Electronic Colloquium on Computational Complexity, Report No. 69 (2024)

Character sums over AG codes

Swastik Kopparty[*] Amnon Ta-Shma[†] Kedem Yakirevitch[‡]

April 7, 2024

Abstract

The Stepanov-Bombieri proof of the Hasse-Weil bound also gives non-trivial bounds on the bias of character sums over curves with small genus, for any low-degree function f that is not completely biased. For high genus curves, and in particular for curves used in AG codes over constant size fields, the technique fails to prove any non-trivial result. We significantly strengthen the Stepanov-Bombieri approach and obtain strong bounds on the bias of character sums over high genus curves. For example, we show that the bias of the quadratic character over the Hermitian function field is small, for any low-degree function f with odd degree. Our results also give non-trivial results for the first levels of the Hermitian tower.

Technique-wise we analyze multiplicity in function fields in a better way, using a new 'universal derivative-fix' lemma we prove, building on the connection between derivatives and differentials in function fields.

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q odd, and let $f(X)$ be a polynomial of (low) degree d. Then, the classical Weil bound on character sums tells us that unless $f(X)$ is the square of a polynomial, we have:

$$\Pr_{x \in \mathbb{F}_q}[f(x) \text{ is a perfect square in } \mathbb{F}_q] = \frac{1}{2} + O(\frac{d}{\sqrt{q}}). \tag{1}$$

[*] Department of Mathematics and Department of Computer Science, University of Toronto. Email: swastik.kopparty@utoronto.ca.

[†] Department of Computer Science, Tel Aviv University. The research leading to these results has received funding from the Israel Science Foundation (grant number 443/22). Email: amnon@tauex.tau.ac.il.

[‡] Department of Computer Science, Tel Aviv University. The research leading to these results has received funding from the Israel Science Foundation (grant number 443/22) and the Blavatnik fund. Email: kedem12@gmail.com

ISSN 1433-8092

Note that about 1/2 of all elements in $\mathbb{F}_q$ are perfect squares; thus the statement above shows that the values taken by a low-degree polynomial are quite randomly distributed.

Apart from being a basic expression of pseudorandomness, the Weil bound has numerous applications in theoretical computer science and combinatorics. For example, it is useful in constructions of epsilon-biased sets [AGHP92], better-than-random nearly-orthogonal vectors in Euclidean space [Tao], k-universal graphs and tournaments [GS71], and extractors [Zuc90, GR08].

This paper is about generalizations of the Weil bound phenomenon to evaluations of algebraic functions over algebraic curves. Evaluating algebraic functions on algebraic curves is a natural and powerful generalization of evaluating polynomials in one variable. The evaluation vectors so obtained are examples of algebraic-geometric codes (AG codes), and choosing the curve to have a large genus and with a large number of $\mathbb{F}_q$-points compared to its genus – such as Hermitian curves or Garcia-Stichtenoth towers – yields amazing "better than random" constructions of error-correcting codes. With an eye on applications in coding theory and pseudorandomness, we are specifically interested in whether the Weil-bound phenomenon occurs on such curves.

Specifically, consider an algebraic curve C over a finite field $\mathbb{F}_q$, and a low-degree algebraic function f on C. What is the probability that f evaluates to a perfect square at a uniformly random $\mathbb{F}_q$-rational point on C?

For curves of small genus $g \ll \sqrt{q}$, the Weil bounds themselves (along with related facts about the zeta functions of curves) do give such a bound. They imply that for any algebraic curve C of genus g contained in the plane, and any polynomial $f(X,Y)$ of degree d, unless f is the square of an algebraic function over C, we have:

$$\mathop{\mathbf{Pr}}_{(x,y)\in C(\mathbb{F}_q)}[f(x,y) \text{ is a perfect square in } \mathbb{F}_q] = \frac{1}{2} + O_{g,d}\left(\frac{1}{\sqrt{q}}\right).$$

For large g (which is the case for the Hermitian and Garcia-Stichtenoth towers), however, the original Weil bound machine does not say anything.

In this paper, we prove exactly this kind of character sum bound on curves such as the Hermitian curves or the first levels of the Hermitian tower. We show, for example for C being the Hermitian curve and $f(X,Y)$ being a polynomial of odd total degree d, and odd pole order at infinity that:

$$\mathop{\mathbf{Pr}}_{(x,y)\in C(\mathbb{F}_q)}[f(x,y) \text{ is a perfect square in } \mathbb{F}_q] = \frac{1}{2} + O\left(\frac{\sqrt{d}}{q^{1/4}}\right), \tag{2}$$

where d is the total degree of the polynomial $f(X,Y)$. We conjecture that the error term can be improved to $O\left(\frac{d}{\sqrt{q}}\right)$.

We can also give similar bounds for the first levels of the Hermitian curve, see Theorem 4.8 for details.

Our proof method is to create a version of the Stepanov-Schmidt-Bombieri approach to the original Weil bounds, ported to the context of C. The original approach of Stepanov-Schmidt-Bombieri is a form of the polynomial method and the method of multiplicities; the size of a set $S \subseteq \mathbb{F}_q$ of points is bounded from above by finding a non-zero, low degree univariate polynomial $g(X)$ that vanishes on all the points of S with high multiplicity. Our version deals with a subset S of the curve C, and to bound its size we find a non-zero, low degree algebraic function g on the curve C that vanishes on all the points of S with high multiplicity. To implement this, we need to understand derivatives and multiplicities on curves. Things can work quite counter-intuitively in this setting; for example, the derivative of a low-degree algebraic function is often an algebraic function of higher degree. One of our key technical contributions is a *universal derivative-fix*, showing that there exists a *universal* low-degree element, that can compensate all poles that may originate by deriving any function from a Riemann space. For a precise statement see Theorem 1.1. We believe our toolkit could enable further applications of the polynomial method and the method of multiplicities to the curve setting.

1.1 More about the technique

In the polynomial method, we want to bound the number of elements with some combinatorial property. We do that by presenting a (low-degree) non-zero polynomial Q such that all these elements can be derived from Q (e.g., they are roots of Q). For example, suppose we are given as input a set $\{(a_i, b_i) \in \mathbb{F}_q \times \mathbb{F}_q\}$ and we want to bound the number of degree d polynomials $H(X) \in \mathbb{F}_q[X]$ such that $H(a_i) = b_i$ for at least A values i. The Guruswami-Sudan algorithm [GS98] does that by first finding a low-degree polynomial $Q \in \mathbb{F}_q[X, Y]$ such that Q vanishes with high multiplicity over all points (a_i, b_i) in the set, and then proves that every solution $H(X)$ gives a factor $Y - F(X)$ of Q. The Guruswami-Sudan algorithm thus bounds the number of such $H(X)$ by the degree of Q, and can explicitly find these solutions by factoring.

The Stepanov method is similar, except that the polynomial Q has to vanish with high multiplicity over a simple variety, rather than just an arbitrary set. For example, in the form of the Weil bound described in Equation (1), we are interested in the (size of the) set of $(x, y) \in \mathbb{F}_q^2$ such that $y^2 = f(x)$, i.e., the variety[1] of points (x, y) satisfying (1) $y^2 = f(x)$, (2) $x^q = x$, (3) $y^q = y$. In the general polynomial method, one usually has independent constraints per different points. However, in this case, independent constraints give nothing. Instead, it is cheaper to enforce that Q vanishes as a polynomial *over the variety*, and this is a key insight in Stepanov's method.

In this work we want to count the number of points $P \in C(\mathbb{F}_q)$, such that $f(P)$ is a non-zero square. As before, this corresponds to the number of points in the set:

$$\{(z, P) \in \mathbb{F}_q \times C(\mathbb{F}_q) \mid z^2 = f(P)\}.$$

[1] Varieties are considered over algebraically closed fields; this is why we have to explicitly introduce the $x^q = x$ and $y^q = y$ equations.

We want to use the Stepanov method to find a Q that vanishes with high multiplicity on this set; this leads us to search for such a Q in the function field $F' = F[Z]/\langle Z^2 - f\rangle$, where F is the function field of C, and thus the function f on C is an element of F. This is fairly straight forward when F is the rational function field. However, when F is a large genus function field, things get complicated. To begin with, one needs to have derivatives in the function field. Even though derivatives in function fields are well studied and share many properties with derivatives over the rational function field, many essential differences exist. For example, the degree of the derivative might be much larger than the degree of the original function. These differences are responsible for many of the complications that arise. To overcome these difficulties, we employ a general, powerful tool relating the pole divisor of derivatives of $f \in F$ with the pole divisor of f. We prove:

Theorem 1.1. *Let F be a function field of genus g, and $x \in F$ a separating element of F. There exists $\omega \in F$ such that for every $f \in F$ with poles only at P_∞ and pole order at most A, the derivative of f with respect to x, denoted $D_x(f)$, satisfies:*

- *$\omega D_x(f)$ has poles only at P_∞*
- *The pole order of $\omega D_x(f)$ is at most $A + 3g - 2 + 2\deg(x)$*

We are unaware of previous results of this form.

