ALGEBRAIC POINTS OF SMALL HEIGHT MISSING A UNION OF VARIETIES

LENNY FUKSHANSKY

ABSTRACT. Let K be a number field, $\overline{\mathbb{Q}}$, or the field of rational functions on a smooth projective curve of genus 0 or 1 over a perfect field, and let V be a subspace of K^N, $N \geq 2$. Let Z_K be a union of varieties defined over K such that $V \nsubseteq Z_K$. We prove the existence of a point of small height in $V \setminus Z_K$, providing an explicit upper bound on the height of such a point in terms of the height of V and the degree of a hypersurface containing Z_K, where dependence on both is optimal. This generalizes and improves upon the results of [6] and [7]. A key tool we develop to treat the function field case of the problem is a version of Siegel's lemma with inhomogeneous heights, which extends a result of [20]. As a corollary of the method, we derive an explicit lower bound for the number of algebraic integers of bounded height in a fixed number field.

CONTENTS

1. INTRODUCTION

In this paper we consider the problem of finding points of small height in a vector space outside of a union of a finite collection of varieties, which can be viewed as an extension of Siegel's lemma. This generalizes previous results of the author [6], [7].

Siegel's lemma is a fundamental principle in Diophantine approximations and transcendental number theory, which is a statement about the existence of points of small height in a vector space over a global field. This is an important instance of a general problem of finding rational points on varieties. We use height functions, which are essential in Diophantine geometry, as a measure of arithmetic complexity; we denote homogeneous height on vectors by H, inhomogeneous height by h, height of a vector space by $\mathcal{H}$, and will define precisely our choice of heights below.

1991 *Mathematics Subject Classification.* Primary 11G50, 11D99; Secondary 11R04, 11R58.
Key words and phrases. heights, Siegel's lemma, polynomials, lattices.

Throughout this paper, we will write K for either a number field, a function field (i.e. a finite algebraic extension of the field of rational functions in one variable over an arbitrary field), or the algebraic closure of one or the other. The following general version of Siegel's lemma was proved in [2] if K is a number field, in [20] if K is a function field, and in [13] if K is the algebraic closure of one or the other (see also [14] for an improved constant).

Theorem 1.1 ([2], [20], [13], [14])**.** *Let K be a number field, a function field, or the algebraic closure of one or the other. Let $V \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$. Then there exists a basis $\boldsymbol{v}_1, ..., \boldsymbol{v}_L$ for V over K such that*

$$\prod_{i=1}^{L} H(\boldsymbol{v}_i) \leq C_K(L) \mathcal{H}(V), \tag{1}$$

where $C_K(L)$ is a field constant defined by equation (13) in section 2 below. In fact, if K is a number field or $\overline{\mathbb{Q}}$, then even more is true: there exists such a basis with

$$\prod_{i=1}^{L} H(\boldsymbol{v}_i) \leq \prod_{i=1}^{L} h(\boldsymbol{v}_i) \leq C_K(L) \mathcal{H}(V). \tag{2}$$

It is interesting to note that the transition from projective height H to inhomogeneous height h in Theorem 1.1 is quite straightforward over number fields (in other words, (2) is a fairly direct corollary of (1) in the number field case and over $\overline{\mathbb{Q}}$). In the function field case, however, such a transition is quite non-trivial. In fact, it seems unlikely that a direct analogue of (2) would hold over an arbitrary function field (see Remark 3.1 below). On the other hand, it is possible to produce such a bound over function fields of genus 0 or 1. In section 3 we prove the following result, which is one of the key tools we use to prove our main result, Theorem 1.4.

Theorem 1.2. *Let $\mathfrak{K}_0$ be any perfect field and let Y be a curve over $\mathfrak{K}_0$ of genus $g = 0$ or 1, i.e. Y is either a rational or an elliptic curve. Let $K = \mathfrak{K}_0(Y)$ be the field of rational functions on Y over $\mathfrak{K}_0$, and let $V \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$. Then there exists a basis $\boldsymbol{u}_1, ..., \boldsymbol{u}_L$ for V over K such that*

$$\prod_{i=1}^{L} H(\boldsymbol{u}_i) \leq \prod_{i=1}^{L} h(\boldsymbol{u}_i) \leq e^{gL} C_K(L) \mathcal{H}(V). \tag{3}$$

where $C_K(L)$ is as in (13).

An immediate consequence of Theorem 1.1 is the existence of a nonzero point $\boldsymbol{v}_1 \in V$ such that

$$H(\boldsymbol{v}_1) \leq \left(C_K(L) \mathcal{H}(V)\right)^{1/L}. \tag{4}$$

The bounds of (1) and (4) are sharp in the sense that the exponents on $H(V)$ are smallest possible. For many applications it is also important to have versions of Siegel's lemma with some additional algebraic conditions. One such example is the so called Faltings' version of Siegel's lemma, which guarantees the existence of a point of bounded norm in a vector space $V \subseteq \mathbb{R}^N$ outside of a subspace in $U \subsetneq V$ (see [5], [10], and [4]). In [6] and [7] I considered a more general related problem. Specifically, using the notation of Theorem 1.1 in the case when K is a number field, let $M \in \mathbb{Z}_{>0}$ and let $U_1, ..., U_M$ be subspaces of K^N such that $V \nsubseteq \bigcup_{i=1}^{M} U_i$. Then we can prove the existence of a non-zero point of small height in $V \setminus \bigcup_{i=1}^{M} U_i$

providing an explicit upper bound on the height of such a point. In particular, the main result of [7] is the following.

Theorem 1.3 ([7])**.** *Let K be a number field of degree d with discriminant $\mathcal{D}_K$. Let $N \geq 2$ be an integer, $l = \left[\frac{N}{2}\right]$, and let V be a subspace of K^N of dimension L, $1 \leq L \leq N$. Let $1 \leq s < L$ be an integer, and let $U_1, ..., U_M$ be nonzero subspaces of K^N with $\max_{1 \leq i \leq M}\{\dim_K(U_i)\} \leq s$. There exists a point $\boldsymbol{x} \in V \setminus \bigcup_{i=1}^M U_i$ such that*

$$H(\boldsymbol{x}) \leq B_K(N,L,s)\mathcal{H}(V)^d \left\{ \left(\sum_{i=1}^M \frac{1}{\mathcal{H}(U_i)^d} \right)^{\frac{1}{(L-s)d}} + M^{\frac{1}{(L-s)d+1}} \right\}, \tag{5}$$

where

$$B_K(N,L,s) = 2^{L(d+3)} |\mathcal{D}_K|^{\frac{L}{2}} \left((Ld)^L \binom{Nd}{ld}^{\frac{1}{2d}} \right)^{\frac{1}{L-s}}. \tag{6}$$

If $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L$ is any basis for V, then it is well known (see for instance Lemma 4.7 of [13]) that

$$\prod_{i=1}^L H(\boldsymbol{x}_i) \geq N^{-\frac{L}{2}} \mathcal{H}(V). \tag{7}$$

Let $M = 1$, and take U_1 to be a subspace of V of dimension $L-1$ generated by the vectors corresponding to the first $L-1$ successive minima of V with respect to an adelic unit cube - these are precisely the vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{L-1}$ in Theorem 1.1. Then the smallest vector in $V \setminus U_1$ will be $\boldsymbol{v}_L$ of Theorem 1.1. If we choose V so that the first $L-1$ successive minima of V are equal to 1, then (7) implies that $H(\boldsymbol{v}_L) \geq N^{-L/2}\mathcal{H}(V)$. This shows that the dependence on $\mathcal{H}(V)$ in the upper bound of Theorem 1.3 is sharp in the case $K = \mathbb{Q}$, however it is natural to expect the exponent on $\mathcal{H}(V)$ to be equal to 1 over any number field.

The proof of Theorem 1.3 relies on a counting argument. Write O_K for the ring of integers of K, and view modules $V \cap O_K$ and $U_i \cap O_K$ for all $1 \leq i \leq M$ as lattices in $\mathbb{R}^{Nd}$ under the canonical embedding of K into $\mathbb{R}^d$. Then one can count points of $V \cap O_K$ and $\bigcup_{i=1}^M U_i \cap O_K$ in a cube of side-length $2R$ centered at the origin in $\mathbb{R}^{Nd}$, and make R sufficiently large so that there exists a point $\boldsymbol{x} \in V \setminus \bigcup_{i=1}^M U_i$; now it is not difficult to estimate the height of this point. However, this argument does not extend to algebraically closed fields, since $\overline{K}$ does not embed into a finite-dimensional Euclidean space.

The main goal of this paper is to produce a generalization of Theorem 1.3 with optimal dependence on $\mathcal{H}(V)$ which holds just as well over $\overline{\mathbb{Q}}$ and over some function fields. Let us say that K is an *admissible field* if it is a number field, $\overline{\mathbb{Q}}$, or the field of rational functions on a curve of genus 0 or 1 over a perfect field. We can now state our main result.

