COUNTING POINTS OF FIXED DEGREE AND GIVEN HEIGHT OVER FUNCTION FIELDS

Jeffrey Lin Thunder and Martin Widmer

Abstract. Let k be a finite algebraic extension of the field of rational functions in one indeterminate over a finite field and let $\overline{k}$ denote an algebraic closure of k. We count points in projective space $\mathbb{P}^{n-1}(\overline{k})$ with given height and generating an extension of fixed degree d over k. If $n > 2d+3$ we derive an asymptotic estimate for the number of such points as the height tends to infinity. As an application we deduce asymptotic estimates concerning certain decomposable forms.

Introduction

The purpose of a height in Diophantine geometry is to give a quantitative measure of the arithmetic complexity of a point on some variety. This has become a very important tool. Given a variety, one would like to know if there are only finitely many points of a given height or height less than a given bound. If so, one would further like to know the number of such points, or at least upper and lower bounds for the number of such points. Another goal would be to find asymptotic estimates for the number of such points as the bound tends to infinity. Before we can discuss particular results here, we must first set some notation.

For any field k and a point $P = (x_1\colon \cdots : x_n) \in \mathbb{P}^{n-1}(\overline{k})$ in projective $n-1$-space over an algebraic closure, let $k(P)$ denote the field of definition of P over k; in other words, $k(P)$ is the field obtained by adjoining all possible quotients x_i/x_j to the field k. For a number field k, integers $n,\ d$ and positive real B, let $N_k(n,d,B)$ denote the number of points in projective space $\mathbb{P}^{n-1}(\overline{\mathbb{Q}})$ with (multiplicative) height less than B and $[k(P)\colon k] \le d$. An important early result in this area is due to Northcott, who proved that $N_k(n,d,B)$ is finite. On the other hand, one easily sees that $N_k(n,d,B)$ grows without bound as $B \to \infty$. Thus, one can ask for an asymptotic estimate, and

1991 *Mathematics Subject Classification.* Primary: 11G50; Secondary: 11G35.

Second author supported by Swiss National Science Foundation Grant #118647 and Austrian Science Fund Grant #M1222

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

it is precisely such estimates that interest us here when the number field is replaced by a function field.

With this notation, $N_{\mathbb{Q}}(n,1,B)$ is simply the number of primitive lattice points in a ball or cube (depending on the exact height used); asymptotic results for $N_{\mathbb{Q}}(n,1,B)$ as $B\to\infty$ are classical. More generally, for any number field k Schanuel [Scha] proved that

$$N_k(n,1,B)=S_k(n,1)B^{ne}+O(B^{ne-1})$$

as $B\to\infty$, where $e=[k\colon\mathbb{Q}]$ and the implicit constant depends on the number field k and the dimension n. (A $\log B$ term must be inserted in the error when $k=\mathbb{Q}$ and $n=2$, though this is not necessary if one uses L_2 norms at the infinite place.) Here $S_k(n,1)$ is an explicitly given constant depending on the field k and the dimension n. It turns out that proving similar asymptotic results for $N_k(n,d,B)$ when $d>1$ is much more difficult. Schmidt in [Schm1] gave non-trivial upper and lower bounds for $N_k(n,d,B)$ and later gave asymptotic estimates for $N_{\mathbb{Q}}(n,2,B)$ in [Schm2]. In an unpublished thesis Schmidt's student Gao found an asymptotic result for $N_{\mathbb{Q}}(n,d,B)$ when $n>d+1>3$. Masser and Vaaler proved an asymptotic result for $N_k(2,d,B)$ when $k=\mathbb{Q}$ in [MV1], and then for arbitrary number fields in [MV2]. More recently, the second author in [W1] proved that

$$N_k(n,d,B)=S_k(n,d)B^{ned}+O(B^{ned-1})$$

under the assumption that $n>5d/2+3+2/(ed)$, where $e=[k\colon\mathbb{Q}]$ as above and $S_k(n,d)$ is the sum of Schanuel constants $S_K(n,1)$ over extension fields K of degree d over k. Our goal here is to prove a result analogous to the theorem of Widmer above where the number field k is replaced by a function field over a finite field.

Fix a prime p, let $\mathbb{F}_p$ denote the finite field with p elements and let T be transcendental over this field, so that $\mathbb{F}_p(T)$ is a field of rational functions. Throughout this article we fix algebraic closures $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ and $\overline{\mathbb{F}_p(T)}\supset\overline{\mathbb{F}_p}$ of $\mathbb{F}_p(T)$. By a *function field* we will mean a finite algebraic extension field $k\supseteq\mathbb{F}_p(T)$ contained in $\overline{\mathbb{F}_p(T)}$. For such a field k we have $k\cap\overline{\mathbb{F}_p}=\mathbb{F}_{q_k}$ for some finite field $\mathbb{F}_{q_k}$; this is called the *field of constants* for k. Further, we will write g_k for the genus, J_k for the number of divisor classes of degree 0 (this is also the cardinality of the Jacobian) and ζ_k for the usual zeta function of k. Serre stated, and later (independently) Wan [Wa] and DiPippo [D] proved an analog for Schanuel's result in this context, where the "Schanuel constant" for a function field k is

$$S_k(n,1) = \frac{J_k}{(q_k-1)\zeta_k(n)q_k^{n(g_k-1)}}. \tag{1}$$

We denote the absolute additive height on $\overline{\mathbb{F}_p(T)}$ by h (defined below). Fix a function field k and set $e = [k \colon \mathbb{F}_{q_k}(T)]$. Suppose $K \supseteq k$ is another function field. In general, the *effective degree* (see [A, chap. 15, §1]) of the extension field K over k is the quotient $\frac{[K \colon k]}{[\mathbb{F}_{q_K} \colon \mathbb{F}_{q_k}]}$. Thus e is the effective degree of k over $\mathbb{F}_p(T)$. Further, if $q_K = q_k$ the effective degree of K over k is just $d = [K \colon k]$ and the effective degree of K over $\mathbb{F}_p(T)$ is ed. In this case the height of a point P with $k(P) = K$ is necessarily of the form $h(P) = m/ed$, where m is a non-negative integer. This is a major difference from the number field situation, and leads us to count not points of height no greater than a given bound, but equal to a possible given bound. Moreover, since the possible heights are naturally indexed by the non-zero integers, we are lead to the following counting function.

Definition. *Let k be a function field and set $e = [k \colon \mathbb{F}_{q_k}(T)]$. For integers $n > 1$, $d \geq 1$ and $m \geq 0$, $N_k(n,d,m)$ denotes the number of points $P \in \mathbb{P}^{n-1}(\overline{\mathbb{F}_p(T)})$ with height $h(P) = m/ed$ and $k(P) = K$ for some function field K of degree d over k with $q_K = q_k$.*

Our main result is the following.

Theorem 1. *Fix a function field k. For all integers n and $d > 1$ satisfying $n > d+2$, the sum*

$$S_k(n,d) = \sum_{\substack{[K \colon k]=d \\ q_K = q_k}} S_K(n,1)$$

converges. Moreover, if $n > 2d+3$ and $\varepsilon > 0$ with $n > 2d+3+\varepsilon$, then for all integers $m \geq 0$ we have

$$N_k(n,d,m) = S_k(n,d)q_k^{mn} + O\big(q_k^{\frac{m}{2}(n+2d+3+\varepsilon)}\big),$$

where the implicit constant depends only on k, n, d and ε.

One may note that the dependency (lower bound) on n in Theorem 1 is weaker than that in the analogous result of the second author for number fields. The reason for this is essentially the absence of archimedean places in the function field setting, leading to a simpler and shorter proof. The case where $d = 1$ is just the function field version of Schanuel's theorem. In that case one can do much better; see Theorem 2 below. We will show that an asymptotic estimate for $N_k(n,d,m)$ of the form given in Theorem 1 can only be possible when $n \geq d+1$. This is done at the very end of this manuscript.

