q^{\dim(\mathcal{J})\left(\frac{p-3}{2p}\right)}(1+2\gamma)^{2kc_1+\left(k-\frac{1}{p}\right)\deg(\mathcal{I})+c_2k(k+1)}(1+\gamma)^{\deg(g)}.$$

By assumption, $\gamma > 0$ and $p \geq 3$, so by taking logarithms to base q, we see that the above reduces to

$$\begin{aligned}&\dim(\mathcal{J}) + \deg(g) + \deg(a_k) + 4k(k-1)(c_1 + k\max\{c_2, 0\}) \ll \\ &2kc_1 + \left(k - \frac{1}{p}\right)\deg(\mathcal{I}) + c_2k(k+1) + \deg(g).\end{aligned} \tag{5.30}$$

By Notation 4.1 and Eq. (5.3) we have

$$\dim(\mathcal{J}) \leq \dim(\mathcal{I}) \leq \deg(\mathcal{I}), \quad \deg(a_k) \leq c_1 + c_2k \tag{5.31}$$

so Eq. (5.30) would follow once we check that

$$c_1 + kc_2 + 4k(k-1)(c_1 + k\max\{c_2, 0\}) \ll 2kc_1 + k(k+1)c_2. \tag{5.32}$$

If $k = 1$ the above is obvious. Otherwise, because

$$c_1 \geq 0,\ c_1+kc_2 \geq \deg a_k \geq 0,\ 2kc_1+k(k+1)c_2 = (k+1)(c_1+kc_2)+(k-1)c_1,$$

we have

$$0 \leq c_1 + kc_2 \leq \frac{2kc_1 + k(k+1)c_2}{k+1}, \quad 0 \leq c_1 \leq \frac{2kc_1 + k(k+1)c_2}{k-1}, \tag{5.33}$$

so any linear combination of c_1 and c_2 is $O(2kc_1 + k(k+1)c_2)$, which establishes Eq. (5.32) and thus concludes the argument that Eq. (5.20) is smaller than Eq. (5.24).

Since Eq. (5.24) is exponential in $\dim(\mathcal{J})$, and there are $O(1)$ intervals $\mathcal{J}$ of any given dimension in our partition of $\mathcal{I}$, summing Eq. (5.24) over the intervals $\mathcal{J}$ that make up $\mathcal{I}$, we get a bound for the sum in Eq. (5.10) of

$$q^{\dim(\mathcal{I})\left(1-\frac{1}{2p}\right)}\gamma^{-\frac{\dim(\mathcal{I})}{p}}(1+2\gamma)^{2kc_1+k\max\{0,c_2+\deg(\mathcal{I})\}+c_2k^2}B(t;\gamma) \tag{5.34}$$

because the highest possible value of $\dim(\mathcal{J})$ is $\dim(\mathcal{J}) = \dim(\mathcal{I})$.

After exponentiating, the second inequality in Eq. (5.1) translates to

$$q^{\alpha} < q^{\frac{1}{2p}}\gamma^{\frac{1}{p}}(1+2\gamma)^{-k} \tag{5.35}$$

so multiplying both sides by q and rearranging we get

$$q^{1-\frac{1}{2p}}\gamma^{-\frac{1}{p}} < q^{1-\alpha}(1+2\gamma)^{-k}. \tag{5.36}$$

Raising to power $\dim(\mathcal{I})$ gives

$$q^{\dim(\mathcal{I})\left(1-\frac{1}{2p}\right)}\gamma^{-\frac{\dim(\mathcal{I})}{p}} \le q^{\dim(\mathcal{I})(1-\alpha)}(1+2\gamma)^{-k\dim(\mathcal{I})} = q^{\dim(\mathcal{I})(1-\alpha)}(1+2\gamma)^{-k(c_2+\dim(\mathcal{I}))+c_2k}$$

which implies that Eq. (5.34) is

$$\ll q^{\dim(\mathcal{I})(1-\alpha)}(1+2\gamma)^{2kc_1+k\max\{-c_2-\dim(\mathcal{I}),\deg(\mathcal{I})-\dim(\mathcal{I})\}+c_2k(k+1)}B(t;\gamma).$$

Recalling that $\beta = (1+2\gamma)^k$, and bounding the maximum of powers of β by their sum, we arrive at Eq. (5.4).

All that remains is to control the error term in Eq. (5.10), which is

$$\max\{E(c_1,c_2,\deg(\mathcal{I})),\deg(g\cdot a_k^{k+1}\cdot\Delta_v(R(F,F_v)))\}^4\prod_{\pi\mid g}r(t_\pi). \tag{5.37}$$

For every $\epsilon > 0$ we have

$$\deg(g\cdot a_k^{k+1}\cdot\Delta_v(R(F,F_v)))^4\prod_{\pi\mid g}r(t_\pi) \ll |g|^\epsilon|a_k|^\epsilon|\Delta_v(R(F,F_v))|^\epsilon\prod_{\pi\mid g}r(t_\pi)$$

so by Proposition 4.22, the above is bounded by Eq. (5.29). We have seen that the latter is bounded by Eq. (5.24) which led us to Eq. (5.4), so this term is controlled.

By the definition of E in Eq. (4.67) we have

$$E(c_1,c_2,\deg(\mathcal{I}))^4\prod_{\pi\mid g}r(t_\pi) \ll q^{\epsilon(2c_1+\max\{0,c_2+\deg(\mathcal{I})\}+c_2k)}\prod_{\pi\mid g}r(t_\pi) \tag{5.38}$$

for every $\epsilon > 0$. In case the maximum is attained at 0, we have

$$c_2+\dim(\mathcal{I}) \le c_2+\deg(\mathcal{I}) \le 0 \tag{5.39}$$

so by Eq. (5.27), the right hand side of Eq. (5.38) is

$$\begin{aligned} q^{\epsilon(2c_1+(k+1)c_2)}q^{-\epsilon c_2}\prod_{\pi\mid g}r(t_\pi) &= q^{\epsilon\dim(\mathcal{I})}q^{\epsilon(2c_1+(k+1)c_2)}q^{\epsilon(-c_2-\dim(\mathcal{I}))}\prod_{\pi\mid g}r(t_\pi) \\ &\ll q^{(1-\alpha)\dim(\mathcal{I})}\beta^{2c_1+(k+1)c_2}\beta^{-c_2-\dim(\mathcal{I})}\prod_{\pi\mid g}r(t_\pi) \end{aligned}$$

which is bounded by Eq. (5.4).

If the maximum in Eq. (5.38) is attained at $c_2+\deg(\mathcal{I})$, then the right hand side of Eq. (5.38) is

$$\begin{aligned} &q^{\epsilon\dim(\mathcal{I})}q^{\epsilon(2c_1+c_2(k+1))}q^{\epsilon(\deg(\mathcal{I})-\dim(\mathcal{I}))}\prod_{\pi\mid g}r(t_\pi) \ll \\ &q^{(1-\alpha)\dim(\mathcal{I})}\beta^{2c_1+c_2(k+1)}\beta^{\deg(\mathcal{I})-\dim(\mathcal{I})}\prod_{\pi\mid g}r(t_\pi) \end{aligned} \tag{5.40}$$

again bounded by Eq. (5.4). □

Corollary 5.2. *Let p be an odd prime, let k be a positive integer, and let*

$$q > 4e^2k^2p^2 \tag{5.41}$$

be a power of p. Take a nonnegative integer n, a scalar $\lambda \in \mathbb{F}_q$, and define the interval

$$\mathcal{I} = \{f_n u^n + f_{n-1}u^{n-1} + \cdots + f_0 u^0 \in \mathbb{F}_q[u] : f_n = \lambda\}. \tag{5.42}$$

Then for a separable polynomial $F(T) \in \mathbb{F}_q[u][T]$ with $\deg_T(F) = k$, and an infinitame trace function t to a squarefree modulus $g \in \mathbb{F}_q[u]$ we have

$$\sum_{f \in \mathcal{I}} \mu(F(f))t(f) \ll q^{n\left(1-\frac{1}{2p}+\frac{\log_q(2ekp)}{p}\right)} \prod_{\pi | g} \left(r(t_\pi)\left(1+\frac{1}{2kp}\right) + \frac{c(t_\pi)}{2kp}\right)^{\deg(\pi)}$$

as $n \to \infty$, with the implied constant depending only on q and F.

Proof. We invoke Theorem 5.1 with

$$\gamma = \frac{1}{2kp}, \quad \alpha = \frac{1}{2p} - \frac{\log_q(2ekp)}{p}, \quad c_1 = \deg_u(F), \quad c_2 = 0, \tag{5.43}$$

and note that the positivity of α follows from Eq. (5.41) by taking logarithms and dividing by $2p$. Moreover we have

$$\begin{aligned} \alpha = \frac{1}{2p} + \frac{\log_q(\gamma)}{p} - \frac{\log_q(e)}{p} &< \frac{1}{2p} + \frac{\log_q(\gamma)}{p} - \frac{\log_q\left(1+\frac{1}{kp}\right)^{kp}}{p} \\ &= \frac{1}{2p} + \frac{\log_q(\gamma)}{p} - k\log_q(1+2\gamma) \end{aligned} \tag{5.44}$$

so the assumptions on γ and α in Theorem 5.1 hold. The result follows by absorbing into the implied constant all the factors in Eq. (5.4) that depend only on q, F, and checking that $\dim(\mathcal{I}) = n = \deg(\mathcal{I})$. □

Now we deduce Theorem 1.3.

Proof of Theorem 1.3. We invoke Corollary 5.2 with

$$n = \lfloor \log_q(X) \rfloor + 1, \quad \lambda = 0, \quad g = 1, \quad t = 1, \tag{5.45}$$

and since $q > 4e^2k^2p^2$, get that

$$\sum_{\substack{f \in \mathbb{F}_q[u] \\ |f| \le X}} \mu(F(f)) \ll X^{1-\frac{1}{2p}+\frac{\log_q(2ekp)}{p}} = o(X) \tag{5.46}$$

as required. □

We similarly deduce Theorem 1.13.

Proof of Theorem 1.13. We invoke Corollary 5.2 with

$$k = 1, \quad \lambda = 1, \quad F(u,T) = T, \quad g = \pi, \tag{5.47}$$

and get that

$$\sum_{f \in \mathcal{M}_n} \mu(f)t(f) \ll |\mathcal{M}_n|^{1-\frac{1}{2p}+\frac{\log_q(2ep)}{p}} \left(r(t)\left(1+\frac{1}{2p}\right) + \frac{c(t)}{2p} \right)^{\deg(\pi)}$$
$$= |\mathcal{M}_n|^{1-\frac{1}{2p}+\frac{\log_q(2ep)}{p}} |\pi|^{\log_q\left(r(t)\left(1+\frac{1}{2p}\right)+\frac{c(t)}{2p}\right)}.$$

□

We will need the following consequence of Theorem 5.1 in the proof of Theorem 1.2.

Corollary 5.3. *Keep Notation 2.16 and Notation 4.1. Fix an odd prime p, and a power q of p. Let $0 < \gamma \leq 1$ and α be real numbers satisfying*

(5.48)
$$0 < \alpha < \min\left\{ \frac{1}{2} - 10\log_q(1+2\gamma) + \log_q(1+3\gamma), \frac{1}{2p} + \frac{\log_q \gamma}{p} - 2\log_q(1+2\gamma) \right\}.$$

Set $\beta = (1+2\gamma)^2$.

Let n be a nonnegative integer, pick $c_1, c_2, c_3 \in \mathbb{R}$ with $c_1 \geq 0 \geq c_2$, and let $a, b, c \in \mathbb{F}_q[u]$ be polynomials satisfying

$$b^2 - 4ac \neq 0, \quad \deg(a) \leq c_1 + 2c_2, \ \deg(b) \leq c_1 + c_2 - n, \ \deg(c) \leq c_1 - 2n.$$

For every nonzero polynomial $y \in \mathbb{F}_q[u]$ of degree at most n put

$$F_y(T) = aT^2 + byT + cy^2 \in \mathbb{F}_q[u][T] \tag{5.49}$$

and let $\mathcal{I}_y$ be an interval in $\mathbb{F}_q[u]$ of degree at most c_3. Then for $h \in \mathbb{F}_q[u]$ we have

(5.50)
$$\sum_{\substack{y \in \mathbb{F}_q[u]\setminus\{0\} \\ \deg(y) \leq n}} \left| \sum_{\substack{x \in \mathcal{I}_y \\ \gcd(x,y)=1}} \mu(F_y(x)) e\left(\frac{h\overline{x}}{y}\right) \right| \ll q^{n+c_3(1-\alpha)} \beta^{2c_1+3c_2} \left(\beta^{-c_2-c_3}+1\right)(1+3\gamma)^n$$

as $n \to \infty$, with the implied constant depending only on q, α, γ.

Proof. Every monic polynomial $y \in \mathbb{F}_q[u]$ can be decomposed uniquely as $y = y_1y_2$ with y_1 a squareful monic polynomial, and y_2 a squarefree monic polynomial coprime to y_1. Explicitly, the polynomial y_2 is the product of all those primes $\pi \in \mathbb{F}_q[u]$ for which π divides y, but π^2 does not divide y. We can therefore bound our sum by

$$\sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{\substack{y_2 \in \mathcal{H}_{n-m} \\ \gcd(y_1,y_2)=1}} \left| \sum_{\substack{x \in \mathcal{I}_{y_1y_2} \\ \gcd(x,y_1y_2)=1}} \mu(F_{y_1y_2}(x)) e\left(\frac{h\overline{x}}{y_1y_2}\right) \right| \tag{5.51}$$

where $\mathcal{S}_m, \mathcal{H}_{n-m} \subseteq \mathbb{F}_q[u]$ are the sets of squareful polynomials of degree m and squarefree polynomials of degree $n-m$ respectively. Since every polynomial in $\mathcal{S}_m$ is the product of a square and a cube, we have

$$|\mathcal{S}_m| \ll q^{\frac{m}{2}}, \tag{5.52}$$

see [RG17, (2.7)].

For every two coprime polynomials $y_1, y_2 \in \mathbb{F}_q[u]$, we can find polynomials $A, B \in \mathbb{F}_q[u]$ with $Ay_1 + By_2 = 1$, so we can rewrite the above as

$$\sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{\substack{y_2 \in \mathcal{H}_{n-m} \\ \gcd(y_1,y_2)=1}} \left| \sum_{\substack{x \in \mathcal{I}_{y_1y_2} \\ \gcd(x,y_1y_2)=1}} \mu(F_{y_1y_2}(x)) e\left(\frac{Bh\overline{x}}{y_1}\right) e\left(\frac{Ah\overline{x}}{y_2}\right) \right|. \tag{5.53}$$

We use the trivial bound for those pairs (y_1, y_2) with $\deg(y_1) > \dim(\mathcal{I}_{y_1y_2})$, which is

$$\sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{\substack{y_2 \in \mathcal{H}_{n-m} \\ \gcd(y_1,y_2)=1}} q^{\dim(\mathcal{I}_{y_1y_2})} \le \sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{y_2 \in \mathcal{H}_{n-m}} q^{\min\{\deg(\mathcal{I}_{y_1y_2}),\deg(y_1)\}} \le$$

$$\sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{y_2 \in \mathcal{H}_{n-m}} q^{\frac{c_3+m}{2}} \ll \sum_{m=0}^{n} q^{\frac{m}{2}} q^{n-m} q^{\frac{c_3+m}{2}} \ll nq^{n+\frac{c_3}{2}} \ll (1+3\gamma)^n q^{n+(1-\alpha)c_3}$$

and that is bounded by the right hand side of Eq. (5.50).

For the other pairs (y_1, y_2) in Eq. (5.53), those with $\dim(\mathcal{I}_{y_1y_2}) \ge \deg(y_1)$, we define the intervals

$$\mathcal{I}^r_{y_1y_2} = \left\{ \frac{f-r}{y_1} : f \in \mathcal{I}_{y_1y_2}, \ f \equiv r \bmod y_1 \right\}, \quad r \in \mathbb{F}_q[u], \ \deg(r) < \deg(y_1),$$

so that the sum over those (y_1, y_2) can be bounded, using the triangle inequality, by

$$\sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{\substack{r \in \mathbb{F}_q[u] \\ \deg(r)<m \\ \gcd(r,y_1)=1}} \sum_{\substack{y_2 \in \mathcal{H}_{n-m} \\ \gcd(y_1,y_2)=1 \\ \dim(\mathcal{I}_{y_1y_2}) \ge m}} \left| \sum_{\substack{z \in \mathcal{I}^r_{y_1y_2} \\ \gcd(y_1z+r,y_2)=1}} \mu(F_{y_1y_2}(y_1z+r)) e\left(\frac{Ah\overline{(y_1z+r)}}{y_2}\right) \right|$$

where $x = y_1z + r$.

Since y_2 is squarefree, from Proposition 2.17 we get that the above is at most

$$\sum_{m=0}^{n} \sum_{y_1 \in \mathcal{S}_m} \sum_{\substack{r \in \mathbb{F}_q[u] \\ \deg(r)<m}} \sum_{\substack{y_2 \in \mathcal{H}_{n-m} \\ \dim(\mathcal{I}_{y_1y_2}) \ge m}} \left| \sum_{\substack{z \in \mathcal{I}^r_{y_1y_2} \\ \gcd(y_1z+r,y_2)=1}} \mu(F_{y_1y_2}(y_1z+r)) t(y_1z+r) \right|$$

where t is an infinitame trace function with

$$r(t) \leq 1, \quad c(t) \leq 2. \tag{5.54}$$

We have

$$\begin{aligned} F_{y_1y_2}(y_1T+r) &= a(y_1T+r)^2 + by_1y_2(y_1T+r) + cy_1^2y_2^2 \\ &= ay_1^2T^2 + (2ary_1 + by_1^2y_2)T + ar^2 + bry_1y_2 + cy_1^2y_2^2. \end{aligned}$$

It follows from our initial assumptions on a, b, c, and c_2 that the degrees of the coefficients of $F_{y_1y_2}(y_1T+r)$ satisfy

$$\deg(ar^2+bry_1y_2+cy_1^2y_2^2) \leq \max\{c_1+2c_2+2m, c_1+c_2-n+m+n, c_1-2n+2n\} \leq c_1+2m,$$

$$\deg(2ary_1+by_1^2y_2) \leq \max\{c_1+2c_2+m+m, c_1+c_2-n+2m+n-m\} \leq c_1+c_2+2m,$$

and

$$\deg(ay_1^2) \leq c_1 + 2c_2 + 2m.$$

We can drop the condition $\gcd(y_1z+r, y_2) = 1$ in the sum above since for any nonconstant common divisor $D \in \mathbb{F}_q[u]$ of y_1z+r and y_2, we see that D^2 divides $F_{y_1y_2}(y_1z+r)$ so $\mu(F_{y_1y_2}(y_1z+r)) = 0$. Since $b^2 - 4ac \neq 0$, the polynomial $F_{y_1y_2}(y_1T+r)$ is separable, so we can invoke Theorem 5.1 with

$$p,\ q,\ k=2,\ \gamma,\ \alpha,\ c_1+2m,\ c_2,\ g=y_2,\ t, \tag{5.55}$$

and get from Eq. (5.54) that the sum above is

$$\ll \sum_{m=0}^{n} \sum_{y_1\in\mathcal{S}_m} \sum_{\substack{r\in\mathbb{F}_q[u] \\ \deg(r)<m}} \sum_{\substack{y_2\in\mathcal{H}_{n-m} \\ \dim(\mathcal{I}_{y_1y_2})\geq m}} q^{\dim(\mathcal{I}^r_{y_1y_2})(1-\alpha)}\beta^{2c_1+4m+3c_2}\left(\beta^{-c_2-\dim(\mathcal{I}^r_{y_1y_2})}+\beta^{\deg(\mathcal{I}^r_{y_1y_2})-\dim(\mathcal{I}^r_{y_1y_2})}\right)\prod_{\pi|y_2}(1+3\gamma)^{\deg(\pi)}. \tag{5.56}$$

Since y_2 is squarefree we have

$$\prod_{\pi|y_2}(1+3\gamma)^{\deg(\pi)} = (1+3\gamma)^{\sum_{\pi|y_2}\deg(\pi)} = (1+3\gamma)^{\deg(y_2)}. \tag{5.57}$$

By our assumptions we have $\gamma \leq 1$ hence

$$\alpha < \frac{1}{2p} + \frac{\log_q \gamma}{p} - 2\log_q(1+2\gamma) \leq 1 - 2\log_q(1+2\gamma) \tag{5.58}$$

so from our choice of β we get

$$\log_q \beta = 2\log_q(1+2\gamma) \leq 1-\alpha \tag{5.59}$$

or equivalently $\beta \leq q^{1-\alpha}$.

Since $\dim(\mathcal{I}_{y_1y_2}) \geq m$ we have

$$\dim(\mathcal{I}^r_{y_1y_2}) = \dim(\mathcal{I}_{y_1y_2}) - m \leq \deg(\mathcal{I}_{y_1y_2}) - m \leq c_3 - m \tag{5.60}$$

so

$$q^{\dim(\mathcal{I}^r_{y_1y_2})(1-\alpha)}\beta^{-c_2-\dim(\mathcal{I}^r_{y_1y_2})} \leq q^{(c_3-m)(1-\alpha)}\beta^{-c_2-(c_3-m)} \tag{5.61}$$

because $\beta \le q^{1-\alpha}$, and similarly

$$q^{\dim(\mathcal{I}^r_{y_1y_2})(1-\alpha)}\beta^{\deg(\mathcal{I}^r_{y_1y_2})-\dim(\mathcal{I}^r_{y_1y_2})} \le q^{(c_3-m)(1-\alpha)}\beta^{c_3-(c_3-m)}. \tag{5.62}$$

It follows from Eq. (5.52), Eq. (5.57), Eq. (5.61), and Eq. (5.62) that Eq. (5.56) is

$$\ll \sum_{m=0}^{n} q^{\frac{m}{2}} q^m q^{n-m} q^{(c_3-m)(1-\alpha)} \beta^{2c_1+4m+3c_2}(\beta^{m-c_2-c_3}+\beta^m)(1+3\gamma)^{n-m} \tag{5.63}$$

which simplifies to

$$q^{n+c_3(1-\alpha)}\beta^{2c_1+3c_2}(\beta^{-c_2-c_3}+1)(1+3\gamma)^n \sum_{m=0}^{n}\left(\frac{q^{\alpha-\frac{1}{2}}\beta^5}{1+3\gamma}\right)^m \tag{5.64}$$

so to obtain the bound in Eq. (5.50), it suffices to check that

$$\frac{q^{\alpha-\frac{1}{2}}\beta^5}{1+3\gamma} < 1. \tag{5.65}$$

After taking logarithms in the above, rearranging, and recalling that by definition $\beta = (1+2\gamma)^2$, the above becomes

$$\alpha < \frac{1}{2} - 10\log_q(1+2\gamma) + \log_q(1+3\gamma) \tag{5.66}$$

which is part of our initial assumptions. □

6. Quadratic congruences

Notation 6.1. Let $N \in \mathbb{F}_q[u]$ be a nonzero polynomial, and set $n = \deg(N)$. We identify $\mathbb{F}_q[u]/(N)$ with the set of representatives

$$\mathcal{P}_{<n} = \{f \in \mathbb{F}_q[u] : \deg(f) < n\} \tag{6.1}$$

for the residue classes. As in Section 2.4.1, for a polynomial $M \in \mathbb{F}_q[u]$ we denote by $\widetilde{M}$ the unique representative of its residue class in $\mathcal{P}_{<n}$.

Proposition 6.2. *For an integer $0 \le d \le n$, the indicator function of the degree of the reduction of M mod N being less than d can be expressed as*

$$\mathbf{1}_{\deg(\widetilde{M})<d} = q^{d-n} \sum_{\substack{h\in\mathbb{F}_q[u] \\ \deg(h)<n-d}} e\left(\frac{hM}{N}\right). \tag{6.2}$$

Proof. We claim first that the indicator function of the $\mathbb{F}_p$-subspace $\mathcal{P}_{<d}$ of $\mathbb{F}_q[u]/(N)$ equals the average over all additive characters of $\mathbb{F}_q[u]/(N)$ that are identically 1 on $\mathcal{P}_{<d}$. Clearly, this average is 1 on $\mathcal{P}_{<d}$, so the claim follows in case $d = n$. In case $d < n$, we restrict to the (nonempty) complementof $\mathcal{P}_{<d}$ in $\mathbb{F}_q[u]/(N)$, and view our average as the average over all characters of the nontrivial quotient group

$$Q_d = \frac{\mathbb{F}_q[u]/(N)}{\mathcal{P}_{<d}}. \tag{6.3}$$

By orthogonality of characters, this average vanishes, so our claim is verified.