Theorem 1.4. *Let K be an admissible field. Let $N \geq 2$ be an integer, and let V be an L-dimensional subspace of K^N, $1 \leq L \leq N$. Let $J \geq 1$ be an integer. For each $1 \leq i \leq J$, let $k_i \geq 1$ be an integer and let*

$$P_{i1}(X_1, \dots, X_N), \dots, P_{ik_i}(X_1, \dots, X_N)$$

be polynomials of respective degrees $m_{i1}, \dots, m_{ik_i} \geq 1$, *and define*

$$M_i = \max_{1 \leq j \leq k_i} m_{ij} \ \forall\ 1 \leq i \leq J, \quad M = \sum_{i=1}^{J} M_i. \tag{8}$$

Let

$$Z_K(P_{i1}, \dots, P_{ik_i}) = \{\boldsymbol{x} \in K^N : P_{i1}(\boldsymbol{x}) = \dots = P_{ik_i}(\boldsymbol{x}) = 0\},$$

and define $\mathcal{Z}_K = \bigcup_{i=1}^{J} Z_K(P_{i1}, \dots, P_{ik_i})$. *Suppose that* $V \not\subseteq \mathcal{Z}_K$. *Let*

$$\delta = \begin{cases} 1 & \text{if } K \text{ is a number field or } \overline{\mathbb{Q}} \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

Then there exists a point $\boldsymbol{x} \in V \setminus \mathcal{Z}_K$ *such that*

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq L^{\delta} e^{(1-\delta)gL} A_K(L, M) C_K(L) \mathcal{H}(V), \tag{10}$$

where $C_K(L)$ *is as in (13),* $A_K(L, M)$ *is as in (14), and* $g = 0$ *or* 1 *is genus of* K *in the function field case.*

In case K is the field of rational functions of a curve of genus 0 or 1 over a finite field, the constant $A_K(L, M)C_K(L)$ in the upper bound of (10) can be slightly simplified: see Remark 2.1 in section 2 below. It should also be remarked that in the function field case all the ingredients of our method (Lemma 2.1, Theorem 4.2, and Lemma 6.2) except for one (Theorem 1.2) work over *any* function field or its algebraic closure. Hence we state and prove our results in their most general form whenever possible, although we end up applying them in only a special case.

An immediate corollary of Theorem 1.4 is the following extension of Theorem 1.3.

Corollary 1.5. *Let* K *be an admissible field. Let* $N \geq 2$ *be an integer, and let* V *be an* L*-dimensional subspace of* K^N, $1 \leq L \leq N$. *Suppose that* $M \geq 1$ *is an integer and let* $U_1, ..., U_M$ *be subspaces of* K^N *such that* $V \not\subseteq \bigcup_{i=1}^{M} U_i$. *Then there exists a point* $\boldsymbol{x} \in V \setminus \bigcup_{i=1}^{M} U_i$ *satisfying (10) above. In particular, in case* K *is a number field,*

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq \sqrt{2} L |\mathcal{D}_K|^{\frac{L+1}{2d}} M^{\frac{1}{d}} \mathcal{H}(V). \tag{11}$$

Proof. Since $V \not\subseteq \bigcup_{i=1}^{M} U_i$, there exist subspaces $\overline{U}_1, \dots, \overline{U}_M$ of K^N of dimension $N-1$ such that $U_i \subseteq \overline{U}_i$ for each $1 \leq i \leq M$, and $V \not\subseteq \bigcup_{i=1}^{M} \overline{U}_i$. Let

$$\mathcal{L}_1(X_1, \dots, X_N), \dots, \mathcal{L}_M(X_1, \dots, X_N) \in K[X_1, \dots, X_N]$$

be linear forms such that $\overline{U}_i = \{\boldsymbol{x} \in K^N : \mathcal{L}(\boldsymbol{x}) = 0\}$ for each $1 \leq i \leq M$, and define

$$P(X_1, \dots, X_N) = \prod_{i=1}^{M} \mathcal{L}_i(X_1, \dots, X_N) \in K[X_1, \dots, X_N].$$

Then P is a polynomial of degree M, and $Z_K(P) = \bigcup_{i=1}^{M} \overline{U}_i$. Now the statement of the corollary follows from Theorem 1.4. □

Notice that although the bound of Corollary 1.5 does not uniformly overrule Theorem 1.3 (in particular, there is no dependence on the heights of U_i and the dependence on M is not as good as in Theorem 1.3), it exhibits the optimal exponent on $\mathcal{H}(V)$, better dependence on $N, L, d, \mathcal{D}_K$, is easier to use (compare (5) with (11)), and extends to $\overline{\mathbb{Q}}$ and over function fields, which is a serious advantage.

Our argument builds on the method of [6] and [7]. We use a variation of the Combinatorial Nullstellensatz of N. Alon [1] along with a counting mechanism. Loosely speaking, Combinatorial Nullstellensatz is the general principle that a polynomial of degree M in N variables cannot uniformly vanish on certain sets of points in K^N, which are built as rectangular grids of cardinality $\gg M^N$. A similar principle has been used in [6] and [7]. The main novelty in our approach is that we restrict this principle to points in a fixed vector space, and then reduce the main counting argument in the number field case to points of O_K viewed as a full-rank lattice in $\mathbb{R}^d$. In the function field case, we use a construction of FML lattices as in [21], pp. 578–583, combined with a lemma from [6] to produce a counting mechanism; we also discuss a possible alternative construction in Remark 7.2. This, along with an application of Siegel's lemma with inhomogeneous heights (Theorems 1.1 and 1.2), allows to produce a sharper estimate. The fact that Combinatorial Nullstellensatz applies over any field (or any sufficiently large subset of a field, for that matter) allows us to extend our results over $\overline{K}$. The dependence on M in the number field case of Theorem 1.4 is optimal in the sense that if $M^{1/d}$ is replaced by a smaller power of M then the corresponding rectangular grid in Combinatorial Nullstellensatz is not sufficiently large, so that the polynomial in question may vanish identically on it (see Remark 7.1 below for an actual example).

As a side product of the counting part of our method, we are also able to produce a uniform lower bound on the number of algebraic integers of bounded height in a number field K. The subject of counting algebraic numbers of bounded height has been started by the famous asymptotic formula of Schanuel [15]. Some explicit upper and lower bounds have also been produced later, for instance by Schmidt [16], [17]. Recently a new sharp upper bound has been given by Loher and Masser [12]. Here we can produce the following estimate for the number of algebraic integers.

Corollary 1.6. *Let K be a number field of degree d over $\mathbb{Q}$ with discriminant $\mathcal{D}_K$ and r_1 real embeddings. Let O_K be its ring of integers. For all $R \geq \left(2^{r_1}|D_K|\right)^{1/2}$,*

$$(2^{r_1}|\mathcal{D}_K|)^{-1/2}\, R^d < \left|\{x \in O_K \ : \ h(x) \leq R\}\right|. \tag{12}$$

The paper is structured as follows: in section 2 we set notation, define heights, and recall Lemma 2.1, which is a useful property of heights for our purposes; in section 3 we prove a function field version of Siegel's lemma with inhomogeneous heights; in section 4 we prove Theorem 4.2, a version of Combinatorial Nullstellensatz on a vector space required for our argument; in section 5 we prove Lemma 5.2, which is our main counting lemma in the number field case, and derive Corollary 1.6 from it; in section 6 we prove Lemma 6.2, the counting lemma over a function field; in section 7 we prove Theorem 1.4; in section 8 we discuss how our results can be extended to inequalities involving twisted height.

2. Notation and heights

We start with some notation. Throughout this paper, K will either be a number field (finite extension of $\mathbb{Q}$), a function field, or algebraic closure of one or the other; in fact, for the rest of this section, unless explicitly specified otherwise, we will assume that K is either a number field or a function field, and will write $\overline{K}$ for its algebraic closure. By a function field we will always mean a finite algebraic extension of the field $\mathfrak{K} = \mathfrak{K}_0(t)$ of rational functions in one variable over a field $\mathfrak{K}_0$, where $\mathfrak{K}_0$ can be any field. When K is a number field, clearly $K \subset \overline{K} = \overline{\mathbb{Q}}$; when K is a function field, $K \subset \overline{K} = \overline{\mathfrak{K}}$, the algebraic closure of $\mathfrak{K}$. In the number field case, we write $d = [K : \mathbb{Q}]$ for the global degree of K over $\mathbb{Q}$; in the function field case, the global degree is $d = [K : \mathfrak{K}]$, and we also define the effective degree of K over $\mathfrak{K}$ to be

$$\mathfrak{m}(K, \mathfrak{K}) = \frac{[K : \mathfrak{K}]}{[K_0 : \mathfrak{K}_0]},$$