Though Theorem 1 counts those points generating an extension of degree d and effective degree d, it is a simple matter to estimate the number of points of given height generating an extension of degree d and effective degree d' (which necessarily is a divisor of d) once we have Theorem 1. We note that the height of such a point is necessarily of the form m/ed' for some non-negative integer m. Let k, d and e be as in the statement of Theorem 1 and suppose one wants to count the number N of points P with $[k(P)\colon k]=d$, $q_{k(P)}=q_k^{d/d'}$ and $h(P)=m/ed'$. Certainly all such points will be counted in $N_{k\mathbb{F}_{q_k^{d/d'}}}(n,d',m)$, where $k\mathbb{F}_{q_k^{d/d'}}$ denotes the compositum field, but this will be an over-count since we have $[k(P)\colon k] \leq [k\mathbb{F}_{q_k^{d/d'}}(P)\colon k\mathbb{F}_{q_k^{d/d'}}]\cdot[\mathbb{F}_{q_k^{d/d'}}\colon \mathbb{F}_{q_k}]$. Put another way, if P is counted in $N_{k\mathbb{F}_{q_k^{d/d'}}}(n,d',m)$, then we have $q_{k(P)}=q_k^r$ for some $r\leq d/d'$. We thus see that

$$N_{k\mathbb{F}_{q_k^{d/d'}}}(n,d',m) \geq N \geq N_{k\mathbb{F}_{q_k^{d/d'}}}(n,d',m) - \sum_{1\leq r<d/d'} N_{k\mathbb{F}_{q_k^r}}(n,d',m).$$

Note that the summands subtracted here are of a lower order of magnitude than $N_{k\mathbb{F}_{q_k^{d/d'}}}(n,d',m)$ by Theorem 1, whence we have an asymptotic estimate for the desired quantity N.

We can also use Theorem 1 to count certain forms. Suppose $F(\mathbf{X}) \in k[\mathbf{X}]$ is a homogeneous polynomial (form) in n variables of degree d. Such a form is called *decomposable* if it factors completely into a product of d linear forms:

$$F(\mathbf{X}) = \prod_{i=1}^{d} L_i(\mathbf{X}),$$

where the linear forms $L_i(\mathbf{X}) \in \overline{k}(\mathbf{X})$. Denote the coefficient vector of the linear factor $L_i(\mathbf{X})$ by $\mathbf{L}_i$. Clearly these $\mathbf{L}_i$ are unique only up to a scalar multiple; we thus identify each $\mathbf{L}_i$ with a point $P(\mathbf{L}_i) \in \mathbb{P}^{n-1}(\overline{\mathbb{F}_p(T)})$. In a similar manner, we identify the set of proportional forms $\lambda F(\mathbf{X})$ with a point $P(F) \in \mathbb{P}^{\binom{d+n-1}{n-1}-1}(k)$. Thus the number of non-proportional forms $F(\mathbf{X}) \in k[\mathbf{X}]$ of degree d in n variables with $h\big(P(F)\big)=m/e$ is exactly $N_k\big(\binom{d+n-1}{n-1},1,m\big)$. We can also use Theorem 1 to count certain decomposable forms.

Definition. *Let k be a function field and set $e=[k\colon \mathbb{F}_{q_k}(T)]$. Fix positive integers n and d, and a non-negative integer m. Then $NF_k(n,d,m)$ denotes the number of non-proportional decomposable* *forms $F(\mathbf{X}) \in k[\mathbf{X}]$ in n variables of degree d with height $h\big(P(F)\big) = m/e$, where each $k\big(P(\mathbf{L}_i)\big)$ is an extension of degree d and effective degree d over k.*

As we noted above, the height $h\big(P(F)\big)$ is necessarily of the form m/e for some integer m whenever $F(\mathbf{X}) \in k[\mathbf{X}]$.

Proposition. *Fix a function field k and positive integers n and d. Let p^r denote the highest power of p dividing d, where p is the characteristic of k. Then for all integers $m \geq 0$ we have*

$$dNF_k(n,d,m) = N_k(n,d,m) + \sum_{i=1}^{r} (p^i - p^{i-1}) N_k(n, d/p^i, m).$$

(As usual, empty sums are to be interpreted as zero.)

This in conjunction with Theorem 1 yields the following.

Corollary. *Fix a function field k and positive integers n and d. Let p^r denote the highest power of p dividing d, where p is the characteristic of k. If $n > 2d+3$ and $\varepsilon > 0$ with $n > 2d+3+\varepsilon$, then for all integers $m \geq 0$ we have*

$$dNF_k(n,d,m) = q_k^{nm} \left(S_k(n,d) + \sum_{i=1}^{r} (p^i - p^{i-1}) S_k(n, d/p^i) \right) + O\big(q_k^{\frac{m}{2}(n+2d+3+\varepsilon)}\big),$$

where the implicit constant depends only on k, n, d and ε.

We will give a proof of the Proposition after our proof of Theorem 1 in the final section. We conclude our introduction with a bit more notation and the definition of the height used above. In the next section we outline our method of proof and state its main ingredients. The following sections are devoted to auxiliary results and the proofs of our main theorems and their corollaries.

For a function field k let $M(k)$ denote the set of places of k. For every place $v \in M(k)$ let k_v denote the topological completion of k and let ord_v denote the order function on k_v normalized to have image $\mathbb{Z} \cup \{\infty\}$. We extend ord_v to k_v^n by defining

$$\mathrm{ord}_v(x_1, ..., x_n) = \min_{1 \leq i \leq n} \{\mathrm{ord}_v x_i\},$$

with the usual convention that $\mathrm{ord}_v 0 = \infty$ (greater than any integer). Each non-zero element $\mathbf{x}$ of k^n gives rise to a divisor

$$\mathrm{div}(\mathbf{x}) = \sum_{v \in M(k)} \mathrm{ord}_v(\mathbf{x}) \cdot v.$$

For such an $\mathbf{x}$ we define the *relative height* to be

$$h_k(\mathbf{x}) = -\deg \operatorname{div}(\mathbf{x}).$$

Clearly h_k is an integer. Moreover, since the degree of a principal divisor is 0, h_k is actually a function on projective space. In particular, we can assume without loss of generality that one of the coordinates of $\mathbf{x}$ is 1, so that $\operatorname{ord}_v(\mathbf{x}) \leq 0$ for all places v and $h_k(\mathbf{x})$ is necessarily a non-negative integer. Now $[k\colon \mathbb{F}_{q_k}(T)]$ is, by definition, the effective degree of the extension k over $\mathbb{F}_p(T)$; we define the *absolute height* h to be

$$h(\mathbf{x}) = \frac{h_k(\mathbf{x})}{[k\colon \mathbb{F}_{q_k}(T)]}.$$

Dividing the relative height by the effective degree gives a height that is not dependent on the choice of field. Specifically, if $P \in \mathbb{P}^{n-1}(\overline{\mathbb{F}_p(T)})$ is defined over k and K is any function field containing k, so that P is in both $\mathbb{P}^{n-1}(k)$ and $\mathbb{P}^{n-1}(K)$, we have

$$h_K(P) = h_k(P)\frac{[K\colon k]}{[\mathbb{F}_{q_K}\colon \mathbb{F}_{q_k}]} = h_k(P)\frac{[K\colon \mathbb{F}_{q_K}(T)]}{[k\colon \mathbb{F}_{q_k}(T)]}.$$

(See [T1, p. 150]). Thus, the height h is a function on $\mathbb{P}^{n-1}(\overline{\mathbb{F}_p(T)})$.

Outline of the proof

As one would suppose from the statement of Theorem 1, we estimate $N_k(n,d,m)$ by summing over all possible function fields $K \supseteq k$ of degree d with $q_K = q_k$. More precisely, for such a field K we let $N_k(n,K,m)$ denote the number of points $P \in \mathbb{P}^{n-1}(K)$ with $h(P) = m/de$ and $k(P) = K$, where $e = [k\colon \mathbb{F}_{q_k}(T)]$. In other words, $N_k(n,K,m)$ is the number of those points P counted in $N_k(n,d,m)$ where $k(P) = K$ for the fixed field K. We thus have

$$N_k(n,d,m) = \sum_{\substack{[K\colon k]=d \\ q_K=q_k}} N_k(n,K,m). \tag{2}$$

It will not be difficult to prove that the main term in the asymptotic estimate for $N_k(n,K,m)$ is $S_K(n,1)q_K^{nm}$. Our efforts will mainly be focused on the error term. The major ingredient of our proof is a version of Schanuel's result for function fields where we pay particular attention to the form of the error term.