Many problems are left open. The most crucial is to generalize the Hermitian curve bound to degrees d above $\sqrt{q}$, or for general curves to work with functions coming from Riemann-Roch spaces with degree above the genus. We remark that such improvements might have far reaching consequences to the construction of explicit binary error correcting codes close to the Gilbert-Varshamov bound.

We also do not know what the true error term in Equation (2) is, for example, it might be that under natural conditions on f, the error is bounded by $O(\frac{d}{q^{3/4}})$. Without any further conditions, the error cannot be reduced below $O(\frac{1}{\sqrt{q}})$.

Another question concerns the derivative-fix bound; we suspect that the $3g$ term in Theorem 1.1 can be improved to $2g$.

This paper is organized as follows. In Section 2 we briefly recall some results from algebraic function fields, and set the notation used throughout this work. In Section 3 we state and prove a generalization of Theorem 1.1. Then, in Section 4 we state our main bound, Theorem 4.6, for a general curve in terms of certain parameters of the underlying curve, and instantiate it for the Hermitian curve and the first levels of the Hermitian tower. In Sections 5 and 6 we prove the main result itself.

2 Some function fields background

We assume familiarity with the basic notions of algebraic function fields (place, valuation, genus, Riemann-Roch space and Riemann-Roch theorem, ramification, etc.).

2.1 Hasse derivatives

Let F/K be a function field and $z \in F$ separating[3]. The m-th Hasse derivative with respect to z, denoted by H_z^m, is defined on $K[z]$ by the K-linear extension of $H_z^m(z^n) \triangleq \binom{n}{m} z^{n-m}$ to all of $K[z]$. H_z^m can be uniquely extended to all of F/K so that they satisfy: (1) $H_z^0 = id_F$, (2), H_z^m vanish on K for all $m > 0$, (3) $H_z^m(fg) = \sum_{j=0}^m H_z^j(f) H_z^{m-j}(g)$ (Product Rule) and $H_z^m \circ H_z^n = \binom{m+n}{m} H_z^{m+n}$ (Composition Rule). These uniquely determined extensions are called the *Hasse derivatives*. A consequence of these properties is that

Corollary 2.1. *Let F/K be a function field of characteristic p and let z be a separating element. Then $m! H_z^m = D_z^m$, where D_z^m is the iterated derivative and H_z^m is the m-th Hasse derivative.*

In particular, when $p = 0$ or when $p > 0$ and $m < p$ we get that H_z^m and D_z^m differ by a non-zero constant, and so $H_z^m(f) = 0$ if and only if $D_z^m(f) = 0$. The fact that Hasse derivatives capture multiplicity is given in the following claim, which is an immediate corollary of [Gol03, Corollary 2.5.14 (Taylor's Theorem)],

Claim 2.2. *Let P be a place in F/K and let t be a separating element with $v_P(t) = 1$. Let $f \in F$ and $M \in \mathbb{N} \setminus \{0\}$, then $v_P(f) \geq M \iff \forall m < M \quad (H_t^m(f))(P) = 0$.*

A simple fact is

Fact 2.3 (Simple change of variable)**.** *Let z be a separating element in F/K, let $f \in F$ and $\alpha \in K$, then for every $m > 0$, $H_z^m(f) = H_{z-\alpha}^m(f)$.*

The following lemma tells us how Hasse derivatives behave on p-th powers:

Claim 2.4. *[Tor00, Remark 2.4 and Remark 2.5], [Jeo11, Theorem 3.1] Let $z \in F/K$ be a separating element of a function field of characteristic $p > 0$. Let $q = p^k$ be a power of p and $f \in F$. then:*

1. *$H_z^m(f^q) = (H_z^{m/q}(f))^q$ if q divides m and $H_z^m(f^q) = 0$ otherwise.*
2. *$H_z^m(f) = 0$ for $m = 1, ..., q-1$ if and only if there exists some $g \in F$ such that $f = g^q$*
3. *$H_z^1(f) = H_z^p(f) = H_z^{p^2}(f) = ... = H_z^{p^{k-1}}(f) = 0$ if and only if there exists some $g \in F$ such that $f = g^q$*

The following corollary will be useful to us later on:

Corollary 2.5. *Let $z \in F/K$ be a separating element of a function field of characteristic $p > 0$. Let q be a power of p, $m < q$ and $f, g \in F$, then: $H_z^m(fg^q) = H_z^m(f)g^q$.*

Proof. Since $m < q$, all of the derivatives of g^q that will appear in the expansion of $H_z^m(fg^q)$ by means of the product rule are zero (from Claim 2.4) except for the term $H_z^m(f)g^q$. □

2.2 Differentials

We follow the presentation at [Sti09, Chapter 4]. Let F/K be a function field. A *derivation* is a K-linear map D from F to some F-module that upholds the product rule of derivatives, i.e. $D(fg) = fD(g) + gD(f)$. For example $H_z^1 : F \to F$ is a derivation for every separable $z \in F$. One can define an F-module Δ_F, such that all derivations of F factor through Δ_F via a canonical mapping $d : F \to \Delta_F$, i.e., if $\delta : F \to M$ is a derivation of F into some F-module M, then there exists a unique F-linear map $\mu : \Delta_F \to M$ such that $\delta = \mu \circ d$. It turns out that d is itself a derivation. For $x \in F$, $d(x)$ is called the differential associated with x and is denoted dx. The set Δ_F of differentials of F contains all elements udx where $u \in F$ and x is separating, where this set is taken modulo the equivalence relation $udx = vdy$ if and only if $\frac{u}{v} = D_x^1(y)$. With this we get a notion of division of differentials via $\frac{udy}{vdx} = \frac{u}{v} D_x^1(y)$.

We now define the notion of valuation of differentials. If $P \in \mathbb{P}_F$ is a place of F and $udx \in \Delta_F$ a differential of F, we define $v_P(udx)$ as follows. We pick a local parameter t of P (i.e., $v_P(t) = 1$) and we find $b \in F$ such that $udx = bdt$. Then $v_P(udx) = v_P(b)$. One can show that this definition is independent of the specific choice of local parameter t. As differentials have valuations, differentials also have zeroes and poles, i.e., places where the valuation is strictly positive or strictly negative, and this can be encoded in a divisor, denoted (udx) and called the divisor associated with the differential udx. It turns out any differential $udx \in \Delta_F$ has only finitely many zeroes or poles and so the associated divisor is indeed well defined. A divisor which is associated to some differential in Δ_F is called a *canonical divisor*. All canonical divisors have degree $2g - 2$ and their Riemann-Roch space has dimension g where $g = genus(F)$. The following claims will be useful:

Claim 2.6. *Let $u \in F$, $x, y \in F$ separating, then:*

- $(udx) = (u) + (dx)$
- $(D_x^1(y)) = (\frac{dy}{dx}) = (dy) - (dx)$

The first bullet is a restatement of [Sti09, Proposition 1.5.13] and the second one is an immediate consequence of the first bullet and the equality $1dy = D_x^1(y)dx$.

There is a close relationship between the zeroes and poles of f and the zeroes and poles of df. The following claim is stated in [Mas84, Chapter I (6)] for the case where K is algebraically closed, but by considering a constant-field extension of F one can verify it holds exactly as stated for any perfect base field K and even when P is not a place of degree one (which is not a consideration when K is algebraically closed). We give the proof for completeness.

Claim 2.7. *Let $f \in F/K$, df its associated differential, then:*

- *For every place P, $v_P(df) \geq v_P(f) - 1$. In particular, If f has zeroes at P, df can lose at most one zero at P. Also, df can have at most one more pole at P. Also,*

- *If $v_P(f) \geq 0$ then $v_P(df) \geq 0$, i.e., df can have poles only at places where f has poles.*

Proof of claim 2.7. Let $f \in F/K$, $P \in \mathbb{P}_F$, $t \in F$ with $v_P(t) = 1$. We are interested in $(df)^F$ the divisor of df over F. We move to $\bar{F}/\bar{K} = \bar{K} \cdot F/K = \bar{K}F/\bar{K}$ which is the constant field extension of F/K with all of $\bar{K}$, the algebraic closure of K. Let $\bar{P} \in \mathbb{P}_{\bar{F}}$ be a place lying over P. Since $\bar{K}$ is algebraically closed we know $\deg(\bar{P}) = 1$. From [Sti09, Theorem 3.6.3] we learn that $v_{\bar{P}}(t) = v_P(t) = 1$ and we can write:

$$f = \sum_{n=n_0 \in \mathbb{Z}}^{\infty} c_n t^n \quad (c_n \in \bar{k}, c_{n_0} \neq 0)$$

$$D_t^1(f) = \sum_{n=n_0 \in \mathbb{Z}}^{\infty} n \cdot c_n t^{n-1} \quad (c_n \in \bar{k}, c_{n_0} \neq 0)$$