where K_0 is the algebraic closure of $\mathfrak{K}_0$ in K. If K is a number field, we let $\mathcal{D}_K$ be its discriminant, ω_K the number of roots of unity in K, r_1 its number of real embeddings, and r_2 its number of conjugate pairs of complex embeddings, so $d = r_1 + 2r_2$. If K is a function field, we will also write $g(K)$ for the genus of K, as defined by the Riemann-Roch theorem (see [20] for details). We will distinguish two cases: if K is a function field, we say that it is of *finite type* q if its subfield of constants is a finite field $\mathbb{F}_q$ for some prime power q, and we say that it is of *infinite type* if its subfield of constants is infinite. If K is a function field of finite type q, then there exists a unique smooth projective curve Y over $\mathbb{F}_q$ such that $K = \mathbb{F}_q(Y)$ is the field of rational functions on Y. In this case, we will write $n(K) = |Y(\mathbb{F}_q)|$ for the number of points of Y over $\mathbb{F}_q$, and h_K for the number of divisor classes of degree zero (which is precisely the cardinality of the Jacobian of Y over $\mathbb{F}_q$). We can now define the field constant $C_K(L)$, which appears in Theorems 1.1 and 1.4:

$$(13) \quad C_K(L) = \begin{cases} \left(\left(\frac{2}{\pi}\right)^{r_2} |\mathcal{D}_K| \right)^{\frac{L}{2d}} & \text{if } K \text{ is a number field} \\ \exp\left(\frac{g(K) - 1 + \mathfrak{m}(K,\mathfrak{K})}{\mathfrak{m}(K,\mathfrak{K})} \right) & \text{if } K \text{ is a function field} \\ e^{\frac{L(L-1)}{4}} + \varepsilon & \text{if } K = \overline{\mathbb{Q}}\text{; here we can take any } \varepsilon > 0 \\ 1 + \varepsilon & \text{if } K = \overline{\mathfrak{K}}\text{; here we can take any } \varepsilon > 0, \end{cases}$$

and the constant $A_K(L, M)$, which appears in the statement of Theorem 1.4:
(14)

$$A_K(L, M) = \begin{cases} \left(M \sqrt{2^{r_1} |\mathcal{D}_K|} \right)^{\frac{1}{d}} & \text{if } K \text{ is a number field with } \omega_K \leq M \\ e^{R_K(M)} & \text{if } K \text{ is a function field of finite type } q \leq M \\ 1 & \text{otherwise,} \end{cases}$$

for all integers $L, M \geq 1$, where for a function field K of finite type $q \leq M$ we define

$$(15) \quad R_K(M) = \frac{n(K) - 1}{2} \left((M - q + 2) h_K \sqrt{n(K)} \right)^{\frac{1}{n(K)-1}} + h_K (n(K) - 1) \sqrt{n(K)}.$$

Remark 2.1. Let Y be a smooth projective curve of genus g over $\mathbb{F}_q$. Then Hasse-Weil-Serre bound (see for instance Theorem 2.3.16 on p. 178 of [21]) gives

$$(16) \qquad n(K) \leq q + 1 + g\,[2\sqrt{q}]\,,$$

where [ ] stands for the integer part function. In case $g = 0$ we also have $h_K = 1$, and if $g = 1$ we have $h_K \leq n(K) \leq q + 1 + \left[2\sqrt{q}\right]$ (see (37) below, which gives a bound on h_K in terms of $n(K)$ and the genus). These observations may help to simplify the formula (15) for $R_K(M)$.

Next we discuss absolute values on K. Let $M(K)$ be the set of places of K. For each place $v \in M(K)$ we write K_v for the completion of K at v and let d_v be the local degree of K at v, which is $[K_v : \mathbb{Q}_v]$ in the number field case, and $[K_v : \mathfrak{K}_v]$

in the function field case. In any case, for each place u of the ground field, be it $\mathbb{Q}$ or $\mathfrak{K}$, we have

$$\sum_{v \in M(K), v | u} d_v = d. \tag{17}$$

If K is a number field, then for each place $v \in M(K)$ we define the absolute value $|\ |_v$ to be the unique absolute value on K_v that extends either the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$ if $v|\infty$, or the usual p-adic absolute value on $\mathbb{Q}_p$ if $v|p$, where p is a prime. For each finite place $v \in M(K)$, $v \nmid \infty$, we define the *local ring of v-adic integers* $\mathfrak{O}_v = \{x \in K : |x|_v \leq 1\}$, whose unique maximal ideal is $\mathfrak{M}_v = \{x \in K : |x|_v < 1\}$. Then $O_K = \bigcap_{v \nmid \infty} \mathfrak{O}_v$.

If K is a function field, then all absolute values on K are non-archimedean. For each $v \in M(K)$, let $\mathfrak{O}_v$ be the valuation ring of v in K_v and $\mathfrak{M}_v$ the unique maximal ideal in $\mathfrak{O}_v$. We choose the unique corresponding absolute value $|\ |_v$ such that:

(i) if $1/t \in \mathfrak{M}_v$, then $|t|_v = e$,
(ii) if an irreducible polynomial $p(t) \in \mathfrak{M}_v$, then $|p(t)|_v = e^{-\deg(p)}$.

In both cases, for each non-zero $a \in K$ the *product formula* reads

$$\prod_{v \in M(K)} |a|_v^{d_v} = 1. \tag{18}$$

We extend absolute values to vectors by defining the local heights. For each $v \in M(K)$ define a local height H_v on K_v^N by

$$H_v(\boldsymbol{x}) = \max_{1 \leq i \leq N} |x_i|_v^{d_v},$$

for each $\boldsymbol{x} \in K_v^N$. Also, for each $v|\infty$ we define another local height

$$\mathcal{H}_v(\boldsymbol{x}) = \left(\sum_{i=1}^N |x_i|_v^2 \right)^{d_v/2}.$$

Then we can define two slightly different global height functions on K^N:

$$H(\boldsymbol{x}) = \left(\prod_{v \in M(K)} H_v(\boldsymbol{x}) \right)^{1/d}, \quad \mathcal{H}(\boldsymbol{x}) = \left(\prod_{v \nmid \infty} H_v(\boldsymbol{x}) \times \prod_{v | \infty} \mathcal{H}_v(\boldsymbol{x}) \right)^{1/d}, \tag{19}$$

for each $\boldsymbol{x} \in K^N$. These height functions are *homogeneous*, in the sense that they are defined on projective space thanks to the product formula (18): $H(a\boldsymbol{x}) = H(\boldsymbol{x})$ and $\mathcal{H}(a\boldsymbol{x}) = \mathcal{H}(\boldsymbol{x})$ for any $\boldsymbol{x} \in K^N$ and $0 \neq a \in K$. It is easy to see that

$$H(\boldsymbol{x}) \leq \mathcal{H}(\boldsymbol{x}) \leq \sqrt{N} H(\boldsymbol{x}).$$

Notice that in case K is a function field, $M(K)$ contains no archimedean places, and so $H(\boldsymbol{x}) = \mathcal{H}(\boldsymbol{x})$ for all $\boldsymbol{x} \in K^N$. We also define the *inhomogeneous* height

$$h(\boldsymbol{x}) = H(1, \boldsymbol{x}),$$

which generalizes Weil height on algebraic numbers: for each $\alpha \in K$, define

$$h(\alpha) = \prod_{v \in M(K)} \max\{1, |\alpha|_v\}^{d_v/d}.$$

Clearly, $h(\boldsymbol{x}) \geq H(\boldsymbol{x})$ for each $\boldsymbol{x} \in K^N$. All our inequalities will use heights H and h for vectors, however we use $\mathcal{H}$ to define the conventional Schmidt height on subspaces in the manner described below. This choice of heights coincides with [2] and [7].

We extend both heights H and $\mathcal{H}$ to polynomials by viewing them as height functions of the coefficient vector of a given polynomial. We also define a height function on subspaces of K^N. Let $V \subseteq K^N$ be a subspace of dimension L, $1 \leq L \leq N$. Choose a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ for V, and write $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_L)$ for the corresponding $N \times L$ basis matrix. Then

$$V = \{X\boldsymbol{t} : \boldsymbol{t} \in K^L\}.$$

On the other hand, there exists an $(N-L) \times N$ matrix A with entries in K such that

$$V = \{\boldsymbol{x} \in K^N : A\boldsymbol{x} = 0\}.$$

Let $\mathcal{I}$ be the collection of all subsets I of $\{1, ..., N\}$ of cardinality L. For each $I \in \mathcal{I}$ let I' be its complement, i.e. $I' = \{1, ..., N\} \setminus I$, and let $\mathcal{I}' = \{I' : I \in \mathcal{I}\}$. Then

$$|\mathcal{I}| = \binom{N}{L} = \binom{N}{N-L} = |\mathcal{I}'|.$$

For each $I \in \mathcal{I}$, write X_I for the $L \times L$ submatrix of X consisting of all those rows of X which are indexed by I, and ${}_{I'}A$ for the $(N-L) \times (N-L)$ submatrix of A consisting of all those columns of A which are indexed by I'. By the duality principle of Brill-Gordan [8] (also see Theorem 1 on p. 294 of [9]), there exists a non-zero constant $\gamma \in K$ such that

$$\det(X_I) = (-1)^{\varepsilon(I')} \gamma \det({}_{I'}A), \tag{20}$$

where $\varepsilon(I') = \sum_{i \in I'} i$. Define the vectors of *Grassmann coordinates* of X and A respectively to be

$$Gr(X) = (\det(X_I))_{I \in \mathcal{I}} \in K^{|I|}, \quad Gr(A) = (\det({}_{I'}A))_{I' \in \mathcal{I}'} \in K^{|I'|},$$

and so by (20) and (18)

$$\mathcal{H}(Gr(X)) = \mathcal{H}(Gr(A)).$$

Define the height of V denoted by $\mathcal{H}(V)$ to be this common value. This definition is legitimate, since it does not depend on the choice of the basis for V. In particular, notice that if

$$\mathcal{L}(X_1, ..., X_N) = \sum_{i=1}^N q_i X_i \in K[X_1, ..., X_N]$$

is a linear form with a non-zero coefficient vector $\boldsymbol{q} \in K^N$, and $V = \{\boldsymbol{x} \in K^N : \mathcal{L}(\boldsymbol{x}) = 0\}$ is an $(N-1)$-dimensional subspace of K^N, then

$$\mathcal{H}(V) = \mathcal{H}(\mathcal{L}) = \mathcal{H}(\boldsymbol{q}). \tag{21}$$