Theorem 2. *Let k be a function field and set $e = [k\colon \mathbb{F}_{q_k}(T)]$. Suppose m is an integer with $m \geq 2g_k - 1$ and $1/4 \geq \varepsilon > 0$. Then for all integers $n \geq 4$ we have*

$$N_k(n,1,m) = S_k(n,1)q_k^{nm} + O\big(q_k^{m(1+\varepsilon)} q_k^{g_k(n-2-2\varepsilon)}\big),$$

and for $n = 2, 3$

$$N_k(n,1,m) = S_k(n,1)q_k^{nm} + O\big(q_k^{m(1+\varepsilon)} q_k^{g_k(1+\varepsilon)}\big).$$

Suppose $m < 2g_k - 1$. Then for all $\varepsilon > 0$ and all integers $n \geq 2$ we have

$$N_k(n,1,m) \ll q_k^{m(\frac{n+1}{2}+\varepsilon)}$$

All the implicit constants here depend only on n, e, q_k and ε.

Corollary 1. *Let k be a function field. For all integers $n \geq 2$ and $m \geq 0$*

$$N_k(n,1,m) \ll q_k^{nm},$$

where the implicit constant depends only on n and q_k.

We will also use the following quantity.

Definition. *For function fields $K \supseteq k$ and integers $n > 1$,*

$$\delta_n(K/k) = \min\{h(P)\colon P \in \mathbb{P}^{n-1}(K),\ k(P) = K\}.$$

We note that $\delta_n(K/k)$ exists by the primitive element theorem (see [H, p. 287], for example) and the fact, proven in Lemma 6 below, that there are only finitely many intermediate fields.

Corollary 2. *Let $K \supseteq k$ be function fields with $q_K = q_k$, set $[K\colon k] = d$ and $e = [k\colon \mathbb{F}_{q_k}(T)]$. Suppose m and n are positive integers satisfying $m \geq de\delta_n(K/k)$ and $\varepsilon > 0$. Then if $n \geq 4$ we have*

$$N_k(n,K,m) = S_K(n,1)q_k^{nm} + \begin{cases} O\big(q_k^{nm/2}\big) & \text{if } m \geq 2g_K - 1, \\ O\big(q_k^{m(\frac{n+1}{2}+\varepsilon)}\big) & \text{otherwise,} \end{cases}$$

and if $n = 2, 3$

$$N_k(n,K,m) = S_K(n,1)q_k^{nm} + \begin{cases} O\big(q_k^{\frac{3m}{2}(1+\varepsilon)}\big) & \text{if } m \geq 2g_K - 1, \\ O\big(q_k^{m(\frac{n+1}{2}+\varepsilon)}\big) & \text{otherwise.} \end{cases}$$

The implicit constants here depend only on n, e, d, q_k and ε. For all integers $m < de\delta_n(K/k)$, $N_k(n,K,m) = 0$ by definition.

We will see that the "main terms" here are majorized by the "error terms" in the case $m < 2g_K - 1$. It will be convenient for our purposes to have a uniform statement, however. Our proof of Theorem 1 will use Corollary 2 and (2) together with some auxiliary results.

Proof of Theorem 2 and its Corollaries

Our proof of Theorem 2 will follow along the same lines as the proof of Theorem 1 of [T2]. Our job here is made easier since we don't look at arbitrary "twisted" heights, but we need to work somewhat harder to get good explicit dependencies on the field. Throughout this section all function fields appearing are assumed to have the same field of constants; we will write q for the cardinality of this field. Before we get to the proof of Theorem 2, we need to recall some concepts from the theory of function fields and prove a few auxiliary results. In what follows, divisors will always be denoted using capital script German font ($\mathfrak{A}$, $\mathfrak{B}$, etc.), with the exception of the zero divisor which will be denoted by 0.

Let k be a function field and n be a positive integer. For a divisor $\mathfrak{A}$, set

$$L(\mathfrak{A},n) = \{\mathbf{x} \in k^n : \mathrm{ord}_v(\mathbf{x}) \geq -\mathrm{ord}_v(\mathfrak{A}) \text{ for all } v \in M(k)\}.$$

Then $L(\mathfrak{A},n)$ is a vector space of finite dimension over $\mathbb{F}_q$ (see [T1,§II]); we denote this dimension by $l(\mathfrak{A},n)$. Thus, the cardinality of $L(\mathfrak{A},n)$ is $q^{l(\mathfrak{A},n)}$. It will prove convenient to write $\lambda(\mathfrak{A},n)$ for the number of non-zero elements of $L(\mathfrak{A},n)$, i.e., $\lambda(\mathfrak{A},n) = q^{l(\mathfrak{A},n)} - 1$. Let $L'(\mathfrak{A},n)$ denote the set of those $\mathbf{x} \in L(\mathfrak{A},n)$ with $\mathrm{ord}_v(\mathbf{x}) = -\mathrm{ord}_v(\mathfrak{A})$ for all places $v \in M(k)$ and write $\lambda'(\mathfrak{A},n)$ for its cardinality.

Lemma 1. *For a function field k and divisor $\mathfrak{A}$ we have*

$$l(\mathfrak{A},n) = nl(\mathfrak{A},1) = n\left(\deg(\mathfrak{A}) + 1 - g_k + l(\mathfrak{W} - \mathfrak{A},1)\right),$$

where $\mathfrak{W}$ is any divisor in the canonical class. In particular, $l(\mathfrak{A},n) = n\big(\deg(\mathfrak{A}) + 1 - g_k\big)$ whenever $\deg(\mathfrak{A}) \geq 2g_k - 1$, $l(\mathfrak{A},n) \leq \frac{n}{2}\big(\deg(\mathfrak{A}) + 2\big)$ whenever $0 \leq \deg(\mathfrak{A}) \leq 2g_k - 2$, and $l(\mathfrak{A},n) = 0 = \lambda(\mathfrak{A},n)$ whenever $\deg(\mathfrak{A}) < 0$.

Proof. One readily sees that $l(\mathfrak{A}, n) = nl(\mathfrak{A}, 1)$. The lemma thus follows from the Riemann-Roch Theorem and Clifford's Theorem (see [S, Chap. 1], for example).

Next, for all integers $l \geq 0$ write $a(l)$ for the number of non-negative divisors of degree l:

$$a(l) = \sum_{\substack{\mathfrak{C} \geq 0 \\ \deg(\mathfrak{C}) = l}} 1.$$

Then the zeta function is given by

$$\sum_{l=0}^{\infty} a(l) q^{-sl} = \zeta_k(s)$$

for all $s > 1$. We let μ denote the usual Möbius function on the divisor group. It is defined by the following four conditions: $\mu(0) = 1$, $\mu(\mathfrak{A} + \mathfrak{B}) = \mu(\mathfrak{A})\mu(\mathfrak{B})$ whenever $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime (i.e., have disjoint support), $\mu(\mathfrak{P}) = -1$ if $\mathfrak{P}$ is a prime divisor, and $\mu(r\mathfrak{P}) = 0$ if $\mathfrak{P}$ is a prime divisor and $r > 1$. Write

$$b(l) = \sum_{\substack{\mathfrak{C} \geq 0 \\ \deg(\mathfrak{C}) = l}} \mu(\mathfrak{C}).$$

Then as is well-known (see [T2, Lemma 4], for example)

$$\sum_{l=0}^{\infty} b(l) q^{-sl} = \frac{1}{\zeta_k(s)} \tag{3}$$

for all $s > 1$.

Lemma 2. *Fix a function field k and set $e = [k \colon \mathbb{F}_q(T)]$. Then $1 < \zeta_k(s) \leq \left(\zeta_{\mathbb{F}_q(T)}(s)\right)^e$ for all $s > 1$. For all integers $m \geq 0$, all $s \leq 1$ and all $\varepsilon > 0$ we have*

$$\sum_{l=0}^{m} a(l) q^{-sl} \ll q^{m(1-s+\varepsilon)},$$

and for all $s > 1 + \varepsilon$

$$\sum_{l \geq m} a(l) q^{-sl} \ll q^{-m(s-1-\varepsilon)},$$

where the implicit constants depend only on q, e and ε. In particular,

$$a(m) \ll q^{m(1+\varepsilon)}$$

for all integers $m \geq 0$ and all $\varepsilon > 0$. Finally, $a(m) = \frac{J_k}{q-1}(q^{m+1-g_k} - 1)$ for all integers $m \geq 2g_k - 1$.