The number of characters we are averaging over is

$$|Q_d| = \left|\frac{\mathbb{F}_q[u]/(N)}{\mathcal{P}_{<d}}\right| = \frac{|\mathbb{F}_q[u]/(N)|}{|\mathcal{P}_{<d}|} = \frac{q^n}{q^d} = q^{n-d} \tag{6.4}$$

so by Section 2.4.1, these characters are

$$\psi_h(M) = e\left(\frac{hM}{N}\right), \quad h \in \mathbb{F}_q[u], \quad \deg(h) < n-d, \tag{6.5}$$

hence the proposition follows. □

Notation 6.3. Let D in $\mathbb{F}_q[u]$ be a polynomial for which the polynomial

$$F(T) = T^2 + D \in \mathbb{F}_q[u][T] \tag{6.6}$$

is irreducible over $\mathbb{F}_q[u]$. For nonnegative integers d, k, and $A \in \mathcal{M}_k$, we set

$$\rho_d(A;F) = |\{f \in \mathcal{M}_d : F(f) \equiv 0 \bmod A\}|, \quad \rho(A;F) = \rho_k(A;F). \tag{6.7}$$

In case $d \geq k$ we clearly have

$$\rho_d(A;F) = q^{d-k}\rho(A;F). \tag{6.8}$$

Corollary 6.4. *Suppose that $d < k$. Then*

$$\rho_d(A;F) = q^{d-k}\rho(A;F) + q^{d-k} \sum_{\substack{h \in \mathbb{F}_q[u] \setminus \{0\} \\ \deg(h) < k-d}} e\left(\frac{-hu^d}{A}\right) \sum_{\substack{f \in \mathbb{F}_q[u]/(A) \\ F(f) \equiv 0 \bmod A}} e\left(\frac{hf}{A}\right).$$

Proof. We have

$$\rho_d(A;F) = \sum_{\substack{f \in \mathbb{F}_q[u]/(A) \\ F(f) \equiv 0 \bmod A}} \mathbf{1}_{f \in \mathcal{M}_d} = \sum_{\substack{f \in \mathbb{F}_q[u]/(A) \\ F(f) \equiv 0 \bmod A}} \mathbf{1}_{\deg(f-u^d)<d} \tag{6.9}$$

which by Proposition 6.2 equals

$$q^{d-k} \sum_{\substack{h \in \mathbb{F}_q[u] \\ \deg(h) < k-d}} e\left(\frac{-hu^d}{A}\right) \sum_{\substack{f \in \mathbb{F}_q[u]/(A) \\ F(f) \equiv 0 \bmod A}} e\left(\frac{hf}{A}\right). \tag{6.10}$$

Separating the contribution of $h = 0$ gives the corollary. □

Proposition 6.5. *For every positive integer k and every $\epsilon > 0$ we have*

$$\sum_{A \in \mathcal{M}_k} \rho(A;F) \ll |\mathcal{M}_k| \cdot |D|^\epsilon \tag{6.11}$$

with the implied constant depending only on q and ϵ.

Proof. We can decompose uniquely $D = D_1 D_2^2$ where

$$D_1 = \prod_{\substack{\pi \mid D \\ v_\pi(D) \equiv 1 \bmod 2}} \pi \tag{6.12}$$

is squarefree. We define a (completely multiplicative) function by

$$\chi(f) = \left(\frac{-D_1}{f}\right), \quad f \in \mathbb{F}_q[u] \setminus \{0\}. \tag{6.13}$$

If $\pi \in \mathbb{F}_q[u]$ is a prime that does not divide D, for every positive integer r we can use Legendre symbols to write

$$\rho(\pi^r; F) = 1 + \left(\frac{-D}{\pi}\right) = 1 + \left(\frac{-D_1 D_2^2}{\pi}\right) = 1 + \chi(\pi) \tag{6.14}$$

in view of Hensel's Lemma.

If $\pi \in \mathbb{F}_q[u]$ is a prime that divides D_1, for every integer $r \geq 1$ we have

$$\rho(\pi^r; F) = \begin{cases} |\pi|^{\lfloor \frac{r}{2} \rfloor} & r \leq v_\pi(D) \\ 0 & r > v_\pi(D). \end{cases} \tag{6.15}$$

Indeed, when $D \equiv 0 \mod \pi^r$, we are counting the elements in $\mathbb{F}_q[u]/(\pi^r)$ which square to zero, or equivalently are zero mod $\pi^{\lceil \frac{r}{2} \rceil}$, so their number is

$$\frac{|\pi|^r}{|\pi|^{\lceil \frac{r}{2} \rceil}} = |\pi|^{r - \lceil \frac{r}{2} \rceil} = |\pi|^{\lfloor \frac{r}{2} \rfloor}. \tag{6.16}$$

Since $v_\pi(D)$ is odd by our definition of D_1 in Eq. (6.12), no element of $\mathbb{F}_q[u]/(\pi^r)$ has square congruent to $-D$ mod π^r for $r > v_\pi(D)$.

Finally, if π divides D_2 and does not divide D_1, for $r \geq 1$ we have

$$\rho(\pi^r; F) = \begin{cases} |\pi|^{\lfloor \frac{r}{2} \rfloor} & r \leq v_\pi(D) \\ (1 + \chi(\pi))|\pi|^{v_\pi(D_2)} & r > v_\pi(D). \end{cases} \tag{6.17}$$

Indeed, the first case is established as in Eq. (6.15). For the second case we note that every element in $\mathbb{F}_q[u]/(\pi^r)$ is of the form $\pi^i \alpha$ for a unique choice of $0 \leq i \leq r$ and $\alpha \in (\mathbb{F}_q[u]/(\pi^{r-i}))^\times$. The elements whose square is $-D$ are those that have

$$i = \frac{v_\pi(D)}{2} = \frac{v_\pi(D_1 D_2^2)}{2} = \frac{v_\pi(D_1) + 2v_\pi(D_2)}{2} = v_\pi(D_2) \tag{6.18}$$

and

$$\alpha^2 \equiv -D\pi^{-v_\pi(D)} \equiv -D_1 D_2^2 \pi^{-2v_\pi(D_2)} \mod \pi^{r - 2v_\pi(D_2)}. \tag{6.19}$$

The number of such $\alpha \in (\mathbb{F}_q[u]/(\pi^{r - v_\pi(D_2)}))^\times$ is

$$\left(1 + \left(\frac{-D_1 D_2^2 \pi^{-2v_\pi(D_2)}}{\pi}\right)\right) \frac{|\pi|^{r - v_\pi(D_2)}}{|\pi|^{r - 2v_\pi(D_2)}} = (1 + \chi(\pi))|\pi|^{v_\pi(D_2)} \tag{6.20}$$

as stated in the second case of Eq. (6.17).

Let us now define the formal power series

$$H(t) = \sum_{k=0}^{\infty} t^k \sum_{A \in \mathcal{M}_k} \rho(A; F).$$

For compactness of notation, we will write d_π for $\deg(\pi)$.

The function $A \mapsto \rho(A, F)$ is multiplicative so in view of Eq. (6.14), Eq. (6.15), and Eq. (6.17), we have the formal Euler product

$$H(t) = \sum_{k=0}^{\infty} t^k \sum_{A \in \mathcal{M}_k} \rho(A; F) = \prod_{\pi} \left(\sum_{r=0}^{\infty} t^{rd_\pi} \rho(\pi^r; F) \right) =$$

$$\prod_{\pi \nmid D} \left(1 + (1 + \chi(\pi)) \sum_{r=1}^{\infty} t^{rd_\pi} \right) \cdot \prod_{\pi | D_1} \left(\sum_{r=0}^{v_\pi(D)} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi} \right) \cdot$$

$$\prod_{\substack{\pi | D_2 \\ \pi \nmid D_1}} \left((1 + \chi(\pi)) |\pi|^{v_\pi(D_2)} \sum_{r > 2v_\pi(D_2)} t^{rd_\pi} + \sum_{r=0}^{2v_\pi(D_2)} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi} \right).$$

We will now express the above as the product of

$$L(t; \chi) \zeta_{\mathbb{F}_q[u]}(t) = \prod_{\pi \nmid D_1} \frac{1}{1 - \chi(\pi) t^{d_\pi}} \cdot \prod_{\pi} \frac{1}{1 - t^{d_\pi}} \tag{6.21}$$

with a rapidly converging Euler product. To do this, note that for primes π not dividing D we have

$$(1 - \chi(\pi) t^{d_\pi})(1 - t^{d_\pi}) \left(1 + (1 + \chi(\pi)) \sum_{r=1}^{\infty} t^{rd_\pi} \right) =$$

$$(1 - \chi(\pi) t^{d_\pi})(1 + \chi(\pi) t^{d_\pi}) = 1 - \chi^2(\pi) t^{2d_\pi} = 1 - t^{2d_\pi}.$$

Similarly, for primes π dividing D_2 but not D_1 we get

$$(1 - \chi(\pi) t^{d_\pi})(1 - t^{d_\pi}) \Big((1 + \chi(\pi)) |\pi|^{v_\pi(D_2)} \sum_{r > 2v_\pi(D_2)} t^{rd_\pi} + \sum_{r=0}^{2v_\pi(D_2)} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi} \Big)$$

$$= |\pi|^{v_\pi(D_2)} t^{2d_\pi v_\pi(D_2)} (1 - t^{2d_\pi}) + (1 - \chi(\pi) t^{d_\pi})(1 - t^{d_\pi}) \sum_{r=0}^{2v_\pi(D_2)-1} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi}.$$

Combining these, we obtain

$$H(t) = L(t; \chi) \zeta_{\mathbb{F}_q[u]}(t) \prod_{\pi \nmid D} \Big(1 - t^{2d_\pi} \Big) \prod_{\pi | D_1} \Big((1 - t^{d_\pi}) \sum_{r=0}^{v_\pi(D)} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi} \Big)$$
$$\prod_{\substack{\pi | D_2 \\ \pi \nmid D_1}} \Big(|\pi|^{v_\pi(D_2)} t^{2d_\pi v_\pi(D_2)} (1 - t^{2d_\pi}) + (1 - \chi(\pi) t^{d_\pi})(1 - t^{d_\pi}) \sum_{r=0}^{2v_\pi(D_2)-1} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi} \Big). \tag{6.22}$$

A priori this is only a formal identity, but $L(t, \chi)$ and $\zeta_{\mathbb{F}_q[u]}(t)$ are absolutely convergent for $|t| < q^{-1}$ and admit meromorphic continuation to the whole complex plane. We will next show that the remaining Euler product terms converge absolutely for $|t| \leq q^{-3/4}$ and in fact are $\ll |D|^\epsilon$ (any cutoff strictly between $\frac{1}{2}$ and 1 in place of $\frac{3}{4}$ would work equally well for our purposes here). It will follow that $H(t)$ is absolutely convergent for $|t| < q^{-1}$ and admits meromorphic continuation to the disc $|t| \leq q^{-3/4}$, and that the identity Eq. (6.22) holds on that disc.

We have

$$\left|\prod_{\pi \nmid D}\left(1 - t^{2d_\pi}\right)\right| \leq \prod_{\pi}\left(1 + |\pi|^{-2\cdot\frac{3}{4}}\right) \leq \prod_{\pi} \frac{1}{1 - |\pi|^{-\frac{3}{2}}} = \frac{1}{1 - q^{-\frac{1}{2}}} \ll 1.$$

The contribution of each prime π dividing D_1 is

$$\left|(1 - t^{d_\pi}) \sum_{r=0}^{v_\pi(D)} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi}\right| \leq (1+|\pi|^{-\frac{3}{4}}) \sum_{r=0}^{\infty} |\pi|^{\frac{r}{2} - \frac{3r}{4}} = (1+|\pi|^{-\frac{3}{4}}) \frac{1}{1 - |\pi|^{-\frac{1}{4}}} \leq |\pi|^{\epsilon}$$

for all but finitely many primes π in $\mathbb{F}_q[u]$. Similarly, every prime π dividing D_2 but not D_1 gives

$$\left| |\pi|^{v_\pi(D_2)} t^{2d_\pi v_\pi(D_2)} (1 - t^{2d_\pi}) + (1 - \chi(\pi) t^{d_\pi})(1 - t^{d_\pi}) \sum_{r=0}^{2v_\pi(D_2)-1} |\pi|^{\lfloor \frac{r}{2} \rfloor} t^{rd_\pi} \right| \leq$$

$$|\pi|^{-\frac{1}{2} v_\pi(D_2)} (1 + |\pi|^{-\frac{3}{2}}) + (1 + |\pi|^{-\frac{3}{4}})^2 \sum_{r=0}^{\infty} |\pi|^{\frac{r}{2} - \frac{3r}{4}} \leq$$

$$|\pi|^{-\frac{1}{2}} (1 + |\pi|^{-\frac{3}{2}}) + (1 + |\pi|^{-\frac{3}{4}})^2 \frac{1}{1 - |\pi|^{-\frac{1}{4}}} \leq |\pi|^{\epsilon}$$

for all but finitely many π. Combining these, we obtain

$$\frac{H(t)}{L(t;\chi)\zeta_{\mathbb{F}_q[u]}(t)} \ll |D|^{\epsilon}, \quad |t| \leq q^{-\frac{3}{4}}, \tag{6.23}$$

and recall that $\zeta_{\mathbb{F}_q[u]}(t) = (1 - qt)^{-1}$.

We now split into two cases. In the first case, D_1 is nonconstant, so $L(t;\chi)$ is a polynomial in t which satisfies

$$L(t;\chi) \ll |D|^{\epsilon}, \quad |t| \leq q^{-\frac{3}{4}}, \tag{6.24}$$

by Weil's Riemann Hypothesis, see for instance [Flo17, Corollary 8.2]. Therefore, the only pole of H with $|t| \leq q^{-\frac{3}{4}}$ is at $t = q^{-1}$, and this pole is simple. By Cauchy's residue theorem, we thus have

$$\begin{aligned}
\sum_{A \in \mathcal{M}_k} \rho(A;F) &\ll \left| \oint_{|t| = q^{-\frac{3}{4}}} \frac{H(t)}{t^{k+1}} \right| + \left| q^{k+1} \operatorname{Res}_{t=q^{-1}} H(t) \right| \\
&\ll \oint_{|t| = q^{-\frac{3}{4}}} \frac{|D|^{\epsilon} \, |1 - qt|^{-1}}{|t|^{k+1}} + q^{k+1} |D|^{\epsilon} \left| \operatorname{Res}_{t=q^{-1}} (1 - qt)^{-1} \right| \\
&\ll |D|^{\epsilon} \left| 1 - q^{\frac{1}{4}} \right|^{-1} q^{\frac{3k}{4}} + q^{k} |D|^{\epsilon} \ll q^{k} |D|^{\epsilon}.
\end{aligned}$$

In the second case D_1 is constant, so

$$L(t;\chi) = \sum_{k=0}^{\infty} t^k \sum_{f\in\mathcal{M}_k} \chi(f) = \sum_{k=0}^{\infty} t^k q^k (-1)^k = \frac{1}{1+qt}. \tag{6.25}$$

Therefore, the only poles of H with $|t| \le q^{-\frac{3}{4}}$ are $t = \pm q^{-1}$, and these poles are simple. From Cauchy's residue theorem we similarly get

$$\begin{aligned}\sum_{A\in\mathcal{M}_k} \rho(A;F) &\ll \left| \oint_{|t|=q^{-\frac{3}{4}}} \frac{H(t)}{t^{k+1}} \right| + \left| q^{k+1} \operatorname{Res}_{t=\pm q^{-1}} H(t) \right| \\ &\ll \oint_{|t|=q^{-\frac{3}{4}}} \frac{|D|^{\epsilon} \left|1-qt\right|^{-1} \left|1+qt\right|^{-1}}{|t|^{k+1}} + q^{k+1}|D|^{\epsilon} \left|\operatorname{Res}_{t=\pm q^{-1}} (1 \mp qt)^{-1}\right| \\ &\ll |D|^{\epsilon} \left|1-q^{\frac{1}{2}}\right|^{-1} q^{\frac{3k}{4}} + q^k|D|^{\epsilon} \ll q^k |D|^{\epsilon}.\end{aligned}$$

□

Notation 6.6. Keep Notation 6.3. For a prime $\pi \in \mathbb{F}_q[u]$ set

$$\chi_F(\pi) = \rho(\pi;F) - 1 = |\{f \in \mathbb{F}_q[u]/(\pi) : F(f) \equiv 0 \bmod \pi\}| - 1 = \left(\frac{-D}{\pi}\right)$$

and define the singular series

$$\mathfrak{S}(F) = \prod_{\pi} \left(1 - (1+\chi_F(\pi))\,|\pi|^{-1}\right)\left(1-|\pi|^{-1}\right)^{-1}. \tag{6.26}$$

Define also the L-function of χ_F (in the variable $t = q^{-s}$) to be

$$L(t;\chi_F) = \prod_{\pi} \frac{1}{1-\chi_F(\pi)t^{\deg(\pi)}}. \tag{6.27}$$

Proposition 6.7. *For a positive integer n we have*

$$\sum_{k=1}^{n} kq^{-k} \sum_{A\in\mathcal{M}_k} \mu(A)\rho(A;F) = -\mathfrak{S}(F) + q^{-\frac{n}{2}+o(n)}, \quad n \to \infty, \tag{6.28}$$

as soon as $\deg_u(F) \ll n$*.*

Proof. We define

$$Z(t) = t\frac{d}{dt}\sum_{k=0}^{\infty} t^k \sum_{A\in\mathcal{M}_k} \mu(A)\rho(A;F) \tag{6.29}$$

and use the multiplicativity in A of $\mu(A)$ and $\rho(A;F)$ to write the above as an Euler product, getting an equality of formal power series

$$Z(t) = t\frac{d}{dt}\prod_{\pi}\left(1-(1+\chi_F(\pi))\,t^{\deg(\pi)}\right) = t\frac{d}{dt}\left((1-qt)G(t)\right) \tag{6.30}$$

where

$$G(t) = \prod_{\pi}\left(1-(1+\chi_F(\pi))\,t^{\deg(\pi)}\right)\left(1-t^{\deg(\pi)}\right)^{-1}. \tag{6.31}$$

An alternative expression for $G(t)$ is

$$G(t) = L(t;\chi_F)^{-1}\prod_{\pi}\left(1 - \frac{t^{2\deg(\pi)}\chi_F(\pi)}{(1-t^{\deg(\pi)})(1-\chi_F(\pi)t^{\deg(\pi)})}\right). \tag{6.32}$$

By the derivative product rule and Eq. (6.26), we have

$$Z\left(\frac{1}{q}\right) = -G\left(\frac{1}{q}\right) = -\mathfrak{S}(F). \tag{6.33}$$

By Cauchy's differentiation formula, the left hand side of Eq. (6.28) differs from the above by

$$\ll \sum_{k>n} kq^{-k}\left|\oint_{|t|=r}\frac{G(t)}{t^{k+1}}\right|, \quad r = q^{-\frac{1}{2}-\epsilon} < \frac{1}{\sqrt{q}} \tag{6.34}$$

where we take $\epsilon = \epsilon(n) > 0$ to satisfy

$$\epsilon = o(1), \quad \epsilon^{-1} = o(\log n). \tag{6.35}$$

To bound the integral in Eq. (6.34), we prove a pointwise bound on G. We first handle the case where D is not a constant (an element of $\mathbb{F}_q^\times$) times a square in $\mathbb{F}_q[u]$. To do that, (assuming none of the factors in Eq. (6.31) is zero) we write

$$\log|G(t)| = \sum_{\pi}\log\left|1 - \frac{\chi_F(\pi)t^{\deg(\pi)}}{1-t^{\deg(\pi)}}\right| \tag{6.36}$$

and using the bound $\log|1-z| = \frac{1}{2}\log|1-z|^2 \ll \log(1-z-\overline{z}+|z|^2)$ get

$$\sum_{\pi}\log\left(1 + \frac{(\chi_F^2(\pi)+2\chi_F(\pi))|t|^{2\deg(\pi)} - \chi_F(\pi)\left(t^{\deg(\pi)}+\overline{t^{\deg(\pi)}}\right)}{|1-t^{\deg(\pi)}|^2}\right).$$

Since $\log(1+x) \leq x$ for any real $x > -1$, and $|1-t^{\deg(\pi)}|^{-2} \ll 1$, the above is

$$\ll \sum_{\pi} r^{2\deg(\pi)} + \left|\sum_{\pi}\frac{\chi_F(\pi)t^{\deg(\pi)}}{|1-t^{\deg(\pi)}|^2}\right| \tag{6.37}$$

so summing separately over each degree we get at most

$$\sum_{\ell=1}^{\infty} q^\ell r^{2\ell} + \left|\sum_{\ell=1}^{\infty}\sum_{\deg(\pi)=\ell}\frac{\chi_F(\pi)t^\ell}{|1-t^\ell|^2}\right| = \frac{1}{1-qr^2} + \left|\sum_{\ell=1}^{\infty}\sum_{\deg(\pi)=\ell}\frac{\chi_F(\pi)t^\ell}{|1-t^\ell|^2}\right|. \tag{6.38}$$

Using the triangle inequality, and the bound $|1-t^\ell|^{-2} \ll 1$, we arrive at

$$\sum_{\ell=1}^{\infty} q^\ell r^{2\ell} + \sum_{\ell=1}^{\infty} r^\ell\left|\sum_{\deg(\pi)=\ell}\chi_F(\pi)\right|. \tag{6.39}$$

For the second sum we use a trivial bound for $\ell \leq 2\log_q \deg(D)$, and invoke Weil's Riemann Hypothesis (see [Rud10, (2.5)]) for all other ℓ to get

$$\ll \frac{1}{1-qr^2} + \sum_{\ell \leq 2\log_q \deg(D)} r^\ell q^\ell + \sum_{\ell > 2\log_q \deg(D)} \deg(D) r^\ell q^{\frac{\ell}{2}}. \tag{6.40}$$

Evaluating the geometric series, and using the bound $(1-q^{-2\epsilon})^{-1} \ll \epsilon^{-1}$ we finally get

$$\log|G(t)| \ll \epsilon^{-1}\deg(D)^{1-2\epsilon}. \tag{6.41}$$

It follows from our assumption that $\deg(D) \ll n$, Eq. (6.34) and Eq. (6.41) that our error term is

$$e^{O(\deg(D)^{1-2\epsilon}\epsilon^{-1})}\sum_{k>n} kq^{-k}r^{-k} \ll q^{O(n^{1-2\epsilon}\epsilon^{-1})} nq^{-\frac{n}{2}+\epsilon n}. \tag{6.42}$$

In view of Eq. (6.35) the above is $\ll q^{-\frac{n}{2}+o(n)}$ as required.

Now we handle the case where $D = \lambda D_0^2$, with $\lambda \in \mathbb{F}_q$ and $D_0 \in \mathbb{F}_q[u]$. Since F is irreducible by assumption, we get that $-\lambda \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$ and $D_0 \neq 0$ so

$$L(t,\chi_F) = \frac{1}{1+qt}\prod_{\pi|D}(1-(-t)^{\deg(\pi)}). \tag{6.43}$$

Therefore, for any $t \in \mathbb{C}$ with $|t| \leq q^{-\frac{1}{2}}$ we have

$$|L(t,\chi_F)|^{-1} = (1+qt)\prod_{\pi|D}|1-(-t)^{\deg(\pi)}|^{-1} \ll \prod_{\pi|D}\frac{1}{1-|\pi|^{-\frac{1}{2}}} \ll |D|^\epsilon. \tag{6.44}$$

In order to obtain a pointwise bound for G in this case, we shall bound the Euler product in Eq. (6.32). Setting $r = |t|$ as in Eq. (6.34), we have

$$\prod_\pi \left|1 - \frac{t^{2\deg(\pi)}\chi_F(\pi)}{(1-t^{\deg(\pi)})(1-\chi_F(\pi)t^{\deg(\pi)})}\right| \leq \prod_\pi \left(1+\frac{r^{2\deg(\pi)}}{(1-r^{\deg(\pi)})^2}\right) =$$
$$\prod_\pi \left(1+\frac{2r^{3\deg(\pi)}}{1-r^{\deg(\pi)}}\right)\frac{1}{1-r^{2\deg(\pi)}} = \frac{1}{1-qr^2}\prod_\pi\left(1+\frac{2r^{3\deg(\pi)}}{1-r^{\deg(\pi)}}\right)$$

in which the final Euler product converges for $r < q^{-\frac{1}{3}}$ and is uniformly bounded for $r \leq q^{-1/2}$, so Eq. (6.32) defines a holomorphic function in this disc.