From the definition of valuation for differential we know that

$$v_{\bar{P}}(1df) = v_{\bar{P}}(D_t^1(f)dt) = v_{\bar{P}}(D_t^1(f)) \geq n_0 - 1$$

From [Sti09, Theorem 3.6.3] we know that $v_{\bar{P}}(1df) = v_P(1df)$ and $v_P(f) = v_{\bar{P}}(f)$ and so we get $v_P(1df) \geq v_P(f) - 1$. Furthermore, if f has no pole at P, then f has no pole at $\bar{P}$ and so $n_0 \geq 0$ and so $D_t^1(f)$ has no pole at $\bar{P}$ and therefore at P, meaning $v_P(1df) \geq 0$. □

We mentioned before that $\deg(df) = 2g-2$ for canonical divisors (df), and therefore when g is large df has many more zeroes than f. We also know that df has a zero wherever f has a zero of multiplicity at least 2. Finding the other zeroes of df is a bit more complicated. It turns out that:

Claim 2.8. *[Sti09, Sections 3.4 and 3.5] The zeroes of df are either at places that are zeroes of f, or, at places of F/K that are ramified when F is viewed as an extension of $K(f)/K$.*

2.3 Kummer extensions

An algebraic function field F'/K' is a *Kummer extension* of F/K if K contains a primitive n-th root of unity,[2] and $F' = F(Z) \mod (Z^n - u)$ where $u \in F$ and $u \neq w^d$ for all $w \in F$ and $d|n$ such that $d > 1$. Kummer extensions are Galois. For $P \in \mathbb{P}_F$ we denote by $\mathcal{L}(P) \overset{\text{def}}{=} \cup_{m \in \mathbb{N}} \mathcal{L}(m \cdot P)$ the K-linear, infinite dimensional vector space of all function that have poles only at P. The following claim follows from [Sti09, Corollary 3.7.4 and Proposition 3.11.1] and the Hurwitz Genus Formula [Sti09, Theorem 3.4.13]:

Claim 2.9. *Let P_∞ be a degree one place of a function field F/K of genus g, ℓ a prime number and $u \in \mathcal{L}(P_\infty)$ which is not an ℓ-th power in F. Denote $d = \deg(u) = -v_{P_\infty}(u)$ and assume d is co-prime to ℓ. Let $F' = F(Z)$ where $Z^\ell = u$ be the Kummer extension with respect to u. Then:*

[2] When $K = \mathbb{F}_q$ this means $n|(q-1)$.

- *F' is a degree ℓ extension of F*
- *P_∞ is totally ramified in F'.*[3] *Also K is the full constant field of F'.*
- *$Z \in \mathcal{L}(P'_\infty)$ and $\deg(Z) = d$*
- *$g' \overset{\text{def}}{=} \text{genus}(F')$ satisfies $\ell(g-1) \le g'-1 \le \ell(g-1)+d$*

From now on we assume that K is a finite field, $K = \mathbb{F}_q$ for some prime power q. Let ℓ be a prime number that divides $q-1$. Let P_∞ be a degree one place, and S a set of degree one places of F that does not contain P_∞. Let $u \in \mathcal{L}(P_\infty) \subset F$ such that u is not an ℓ-th power in F. We are interested in the number of $P \in S$ such that $u|_P \overset{\text{def}}{=} \phi_P(u) \in K$ is an ℓ-th power as an element of K (where ϕ_P is the evaluation function at P). [4] The following claim is standard and we omit its proof:

Claim 2.10. *Suppose $u|_P \neq 0$ for some degree one place $P \in S$. Then:*

- *If $u|_P$ is not an ℓ-th power in K, then there is a single place above P in F' and it is a place of degree ℓ (and ramification 1).*
- *If, however, $u|_P$ is a non-zero ℓ-th power in K, then the place P is totally split in F', i.e. there are ℓ distinct degree one places above P (that have all ramification 1).*

Definition 2.11. *Let F be a function field with constant field K. Let S be a set of degree one places of F/K. We say $z \in F$ is* derivative-useful *for S, or, in short, S-useful, if for every $P \in S$ there exists $\alpha \in K$ such that $v_P(z-\alpha) = 1$.*

The term "S-useful" is not standard and does not hold any deeper meaning then saying z "works" for every place of S in the sense discussed above. We have:

Claim 2.12. *Let $F' = F(Z) \mod (Z^\ell - u)$ be a Kummer extension with ℓ prime and $u \in \mathcal{L}(P_\infty) \subset F$ such that u is not an ℓ'th power of an element in F. Further assume K is the full constant field of F'. Let S be a set of degree one places F/K and assume $P_\infty \notin S$. Suppose $S_\ell \subset S$ is such that $u|_P$ is a non-zero ℓ-th power for all $P \in S_\ell$, and let S'_ℓ be the set of all places of F' lying over S_ℓ.*

Then: If $x \in F$ is S_ℓ-useful [5] *then x when considered as an element of F' is S'_ℓ-useful.*

Proof. Let $Q \in S'_\ell$ and denote $P \in S_\ell$ the place of F lying below Q. Since $u|_P$ is a non-zero ℓ-th power, P is totally split in F' (by claim 2.10). This means there are ℓ places lying over P (Q among them), each of them with relative degree one and ramification 1 over P. Since $x \in F$ is S-useful and $P \in S_\ell \subset S$ there exists an $\alpha \in K$ such that $v_P(X-\alpha) = 1$. Since Q is lying over P and has ramification 1 we get $v_Q(X-\alpha) = e(Q|P)v_P(X-\alpha) = 1 \cdot 1 = 1$. So for any $Q \in S'_\ell$ we found $\alpha \in K$ with $v_Q(X-\alpha) = 1$ completing the proof. □

[3] We remind the reader that this means that P'_∞ is the only place of F' above P_∞, has degree one and its ramification index over P_∞ is ℓ.

[4] Notice that $u|_P$ is defined because u does not have a pole at any $P \in S$, and $u|_P \in K$ because any $P \in S$ is degree one.

[5] In practice, our way of ensuring x is S_ℓ-useful will be to find an x which is useful for all of S.

3 The universal derivative-fix lemma

In the polynomial ring $K[X]$, the derivative of a non-constant polynomial is a polynomial of a strictly smaller degree, and the more times we derive the smaller the degree gets until we reach the zero polynomial. This gives the impression that derivatives are simpler, i.e. have less poles than the original function. When transitioning to rational functions, this is no longer the case. For example, when m is smaller then the characteristic of K, $D_x^m(\frac{1}{x}) = \frac{c_m}{x^{m+1}}$ for some non-zero constants c_m. Now, the more we derive the more poles we get, and each derivation increases the pole order by one. Similarly, if we look at $D_x^m(\frac{f}{g})$ we get some polynomial in the derivatives of f and g divided by g^{m+1}, meaning the poles at the zeroes of g increase many-fold as we derive. Thus, both in the case of $\frac{1}{x}$ and in the more general case of $\frac{f}{g}$, the poles "stay where they were", but the pole order increases. This gives us reason to hope that deriving a regular function will leave us with a regular function.

Now consider derivatives of the form $D_g^1(f)$ where $f, g \in K(x)/K$. From the chain rule $D_g^1(f) = \frac{df}{dg} = \frac{df}{dx}\frac{dx}{dg} = \frac{f'}{g'}$ we see that $D_g^1(f)$ may have poles also where g' has zeroes, and the more zeroes g has, the more new poles we introduce when deriving. Thus, it greatly matters with respect to which function g we choose to derive.

Next, we look beyond the genus zero rational function field. We take the Hermitian function field. Let $F = \mathbb{F}_{p^2}(x,y) \mod y^p + y - x^{p+1}$. The elements x and y are regular, i.e., they only have poles at a single degree one place, which we denote P_∞. It holds that $v_{P_\infty}(x) = -p$ and $v_{P_\infty}(y) = -(p+1)$. Now, $x^p = D_x(x^{p+1}) = D_x(y^p + y) = D_x(y^p) + D_x(y) = D_x(y)$, and so, $D_x(y) = x^p$ has p^2 poles at P_∞ while y has only $p+1$ poles at P_∞, an increase of $p^2 - p - 1 = 2\text{genus}(F) - 1$.