An important observation is that due to the normalizing exponent $1/d$ in (19) all our heights are *absolute*, meaning that they do not depend on the number field or function field of definition, hence are well defined over $\overline{K}$.

We will also need the following basic property of heights.

Lemma 2.1. *For $\xi_1, ..., \xi_L \in \overline{K}$ and $\boldsymbol{x}_1, ..., \boldsymbol{x}_L \in \overline{K}^N$,*

$$H\left(\sum_{i=1}^L \xi_i \boldsymbol{x}_i\right) \leq h\left(\sum_{i=1}^L \xi_i \boldsymbol{x}_i\right) \leq L^\delta H(\boldsymbol{\xi}) \prod_{i=1}^L h(\boldsymbol{x}_i),$$

where $\boldsymbol{\xi} = (\xi_1, ..., \xi_L) \in \overline{K}^L$, and δ is as in (9) above.

We are now ready to proceed.

3. Siegel's lemma over a function field

In this section we produce a version of Siegel's lemma with inhomogeneous heights over fields of rational functions of rational and elliptic curves, which is a function field analogue of (2). Let all notation be as in section 2 above. We now prove Theorem 1.2.

Proof of Theorem 1.2. In fact, the first part of our argument works for curves of any genus, so let us first assume that Y is a smooth projective curve over a perfect field $\mathfrak{K}_0$ and $K = \mathfrak{K}_0(Y)$. Then $g(K)$ is precisely the genus of Y. Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L$ be a basis for V over K satisfying (1) of Theorem 1.1. For each $1 \leq i \leq L$ and $v \in M(K)$,

$$H_v^{1/d_v}(\boldsymbol{x}_i) = \max_{1 \leq j \leq N} |x_{ij}|_v = \max_{1 \leq j \leq N} e^{-\operatorname{ord}_v(x_{ij})} = \exp\left(- \min_{1 \leq j \leq N} \operatorname{ord}_v(x_{ij}) \right),$$

where $\operatorname{ord}_v(x_{ij})$ is order of x_{ij} at the place v; clearly, for each $1 \leq i \leq L$, $1 \leq j \leq N$, $\operatorname{ord}_v(x_{ij}) \neq 0$ at only finitely many places $v \in M(K)$.

Fix $1 \leq i \leq L$, and let $v_1, \dots, v_s$ be the places of K at which $\operatorname{ord}_v(x_{ij}) \neq 0$ for some $1 \leq j \leq N$. As in section 2, for each $1 \leq m \leq s$

$$\mathfrak{O}_{v_m} = \{x \in K : \operatorname{ord}_{v_m}(x) \leq 0\}$$

is the valuation ring at v_m with the unique maximal ideal

$$\mathfrak{M}_{v_m} = \{x \in K : \operatorname{ord}_{v_m}(x) < 0\},$$

and let us write $\mathfrak{K}_0(v_m)$ for the residue field $\mathfrak{O}_{v_m}/\mathfrak{M}_{v_m}$. Clearly $\mathfrak{K}_0^* \subseteq \mathfrak{O}_{v_m} \setminus \mathfrak{M}_{v_m}$, so $\mathfrak{K}_0(v_m)$ is a field extension of $\mathfrak{K}_0$. By Exercise 2.3.1 on p. 171 of [21], $\delta_m := [\mathfrak{K}_0(v_m) : \mathfrak{K}_0]$ is finite. Following the construction on p.171 of [21], we say that each v_m determines a point $P(v_m)$ of Y of degree δ_m (we will also denote this degree by $\deg_{\mathfrak{K}_0}(v_m)$), and write $\overline{Y}$ for the closure of the curve Y over $\overline{\mathfrak{K}_0}$. Then the Galois orbit of $P(v_m)$ over $\mathfrak{K}_0(v_m)$ consists of δ_m points $P_1(v_m), \dots, P_{\delta_m}(v_m)$ on $\overline{Y}$, i.e.

$$\left\{ \sigma(P(v_m)) : \sigma \in \operatorname{Gal}(\overline{\mathfrak{K}_0}/\mathfrak{K}_0) \right\} = \{P_1(v_m), \dots, P_{\delta_m}(v_m)\}.$$

We will say that the points $P_1(v_m), \dots, P_{\delta_m}(v_m)$ lie over v_m. Since $\mathfrak{K}_0$ is perfect, $\overline{\mathfrak{K}_0}$ is separable over $\mathfrak{K}_0$, and so $P_k(v_{m_1}) = P_l(v_{m_2})$ if and only if $m_1 = m_2$ and $k = l$. Define the divisor of $\boldsymbol{x}_i$ over $\overline{\mathfrak{K}_0}$ by the formal sum

$$\operatorname{div}(\boldsymbol{x}_i) = \sum_{m=1}^{s} \left(- \min_{1 \leq j \leq N} \operatorname{ord}_{v_m}(x_{ij}) \right) (P_1(v_m) + \dots + P_{\delta_m}(v_m)),$$

then as usual

$$\deg(\operatorname{div}(\boldsymbol{x}_i)) = - \sum_{m=1}^{s} \delta_m \min_{1 \leq j \leq N} \operatorname{ord}_{v_m}(x_{ij}).$$

In the same manner, each element $f \in \mathfrak{K}_0(Y)$ defines a principal divisor

$$(f) = \sum_{v \in M(\mathfrak{K}_0(Y))} (\operatorname{ord}_v(f)) \, (P_1(v) + \dots + P_{\deg_{\mathfrak{K}_0}(v)}(v)),$$

so that $\deg(f) = \sum_{v \in M(\mathfrak{K}_0(Y))} \deg_{\mathfrak{K}_0}(v) \operatorname{ord}_v(f) = 0$. In particular notice that

$$0 = -\sum_{m=1}^{s} \delta_m \operatorname{ord}_{v_m}(x_{i1}) \leq -\sum_{m=1}^{s} \delta_m \min_{1 \leq j \leq N} \operatorname{ord}_{v_m}(x_{ij}) = \deg(\operatorname{div}(\boldsymbol{x}_i)). \tag{22}$$

Let us first assume that $\deg(\operatorname{div}(\boldsymbol{x}_i)) > g(K) - 1$. An immediate implication of the Riemann-Roch theorem (see for instance Theorem 2.2.17 on p. 150 of [21]) is that there exists $f_i \in \overline{\mathfrak{K}_0}(Y)$ such that the divisor $\operatorname{div}(\boldsymbol{x}_i) + (f_i)$ is effective. Then, by Exercise 2.3.6 on p. 174 of [21], there in fact exists such $f_i \in K$, so

$$\deg(v) \left(-\min_{1 \leq j \leq N} \operatorname{ord}_v(x_{ij}) + \operatorname{ord}_v(f_i) \right) \geq 0$$

for all $v \in M(K)$. Since $\deg(v) \geq 1$, this means that $-\min_{1 \leq j \leq N} \operatorname{ord}_v(x_{ij}) + \operatorname{ord}_v(f_i) \geq 0$ for all $v \in M(K)$. Then define $\boldsymbol{u}_i = \frac{1}{f_i} \boldsymbol{x}_i$, and notice that

$$H_v^{1/d_v}(\boldsymbol{u}_i) = \exp \left(-\min_{1 \leq j \leq N} \operatorname{ord}_v(x_{ij}) + \operatorname{ord}_v(f_i) \right) \geq 1,$$

for all $v \in M(K)$. Therefore

$$h(\boldsymbol{u}_i) = H(\boldsymbol{u}_i) = \left(\prod_{v \in M(K)} \left| \frac{1}{f_i} \right|_v^{d_v} H_v(\boldsymbol{x}_i) \right)^{1/d} = H(\boldsymbol{x}_i), \tag{23}$$

by the product formula. If Y is a rational curve, then $g(K) - 1 = -1$, and so by (22) the condition $\deg(\operatorname{div}(\boldsymbol{x}_i)) > g(K) - 1$ always holds. Then (3) follows by combining (23) with (1).