By Eq. (6.34) we have

$$\frac{1}{1-qr^2} = \frac{1}{1-q^{-2\epsilon}} \ll \epsilon^{-1} \tag{6.45}$$

so the error term is bounded by

$$\sum_{k>n} kq^{-k}\frac{\epsilon^{-1}}{r^{k+1}} = \epsilon^{-1}\sum_{k>n} kq^{(\epsilon-\frac{1}{2})(k+1)-1} \ll \epsilon^{-1}q^{-\frac{n}{2}+\epsilon n} \tag{6.46}$$

which is $\ll q^{-\frac{n}{2}+o(n)}$ in view of Eq. (6.35). □

7. Quadratic forms

We establish here analogs over $\mathbb{F}_q[u]$ of several facts mentioned in [Hoo63].

Proposition 7.1. *For every (binary) quadratic form*

$$Q(X,Y) = aX^2 + bXY + cY^2 \tag{7.1}$$

over $\mathbb{F}_q[u]$ there exists a unique symmetric 2×2 matrix K over $\mathbb{F}_q[u]$ with

$$Q(X,Y) = (X,Y)K(X,Y)^T. \tag{7.2}$$

Proof. For the existence of K as above, just note that

$$(X,Y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}(X,Y)^T = \left(aX + \frac{bY}{2}, \frac{bX}{2} + cY\right)(X,Y)^T = Q(X,Y).$$

For uniqueness, let K be a symmetric matrix satisfying Eq. (7.2). Then

$$K_{11} = (1,0)K(1,0)^T = Q(1,0), \; K_{22} = (0,1)K(0,1)^T = Q(0,1) \tag{7.3}$$

and since K is symmetric, we get from Eq. (7.2) that

$$\begin{aligned} 2K_{12} = K_{12} + K_{21} &= (1,1)K(1,1)^T - (1,0)K(1,0)^T - (0,1)K(0,1)^T \\ &= Q(1,1) - Q(1,0) - Q(0,1) \end{aligned}$$

so K is indeed uniquely determined by Q. □

Definition 7.2. Keep the notation of the above proposition. We say that the symmetric 2×2 matrix K is the matrix corresponding to the quadratic form Q, and define the discriminant D of Q to be the determinant

$$D = \det(K) = ac - \frac{b^2}{4}. \tag{7.4}$$

In case the polynomial

$$F(T) = T^2 + D \in \mathbb{F}_q[u][T] \tag{7.5}$$

is reducible over $\mathbb{F}_q[u]$, that is, negative D is a square in $\mathbb{F}_q[u]$, we say that Q is degenerate, and otherwise we say that it is nondegenerate.

Remark 7.3. For a nondegenerate form $Q(X,Y) = aX^2 + bXY + cY^2$, the polynomial $a = Q(1,0)$ is nonzero. For if $a = 0$ then

$$-D = \frac{b^2}{4} - ac = \left(\frac{b}{2}\right)^2 - 0 \cdot c = \left(\frac{b}{2}\right)^2 \tag{7.6}$$

contrary to our assumption that Q is nondegenerate.

Definition 7.4. Let the group $\mathrm{SL}_2(\mathbb{F}_q[u])$ act from the right on row vectors in $\mathbb{F}_q[u]^2$ via the dual of the usual action by multiplication. This means that for a matrix of polynomials

$$M \in \mathrm{SL}_2(\mathbb{F}_q[u]), \; M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}, \; M_{11}M_{22} - M_{12}M_{21} = 1, \tag{7.7}$$

and $(x, y) \in \mathbb{F}_q[u]^2$, the action is given by

$$\begin{aligned}(x, y) \star M = (x, y)M^{-T} &= (x, y)\begin{pmatrix} M_{22} & -M_{21} \\ -M_{12} & M_{11}\end{pmatrix} \\ &= (M_{22}x - M_{12}y, -M_{21}x + M_{11}y).\end{aligned} \tag{7.8}$$

It is straightforward to check that the stabilizer of the vector $(1, 0)$ is

$$\{M \in \mathrm{SL}_2(\mathbb{F}_q[u]) : (1, 0)M^{-T} = (1, 0)\} = \left\{\begin{pmatrix} 1 & g \\ 0 & 1\end{pmatrix} : g \in \mathbb{F}_q[u]\right\}. \tag{7.9}$$

Notation 7.5. A vector $(x, y) \in \mathbb{F}_q[u]^2$ is called primitive if $\gcd(x, y) = 1$, or equivalently, if the ideal of $\mathbb{F}_q[u]$ generated by x and y contains 1. For such a vector, we denote by $\overline{x} \in \mathbb{F}_q[u]$ the polynomial of least degree for which

$$\overline{x}x = 1 \mod y, \tag{7.10}$$

and let $y_x \in \mathbb{F}_q[u]$ be the polynomial of least degree satisfying

$$\overline{x}x - y_x y = 1. \tag{7.11}$$

Put

$$M_{(x,y)} = \begin{pmatrix} x & y_x \\ y & \overline{x}\end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q[u]) \tag{7.12}$$

and note that

$$(1, 0) = (x, y)M_{(x,y)}^{-T}. \tag{7.13}$$

In particular, the primitive vectors form an orbit under the action of $\mathrm{SL}_2(\mathbb{F}_q[u])$.

Definition 7.6. The group $\mathrm{SL}_2(\mathbb{F}_q[u])$ also acts from the right on quadratic forms by

$$Q(X, Y) \star M = Q((X, Y)M^T) = Q(M_{11}X + M_{12}Y, M_{21}X + M_{22}Y). \tag{7.14}$$

We say that two quadratic forms are equivalent if they belong to the same orbit in this action.

For instance, if

$$Q(X, Y) = aX^2 + bXY + cY^2, \quad M = \begin{pmatrix} 1 & g \\ 0 & 1\end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q[u]) \tag{7.15}$$

then we have

$$\begin{aligned}Q((X, Y)M^T) = Q(X + gY, Y) &= a(X + gY)^2 + b(X + gY)Y + cY^2 \\ &= aX^2 + (b + 2ag)XY + (ag^2 + bg + c)Y^2.\end{aligned} \tag{7.16}$$

We show that equivalent quadratic forms have the same discriminant.

Proposition 7.7. *Let Q be a quadratic form, and let $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$. Then the discriminant of the quadratic form $Q'(X, Y) = Q((X, Y)M^T)$ equals the discriminant of Q.*

Proof. For the symmetric 2×2 matrix K corresponding to Q in Definition 7.2 we have

$$Q'(X,Y) = Q((X,Y)M^T) = (X,Y)M^TKM(X,Y)^T \tag{7.17}$$

so Q' and M^TKM satisfy the assumptions of Proposition 7.1 as the latter matrix is symmetric. We conclude that M^TKM is the matrix corresponding to Q', so the discriminant of Q' is

$$\det(M^TKM) = \det(M^T)\det(K)\det(M) = 1\cdot\det(K)\cdot 1 = \det(K) \tag{7.18}$$

which is the discriminant of Q. □

Definition 7.8. A representation of a polynomial $A \in \mathbb{F}_q[u]$ by a quadratic form is an ordered pair $(Q,(x,y))$ where $(x,y)\in\mathbb{F}_q[u]^2$, Q is a quadratic form, and $Q(x,y) = A$. The representation is said to be primitive if (x,y) is primitive and Q is nondegenerate. One checks that the actions defined in Definition 7.4 and Definition 7.6 combine to a coordinatewise action of $\mathrm{SL}_2(\mathbb{F}_q[u])$ from the right on (primitive) representations of A. We call two representations equivalent if they belong to the same orbit in this action.

Next we show that the action of $\mathrm{SL}_2(\mathbb{F}_q[u])$ on primitive representations is free, namely that the stabilizer of any primitive representation is trivial.

Proposition 7.9. *Let Q be a nondegenerate quadratic form over $\mathbb{F}_q[u]$, and let $v\in\mathbb{F}_q[u]^2$ be a primitive vector. Then the only matrix $M\in\mathrm{SL}_2(\mathbb{F}_q[u])$ that satisfies*

$$Q((X,Y)M^T) = Q(X,Y), \quad vM^{-T} = v, \tag{7.19}$$

is the identity matrix.

Proof. Write $Q(X,Y) = aX^2+bXY+cY^2$, and suppose first that $v = (1,0)$. In this case, we know that $(1,0)M^{-T} = (1,0)$ so by Eq. (7.9), there exists a polynomial $g\in\mathbb{F}_q[u]$ such that

$$M = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}. \tag{7.20}$$

Using our assumption that M stabilizes Q and Eq. (7.16) we get

$$\begin{aligned} aX^2+bXY+cY^2 &= Q(X,Y) = Q((X,Y)M^T) \\ &= aX^2+(b+2ag)XY+(ag^2+bg+c)Y^2. \end{aligned} \tag{7.21}$$

Since Q is nondegenerate, we get from Definition 7.2 that $4ac-b^2\neq 0$. It follows that either $a\neq 0$ or $b\neq 0$ (or both). In case $a\neq 0$, from comparing the coefficients of XY above, we get that $2ag = 0$ so $g = 0$. If $a = 0$ then $b\neq 0$, so from equating the coefficients of Y^2 above, we deduce that $bg = 0$ hence $g = 0$. We have thus shown that M is indeed the identity matrix in case $v = (1,0)$.

Assume now that v is an arbitrary primitive vector. In Eq. (7.12) we have written a matrix $M_v\in\mathrm{SL}_2(\mathbb{F}_q[u])$ such that $v = (1,0)M_v^T$. We set

$$Q'(X,Y) = Q((X,Y)M_v^T), \tag{7.22}$$

infer from Proposition 7.7 that Q' is a nondegenerate quadratic form, and note that $Q(X,Y) = Q'((X,Y)M_v^{-T})$. Now if $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$ is a matrix satisfying Eq. (7.19) then

$$Q'((X,Y)M^T M_v^{-T}) = Q'((X,Y)M_v^{-T}), \quad (1,0)M_v^T M^{-T} = (1,0)M_v^T$$

so

$$Q'((X,Y)(M_v^{-1}MM_v)^T) = Q'((X,Y)), \quad (1,0)\left(M_v^{-1}MM_v\right)^{-T} = (1,0).$$

From the previous special case where the primitive vector was $(1,0)$ we conclude that $M_v^{-1}MM_v$ is the identity, so M is the identity as well. □

Definition 7.10. If Q is a nondegenerate quadratic form of discriminant D as in Definition 7.2, and $(Q,(1,0))$ represents a polynomial A, then we can write

$$Q(X,Y) = AX^2 + bXY + cY^2 \tag{7.23}$$

so from the definition of the discriminant in Eq. (7.4) we get

$$\left(\frac{b}{2}\right)^2 + D = \frac{b^2}{4} + Ac - \frac{b^2}{4} = Ac \equiv 0 \mod A. \tag{7.24}$$

We say that $f = \frac{b}{2} \in \mathbb{F}_q[u]/(A)$ is the solution of the equation

$$F(T) = T^2 + D \equiv 0 \mod A \tag{7.25}$$

associated to the primitive representation $(Q,(1,0))$ of A. Note that $A \neq 0$ by Remark 7.3.

Proposition 7.11. *Let $(Q,(1,0))$ and $(Q',(1,0))$ be representations of a polynomial $A \in \mathbb{F}_q[u]$ by nondegenerate quadratic forms of discriminant D. Then the solutions to Eq. (7.25) associated to the representations $(Q,(1,0))$ and $(Q',(1,0))$ coincide if and only if these representations are equivalent.*

Proof. Suppose first that the representations $(Q,(1,0))$ and $(Q',(1,0))$ are equivalent. By the definitions in Eq. (7.8) and Eq. (7.14), equivalence means that there exists a matrix $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$ such that

$$(1,0)M^{-T} = (1,0), \quad Q'(X,Y) = Q((X,Y)M^T). \tag{7.26}$$

We have checked in Eq. (7.9) that the first equality above implies

$$M = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \tag{7.27}$$

for some $g \in \mathbb{F}_q[u]$.

Since $Q(1,0) = A$, we can write

$$Q(X,Y) = AX^2 + bXY + cY^2 \tag{7.28}$$

and get from the second equality in Eq. (7.26) and Eq. (7.16) that

$$Q'(X,Y) = Q((X,Y)M^T) = AX^2 + (b+2gA)XY + (Ag^2+bg+c)Y^2 \tag{7.29}$$

so the coefficient of XY in Q' is

$$2gA + b \equiv b \mod A. \tag{7.30}$$

Hence the solution of Eq. (7.25) associated to $(Q', (1,0))$ via Eq. (7.24) is $f = \frac{b}{2}$, which is also the solution associated to $(Q, (1,0))$.

Suppose now that the representations $(Q, (1,0))$ and $(Q', (1,0))$ of A give rise to the same solution of Eq. (7.25). We can therefore write

$$Q(X,Y) = AX^2 + bXY + cY^2, \quad Q'(X,Y) = AX^2 + b'XY + c'Y^2 \tag{7.31}$$

with b' congruent to b mod A. Since Q and Q' are of discriminant D, using Definition 7.2 we see that $4Ac = b^2 + 4D$ and that $4Ac' = b'^2 + 4D$. By Remark 7.3, A is nonzero so we can rewrite our forms as

$$Q(X,Y) = AX^2 + bXY + \frac{b^2+4D}{4A}Y^2, \; Q'(X,Y) = AX^2 + b'XY + \frac{b'^2+4D}{4A}Y^2. \tag{7.32}$$

In order to exhibit the equivalence of our representations, we take

$$M = \begin{pmatrix} 1 & \frac{b'-b}{2A} \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q[u]) \tag{7.33}$$

and note that $(1,0) = (1,0)M^{-T}$. Using Eq. (7.32) and Eq. (7.16) we get

$$Q((X,Y)M^T) =$$

$$AX^2 + \left(b + 2A \cdot \frac{b'-b}{2A}\right) XY + \left(A\left(\frac{b'-b}{2A}\right)^2 + b \cdot \frac{b'-b}{2A} + \frac{b^2+4D}{4A}\right) Y^2 =$$

$$AX^2 + b'XY + \left(\frac{b'^2 - 2bb' + b^2}{4A} + \frac{2bb' - 2b^2}{4A} + \frac{b^2+4D}{4A}\right) Y^2 =$$

$$AX^2 + b'XY + \left(\frac{b'^2+4D}{4A}\right) Y^2 = Q'(X,Y)$$

so our representations are indeed equivalent. □

Definition 7.12. To a primitive representation $(Q, (x,y))$ of a polynomial $A \in \mathbb{F}_q[u]$ by a quadratic form

$$Q(X,Y) = aX^2 + bXY + cY^2 \tag{7.34}$$

of discriminant D, using Notation 7.5 we associate the solution

$$f = ay_x x + \frac{b}{2}(\overline{x}x + y_x y) + c\overline{x}y \in \mathbb{F}_q[u]/(A) \tag{7.35}$$

of the congruence $T^2 \equiv -D \mod A$ from Eq. (7.25). Note that this agrees with our previous definition $f = \frac{b}{2}$ for the case $(x,y) = (1,0)$.

Now we check that Eq. (7.35) is indeed a solution for Eq. (7.25). We use Notation 7.5 to associate with $(Q,(x,y))$ the quadratic form

$$Q_{x,y}(X,Y) = Q\left((X,Y)M^T_{(x,y)}\right) = Q(xX + y_xY, yX + \overline{x}Y) \\ = a(xX + y_xY)^2 + b(xX + y_xY)(yX + \overline{x}Y) + c(yX + \overline{x}Y)^2 \tag{7.36}$$

and use Eq. (7.13) to conclude that $(Q,(x,y))$ is equivalent to $(Q_{x,y},(1,0))$. One readily checks that dividing the coefficient of XY above by 2 gives the right hand side of Eq. (7.35), so the latter is indeed a solution of Eq. (7.25). In other words, the solution of Eq. (7.25) associated to $(Q,(x,y))$ is the solution of Eq. (7.25) associated to the equivalent representation $(Q_{x,y},(1,0))$ in Definition 7.10. At last note that by Remark 7.3 we have

$$A = Q(x,y) = Q_{x,y}(1,0) \neq 0. \tag{7.37}$$

Corollary 7.13. *Primitive representations $(Q,(x,y))$ and $(Q',(x',y'))$ of a polynomial A by quadratic forms of discriminant D are equivalent if and only if their associated solutions to the equation $T^2 + D \equiv 0 \mod A$ coincide.*

Proof. The representations $(Q,(x,y))$ and $(Q',(x',y'))$ are equivalent if and only if $(Q_{x,y},(1,0))$ and $(Q'_{x',y'},(1,0))$ are equivalent. From Proposition 7.11 applied to $Q_{x,y}$ and $Q'_{x',y'}$, we get that $(Q_{x,y},(1,0))$ and $(Q'_{x',y'},(1,0))$ are equivalent if and only if they give rise to the same solution for the congruence $T^2 + D \equiv 0 \mod A$. Our corollary now follows because the solution associated to $(Q,(x,y))$ is the one associated to $(Q_{x,y},(1,0))$, and the solution associated to $(Q',(x',y'))$ is also associated to $(Q'_{x',y'},(1,0))$. □

Proposition 7.14. *Let $A \in \mathbb{F}_q[u]$ be a nonzero polynomial, and let $D \in \mathbb{F}_q[u]$ be a polynomial with $-D$ not a square. Then every solution $f \in \mathbb{F}_q[u]/(A)$ of*

$$T^2 + D \equiv 0 \mod A \tag{7.38}$$

arises from a primitive representation of A by a quadratic form of discriminant D.

Proof. We lift f to a polynomial in $\mathbb{F}_q[u]$, which by an abuse of notation, we continue to denote by f. Consider the quadratic form

$$Q(X,Y) = AX^2 + 2fXY + \frac{f^2 + D}{A}Y^2 \in \mathbb{F}_q[u][X,Y] \tag{7.39}$$

that satisfies $Q(1,0) = A$. By Definition 7.2, the discriminant of Q is

$$A \cdot \frac{f^2 + D}{A} - \frac{(2f)^2}{4} = f^2 + D - f^2 = D. \tag{7.40}$$

By Eq. (7.24), $f = \frac{2f}{2}$ is associated to the primitive representation $(Q,(1,0))$ of A, as required. □

Proposition 7.15. *As in Definition 7.12, let $(Q,(x,y))$ be a primitive representation of a polynomial $A \in \mathbb{F}_q[u]$ by a quadratic form*

$$Q(X,Y) = aX^2 + bXY + cY^2 \tag{7.41}$$

of discriminant D, and let

$$f = ay_x x + \frac{b}{2}(\overline{x}x + y_x y) + c\overline{x}y \in \mathbb{F}_q[u]/(A) \tag{7.42}$$

be the associated solution to the equation $T^2 + D \equiv 0 \mod A$. Suppose that $y \neq 0$. Then

$$e\left(\frac{hf}{A}\right) = e\left(\frac{h\overline{x}}{y}\right) \tag{7.43}$$

for any polynomial $h \in \mathbb{F}_q[u]$ satisfying

$$\deg(h) < \deg(A) - \deg(b) - 1 \tag{7.44}$$

and

$$\deg(h) < \deg(A) + \deg(y) - \deg(a) - \deg(x) - 1. \tag{7.45}$$

Proof. We have an equality of rational functions

$$\begin{gathered} \frac{c\overline{x}y^2 + ax(\overline{x}x-1) + \frac{b}{2}y(2\overline{x}x-1)}{yA} + \frac{ax+\frac{b}{2}y}{yA} = \\ \frac{\overline{x}(ax^2+bxy+cy^2)}{yA} = \frac{\overline{x}Q(x,y)}{yA} = \frac{\overline{x}A}{yA} = \frac{\overline{x}}{y}. \end{gathered} \tag{7.46}$$

By Eq. (7.11), we have $\overline{x}x - 1 = y_x y$ and thus $2\overline{x}x - 1 = \overline{x}x + y_x y$, so plugging these in the first term of Eq. (7.46) we get

$$\frac{c\overline{x}y^2 + axy_x y + \frac{b}{2}y(\overline{x}x + y_x y)}{yA} \equiv \frac{f}{A} \mod \mathbb{F}_q[u] \tag{7.47}$$

from the definition of the associated solution f in Eq. (7.42). We conclude from the above and Eq. (7.46) that

$$\frac{f}{A} + \frac{ax+\frac{b}{2}y}{yA} \equiv \frac{\overline{x}}{y} \mod \mathbb{F}_q[u]. \tag{7.48}$$

Multiplying the above by a polynomial h and exponentiating, we obtain

$$e\left(\frac{h\overline{x}}{y}\right) = e\left(\frac{hf}{A}\right) e\left(\frac{hax+\frac{b}{2}hy}{yA}\right). \tag{7.49}$$

The second factor in the right hand side above equals 1 provided

$$\deg\left(hax + \frac{b}{2}hy\right) < \deg(yA) - 1. \tag{7.50}$$

The latter holds in case the two inequalities

$$\deg(h) < \deg(A) + \deg(y) - \deg(a) - \deg(x) - 1, \ \deg(h) < \deg(A) - \deg(b) - 1$$

are satisfied. □

Definition 7.16. Let $D \in \mathbb{F}_q[u]$ be a polynomial for which

$$F(T) = T^2 + D \in \mathbb{F}_q(u)[T] \tag{7.51}$$

is irreducible over $\mathbb{F}_q(u)$, that is $-D$ is not a square of a polynomial. We say that D is indefinite if the infinite place of $\mathbb{F}_q(u)$ splits in the splitting field of F. By [Ros02, Proposition 14.6], this is equivalent to the degree of D being even and the leading coefficient of $-D$ being a square in $\mathbb{F}_q^\times$. Otherwise (if the infinite place of $\mathbb{F}_q(u)$ is ramified or inert in the splitting field of F) we say that D is definite. A nondegenerate quadratic form is called definite (respectively, indefinite) if its discriminant is definite (respectively, indefinite).

7.1. Definite quadratic forms.

Definition 7.17. We say that a definite quadratic form

$$Q(X, Y) = aX^2 + bXY + cY^2 \in \mathbb{F}_q[u][X, Y] \tag{7.52}$$

is standard if $\deg c \geq \deg a > \deg b$.

Remark 7.18. For the discriminant D of a standard Q we have

$$\deg(a) + \deg(c) = \deg(D). \tag{7.53}$$

Indeed, otherwise $\deg(ac) = \deg(a) + \deg(c) \neq \deg(D)$, and thus

$$\begin{aligned} 2\deg(b) &= \deg(b^2) = \deg(4ac - 4D) = \max\{\deg(ac), \deg(D)\} \\ &\geq \deg(ac) = \deg(a) + \deg(c) > \deg(b) + \deg(b) = 2\deg(b), \end{aligned} \tag{7.54}$$

a contradiction. We infer that

$$\deg(a) = \frac{\deg(a) + \deg(a)}{2} \leq \frac{\deg(a) + \deg(c)}{2} = \frac{\deg(D)}{2}. \tag{7.55}$$

Proposition 7.19. *For a standard definite quadratic form, and $x, y \in \mathbb{F}_q[u]$ we have*

$$\deg(Q(x, y)) = \max(\deg(a) + 2\deg(x), \deg(c) + 2\deg(y)) > \deg(bxy).$$

Proof. We have

$$\deg(ax^2) = \deg(a) + 2\deg(x), \quad \deg(cy^2) = \deg(c) + 2\deg(y), \tag{7.56}$$

so since $\deg(c), \deg(a) > \deg(b)$ by Definition 7.17, we get

$$\begin{aligned} \deg(bxy) = \deg(b) + \deg(x) + \deg(y) &< \frac{\deg(a) + \deg(c)}{2} + \deg(x) + \deg(y) \\ &= \frac{\deg(ax^2) + \deg(cy^2)}{2} \leq \max(\deg(ax^2), \deg(cy^2)). \end{aligned} \tag{7.57}$$

Suppose toward a contradiction that the leading terms of ax^2 and $-cy^2$ are equal. Then the leading terms of a and $-c$ are equal up to multiplication by the square of a monomial, so the leading term of $-ac$ is a square.

Since $\deg(ac) > \deg(b^2)$, we conclude that the leading term of the negated discriminant

$$-D = \frac{b^2}{4} - ac \tag{7.58}$$

of Q is a square, which contradicts the assumption that Q is definite.

We infer that the leading terms of ax^2 and cy^2 do not cancel each other out, so Eq. (7.57) implies that $\deg(bxy) < \deg(ax^2 + cy^2)$ and thus the desired statement. □

Definition 7.20. We say that a primitive vector $(x, y) \in \mathbb{F}_q[u]^2$ is a short vector of a definite quadratic form Q if

$$\deg(Q(x, y)) = \min\{\deg(Q(v)) \mid v \in \mathbb{F}_q[u]^2,\ v \text{ is primitive}\}. \tag{7.59}$$

By Eq. (7.37), the degrees of polynomials primitively represented by Q form a (nonempty) subset of the nonnegative integers. Such a subset necessarily has a least element, so Q admits short vectors.