For a divisor D we let $(D)_0$ denote the zero-divisor of D, and $(D)_\infty$ the pole divisor of D, so that $D = (D)_0 - (D)_\infty$. We let $\text{DegSupp}((x)_\infty)$ be the degree of the support of the pole divisor of x, i.e., the degree of the pole divisor of x when all positive coefficients are reduced to one. We prove:

Theorem 3.1. *Let F/K be a function field of genus g. Let $x \in F$ be a separating element of F/K and P_∞ a degree one place of F. Let*

$$G = 3g - 2 + \deg(x) + \text{DegSupp}((x)_\infty).$$

Then there exists an element

$$0 \neq \omega = \omega(x, P_\infty) \in \mathcal{L}(G \cdot P_\infty - (dx)_0) \subseteq \mathcal{L}((G - \max\{v_\infty(dx), 0\})P_\infty)$$

such that for every $A \geq 0$ and every $f \in \mathcal{L}(AP_\infty)$ it holds that

$$\omega \cdot H_x(f) \in \mathcal{L}((A + G + \min\{v_\infty(dx), 0\} + 1) \cdot P_\infty).$$

Proof. Let us denote $f' := H_x^1(f) = D_x^1(f)$. By Claim 2.6, $f' = \frac{df}{dx}$ and $(f') = (df) - (dx)$. It follows that the poles of f' can come either from poles of df, or, from zeroes of dx. Since

$f \in \mathcal{L}(AP_\infty)$, Claim 2.7 tells us all the poles of f and df are at P_∞. Claim 2.7 also tells us that $v_\infty(df) \geq v_\infty(f) - 1 \geq -(A+1)$, and so df has at most $A+1$ poles, all of which must be at P_∞. We wish to find $\omega \in F$ s.t. $\omega \cdot f' \in \mathcal{L}(P_\infty)$ so we need to choose ω that cancels the poles of f' at all places other than P_∞. These poles can arise only from zeroes of dx. More precisely, we are interested in the zeroes of dx *outside* P_∞. While we are interested in the zeroes of dx, we first consider the *poles* of dx. By Claim 2.7:

- The poles of dx are at the same places as the poles of x, i.e., $v_P(dx) < 0$ implies $v_P(x) < 0$, and,
- At any place P where dx and x have a pole, dx may have at most one more pole than x, i.e., $v_P(dx) \geq v_P(x) - 1$.

It therefore follows that $\deg((dx)_\infty) \leq \deg(x) + \mathrm{DegSupp}((x)_\infty)$. We now use the fact that (dx) is a canonical divisor, and therefore has degree $2g-2$. Thus, the number of zeroes of dx is exactly $2g-2$ more than the number of poles of dx, and in total we get

$$\deg((dx)_0) \leq \deg(x) + \mathrm{DegSupp}((x)_\infty) + 2g - 2 = G - g.$$

Now, set $D = G \cdot P_\infty - (dx)_0$. Thus,

$$\deg(D) = G - \deg((dx)_0) \geq g.$$

By the Riemann-Roch Theorem there exists some $0 \neq \omega \in \mathcal{L}(D)$. Fix any such ω. Set $\Delta = G + \min\{v_\infty(dx), 0\}$. Then,

Claim 3.2. $\omega f' = \omega \cdot \frac{df}{dx} \in \mathcal{L}((A+1+\Delta)P_\infty)$.

Proof. For any $P \neq P_\infty$, $v_P(D) = -v_P((dx)_0)$. Hence,

$$\begin{aligned} v_P(\omega) &\geq -v_P(D) = v_P((dx)_0), \text{ and,} \\ v_P(\omega f') &= v_P(\omega) + v_P(df) - v_P(dx) \\ &\geq v_P(\omega) + v_P(df) - v_P((dx)_0) \geq v_P(df) \geq 0. \end{aligned}$$

Next we compute the pole order of wf' at P_∞. We have $w \in \mathcal{L}(D) \subseteq \mathcal{L}((G - \max\{v_\infty(dx), 0\})P_\infty)$. Thus,

$$\begin{aligned} -v_\infty(\omega f') &= v_\infty(dx) - v_\infty(\omega) - v_\infty(df) \\ &= v_\infty(dx) + G - \max\{v_\infty(dx), 0\} - v_\infty(df) \\ &\leq A + 1 + G + v_\infty(dx) - \max\{v_\infty(dx), 0\}, \end{aligned}$$

because $v_\infty(df) \geq v_\infty(f) - 1 \geq -A - 1 = -(A+1)$. However,

$$v_\infty(dx) - \max\{v_\infty(dx), 0\} = \min\{0, v_\infty(dx)\},$$

and the proof is complete. □

□

3.1 General derivation order

We now generalize Theorem 3.1 to any derivation order m. We remind the reader that $H_x^m(f)$ is the m-th Hasse derivative of f with respect to x.

Theorem 3.3. *Let F/K be a function field of genus g over a base field of characteristic p. Let $x \in F$ be a separating element of F/K and P_∞ a degree one place of F. Let G be as before, and,*

$$\begin{aligned} W &= G - \max\{v_\infty(dx), 0\} \\ \Delta &= G + \min\{v_\infty(dx), 0\}. \end{aligned}$$

There exists an element $0 \neq \omega = w(x, P_\infty) \in \mathcal{L}(G \cdot P_\infty - (dx)_0) \subseteq \mathcal{L}(WP_\infty)$ such that for every positive integer $m < p$ (or any integer m, if $p = 0$) and every $f \in \mathcal{L}(A \cdot P_\infty)$,

$$\omega^{2m-1} \cdot H_x^m(f) \in \mathcal{L}(A_m \cdot P_\infty).$$

where $A_m = A - W + m \cdot (\Delta + W + 1)$.

Proof. We use the same w as before. We prove by induction. We already saw the $m = 1$ case. Assume for m and let us prove for $m + 1$. The $m + 1$-th Hasse derivative is the same as the $m+1$-th iterated derivative D_x^{m+1} up to multiplication by a non-zero scalar (see corollary 2.1 and using $m + 1 < p$ when the characteristics is finite). Now,

$$\begin{aligned} \omega^2 D_x(\omega^{2m-1} D_x^m f) &= \omega^2 \ [\ D_x(\omega^{2m-1}) D_x^m f + \omega^{2m-1} D_x(D_x^m f)\ ] \\ &= (2m-1) \cdot \omega D_x(\omega) \cdot \omega^{2m-1} D_x^m f + \omega^{2m+1} D_x^{m+1} f \end{aligned}$$

Thus,

$$\omega^{2m+1} D_x^{m+1} f = \omega^2 D_x(\omega^{2m-1} D_x^m f) - (2m-1) \cdot \omega D_x(\omega) \cdot \omega^{2m-1} D_x^m f.$$

By the induction hypothesis and the $m = 1$ case:

$$\begin{aligned} \omega^{2m-1} \cdot D_x^m f &\in \mathcal{L}(A_m \cdot P_\infty), \\ \omega D_x(\omega^{2m-1} D_x^m f) &\in \mathcal{L}((A_m + (\Delta + 1)) \cdot P_\infty). \end{aligned}$$

Also $\omega \in \mathcal{L}(WP_\infty)$. By the $m = 1$ case,

$$\omega \cdot D_x(\omega) \in \mathcal{L}((W + (\Delta + 1)) \cdot P_\infty)$$

The term $\omega^2 D_x(\omega^{2m-1} D_x^m f)$ is in $\mathcal{L}((A_m + W + \Delta + 1)P_\infty)$. The term $\omega D_x(\omega) \cdot \omega^{2m-1} D_x^m f$ is also in $\mathcal{L}((A_m + W + \Delta + 1)P_\infty)$. Altogether, $\omega^{2m+1} D_x^{m+1} f$ is in $\mathcal{L}(A_{m+1} P_\infty) = \mathcal{L}((A_m + W + \Delta + 1)P_\infty)$. □

Remark 3.4. *Note that if $D_x(\omega)$ is in $\mathcal{L}(P_\infty)$, we can multiply by a single ω per derivative, instead of multiplying by ω^2.*

Corollary 3.5. *Assume the above setting. Let $m > 0$ then $\omega \in \mathcal{L}((3g + 2\deg(x) - 1)P_\infty)$, and $A_m \leq A + (2m-1)(3g + 2\deg(x) - 1)$.*

3.2 Discussion

Example 3.6. *Consider the Hermitian function field when we derive by x. $D_x(y) = x^p$. In fact, $(dx) = (2g-2)P_\infty$, i.e., it has no poles, and all its zeroes are at P_∞. Then, we can take $w = 1$. Furthermore, for every $f \in \mathcal{L}(AP_\infty)$, $-v_\infty(H_x(f)) = v_\infty(dx) - v_\infty(df) \leq 2g-2+A+1$. For a general m, $A_m \leq A + m(2g-1)$.*

Example 3.7. *Now consider the Hermitian function field when we derive by y. Then, $D_y(x) = \frac{1}{x^p}$ and $(dy) = (p+2)P_\infty - p(x)_0$. Nevertheless, since all functions in $\mathcal{L}(P_\infty)$ are polynomials in x and y, we get that if we are deriving with respect to y we can choose w to be x^p to cancel out the $\frac{1}{x^p}$ which is the derivative of x with respect to y. With this choice of ω we again get that if $f \in \mathcal{L}(AP_\infty)$ then $\omega^m H^m(f) \in \mathcal{L}((A + m(2g-1))P_\infty)$.*

The bounds we obtained are worse. This is because:

- We paid an additive g to guarantee a certain Riemann-Roch space is nonempty, by forcing the degree of its divisor to be at least g. While there are divisors of degree $g-1$ which have empty Riemann-Roch spaces, there are divisors of degree 0 which have non-empty Riemann-Roch spaces. It is conceivably possible that the $3g-1$ we have is not mandatory and can be replaced with $2g-1$ as we have in the Hermitian curve. Perhaps, using the Riemann-Roch theorem with canonical divisors would do the trick.