Proof. We have (see [S, V.1.4 Lemma], for example)

$$a(m) = \frac{1}{q-1}\sum_{j=1}^{J_k} q^{l(\mathfrak{C}_j,1)} - 1, \tag{4}$$

where $\mathfrak{C}_1, \ldots, \mathfrak{C}_{J_K}$ are representatives of the divisor classes of degree m. In particular, $a(0) = 1$ and $a(m) = \frac{J_k}{q-1}(q^{m+1-g_k} - 1)$ for all $m \geq 2g_k - 1$ by the Riemann-Roch Theorem. We get $1 < \zeta_k(s)$ at once. Since the genus is 0 and the number of divisor classes of degree 0 is 1 for a field of rational functions, we get the well-known formula

$$\zeta_{\mathbb{F}_q(T)}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$$

for all $s > 1$. In particular,

$$\zeta_{\mathbb{F}_q(T)}(1+\varepsilon) \ll 1.$$

We next use the Euler product (see [S, V.1.8 Proposition], for example):

$$\zeta_k(s) = \prod_{v \in M(k)} (1 - q^{-s\deg(v)})^{-1}.$$

For a place $v \in M(k)$ lying over a place $w \in M(\mathbb{F}_q(T))$, write f_v for the residue class degree and e_v for the ramification index. Then as is well-known, $\sum_{v|w} e_v f_v = [k\colon \mathbb{F}_q(T)]$ for all places $w \in M(\mathbb{F}_q(T))$. Since the ramification indices e_v are always positive integers, we get

$$\begin{aligned}\prod_{v|w}(1-q^{-s\deg(v)})^{-1} &= \prod_{v|w}(1-q^{-sf_v\deg(w)})^{-1}\\ &\leq \left((1-q^{-s\deg(w)})^{-1}\right)^{\sum_{v|w} f_v}\\ &\leq \left((1-q^{-s\deg(w)})^{-1}\right)^{\sum_{v|w} e_v f_v}\\ &= \left((1-q^{-s\deg(w)})^{-1}\right)^{[k\colon\, \mathbb{F}_q(T)]}\end{aligned}$$

for all places $w \in M(\mathbb{F}_q(T))$. Thus $\zeta_k(s) \leq \left(\zeta_{\mathbb{F}_q(T)}(s)\right)^e$.

Now if $s \leq 1$ we have

$$\begin{aligned}\sum_{l=0}^{m} a(l)q^{-sl} &\leq \sum_{l=0}^{m} q^{(m-l)(1-s+\varepsilon)}a(l)q^{-sl}\\ &= q^{m(1-s+\varepsilon)}\sum_{l=0}^{m} a(l)q^{-l(1+\varepsilon)}\\ &< q^{m(1-s+\varepsilon)}\sum_{l=0}^{\infty} a(l)q^{-l(1+\varepsilon)}\\ &= q^{m(1-s+\varepsilon)}\zeta_k(1+\varepsilon)\\ &\leq q^{m(1-s+\varepsilon)}\left(\zeta_{\mathbb{F}_q(T)}(1+\varepsilon)\right)^e\\ &\ll q^{m(1-s+\varepsilon)},\end{aligned}$$

and if $s > 1+\varepsilon$

$$\begin{aligned}\sum_{l\geq m} a(l)q^{-sl} &= \sum_{l\geq m} a(l)q^{-(1+\varepsilon)l}q^{-(s-1-\varepsilon)l}\\ &< q^{-m(s-1-\varepsilon)}\sum_{l\geq m} a(l)q^{-(1+\varepsilon)l}\\ &\leq q^{-m(s-1-\varepsilon)}\zeta_k(1+\varepsilon)\\ &\ll q^{-m(s-1-\varepsilon)}.\end{aligned}$$

Lemma 3. *Fix a function field k. Then for all $\varepsilon > 0$*

$$q^{g_k(1-\varepsilon)} \ll J_k \ll q^{g_k(1+\varepsilon)},$$

where the implicit constants depend only on q, $[k\colon \mathbb{F}_q(T)]$ and ε.

We note that the lower bound in Lemma 3 will not be required subsequently; we include it for completeness and because the bound has interest beyond our purposes here.

Proof. If the genus is 0, then $J_k = 1$ and the statement is true, so assume that $g_k \geq 1$.

By Lemma 2

$$\begin{aligned}J_k q^{g_k} &\ll \frac{J_k}{q-1}(q^{g_k}-1)\\ &= a(2g_k-1)\\ &\ll q^{(2g_k-1)(1+\varepsilon/2)}\\ &< q^{g_k(2+\varepsilon)},\end{aligned}$$

so that $J_k \ll q^{g_k(1+\varepsilon)}$.

By Lemma 2,

$$\begin{aligned}\zeta_k(s) &= \sum_{l=0}^{\infty} a(l)q^{-sl} \\ &= \frac{J_k}{q-1}\sum_{l=2g_k-1}^{\infty}(q^{l+1-g_k}-1)q^{-sl} + \sum_{l=0}^{2g_k-2} a(l)q^{-sl} \\ &= \frac{J_k q^{s(1-2g_k)}}{q-1}\left(\frac{q^{g_k}}{1-q^{1-s}} - \frac{1}{1-q^{-s}}\right) + \sum_{l=0}^{2g_k-2} a(l)q^{-sl}.\end{aligned}$$

This identity is used to analytically continue the zeta function to the complex plane, with simple poles at $s = 0, 1$. Further, by the "Riemann Hypothesis", i.e., Hasse-Weil Theorem (see [S, V.2.1 Theorem], for example), this analytic continuation has exactly $2g_k$ zeros (counting multiplicity), all of which have real part equal to $1/2$. In particular, the analytically continued zeta function is negative for all $1/2 < s < 1$. Hence, setting $s = 1-\varepsilon$, we have for all positive $\varepsilon < 1/2$

$$\frac{J_k q^{(1-\varepsilon)(1-2g_k)}}{q-1}\left(\frac{q^{g_k}}{1-q^{\varepsilon}} - \frac{1}{1-q^{\varepsilon-1}}\right) + \sum_{l=0}^{2g_k-2} a(l)q^{l(\varepsilon-1)} < 0.$$

Since we are assuming $g_k \geq 1$, we have $\sum_{l=0}^{2g_k-2} a(l)q^{l(\varepsilon-1)} \geq a(0) = 1$. Thus

$$\frac{J_k q^{(1-\varepsilon)(1-2g_k)}}{q-1}\left(\frac{q^{g_k}}{1-q^{\varepsilon}} - \frac{1}{1-q^{\varepsilon-1}}\right) < -1.$$

Multiplying both sides by $(1-q^{\varepsilon})(1-q^{\varepsilon-1})$ (which is negative), we get

$$\begin{aligned}(q^{\varepsilon}-1)(1-q^{\varepsilon-1}) &< \frac{J_k q^{(1-\varepsilon)(1-2g_k)}}{q-1}\left(q^{g_k}(1-q^{\varepsilon-1}) - (1-q^{\varepsilon})\right) \\ &\leq \frac{J_k q^{(1-\varepsilon)(1-2g_k)}}{q-1}(q^{g_k}-1) \\ &< \frac{J_k q^{g_k(2\varepsilon-1)} q^{(1-\varepsilon)}}{q-1}.\end{aligned}$$

This shows the other inequality.

We note that there always exists a divisor of degree 1 [S, V.1.11 Corollary].

Lemma 4. *Let k be a function field and suppose $n \geq 2$ is an integer. Set representatives $\mathfrak{A}_1, \ldots, \mathfrak{A}_{J_k}$ of the divisor classes of degree 0 and fix a divisor $\mathfrak{A}_0$ of degree 1. Then for all integers $0 \leq i \leq 2g_k - 2$ we have*

$$\sum_{j=1}^{J_k} \lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) \ll a(i)q^{(n-1)i/2},$$

where the implicit constant depends only on n and q.