Proposition 7.21. *Let $Q(X, Y) = aX^2 + bXY + cY^2$ be a standard definite quadratic form over $\mathbb{F}_q[u]$. Then the short vectors of Q are*

$$\begin{cases} \mathbb{F}_q^\times \times \{0\} & \deg(a) < \deg(c) \\ \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0)\} & \deg(a) = \deg(c). \end{cases} \tag{7.60}$$

Proof. We first determine the minimum in the right hand side of Eq. (7.59). Invoke Proposition 7.19, and note that the minimum value of

$$\deg(Q(x, y)) = \max(\deg(a) + 2\deg(x), \deg(c) + 2\deg(y)) \tag{7.61}$$

over all primitive vectors $(x, y) \in \mathbb{F}_q[u]^2$ is attained (at least) whenever $\deg(x)$ and $\deg(y)$ are as small as possible, subject to $\gcd(x, y) = 1$. That is, the minimum occurs (at least) in case

$$\{\deg(x), \deg(y)\} = \{0, -\infty\}, \tag{7.62}$$

so this minimum is $\min(\deg(a), \deg(c))$ which is $\deg(a)$ since the form Q is standard.

To determine all short vectors, let $(x, y) \in \mathbb{F}_q[u]^2$ be a primitive vector. If $\deg(c) > \deg(a)$, then we have

$$\max(\deg(a) + 2\deg(x), \deg(c) + 2\deg(y)) = \deg(a) \tag{7.63}$$

if and only if $y = 0$ and x is a nonzero constant polynomial. Otherwise, since Q is standard we have $\deg(c) = \deg(a)$ so Eq. (7.63) is satisfied if and only if x and y are both constant polynomials (but not both zero). □

The following proposition shows that the action of $\mathrm{SL}_2(\mathbb{F}_q[u])$ on representations restricts to an action on representations by short vectors of definite quadratic forms.

Proposition 7.22. *Let v be a short vector of a definite quadratic form Q over $\mathbb{F}_q[u]$, and let $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$. Then the primitive vector $v' = vM^{-T}$ is a short vector of the definite quadratic form $Q'(X, Y) = Q((X, Y)M^T)$.*

Proof. The form Q' is definite since its discriminant is the discriminant of Q by Proposition 7.7. Since $Q(X,Y) = Q'((X,Y)M^{-T})$, and v is a short vector of Q, for any primitive vector $v_0 \in \mathbb{F}_q[u]^2$ we have

$$\begin{aligned} \deg(Q'(v_0)) &= \deg(Q(v_0 M^T)) \geq \deg(Q(v)) \\ &= \deg(Q'(vM^{-T})) = \deg(Q'(v')) \end{aligned} \tag{7.64}$$

so v' is indeed a short vector of Q'. □

Definition 7.23. Let Q be a definite quadratic form over $\mathbb{F}_q[u]$, and let v be a short vector of Q. A standardizing matrix of Q at v is a matrix $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$ for which $vM^{-T} = (1,0)$ and $Q((X,Y)M^T)$ is a standard definite quadratic form.

Proposition 7.24. *There exists a unique standardizing matrix of Q at v.*

Proof. We start by proving existence. By Definition 7.20, the vector v is primitive, so as in Eq. (7.13) there exists a matrix $M_v \in \mathrm{SL}_2(\mathbb{F}_q[u])$ with $vM_v^{-T} = (1,0)$. By Proposition 7.22, the vector $(1,0)$ is then a short vector of the definite quadratic form

$$Q'(X,Y) = Q((X,Y)M_v^T) = aX^2 + bXY + cY^2. \tag{7.65}$$

By Remark 7.3, a is nonzero so division with remainder (Euclidean division) provides us with a polynomial $g \in \mathbb{F}_q[u]$ for which $\deg(b-ag) < \deg(a)$. Setting

$$N = \begin{pmatrix} 1 & -\frac{g}{2} \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q[u]) \tag{7.66}$$

and applying Eq. (7.16), we get the quadratic form

$$S(X,Y) = Q'((X,Y)N^T) = aX^2 + (b-ag)XY + c_0Y^2 \tag{7.67}$$

for some $c_0 \in \mathbb{F}_q[u]$.

Applying Proposition 7.22 again, we find that the vector $(1,0) = (1,0)N^{-T}$ is a short vector of the definite quadratic form S. Therefore

$$\deg(c_0) = \deg(S(0,1)) \geq \deg(S(1,0)) = \deg(a) \tag{7.68}$$

so S is standard by Definition 7.17. The existence part of our proposition then follows by taking $M = M_vN$ as

$$vM^{-T} = v(M_vN)^{-T} = vM_v^{-T}N^{-T} = (1,0)N^{-T} = (1,0) \tag{7.69}$$

and

$$Q((X,Y)M^T) = Q((X,Y)N^TM_v^T) = Q'((X,Y)N^T) = S(X,Y). \tag{7.70}$$

To demonstrate uniqueness, let $M_1, M_2 \in \mathrm{SL}_2(\mathbb{F}_q[u])$ be standardizing matrices of Q at v. Then we have $vM_1^{-T} = (1,0) = vM_2^{-T}$ so

$$(1,0)(M_1^{-1}M_2)^{-T} = (1,0) \tag{7.71}$$

and the quadratic forms

$$S_1(X,Y) = Q((X,Y)M_1^T) = aX^2 + bXY + cY^2, \ S_2(X,Y) = Q((X,Y)M_2^T) \tag{7.72}$$

are standard definite. From Eq. (7.71) and Eq. (7.9) we get that

$$M_1^{-1}M_2 = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \tag{7.73}$$

for some $g \in \mathbb{F}_q[u]$, so from Eq. (7.72) and Eq. (7.16) we get that

$$\begin{aligned} S_2(X,Y) &= Q((X,Y)M_2^T) = S_1((X,Y)M_2^T M_1^{-T}) = S_1((X,Y)(M_1^{-1}M_2)^T) \\ &= aX^2 + (b+2ag)XY + (ag^2+bg+c)Y^2. \end{aligned}$$

Suppose toward a contradiction that $g \neq 0$. As the form S_1 is standard definite we know that $\deg(a) > \deg(b)$, so since S_2 is also standard definite, we get from the above that

$$\deg(a) > \deg(b+2ag) = \deg(2ag) \geq \deg(a) \tag{7.74}$$

which is an absurdity. We conclude that $g = 0$ and thus $M_1^{-1}M_2$ is the identity in view of Eq. (7.73), so $M_1 = M_2$ as required. □

Definition 7.25. Let Q be a definite quadratic form, let v be a short vector of Q, let M be the standardizing matrix of Q at v, and let $w \in \mathbb{F}_q[u]^2$ be a primitive vector. We say that the standard quadratic form $Q((X,Y)M^T)$ is the standardization of Q at v, and that the representation

$$(Q((X,Y)M^T), wM^{-T}) \tag{7.75}$$

is the standardization at v of the representation (Q,w). A primitive representation (S,w) by a definite quadratic form is called standard if S is standard.

Theorem 7.26. *Let (Q,w) be a primitive representation of a polynomial A by a quadratic form Q of definite discriminant D. Then the function that maps a short vector v of Q to the standardization of (Q,w) at v is a bijection between the set of short vectors of Q and the set of those standard representations of A that are equivalent to (Q,w).*

Proof. To show that our function is injective, let v_1, v_2 be short vectors of Q, let $M_1, M_2 \in \mathrm{SL}_2(\mathbb{F}_q[u])$ be the standardizing matrices of Q at v_1 and v_2 respectively, and suppose that the standardization of (Q,w) at v_1 coincides with the standardization of (Q,w) at v_2, namely

$$wM_1^{-T} = wM_2^{-T}, \quad Q((X,Y)M_1^T) = Q((X,Y)M_2^T). \tag{7.76}$$

We can rewrite the above as

$$w = w(M_2M_1^{-1})^{-T}, \quad Q(X,Y) = Q((X,Y)(M_2M_1^{-1})^T) \tag{7.77}$$

so from the freeness of the action of $\mathrm{SL}_2(\mathbb{F}_q[u])$ on primitive representations established in Proposition 7.9, we conclude that $M_2 M_1^{-1}$ is the identity matrix. We therefore have $M_1 = M_2$ and thus

$$v_1 = (1,0)M_1^T = (1,0)M_2^T = v_2 \tag{7.78}$$

so injectivity is proven.

To obtain surjectivity, let (S, z) be a standard representation of A which is equivalent to (Q, w). We can therefore find a matrix $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$ with

$$S((X,Y)M^T) = Q(X,Y), \quad zM^{-T} = w. \tag{7.79}$$

The qudratic form S is standard, so by Proposition 7.21, the vector $(1, 0)$ is a short vector of S. We conclude from Proposition 7.22 that $v = (1, 0)M^{-T}$ is a short vector of Q, hence M^{-1} is the standardizing matrix of Q at v, and (S, z) is the standardization of (Q, w) at v. □

Corollary 7.27. *Let $D \in \mathbb{F}_q[u]$ be definite. Consider the function*

$$(aX^2 + bXY + cY^2, (x, y)) \mapsto (ax^2 + bxy + cy^2, ay_x x + \frac{b}{2}(\overline{x}x + y_x y) + c\overline{x}y)$$

which maps a standard representation (S, w) by a quadratic form of discriminant D to the represented polynomial $A = S(w)$ and the associated solution f to the congruence $T^2 + D \equiv 0 \mod A$. Then the image of this function is

$$\{(A, f) : A \in \mathbb{F}_q[u] \setminus \{0\},\ f \in \mathbb{F}_q[u]/(A),\ f^2 + D \equiv 0 \mod A\}. \tag{7.80}$$

Moreover, the preimage of any (f, A) as above is either a set of $q - 1$ representations, all satisfying $\deg(a) < \deg(c)$*, or a set of $q^2 - 1$ representations, all satisfying* $\deg(a) = \deg(c)$.

Proof. The fact that the image of our function is contained in Eq. (7.80) is immediate from Definition 7.12. Taking (A, f) from the set in Eq. (7.80), Proposition 7.14 provides us with a primitive representation (Q, w) of A by a quadratic form of discriminant D such that f is the associated solution to this representation. Standardizing (Q, w) at a short vector of Q, we obtain a standard representation

$$(S(X, Y) = aX^2 + bXY + cY^2, w') \tag{7.81}$$

of A, which is equivalent to (Q, w). It follows from Corollary 7.13 that f is also the solution associated to (S, w'), so our function maps (S, w') to (A, f), hence its image is indeed given by Eq. (7.80).

By the other implication in Corollary 7.13, the preimage of (A, f) under our function consists of all those standard representations of A that are equivalent to (S, w'). These representation are in bijection with the short vectors of S in view of Theorem 7.26. Since S is a standard definite quadratic form, it follows from Proposition 7.21 that this set has $q-1$ elements in case $\deg(a) < \deg(c)$ and $q^2 - 1$ elements in case $\deg(a) = \deg(c)$.

Now if

$$(S'(X, Y) = a'X^2 + b'XY + c'Y^2, w'') \tag{7.82}$$

is any other representation (of A) in the preimage of (A, f), then it is equivalent to (S, w'). It follows from Proposition 7.22 that the number of short vectors of (S', w'') equals the number of short vectors of (S, w'), so since $q-1 \neq q^2-1$, we conclude from Proposition 7.21 that $\deg(a') < \deg(c')$ in case $\deg(a) < \deg(c)$ and that $\deg(a') = \deg(c')$ if $\deg(a) = \deg(c)$. □

Notation 7.28. For a definite polynomial $D \in \mathbb{F}_q[u]$ we denote by

$$S(D) = \left\{(a,b,c) \in \mathbb{F}_q[u]^3 : \deg(c) \geq \deg(a) > \deg(b),\ ac - \frac{b^2}{4} = D\right\}$$

the set of all standard quadratic forms of discriminant D.

Corollary 7.29. *For every $\epsilon > 0$ we have $|S(D)| \ll |D|^{\frac{1}{2}+\epsilon}$.*

Proof. For $i \in \{0,1\}$ set

$$S(D;i) = \{(a,b,c) \in S(D) : \deg(c) \equiv i \mod 2\} \tag{7.83}$$

and note that $S(D) = S(D;0) \cup S(D;1)$ so it suffices to show that

$$|S(D;i)| \ll |D|^{\frac{1}{2}+\epsilon}, \quad i \in \{0,1\}. \tag{7.84}$$

Fix $i \in \{0,1\}$, let $(a,b,c) \in S(D;i)$, and let $n \geq \deg(D)$ be an integer with

$$n \equiv i \text{ mod } 2. \tag{7.85}$$

It follows from Proposition 7.19 that for coprime polynomials $x, y \in \mathbb{F}_q[u]$ with

$$\deg(x) < \frac{n - \deg(a)}{2}, \quad \deg(y) = \frac{n - \deg(c)}{2}, \tag{7.86}$$

the polynomial $A = ax^2 + bxy + cy^2$ has degree n. From the count of pairs of coprime polynomials (x,y) in [ABSR15, Proof of Lemma 7.3], and Remark 7.18, it follows that the number of standard representations of degree n polynomials by quadratic forms of discriminant D is

$$\gg |S(D;i)| q^{\frac{n-\deg(a)}{2} + \frac{n-\deg(c)}{2}} = |S(D;i)| q^{n - \frac{\deg(D)}{2}}. \tag{7.87}$$

On the other hand, using Notation 6.3, this number is

$$\ll \sum_{A \in \mathcal{M}_n} \rho(A;F) \tag{7.88}$$

in view of Corollary 7.27. By Proposition 6.5 the above is $\ll q^n |D|^\epsilon$ so

$$|S(D;i)| \ll q^{\frac{\deg(D)}{2}} |D|^\epsilon = |D|^{\frac{1}{2}+\epsilon}$$

as desired. □

Remark 7.30. Keeping track of all the constants in the proofs of Corollary 7.29 and Proposition 6.5 would give a precise estimate for the number of standard quadratic forms, weighted by the inverse of their number of short vectors, in terms of a special value of the L-function. This would be an analogue of a classical proof of the class number formula, though we have here avoided the relationship between quadratic forms and ideal classes.

7.2. **Indefinite quadratic forms.**

Definition 7.31. We say that a primitive representation $(Q,(x,y))$ of a polynomial $A \in \mathbb{F}_q[u]$ by a quadratic form $Q(X,Y) = aX^2 + bXY + cY^2$ of indefinite discriminant D is standard if there exists a nonnegative integer s such that

$$\deg(a) \leq \frac{\deg(D)}{2} - s, \quad \deg(b) \leq \frac{\deg(D)}{2}, \quad \deg(c) \leq \frac{\deg(D)}{2} + s \tag{7.89}$$

and

$$\deg(x) \leq \frac{\deg(A)}{2} - \frac{\deg(D)}{4} + \frac{s}{2}, \quad \deg(y) \leq \frac{\deg(A)}{2} - \frac{\deg(D)}{4} - \frac{s}{2}. \tag{7.90}$$

Define the weight of a standard representation as above to be

$$\omega(Q,(x,y)) = \omega_s = \begin{cases} \frac{1}{q^3-q} & s = 0 \\ \frac{1}{(q-1)q^{s+1}} & s > 0. \end{cases} \tag{7.91}$$

We show that the weight is well-defined.

Proposition 7.32. *At least one of the inequalities in Eq. (7.89) is an equality, and at least one of the inequalities in Eq. (7.90) is an equality, so the integer s is uniquely determined by the standard representation $(Q,(x,y))$ of the polynomial A and satisfies*

$$s \equiv \frac{\deg(D)}{2} - \deg(A) \mod 2, \quad s \leq \frac{\deg(D)}{2}. \tag{7.92}$$

Proof. For the first claim note that if all inequalities in Eq. (7.89) were strict, we would have

$$\deg(D) = \deg\left(ac - \frac{b^2}{4}\right) \leq \max\{\deg(a) + \deg(c), 2\deg(b)\} < \deg(D).$$

which is contradictory.

We turn to the second claim. Since $Q(x,y) = A$ we have

$$\begin{aligned} \deg(A) &= \deg(Q(x,y)) = \deg(ax^2 + bxy + cy^2) \\ &\leq \max\{\deg(a) + 2\deg(x), \deg(b) + \deg(x) + \deg(y), \deg(c) + 2\deg(y)\}. \end{aligned} \tag{7.93}$$

We assume that the maximum is attained by the first element above. Then from Eq. (7.89) and Eq. (7.90) we get

$$\deg(a) + 2\deg(x) \leq \frac{\deg(D)}{2} - s + \deg(A) - \frac{\deg(D)}{2} + s = \deg(A) \tag{7.94}$$

so lest we arrive using Eq. (7.93) and the above at $\deg(A) < \deg(A)$, all our inequalities must be equalities. In particular

$$\deg(x) = \frac{\deg(A)}{2} - \frac{\deg(D)}{4} + \frac{s}{2}. \tag{7.95}$$

A calculation similar to that in Eq. (7.94), using Eq. (7.89) and Eq. (7.90), shows that in case the maximum in Eq. (7.93) is attained by the second element, Eq. (7.95) still holds. In case the maximum is attained by the third element in Eq. (7.93), we get that

$$\deg(y) = \frac{\deg(A)}{2} - \frac{\deg(D)}{4} - \frac{s}{2}. \tag{7.96}$$

In all three cases s is uniquely determined by $(Q,(x,y))$ and

$$\pm s + \deg(A) - \frac{\deg(D)}{2} \in \{2\deg(x), 2\deg(y)\} \subseteq 2\mathbb{Z} \tag{7.97}$$

for an appropriate choice of sign (namely either + or − depending on which of the three cases is being considered), so the congruence in Eq. (7.92) holds. At last note that

$$0 \leq \deg(a) \leq \frac{\deg(D)}{2} - s \tag{7.98}$$

in view of Eq. (7.89) and Remark 7.3, so the inequality in Eq. (7.92) holds. □

Definition 7.33. A valuation on $\mathbb{F}_q[u]^2$ is a function

$$v \colon \mathbb{F}_q[u]^2 \to \mathbb{Z} \cup \{-\infty\} \tag{7.99}$$

satisfying the following three conditions.

(1) For every $a, x, y \in \mathbb{F}_q[u]$ we have
$$v(ax, ay) = \deg(a) + v(x,y);$$

(2) For all $x_1, x_2, y_1, y_2 \in \mathbb{F}_q[u]$ we have
$$v(x_1 + x_2, y_1 + y_2) \leq \max\{v(x_1,y_1), v(x_2,y_2)\};$$

(3) The values of v on nonzero vectors are bounded below, i.e.
$$\inf_{(x,y)\neq(0,0)} v(x,y) > -\infty.$$

For v a valuation, let
$$m_v = \inf_{(x,y)\neq(0,0)} v(x,y).$$

Because m_v is the infimum of a set of integers bounded below, m_v is attained by some x, y.

Notation 7.34. For integers γ and δ one readily checks that the function

$$v_{\gamma,\delta}(x,y) = \max\{\gamma + \deg(x), \delta + \deg(y)\} \tag{7.100}$$

is a valuation. We say that a valuation v is standard if there exist integers $\gamma \leq \delta$ such that $v = v_{\gamma,\delta}$. In this case $m_v = v(1,0) = \gamma$.

Definition 7.35. We have an action of $\mathrm{SL}_2(\mathbb{F}_q[u])$ from the right on valuations by

$$(v \star M)(x,y) = v((x,y)M^T), \quad M \in \mathrm{SL}_2(\mathbb{F}_q[u]),\ x,y \in \mathbb{F}_q[u]. \tag{7.101}$$

Valuations in the same orbit will be called equivalent.

We calculate the order of the stabilizer of a standard valuation.

Proposition 7.36. *For a standard valuation $v_{\gamma,\delta}$ define the subgroup*

$$G_{\gamma,\delta} = \{M \in \mathrm{SL}_2(\mathbb{F}_q[u]) : v_{\gamma,\delta} \star M = v_{\gamma,\delta}\}. \tag{7.102}$$

Then

$$|G_{\gamma,\delta}| = \begin{cases} q^3 - q & \gamma = \delta \\ (q-1)q^{\delta-\gamma+1} & \gamma < \delta. \end{cases} \tag{7.103}$$

Proof. For each integer $s \geq 0$, we define a subgroup of $\mathrm{SL}_2(\mathbb{F}_q[u])$ by

$$H_s = \begin{cases} \mathrm{SL}_2(\mathbb{F}_q) & s = 0 \\ \left\{ \begin{pmatrix} \lambda & f \\ 0 & \lambda^{-1} \end{pmatrix} : \lambda \in \mathbb{F}_q^\times,\ f \in \mathbb{F}_q[u],\ \deg(f) \leq s \right\} & s \geq 1 \end{cases} \tag{7.104}$$

and claim that $G_{\gamma,\delta} = H_{\delta-\gamma}$. The asserted number of elements in $G_{\gamma,\delta}$ is immediate from this claim.

To prove one inclusion let $M \in G_{\gamma,\delta}$. We have

$$\begin{aligned} \gamma = v_{\gamma,\delta}(1,0) = v_{\gamma,\delta}((1,0)M^T) &= v_{\gamma,\delta}(M_{11}, M_{21}) \\ &= \max\{\gamma + \deg(M_{11}), \delta + \deg(M_{21})\}. \end{aligned} \tag{7.105}$$

We deduce that $\deg(M_{11})$ and $\deg(M_{21})$ are nonpositive, and in case $\gamma < \delta$ we can moreover say that $M_{21} = 0$. Similarly we have

$$\begin{aligned} \delta = v_{\gamma,\delta}(0,1) = v_{\gamma,\delta}((0,1)M^T) &= v_{\gamma,\delta}(M_{12}, M_{22}) \\ &= \max\{\gamma + \deg(M_{12}), \delta + \deg(M_{22})\} \end{aligned} \tag{7.106}$$

so $\deg(M_{22}) \leq 0$. In case $\gamma = \delta$ we infer that $\deg(M_{12}) \leq 0$ as well, while in case $\gamma < \delta$ we get that $\deg(M_{12}) \leq \delta - \gamma$. Since our matrices have determinant 1, this establishes the inclusion $G_{\gamma,\delta} \leq H_{\delta-\gamma}$ towards our claim.

For the other inclusion pick $M \in H_{\delta-\gamma}$. In case $\gamma = \delta$ this is a matrix of polynomials of nonpositive degree, so we have

$$\begin{aligned} v_{\gamma,\delta}((x,y)M^T) &= v_{\gamma,\delta}(M_{11}x + M_{12}y, M_{21}x + M_{22}y) \\ &= \gamma + \max\{\deg(M_{11}x + M_{12}y), \deg(M_{21}x + M_{22}y)\} \\ &\leq \gamma + \max\{\deg x, \deg y\} = v_{\gamma,\delta}(x,y). \end{aligned}$$

In case $\gamma < \delta$ we have

$$\deg(M_{11}) = 0,\ \deg(M_{12}) \leq \delta - \gamma,\ \deg(M_{21}) = -\infty,\ \deg(M_{22}) = 0 \tag{7.107}$$

so in this case we have the similar inequality

$$\begin{aligned} v_{\gamma,\delta}((x,y)M^T) &= v_{\gamma,\delta}(M_{11}x + M_{12}y, M_{21}x + M_{22}y) \\ &= \max\{\gamma + \deg(M_{11}x + M_{12}y), \delta + \deg(M_{21}x + M_{22}y)\} \\ &\leq \max\{\gamma + \max\{\deg(M_{11}x), \deg(M_{12}y)\}, \delta + \deg(y)\} \\ &\leq \max\{\gamma + \deg x, \delta + \deg y\} = v_{\gamma,\delta}(x,y). \end{aligned}$$

Since $M^{-1} \in H_{\delta-\gamma}$, we can plug M^{-1} in place of M and then plug $(x,y)M^T$ in place of (x,y), getting the inequality $v_{\gamma,\delta}(x,y) \leq v_{\gamma,\delta}((x,y)M^T)$. In conjunction with the above we have $v_{\gamma,\delta}((x,y)M^T) = v_{\gamma,\delta}(x,y)$ so M is in $G_{\gamma,\delta}$ and thus $H_{\delta-\gamma} \leq G_{\gamma,\delta}$. This concludes the proof that $G_{\gamma,\delta} = H_{\delta-\gamma}$. □

Proposition 7.37. *Every valuation v on $\mathbb{F}_q[u]^2$ is equivalent to a unique standard valuation.*

Proof. Let $(x,y) \neq (0,0)$ be a vector attaining the minimal valuation, namely

$$v(x,y) = m_v. \tag{7.108}$$

From Definition 7.33(1) and the minimality of (x,y) we get that

$$\begin{aligned} v(x,y) &= v\left(\gcd(x,y)\frac{x}{\gcd(x,y)}, \gcd(x,y)\frac{y}{\gcd(x,y)}\right) \\ &= \deg(\gcd(x,y)) + v\left(\frac{x}{\gcd(x,y)}, \frac{y}{\gcd(x,y)}\right) \\ &\geq \deg(\gcd(x,y)) + v(x,y) \end{aligned} \tag{7.109}$$

so $\deg(\gcd(x,y)) \leq 0$, hence x and y are coprime.