Next assume that $0 \leq \deg(\operatorname{div}(\boldsymbol{x}_i)) \leq g(K) - 1$. Here we need to assume that Y is an elliptic curve, so $g(K) = 1$ and $\deg(\operatorname{div}(\boldsymbol{x}_i)) = 0$. Since $\operatorname{div}(\boldsymbol{x}_i)$ is defined over $\mathfrak{K}_0$, then by Proposition 2.4.1 on p. 192 of [21] (also see Proposition 3.4 on p. 66 of [18]), there exist points Q, T on $\overline{Y}$ and a rational function f_i in some algebraic extension of K such that

$$\operatorname{div}(\boldsymbol{x}_i) = (f_i) + Q - T. \tag{24}$$

Once again, Exercise 2.3.6 on p. 174 of [21] implies that in fact there exists such f_i in K. Then Q and T must lie over some places of K, in fact since the coefficients in front of Q and T in (24) are different (1 and -1 respectively), they must lie over different places of K, call them v_1 and v_2 respectively. Let $\boldsymbol{u}_i = \frac{1}{f_i} \boldsymbol{x}_i$, then

$$H_{v_1}^{1/d_{v_1}}(\boldsymbol{u}_i) = e, \ H_{v_2}^{1/d_{v_2}}(\boldsymbol{u}_i) = \frac{1}{e}, \ H_v^{1/d_v}(\boldsymbol{u}_i) = 1 \ \forall \ v \neq v_1, v_2.$$

Therefore

$$h(\boldsymbol{u}_i) \leq e H(\boldsymbol{x}_i), \tag{25}$$

since $H(\boldsymbol{u}_i) = H(\boldsymbol{x}_i) = 1$. Then combining (23) and (25) with (1), we see that there exists a basis $\boldsymbol{u}_1, ..., \boldsymbol{u}_L$ for V over K such that

$$\prod_{i=1}^{L} H(\boldsymbol{u}_i) \leq \prod_{i=1}^{L} h(\boldsymbol{u}_i) \leq e^L \prod_{i=1}^{L} H(\boldsymbol{x}_i) \leq e^L C_K(L) \mathcal{H}(V).$$

This completes the proof. □

Remark 3.1. Notice that the first part of the proof of Theorem 1.2 works for curves of any genus; in other words, as long as $\deg(\operatorname{div}(\boldsymbol{x}_i)) > g(K) - 1$ Riemann-Roch implies that $\operatorname{div}(\boldsymbol{x}_i)$ is linearly equivalent to an effective divisor, and one easily constructs a vector over K with inhomogeneous height equal to $H(\boldsymbol{x}_i)$. In case $\deg(\operatorname{div}(\boldsymbol{x}_i)) \leq g(K) - 1$ we need to be able to bound the coefficients of the divisor $\operatorname{div}(\boldsymbol{x}_i)$, and the principle that allows us to do it for curves of genus 1 (Proposition 3.4 on p. 66 of [18]) is precisely the reason for the existence of group structure on elliptic curves. This consideration suggests that it is unlikely that one could extend Theorem 1.2 to curves of higher genus.

4. Combinatorial Nullstellensatz

In [1] the following lemma is proved (compare with Lemma 2.1 of [6], which is an immediate corollary of Lemma 1 on p. 261 of [3]).

Lemma 4.1 ([1])**.** *Let $P(X_1, \dots, X_N)$ be a polynomial in N variables with coefficients in an arbitrary field $\mathbb{F}$. Suppose that $\deg_{X_i} P \leq t_i$ for $1 \leq i \leq N$, and let $S_i \subset \mathbb{F}$ be a set of at least $t_i + 1$ distinct elements of $\mathbb{F}$. If $P(\boldsymbol{\xi}) = 0$ for all N-tuples*

$$\boldsymbol{\xi} = (\xi_1, \dots, \xi_N) \in S_1 \times \dots \times S_N,$$

then $P \equiv 0$.

We will refer to this lemma as Combinatorial Nullstellensatz (Alon uses this name for a slightly different related result, which is derived from this lemma). We use this lemma to derive a somewhat more specialized version of such a result with restriction to a vector space.

Theorem 4.2. *Let $P(X_1, \dots, X_N)$ be a polynomial in N variables with coefficients in an arbitrary field $\mathbb{F}$. Suppose that $\deg_{X_i} P \leq t_i$ for $1 \leq i \leq N$, and let $S_i \subset \mathbb{F}$ be a set of at least $t_i + 1$ distinct elements of $\mathbb{F}$. Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_L$ be vectors in $\mathbb{F}^N$, $1 \leq L \leq N$, and let $V = \operatorname{span}_{\mathbb{F}}\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_L\}$ be a subspace of $\mathbb{F}^N$. Write $S = S_1 \times \dots \times S_L$, and for each L-tuple $\boldsymbol{\xi} = (\xi_1, \dots, \xi_L) \in S$, let $\boldsymbol{v}(\boldsymbol{\xi}) = \sum_{i=1}^{L} \xi_i \boldsymbol{v}_i$. If $P(\boldsymbol{v}(\boldsymbol{\xi})) = 0$ for all $\boldsymbol{\xi} \in S$, then P is identically 0 on V.*

Proof. Assume that P is not identically zero on V, so there exists $\boldsymbol{x} \in V$ such that $P(\boldsymbol{x}) \neq 0$. We will show that there must exist $\boldsymbol{\xi} \in S$ such that $P(\boldsymbol{v}(\boldsymbol{\xi})) \neq 0$. Let

$$A = (\boldsymbol{v}_1 \dots \boldsymbol{v}_L \ \boldsymbol{0} \dots \boldsymbol{0})$$

be the $N \times N$ matrix the first L columns of which are the vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_L$, and the remaining $N - L$ columns are zero vectors. Write $\boldsymbol{X} = (X_1, \dots, X_N)$ for the variable vector, and define the restriction of P to V with respect to the spanning set $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_L\}$ by

$$P_V(X_1, \dots, X_L) = P(A\boldsymbol{X}^t).$$

Notice that if $\boldsymbol{v}(\boldsymbol{\xi}) = \sum_{i=1}^{L} \xi_i \boldsymbol{v}_i$ for some $\boldsymbol{\xi} = (\xi_1, \dots, \xi_L) \in \mathbb{F}^L$, then $P(\boldsymbol{v}(\boldsymbol{\xi})) = P_V(\boldsymbol{\xi})$. Since P is not identically zero on V, there must exist $\boldsymbol{\xi} \in \mathbb{F}^L$ such that $P_V(\boldsymbol{\xi}) \neq 0$. Moreover, for each $1 \leq i \leq L$, $\deg_{X_i} P_V \leq \deg_{X_i} P \leq t_i$. Therefore by Lemma 4.1, there exists $\boldsymbol{\xi} \in S$ such that

$$P_V(\boldsymbol{\xi}) = P(\boldsymbol{v}(\boldsymbol{\xi})) \neq 0.$$

This completes the proof. □

5. A counting mechanism: number field case

Here we produce a certain refinement of Theorem 0 on p. 102 of [11] with explicit constants (also compare with Lemma 4.1 of [7]), which will serve as our main counting mechanism in the number field case. We start by recalling Lemma 2.1 of [7].

Lemma 5.1 ([7]). *For a real number $R \geq 1$, let*

$$C_R^n = \{\boldsymbol{x} \in \mathbb{R}^n : \max_{1 \leq i \leq n} |x_i| \leq R\} \tag{26}$$

be a cube in $\mathbb{R}^n$, $n \geq 1$, centered at the origin with sidelength $2R$. Let Λ be a lattice of full rank in $\mathbb{R}^n$ of determinant Δ such that there exists a positive constant c and an uppertriangular basis matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ of Λ with diagonal entries $a_{ii} \geq c$ for all $1 \leq i \leq n$. Assume that $2R \geq \max\left\{\frac{\Delta}{c^{n-1}}, c\right\}$. Then for each point $\boldsymbol{z}$ in $\mathbb{R}^n$ we have

$$\begin{aligned} \left(\frac{2Rc^{n-1}}{\Delta} - 1\right)\left(\frac{2R}{c} - 1\right)^{n-1} &\leq |\Lambda \cap (C_R^n + \boldsymbol{z})| \\ &\leq \left(\frac{2Rc^{n-1}}{\Delta} + 1\right)\left(\frac{2R}{c} + 1\right)^{n-1}. \end{aligned} \tag{27}$$

For our number field K, define the set

$$S_R(K) = \{x \in O_K \ : \ |x|_v \leq R \ \forall \ v|\infty\}, \tag{28}$$

where $R \geq 1$ is a real number (compare with the set $S_M(K)$ in the proof of Lemma 4.1 in [7]). We use Lemma 5.1 to prove the following estimate, which will be essential in the proof of Theorem 1.4.

