LATTICE POINT COUNTING AND HEIGHT BOUNDS OVER NUMBER FIELDS AND QUATERNION ALGEBRAS

LENNY FUKSHANSKY AND GLENN HENSHAW

Abstract. An important problem in analytic and geometric combinatorics is estimating the number of lattice points in a compact convex set in a Euclidean space. Such estimates have numerous applications throughout mathematics. In this note, we exhibit applications of a particular estimate of this sort to several counting problems in number theory: counting integral points and units of bounded height over number fields, counting points of bounded height over positive definite quaternion algebras, and counting points of bounded height with a fixed support over global function fields. Our arguments use a collection of height comparison inequalities for heights over a number field and over a quaternion algebra. We also show how these inequalities can be used to obtain existence results for points of bounded height over a quaternion algebra, which constitute non-commutative analogues of variations of the classical Siegel's lemma and Cassels' theorem on small zeros of quadratic forms.

1. Introduction and statement of results

The classical combinatorial problem of estimating the number of lattice points in a compact set in the Euclidean space $\mathbb{R}^N$, $N \geq 2$, has been studied extensively: see [15] for an overview of some of the main results. Estimates of this type have a great number of applications in many different areas of mathematics. In number theory and arithmetic geometry such results lead to the development of counting estimates for rational points on varieties over global fields.

A compact convex set in $\mathbb{R}^N$ can be defined with the use of a norm, a device which measures "size" of points in the space. Since $\mathbb{R}$ is a local field, all norms on $\mathbb{R}^N$ are equivalent. An analogous device over a global field is a height function, a standard tool of Diophantine geometry which measures size with respect to a full collection of infinitely many inequivalent norms simultaneously. A famous theorem of Northcott [23] implies that any set of points of bounded height over a number field is finite. This observation is analogous to the statement that any compact set in $\mathbb{R}^N$ contains only finitely many lattice points: in this more general case the number field plays the role of a lattice in the ambient adelic space, where inequalities on height define compact sets.

The first counting estimate on the number of algebraic numbers of bounded height in a fixed number field was produced by Schanuel [25]. Schanuel's celebrated theorem has been extended and generalized in many ways by a number of authors over all global fields. While there are many further asymptotic results,

2010 *Mathematics Subject Classification.* Primary 11H06, 52C07, 11G50, 11E12, 11E39.

Key words and phrases. heights, lattice points, counting, quaternion algebras, Siegel's lemma, quadratic and hermitian forms.

The first author was partially supported by a grant from the Simons Foundation (#208969 to Lenny Fukshansky) and by the NSA Young Investigator Grant #1210223.

extending Schanuel's original approach (see [22] and [32] for some recent results and an overview), there are also several explicit bounds in the literature (see, for instance, [26] and [21]). It should be remarked that only [26] details some lower bounds, while the rest of the explicit estimates in the literature are upper bounds.

On the other hand, the problem of counting algebraic integers of bounded height in a fixed number field has received attention only more recently. While a mention of an asymptotic estimate without proof can be found in Lang's book [16] (Theorem 5.2 on p. 70), to the best of our knowledge the first complete proofs of asymptotic estimates of this kind were obtained in [31] and [1]. Explicit bounds in this situation are even more scarce, especially lower bounds. One explicit lower bound for the number of algebraic integers in a fixed number field was previously obtained by the first author in [13] (Corollary 1.6). Our first result is the following generalization of this bound; definition of the height function h and other necessary notation is reviewed in Section 2 below.