We can therefore take $M_{(x,y)} \in \mathrm{SL}_2(\mathbb{F}_q[u])$ to be the matrix from Eq. (7.12) satisfying $(1,0) = (x,y)M_{(x,y)}^{-T}$. For the valuation $v' = v \star M_{(x,y)}$ we then have

$$v'(z,w) = v((z,w)M_{(x,y)}^T) \geq m_v, \ (z,w) \neq (0,0), \quad v'(1,0) = v(x,y) = m_v$$

so $v'(1,0) = m_{v'}$.

Let $(z,1) \in \mathbb{F}_q[u]^2$ be a vector with

$$v'(z,1) = \min\{v'(x,1) : x \in \mathbb{F}_q[u]\}. \tag{7.110}$$

Let

$$M = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q[u]) \tag{7.111}$$

and note that $(1,0)M^T = (1,0)$. For the valuation $v'' = v' \star M$ we then have

$$v''(t,w) = v'((t,w)M^T) \geq m_{v'}, \ (t,w) \neq (0,0), \quad v''(1,0) = v'(1,0) = m_{v'}$$

so $v''(1,0) = m_{v''}$. Moreover

$$\begin{aligned} \min\{v''(x,1) : x \in \mathbb{F}_q[u]\} &= \min\{v'((x,1)M^T) : x \in \mathbb{F}_q[u]\} \\ &= \min\{v'(x+z,1) : x \in \mathbb{F}_q[u]\} \\ &= \min\{v'(x,1) : x \in \mathbb{F}_q[u]\} = v'(z,1) = v''(0,1). \end{aligned}$$

Set $\gamma = v''(1,0) = m_{v''}$ and $\delta = v''(0,1)$ so that $\gamma \leq \delta$. We claim that

$$v'' = v_{\gamma,\delta} \tag{7.112}$$

and thus v is equivalent to the standard valuation v''. To prove the claim, note first that by Definition 7.33(2) and Definition 7.33(1) we have

$$\begin{aligned} v''(x,y) &= v''(x(1,0)+y(0,1)) \leq \max\{v''(x(1,0)), v''(y(0,1))\} \\ &= \max\{\deg(x)+v''(1,0), \deg(y)+v''(0,1)\} = v_{\gamma,\delta}(x,y). \end{aligned} \tag{7.113}$$

Suppose toward a contradiction that there exists a vector (x,y) with

$$v''(x,y) < v_{\gamma,\delta}(x,y) \tag{7.114}$$

so in particular $(x,y) \neq (0,0)$. If $\gamma + \deg(x) > \delta + \deg(y)$ then we have

$$\begin{aligned} \gamma + \deg(x) = v''(1,0) + \deg(x) = v''(x(1,0)) &= v''((x,y)+(0,-y)) \\ &\leq \max\{v''(x,y), v''(-y(0,1))\} = \max\{v''(x,y), v''(0,1)+\deg(y)\} \\ &= \max\{v''(x,y), \delta+\deg(y)\} < \max\{v_{\gamma,\delta}(x,y), \gamma+\deg(x)\} = \gamma+\deg(x), \end{aligned}$$

a contradiction. Similarly, if $\delta + \deg y > \gamma + \deg x$, we have

$$\begin{aligned} \delta + \deg(y) = v''(y(0,1)) &\leq \max\{v''(x,y), v''(-x(1,0))\} \\ &= \max\{v''(x,y), \gamma+\deg(x)\} < \delta+\deg(y), \end{aligned}$$

a contradiction.

Finally, if $\gamma + \deg(x) = \delta + \deg(y)$, so in particular

$$\deg(x) = \delta - \gamma + \deg(y) \geq \deg(y) \geq 0, \tag{7.115}$$

we can use division with remainder in $\mathbb{F}_q[u]$ to write

$$x = wy + r, \quad \deg(r) < \deg(y) \leq \deg(x),\ \deg(w) = \deg(x) - \deg(y). \tag{7.116}$$

Since $v''(0,1) = \min\{v''(z,1) : z \in \mathbb{F}_q[u]\}$ we have

$$\begin{aligned} \delta + \deg(y) = v''(0,1) + \deg(y) \leq v''(w,1) + \deg(y) &= v''(wy,y) = v''(x-r,y) \\ &\leq \max\{v''(x,y), v''(-r(1,0))\} = \max\{v''(x,y), v'''(1,0)+\deg(r)\} \\ &= \max\{v''(x,y), \gamma+\deg(r)\} < \max\{v_{\gamma,\delta}(x,y), \gamma+\deg(x)\} = \delta+\deg(y), \end{aligned}$$

the final contradiction.

We have seen that v is equivalent to the standard valuation $v_{\gamma,\delta}$. To prove uniqueness, assume that v is also equivalent to some standard valuation $v_{\gamma',\delta'}$. We conclude that $v_{\gamma,\delta}$ is equivalent to $v_{\gamma',\delta'}$ so

$$\gamma = v_{\gamma,\delta}(1,0) = m_{v_{\gamma,\delta}} = m_{v_{\gamma',\delta'}} = v_{\gamma',\delta'}(1,0) = \gamma'. \tag{7.117}$$

Since the valuations $v_{\gamma,\delta}$ and $v_{\gamma',\delta'}$ belong to the same orbit under the action of $\mathrm{SL}_2(\mathbb{F}_q[u])$, their stabilizers are conjugate subgroups of $\mathrm{SL}_2(\mathbb{F}_q[u])$, so they have the same cardinality. We conclude from Proposition 7.36 that

$$\begin{cases} q^3 - q & \gamma = \delta \\ (q-1)q^{\delta-\gamma+1} & \gamma < \delta \end{cases} = \begin{cases} q^3 - q & \gamma = \delta' \\ (q-1)q^{\delta'-\gamma+1} & \gamma < \delta'. \end{cases} \tag{7.118}$$

As $q^3 - q$ is not equal to $q-1$ times a power of q, we infer that $\delta' = \delta$ and thus $v_{\gamma,\delta} = v_{\gamma',\delta'}$ as required for uniqueness. □

Proposition 7.38. *For every indefinite quadratic form $Q(X,Y)$ over $\mathbb{F}_q[u]$ there exist linear forms $L_1(X,Y)$ and $L_2(X,Y)$ over $\mathbb{F}_q((u^{-1}))$ such that*

$$Q(X,Y) = L_1(X,Y)L_2(X,Y). \tag{7.119}$$

This factorization is unique up to scaling L_1 by an element of $\mathbb{F}_q((u^{-1}))^\times$ and L_2 by its inverse, and up to changing the order of the factors.

Proof. The discriminant $D = ac - b^2/4$ of $Q(X,Y) = aX^2 + bXY + cY^2$ is indefinite, namely the infinite place of $\mathbb{F}_q(u)$ splits in the splitting field of $F(T) = T^2 + D$ over $\mathbb{F}_q(u)$, or equivalently $-D$ is a square in the completion $\mathbb{F}_q((u^{-1}))$ of $\mathbb{F}_q(u)$ at infinity. This means that there exists a unique (unordered) pair of scalars $\lambda_1, \lambda_2 \in \mathbb{F}_q((u^{-1}))$ such that

$$\begin{aligned} Q(X,Y) &= Y^2\left(a\left(\frac{X}{Y}\right)^2 + b\frac{X}{Y} + c\right) = Y^2 a\left(\frac{X}{Y} - \lambda_1\right)\left(\frac{X}{Y} - \lambda_2\right) \\ &= a(X - \lambda_1 Y)(X - \lambda_2 Y). \end{aligned}$$

□

Notation 7.39. Using the notation of Proposition 7.38, for a primitive representation $(Q,(x,y))$ we define a function on $\mathbb{F}_q[u]^2$ by

$$v^Q_{(x,y)}(z,w) = \max\{\deg(L_1(z,w)) - \deg(L_1(x,y)), \deg(L_2(z,w)) - \deg(L_2(x,y))\}$$

where the degree of a nonzero element of $\mathbb{F}_q((u^{-1}))$ is the degree of its highest-order term in u. It follows from the uniqueness part of Proposition 7.38 that the function $v^Q_{(x,y)}$ is well-defined.

Lemma 7.40. *The function $v^Q_{(x,y)}(z,w)$ is a valuation, and it satisfies*

$$v^Q_{(x,y)}(z,w) \geq \frac{\deg(Q(z,w)) - \deg(Q(x,y))}{2}. \tag{7.120}$$

Proof. To check Definition 7.33(1), we just need to note that for every polynomial $a \in \mathbb{F}_q[u]$ we have

$$\deg(L_i(az,aw)) = \deg(a) + \deg(L_i(z,w)), \quad i \in \{1,2\}.$$

For Definition 7.33(2), one has to observe that for $i \in 1,2$ we have

$$\deg(L_i(z+r,w+s)) = \deg(L_i(z,w) + L_i(r,s)) \leq \max\{\deg(L_i(z,w)), \deg(L_i(r,s))\}.$$

To verify Definition 7.33(3) note that twice the value of the function equals

$$\begin{aligned} &2\max\{\deg(L_1(z,w)) - \deg(L_1(x,y)), \deg(L_2(z,w)) - \deg(L_2(x,y))\} \geq \\ &\deg(L_1(z,w)) - \deg(L_1(x,y)) + \deg(L_2(z,w)) - \deg(L_2(x,y)) = \\ &\deg(L_1(z,w)L_2(z,w)) - \deg(L_1(x,y)L_2(x,y)) = \deg(Q(z,w)) - \deg(Q(x,y)) \end{aligned}$$

and $Q(z,w)\neq 0$ for $(z,w)\neq(0,0)$ by the homogeneity of Q and Eq. (7.37), so the above is at least $-\deg(Q(x,y))$. This concludes the verification of Eq. (7.120) and of all the conditions a valuation must satisfy. □

Associating a valuation to a representation is an $\mathrm{SL}_2(\mathbb{F}_q[u])$-equivariant operation, as we shall now see.

Proposition 7.41. *Let $(Q,(x,y))$ be a representation by an indefinite quadratic form, and let $M\in\mathrm{SL}_2(\mathbb{F}_q[u])$ be a matrix. Then*

$$v^{Q\star M}_{(x,y)\star M}=v^{Q}_{(x,y)}\star M. \tag{7.121}$$

Proof. Since $Q(X,Y)=L_1(X,Y)L_2(X,Y)$, we get from Definition 7.6 that

$$(Q\star M)(X,Y)=Q((X,Y)M^T)=L_1((X,Y)M^T)L_2((X,Y)M^T) \tag{7.122}$$

and from Definition 7.4 that $(x,y)\star M=(x,y)M^{-T}$. Therefore

$$\begin{aligned}v^{Q\star M}_{(x,y)\star M}(z,w)&=\max_{i\in\{1,2\}}\{\deg(L_i((z,w)M^T))-\deg(L_i((x,y)M^{-T}M^T))\}\\&=\max_{i\in\{1,2\}}\{\deg(L_i((z,w)M^T))-\deg(L_i(x,y))\}=(v^{Q}_{(x,y)}\star M)(z,w)\end{aligned}$$

for every vector $(z,w)\in\mathbb{F}_q[u]^2$, in view of Definition 7.35. □

Remark 7.42. We can think of the set of valuations on $\mathbb{F}_q[u]^2$ as an analogue of the upper half-plane, on which $\mathrm{SL}_2(\mathbb{F}_q[u])$ acts, and our set of (standard) representatives of each $\mathrm{SL}_2(\mathbb{F}_q[u])$-orbit as an analog of the usual fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half-plane. To each indefinite quadratic form Q one associates a geodesic in the upper half-plane, which for us consists of the valuations $v^{Q}_{(x,y)}$ for the various vectors (x,y). We will show that the standard representations correspond to points on this geodesic that lie in the fundamental domain.

Lemma 7.43. *Let $(Q,(x,y))$ be a primitive representation of $A\in\mathbb{F}_q[u]$ by an indefinite quadratic form. If the associated valuation is standard, namely*

$$v^{Q}_{(x,y)}=v_{\gamma,\delta},\quad \gamma\le\delta, \tag{7.123}$$

then $(Q,(x,y))$ is a standard representation of weight

$$\omega(Q,(x,y))=\omega_{\delta-\gamma}=\begin{cases}\frac{1}{q^3-q} & \gamma=\delta\\ \frac{1}{(q-1)q^{\delta-\gamma+1}} & \gamma<\delta.\end{cases} \tag{7.124}$$

Proof. It follows from Lemma 7.40 and our assumptions that

(7.125)
$$\begin{aligned}&\deg(az^2+bzw+cw^2)=\deg(Q(z,w))\le 2v^{Q}_{(x,y)}(z,w)+\deg(Q(x,y))=\\&2v_{\gamma,\delta}(z,w)+\deg(A)=\max\{2\gamma+2\deg(z),2\delta+2\deg(w)\}+\deg(A).\end{aligned}$$

Taking $w=0,\ z=1$ above, we see that

$$\deg(a)\le 2\gamma+\deg(A), \tag{7.126}$$

taking $z = 0,\ w = 1$, we see that

$$\deg(c) \leq 2\delta + \deg(A), \tag{7.127}$$

taking $z = u^{\delta-\gamma},\ w = 1$ in Eq. (7.125), and using Eq. (7.126), Eq. (7.127) we see that

$$\begin{aligned}&\deg(b) + \delta - \gamma = \deg(bu^{\delta-\gamma}) = \deg(Q(u^{\delta-\gamma}, 1) - au^{2\delta-2\gamma} - c) \leq \\ &\max\{\deg(Q(u^{\delta-\gamma}, 1)), \deg(au^{2\delta-2\gamma}), \deg(c)\} \leq 2\delta + \deg(A)\end{aligned}$$

so

$$\deg(b) \leq \gamma + \delta + \deg(A). \tag{7.128}$$

From Eq. (7.37) we get that $Q(x, y) \neq 0$ so for the linear forms L_1 and L_2 from Proposition 7.38 we have that $\deg(L_1(x, y))$ and $\deg(L_2(x, y))$ are finite, hence

$$0 = v^Q_{(x,y)}(x, y) = v_{\gamma,\delta}(x, y) = \max\{\gamma + \deg(x), \delta + \deg(y)\}. \tag{7.129}$$

Therefore

$$\deg(x) \leq -\gamma, \quad \deg(y) \leq -\delta. \tag{7.130}$$

Set $s = \delta - \gamma$. Our proposition reduces to showing that the discriminant $D = ac - b^2/4$ of Q satisfies

$$\deg(D) = 2\gamma + 2\delta + 2\deg(A). \tag{7.131}$$

Indeed it follows from $s = \delta - \gamma$ and Eq. (7.131) that

$$\gamma = \frac{\deg(D)}{4} - \frac{\deg(A)}{2} - \frac{s}{2}, \quad \delta = \frac{\deg(D)}{4} - \frac{\deg(A)}{2} + \frac{s}{2} \tag{7.132}$$

so Eq. (7.89) and Eq. (7.90) follow from Eq. (7.126), Eq. (7.128), Eq. (7.127), and Eq. (7.130).

To check Eq. (7.131), write

$$L_1(X, Y) = \alpha_1 X + \beta_1 Y,\ L_2(X, Y) = \alpha_2 X + \beta_2 Y,\ \alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{F}_q((u^{-1}))$$

so that

$$Q(X, Y) = (\alpha_1 X+\beta_1 Y)(\alpha_2 X+\beta_2 Y) = \alpha_1\alpha_2 X^2+(\alpha_1\beta_2+\beta_1\alpha_2)XY+\beta_1\beta_2 Y^2$$

and thus

$$-D = \frac{(\alpha_1\beta_2 + \beta_1\alpha_2)^2}{4} - \alpha_1\alpha_2\beta_1\beta_2 = \frac{(\alpha_1\beta_2 - \beta_1\alpha_2)^2}{4}. \tag{7.133}$$

Therefore, it suffices to show that

$$\deg(\alpha_1\beta_2 - \beta_1\alpha_2) = \gamma + \delta + \deg(A). \tag{7.134}$$

For $i \in \{1, 2\}$ we have

$$\begin{aligned}\gamma = v_{\gamma,\delta}(1, 0) = v^Q_{(x,y)}(1, 0) &\geq \deg(L_i(1, 0)) - \deg(L_i(x, y)) \\ &= \deg(\alpha_i) - \deg(L_i(x, y))\end{aligned} \tag{7.135}$$

and similarly

$$\delta = v_{\gamma,\delta}(0,1) = v^{Q}_{(x,y)}(0,1) \geq \deg(\beta_i) - \deg(L_i(x,y)) \tag{7.136}$$

so

$$\deg(\alpha_i) \leq \gamma + \deg(L_i(x,y)), \quad \deg(\beta_i) \leq \delta + \deg(L_i(x,y)). \tag{7.137}$$

We conclude that

$$\begin{gathered}\deg(\alpha_1\beta_2 - \beta_1\alpha_2) \leq \max\{\deg(\alpha_1)+\deg(\beta_2), \deg(\beta_1)+\deg(\alpha_2)\} \leq \\ \gamma+\delta+\deg(L_1(x,y)L_2(x,y)) = \gamma+\delta+\deg(Q(x,y)) = \gamma+\delta+\deg(A)\end{gathered}$$

so we have established one inequality towards Eq. (7.134).

Assume for contradiction that the inequality above is strict. Denoting by $\alpha_i^{(0)}$ the coefficient of α_i in degree $\gamma + \deg(L_i(x,y))$ for $i \in \{1,2\}$, and by $\beta_i^{(0)}$ the coefficient of β_i in degree $\delta + \deg(L_i(x,y))$, we can interpret our assumption for contradiction as

$$\det\begin{pmatrix}\alpha_1^{(0)} & \alpha_2^{(0)} \\ \beta_1^{(0)} & \beta_2^{(0)}\end{pmatrix} = \alpha_1^{(0)}\beta_2^{(0)} - \beta_1^{(0)}\alpha_2^{(0)} = 0. \tag{7.138}$$

Let $(r,t) \in \mathbb{F}_q^2$ be a nonzero vector in the kernel of the matrix above. By examining the coefficients in degree $\delta + \deg(L_i(x,y))$ we see that

$$\deg(L_i(ru^{\delta-\gamma},t)) = \deg(ru^{\delta-\gamma}\alpha_i + t\beta_i) < \delta + \deg(L_i(x,y)), \quad i \in \{1,2\}.$$

Since (at least) one of the scalars r,t is nonzero, we get that

$$\begin{aligned}\delta &= \max\{\deg(r)+\delta, \deg(t)+\delta\} = v_{\gamma,\delta}(ru^{\delta-\gamma},t) \\ &= v^{Q}_{(x,y)}(ru^{\delta-\gamma},t) = \max_{i\in\{1,2\}}\{\deg(L_i(ru^{\delta-\gamma},t)) - \deg(L_i(x,y))\} < \delta\end{aligned}$$

which is a contradiction. This verifies Eq. (7.134), completing the proof. □

Lemma 7.44. *For every standard representation $(Q,(x,y))$ of a polynomial A by an indefinite quadratic form, there exist integers $\gamma \leq \delta$ such that*

$$v^{Q}_{(x,y)} = v_{\gamma,\delta}. \tag{7.139}$$

Proof. Following Definition 7.31, and Eq. (7.132) we define

$$\gamma = \frac{\deg(D)}{4} - \frac{\deg(A)}{2} - \frac{s}{2}, \quad \delta = \frac{\deg(D)}{4} - \frac{\deg(A)}{2} + \frac{s}{2} \tag{7.140}$$

and note that γ,δ are indeed integers by Proposition 7.32. Our assumption that $(Q,(x,y))$ is standard then gives

$$\deg(x) \leq -\gamma,\ \deg(y) \leq -\delta,\ \delta-\gamma = s,\ \gamma+\delta = \frac{\deg(D)}{2} - \deg(A). \tag{7.141}$$

By Proposition 7.38, for $i \in \{1,2\}$ there exist linear forms

$$L_i(X,Y) = \alpha_i X + \beta_i Y, \quad \alpha_i,\beta_i \in \mathbb{F}_q((u^{-1})) \tag{7.142}$$

such that

$$Q(X,Y) = L_1(X,Y)L_2(X,Y) = \alpha_1\alpha_2X^2 + (\alpha_1\beta_2+\beta_1\alpha_2)XY + \beta_1\beta_2Y^2$$

and

$$-D = \frac{(\alpha_1\beta_2 - \beta_1\alpha_2)^2}{4} \tag{7.143}$$

as in Eq. (7.133).

It follows from our expression for Q, Eq. (7.89), and Eq. (7.143) that

$$\deg(\alpha_1\beta_2 + \beta_1\alpha_2), \deg(\alpha_1\beta_2 - \beta_1\alpha_2) \leq \frac{\deg(D)}{2} \tag{7.144}$$

and therefore that

$$\deg(\alpha_1\beta_2), \deg(\beta_1\alpha_2) \leq \frac{\deg(D)}{2}. \tag{7.145}$$

We further infer from our expression for Q, Eq. (7.89), and Eq. (7.141) that

$$\deg(\alpha_1\alpha_2) \leq \frac{\deg(D)}{2} - \delta + \gamma, \quad \deg(\beta_1\beta_2) \leq \frac{\deg(D)}{2} + \delta - \gamma. \tag{7.146}$$

By Eq. (7.141), for $i \in \{1, 2\}$ we have

$$\begin{aligned} \deg(L_i(x,y)) &\leq \max\{\deg(\alpha_i) + \deg(x), \deg(\beta_i) + \deg(y)\} \\ &\leq \max\{\deg(\alpha_i) - \gamma, \deg(\beta_i) - \delta\} \end{aligned} \tag{7.147}$$

which either gives a lower bound on the degree of α_i or a lower bound on the degree of β_i (or both). Combined with the upper bounds on $\deg(\alpha_i\alpha_{3-i})$ and $\deg(\beta_i\alpha_{3-i})$ in the first case, or $\deg(\alpha_i\beta_{3-i})$ and $\deg(\beta_i\beta_{3-i})$ in the second case, we obtain using Eq. (7.141) that

$$\begin{aligned} \deg(\alpha_i) \leq \begin{cases} \frac{\deg(D)}{2} - \delta + \gamma - \deg(\alpha_{3-i}) \\ \frac{\deg(D)}{2} - \deg(\beta_{3-i}) \end{cases} &\leq \frac{\deg(D)}{2} - \delta - \deg(L_{3-i}(x,y)) \\ = \deg(A) + \gamma - \deg(L_{3-i}(x,y)) &= \deg(L_i(x,y)) + \gamma \end{aligned}$$

and

$$\begin{aligned} \deg(\beta_i) \leq \begin{cases} \frac{\deg(D)}{2} - \deg(\alpha_{3-i}) \\ \frac{\deg(D)}{2} + \delta - \gamma - \deg(\beta_{3-i}) \end{cases} &\leq \frac{\deg(D)}{2} - \gamma - \deg(L_{3-i}(x,y)) \\ = \deg(A) + \delta - \deg(L_{3-i}(x,y)) &= \deg(L_i(x,y)) + \delta. \end{aligned}$$

The bounds on $\deg(\alpha_i), \deg(\beta_i)$ imply that for $(z, w) \in \mathbb{F}_q[u]^2$ we have

$$\begin{aligned} v^Q_{(x,y)}(z,w) &= \max_{i\in\{1,2\}} \{\deg(\alpha_i z + \beta_i w) - \deg(L_i(x,y))\} \\ &\leq \max_{i\in\{1,2\}} \{\max\{\deg(\alpha_i) + \deg(z), \deg(\beta_i) + \deg(w)\} - \deg(L_i(x,y))\} \\ &\leq \max\{\gamma + \deg(z), \delta + \deg(w)\} = v_{\gamma,\delta}(z,w). \end{aligned}$$

We must prove that this inequality is in fact an equality.