- Additionally, the $2m$ factor is a side effect of the inductive argument which requires us to apply the induction hypothesis twice - once for $H^{m-1}(f)$ and once for $H^1\omega$. If, however, $H^1\omega$ is regular, we can apply the induction hypothesis once and so ω^m would be sufficient. Alternatively, if the poles of $D^m(f)$ which exceed those of $D^{m-1}(f)$ behave like "dividing by a function again and again", similarly to what we saw with $D_x^m(\frac{f}{g})$ in $K(x)$ or to $D_y(f)$ for regular f in the Hermitian function field, we would again get that ω^m is sufficient.

- The requirement $m < p$ is also a side effect of the induction, but when looking at the p-th Hasse derivative of y^p we get from claim 2.4 $H_x^p(y^p) = H_x^1(y)^p = x^{p^2}$ which is of pole order $p^3 = p(p+1) + (2g-1)p$, an increase of exactly $2g-1$ times the order of the derivative.

To summarize this, an optimistic reading of the proof would lead us to believe that the following version of theorem 3.3 could hold:

Conjecture 3.8. *Let F/K be a function field of genus g. Let $x \in F$ be a separating element of F/k. Let P_∞ be a degree one place of F. There exists an element $0 \neq \omega = w(x, P_\infty) \in F$ such that for every $m \in \mathbb{N}$ and every $f \in \mathcal{L}(P_\infty)$, $\omega^m \cdot H_x^m(f) \in \mathcal{L}(P_\infty)$. Furthermore, $\omega \in \mathcal{L}((2g-1+\deg(x)+\mathrm{DegSupp}((x)_\infty)) \cdot P_\infty)$ and so if $f \in \mathcal{L}(A \cdot P_\infty)$ then $\omega^m \cdot H_x^m(f) \in \mathcal{L}(A_m \cdot P_\infty)$ for $A_m = A + m(2g-1+\deg(x)+\mathrm{DegSupp}((x)_\infty)+\min\{v_\infty(dx), 0\})$.*

4 The character sum bound

4.1 The function fields we work with

Let F be a function field with constant field K. Let S be a set of degree one places of F/K. We recall that $z \in F$ is S-useful, if for every $P \in S$ there exists $\alpha \in K$ such that $v_P(z-\alpha) = 1$. We have:

Claim 4.1. *If z is S-useful and for all $0 \leq m < M$ the function $H_z^m(f)$ vanishes at all places in S, then f vanishes with multiplicity at least M at every place of S.*

Proof. Fix $P \in S$. As z is S-useful there exists some $\alpha \in K$ such that $v_P(z-\alpha) = 1$. By Fact 2.3 we see that $\left(H_{z-\alpha}^m(f)\right)|_P = \left(H_z^m(f)\right)|_P = 0$ for all $0 \leq m < M$. Hence Claim 2.2 tells us $v_P(f) \geq M$ as desired. □

In the following, we will work with a function field $F/\mathbb{F}_q$, a set S of degree one places, a degree one place we call P_∞, and, an element $X_0 \in \mathcal{L}(P_\infty)$ that is S-useful. Note that this implies that $P_\infty \notin S$. We now state the assumptions we put on the function field $F/\mathbb{F}_q$, S and X_0.

1. We assume $q = p^2$ and p is a prime number.[6]

2. We also want F to have many degree one places and a small genus. Let $\mathbb{P}_F^1$ denote the set of degree one places of F, and $N_1 = |\mathbb{P}_F^1|$. From the Drinfeld-Vladut Bound [Sti09, Theorem 7.1.3] we know that in any sequence of function fields over $\mathbb{F}_q$, with N_1 going to infinity, the genus tends in the limit to at least $\frac{N_1}{p-1}$, and there are several constructions attaining this bound [Sti09, Section 7]. In particular we assume:

$$g_F \overset{\text{def}}{=} \text{genus}(F) \leq a \cdot \frac{N_1}{p}, \tag{3}$$

   for some constant $a \geq \frac{p}{p-1} \geq 1$.

3. We would like $\deg(X_0)$ to be as small as possible. It is well-known that every element $f \in F$ with $\deg(f) > 0$ has $\deg(f) \geq \frac{N_1}{q+1}$ (see, e.g., [BATS09, Lemma 10]). We assume

$$\deg(X_0) = b \cdot \frac{N_1}{q}, \tag{4}$$

   for some constant b, and so $b \geq 1 - \frac{1}{q+1}$. We want b to be small.

[6] A large part of our work is applicable even when p is a prime power and not just prime, but the use of theorem 3.3 is pivotal, and at this point our proof only holds for $M < p$ where p is the characteristic of the field.

We now see several examples of such function fields:

Example 4.2. *Let $F/\mathbb{F}_q$ be the Hermitian function field, with $N_1 = p^3 + 1$ and genus $\frac{p(p-1)}{2}$. Let $S = \mathbb{P}^1_F \setminus P_\infty$, $|S| = p^3$. Let $X_0 = x$ and notice that indeed $X_0 = x$ is S-useful. We have* $\deg(X_0) = p$. *Thus, $a = \frac{1}{2} > \frac{p \cdot g}{N_1} = \frac{p^3 - p}{2N_1}$, and, $b = \frac{q \cdot \deg(x)}{N_1} = 1 - \frac{1}{N_1}$.*

Example 4.3. *Next, we look at the Hermitian tower function field of level e, F_e (where the Hermitian function field is F_2). When $2e < p$ we have the genus of F_e is at most ep^e. Let S be all the degree one places other than P_∞, $|S| = p^{e+1}$. Let $X_0 = x_1$ and notice that indeed X_0 is S-useful. We have* $\deg(X_0) = p^{e-1}$. *Then, $a \leq e$ (because $e = \frac{ep^{e+1}}{p^{e+1}} \geq \frac{p \cdot g}{N_1}$), and, $b = \frac{q \cdot \deg(X_0)}{N_1} = \frac{q \cdot p^{e-1}}{p^{e+1}+1} = 1 - \frac{1}{N_1}$.*

Example 4.4. *Our final example is the GS tower of level e. The genus of F_e is less then p^e. $X_0 = x_1$ is S-useful for a set of $p^e(p-1)$ degree one places (which are exactly the evaluation points in the GS error correcting code). We have* $\deg(X_0) = p^{e-1}$. *Thus, $a = \frac{p}{p-1} = \frac{p \cdot p^e}{p^e(p-1)} \geq \frac{p \cdot g}{N_1}$, and, $b = \frac{q \cdot \deg(x)}{N_1} \leq \frac{q \cdot p^{e-1}}{p^e(p-1)} = \frac{p}{p-1}$.*

4.2 The problem

We continue with the notation set before. Let ℓ be a prime number dividing $q - 1$. Note that ℓ is different from the characteristic of F. $f \in \mathcal{L}(rN_1 P_\infty)$, where r is a parameter. We assume $\deg(f) = -v_{P_\infty}(f)$ is coprime to ℓ. This assumption implies f is not an ℓ-th power in $\overline{\mathbb{F}_q}F$, where $\overline{\mathbb{F}_q}F$ is the constant field extension of F with the algebraic closure of $\mathbb{F}_q$. Our goal is to estimate the number of places $P \in S$ such that $f|_P \in \mathbb{F}_q$ is an ℓ-th power. We define

$$F' = F(Z) \mod Z^\ell - f.$$

By Claim 2.9, F' is a Kummer extension of F and P_∞ is totally ramified in F'. Also $g' = \text{genus}(F')$ satisfies $\ell(g-1) \leq g' - 1 \leq \ell(g-1) + \deg^F(f)$. Let P'_∞ denote the single place of F' above P_∞. As P'_∞ is totally ramified we have:

- $deg(P'_\infty) = 1$,
- $v_{P'_\infty}(X_0) = \ell \cdot v_{P_\infty}(X_0)$, and $v_{P'_\infty}(f) = \ell \cdot v_{P_\infty}(f)$,
- $\ell \cdot v_{P'_\infty}(Z) = v_{P'_\infty}(f) = \ell \cdot v_{P_\infty}(f)$ and so $v_{P'_\infty}(Z) = v_{P_\infty}(f) \leq rN_1$. In fact, $Z \in \mathcal{L}(rNP'_\infty)$.