Lemma 5.2. *For all $R \geq (2^{r_1}|D_K|)^{1/2}$,*

$$(2^{r_1}|\mathcal{D}_K|)^{-1/2} R^d < |S_R(K)| < 2^{2d+1/2} (2^{r_1}|\mathcal{D}_K|)^{-1/2} R^d. \tag{29}$$

Proof. As in [7], let

$$\sigma_1, ..., \sigma_{r_1}, \tau_1, ..., \tau_{r_2}, \tau_{r_2+1}, ..., \tau_{2r_2}$$

be the embeddings of K into $\mathbb{C}$ with $\sigma_1, ..., \sigma_{r_1}$ being real embeddings and $\tau_j, \tau_{r_2+j} = \bar{\tau}_j$ for each $1 \leq j \leq r_2$ being the pairs of complex conjugate embeddings. For each $x \in K$ and each complex embedding τ_j, write $\tau_{j1}(x) = \Re(\tau_j(x))$ and $\tau_{j2}(x) = \Im(\tau_j(x))$, where $\Re$ and $\Im$ stand respectively for real and imaginary parts of a complex number. We will view $\tau_j(x)$ as a pair $(\tau_{j1}(x), \tau_{j2}(x)) \in \mathbb{R}^2$. Then $d = r_1 + 2r_2$, and we define an embedding

$$\sigma = (\sigma_1, ..., \sigma_{r_1}, \tau_1, ..., \tau_{r_2}) : K \longrightarrow K_\infty,$$

where

$$K_\infty = \prod_{v|\infty} K_v = \prod_{v|\infty} \mathbb{R}^{d_v} = \mathbb{R}^d,$$

since $\sum_{v|\infty} d_v = d$. Then $\Lambda := \sigma(O_K)$ is a lattice of full rank in $\mathbb{R}^d$. Let us write $M_\infty(K)$ for the set of archimedean places of K, then

$$M_\infty(K) = \{v_1, \dots, v_{r_1}, w_1, \dots, w_{r_2}\},$$

where for each $x \in K$, $1 \leq i \leq r_1$, $1 \leq j \leq r_2$,

$$|x|_{v_i} = |\sigma_i(x)|_\infty, \ |x|_{w_j} = |\tau_j(x)|_\infty,$$

where $|\ |_\infty$ stands for the usual absolute value on $\mathbb{C}$. Therefore for each $x \in O_K$,

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \tau_{11}(x), \tau_{12}(x), \dots, \tau_{r_2 1}(x), \tau_{r_2 2}(x)) \in \Lambda,$$

and if $x \in S_R(K)$, then for each $1 \leq i \leq r_1$, $|\sigma_i(x)|_\infty \leq R$, and for each $1 \leq j \leq r_2$, $\sqrt{\tau_{j1}(x)^2 + \tau_{j2}(x)^2} \leq R$, thus

$$\Lambda \cap C^d_{R/\sqrt{2}} \subseteq \sigma(S_R(K)) \subseteq \Lambda \cap C^d_R, \tag{30}$$

and since σ is injective,

$$|\Lambda \cap C^d_{R/\sqrt{2}}| \leq |S_R(K)| \leq |\Lambda \cap C^d_R|. \tag{31}$$

Now if $x \in O_K$, then $|x|_v \leq 1$ for all $v \nmid \infty$, and so $|x|_v \geq 1$ for at least one $v | \infty$, call this place v_*. If v_* is real, say $v_* = v_i$ for some $1 \leq i \leq r_1$, then $|\sigma_j(x)|_\infty \geq 1$. If v_* is complex, say $v_* = w_j$ for some $1 \leq j \leq r_2$, then $\sqrt{\tau_{j1}(x)^2 + \tau_{j2}(x)^2} \geq 1$, hence $\max\{|\tau_{j1}(x)|_\infty, |\tau_{j2}(x)|_\infty\} \geq \frac{1}{\sqrt{2}}$. Therefore,

$$\max\{|\sigma_1(x)|, ..., |\sigma_{r_1}(x)|, |\tau_{11}(x)|, |\tau_{12}(x)|, ..., |\tau_{r_2 1}(x)|, |\tau_{r_2 2}(x)|\} \geq \frac{1}{\sqrt{2}}, \tag{32}$$

in other words the maximum of the Euclidean absolute values of all conjugates of an algebraic integer is at least $\frac{1}{\sqrt{2}}$.

Finally, recall that

$$\Delta := |\det(\Lambda)| = \frac{|\mathcal{D}_K|^{1/2}}{2^{r_2}}, \tag{33}$$

which follows immediately from Lemma 2 on p. 115 of [11]. We are now ready to apply Lemma 5.1. By Corollary 1 on p. 13 of [3], we can select a basis for Λ so that the basis matrix is upper triangular, all of its nonzero entries are positive, and the maximum entry of each row occurs on the diagonal. By (32) each of these maximum values is at least $\frac{1}{\sqrt{2}}$, so the lattice Λ satisfies the conditions of Lemma 5.1 with $c = \frac{1}{\sqrt{2}}$, $n = d$, and Δ as in (33). Therefore, if we take $R \geq \left(2^{r_1} |\mathcal{D}_K|\right)^{1/2}$, then by (31) combined with Lemma 5.1

$$\begin{aligned} |S_R(K)| \geq |\Lambda \cap C^d_{R/\sqrt{2}}| \ &\geq \ \left(\frac{R}{2^{\frac{r_1-2}{2}} |\mathcal{D}_K|^{1/2}} - 1 \right) (2R-1)^{d-1} \\ &> \ \left(2^{r_1} |\mathcal{D}_K|\right)^{-1/2} R^d, \end{aligned} \tag{34}$$

which proves the lower bound of (29). Also

$$\begin{aligned} |S_R(K)| \leq |\Lambda \cap C^d_R| \ &\leq \ \left(\frac{R}{2^{\frac{r_1-3}{2}} |\mathcal{D}_K|^{1/2}} + 1 \right) \left(2\sqrt{2}R + 1\right)^{d-1} \\ &< \ 2^{2d+1/2} \left(2^{r_1} |\mathcal{D}_K|\right)^{-1/2} R^d, \end{aligned} \tag{35}$$

which proves the upper bound of (29). □

We can now easily derive Corollary 1.6.

Proof of Corollary 1.6. Notice that $R \geq \left(2^{r_1} |D_K|\right)^{1/2} > 1$, so if $x \in S_R(K)$, then

$$h(x) = \prod_{v \in M(K)} \max\{1, |x|_v\}^{d_v/d} \leq \prod_{v \in M(K)} R^{d_v/d} = R,$$

hence $S_R(K) \subseteq \{x \in O_K \ : \ h(x) \leq R\}$. The statement of the corollary now follows from Lemma 5.2. □

6. A counting mechanism: function field case

Here we produce a counting estimate analogous to Lemma 5.2 over a function field with a finite field of constants. First we recall a lemma (Theorems 4.2 and 4.3 of [6]) which we will need here.

Lemma 6.1 ([6])**.** *Suppose that $\Lambda \subseteq \mathbb{Z}^n$ is a lattice of rank $n-l$, where $1 \leq l \leq n-1$. Let Δ be the maximum of absolute values of Grassmann coordinates of Λ. Then for every R that is a positive integer multiple of $(n-l)\Delta$, we have*

$$\frac{(2R)^{n-l}}{(n-l)^{n-l}\Delta} \leq |\Lambda \cap C_R^n| \leq \left(\frac{2R}{\Delta} + 1\right)(2R+1)^{n-l-1}, \tag{36}$$

where C_R^n is as in (26). The upper bound of (36) holds for R that is not an integer multiple of $(n-l)\Delta$ as well.