Assume toward a contradiction that for some (nonzero) vector (z, w) the inequality above is strict, namely

$$\max_{i\in\{1,2\}} \{\deg(\alpha_i z + \beta_i w) - \deg(L_i(x,y))\} < v_{\gamma,\delta}(z,w). \tag{7.148}$$

For $i \in \{1,2\}$ let $\alpha_i^{(0)}$ be the coefficient of α_i in degree $\deg(L_i(x,y)) + \gamma$, and let $\beta_i^{(0)}$ be the coefficient of β_i in degree $\deg(L_i(x,y)) + \delta$. Let moreover $z^{(0)}$ be the coefficient of z in degree $v_{\gamma,\delta}(z,w) - \gamma$, and let $w^{(0)}$ be the coefficient of w in degree $v_{\gamma,\delta}(z,w) - \delta$. Note that all the coefficients in degrees higher than these are necessarily zero, and that $(z^{(0)}, w^{(0)}) \neq (0,0)$ because $(z,w) \neq (0,0)$.

In the notation above, Eq. (7.148) translates to

$$\begin{pmatrix} z^{(0)} & w^{(0)} \end{pmatrix} \begin{pmatrix} \alpha_1^{(0)} & \alpha_2^{(0)} \\ \beta_1^{(0)} & \beta_2^{(0)} \end{pmatrix} = \begin{pmatrix} 0 & 0 \end{pmatrix} \tag{7.149}$$

so the determinant of the matrix above vanishes, that is

$$\alpha_1^{(0)}\beta_2^{(0)} - \alpha_2^{(0)}\beta_1^{(0)} = 0. \tag{7.150}$$

We conclude, using Eq. (7.141), that

$$\begin{aligned}\deg(\alpha_1\beta_2 - \alpha_2\beta_1) < \deg(L_1(x,y)) + \deg(L_2(x,y)) + \gamma + \delta = \deg(A) + \gamma + \delta \\ = \frac{\deg(D)}{2}\end{aligned}$$

which contradicts Eq. (7.143). □

Corollary 7.45. *Let $D \in \mathbb{F}_q[u]$ be indefinite. Consider the function*

$$(aX^2 + bXY + cY^2, (x,y)) \mapsto (ax^2 + bxy + cy^2, ay_x x + \frac{b}{2}(\overline{x}x + y_x y) + c\overline{x}y)$$

which maps a standard representation (Q,v) by a quadratic form of discriminant D to the represented polynomial $A = Q(v)$ and the associated solution f to the congruence $T^2 + D \equiv 0 \mod A$. Then the image of this function is

$$\{(A,f) : A \in \mathbb{F}_q[u] \setminus \{0\},\ f \in \mathbb{F}_q[u]/(A),\ f^2 + D \equiv 0 \mod A\}. \tag{7.151}$$

Moreover the number of elements in the preimage of any (A,f) from Eq. (7.151) equals the inverse of the weight of any representation in this preimage.

Proof. It is immediate from Definition 7.12 that the image of our function is contained in Eq. (7.151). For (A,f) in this set, Proposition 7.14 gives us a primitive representation $(Q,(x,y))$ of A by a quadratic form of discriminant D such that the associated solution is f. By Proposition 7.37 there exist integers $\gamma \le \delta$ and a matrix $M \in \mathrm{SL}_2(\mathbb{F}_q[u])$ such that

$$v^Q_{(x,y)} \star M = v_{\gamma,\delta}. \tag{7.152}$$

Proposition 7.41 then implies that

$$v^{Q\star M}_{(x,y)\star M} = v_{\gamma,\delta}. \tag{7.153}$$

Lemma 7.43 tells us that the representation $(Q',(x',y')) = (Q\star M, (x,y)\star M)$ is a standard representation of A with weight

$$\omega(Q',(x',y')) = \begin{cases} \frac{1}{q^3-q} & \gamma = \delta \\ \frac{1}{(q-1)q^{\delta-\gamma+1}} & \gamma < \delta. \end{cases} \tag{7.154}$$

It follows from Corollary 7.13 that our function maps $(Q', (x', y'))$ to (A, f) so its image is indeed given by Eq. (7.151).

By Corollary 7.13, the preimage of (A, f) under our function consists of the standard representations of A that are equivalent to $(Q', (x', y'))$. These are parametrized by matrices $N \in \mathrm{SL}_2(\mathbb{F}_q[u])$ for which the representation

$$(Q' \star N, (x', y') \star N) \tag{7.155}$$

is standard. By Lemma 7.43 and Lemma 7.44 this is equivalent to the valuation

$$v^{Q' \star N}_{(x', y') \star N} \tag{7.156}$$

being standard. In view of Proposition 7.41 and Eq. (7.153), we are looking for the set of all $N \in \mathrm{SL}_2(\mathbb{F}_q[u])$ for which the valuation

$$v^{Q'}_{(x', y')} \star N = v_{\gamma,\delta} \star N \tag{7.157}$$

is standard.

Using the uniqueness part of Proposition 7.37, we see that the valuation above is standard if and only if

$$v_{\gamma,\delta} \star N = v_{\gamma,\delta}. \tag{7.158}$$

We conclude from Proposition 7.36 that the number of elements in the preimage of (A, f) is

$$|\{N \in \mathrm{SL}_2(\mathbb{F}_q[u]) : v_{\gamma,\delta} \star N = v_{\gamma,\delta}\}| = \begin{cases} q^3 - q & \gamma = \delta \\ (q-1)q^{\delta-\gamma+1} & \gamma < \delta. \end{cases} \tag{7.159}$$

At last, note that the above is the inverse of the weight of the representation $(Q', (x', y'))$ given in Eq. (7.154). □

Notation 7.46. Following Definition 7.31, for an indefinite polynomial D in $\mathbb{F}_q[u]$ we set

$$S(D) = \Bigg\{ (s, a, b, c) \in \mathbb{Z} \times \mathbb{F}_q[u]^3 : \deg(a) \leq \frac{\deg(D)}{2} - s, \ \deg(b) \leq \frac{\deg(D)}{2}$$
$$\deg(c) \leq \frac{\deg(D)}{2} + s, \ ac - \frac{b^2}{4} = D, \ s \geq 0 \Bigg\}.$$

For $(s, a, b, c) \in S(D)$ let $a_{(0)}, b_{(0)}, c_{(0)}$ be the coefficients of a, b, c in degrees

$$\frac{\deg(D)}{2} - s, \quad \frac{\deg(D)}{2}, \quad \frac{\deg(D)}{2} + s. \tag{7.160}$$

For a standard representation $ax^2 + bxy + cy^2$ of a degree n polynomial, we denote by $x_{(0)}, y_{(0)}$ the coefficients of x, y in degrees

$$\frac{n}{2} - \frac{\deg(D)}{4} + \frac{s}{2}, \quad \frac{n}{2} - \frac{\deg(D)}{4} - \frac{s}{2}. \tag{7.161}$$

Corollary 7.47. *For every $\epsilon > 0$ we have*

$$\sum_{(s,a,b,c)\in S(D)} \omega_s \ll |D|^{\frac{1}{2}+\epsilon}. \tag{7.162}$$

Proof. For $i \in \mathbb{Z}/2\mathbb{Z}$ set $S(D;i) = \{(s,a,b,c) \in S(D) : s \equiv i \mod 2\}$, and note that it is enough to obtain the bound

$$\sum_{(s,a,b,c)\in S(D;i)} \omega_s \ll |D|^{\frac{1}{2}+\epsilon}. \tag{7.163}$$

Fix $i \in \mathbb{Z}/2\mathbb{Z}$, and let $(s,a,b,c) \in S(D;i)$. Arguing as in the proof of the first claim in Proposition 7.32, we find that (at least) one of the coefficients $a_{(0)}, b_{(0)}, c_{(0)}$ is nonzero. Therefore choosing $x_0, y_0 \in \mathbb{F}_q$ via

$$(x_0, y_0) = \begin{cases} (1,0) & a_{(0)} \neq 0 \\ (0,1) & a_{(0)} = 0,\ c_{(0)} \neq 0 \\ (1,1) & a_{(0)} = 0,\ c_{(0)} = 0,\ b_{(0)} \neq 0 \end{cases} \tag{7.164}$$

we see that

$$a_{(0)}x_0^2 + b_{(0)}x_0y_0 + c_{(0)}y_0^2 \neq 0. \tag{7.165}$$

Let $n \geq \frac{\deg(D)}{2} + s$ be an integer with

$$n \equiv \frac{\deg(D)}{2} + i \mod 2, \tag{7.166}$$

and let $x, y \in \mathbb{F}_q[u]$ be coprime polynomials with

$$\deg(x) \leq \frac{n}{2} - \frac{\deg(D)}{4} + \frac{s}{2},\ \deg(y) \leq \frac{n}{2} - \frac{\deg(D)}{4} - \frac{s}{2},\ x_{(0)} = x_0,\ y_{(0)} = y_0.$$

It follows from our choices that the polynomial $A = ax^2 + bxy + cy^2$ has degree n, so this representation is standard. From the count of coprime pairs (x,y) in [ABSR15, Proof of Lemma 7.3], it follows that the weighted number of standard representations of degree n polynomials by forms of discriminant D is

$$\gg \sum_{(s,a,b,c)\in S(D;i)} \omega_s q^{\frac{n}{2}-\frac{\deg(D)}{4}+\frac{s}{2}} q^{\frac{n}{2}-\frac{\deg(D)}{4}-\frac{s}{2}} = q^{n-\frac{\deg(D)}{2}} \sum_{(s,a,b,c)\in S(D;i)} \omega_s.$$

On the other hand, using Notation 6.3, the number of such representations is

$$\ll \sum_{A\in\mathcal{M}_n} \rho(A;F) \tag{7.167}$$

in view of Corollary 7.27. By Proposition 6.5 the above is $\ll q^n|D|^\epsilon$ so

$$\sum_{(s,a,b,c)\in S(D;i)} \omega_s \ll q^{\frac{\deg(D)}{2}}|D|^\epsilon = |D|^{\frac{1}{2}+\epsilon}$$

as desired. □

8. Primes in quadratic sequences

We state and prove a uniform version of Theorem 1.2.

Theorem 8.1. *Fix $0 < \delta \leq 1$. Let p be an odd prime, let*

$$q > \max\left\{\left(16pe\delta^{-1}\right)^3, \left(96ep^2\delta^{-1}\right)^2\right\} \tag{8.1}$$

be a power of p, and let

$$\gamma = 1 - \frac{\delta}{12p-1} \min\left\{2 - 6\log_q\left(16pe\delta^{-1}\right), \frac{1}{2p} - \frac{\log_q\left(96ep^2\delta^{-1}\right)}{p}\right\}. \tag{8.2}$$

Let d be a nonnegative integer and D a polynomial in $\mathbb{F}_q[u]$ with

$$\deg(D) \leq 2d(1-\delta). \tag{8.3}$$

Let $F(T) = T^2 + D$, and assume that F is irreducible in $(\mathbb{F}_q[u])[T]$. Then

$$\sum_{f \in \mathcal{M}_d} \Lambda(f^2 + D) = \mathfrak{S}(F)q^d + O(q^{\gamma d}), \quad d \to \infty, \tag{8.4}$$

with the implied constant depending only on δ and q.

Note that $\gamma < 1$ in view of Eq. (8.1), so Eq. (8.4) always gives a power saving. If $q > (96ep^2)^2 = \max\{(16pe)^3, (96ep^2)^2\}$ we can choose $\delta < 1$ satisfying Eq. (8.1), and in this way obtain a power saving bound for d sufficiently large depending on $\deg(D)$. Specifically, we obtain a power savings of $\frac{1}{2p(12p-1)}\left(1 - 2\log_q\left(96ep^2\right)\right)$ as this term always dominates in Eq. (8.2).

Proof. The identity $\Lambda = -1 * (\mu \cdot \deg)$ expressing the von Mangoldt function in terms of the Möbius function gives

$$\Lambda(F(f)) = -\sum_{k=1}^{2d} k \sum_{\substack{A \in \mathcal{M}_k \\ AB = F(f)}} \sum_{B \in \mathcal{M}_{2d-k}} \mu(A) \tag{8.5}$$

for any polynomial $f \in \mathcal{M}_d$. Summing Eq. (8.5) over all degree d monic polynomials $f \in \mathbb{F}_q[u]$ we get

$$\sum_{f \in \mathcal{M}_d} \Lambda(F(f)) = -\sum_{k=1}^{2d} k \sum_{f \in \mathcal{M}_d} \sum_{\substack{A \in \mathcal{M}_k \\ AB = F(f)}} \sum_{B \in \mathcal{M}_{2d-k}} \mu(A). \tag{8.6}$$

Fix $\epsilon = \epsilon(q) \in (0, \delta/4)$. The contribution of the range $(1+\epsilon)d \leq k \leq 2d$ is

$$-\sum_{(1+\epsilon)d \leq k \leq 2d} k \sum_{B \in \mathcal{M}_{2d-k}} \sum_{\substack{g \in \mathbb{F}_q[u] \\ \deg(g) < 2d-k \\ F(g) \equiv 0 \bmod B}} \sum_{\substack{f \in \mathcal{M}_d \\ f \equiv g \bmod B}} \mu\left(\frac{f^2 + D}{B}\right). \tag{8.7}$$

Writing $f = g + CB$ we get

$$-\sum_{(1+\epsilon)d\le k\le 2d} k \sum_{B\in\mathcal{M}_{2d-k}} \sum_{\substack{g\in\mathbb{F}_q[u]\\ \deg(g)<2d-k\\ F(g)\equiv 0 \bmod B}} \sum_{C\in\mathcal{M}_{k-d}} \mu\left(BC^2+2gC+\frac{g^2+D}{B}\right).$$

We note that the quadratic polynomials

$$G(T) = BT^2 + 2gT + \frac{g^2+D}{B} \in \mathbb{F}_q[u][T] \tag{8.8}$$

(appearing in the Möbius function above) are separable in the variable T for every B, g. Indeed the discriminant of G in T is

$$(2g)^2 - 4B\frac{g^2+D}{B} = 4g^2 - 4(g^2+D) = -4D \neq 0. \tag{8.9}$$

We can therefore apply Theorem 5.1 with

$c_1 = \max\{2d-k, \deg(D)-(2d-k)\}$, $c_2 = 0$, $g = 1$, $\mathcal{I} = \mathcal{M}_{k-d}$, $\beta_1 = (1+2\gamma_1)^2$

obtaining

$$\begin{aligned}\sum_{C\in\mathcal{M}_{k-d}} \mu\left(BC^2+2gC+\frac{g^2+D}{B}\right) &\ll q^{(k-d)(1-\alpha_1)}\beta_1^{2\max\{2d-k,\deg(D)-(2d-k)\}}\\ &\le q^{(k-d)(1-\alpha_1)}\left(\beta_1^{2(2d-k)}+\beta_1^{2\deg(D)-2(2d-k)}\right)\\ &= q^{(k-d)(1-\alpha_1)}\left((1+2\gamma_1)^{4(2d-k)}+(1+2\gamma_1)^{4\deg(D)-4(2d-k)}\right)\end{aligned}$$

for any α_1 and $0 < \gamma_1 \le 1$ satisfying Eq. (5.1), namely

$$0 < \alpha_1 < \frac{1}{2p} + \frac{\log_q \gamma_1}{p} - 2\log_q(1+2\gamma_1). \tag{8.10}$$

By Proposition 6.5, the contribution of each k with $(1+\epsilon)d \le k \le 2d$ to Eq. (8.7) is then

$$\begin{aligned}&\ll q^{(k-d)(1-\alpha_1)}\left((1+2\gamma_1)^{4(2d-k)}+(1+2\gamma_1)^{4\deg(D)-4(2d-k)}\right)\sum_{B\in\mathcal{M}_{2d-k}}\sum_{\substack{g\in\mathbb{F}_q[u]\\ \deg(g)<2d-k\\ F(g)\equiv 0 \bmod B}} 1\\ &= q^{(k-d)(1-\alpha_1)}\left((1+2\gamma_1)^{4(2d-k)}+(1+2\gamma_1)^{4\deg(D)-4(2d-k)}\right)\cdot|D|^{o(1)}q^{2d-k}\\ &= |D|^{o(1)}q^dq^{-\alpha_1(k-d)}(1+2\gamma_1)^{4(2d-k)}+|D|^{o(1)}q^dq^{-\alpha_1(k-d)}(1+2\gamma_1)^{4\deg(D)-4(2d-k)}.\end{aligned}$$

The first term is exponentially decreasing as a function of k. Hence for $k \ge (1+\epsilon)d$ it is bounded from above by

$$|D|^{o(1)}q^dq^{-\alpha_1\epsilon d}(1+2\gamma_1)^{4(1-\epsilon)d}. \tag{8.11}$$

Therefore, in order to obtain power savings, we need

$$q^{-\alpha_1\epsilon}(1+2\gamma_1)^{4(1-\epsilon)} < 1. \tag{8.12}$$

If we assume for the moment that Eq. (8.12) holds, using our assumptions that $\epsilon \leq \frac{\delta}{4} \leq \frac{1}{2}$, we get

$$q^{-\alpha_1}(1+2\gamma_1)^4 < 1 \tag{8.13}$$

so the second term $|D|^{o(1)} q^d q^{-\alpha_1(k-d)}(1+2\gamma_1)^{4\deg(D)-4(2d-k)}$ is exponentially decreasing as a function of k, and thus is bounded from above by

$$|D|^{o(1)} q^d q^{-\alpha_1 \epsilon d}(1+2\gamma_1)^{4\deg(D)-4(1-\epsilon)d} \tag{8.14}$$

which is also bounded by Eq. (8.11) since

$$\deg(D) \leq 2(1-\delta)d \leq 2(1-\epsilon)d. \tag{8.15}$$

Consequently, the contribution of the range $(1+\epsilon)d \leq k \leq 2d$ to Eq. (8.6) is at most

$$d^2 |D|^{o(1)} q^d q^{-\alpha_1 \epsilon d}(1+2\gamma_1)^{4(1-\epsilon)d} \tag{8.16}$$

as long as we have Eq. (8.10) and Eq. (8.12). We now specialize

$$\epsilon = \frac{\delta}{12p-1}, \gamma_1 = \frac{\epsilon}{2(4-2\epsilon)p} = \frac{\delta}{2p(48p-4-2\delta)}, \alpha_1 = \frac{1}{2p} + \frac{\log_q \gamma_1}{p} - \frac{4\gamma_1}{\log q}$$

which satisfies the second inequality in Eq. (8.10) because

$$\alpha_1 = \frac{1}{2p} + \frac{\log_q \gamma_1}{p} - \frac{4\gamma_1}{\log q} < \frac{1}{2p} + \frac{\log_q \gamma_1}{p} - 2\log_q(1+2\gamma_1) \tag{8.17}$$

and satisfies Eq. (8.12), and thus the first inequality in Eq. (8.10), because

$$\begin{aligned} q^{-\alpha_1 \epsilon}(1+2\gamma_1)^{4(1-\epsilon)} &< q^{-\alpha_1 \epsilon} e^{8\gamma_1(1-\epsilon)} = q^{-\frac{\epsilon}{2p}} \gamma_1^{-\frac{\epsilon}{p}} e^{4\epsilon\gamma_1 + 8(1-\epsilon)\gamma_1} \\ &= q^{-\frac{\epsilon}{2p}} \gamma_1^{-\frac{\epsilon}{p}} e^{\frac{\epsilon}{p}} = \left(\frac{q^{\frac{1}{2}}\delta}{2pe(48p-4-2\delta)} \right)^{-\frac{\epsilon}{p}} \end{aligned} \tag{8.18}$$

which is < 1 since $q > (96ep^2\delta^{-1})^2 > (2pe(48p-4-2\delta)\delta^{-1})^2$ by Eq. (8.1).

Applying Eq. (8.18), and using our assumption $|D| \leq q^{2d(1-\delta)}$, which guarantees that $d^2|D|^{o(1)}$ is bounded by any exponential in d, we conclude that the total contribution of the range $(1+\epsilon)d \leq k \leq 2d$ to Eq. (8.6) is

$$\ll q^d \left(\frac{2pe(48p-4-2\delta)}{q^{\frac{1}{2}}\delta} \right)^{d\frac{\epsilon}{p}} = \left(q^d\right)^{1-\frac{\delta}{2p(12p-1)}(1-2\log_q(\frac{2pe(48p-4-2\delta)}{\delta}))}. \tag{8.19}$$

This is bounded by $q^{\gamma d}$, for our choice of γ in Eq. (8.2).

The contribution of the range $k < (1+\epsilon)d$ to Eq. (8.6) is

$$-\sum_{1 \leq k < (1+\epsilon)d} k \sum_{A \in \mathcal{M}_k} \mu(A)\rho_d(A;F) \tag{8.20}$$

so by Eq. (6.8) from $k \leq d$ we get

$$-\sum_{k=1}^{d} k q^{d-k} \sum_{A \in \mathcal{M}_k} \mu(A)\rho(A;F). \tag{8.21}$$

By Corollary 6.4, from $d < k < (1+\epsilon)d$ we have

$$\begin{aligned}\sum_{d<k<(1+\epsilon)d} -kq^{d-k} \sum_{A\in\mathcal{M}_k} \mu(A)\rho(A;F) + \\ \sum_{d<k<(1+\epsilon)d} -kq^{d-k} \sum_{\substack{h\in\mathbb{F}_q[u]\setminus\{0\}\\ \deg(h)<k-d}} e\left(\frac{-hu^d}{A}\right) \sum_{A\in\mathcal{M}_k} \mu(A) \sum_{\substack{f\in\mathbb{F}_q[u]/(A)\\ F(f)\equiv 0 \bmod A}} e\left(\frac{hf}{A}\right).\end{aligned} \tag{8.22}$$

Uniting the first term in Eq. (8.22) with Eq. (8.21), and applying Proposition 6.7, we get

$$- \sum_{1\le k<(1+\epsilon)d} kq^{d-k} \sum_{A\in\mathcal{M}_k} \mu(A)\rho(A;F) = \mathfrak{S}(F)q^d + o\left(q^{\frac{d}{2}}\right) \tag{8.23}$$

which gives us our main term and an admissible error term. The second term in Eq. (8.22) is

$$\ll d^2 \sup_{d<k<(1+\epsilon)d} \sup_{h\in\mathbb{F}_q[u]} \left| \sum_{A\in\mathcal{M}_k} \mu(A) \sum_{\substack{f\in\mathbb{F}_q[u]/(A)\\ F(f)\equiv 0 \bmod A}} e\left(\frac{hf}{A}\right) \right|. \tag{8.24}$$

By Corollary 7.27, and Proposition 7.15, the sum in absolute value above, in the definite case, equals

$$\sum_{\substack{a,b,c\in\mathbb{F}_q[u]\\ \deg(c)\ge\deg(a)>\deg(b)\\ 4ac-b^2=4D}} \frac{1+q\cdot\mathbf{1}_{\deg(c)>\deg(a)}}{q^2-1} \sum_{\substack{x,y\in\mathbb{F}_q[u]\\ \gcd(x,y)=1,\ y\neq 0\\ ax^2+bxy+cy^2\in\mathcal{M}_k}} \mu(ax^2+bxy+cy^2) e\left(\frac{h\overline{x}}{y}\right) \tag{8.25}$$

where we have excluded $y = 0$ because then we have a factor of $\mu(ax^2)$ which is zero. Indeed if it were nonzero, then x would be a nonzero constant, so from Eq. (7.55) and our initial assumption on $\deg_u(F)$ we would get

$$\begin{aligned} k &= \deg(A) = \deg(ax^2+bxy+cy^2) = \deg(ax^2) \\ &= \deg(a) \le \frac{\deg(D)}{2} = \frac{\deg_u(F)}{2} \le \frac{2d(1-\delta)}{2} < d \end{aligned} \tag{8.26}$$

which is impossible because we are in the range $d < k < (1+\epsilon)d$.

Let us now check that the assumptions of Proposition 7.15 are indeed met here, namely that Eq. (7.44) and Eq. (7.45) hold. Using the second line in Eq. (8.26), and the fact that $\deg(b) < \deg(a)$ we get

$$\deg(h) < k-d = \deg(A)-d \le \deg(A)-\deg(a) \le \deg(A)-\deg(b)-1 \tag{8.27}$$

so Eq. (7.44) is verified. By Proposition 7.19 and Eq. (8.26) we have

$$\begin{aligned}&\deg(A)+\deg(y)-\deg(a)-\deg(x)=\\&\max\{\deg(a)+2\deg(x),\deg(c)+2\deg(y)\}+\deg(y)-\deg(a)-\deg(x)\geq\\&\max\{\deg(x)+\deg(y),\deg(c)-d(1-\delta)-\deg(x)\}.\end{aligned}$$

If toward a contradiction Eq. (7.45) fails, then the above is at most $\deg(h)+1$ which is bounded by $k-d$. The latter does not exceed ϵd, so

$$\deg(x),\deg(y)\leq\epsilon d,\ \deg(c)\leq d(1-\delta)+\deg(x)+\epsilon d \tag{8.28}$$

and thus

$$\begin{aligned}k&=\deg(A)=\deg(ax^2+bxy+cy^2)\\&=\max\{\deg(a)+2\deg(x),\deg(c)+2\deg(y)\}\\&\leq\max\{d(1-\delta)+2\epsilon d,d(1-\delta)+4\epsilon d\}=d(1-\delta+4\epsilon)\leq k(1-\delta+4\epsilon)\end{aligned}$$

a contradiction since $\epsilon<\delta/4$. Our invocation of Proposition 7.15 is thus justified.