Let $S_\ell \subseteq S$ be the set of all places $P \in S$ where $f|_P \in \mathbb{F}_q$ is a non-zero ℓ-th power. Let S'_ℓ be the places of F' that lie over S_ℓ. By Claim 2.10, S_ℓ totally split in F', and so

$$|S'_\ell| = \ell |S_\ell|.$$

In this terminology, our goal is to identify a large vector space of functions f, for which $|S_\ell|$, or equivalently, $|S'_\ell|$, is about right.

4.3 Our result

Our bound will be good for f such that $t = -v_{P'_\infty}(Z) = -v_{P_\infty}(f)$ is close to a multiple of $v_{P_\infty}(X_0)$ which is not a multiple of $\ell \cdot v_{P_\infty}(X_0)$.[7] Formally, write

$$-v_{P_\infty}(f) = -(\ell c_1 + d_1)v_{P_\infty}(X_0) + e_1 \tag{5}$$

where $c_1, d_1, e_1 \in \mathbb{Z}$, $0 < d_1 < \ell$ and $|e_1|$ minimal. Note that we do not allow d_1 to be zero. We want $|e_1|$ to be small, and if $t = -v_{P_\infty}(f)$ is close to a multiple of $v_{P_\infty}(X_0)$ which is not a multiple of $\ell \cdot v_{P_\infty}(X_0)$, then $|e_1|$ is indeed small. If, however, t is close to a multiple of $\ell \cdot v_{P_\infty}(X_0)$, then, as we do not allow $d_1 = 0$, we must take $|e_1|$ to be fairly large (about $|v_{P_\infty}(X_0)|$).

Let A be some (large) positive integer. In Section 5 we prove:

Theorem 4.5. *In the above notation, suppose $A < bN_1 - (\ell-1)q|e_1|$ and let $\{a_i\}$ be any basis of $\mathcal{L}(AP'_\infty)$. Then $\{a_i X^{jq} Z^{kq} | j \in \mathbb{N}; 0 \le k < \ell\}$ are independent over $\mathbb{F}_q$.*

In Section 6 we prove:

Theorem 4.6. *In the above notation, assume further*

$$r < \frac{a}{p} \tag{6}$$

$$\frac{\ell^2}{\ell-1} < \frac{1}{9a+3b}(b - \frac{\ell q|e_1|+1}{N_1})\sqrt{\frac{rp^3}{a}}. \tag{7}$$

Then:

$$|S_\ell| \le \frac{bN_1}{\ell}\left(1 + (\ell-1)\sqrt{\frac{rp}{a}} + \frac{\ell(9a+3b)\sqrt{a}(\frac{qr}{b} + \frac{\ell}{\ell-1})}{b\sqrt{rp^3} - \frac{\ell}{\ell-1}(9a+3b)\sqrt{a} - \frac{q\ell|e_1|+1}{N_1}}\right)$$

Note that if p is large and a and $|e_1|$ are small, then we can bound the second error term with:

$$\frac{\ell(9a+3b)\sqrt{a}(\frac{qr}{b} + \frac{\ell}{\ell-1})}{b\sqrt{rp^3} - \frac{\ell}{\ell-1}(9a+3b)\sqrt{a} - \frac{q\ell|e_1|+1}{N_1}} = O(\frac{\ell qr}{b\sqrt{rp^3}}) = O(\frac{\ell}{b} \cdot \sqrt{rp})$$

making it roughly equal to the first error term which is $(\ell-1)\sqrt{\frac{rp}{a}}$.

For the Hermitian function field the following simplification holds:

[7] Recall that $f, X_0 \in \mathcal{L}(P_\infty)$. If f is a polynomial in X_0, i.e., $f = P(X_0)$, then the requirement that $\deg(f)$ is not an ℓ-multiple of $\deg(X_0)$, implies that $\deg(P)$ is coprime to ℓ, and, in particular, f is not an ℓ'th power of a polynomial in X_0.

Theorem 4.7. *Let $p > 500$ be a prime number, $q = p^2$ and let ℓ be a prime number that divides $q-1$. Let $f(x,y)$ be a rational function in the Hermitian function field with total degree d and pole order at infinity d_∞. Assume that: Both d and d_∞ are not divisible by ℓ, $\ell < O(\sqrt{dp})$, and, $d < O\left(\frac{q}{\ell}\right)$. Then:*

$$\left|\{P \in C(\mathbb{F}_q) \mid f(P) \text{ is a perfect } \ell^{th} \text{ power in } \mathbb{F}_q\}\right| = \frac{p^3}{\ell}\left(1 + O\left(\ell\sqrt{\frac{d}{p}}\right)\right)$$

For $\ell = 2$ we can also prove the above under the more general assumption that f is not a square of any function in a constant field extension of the Hermitian function field (replacing the conditions that d and d_∞ are odd), but for brevity, we decided to omit it from this paper.

For the Hermitian tower of level e (as in Example 4.3), we have $a = e$ and $b = 1 - \frac{1}{N_1}$. Fix $r = \beta\frac{e}{p}$ for some $\beta < 1$ that will be determined later. This allows every $f \in \mathcal{L}(rN_1P_\infty)$, and, in particular, all polynomials $f(x_0, x_1, \ldots, x_{e-1})$ of total degree at most d for $d < \frac{rN_1}{(p+1)^{e-1}} \approx \frac{rp^{e+1}}{p^{e-1}} = rq = \beta ep$. We assume $b - \frac{\ell q|e_1|+1}{N_1} \geq \frac{1}{2}$. As $b \approx 1$ and $N_1 \geq p^{e+1}$, this allows $|e_1|$ as large as about $\frac{p^{e-1}}{2\ell}$. Then, Equation (7) becomes (approximately) $\frac{\ell^2}{\ell-1} < O_e(\sqrt{dp})$, and is satisfied for p large enough. Theorem 4.6 shows that $|S_\ell|$ is about $\frac{N_1}{\ell}(1 + \ell\sqrt{\beta} + O_{\ell,e}(\frac{qr}{p\sqrt{rp}}))$, where $O(\frac{qr}{p\sqrt{rp}})) = O(\sqrt{rp}) = O(\sqrt{\beta e})$. Thus, the error term is $O_{\ell,e}(\sqrt{\frac{d}{p}})$, and we get meaningful results for polynomials of total degree $d \leq cp$, for some $c < 1$ that depends only e and ℓ. Formally,

Theorem 4.8. *Fix ℓ. Let e be constant and $F_e(x_0, \ldots, x_{e-1})$ the e-level of the Hermitian tower over $\mathbb{F}_q$, where p is a large enough prime (as a function of e and ℓ) and $q = p^2$, and further assume ℓ divides $q-1$. Let $f(x_0, \ldots, x_{e-1})$ have total degree at most d. Assume that d is not not divisible by ℓ, and, furthermore, if we express*

$$-v_{P_\infty}(f) = -(\ell c_1 + d_1)v_{P_\infty}(X_0) + e_1 \tag{8}$$

where $c_1, d_1, e_1 \in \mathbb{Z}$, $0 < d_1 < \ell$ and $|e_1|$ minimal then $|e_1| \leq p^{e-1}/2\ell$. Then:

$$\left|\{P \in C(\mathbb{F}_q) \mid f(P) \text{ is a perfect } \ell^{th} \text{ power in } \mathbb{F}_q\}\right| = \frac{p^{e+1}}{\ell}\left(1 + O_{\ell,e}\left(\sqrt{\frac{d}{p}}\right)\right)$$

5 Independence

Before we prove Theorem 4.5 we focus on a special basis of a relevant Riemann-Roch space. Let A be some positive integer. Let $T \subseteq \mathbb{N}$ be the set of integers i such that there exists an element $b_i \in \mathcal{L}(P'_\infty)$ with $v_{P'_\infty}(b_i) = -i$.[8] The set $\{b_i\}_{i \in T, i \leq A}$ is a basis of $\mathcal{L}(A \cdot P'_\infty) \subset F'$.

[8] If $g' = \text{genus}(F') > 0$ then T is non-consecutive and contains up to g' gaps. However, it is a semi-group, and is called the Weierstrass semigroup of P'_∞.