The following is a construction of function field lattices (FML) as on pages 578–583 of [21]. Let K be a function field over a finite field $\mathbb{F}_q$ for a prime power q, then there exists a curve Y over $\mathbb{F}_q$ such that $K = \mathbb{F}_q(Y)$ is the field of rational functions on Y. Let the set of points of Y over $\mathbb{F}_q$ be

$$Y(\mathbb{F}_q) = \{P_1, \dots, P_{n(K)}\},$$

where $n(K) = |Y(\mathbb{F}_q)|$, and let $\mathcal{M}_Y = \{v_1, \dots, v_{n(K)}\} \subset M(K)$ be a subset of places of K corresponding to these points. In other words, for every $f \in K$ and for each $1 \leq i \leq n(K)$, we have $|f|_{v_i} = e^{-\operatorname{ord}_{v_i}(f)}$, where

$$\operatorname{ord}_{v_i}(f) = \begin{cases} k & \text{if } f \text{ has a zero of multiplicity } k \text{ at } P_i \\ -k & \text{if } f \text{ has a pole of multiplicity } k \text{ at } P_i \\ 0 & \text{otherwise.} \end{cases}$$

Let

$$O_K(Y) = \{f \in K^* : \operatorname{ord}_v(f) = 0 \ \forall \ v \in M(K) \setminus \mathcal{M}_Y\}$$

be the ring of rational functions from K with zeros and poles only at the places in $\mathcal{M}_Y$. Then for each $f \in O_K(Y)$

$$\sum_{v \in \mathcal{M}_Y} \operatorname{ord}_v(f) = 0,$$

since f defines a principal divisor. Define

$$\mathcal{H}_{n(K)} = \left\{ \boldsymbol{x} \in \mathbb{R}^{n(K)} : \sum_{i=1}^{n(K)} x_i = 0 \right\},$$

so $\mathcal{H}_{n(K)}$ is an $(n(K)-1)$-dimensional subspace of $\mathbb{R}^{n(K)}$. We now have a natural embedding $\varphi_Y : O_K(Y) \to \mathbb{Z}^{n(K)} \cap \mathcal{H}_{n(K)}$ given by

$$\varphi_Y(f) = (\operatorname{ord}_{v_1}(f), \dots, \operatorname{ord}_{v_{n(K)}}(f)).$$

Then $\ker(\varphi_Y) = \mathbb{F}_q^*$; also, by Theorem 5.4.9 on p. 579 of [21], $\Lambda_Y := \varphi(O_K(Y))$ is a lattice of full rank in $\mathcal{H}_{n(K)}$, hence a sublattice of $\mathbb{Z}^{n(K)}$ of rank $n(K)-1$, and

$$\sqrt{n(K)} \leq \det \Lambda_Y \leq \sqrt{n(K)}\ h_K \leq \sqrt{n(K)} \left(\frac{(g(K)-1)(q+1)+n(K)}{g(K)} \right)^{g(K)}, \tag{37}$$

where h_K is the class number of K, and $g(K)$ is the genus of Y, and hence of K. If $g(K)=0$, the upper bound of (37) becomes simply $\sqrt{n(K)}$, thus enforcing equality throughout ($h(K)=1$ in this case). For a positive real number R define

$$S_R(K) = \{ f \in O_K(Y) \ : \ \operatorname{ord}_v(f) \leq R \ \forall \ v \in \mathcal{M}_Y \}, \tag{38}$$

then

$$|S_R(K)| = |\Lambda_Y \cap C_R^{n(K)}| + |\ker(\varphi_Y)| = |\Lambda_Y \cap C_R^{n(K)}| + q - 1, \tag{39}$$

and we have the following estimate.

Lemma 6.2. *For every real number $R \geq (n(K)-1)\sqrt{n(K)}\ h_K$,*

$$\begin{aligned} &\frac{2^{n(K)-1}}{\sqrt{n(K)}\ h_K} \left(\frac{R}{n(K)-1} - \sqrt{n(K)}\ h_K \right)^{n(K)-1} + q - 1 \\ &\leq |S_R(K)| \leq (2R+1)^{n(K)-1} + q - 1. \end{aligned} \tag{40}$$

Proof. By (39), we need to estimate $|\Lambda_Y \cap C_R^{n(K)}|$. Let Δ_Y be the maximum of absolute values of Grassmann coordinates of Λ_Y. By Cauchy-Binet formula

$$\Delta_Y \leq \det \Lambda_Y \leq \sqrt{n(K)}\Delta_Y. \tag{41}$$

Let $R_1 = \left[\frac{R}{(n(K)-1)\Delta_Y} \right] (n(K)-1)\Delta_Y$, where [ ] denotes the integer part function, then by combining Lemma 6.1 with (41), we have

$$\begin{aligned} |\Lambda_Y \cap C_R^{n(K)}| &\geq |\Lambda_Y \cap C_{R_1}^{n(K)}| \geq \frac{(2R_1)^{n(K)-1}}{(n(K)-1)^{n(K)-1}\Delta_Y} \\ &= 2^{n(K)-1}\Delta_Y^{n(K)-2} \left[\frac{R}{(n(K)-1)\Delta_Y} \right]^{n(K)-1} \\ &\geq \frac{2^{n(K)-1}}{\Delta_Y} \left(\frac{R}{n(K)-1} - \Delta_Y \right)^{n(K)-1} \\ &\geq \frac{2^{n(K)-1}}{\det \Lambda_Y} \left(\frac{R}{n(K)-1} - \det \Lambda_Y \right)^{n(K)-1}. \end{aligned} \tag{42}$$

The lower bound of (40) follows by combining (42) with (37) and (39). The upper bound also follows readily by combining Lemma 6.1 with (39), (41) and (37). □

7. Proof of Theorem 1.4

In this section we prove our main result. All the notation is as in section 2 and in the statement of Theorem 1.4. Let K be an admissible field, let $V \subseteq K^N$ be an L-dimensional vector space, and let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_L$ be the basis for V guaranteed by Theorems 1.1 and 1.2 (inequalities (2) and (3)). We will start by proving the theorem for the case of just one polynomial $P(X_1, \dots, X_N)$ of degree M, in other words first suppose $\mathcal{Z}_K = Z_K(P)$. Assume that P is not identically zero on V, so $V \nsubseteq Z_K(P)$. We will prove the existence of a point $\boldsymbol{x} \in V \setminus Z_K(P)$ satisfying (10).

Let S_1 be a finite subset of K such that $|S_1| > M$, and let $S = S_1^L$. Then, by Theorem 4.2, there exists $\boldsymbol{\xi} \in S$ such that $P(\boldsymbol{v}(\boldsymbol{\xi})) \neq 0$, where

$$\boldsymbol{v}(\boldsymbol{\xi}) = \sum_{i=1}^{L} \xi_i \boldsymbol{v}_i \in V. \tag{43}$$

By Lemma 2.1 combined with Theorems 1.1 and 1.2

$$H(\boldsymbol{v}(\boldsymbol{\xi})) \leq h(\boldsymbol{v}(\boldsymbol{\xi})) \leq L^{\delta} H(\boldsymbol{\xi}) \prod_{i=1}^{L} h(\boldsymbol{v}_i) \leq L^{\delta} e^{(1-\delta)g(K)L} C_K(L) H(\boldsymbol{\xi}) \mathcal{H}(V). \tag{44}$$

We now want to select the set S_1 in a way that would minimize $H(\boldsymbol{\xi})$; this choice will depend on the nature of the field K. We will show that the upper bound on $H(\boldsymbol{\xi})$ is precisely the constant $A_K(L, M)$ as in (14). Then we can take $\boldsymbol{x}$ in the statement of Theorem 1.4 to be $\boldsymbol{v}(\boldsymbol{\xi})$.

First assume that K is a number field with $\omega_K \leq M$. Then take

$$R = \left(2^{r_1} |\mathcal{D}_K|\right)^{1/2d} M^{1/d},$$

and let $S_1 = S_R(K)$, where $S_R(K)$ is as in (28). By Lemma 5.2

$$|S_R(K)| > \left(2^{r_1} |\mathcal{D}_K|\right)^{-1/2} R^d = M,$$

therefore $|S_R(K)| \geq M + 1$. We now can estimate $H(\boldsymbol{\xi})$. Since $\boldsymbol{\xi} \in S = S_R(K)^L$,

$$H_v(\boldsymbol{\xi}) \leq 1 \ \forall \ v \nmid \infty, \ H_v(\boldsymbol{\xi}) \leq R^{d_v} \ \forall \ v | \infty,$$

therefore

$$H(\boldsymbol{\xi}) \leq R = \left(2^{r_1} |\mathcal{D}_K|\right)^{1/2d} M^{1/d}. \tag{45}$$

Combining (44) with (45) produces (10).

Remark 7.1. Notice that in our choice of $R = \left(2^{r_1} |\mathcal{D}_K|\right)^{1/2d} M^{1/d}$ in the argument above it is essential to take $M^{1/d}$: if we take a smaller power of M, then $|S_R(K)|$ can be smaller than $M + 1$, in which case a polynomial P_V could vanish identically on $S_R(K)^L$. Indeed, as is discussed in [6], if $S_1 = \{\alpha_1, ..., \alpha_M\} \subset K$ and

$$P(X_1, ..., X_N) = \sum_{i=1}^{N} \prod_{j=1}^{M} (X_i - \alpha_j),$$

then for each $\boldsymbol{x} \in S_1^N$ we have $P(\boldsymbol{x}) = 0$.

Next suppose that K is an admissible function field of finite type $q \leq M$. Let Y be the smooth projective curve so that $K = \mathbb{F}_q(Y)$, as in section 6. Then take $R = R_K(M)$ as in (15), and let $S_1 = S_R(K)$, where $S_R(K)$ is as in (38). By Lemma 6.2

$$|S_R(K)| \geq \frac{2^{n(K)-1}}{\sqrt{n(K)}\ h_K} \left(\frac{R}{n(K) - 1} - \sqrt{n(K)}\ h_K \right)^{n(K)-1} + q - 1 = M + 1.$$

We now can estimate $H(\boldsymbol{\xi})$. Since $\boldsymbol{\xi} \in S = S_R(K)^L$,

$$H_v(\boldsymbol{\xi}) = 1 \ \forall \ v \notin \mathcal{M}_Y, \ H_v(\boldsymbol{\xi}) \leq e^{R d_v} \ \forall \ v \in \mathcal{M}_Y,$$

therefore

$$H(\boldsymbol{\xi}) \leq e^{R_K(M)}. \tag{46}$$

Combining (44) with (46) produces (10).