We then apply the triangle inequality to the sum over a,b,c,y in Eq. (8.25), to get

$$\ll\sum_{\substack{a,b,c\in\mathbb{F}_q[u]\\\deg(c)\geq\deg(a)>\deg(b)\\4ac-b^2=4D}}\ \sum_{\substack{y\in\mathbb{F}_q[u]\\y\neq0\\\deg(y)\leq\frac{k-\deg(c)}{2}}}\left|\sum_{\substack{x\in S_{a,b,c,y}\\\gcd(x,y)=1}}\mu(ax^2+bxy+cy^2)e\left(\frac{h\overline{x}}{y}\right)\right| \tag{8.29}$$

where

$$S_{a,b,c,y}=\{x\in\mathbb{F}_q[u]:ax^2+bxy+cy^2\in\mathcal{M}_k\}. \tag{8.30}$$

We claim that for a,b,c,y as above, the set $S_{a,b,c,y}$ is a disjoint union of at most two intervals in $\mathbb{F}_q[u]$, the degree of which is at most $(k-\deg(a))/2$. To show this, recall from Proposition 7.19 that since $D=ac-b^2/4$ is definite, we have

$$\begin{aligned}k&=\deg(ax^2+bxy+cy^2)\\&=\max\{\deg(a)+2\deg(x),\deg(c)+2\deg(y)\}>\deg(bxy).\end{aligned} \tag{8.31}$$

In case $\deg(c)+2\deg(y)<k$, the leading coefficient 1 of the monic polynomial $ax^2+bxy+cy^2$ is the leading coefficient of ax^2, that is the leading coefficient of a times the square of the leading coefficient of x. Hence, if the leading coefficient of a is not a square in $\mathbb{F}_q^\times$, the set $S_{a,b,c,y}$ is empty. Otherwise, if the leading coefficient of a is λ^2, for some $\lambda\in\mathbb{F}_q^\times$, then

$$S_{a,b,c,y}=\lambda^{-1}\cdot\mathcal{M}_{\frac{k-\deg(a)}{2}}\cup(-\lambda^{-1})\cdot\mathcal{M}_{\frac{k-\deg(a)}{2}}. \tag{8.32}$$

Suppose now $\deg(c) + 2\deg(y) = k$. If cy^2 is monic, we have

$$S_{a,b,c,y} = \left\{ x \in \mathbb{F}_q[u] : \deg(x) < \frac{k - \deg(a)}{2} \right\}. \tag{8.33}$$

If cy^2 is not monic, then the set $S_{a,b,c,y}$ is empty in case $k \not\equiv \deg(a) \bmod 2$, while in case $k \equiv \deg(a) \bmod 2$, denoting by f_0 the leading coefficient of a polynomial $f \in \mathbb{F}_q[u]$, we get

$$S_{a,b,c,y} = \left\{ x \in \mathbb{F}_q[u] : \deg(x) = \frac{k - \deg(a)}{2},\ x_0^2 = \frac{1 - c_0 y_0^2}{a_0} \right\} \tag{8.34}$$

which is a disjoint union of two (possibly empty) intervals corresponding to polynomials with leading coefficient equal to one of the square roots of $(1 - c_0 y_0^2)/a_0$ in $\mathbb{F}_q^\times$. This concludes the verification of our claim in all cases.

We use Corollary 7.29 to bound the number of triples (a, b, c) in the outer sum of Eq. (8.29), and recall from Remark 7.18 that $\deg(c) \le \deg(D)$, so it suffices to control

$$|D|^{\frac{1}{2}+o(1)} \max_{\substack{a,b,c \in \mathbb{F}_q[u] \\ 4ac - b^2 = 4D \\ \deg(b) < \deg(a) \le \deg(c) \le \deg(D)}} \sum_{\substack{y \in \mathbb{F}_q[u] \\ y \neq 0 \\ \deg(y) \le \frac{k - \deg(c)}{2}}} \left| \sum_{\substack{x \in \mathcal{I}_{a,b,c,y} \\ \gcd(x,y)=1}} \mu(ax^2 + bxy + cy^2) e\left(\frac{h\overline{x}}{y}\right) \right| \tag{8.35}$$

where $\mathcal{I}_{a,b,c,y}$ is an interval in $\mathbb{F}_q[u]$ with

$$\deg(\mathcal{I}_{a,b,c,y}) \le \frac{k - \deg(a)}{2} \tag{8.36}$$

for all a, b, c, y.

Fixing a, b, c, we define the polynomial

$$F_y(T) = aT^2 + byT + cy^2 \in \mathbb{F}_q[u][T] \tag{8.37}$$

for any $y \in \mathbb{F}_q[u] \setminus \{0\}$, and note that its discriminant in the variable T is

$$(by)^2 - 4acy^2 = y^2(b^2 - 4ac) = (2y)^2 \cdot (-D) \neq 0 \tag{8.38}$$

so F_y is a separable polynomial in T.

Setting

$$n = \frac{k - \deg(c)}{2}, \quad c_1 = k, \quad c_2 = -\frac{k - \deg(a)}{2}, \quad c_3 = \frac{k - \deg(a)}{2}$$

we see that the coefficient of T^i in $F_y(T)$ has degree at most $c_1 + ic_2$ for $i \in \{0, 1, 2\}$. Therefore, Corollary 5.3 allows us to bound Eq. (8.35) by

$$|D|^{\frac{1}{2}+o(1)} \max_{\substack{a,b,c \in \mathbb{F}_q[u] \\ 4ac - b^2 = 4D \\ \deg(b) < \deg(a) \le \deg(c) \le \deg(D)}} q^{\frac{k-\deg(c)}{2}} q^{\frac{k-\deg(a)}{2}(1-\alpha_2)} \beta_2^{2k - 3\frac{k-\deg(a)}{2}} (1+3\gamma_2)^{\frac{k-\deg(c)}{2}} \tag{8.39}$$

where α_2 and $0 < \gamma_2 \leq 1$ satisfy Eq. (5.48), namely

$$0 < \alpha_2 < \min\left\{\frac{1}{2} - 10\log_q(1+2\gamma_2) + \log_q(1+3\gamma_2), \frac{1}{2p} + \frac{\log_q \gamma_2}{p} - 2\log_q(1+2\gamma_2)\right\} \tag{8.40}$$

and $\beta_2 = (1+2\gamma_2)^2$.

We can separate the terms involving k from those involving $a, b, c,$ in Eq. (8.39), rewriting the latter as

$$|D|^{\frac{1}{2}+o(1)} \max_{\substack{a,b,c\in\mathbb{F}_q[u] \\ 4ac-b^2=4D \\ \deg(b)<\deg(a)\leq\deg(c)\leq\deg(D)}} q^{-\frac{\deg(D)}{2}+\frac{\deg(a)}{2}\alpha_2}\beta_2^{3\frac{\deg(a)}{2}}(1+3\gamma_2)^{-\frac{\deg(c)}{2}} q^{k(1-\frac{\alpha_2}{2})}\beta_2^{\frac{k}{2}}(1+3\gamma_2)^{\frac{k}{2}}.$$

Observe that the terms depending on $\deg(a)$ are increasing, and those depending on $\deg(c)$ are decreasing. We may therefore replace $\deg(a)$ by its upper bound $\frac{\deg(D)}{2}$ and $\deg(c)$ by its lower bound $\frac{\deg(D)}{2}$, obtaining

$$\begin{aligned}
&\ll q^{(\frac{1}{2}+o(1))\deg(D)} q^{-\frac{\deg(D)}{2}+\frac{\deg(D)}{4}\alpha_2}\beta_2^{\frac{3\deg(D)}{4}}(1+3\gamma_2)^{-\frac{\deg(D)}{4}} q^{k(1-\frac{\alpha_2}{2})}\beta_2^{\frac{k}{2}}(1+3\gamma_2)^{\frac{k}{2}} \\
&= \left(q^{\frac{\alpha_2}{4}+o(1)}\beta_2^{\frac{3}{4}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{\deg(D)} \left(q^{1-\frac{\alpha_2}{2}}\beta_2^{\frac{1}{2}}(1+3\gamma_2)^{\frac{1}{2}}\right)^{k} \\
&= \left(q^{\frac{\alpha_2}{4}+o(1)}(1+2\gamma_2)^{\frac{3}{2}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{\deg(D)} \left(q^{1-\frac{\alpha_2}{2}}(1+2\gamma_2)(1+3\gamma_2)^{\frac{1}{2}}\right)^{k} \\
&\leq \left(q^{\frac{\alpha_2}{4}+o(1)}(1+2\gamma_2)^{\frac{3}{2}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{2d(1-\delta)} \left(q^{1-\frac{\alpha_2}{2}}(1+2\gamma_2)(1+3\gamma_2)^{\frac{1}{2}}\right)^{d(1+\epsilon)} \\
&= \left(q^{1+\epsilon-\frac{(\delta+\epsilon)\alpha_2}{2}+o(1)}(1+2\gamma_2)^{(4+\epsilon-3\delta)}(1+3\gamma_2)^{\frac{\delta+\epsilon}{2}}\right)^{d}.
\end{aligned} \tag{8.41}$$

We now specialize to

$$\epsilon = \frac{\delta}{12p-1}, \gamma_2 = \frac{3\delta}{4(12p-1)-(15p-4)\delta}, \alpha_2 = \frac{1}{2p} + \frac{\log_q \gamma_2}{p} - \frac{4\gamma_2}{\log q}$$

which satisfies the third inequality in Eq. (8.40) because

$$\alpha_2 = \frac{1}{2p} + \frac{\log_q \gamma_2}{p} - \frac{4\gamma_2}{\log q} < \frac{1}{2p} + \frac{\log_q \gamma_2}{p} - 2\log_q(1+2\gamma_2).$$

To check that the second inequality in Eq. (8.40) holds, we first note that

$$q > 3.57\ldots = e^{\frac{84}{66}} \geq e^{\frac{84}{33(p-1)}} = e^{\frac{42}{4(12p-1)-(15p-4)}\frac{2p}{p-1}}. \tag{8.42}$$

As a result, since $0 < \gamma_2 \leq 1$ we have

$$\gamma_2^{\frac{1}{p}}\frac{(1+2\gamma_2)^8}{(1+3\gamma_2)} \leq (1+2\gamma_2)^7 \leq e^{14\gamma_2} = e^{\frac{42\delta}{4(12p-1)-(15p-4)\delta}} \leq e^{\frac{42}{4(12p-1)-(15p-4)}} < q^{\frac{p-1}{2p}}.$$

Taking logarithms to base q gives

$$\frac{\log_q \gamma_2}{p} + 8\log_q(1+2\gamma_2) - \log_q(1+3\gamma_2) \leq \frac{p-1}{2p} \tag{8.43}$$

or equivalently

$$\frac{1}{2p} + \frac{\log_q \gamma_2}{p} - 2\log_q(1+2\gamma_2) \le \frac{1}{2} - 10\log_q(1+2\gamma_2) + \log_q(1+3\gamma_2)$$

which implies that the second inequality in Eq. (8.40) holds as the third does.

Multiplying Eq. (8.41) by the factor d^2 from Eq. (8.24), we absorb it, together with $q^{o(d)}$, into an exponential savings in d, so we get

$$\begin{aligned}
&d^2 \left(q^{1+\frac{\delta}{12p-1}-\frac{6p\delta\alpha_2}{12p-1}+o(1)} (1+2\gamma_2)^{(4-\frac{36p-4}{12p-1}\delta)} (1+3\gamma_2)^{\frac{6p\delta}{12p-1}} \right)^d \\
&\ll \left(q^{1+\frac{\delta}{12p-1}-\frac{6p\delta\alpha_2}{12p-1}} e^{2\gamma_2\left(4-\frac{36p-4}{12p-1}\delta\right)+3\gamma_2\frac{6p\delta}{12p-1}} \right)^d \\
&= \left(q^{1+\frac{\delta}{12p-1}-\frac{3\delta}{12p-1}} \gamma_2^{-\frac{6\delta}{12p-1}} e^{\frac{24p\gamma_2\delta}{12p-1}+2\gamma_2\left(4-\frac{36p-4}{12p-1}\delta\right)+3\gamma_2\frac{6p\delta}{12p-1}} \right)^d \\
&= \left(q^{1-\frac{2\delta}{12p-1}} \gamma_2^{-\frac{6\delta}{12p-1}} e^{\gamma_2\frac{8(12p-1)-(30p-8)\delta}{12p-1}} \right)^d \\
&= \left(q^{1-\frac{2\delta}{12p-1}} \gamma_2^{-\frac{6\delta}{12p-1}} e^{\frac{6\delta}{12p-1}} \right)^d \\
&= \left(q^d\right)^{1-\frac{2\delta}{12p-1}\left(1-3\log_q(e/\gamma_2)\right)} \\
&= \left(q^d\right)^{1-\frac{2\delta}{12p-1}\left(1-3\log_q(e^{\frac{4(12p-1)-(15p-4)\delta}{3\delta}})\right)}.
\end{aligned}$$

In particular, by our definition of γ in Eq. (8.2), this is bounded by $q^{\gamma d}$. This also verifies the first inequality in Eq. (8.40).

In case D is indefinite, we get from Notation 7.46, Corollary 7.45 and Proposition 7.15 that the sum in absolute value in Eq. (8.24) equals

$$\sum_{(s,a,b,c)\in S_D} \omega_s \sum_{\substack{x,y\in\mathbb{F}_q[u] \\ \gcd(x,y)=1, y\neq 0 \\ \deg(x)\le\frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2} \\ \deg(y)\le\frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2} \\ ax^2+bxy+cy^2\in\mathcal{M}_k}} \mu(ax^2+bxy+cy^2) e\left(\frac{h\overline{x}}{y}\right). \tag{8.44}$$

The condition $y \neq 0$ is justified here in the same way as in the definite case, only that here we need to refer to Eq. (7.89) instead of Eq. (7.55).

We check that the assumptions of Proposition 7.15 are satisfied in this case. From our initial assumption on $\deg_u(F)$ we get that

$$\deg(h) \le k-d-1 = \deg(A)-d-1 < \deg(A)-\frac{\deg(D)}{2}-1 \le \deg(A)-\deg(b)-1$$

so Eq. (7.44) is satisfied. Moreover we have

$$\deg(h)+\deg(a)+\deg(x)-\deg(A) < k-d+\frac{\deg(D)}{2}-s+\frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2}-k = \frac{\deg(D)}{4}-\frac{s}{2}-d+\frac{k}{2} \leq \frac{d(1-\delta)}{2}-d+\frac{(1+\epsilon)d}{2} = \frac{d(\epsilon-\delta)}{2} \leq -1 \leq \deg(y)-1$$

so Eq. (7.45) is satisfied as well.

Arguing as in the definite case, we arrive at
(8.45)

$$\sum_{(s,a,b,c)\in S_D} \omega_s \sum_{\substack{y\in\mathbb{F}_q[u]\setminus\{0\} \\ \deg(y)\leq \frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2}}} \left| \sum_{\substack{x\in S_{s,a,b,c,y} \\ \gcd(x,y)=1}} \mu(ax^2+bxy+cy^2)e\left(\frac{h\overline{x}}{y}\right) \right|$$

where

$$S_{s,a,b,c,y} = \{x\in\mathbb{F}_q[u] : \deg(x)\leq \frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2},\ ax^2+bxy+cy^2\in\mathcal{M}_k\}.$$

We can rewrite the set above as

$$S_{s,a,b,c,y} = \{x\in\mathbb{F}_q[u] : \deg(x)\leq \frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2},\ a_{(0)}x_{(0)}^2+b_{(0)}x_{(0)}y_{(0)}+c_{(0)}y_{(0)}^2 = 1\}$$

where (for instance) $x_{(0)}, y_{(0)}$ are the coefficients of x, y in degrees

$$\frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2}, \quad \frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2} \tag{8.46}$$

as in Notation 7.46. Therefore the set $S_{a,b,c,y}$ is a disjoint union of at most two intervals in $\mathbb{F}_q[u]$, corresponding to the solutions of the (possibly degenerate) quadratic equation in $x_{(0)}$.

As in the definite case it is thus enough to control

$$\sum_{(s,a,b,c)\in S_D} \omega_s \sum_{\substack{y\in\mathbb{F}_q[u]\setminus\{0\} \\ \deg(y)\leq \frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2}}} \left| \sum_{\substack{x\in \mathcal{I}_{s,a,b,c,y} \\ \gcd(x,y)=1}} \mu(F_y(x))e\left(\frac{h\overline{x}}{y}\right) \right| \tag{8.47}$$

where $F_y(T)$ is the separable polynomial $aT^2+byT+cy^2$, and $\mathcal{I}_{s,a,b,c,y}$ is an interval in $\mathbb{F}_q[u]$ with

$$\deg(\mathcal{I}_{s,a,b,c,y}) \leq \frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2}. \tag{8.48}$$

Applying Corollary 5.3 with

$$n=\frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2}, \quad c_1=k, \quad c_2=\frac{\deg(D)}{4}-\frac{s}{2}-\frac{k}{2}, \quad c_3=\frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2}$$

we get a bound of

$$q^{\left(\frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2}\right)+\left(\frac{k}{2}-\frac{\deg(D)}{4}+\frac{s}{2}\right)(1-\alpha_2)} \beta_2^{2k+3\left(\frac{\deg(D)}{4}-\frac{s}{2}-\frac{k}{2}\right)} (\beta_2^0+1)(1+3\gamma_2)^{\frac{k}{2}-\frac{\deg(D)}{4}-\frac{s}{2}}$$

for the sum over y in Eq. (8.47). The above can be rewritten as

$$2\left(q^{\frac{2-\alpha_2}{2}}\beta_2^{\frac{1}{2}}(1+3\gamma_2)^{\frac{1}{2}}\right)^k\left(q^{-\frac{2-\alpha_2}{4}}\beta_2^{\frac{3}{4}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{\deg(D)}\left(q^{-\frac{\alpha_2}{2}}\beta_2^{-\frac{3}{2}}(1+3\gamma_2)^{-\frac{1}{2}}\right)^s$$
$$\ll\left(q^{\frac{2-\alpha_2}{2}}\beta_2^{\frac{1}{2}}(1+3\gamma_2)^{\frac{1}{2}}\right)^k\left(q^{-\frac{2-\alpha_2}{4}}\beta_2^{\frac{3}{4}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{\deg(D)}$$

since $s \geq 0$ and the term being raised to the power s is a product of factors that are individually at most 1, hence is bounded by 1.

Summing over S_D we get from Corollary 7.47 that

$$\left(q^{\frac{2-\alpha_2}{2}}\beta_2^{\frac{1}{2}}(1+3\gamma_2)^{\frac{1}{2}}\right)^k\left(q^{-\frac{2-\alpha_2}{4}}\beta_2^{\frac{3}{4}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{\deg(D)}\sum_{(s,a,b,c)\in S_D}\omega_s =$$
$$\left(q^{1-\frac{\alpha_2}{2}}\beta_2^{\frac{1}{2}}(1+3\gamma_2)^{\frac{1}{2}}\right)^k\left(q^{\frac{\alpha_2}{4}+o(1)}\beta_2^{\frac{3}{4}}(1+3\gamma_2)^{-\frac{1}{4}}\right)^{\deg(D)}.$$

This is identical to the bound obtained in the definite case, more specifically on the second line of Eq. (8.41). We may thus give the same argument (choosing the same $\epsilon, \alpha_2, \gamma_2$), and again obtain a bound which is $\ll q^{\gamma d}$. □

Remark 8.2. The optimal value of ϵ depends on q, p, δ. As δ becomes smaller, the contribution of the range $d < k < (1+\epsilon)d$ becomes more difficult to bound, forcing us to lower ϵ. As q grows, this contribution becomes easier to bound (even compared to the contribution from $k \geq (1+\epsilon)d$), allowing us to raise ϵ.

There is likely no closed-form formula for the exact optimal value of ϵ, and if there was it would make our formulas distressingly complicated, so we have chosen to approximate. Specifically, we have chosen ϵ to roughly optimize the range of q, δ in which we have some savings, rather than to optimize the amount of savings when q is large and $\delta \sim 1$. (This would require a much larger value of ϵ, close to $\frac{1}{4p+1}$, obtaining power savings tending to $\frac{1}{8p^2+4p}$ as $q \to \infty$ and $\delta \to 1$ with p fixed.)

The specific nature of our choice of ϵ is that it makes the first lower bound in Eq. (8.1) proportional to δ^{-3}. We have chosen ϵ this way because making that lower bound proportional to δ^{-2} is impossible, requiring $\epsilon = 0$. We could choose an intermediate growth rate (the optimum should be roughly $\delta^{-2}\log(\delta^{-1})$), but this would again give a messier formula, for a mild gain.

9. Trace functions vs Primes

Lemma 9.1. *For a prime $\pi \in \mathbb{F}_q[u]$ and an integer $k \geq \deg(\pi)$ we have*

$$\sum_{\substack{A\in\mathcal{M}_k\\ \pi|A}}\mu(A)=\begin{cases}-1 & k\equiv 0 \mod \deg(\pi)\\ q & k\equiv 1 \mod \deg(\pi)\\ 0 & \textit{otherwise.}\end{cases}\tag{9.1}$$

Proof. We rewrite our sum as

$$\begin{aligned}\sum_{B\in\mathcal{M}_{k-\deg(\pi)}}\mu(B\pi) &= \sum_{\substack{B\in\mathcal{M}_{k-\deg(\pi)}\\ \pi\nmid B}}\mu(B\pi) = \mu(\pi)\sum_{\substack{B\in\mathcal{M}_{k-\deg(\pi)}\\ \pi\nmid B}}\mu(B) \\ &= \sum_{\substack{B\in\mathcal{M}_{k-\deg(\pi)}\\ \pi\mid B}}\mu(B) - \sum_{C\in\mathcal{M}_{k-\deg(\pi)}}\mu(C)\end{aligned} \tag{9.2}$$

and argue by induction on k. For the base case $k < 2\deg(\pi)$, the last sum over B above is empty, so we are only left with minus the sum over C which equals -1 in case $k = \deg(\pi)$, equals q in case $k = \deg(\pi)+1$, and otherwise vanishes by [Ros02, Exercise 2.12]. This matches the right hand side of Eq. (9.1), so the base case is established. If $k \geq 2\deg(\pi)$ then the sum over C vanishes, and the lemma follows from the induction hypothesis. □

We shall now deduce Corollary 1.15 from Lemma 9.1, Theorem 1.10, and Theorem 1.13. Our task is to show that for a Dirichlet character χ of prime conductor $\pi \in \mathbb{F}_q[u]$, where q is a power of a prime number p satisfying $q > 4e^2p^2$, we have

$$\sum_{f\in\mathcal{M}_n}\chi(f+h)\Lambda(f) = O\left(|\mathcal{M}_n|^{\frac{1+\zeta}{2}+\epsilon}|\pi|^{\log_q(3)} + |\mathcal{M}_n|^{1+\epsilon}|\pi|^{-1}\right)$$

for any $h \in \mathbb{F}_q[u]$, $\epsilon > 0$, and $\zeta = \left(1+\frac{1}{p}-\frac{\log_q(4e^2p^2)}{p}\right)^{-1}$.

Proof of Corollary 1.15. The identity $\Lambda = (\mu\cdot\deg)*(-1)$ gives

$$\sum_{f\in\mathcal{M}_n}\chi(f+h)\Lambda(f) = -\sum_{k=1}^{n}k\sum_{A\in\mathcal{M}_k}\mu(A)\sum_{B\in\mathcal{M}_{n-k}}\chi(AB+h). \tag{9.3}$$

For any $k \leq \zeta n$ and any $A \in \mathcal{M}_k$ that is not divisible by π, the contribution to Eq. (9.3) is

$$\ll n\sum_{\substack{C\in\mathbb{F}_q[u]\\ \deg(C)<n-k}}\chi(AC+AT^{n-k}+h) \tag{9.4}$$

where $C = B - T^{n-k}$. Since $\pi\nmid A$, we are in the situation of Example 1.7, so we can invoke Theorem 1.10 and get that the above is $\ll nq^{\frac{n-k}{2}}|\pi|^{\log_q(3)}$. The contribution from all such k and A is thus

$$\ll \max_{k\leq\zeta n} n^2|\mathcal{M}_k|q^{\frac{n-k}{2}}|\pi|^{\log_q(3)} \leq n^2q^{\frac{n(1+\zeta)}{2}}|\pi|^{\log_q(3)} \ll q^{\frac{n(1+\zeta+2\epsilon)}{2}}|\pi|^{\log_q(3)} \tag{9.5}$$

for any $\epsilon > 0$.