Proof. By (4) we have $\sum_{j=1}^{J_k} q^{l(\mathfrak{A}_j+i\mathfrak{A}_0,1)} - 1 = (q-1)a(i)$. Setting $c_j = l(\mathfrak{A}_j + i\mathfrak{A}_0, 1)$, we get $c_j \leq \frac{i+2}{2}$ by Lemma 1, whence

$$\begin{aligned}\sum_{j=1}^{J_k} \lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) &= \sum_{j=1}^{J_k} q^{nc_j} - 1 \\ &= \sum_{j=1}^{J_k} \big(q^{c_j}-1\big)\big(q^{(n-1)c_j} + q^{(n-2)c_j} + \cdots + 1\big) \\ &\ll \sum_{j=1}^{J_k} \big(q^{c_j}-1\big) q^{(n-1)i/2} \\ &\ll a(i) q^{(n-1)i/2}.\end{aligned}$$

Lemma 5. *Let k be a function field and suppose $n \geq 2$ is an integer. Set representatives $\mathfrak{A}_1, \ldots, \mathfrak{A}_{J_k}$ of the divisor classes of degree 0 and fix a divisor $\mathfrak{A}_0$ of degree 1. For all integers $0 \leq i \leq 2g_k - 2$ we have*

$$\sum_{j=1}^{J_k} \lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) - (q^{n(i+1-g_k)} - 1) = q^{n(i+1-g_k)} \sum_{j=1}^{J_k} \lambda(\mathfrak{A}_j + (2g_k-2-i)\mathfrak{A}_0, n).$$

Proof. Let $\mathfrak{W}$ be a divisor in the canonical class. By the definition of λ and Lemma 1,

$$\begin{aligned}\lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) - (q^{n(i+1-g_k)} - 1) &= q^{nl(\mathfrak{A}_j+i\mathfrak{A}_0,1)} - q^{n(i+1-g_k)} \\ &= q^{n(i+1-g_k)}\left(q^{nl(\mathfrak{W}-\mathfrak{A}_j-i\mathfrak{A}_0,1)} - 1\right)\end{aligned}$$

for all $0 \leq i \leq 2g_k - 2$ and $j = 1, \ldots, J_k$. Clearly $\mathfrak{W} - \mathfrak{A}_j - i\mathfrak{A}_0$ runs through all divisor classes of degree $2g_k - 2 - i$ as j goes from 1 to J_k, since $\deg(\mathfrak{W}) = 2g_k - 2$. Thus

$$\sum_{j=1}^{J_k} \lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) - \big(q^{n(i+1-g_k)} - 1\big) = q^{n(i+1-g_k)} \sum_{j=1}^{J_k} \lambda\big(\mathfrak{A}_j + (2g_k-2-i)\mathfrak{A}_0, n\big).$$

Proof of Theorem 2. To ease notation, write J and g for J_k and g_k, respectively. Set representatives $\mathfrak{A}_1, \ldots, \mathfrak{A}_J$ of the divisor classes of degree 0 and fix a divisor $\mathfrak{A}_0$ of degree 1. All implicit constants appearing in our proof depend only on (at most) n, e, q and ε.

Using Möbius inversion exactly as in [T2, §4], we get

$$\begin{aligned}(q-1)N_k(n,1,m) &= \sum_{j=1}^{J} \lambda'(\mathfrak{A}_j + m\mathfrak{A}_0, n) \\ &= \sum_{j=1}^{J} \sum_{\mathfrak{C}\geq 0} \mu(\mathfrak{C})\lambda(\mathfrak{A}_j + m\mathfrak{A}_0 - \mathfrak{C}, n) \\ &= \sum_{l=0}^{m} b(l) \sum_{j=1}^{J} \lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n),\end{aligned} \tag{5}$$

where the last equation follows from the fact that $l(\mathfrak{A}, n) = l(\mathfrak{B}, n)$ whenever $\mathfrak{A}$ and $\mathfrak{B}$ are linearly equivalent divisors.

Now assume $m \geq 2g-1$. From (5) and Lemma 1 we have

$$\begin{aligned}(q-1)N_k(n,1,m) &= \sum_{l=0}^{m} b(l) \sum_{j=1}^{J} \lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) \\ &= \sum_{j=1}^{J}\sum_{l=0}^{\infty} b(l)q^{n(m-l+1-g)} - \sum_{j=1}^{J}\sum_{l=0}^{m} b(l) - \sum_{j=1}^{J}\sum_{l=m+1}^{\infty} b(l)q^{n(m-l+1-g)} \\ &\quad + \sum_{j=1}^{J}\sum_{l=m-2g+2}^{m} b(l)\left(\lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) - (q^{n(m-l+1-g)} - 1)\right).\end{aligned} \tag{6}$$

By (3)

$$\sum_{j=1}^{J}\sum_{l=0}^{\infty} b(l)q^{n(m-l+1-g)} = \frac{Jq^{n(m+1-g)}}{\zeta_k(n)}. \tag{7}$$

Clearly $a(l) \geq |b(l)|$ always, so that by Lemmas 2 and 3

$$\left|\sum_{j=1}^{J}\sum_{l=0}^{m} b(l)\right| \leq \sum_{j=1}^{J}\sum_{l=0}^{m} a(l) \ll Jq^{m(1+\varepsilon)} \ll q^{m(1+\varepsilon)}q^{g(1+\varepsilon)} \tag{8}$$

for all $\varepsilon > 0$. Similarly (and since $n \geq 2$)

$$\left|\sum_{j=1}^{J}\sum_{l=m+1}^{\infty} b(l)q^{n(m-l+1-g)}\right| \leq \sum_{j=1}^{J}\sum_{l=m+1}^{\infty} a(l)q^{n(m-l+1-g)} \ll Jq^{-ng}q^{m(1+\varepsilon)} \ll q^{m(1+\varepsilon)}. \tag{9}$$

We now turn to the last term in (6). First, by Lemma 1 we have

$$0 \leq \lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) - (q^{n((m-l)+1-g)} - 1)$$

for all $j = 1, \dots, J$ and $l = m - 2g + 2, \dots, m$. Hence

$$\begin{aligned}
&\left| \sum_{j=1}^{J} \sum_{l=m-2g+2}^{m} b(l) \left(\lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) - (q^{n(m-l+1-g)} - 1) \right) \right| \\
&\qquad \leq \sum_{j=1}^{J} \sum_{l=m-2g+2}^{m} a(l) \left(\lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) - (q^{n(m-l+1-g)} - 1) \right) \qquad (10) \\
&\qquad = \sum_{i=0}^{2g-2} \sum_{j=1}^{J} a(m-i) \left(\lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) - (q^{n(i+1-g)} - 1) \right),
\end{aligned}$$

where we have written i for $m-l$. Setting $i' = 2g-2-i$, by Lemmas 2 (applied to $a(m+i'-2g+2)$), 4 and 5

$$\begin{aligned}
&\sum_{i=0}^{2g-2} \sum_{j=1}^{J} a(m-i) \left(\lambda(\mathfrak{A}_j + i\mathfrak{A}_0, n) - (q^{n(i+1-g)} - 1) \right) \\
&\qquad = \sum_{i'=0}^{2g-2} \sum_{j=1}^{J} a(m+i'-2g+2) q^{n(g-1-i')} \lambda(\mathfrak{A}_j + i'\mathfrak{A}_0, n) \\
&\qquad \ll \sum_{i'=0}^{2g-2} a(m+i'-2g+2) q^{n(g-1-i')} a(i') q^{(n-1)i'/2} \qquad (11) \\
&\qquad \ll q^{m(1+\varepsilon)} q^{g(n-2-2\varepsilon)} \sum_{i'=0}^{2g-2} a(i') q^{i'(1+\varepsilon-(n+1)/2)}.
\end{aligned}$$