Theorem 5.1. *In the above notation, suppose $A < bN_1 - (\ell - 1)q|e_1|$. Let i, i', j, j', k, k' be non-negative integers, such that $i, i' \leq A$ and $k, k' < \ell$. Then two elements $b_i X^{jq} Z^{kq}$ and $b_{i'} X^{j'q} Z^{k'q}$ have the same P'_∞-valuation if and only if $(i, j, k) = (i', j', k')$.*

Proof. Let us compute $v_{P'_\infty}(b_i X_0^{jq} Z^{kq})$:

$$\begin{aligned} v_{P'_\infty}(b_i X_0^{jq} Z^{kq}) &= v_{P'_\infty}(b_i) + jq \cdot v_{P'_\infty}(X_0) + kq \cdot v_{P'_\infty}(Z) \\ &= -i + jq\ell \cdot v_{P_\infty}(X_0) + kq(\ell c_1 + d_1) \cdot v_{P_\infty}(X_0) - e_1 kq. \end{aligned}$$

Plugging in $v_{P_\infty}(X_0) = -b\frac{N_1}{q}$ we get:

$$v_{P'_\infty}(b_i X_0^{jq} Z^{kq}) = -i - bN_1(\ell j + (\ell c_1 + d_1)k) - e_1 kq \; = -\ell bN_1(j + kc_1 + k\frac{d_1}{\ell} + \frac{i + e_1 kq}{\ell b N_1})$$

and so if $v_{P'_\infty}(b_i X_0^{jq} Z^{kq}) = v_{P'_\infty}(b_{i'} X_0^{j'q} Z^{k'q})$ we get that:

$$j - j' + (k - k')(c_1 + \frac{d_1}{\ell}) = \frac{i' - i + (k' - k)qe_1}{\ell b N_1}$$

Which means $\frac{i'-i+(k'-k)qe_1}{\ell b N_1}$ must be an integer multiple of $\frac{1}{\ell}$. However, this quantity (in absolute value) is at most $\frac{A+(\ell-1)q|e_1|}{\ell b N_1} < \frac{1}{\ell}$ by the assumption on A. We get that $\frac{i'-i+(k'-k)qe_1}{\ell b N_1} = 0$, giving us $j - j' + (k - k')(c_1 + \frac{d_1}{\ell}) = 0$. Considering the fractional part of this equation and remembering $0 < d_1 < \ell$ gives $k = k'$, which in turn gives us $j = j'$ and $i = i'$. □

Remark 5.2. *In the case where $v_{P_\infty}(f)$ is divisible by ℓ there are two cases to consider. If P_∞ does not split at all, and has a single extension in F' with full relative index, the proof can be modified to get a similar result to theorem 5.1, which is enough for us to continue the analysis as in the later sections of this work. If, however P_∞ has more than one place lying over it in F' the whole framework of our proof is no longer applicable. As the more general case is the one where P_∞ splits in F' we limit ourselves to the case where $v_{P_\infty}(f)$ is not divisible by ℓ for the sake of both simplicity and brevity.*

We are ready to prove Theorem 4.5:

Proof. (of Theorem 4.5) We first prove it for the basis $\{b_i\}_{i \in T, i \leq A}$ from Theorem 5.1. Suppose $\sum c_{i,j,k} b_i X^{jq} Z^{kq} = 0$. As all the elements in the sum have distinct valuations at P'_∞, the valuation of the sum is the minimal valuation of $b_i X^{jq} Z^{kq}$ with a non-zero coefficient $c_{i,j,k}$. However, the valuation is $v(0) = \infty$. Hence all the coefficients $c_{i,j,k}$ are zero.

Now suppose $\sum_{j,k} g_{j,k} X_0^{jq} Z^{kq} = 0$ for $g_{j,k} \in \mathcal{L}(AP'_\infty)$. Write each $g_{j,k}$ as $\sum_i c_{i,j,k} b_i$. From the previous argument we see that all $c_{i,j,k}$ are zero, hence all $g_{j,k}$ are zero. In particular let $\{a_i\}$ be an arbitrary basis of $\mathcal{L}(AP'_\infty)$. Let $g_{j,k} = \sum_i c_{i,j,k} a_i \in \mathcal{L}(AP'_\infty)$ to obtain $g_{j,k} = 0$ for all j, k. From the independence of a_i we conclude that all $c_{i,j,k}$ must be zero, finishing the proof. □

6 Bounding the bias

In this section we prove Theorem 4.6. We do this using a version of Stepanov method. We remind the reader that $S_\ell \subseteq S$ is the set of all places $P \in S$ where $f|_P \in \mathbb{F}_q$ is a non-zero ℓ-th power, and S'_ℓ is the set of places of F' that lie over S_ℓ. We also saw that by Claim 2.10, S_ℓ totally split in F', and so $|S'_\ell| = \ell|S_\ell|$.

Proof of theorem 4.6. Set an integer $M < p$ to be determined later. Our goal is to find $0 \neq R \in F'$ such that $\deg(R)$ is not too large, and, for every $P' \in S'_\ell$, $v_{P'}(R) \geq M$. It then follows that $M \cdot |S'_\ell| \leq \deg(R)$ and therefore $|S_\ell| \leq \frac{\deg(R)}{\ell M}$. We search for R in the following vector space: Let $A < bN_1 - (\ell-1)q|e_1|$ and B be parameters that will be chosen later. Let $\{a_i\}$ be a basis of $\mathcal{L}(AP'_\infty)$. Set

$$U = \{a_i X_0^{jq} Z^{kq} \mid j < b \text{ and } k < \ell\}$$

We search for R in the $\mathbb{F}_q$-linear span of U. By Theorem 4.5 the elements in U are independent and so the dimension of span(U) is the size of U. Hence,

$$\dim(\text{span}(U)) \geq \ell \cdot B \cdot (A - g' + 1).$$

As $a_i \in \mathcal{L}(AP'_\infty)$, $X_0 \in \mathcal{L}(\ell b \frac{N}{q} P'_\infty)$, and $Z \in \mathcal{L}(rN_1 P'_\infty)$, we see that

$$\text{span}(U) \subseteq \mathcal{L}((A + \ell(B-1)bN_1 + (\ell-1)qrN_1)P'_\infty). \tag{9}$$

In particular, if $R \in \text{span}(U)$ then $\deg(R) \leq A + \ell(B-1)bN_1 + (\ell-1)qrN_1$.

Express $R = \sum c_{i,j,k} a_i X_0^{jq} Z^{kq}$. We want to find a set of linear constraints on $c_{i,j,k}$ that guarantees that $v_{P'}(R) \geq M$ for all $P' \in S'_\ell$. For that end, for $0 \leq m < M$ define:

$$g_m = \omega_m \cdot \sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k,$$

where $\omega_0 = 1$ and $\omega_m = \omega^{2m-1}$ for $0 < m < M$, and ω is as in Theorem 3.3. We claim:

Lemma 6.1. *If for every $0 \leq m < M$, $g_m = 0$ as an element of F', then R vanishes M times on all of S'_ℓ.*

Proof. (of Lemma 6.1) Fix $P' \in S'_\ell$ and $0 \leq m < M$. Assume $g_m = \omega_m \cdot \left(\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k\right)$ is zero as an element of F'. Notice that ω_m is either 1 or ω^{2m-1} where ω is not zero, and so ω_m is never the zero function, meaning it is invertible in F'. Therefore, $\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k$ is zero as an element of F'. In particular it is zero on P'. Now,

$$H^m_{X_0}(R)|_{P'} = H^m_{X_0}(\sum c_{i,j,k} a_i X_0^{jq} Z^{kq})|_{P'} \ = (\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^{jq} Z^{kq})|_{P'},$$

using Corollary 2.5 and the $\mathbb{F}_q$-linearity of H^m. P' is a degree one place of F', and so $\varphi_{P'}(X_0) = X_0|_{P'}$ and $\varphi_{P'}(Z) = Z|_{P'}$ are both elements of $\mathbb{F}_q$ ($P' \neq P'_\infty$ so X_0 and Z are indeed defined at P'). Therefore

$$\begin{aligned} X_0^q|_{P'} &= \varphi_{P'}(X_0^q) = \varphi_{P'}(X_0)^q = \varphi_{P'}(X_0) = X_0|_{P'}, \\ Z^q|_{P'} &= \varphi_{P'}(Z^q) = \varphi_{P'}(Z)^q = \varphi_{P'}(Z) = Z|_{P'}, \end{aligned}$$

and $H^m_{X_0}(R)|_{P'} = \left(\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k\right)|_{P'} = 0$. We conclude that $H^m_{X_0}(R)$ vanishes on P'.