The contribution to Eq. (9.3) of all $\deg(\pi) \leq k \leq \zeta n$ and all $A \in \mathcal{M}_k$ that are divisible by π is

$$\ll \max_{k\geq \deg(\pi)} n^2 \left| \sum_{\substack{A\in\mathcal{M}_k\\ \pi|A}} \mu(A) \sum_{B\in\mathcal{M}_{n-k}} \chi(h)\right| = \max_{k\geq\deg(\pi)} n^2 q^{n-k}|\chi(h)| \left|\sum_{\substack{A\in\mathcal{M}_k\\ \pi|A}}\mu(A)\right|$$

$$\ll \max_{k\geq\deg(\pi)} n^2 q^{n-k} \ll n^2 q^{n-\deg(\pi)}$$

in view of Lemma 9.1.

The contribution of all $k \geq \zeta n$ to Eq. (9.3) is

$$\ll \max_{k\geq\zeta n} n^2 \left|\sum_{B\in\mathcal{M}_{n-k}}\sum_{A\in\mathcal{M}_k}\mu(A)\chi(AB+h)\right| \ll \max_{\substack{k\geq\zeta n\\ B\in\mathcal{M}_{n-k}}} n^2q^{n-k}\left|\sum_{A\in\mathcal{M}_k}\mu(A)\chi(AB+h)\right|$$

and by Theorem 1.13 this is

$$\ll \max_{k\geq\zeta n} n^2 q^{n-k}|\mathcal{M}_k|^{1-\frac{1}{2p}+\frac{\log_q(2ep)}{p}}|\pi|^{\log_q(3)} \ll \max_{k\geq\zeta n} q^{n-\frac{k}{2p}+\frac{k\log_q(2ep)}{p}+\epsilon n}|\pi|^{\log_q(3)}$$

for any $\epsilon > 0$. Since $q > 4e^2p^2$ by assumption, the above is largest once k is as small as possible, so we put $k = \zeta n$ and get

$$q^{n(1-\frac{\zeta}{2p}+\frac{\zeta\log_q(2ep)}{p}+\epsilon)}|\pi|^{\log_q(3)}. \tag{9.6}$$

One readily checks that our choice of ζ in Eq. (1.34) (recalled before the proof) is such that the bounds in Eq. (9.5) and Eq. (9.6) coincide, giving the final bound

$$q^{\frac{n(1+\zeta)}{2}+\epsilon n}|\pi|^{\log_q(3)} + q^{n(1+\epsilon)-\deg(\pi)}. \tag{9.7}$$

□

Proposition 9.2. *Let $\pi \in \mathbb{F}_q[u]$ be a prime, and let $t\colon \mathbb{F}_q[u]/(\pi) \to \mathbb{C}$ be an infinitame trace function arising from a sheaf $\mathcal{F}$ whose geometric monodromy representation does not admit the trivial representation $\overline{\mathbb{Q}_\ell}$ as a quotient. For an integer $n \geq \deg(\pi)$ and a polynomial $h \in \mathbb{F}_q[u]$ we then have*

$$\left|\sum_{\substack{f\in\mathbb{F}_q[u]\\ \deg(f)<n}} t(f)e\left(\frac{hf}{\pi}\right)\right| \leq c(t)q^n|\pi|^{-\frac{1}{2}}. \tag{9.8}$$

Proof. In every residue class mod π there are $q^{n-\deg(\pi)}$ polynomials of degree less than n, so

$$\left|\sum_{\substack{f\in\mathbb{F}_q[u]\\ \deg(f)<n}} t(f)e\left(\frac{hf}{\pi}\right)\right| = \frac{q^n}{|\pi|}\left|\sum_{f\in\mathbb{F}_q[u]/(\pi)} t(f)e\left(\frac{hf}{\pi}\right)\right|. \tag{9.9}$$

Setting $\mathcal{F}_h = \mathcal{F} \otimes \mathcal{L}_\psi(hx)$, and using the Grothendieck-Lefschetz trace formula, we get

(9.10)
$$\left| \sum_{f \in \mathbb{F}_q[u]/(\pi)} t(f) e\left(\frac{hf}{\pi}\right) \right| = \left| \sum_{y \in \mathbb{A}^1(\mathbb{F}_q[u]/(\pi))} t_{\mathcal{F}_h}(y) \right| \leq \sum_{i=0}^{2} \left| \mathrm{tr}(\mathrm{Frob}_{|\pi|}, H^i_c(\mathbb{A}^1_{\overline{\mathbb{F}_q[u]/(\pi)}}, \overline{\mathcal{F}_h})) \right|$$

where $\overline{\mathcal{F}_h}$ is the base change of $\mathcal{F}_h$ to the algebraic closure of $\mathbb{F}_q[u]/(\pi)$.

For $i = 0$ there is no cohomology by the fact that $\mathcal{F}$ has no finitely supported sections, Lemma 2.15(5), and Lemma 2.13(2). For $i = 2$ the cohomology equals the geometric monodromy coinvariants of $\mathcal{F}_h$. These vanish for $h = 0$ in view of our assumption that the geometric monodromy representation of $\mathcal{F} = \mathcal{F}_0$ does not admit trivial quotients, and also vanish for $h \neq 0$ because $\mathcal{F}$ is infinitame hence its geometric monodromy representation does not have Artin-Schreier quotients.

Consequently, using Lemma 2.10 and Eq. (2.22) we get

$$\dim H^1_c(\mathbb{A}^1_{\overline{\mathbb{F}_q[u]/(\pi)}}, \overline{\mathcal{F}_h}) = -\chi(\mathbb{A}^1_{\overline{\mathbb{F}_q[u]/(\pi)}}, \overline{\mathcal{F}_h}) = \mathbf{sw}_\infty(\mathcal{F}_h) - \mathbf{r}(\mathcal{F}_h) + \sum_{x \in |\mathbb{A}^1|} \mathbf{c}_x(\mathcal{F}_h).$$

From Lemma 2.13(5) and Lemma 3.10(5) we get that the above equals

$$\mathbf{sw}_\infty(\mathcal{F}_h) - \mathbf{r}(\mathcal{F}) + c_F(\mathcal{F}_h) - \mathbf{sw}'_\infty(\mathcal{F}_h). \tag{9.11}$$

In case $h = 0$ the above reduces to $c(t) - r(t)$ because $\mathcal{F}$ is infinitame. In case $h \neq 0$ we still have $c_F(\mathcal{F}_h) = c_F(\mathcal{F})$ in view of Definition 3.8, and since $\mathcal{F}$ is infinitame, the local monodromy at ∞ of $\mathcal{F}_h$ is a direct sum of $\mathbf{r}(\mathcal{F})$ copies of the local monodromy of $\mathcal{L}_\psi(hx)$, so Eq. (9.11) equals

$$c_F(\mathcal{F}) + \mathbf{r}(\mathcal{F})\mathrm{slope}_\infty(\mathcal{L}_\psi(hx)) - \mathbf{r}(\mathcal{F}) \max\{\mathrm{slope}_\infty(\mathcal{L}_\psi(hx)) - 1, 0\} - \mathbf{r}(\mathcal{F})$$

where the slopes are taken with respect to the representation of the inertia group I_∞ on the generic fiber. Since $\mathrm{slope}_\infty(\mathcal{L}_\psi(hx)) = 1$ by Lemma 2.15(3), the above equals $c(t)$.

Since $\mathcal{F}_h$ is mixed of nonpositive weights by Lemma 2.13(4), each eigenvalue of $\mathrm{Frob}_{|\pi|}$ acting on $H^1_c(\mathbb{A}^1_{\overline{\mathbb{F}_q[u]/(\pi)}}, \overline{\mathcal{F}_h})$ is of absolute value at most $|\pi|^{\frac{1}{2}}$ by Deligne's bound, so Eq. (9.10) is bounded by

$$\dim H^1_c(\mathbb{A}^1_{\overline{\mathbb{F}_q[u]/(\pi)}}, \overline{\mathcal{F}_h})|\pi|^{\frac{1}{2}} \leq c(t)|\pi|^{\frac{1}{2}}. \tag{9.12}$$

It follows from Eq. (9.9) that our original sum is bounded by

$$q^n|\pi|^{-1}c(t)|\pi|^{\frac{1}{2}} = c(t)q^n|\pi|^{-\frac{1}{2}} \tag{9.13}$$

as required. □

Corollary 9.3. *With assumptions as above, for an integer $0 \le d < \deg(\pi)$ we have*

$$\left| \sum_{\substack{f \in \mathbb{F}_q[u] \\ \deg(f) < d}} t(f) \right| \le c(t) |\pi|^{\frac{1}{2}}. \tag{9.14}$$

Proof. By Proposition 6.2 and Proposition 9.2 we have

$$\begin{aligned} \left| \sum_{\substack{f \in \mathbb{F}_q[u] \\ \deg(f) < d}} t(f) \right| &= \frac{q^d}{|\pi|} \left| \sum_{\substack{h \in \mathbb{F}_q[u] \\ \deg(h) < \deg(\pi) - d}} \sum_{\substack{f \in \mathbb{F}_q[u] \\ \deg(f) < \deg(\pi)}} t(f) e\left(\frac{hf}{\pi}\right) \right| \\ &\le \sup_{\substack{h \in \mathbb{F}_q[u] \\ \deg(h) < \deg(\pi) - d}} \left| \sum_{\substack{f \in \mathbb{F}_q[u] \\ \deg(f) < \deg(\pi)}} t(f) e\left(\frac{hf}{\pi}\right) \right| \le c(t) q^{\deg(\pi)} |\pi|^{-\frac{1}{2}} = c(t)|\pi|^{\frac{1}{2}}. \end{aligned}$$

□

We shall now deduce Corollary 1.14.

Proof of Corollary 1.14. The identity $\Lambda = (\mu \cdot \deg) * (-1)$ gives

$$\sum_{f \in \mathcal{M}_n} t(f)\Lambda(f) = -\sum_{k=1}^{n} k \sum_{A \in \mathcal{M}_k} \mu(A) \sum_{B \in \mathcal{M}_{n-k}} t(AB). \tag{9.15}$$

For any $k \le \zeta n$ and any $A \in \mathcal{M}_k$ that is not divisible by π, the contribution to Eq. (9.15) is

$$\ll n \sum_{\substack{C \in \mathbb{F}_q[u] \\ \deg(C) < n-k}} t(AC + AT^{n-k}) \tag{9.16}$$

where $C = B - T^{n-k}$. Since $\pi \nmid A$, the function $C \mapsto t(AC + AT^{n-k})$ satisfies the hypothesis of Proposition 9.2 and Corollary 9.3, so the above is bounded by

$$nc(t)|\pi|^{\frac{1}{2}} \left(1 + \frac{q^{n-k}}{|\pi|}\right). \tag{9.17}$$

The contribution from all such k and A is thus

$$\ll \max_{k \le \zeta n} n^2 c(t) |\pi|^{\frac{1}{2}} |\mathcal{M}_k| \left(1 + \frac{q^{n-k}}{|\pi|}\right) \ll c(t)|\pi|^{\frac{1}{2}} \left(q^{n(\zeta+\epsilon)} + \frac{q^{n(1+\epsilon)}}{|\pi|}\right) \tag{9.18}$$

for any $\epsilon > 0$.

The contribution to Eq. (9.15) of all $\deg(\pi) \leq k \leq \zeta n$ and all $A \in \mathcal{M}_k$ that are divisible by π is

$$\ll \max_{k \geq \deg(\pi)} n^2 \left| \sum_{\substack{A \in \mathcal{M}_k \\ \pi | A}} \mu(A) \sum_{B \in \mathcal{M}_{n-k}} t(0) \right| = \max_{k \geq \deg(\pi)} n^2 q^{n-k} |t(0)| \left| \sum_{\substack{A \in \mathcal{M}_k \\ \pi | A}} \mu(A) \right|$$
$$\ll \max_{k \geq \deg(\pi)} n^2 q^{n-k} r(t) \ll n^2 q^{n-\deg(\pi)} r(t)$$

in view of Lemma 9.1.

The contribution of all $k \geq \zeta n$ to Eq. (9.15) is

$$\ll \max_{k \geq \zeta n} n^2 \left| \sum_{B \in \mathcal{M}_{n-k}} \sum_{A \in \mathcal{M}_k} \mu(A) t(AB) \right| \ll \max_{\substack{k \geq \zeta n \\ B \in \mathcal{M}_{n-k}}} n^2 q^{n-k} \left| \sum_{A \in \mathcal{M}_k} \mu(A) t(AB) \right|$$

and by Theorem 1.13 this is

$$\begin{aligned} &\ll n^2 \max_{k \geq \zeta n} q^{n-k} |\mathcal{M}_k|^{1 - \frac{1}{2p} + \frac{\log_q(2ep)}{p}} |\pi|^{\log_q \left(r(t) \left(1 + \frac{1}{2p}\right) + \frac{c(t)}{2p} \right)} \\ &\ll \max_{k \geq \zeta n} q^{n - \frac{k}{2p} + \frac{k \log_q(2ep)}{p} + \epsilon n} |\pi|^{\log_q \left(r(t) \left(1 + \frac{1}{2p}\right) + \frac{c(t)}{2p} \right)} \end{aligned} \tag{9.19}$$

for any $\epsilon > 0$. The above is largest once $k = \zeta n$ so we have the bound

$$q^{n - \frac{\zeta n}{2p} + \frac{\zeta n \log_q(2ep)}{p} + \epsilon n} |\pi|^{\log_q \left(r(t) \left(1 + \frac{1}{2p}\right) + \frac{c(t)}{2p} \right)} \tag{9.20}$$

It follows from the choice of ζ in Eq. (1.32), and our assumption on n that

$$\begin{aligned} c(t) |\pi|^{\frac{1}{2}} q^{n(\zeta + \epsilon)} = c(t) q^{n(\zeta+\epsilon) + \frac{1}{2}\deg(\pi)} &\leq c(t) q^{n(\frac{1}{1+2\delta} + \zeta + \epsilon)} \\ &\ll q^{n(1 - \frac{\zeta}{2p} + \frac{\zeta \log_q(2ep)}{p} + \epsilon)} |\pi|^{\log_q \left(r(t) \left(1 + \frac{1}{2p}\right) + \frac{c(t)}{2p} \right)} \end{aligned} \tag{9.21}$$

so the bound in Eq. (9.20) dominates the first summand in Eq. (9.18), hence we can use

$$q^{n(1 - \frac{\zeta}{2p} + \frac{\zeta \log_q(2ep)}{p} + \epsilon)} |\pi|^{\log_q \left(r(t) \left(1 + \frac{1}{2p}\right) + \frac{c(t)}{2p} \right)} + (c(t) + r(t)) \frac{q^{n(1+\epsilon)}}{|\pi|^{\frac{1}{2}}} \tag{9.22}$$

as a final bound. □

10. Acknowledgments

We are grateful to de Jong for a very helpful discussion of the proof of Lemma 4.6. We would also like to thank the referee for a large number of helpful suggestions.

References

[ABSR15] J. Andrade, L. Bary-Soroker, Z. Rudnick, *Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$*, Number fields and function fields: coalescences, contrasts and emerging applications. Phil. Trans. R. Soc. A 373, 2015.

[BBD82] A. A. Beilinson, J. Bernstein, P. Deligne, *Faisceaux Pervers*, Asterisque 100 (1982).

[BR20] F. Balestrieri, N. Rome, *Average Bateman-Horn for Kummer polynomials*, arXiv preprint, https://arxiv.org/abs/2005.11835 , 2020.

[BSE21] L. Bary-Soroker, A. Entin (2021). *Explicit Hilbert's Irreducibility Theorem in Function Fields*, Contemporary Math. 767, Abelian Varieties and Number Theory, 125-134.

[Bur] D. A. Burgess, *On Dirichlet characters of polynomials*, Proc. London Math. Soc. 13 (1963) 537-548.

[MC09] M. C. Chang, (2009). *On character sums of binary quadratic forms*, Jour. Num. Th. 129(9), 2064-2071.

[Coh81] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3) 43 (1981), 2, 227-250.

[Ch65] S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Mathematics and its Applications, Gordon and Breach Science Publishers, New York, 1965.

[CDO03] D. C. Cohen, A. Dimca, and P. Orlik, Nonresonance conditions for arrangements, *Annales de l'Institut Fourier*, **53** (2003), 1883-1896.

[CCG08] B. Conrad, K. Conrad, R. Gross (2008) *Prime specialization in genus 0*, Trans. AMS, 360(6), 2867-2908.

[dlB15] R. de la Bretéche (2015). *Plus grand facteur premier de valeurs de polynômes aux entiers*, Acta Arith. 169, 221-250.

[Ent16] A. Entin, (2016). *On the Bateman-Horn conjecture for polynomials over large finite fields*, Compositio Math. 152(12), 2525-2544.

[Ent21] A. Entin, (2021). *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, IMRN, 14, 10409-10441.

[Fe20] T. Feng, (2020). *Nearby cycles of parahoric shtukas, and a fundamental lemma for base change*, Selecta Mathematica, 26(2), 1-59.

[Flo17] A. Florea, *The fourth moment of quadratic Dirichlet L-functions over function fields*, Geom. Funct. Anal. Vol. 27 (2017) 541-595.

[FH17] N. Frantzikinakis, B. Host, (2017). *Higher order Fourier analysis of multiplicative functions and applications*, JAMS, 30(1), 67-157.

[FKM15] É. Fouvry, E. Kowalski, P. Michel, (2015). *Algebraic twists of modular forms and Hecke orbits*, Geom. Funct. Anal. 25, 2, 580-657.

[FKM21] É. Fouvry, E. Kowalski, P. Michel, (2021). *On the conductor of cohomological transforms*, Annales de la Faculté des sciences de Toulouse, Mathématiques, 6, 30, 1, 203-254.

[FKM14] E. Fouvry, E. Kowalski, P. Michel, (2014). *Algebraic trace functions over the primes*, Duke Math. J. 163(9), 1683-1736.

[FKMRRS17] E. Fouvry, E. Kowalski, P. Michel, C. Raju, J. Rivat, K. Soundararajan, (2017). *On short sums of trace functions*, Annales de l'Institut Fourier, 67, 1, 423-449.

[FKMS19] É. Fouvry, E. Kowalski, P. Michel, W. Sawin, (2019). *Lectures on applied ℓ-adic cohomology*, Contemporary Math. Analytic Methods in Arithmetic Geometry, 740, 113-196.

[FM98] E. Fouvry, P. Michel, (1998). *Sur certaines sommes d'exponentielles sur les nombres premiers*, Ann. scient. Ec. Norm. Sup., 4e serie, t. 31, 93-130.

[FI98] J. Friedlander, H. Iwaniec, (1998). *The polynomial x^2+y^4 captures its primes*, Ann. Math. 148, 945-1040.

[GKZ08] I. Gelfand, M. Kapranov, A. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Springer Science & Business Media, 2008.

[Hay66] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. 11:461-488, 1966.

[HM04] R. Heath-Brown, B. Moroz, (2004). *On the representation of primes by cubic polynomials in two variables*, Proc. LMS 88(2), 289-312.

[Hel06] H. Helfgott, *The parity problem for reducible polynomials*, J. London Math. Soc. 73 (2006), 415-435.

[Hoo63] C. Hooley, 1963, *On the number of divisors of quadratic polynomials*, Acta Math. 110, 97-114.

[Irv14] A. J. Irving, (2014). *Average bounds for Kloosterman sums over primes*, Funct. Approx. Comment. Math. 51(2): 221-235.

[Iw78] H. Iwaniec, (1978). *Almost-primes represented by quadratic polynomials*, Invent. math. 47(2), 171-188.

[IK04] H. Iwaniec, E. Kowalski, *Analytic number theory*, Vol. 53. Amer. Math. Soc. 2004.

[Ka88] N. Katz, (1988). *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Princeton university press.

[KL85] N. Katz, G. Laumon, (1985), *Transformation de Fourier et majoration de sommes exponentielles*, Publications Mathématiques de l'IHÉS 62, 145-202.

[KR14] L. Kindler, K. Rülling, (2014). *Introductory course on ℓ-adic sheaves and their ramification theory on curves*, arXiv preprint, 1409.6899.

[Kow16] E. Kowalski, (2016). *The geometric Bunyakowsky problem*, preprint.

[La18] A. Lachand, (2018) *Fonctions arithmétiques et formes binaires irréductibles de degré* 3, Annales de l'Institut Fourier, 68, 3, 1297-1363.

[La81] G. Laumon, (1981), *Semi-continuité du conducteur de Swan (d'après P. Deligne)*, Astérisque, 82-83, p. 173-219.

[LO12] R. Lemke-Oliver, *Almost-primes represented by quadratic polynomials*, Acta Arith., 151 (2012), pp. 241-261.

[MRT19] K. Matomäki, M. Radziwiłł, T. Tao, (2019). *Fourier uniformity of bounded multiplicative functions in short intervals on average*, Invent. math. 1-58.

[May20] J. Maynard, (2020). *Primes represented by incomplete norm forms*, Forum Math. Pi (8).

[Mer19] J. Merikoski, (2019). *Largest prime factor of $n^2 + 1$*, arXiv preprint, 1908.08816.

[Mil13] J. Milne, *Lectures on Étale Cohomology*, preprint, `http://www.jmilne.org/math/CourseNotes/LEC.pdf`.

[Pol06] P. Pollack, (2006). *An explicit approach to Hypothesis H for polynomials over a finite field*, Proc. Anatomy of Integers Conf. Montréal.

[Rakh18] Z. Rakhmonov, (2018). *Sums of Values of Nonprincipal Characters over Shifted Primes*, Irregularities in the Distribution of Prime Numbers, 187-217, Springer.

[RL20] A. Rojas-León, (2020). *Tensor and convolution direct image of l-adic sheaves*, Mathematika 66,pp, 125–143.

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics Vol. 210. Springer Science & Business Media, 2002.

[RG17] E. Roditty-Gershon, (2017). *Square-full polynomials in short intervals and in arithmetic progressions*, Research in Number Theory, 3(1), 3.

[Rud10] Z. Rudnick, (2010). *Traces of high powers of the Frobenius class in the hyperelliptic ensemble*, Acta Arith. 143, 81-99.

[SGA1] A. Grothendieck, *Revêtements étales et groupe fondamental*, Lecture Notes in Math. 224, Springer-Verlag, NY, 1971.

[SGA4-3] M. Artin, A. Grothendieck. J.-L. Verdier, eds, *Séminaire de Géométrie Algébrique du Bois Marie - 1963-64 - Théorie des topos et cohomologie étale des schémas - (SGA 4) - vol. 3*, Lecture Notes in Mathematics **305** Springer-Verlag, 1972.

[SGA4$\frac{1}{2}$] P. Deligne, ed, *Séminaire de Géométrie Algébrique du Bois Marie - Cohomologie étale - (SGA 4$\frac{1}{2}$)*, Lecture Notes in Mathematics **569** Springer-Verlag, 1977.

[SGA5] A. Grothendieck, 1977), *Séminaire de Géométrie Algébrique du Bois Marie – 1965-66 – Cohomologie ℓ-adique et Fonctions L – (SGA 5)*, Lecture notes in mathematics, **589**, Berlin; New York: Springer-Verlag.

[Saw20] W. Sawin, *Singularities and vanishing cycles in number theory over function fields*, arXiv preprint, 2020.

[SFFK21] W. Sawin, A. Forey, J. Fresán, E. Kowalski, *Quantitative sheaf theory*, preprint, https://arxiv.org/abs/2101.00635, 2021.

[SS19] W. Sawin, M. Shusterman (2019) *On the Chowla and twin primes conjectures over $\mathbb{F}_q[T]$*, arXiv:1808.04001

[Sz09] T. Szamuely, (2009). *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press.

[WX16] J. Wu, P. Xi, (2016). *Arithmetic exponent pairs for algebraic trace functions and applications*, with an appendix by W. Sawin, preprint, arXiv:1603.07060.

[Yau19] K. H. Yau, (2019). *On primes represented by quartic polynomials on average*, arXiv preprint 1908.09439.

Department of Mathematics, Columbia University, New York, NY 10027, USA

Email address: sawin@math.columbia.edu

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA

Email address: mshusterman@math.harvard.edu