If $n \geq 4$ and $\varepsilon \leq 1/4$, then $(1+\varepsilon) - (n+1)/2 \leq -5/4$, so that by (10), (11) and Lemma 2

$$\begin{aligned}
&\left| \sum_{j=1}^{J} \sum_{l=m-2g+2}^{m} b(l) \left(\lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) - (q^{n(m-l+1-g)} - 1) \right) \right| \\
&\qquad \ll q^{m(1+\varepsilon)} q^{g(n-2-2\varepsilon)} \sum_{i'=0}^{2g-2} a(i') q^{i'(-5/4)} \\
&\qquad < q^{m(1+\varepsilon)} q^{g(n-2-2\varepsilon)} \zeta_k(5/4) \\
&\qquad \ll q^{m(1+\varepsilon)} q^{g(n-2-2\varepsilon)}. \qquad (12)
\end{aligned}$$

If $n = 2, 3$ we use $a(i') \ll q^{i'(1+\varepsilon/2)}$, so by (10) and (11)

$$\begin{aligned}\left|\sum_{j=1}^{J}\sum_{l=m-2g+2}^{m} b(l)\left(\lambda(\mathfrak{A}_j + (m-l)\mathfrak{A}_0, n) - (q^{n(m-l+1-g)} - 1)\right)\right| \\ \ll q^{m(1+\varepsilon)}q^{g(n-2-2\varepsilon)}\sum_{i'=0}^{2g-2} a(i')q^{i'(1+\varepsilon-(n+1)/2)} \\ \ll q^{m(1+\varepsilon)}q^{g(n-2-2\varepsilon)}\sum_{i'=0}^{2g-2} q^{(i'/2)(4+3\varepsilon-(n+1))} \\ \ll q^{m(1+\varepsilon)}q^{g(n-2-2\varepsilon)}q^{g(4+3\varepsilon-(n+1))} \\ = q^{m(1+\varepsilon)}q^{g(1+\varepsilon)}.\end{aligned} \tag{13}$$

The case where $m \geq 2g - 1$ follows from (1), (6)-(9), (12), (13) and Lemma 2.

We now turn to the case where $m \leq 2g - 2$. By (5) and the definitions we have

$$\begin{aligned}(q-1)N_k(n, 1, m) &= \sum_{j=1}^{J}\lambda'(\mathfrak{A}_j + m\mathfrak{A}_0, n) \\ &\leq \sum_{j=1}^{J}\lambda(\mathfrak{A}_j + m\mathfrak{A}_0, n).\end{aligned}$$

The proof is completed by this and Lemmas 2 and 4.

Proof of Corollary 1. By (1) and Lemmas 2 and 3,

$$S_k(n, 1) < J_k q^{-ng_k} \ll 1 \tag{14}$$

for all function fields k and all integers $n \geq 2$. One readily verifies that

$$q^{m(1+\varepsilon)}q^{g_k(n-2-2\varepsilon)} \ll q^{nm/2} \tag{15}$$

for all integers $n \geq 4,\ m \geq 2g_k - 1$ and all $\varepsilon \leq 1/4$. Also,

$$q^{m(1+\varepsilon)}q^{g_k(1+\varepsilon)} \ll q^{(3m/2)(1+\varepsilon)} \tag{16}$$

for all integers $m \geq 2g_k - 1$ and all $\varepsilon > 0$. Corollary 1 follows from Theorem 2 and (14)-(16).

The proof of Corollary 2 will require one further auxiliary result.

Lemma 6. *Suppose $K \supseteq k$ are function fields and write $d = [K\colon k]$. Then the number N of intermediate fields L with $k \subseteq L \subseteq K$ satisfies $N \leq d2^{d!}$.*

Proof. Let $k \subseteq L \subseteq K$. Suppose first that L is a separable extension of k. We have $[L\colon k] \leq [K\colon k] = d$, whence by elementary Galois theory at most $2^{d!}$ possible L. Now suppose that L is not a separable extension of k. Then we have $k \subseteq L_s \subset L$, where L_s is the separable closure of k in L. Then we must have $[L\colon L_s] = p^r$ for some positive integer r (recall that p is the characteristic of all our fields). Moreover, $L_s = \{a^{p^r} : a \in L\}$ (see [S, Proposition III.9.2], for example). Since each element of L_s has a unique p^r-th root, we therefore have $L = \{a \in K\colon a^{p^r} \in L_s\}$, so that L_s and p^r completely determine L. Since both $[L\colon L_s]$ and $[L_s\colon k]$ are no greater than d, we get our estimate.

Proof of Corollary 2. Set $d = [K\colon k]$. We then have

$$N_k(n, K, m) = N_K(n, 1, m) - \sum_{\substack{d' < d \\ d' | d}} \sum_{\substack{k \subseteq L \subset K \\ [L\colon k] = d'}} N_k(n, L, d'm/d). \tag{17}$$

Clearly $N_k(n, L, d'm/d) \leq N_L(n, 1, d'm/d)$ always. The case where $m \geq 2g_K - 1$ of Corollary 2 follows from Theorem 2, Corollary 1, Lemma 6, and (15)-(17). Now suppose $m \leq 2g_K - 2$. We have the trivial bound $N_k(n, K, m) \leq N_K(n, 1, m)$. As remarked following the statement of Corollary 2, we have $S_K(n, 1)q^{nm} \ll q^{m(\frac{n+1}{2}+\varepsilon)}$ when $m < 2g_K - 1$ by Lemmas 2 and 3. Thus, this case of Corollary 2 follows directly from Theorem 2.

Proof of Theorem 1

As stated before, we will use Corollary 2 and (2) to prove Theorem 1. Throughout this section the function field k is fixed and, as before, we simply write q for q_k. We write $e = [k\colon \mathbb{F}_q(T)]$ as in the statement of Theorem 1. All implicit constants depend only on (at most) n, d, e, k and ε.

Corollary 2 to Theorem 1 uses the quantity $\delta_n(K/k)$. It turns out simpler to use $\delta_2(K/k)$. We thus need to compare the two quantities and get some useful estimates.

Lemma 7. *Let $d > 1$ and let $K \supseteq k$ be a function field with $d = [K\colon k]$ and $q_K = q$. Then*

$$\delta_2(K/k) + 1 - d \leq \delta_i(K/k) \leq \delta_j(K/k)$$

for all $2 \leq j \leq i$. *Also*

$$\frac{g_K}{d-1} - c_1(k,d) \leq de\delta_2(K/k) \leq g_K + c_2(k,d),$$

where $c_1(k,d)$ *and* $c_2(k,d)$ *are positive integers depending only on* k *and* d.

Proof. Suppose $\delta_j(K/k) = h(P)$ for $P \in \mathbb{P}^{j-1}(K)$ with $k(P) = K$. Without loss of generality we have $P = (1\colon \alpha_1\colon \cdots : \alpha_{j-1})$. But then $P' = (1\colon \cdots : 1\colon \alpha_1\colon \cdots : \alpha_{j-1})$ also generates K over k for any number of 1's, and clearly $h(P') = h(P)$. Thus, $\delta_i(K/k) \leq \delta_j(K/k)$ whenever $i \geq j \geq 2$.

Now suppose $i > 2$ and write $\delta_i(K/k) = h(1 : \alpha_1 : \cdots : \alpha_{i-1})$, where $K = k(\alpha_1, \ldots, \alpha_{i-1})$. Write K_s for the separable closure of k in K and set $s = [K_s\colon k]$. Arguing exactly as in the proof of [T1, Lemma 7], we claim that there exist polynomials $f_1, ..., f_{i-1}$ in $\mathbb{F}_q[T]$, either zero or of degree at most $s-1$, such that $K_s \subseteq k(\alpha)$ for $\alpha = \sum_{l=1}^{i-1} f_l\alpha_l$. This is trivially true if $s = 1$, so assume $s > 1$. For $l = 1, \ldots, s$ let $\sigma_l : K \to \overline{\mathbb{F}_p(T)}$ be the k-homomorphisms of K. By induction on i we easily deduce that for each nonzero homogeneous polynomial $P(X_1, ..., X_{i-1}) \in \overline{\mathbb{F}_p(T)}[X_1, ..., X_{i-1}]$ of degree A there exist elements $f_1, ..., f_{i-1} \in \mathbb{F}_q[T]$, either zero or of degree at most A, such that $P(f_1, ..., f_{i-1}) \neq 0$. We let

$$P(X_1, ..., X_{i-1}) = \prod_{l=2}^{s}\sum_{j=1}^{i-1}(\sigma_1(\alpha_j) - \sigma_l(\alpha_j))X_j.$$

Since the σ_l are pairwise distinct k-homomorphisms on K and $K = k(\alpha_1, \ldots, \alpha_{i-1})$, we conclude that for each $l > 1$ there exists an α_j among $\alpha_1, ..., \alpha_{i-1}$ with $\sigma_1(\alpha_j) \neq \sigma_l(\alpha_j)$. Therefore P is not the zero polynomial. Furthermore the degree of P is $s-1$. Hence we can find $f_1, \ldots, f_{i-1} \in \mathbb{F}_q[T]$, either zero or of degree at most $s-1$, with $P(f_1, \ldots, f_{i-1}) \neq 0$. But this means that $\sigma_1(\alpha) \neq \sigma_l(\alpha)$ for $l = 2, \ldots, s$ where $\alpha = \sum_{j=1}^{i-1} f_j\alpha_j$. Therefore $K_s \subseteq k(\alpha)$.