Theorem 1.1. *Let K be a number field of degree d over $\mathbb{Q}$, O_K its ring of integers, $N \geq 1$ an integer, and $\mathcal{M} \subset K^N$ a finitely generated O_K-module such that $\mathcal{M} \otimes_K K \cong K^L$, $1 \leq L \leq N$. Let $\mathcal{D}_K(\mathcal{M})$ be the discriminant of the module $\mathcal{M}$, as given in* (52) *below. For a positive real number R, define*

$$S_{K,N}(\mathcal{M}, R) = \{\boldsymbol{x} \in \mathcal{M} : h(\boldsymbol{x}) \leq R\}.$$

Then

$$|S_{K,N}(\mathcal{M}, R)| \geq \left(\frac{R}{\mathcal{E}_1(K, \mathcal{M}, L)|\mathcal{D}_K(\mathcal{M})|^{\frac{L}{2}}} - 1 \right) (\mathcal{E}_2(K, \mathcal{M}, L)R - 1)^{Ld-1}, \tag{1}$$

for each

$$R \geq \mathcal{E}_1(K, \mathcal{M}, L)|\mathcal{D}_K(\mathcal{M})|^{L/2},$$

where constants $\mathcal{E}_1(K, \mathcal{M}, L)$ and $\mathcal{E}_2(K, \mathcal{M}, L)$ are defined in (14) *and* (15) *below, respectively.*

Our method of proof makes use of techniques in analytic and geometric combinatorics. Specifically, we employ the Minkowski embedding of the vector space K^N into the Euclidean space $\mathbb{R}^{Nd}$. The module $\mathcal{M}$ under this embedding becomes a lattice of rank Ld, and the problem of counting points of bounded height in $\mathcal{M}$ translates into the problem of counting lattice points in a certain compact domain in $\mathbb{R}^{Nd}$. We then use a convenient explicit lattice point counting estimate in cubes as given by Lemma 3.1 below.

Remark 1.1. A simple upper bound on $|S_{K,N}(\mathcal{M}, R)|$ can be obtained from explicit estimates on the number of points of bounded height in K^L, as given in [26] and [21].

As an application of Theorem 1.1, we obtain estimates on the number of points of bounded height which are integral over a fixed order in a positive definite quaternion algebra. To the best of our knowledge, this is the first application of lattice point counting techniques in a non-commutative situation. We start out by setting some basic notation. Let K be a totally real number field of degree d over $\mathbb{Q}$, then K has precisely d real embeddings $\sigma_1, \dots, \sigma_d$. Let O_K be the ring of integers in K and let $\alpha, \beta \in O_K$ be totally negative elements, meaning that $\alpha^{(n)} := \sigma_n(\alpha) < 0$ and $\beta^{(n)} := \sigma_n(\beta) < 0$ for all $1 \leq n \leq d$. Let $D = \left(\frac{\alpha,\beta}{K}\right)$ be a positive definite quaternion algebra over K, generated by the elements i, j, k which satisfy the following relations:

$$i^2 = \alpha,\ j^2 = \beta,\ ij = -ji = k,\ k^2 = -\alpha\beta. \tag{2}$$

It is possible to define height functions on D; we discuss definitions of three such heights in Section 2 below: h, $H_{\inf}$, and $H^{\mathcal{O}}$, the last being a height function dependent on the choice of an order $\mathcal{O}$ is D. With this notation, we prove the following "non-commutative analogue" of Theorem 1.1.

Theorem 1.2. *Let $D = \binom{\alpha,\beta}{K}$ be as above and let $\mathcal{O}$ be an order in D. Let $N \geq 2$ be an integer, and let $Z \subseteq D^N$ be an L-dimensional right D-subspace, $1 \leq L \leq N$. For a positive real number R, define*

$$S_{D,N}(Z, \mathcal{O}, R) = \left\{ \boldsymbol{x} \in Z \cap \mathcal{O}^N : h(\boldsymbol{x}) \leq R \right\}.$$

Then $|S_{D,N}(Z, \mathcal{O}, R)| \geq$

$$\left(\frac{R}{\mathcal{E}_3(D, \mathcal{O}, Z, d, L) H^{\mathcal{O}}(Z)^{4d}} - 1 \right) \left(\mathcal{E}_4(D, \mathcal{O}, Z, d, L) R - 1 \right)^{4Ld-1}, \tag{3}$$

for each

$$R \geq \mathcal{E}_3(D, \mathcal{O}, Z, d, L) H^{\mathcal{O}}(Z)^{4d},$$

where constants $\mathcal{E}_3(D, \mathcal{O}, Z, d, L)$ and $\mathcal{E}_4(D, \mathcal{O}, Z, d, L)$ are defined in (39) *and* (40) *below, respectively.*