Remark 7.2. Another way of selecting the set S_1 in case of a function field K of finite type $q \leq M$ is by employing bounds on the number of elements of K of bounded height as in [19]. Specifically, Corollary 1 of [19] with $n = 2$ and $m = R$ implies that there exists a constant $T(K)$ such that the number of elements $f \in K$ with height $h(f) \leq e^R$ is $> T(K)q^{2R}$. If we pick

$$R = \frac{1}{2\log q} \log\left(\frac{M}{T(K)}\right), \tag{47}$$

then the set

$$S_1 = \{f \in K : h(f) \leq e^R\}$$

will have cardinality $|S_1| \geq M + 1$. Taking $S = S_1^L$, and letting $\boldsymbol{\xi} \in S$ guarantees that

$$H(\boldsymbol{\xi}) \leq \prod_{i=1}^{L} h(\xi_i) \leq e^{LR},$$

and so we can take $A_K(L, M) = e^{LR}$ with R as in (47). It should be remarked however that Thunder's estimate in Corollary 1 of [19] is asymptotic, and so an explicit value for the constant $T(K)$ is not specified.

Now suppose that K is any other admissible field except for those discussed above (i.e. K is either a number field with $\omega_K > M$, an admissible function field of finite type $q > M$ or of infinite type, or $K = \overline{\mathbb{Q}}$). Then K contains a set S_1 of cardinality at least $M+1$ such that for every $\xi \in S_1$ and every $v \in M(K)$, $|\xi|_v = 1$. Let $S = S_1^L$, and notice that for each $\boldsymbol{\xi} \in S$, $H(\boldsymbol{\xi}) = 1$. Combining this observation with (44) produces (10).

We have so far proved Theorem 1.4 for the case when $\mathcal{Z}_K$ is just a hypersurface defined over K. We can now extend our argument to any finite union of varieties $\mathcal{Z}_K$ as in the statement of Theorem 1.4. Since $V \not\subseteq \mathcal{Z}_K$, $V \not\subseteq Z_K(P_{i1}, \dots, P_{ik_i})$ for all $1 \leq i \leq J$, and so for each i at least one of the polynomials $P_{i1}, \dots, P_{ik_i}$ is not identically zero on V, say it is P_{ij_i} for some $1 \leq j_i \leq k_i$. Clearly for each $1 \leq i \leq J$, $Z_K(P_{i1}, \dots, P_{ik_i}) \subseteq Z_K(P_{ij_i})$, and $\deg(P_{ij_i}) = m_{ij_i} \leq M_i$. Define

$$P(X_1, \dots, X_N) = \prod_{i=1}^{J} P_{ij_i}(X_1, \dots, X_N),$$

so that $V \not\subseteq Z_K(P)$ while $\mathcal{Z}_K \subseteq Z_K(P)$. Then it is sufficient to construct a point of bounded height $\boldsymbol{x} \in V \setminus Z_K(P)$. Now notice that $\deg(P) = \sum_{i=1}^{J} m_{ij_i} \leq M$ and apply our argument above for the case of just one polynomial. This completes the proof of the theorem.

8. Twisted height

In this section we remark that all the results of this paper extend to bounds on *twisted height* of the point in question. Let us write $K_{\mathbb{A}}$ for the ring of adeles of K, and view K as a subfield of $K_{\mathbb{A}}$ under the diagonal embedding (see [22] for details). Let $A \in GL_N(K_{\mathbb{A}})$ with local components $A_v \in GL_N(K_v)$. The corresponding twisted height on K^N (as introduced by J. L. Thunder) is defined by

$$H_A(\boldsymbol{x}) = \left(\prod_{v \in M(K)} H_v(A_v \boldsymbol{x}) \right)^{1/d}, \tag{48}$$

for all $\boldsymbol{x} \in K^N$. Given any finite extension E/K, $K_{\mathbb{A}}$ can be viewed as a subring of $E_{\mathbb{A}}$, and let us also write A for the element of $GL_N(E_{\mathbb{A}})$ which coincides with A on $K_{\mathbb{A}}^N$. The corresponding twisted height on E^N extends the one on K^N, hence H_A is a height on $\overline{K}$. Notice also that the usual height H as defined above is simply H_I, where I is the identity element of $GL_N(K_{\mathbb{A}})$ all of whose local components are given by $N \times N$ identity matrices.

For each element $A \in GL_N(K_{\mathbb{A}})$, the height H_A is comparable to the canonical height H by means of certain dilation constants that, roughly speaking, indicate by how much does a given automorphism A of $K_{\mathbb{A}}^N$ "distort" the corresponding twisted height H_A as compared to H. We will only need one of these constants. Let $A_v = (a_{ij}^v)_{1 \leq i,j \leq N} \in GL_N(K_v)$ be local components of A for each $v \in M(K)$. Then for all but finitely many places $v \in M(K)$ the corresponding map A_v is an isometry; in fact, let $M_A(K) \subset M(K)$ be the finite (possibly empty) subset of places v at which A_v is *not* an isometry. For each $v \notin M_A(K)$, define $\mathcal{C}_v(A) = 1$, and for each $v \in M_A(K)$, let

$$\mathcal{C}_v(A) = \sum_{i=1}^N \sum_{j=1}^N |a_{ij}^v|_v, \tag{49}$$

and define

$$\mathcal{C}(A) = \prod_{v \in M(K)} \mathcal{C}_v^{d_v/d}, \tag{50}$$

which is a product of only a finite number of non-trivial terms. Clearly, in the case when $A = I$ is the identity element of $GL_N(K_{\mathbb{A}})$, $\mathcal{C}(A) = 1$. Then Proposition 4.1 of [13] states that

$$H_A(\boldsymbol{x}) \leq \mathcal{C}(A) H(\boldsymbol{x}), \tag{51}$$

for all $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$. Now one can use (51) to restate Theorem 1.4 replacing $H(\boldsymbol{x})$ by $H_A(\boldsymbol{x})$ - the only change is the appearance of the dilation constant $\mathcal{C}(A)$ in the upper bound.

Acknowledgment. I would like to thank Jeff Thunder for his helpful remarks, and for providing me with a copy of his preprint [19]. I would also like to acknowledge the wonderful hospitality of Max-Planck-Institut für Mathematik in Bonn, Germany, where a large part of this work has been done.

References

[1] N. Alon. Combinatorial nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7–29, 1999.

[2] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[3] J. W. S. Cassels. *An Introduction to the Geometry of Numbers.* Springer-Verlag, 1997.

[4] B. Edixhoven. Arithmetic part of Faltings's proof. *Diophantine approximation and abelian varieties (Soesterberg, 1992)*, Lecture Notes in Math.(1566):97–110, 1993.

[5] G. Faltings. Diophantine approximation on abelian varieties. *Ann. of Math.*, 133(2):549–576, 1991.

[6] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatsh. Math.*, 147(1):25–41, 2006.

[7] L. Fukshansky. Sigel's lemma with additional conditions. *J. Number Theory*, 120(1):13–25, 2006.

[8] P. Gordan. Uber den grossten gemeinsamen Factor. *Math. Ann.*, 7:443–448, 1873.

[9] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1.* Cambridge Univ. Press, 1947.

[10] R. J. Kooman. Faltings's version of Siegel's lemma. *Diophantine approximation and abelian varieties (Soesterberg, 1992)*, Lecture Notes in Math.(1566):93–96, 1993.

[11] S. Lang. *Algebraic Number Theory.* Springer-Verlag, 1994.

[12] T. Loher and D. Masser. Uniformly counting points of bounded height. *Acta Arith.*, 111(3):277–297, 2004.

[13] D. Roy and J. L. Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.

[14] D. Roy and J. L. Thunder. Addendum and erratum to: An absolute Siegel's lemma. *J. Reine Angew. Math.*, 508:47–51, 1999.

[15] S. Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[16] W. M. Schmidt. Northcott's theorem on heights. I. A general estimate. *Monatsh. Math.*, 115(1-2):169–181, 1993.

[17] W. M. Schmidt. Northcott's theorem on heights. II. The quadratic case. *Acta Arith.*, 70(4):343–375, 1995.

[18] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[19] J. L. Thunder. Counting subspaces of given height defined over a function field. *to appear in J. Number Theory.*

[20] J. L. Thunder. Siegel's lemma for function fields. *Michigan Math. J.*, 42(1):147–162, 1995.

[21] M. A. Tsfasman and S. G. Vladut. *Algebraic-Geometric Codes.* Kluwer Academic Publishers, 1991.

[22] A. Weil. *Basic Number Theory.* Springer-Verlag, 1973.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711

E-mail address: lenny@cmc.edu