With α as above, an easy calculation shows that

$$h(1\colon \alpha) \leq h(1\colon \alpha_1\colon \cdots : \alpha_{i-1}) + (s-1)h(1\colon T) = \delta_i(K/k) + s - 1,$$

where the inequality holds in fact for each local component of the height. This suffices to prove that $\delta_2(K/k) - d + 1 \leq \delta_i(K/k)$ in the case where $K_s = K$. If $K_s \neq K$, then α may not generate the entire field K, but some p^rth root θ of α does by [S, Proposition III.9.2]. In this case we have $p^r h(1\colon \theta) = h(1\colon \alpha) \leq \delta_i(K/k) + s - 1$ and again $\delta_2(K/k) - d + 1 \leq \delta_i(K/k)$.

The upper bound for $\delta_2(K/k)$ is [W2, Theorem 1.1]. The lower bound is [T1, Lemma 6]. (Although separability is a stated assumption in §IV of [T1], the proof of Lemma 6 does not use this.)

As noted in the introduction, all of our $\delta_2(K/k)$ (since they are the height of some point in $\mathbb{P}^1(K)$) are necessarily of the form m/de for some non-negative integer m. We will need the following estimate.

Lemma 8. *For all $d \geq 2$ we have*

$$\sum_{\substack{[K:\, k]=d\\ q_K=q\\ \delta_2(K/k)=m/de}} 1 \ll q^{(d+1)m}.$$

Proof. Certainly the number of function fields K with $\delta_2(K/k) = m/de$ for a given m is no greater than the number of α of degree d over k and $h(1\colon \alpha) = m/de$. Each such α has a defining polynomial P of degree d over k, and by [RT, Lemma 4.9] we have $h(P) = dh(1\colon \alpha) = m/e$, where $h(P)$ denotes the height of the coefficient vector of P, which we view as a point in $\mathbb{P}^d(k)$. We conclude that the number of α of degree d over k with height $h(1\colon \alpha) = m/de$ is no more than $dN_k(d+1, 1, m)$. Thus, by Corollary 1 we have

$$\sum_{\substack{[K:\, k]=d\\ q_K=q\\ \delta_2(K/k)=m/de}} 1 \leq dN_k(d+1, 1, m) \ll q^{(d+1)m}.$$

Lemma 9. *For all integers $d > 1$ and $m \geq 0$,*

$$\sum_{\substack{[K:\, k]=d\\ q_K=q\\ g_K=m}} 1 \leq \sum_{\substack{[K:\, k]=d\\ q_K=q\\ g_K\leq m}} 1 \ll q^{(d+1)m}.$$

Proof. By Lemmas 7 and 8

$$\begin{aligned}\sum_{\substack{[K:\,k]=d\\ q_K=q\\ g_K\le m}} 1 &\le \sum_{\substack{[K:\,k]=d\\ q_K=q\\ de\delta_2(K/k)\le m+c_2(k,d)}} 1\\ &= \sum_{i=0}^{m+c_2(k,d)} \sum_{\substack{[K:\,k]=d\\ q_K=q\\ de\delta_2(K/k)=i}} 1\\ &\ll \sum_{i=0}^{m+c_2(k,d)} q^{(d+1)i}\\ &\ll q^{(d+1)m}.\end{aligned}$$

Proof of Theorem 1. We assume that $\varepsilon>0$ and that n and d are positive integers with $n\ge 4$ and $d>1$ initially. By (2) and Corollary 2 to Theorem 2,

$$\begin{aligned}N_k(n,d,m) &= \sum_{\substack{[K:\,k]=d\\ q_K=q}} N_k(n,K,m)\\ &= \sum_{\substack{[K:\,k]=d\\ q_K=q\\ de\delta_n(K/k)\le m}} S_K(n,1)q_K^{nm} + O\left(\sum_{\substack{[K:\,k]=d\\ q_K=q\\ 2g_K-1\le m}} q^{nm/2}\right)\\ &\quad + O\left(\sum_{\substack{[K:\,k]=d\\ q_K=q\\ de\delta_n(K/k)\le m<2g_K-1}} q^{m(\frac{n+1+\varepsilon}{2})}\right).\end{aligned} \tag{18}$$

First, for the main term we claim that

$$S_k(n,d)=\sum_{\substack{[K:\,k]=d\\ q_K=q}} S_K(n,1)$$

converges whenever $n>d+2$. Moreover, we claim that

$$\sum_{\substack{[K:\,k]=d\\ q_K=q\\ de\delta_n(K/k)\ge m}} S_K(n,1)\ll q^{m(d+2+\varepsilon-n)} \tag{19}$$

whenever $n>d+2+\varepsilon$. Recalling the definition of $S_K(n,1)$ from (1) and applying Lemmas 2 and

3, we get $S_K(n,1) \ll q^{g_K(1+\varepsilon-n)}$ and therefore by Lemmas 7 and 8

$$\begin{aligned}
\sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_n(K/k)\geq m}} S_K(n,1) &\ll \sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_n(K/k)\geq m}} q^{g_K(1+\varepsilon-n)} \\
&\leq \sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_2(K/k)\geq m}} q^{g_K(1+\varepsilon-n)} \\
&\ll \sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_2(K/k)\geq m}} q^{de\delta_2(K/k)(1+\varepsilon-n)} \\
&= \sum_{i=m}^{\infty} \sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_2(K/k)=i}} q^{i(1+\varepsilon-n)} \\
&\ll \sum_{i=m}^{\infty} q^{i(d+2+\varepsilon-n)} \\
&\ll q^{m(d+2+\varepsilon-n)},
\end{aligned}$$

proving (19) and also that the sum defining $S_k(n,d)$ converges.

Now for the error terms. By Lemma 9

$$\sum_{\substack{[K:\ k]=d \\ q_K=q \\ 2g_K-1\leq m}} q^{nm/2} \ll q^{nm/2} q^{m(d+1)/2} = q^{\frac{m}{2}(n+d+1)}, \tag{20}$$

and by Lemmas 7 and 8

$$\begin{aligned}
\sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_n(K/k)\leq m}} q^{m(\frac{n+1+\varepsilon}{2})} &\leq \sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_2(K/k)\leq m+de(d-1)}} q^{m(\frac{n+1+\varepsilon}{2})} \\
&= \sum_{i=0}^{m+de(d-1)} \sum_{\substack{[K:\ k]=d \\ q_K=q \\ de\delta_2(K/k)=i}} q^{m(\frac{n+1+\varepsilon}{2})} \\
&\ll \sum_{i=0}^{m+de(d-1)} q^{m(\frac{n+1+\varepsilon}{2})} q^{i(d+1)} \\
&\ll q^{m(\frac{n+1+\varepsilon}{2})} q^{m(d+1)} \\
&= q^{\frac{m}{2}(n+2d+3+\varepsilon)}.
\end{aligned} \tag{21}$$

The proof of Theorem 1 is completed by (18)-(21).