Now X_0 is S-useful, and therefore it is S_ℓ-useful. By Claim 2.12, X_0 is S'_ℓ-useful. As this is true for every $m < M$, Claim 4.1 implies that R vanishes M times on P' as desired. □

Our next step is to show each requirement $g_i = 0$ imposes a bounded number of homogeneous linear constraints on the coefficients $c_{i,j,k}$. We prove:

Lemma 6.2. *For every m,i, j, k, $\omega_m H^m_{X_0}(a_i) X_0^j Z^k \in \mathcal{L}(A_m P'_\infty)$ where $A_0 = A + (B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1$ and $A_m = A_0 + (2m-1)(3g' + 2b\frac{N_1}{q})$ for $m > 0$, where $g' = \text{genus}(F') \leq \ell g + rN_1$.*

Proof. (of Lemma 6.2) $X_0^j Z^k$ and $\omega_m H^m_{X_0}(a_i)$ are regular at P'_∞. The degree of $X_0^j Z^k$ is at most $(B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1$. For $m = 0$, the degree of $\omega_m H^m_{X_0}(a_i) = a_i$ is at most A. For $m > 0$ we have $\omega_m H^m_{X_0}(a_i) = \omega^{2m-1} H^m_{X_0}(a_i)$, which by corollary 3.5 is a regular function with degree at most $A + (3g' - 1 + 2\deg(X_0))(2m-1)$. Altogether, $w_m H^m_{X_0}(a_i) X_0^j Z^k \in \mathcal{L}(A_m P'_\infty)$ for every i, j, k. □

Now choose a basis for $\mathcal{L}(A_m P'_\infty)$ and represent each $\omega_m H^m_{X_0}(a_i) X_0^j Z^k \in \mathcal{L}(A_m P'_\infty)$ as a vector of length $\dim(A_m P'_\infty)$. $g_m = \sum c_{i,j,k} \omega_m H^m_{X_0}(a_i) X_0^j Z^k$ and therefore the constraint $g_m = 0$ gives $\dim(A_m P'_\infty) \leq A_m$ linear homogeneous equations in the variables $c_{i,j,k}$. Altogether we get a system of $\sum_{m=0}^{M-1} A_m$ linear, homogeneous equations in $\ell \cdot B \cdot \dim(AP'_\infty)$ variables. Choosing parameters such that $\sum_{m=0}^{M-1} A_m \leq \ell \cdot B \cdot \dim(AP'_\infty)$ guarantees a non-zero solution R, and then $|S_\ell| \leq \frac{\deg(R)}{\ell M}$.

The number of constraints is at most

$$\begin{aligned} \sum_{m=0}^{M-1} A_m \leq \sum_{m=0}^{M-1} (A_0 + (6g' + 4b\frac{N_1}{q})m) \;\leq\; MA_0 + (6g' + 4b\frac{N_1}{q})\frac{M^2}{2} \\ \leq MA + (3g' + 2b\frac{N_1}{q})M^2 + M((B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1). \end{aligned}$$

Notice that the number of degrees of freedom is less than ℓBA while the number of constrains is more than MA. Therefore, in order for the number of degrees of freedom to exceed the number of constraints, we must have $M < \ell B$. We shall therefore write

$$\ell B = M + E.$$

We now compare the number of constraints with the number of degrees of freedom, demanding that the number of constraints be smaller:

$$\begin{aligned}(M+E)(A-g'+1) > MA + (3g'+2b\frac{N_1}{q})M^2 + M((B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1)\\ EA > \ell B(g'-1) + (3g'+2b\frac{N_1}{q})M^2 + M((B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1)\end{aligned}$$

And so it is enough to ask:

$$\begin{aligned}\frac{E}{M} &> g'(\frac{3M}{A}+\frac{\ell B}{MA}) + 2b\frac{MN_1}{qA} + (B-1)\ell b\frac{N_1}{qA} + (\ell-1)\frac{rN_1}{A}, \text{ or,}\\ \frac{E}{M} &\geq \frac{N_1}{A}\left((3M+\frac{\ell B}{M})(\frac{a\ell}{p}+r) + \frac{2bM+(B-1)\ell b}{q} + r(\ell-1)\right), \qquad (10)\end{aligned}$$

because $g' \leq \ell g + rN_1 \leq N_1(\frac{a\ell}{p}+r)$. We now choose

$$\begin{aligned}A &= bN_1 - q\ell|e_1| - 1,\\ M &= \lfloor \frac{\ell-1}{\ell(9a+3b)}\frac{A}{N_1}\sqrt{\frac{rp^3}{a}}\rfloor,\\ B &= \lceil \frac{M}{\ell}(1+\frac{MN_1\ell}{A}(\frac{4a}{p}+\frac{4r}{\ell}+\frac{3b}{q}+\frac{r(\ell-1)}{M\ell}))\rceil\end{aligned}$$

and denote $E = \ell B - M$. We check that these choices satisfy our constraints. First, clearly, $A < bN_1 - q(\ell-1)|e_1|$. Also, $A < bN_1$ and $r < \frac{a}{p}$ (Equation (6)) and therefore $M < \frac{b}{9a+3b}p < p$. Also,

Claim 6.3. *$B \leq M$ and $\ell \leq M$.*

Proof. We first prove $\ell \leq M$. Since ℓ is an integer it is enough to show that $\ell < \frac{\ell-1}{\ell(9a+3b)}\frac{A}{N_1}\sqrt{\frac{rp^3}{a}}$, which holds because of our choice of A and Equation (7). We next prove $B \leq M$. It is enough to show that

$$1 + \frac{MN_1\ell}{A}(\frac{4a}{p}+\frac{4r}{\ell}+\frac{3b}{q}+\frac{r(\ell-1)}{M\ell}) \leq \ell.$$

We have $\frac{4r}{\ell} \leq \frac{4a}{p}$, $\frac{r(\ell-1)}{M\ell} \leq \frac{a}{p}$ (because of Equation (6)), and, therefore, it is enough to show that $M \leq \frac{\ell-1}{\ell}\frac{A}{N_1}\frac{p}{9a+3b}$. This last inequality holds because of Equation (6) and the definition of M. □

Also note that

$$\frac{E}{M} = \frac{\ell B}{M} - 1 \geq \frac{N_1}{A}M\ell(\frac{4a}{p}+\frac{4r}{\ell}+\frac{3b}{q}+\frac{r(\ell-1)}{M\ell})$$

and Equation (10) follows (using Claim 6.3 and $\frac{\ell B}{M} \leq M$). This concludes the check that our choices satisfy our constraints. We conclude that $|S_\ell| < \frac{degR}{M}$. By Equation (9), $\deg(R) \leq A + \ell(B-1)bN_1 + (\ell-1)qrN_1$, and

$$\begin{aligned} |S_\ell| \leq \frac{\deg(R)}{\ell M} &\leq \frac{A}{\ell M} + \frac{\ell(B-1)bN_1}{\ell M} + \frac{(\ell-1)qrN_1}{\ell M} \\ &< \frac{A}{\ell M} + \frac{(M+E)bN_1}{\ell M} + \frac{(\ell-1)qrN_1}{\ell M} < \frac{bN_1}{\ell}\left(1 + \frac{E}{M} + \frac{(\ell-1)qr}{bM} + \frac{A}{bN_1 M}\right) \end{aligned}$$

and so $|S_\ell| < \frac{bN_1}{\ell}(1+\mathbb{E})$ where $\mathbb{E} = \frac{E+1}{M} + \frac{(\ell-1)qr}{bM}$. Substituting M and E we get

$$\begin{aligned} \mathbb{E} = \frac{E+1}{M} + \frac{(\ell-1)qr}{bM} &\leq \frac{MN_1\ell}{A}(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell}) + \frac{\ell}{M} + \frac{(\ell-1)qr}{bM} \\ &\leq \frac{\ell-1}{p}\sqrt{\frac{rp^3}{a}} + \frac{b\ell + (\ell-1)qr}{bM} \leq (\ell-1)\sqrt{\frac{rp}{a}} + \frac{\ell(9a+3b)\sqrt{a}(\frac{qr}{b} + \frac{\ell}{\ell-1})}{b\sqrt{rp^3} - \frac{\ell}{\ell-1}(9a+3b)\sqrt{a} - \frac{q\ell|e_1|+1}{N}}, \end{aligned}$$

completing the proof. □

References

[AGHP92] Noga Alon, Oded Goldreich, Johan Håstad, and René Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures & Algorithms*, 3(3):289–304, 1992.

[BATS09] Avraham Ben-Aroya and Amnon Ta-Shma. Constructing small-bias sets from algebraic-geometric codes. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 191–197. IEEE, 2009.

[Gol03] David M. Goldschmidt. *Algebraic Functions and Projective Curves*, volume 215. Springer New York, NY, 2003.

[GR08] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Comb*, 28(4):415–440, 2008.

[GS71] Ronald L. Graham and Joel H. Spencer. A constructive solution to a tournament problem. *Canad. Math. Bull.*, 14:45–48, 1971.

[GS98] Venkatesan Guruswami and Madhu Sudan. Improved decoding of reed-solomon and algebraic-geometric codes. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 28–37. IEEE, 1998.

[Jeo11] Sangtae Jeong. Calculus in positive characteristic p. *Journal of Number Theory*, 131(6):1089–1104, 2011.

[Mas84] R. C. Mason. *Diophantine Equations over Function Fields*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1984.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[Tao] Terry Tao. A cheap version of the kabatjanskii-levenstein bound for almost orthogonal vectors. `https://terrytao.wordpress.com/2013/07/18/a-cheap-version-of-the-kabatjanskii-levenstein-bound-for-almost-orthogonal-vec` Accessed: 2023-04-01.

[Tor00] Fernando Torres. The approach of stöhr-voloch to the hasse-weil bound with applications to optimal curves and plane arcs, 2000.

[Zuc90] Zuckerman. General weak random sources. In *FOCS: IEEE Symposium on Foundations of Computer Science (FOCS)*, 1990.