To establish this result, we view $\mathcal{O}$ as an O_K-module, which allows us to apply Theorem 1.1. Now the estimate is derived with the help of the height comparison lemmas proved in [5]: these are inequalities relating heights over the number field K to heights over the quaternion algebra D over K. In fact, these inequalities can also be used to produce an upper bound on the number of points of bounded height in D by an application of a result of [21].

Theorem 1.3. *Let D be as above, $R > 0$ be a real number, and define*

$$S_{D,N}(R) = \{ \boldsymbol{x} \in D^N : h(\boldsymbol{x}) \leq R \}. \tag{4}$$

Then

$$|S_{D,N}(R)| \leq (1088 d \log d)^{4N} \left(\frac{R}{t(\alpha, \beta)} \right)^{(4N+1)d}, \tag{5}$$

where the constant $t(\alpha, \beta)$ is defined below.

Remark 1.2. Notice, in particular, that Theorem 1.3 implies Northcott's finiteness property for sets of points of bounded height on positive definite quaternion algebras over totally real number fields. Further, it is clear that $|S_{D,N}(R)| \geq |S_{D,N}(Z, \mathcal{O}, R)|$, which implies the upper bound of (5) on $|S_{D,N}(Z, \mathcal{O}, R)|$. In addition, (3) implies that

$$|S_{D,N}(R)| \gg_{N,K,D} R^{4Nd}.$$

This paper is organized as follows. In Section 2 we set the necessary notation, introduce height functions, and define the constants used in our estimates. We prove Theorems 1.1, 1.2, and 1.3 in Section 3. We also include two appendices with related results. In Appendix A we show two more applications of the lattice point counting mechanism of Lemma 3.1 to counting problems over global fields. Specifically, we obtain explicit estimates on the number of S-units of bounded height in an arbitrary number field as well as number of rational functions of bounded height supported on a given curve over a fixed finite field. Finally, in Appendix B we formulate a basic method (already used in deriving Theorem 1.2 from Theorem 1.1) for obtaining results over quaternion algebras by "transferring" analogous results over number fields with the use of height comparison lemmas of [5]. We further exhibit this method at work by obtaining existence results for points of bounded height in linear and quadratic spaces.

2. Notation and heights

In this section we review the notation used in our main results and their proofs, as well as some further notation used in the appendices.

2.1. **Heights, quadratic forms, and constants over number fields.** Let K be a number field of degree d over $\mathbb{Q}$, O_K its ring of integers, $M(K)$ its set of places, $\mathcal{D}_K$ its discriminant, and let us write $\mathbb{N}$ for the norm from K to $\mathbb{Q}$. For each place $v \in M(K)$ we write K_v for the completion of K at v and let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree of K at v, so that for each $u \in M(\mathbb{Q})$

$$\sum_{v \in M(K), v|u} d_v = d. \tag{6}$$

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 rational prime. Then for each non-zero $a \in K$ the *product formula* reads

$$\prod_{v \in M(K)} |a|_v^{d_v} = 1. \tag{7}$$

We extend absolute values to vectors by defining the local heights. Let $N \geq 1$, and for each $v \in M(K)$ define a local height H_v on K_v^N by

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

and for each $v|\infty$ define another local height $\mathcal{H}_v$ on K_v^N by

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

for each $\boldsymbol{x} \in K_v^N$. Then we define two global height function on K^N:

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} H_v(\boldsymbol{x})^{d_v/d},\ \mathcal{H}(\boldsymbol{x}) = \prod_{v \nmid \infty} H_v(\boldsymbol{x})^{d_v/d} \times \prod_{v | \infty} \mathcal{H}_v(\boldsymbol{x})^{d_v/d}$$

for each $\boldsymbol{x} \in K^N$. Notice that due to the normalizing exponent $1/d$, our global height functions are absolute, i.e. for points over $\overline{\mathbb{Q}}$ their values do not depend on the field of definition. This means that if $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$ then $H(\boldsymbol{x})$ and $\mathcal{H}(\boldsymbol{x})$ can be evaluated over any number field containing the coordinates of $\boldsymbol{x}$.