We now turn to the Proposition. At this point we are forced to distinguish between separable and inseparable extensions of the field k. Similar to (2), we write

$$N_k^{\mathrm{sep}}(n,d,m) = \sum_{\substack{[K\colon k]=d \\ q_K=q_k}}^{\mathrm{sep}} N_k(n,K,m)$$

where the superscript on the summation indicates that we sum only over separable extensions K. Similarly, we write $NF_k^{\mathrm{sep}}(n,d,m)$ for the number of forms counted in $NF_k(n,d,m)$ where each $k\big(P(\mathbf{L}_i)\big)$ is a separable extension of k.

We first show that

$$NF_k^{\mathrm{sep}}(n,d,m) = \frac{1}{d} N_k^{\mathrm{sep}}(n,d,m). \tag{22}$$

Towards that end, let $\mathcal{N}_k^{\mathrm{sep}}(n,d,m)$ be the set counted by $N_k^{\mathrm{sep}}(n,d,m)$, and let $\mathcal{NF}_k^{\mathrm{sep}}(n,d,m)$ be the set counted by $NF_k^{\mathrm{sep}}(n,d,m)$. Suppose $F(\mathbf{X}) = \prod_{i=1}^d L_i(\mathbf{X})$ is a decomposable form in $k[\mathbf{X}]$ of degree d. By unique factorisation the unordered d-tuple $\big(P(\mathbf{L}_1),\ldots,P(\mathbf{L}_d)\big)$ is uniquely determined by F. Now if $F \in \mathcal{NF}_k^{\mathrm{sep}}(n,d,m)$ then $P(\mathbf{L}_1),\ldots,P(\mathbf{L}_d)$ are the d pairwise distinct conjugates (over k) of some point P, and, by definition of $\mathcal{NF}_k^{\mathrm{sep}}(n,d,m)$, each $P(\mathbf{L}_i)$ generates a separable extension of k of degree d and effective degree d. Hence $dh\big(P(\mathbf{L}_i)\big) = dh\big(P\big)$ for each $i = 1,\ldots,d$. From [RT, Lemma 4.9] we have $h\big(P(F)\big) = dh\big(P\big)$, so that each $P(\mathbf{L}_i)$ lies in $\mathcal{N}_k^{\mathrm{sep}}(n,d,m)$ (recall that the counting function N_k takes into account the effective degree). On the other hand any $P \in \mathcal{N}_k^{\mathrm{sep}}(n,d,m)$ has d pairwise distinct conjugates $P_1,\ldots,P_d$ over k of equal height, and each of these generates a separable extension of k of degree d and effective degree d. These conjugates give rise to linear forms $L_1,\ldots,L_d$ (i.e., $P_i = P(\mathbf{L}_i)$ for $i = 1,\ldots d$) whose product $F(\mathbf{X}) = \prod_{i=1}^d L_i(\mathbf{X})$ lies in $\mathcal{NF}_k^{\mathrm{sep}}(n,d,m)$. This shows that there exists a d-to-1 correspondence between $\mathcal{N}_k^{\mathrm{sep}}(n,d,m)$ and $\mathcal{NF}_k^{\mathrm{sep}}(n,d,m)$, and this proves (22).

As in the proof of Lemmas 6 and 7, for an extension K of k we write K_s for the separable closure of k in K. For such a field K we have $[K\colon K_s] = p^r$ for some integer $r \geq 0$ and $K_s = \{a^{p^r} : a \in K\}$. As remarked above in the proofs of Lemmas 6 and 7, if $P = (\alpha_0\colon \cdots : \alpha_n) \in \mathbb{P}^n(K)$ with $k(P) = K$, then $Q = (\alpha_0^{p^r} : \cdots : \alpha_n^{p^r}) \in \mathbb{P}^n(K_s)$ with $K_s = k(Q)$ and $p^r h(P) = h(Q)$. Hence $N_k(n,K_s,m) = N_k(n,K,m)$ (recall that the definition of N_k takes into account the effective degree of the extension), so that

$$\begin{aligned} N_k(n,d,m) &= \sum_{p^r|d} N_k^{\mathrm{sep}}(n, d/p^r, m) \\ NF_k(n,d,m) &= \sum_{p^r|d} NF_k^{\mathrm{sep}}(n, d/p^r, m). \end{aligned} \tag{23}$$

We claim that

$$N_k^{\mathrm{sep}}(n,d,m) = \begin{cases} N_k(n,d,m) - N_k(n,d/p,m) & \text{if } p|d, \\ N_k(n,d,m) & \text{if } p \nmid d. \end{cases} \tag{24}$$

We prove this by induction on the highest power of p dividing d. This is clearly true if $p \nmid d$, so assume p^r is the highest power of p dividing d with $r > 0$. Then by (23) and the induction hypothesis,

$$\begin{aligned} N_k(n,d,m) &= \sum_{i=0}^{r} N_k^{\mathrm{sep}}(n, d/p^i, m) \\ &= N_k^{\mathrm{sep}}(n,d,m) + \sum_{i=1}^{r} N_k^{\mathrm{sep}}(n, d/p^i, m) \\ &= N_k^{\mathrm{sep}}(n,d,m) + N_k(n, d/p^r, m) + \sum_{i=1}^{r-1} N_k(n, d/p^i, m) - N_k(n, d/p^{i+1}, m) \\ &= N_k^{\mathrm{sep}}(n,d,m) + N_k(n, d/p, m). \end{aligned}$$

The proof of the Proposition is completed with (22) – (24).

Finally, we turn to our remark regarding possible asymptotic results. Though we did not need it for the proof of Lemma 9 above, it is known (see [T3, Theorem 1]) that $N_k(2,d,m)$ is actually asymptotic to $dN_k(d+1,1,m)$. In particular,

$$N_k(2,d,m) \gg\ll q^{m(d+1)}.$$

On the other hand, we clearly have $N_k(n,d,m) \geq N_k(2,d,m)$ for all $n \geq 2$. This immediately implies that $N_k(n,d,m)$ cannot be asymptotic to cq^{nm} for any real c when $n < d+1$.

Acknowledgements

The second author thanks Paula Tretkoff for inspiring questions and the Institut des Hautes Études Scientifiques in Bures-sur-Yvette, where parts of this work have been done, for the wonderful hospitality. The authors also thank the anonymous referee for his or her careful reading of the original manuscript.

References

[A] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.

[D] S. A. DiPippo, *Spaces of Rational Functions on Curves Over Finite Fields*, Ph. D. Thesis, Harvard, 1990.

[H] T. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[MV1] D. Masser and J. Vaaler, *Counting algebraic numbers of large height I*, Dev. Math. **16** (2008), 237-243.

[MV2] ———, *Counting algebraic numbers of large height II*, Trans. Amer. Math. Soc. **359** (2007), 427-445.

[RT] D. Roy and J.L. Thunder, *An absolute Siegel's lemma*, J. reine angew. Math **476** (1996), 1-26.

[Scha] S. Schanuel, *Heights in number fields*, Bull. Math. Soc. France **107** (1979), 433-449.

[Schm1] W.M. Schmidt, *Northcott's Theorem on heights I*, Monatsh. Math. **115** (1993), 169-183.

[Schm2] ———, *Northcott's Theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343-375.

[S] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[T1] J.L. Thunder, *Siegel's lemma for function fields*, Mich. Math. J. **42** (1995), 147-162.

[T2] ———, *Counting subspaces of given height defined over a function field*, J. Number Theory **128** (2008), 2973-3004.

[T3] ———, *More on heights defined over a function field*, Rocky Mountain J. Math. **29** (2009), 1303-1322.

[Wa] D. Wan, *Heights and zeta functions in function fields*, The Arithmetic of Function Fields, W. de Gruyter, Berlin, 1992, pp. 455-463.

[W1] M. Widmer, *Counting points of fixed degree and bounded height*, Acta Arith. **140.2** (2009), 145-168.

[W2] ———, *Small generators of function fields*, J. Théorie Nombres Bordeaux **22 no. 3** (2010), 544-551.

Dept. of Mathematics, Northern Illinois University, DeKalb, IL 60115, USA
E-mail address: `jthunder@ math.niu.edu`

Dept. for Analysis and Computational Number Theory, Graz Univ. of Technology, Steyrergasse 30/II, A-8010 Graz, Austria
E-mail address: `widmer@ math.tugraz.at`