We also define an *inhomogeneous* height function on vectors by

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

hence $h(\boldsymbol{x}) \geq H(\boldsymbol{x})$ for each $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$. In fact, the values of H and h are also related in the following sense: for each $\boldsymbol{x} \in K^N$, there exists $a \in K$ such that $a\boldsymbol{x} \in O_K^N$ and

$$H(\boldsymbol{x}) = h(a\boldsymbol{x}) \tag{8}$$

when $N > 1$; when $N = 1$, h is just the usual Weil height.

We will also define two different height functions on matrices. First, let B be an $N \times N$ matrix with entries in K, then we can view B as a vector in K^{N^2} and write $H(B)$ to denote the height of this vector. In particular, if B is a symmetric matrix, then

$$Q(\boldsymbol{X}, \boldsymbol{Y}) = \boldsymbol{X}^t B \boldsymbol{Y}$$

is a symmetric bilinear form in $2N$ variables over K, and

$$Q(\boldsymbol{X}) := Q(\boldsymbol{X}, \boldsymbol{X}) = \boldsymbol{X}^t B \boldsymbol{X}$$

is the associated quadratic form in N variables. We define $H(Q)$, the height of such quadratic and bilinear forms, to be $H(B)$.

The second height we define on matrices is the same as height function on subspaces of K^N. Let $X = (\boldsymbol{x}_1 \dots \boldsymbol{x}_L)$ be an $N \times L$ matrix of rank L over K, $1 \leq L \leq N$. Define

$$\mathcal{H}(X) = \mathcal{H}(\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_L). \tag{9}$$

For each $v | \infty$, the Cauchy-Binet formula guarantees that

$$\mathcal{H}_v(X) = |\det(X^* X)|_v^{1/2}, \tag{10}$$

where X^* is the complex conjugate transpose of X. On the other hand, $\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_L$ can be identified with the vector $\mathrm{Gr}(X)$ of *Grassmann coordinates* of X under the canonical embedding into $K^{\binom{N}{L}}$. Namely, let $\mathcal{I}$ be the collection of all subsets I of $\{1, ..., N\}$ of cardinality L, then $|\mathcal{I}| = \binom{N}{L}$. 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. Define

$$\mathrm{Gr}(X) = (\det(X_I))_{I \in \mathcal{I}} \in K^{\binom{N}{L}}. \tag{11}$$

By our remark above, $\mathcal{H}(X) = \mathcal{H}(\mathrm{Gr}(X))$. Now let $V \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$. Choose a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ for V over K, and let $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_L)$ be the corresponding $N \times L$ basis matrix. Define height of V to be

$$H(V) := \mathcal{H}(X).$$

This height is well defined, since it does not depend on the choice of the basis for V: let $\boldsymbol{y}_1, ..., \boldsymbol{y}_L$ be another basis for V over K and $Y = (\boldsymbol{y}_1 \dots \boldsymbol{y}_L)$ the corresponding $N \times L$ basis matrix, then there exists $C \in \mathrm{GL}_L(K)$ such that $Y = XC$, and so

$$\boldsymbol{y}_1 \wedge \dots \wedge \boldsymbol{y}_L = (\det C) \ \boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_L,$$

hence, by the product formula $\mathcal{H}(\boldsymbol{y}_1 \wedge \dots \wedge \boldsymbol{y}_L) = \mathcal{H}(\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_L)$.

It will be convenient for us to define certain field constants that we use in our inequalities. First define

$$c_K(\mathcal{M}) = \min \left\{ h(\alpha) : \alpha \in K \text{ such that } \alpha\mathcal{M} \subset O_K^L \right\}, \tag{12}$$

as well as

$$z_K(\mathcal{M}) = \min \left\{ h(\alpha)h(\alpha^{-1}) : \alpha \in K \text{ such that } \alpha\mathcal{M} \subset O_K^L \right\}. \tag{13}$$

Now the constants used in the statement of Theorem 1.1 are given by

$$\mathcal{E}_1(K,\mathcal{M},L) = 2^{\frac{Lr_1-3}{2}} Ld\ z_K(\mathcal{M}) c_K(\mathcal{M})^{Ld-1} \tag{14}$$

and

$$\mathcal{E}_2(K,\mathcal{M},L) = \frac{2\sqrt{2}\ c_K(\mathcal{M})}{Ld\ z_K(\mathcal{M})}. \tag{15}$$

Finally, for each $v|\infty$ and positive integer j we define, as in [28],

$$r_v(j) = \begin{cases} \pi^{-1/2}\Gamma(j/2+1)^{1/j} & \text{if } v|\infty \text{ is real,} \\ (2\pi)^{-1/2}\Gamma(j+1)^{1/2j} & \text{if } v|\infty \text{ is complex,} \end{cases}$$

and for any positive integers ℓ and j, define the constant $T_K(\ell, j)$ by

$$\begin{aligned} T_K(\ell,j) \quad &= \quad 27\left(\frac{1}{\pi}\right)^{\frac{r_2\ell(9\ell+14)}{2d}} 2^{\frac{r_2\ell(9\ell+14)+(21\ell-21)d+5r_1+4}{2d}+\max\{\ell,9\}} \ell^{\frac{27\ell+51}{2}} j^{\frac{2}{d}} (j+2)^{\frac{3}{d}} \\ &\times \quad |\mathcal{D}_K|^{\frac{\ell(9\ell+14)+14}{2d}+\max\{\ell,9\}} \left(\prod_{v|\infty} r_v(\ell-1)^{d_v/d}\right)^{\max\{\ell,9\}} . \end{aligned} \tag{16}$$

This constant is used in formula (42), which is the definition of $\mathcal{A}_{K,\mathcal{O}}(L,M,J,\alpha,\beta)$, the constant in the inequality (85) of Theorem B.2.

2.2. **Heights, quadratic forms, and constants over quaternion algebras.** We can also extend the height machinery to the context of quaternion algebras, using the approach of [18]. Let K be a totally real number field, $\alpha, \beta \in O_K$ be totally negative, and $D = \left(\frac{\alpha,\beta}{K}\right)$ be a positive definite quaternion algebra over K, as defined in Section 1 above. As a vector space, D has dimension four over K, and $1, i, j, k$ is a basis. From now on we will fix this basis, and thus will always write each element $x \in D$ as

$$x = x(0) + x(1)i + x(2)j + x(3)k,$$

where $x(0), x(1), x(2), x(3) \in K$ are respective components of x, and the standard involution on D is conjugation:

$$\overline{x} = x(0) - x(1)i - x(2)j - x(3)k.$$

We define trace and norm on D by

$$\mathrm{Tr}(x) = x + \overline{x} = 2x(0),\ \mathrm{N}(x) = x\overline{x} = x(0)^2 - \alpha x(1)^2 - \beta x(2)^2 + \alpha\beta x(3)^2.$$

The algebra D is said to be positive definite because the norm $\mathrm{N}(x)$ is given by a positive definite quadratic form. In fact, since the norm form $\mathrm{N}(x)$ is positive definite, $D_{v_n} := D \otimes_K K_{v_n}$ is isomorphic to the real quaternion $\mathbb{H} = \mathbb{R}+\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$ for each $1 \leq n \leq d$. Hence each embedding σ_n of K, $1 \leq n \leq d$, induces an embedding $\sigma_n : D \to D_{v_n}$, given by

$$\sigma_n(x) = x(0)^{(n)} + x(1)^{(n)}i + x(2)^{(n)}j + x(3)^{(n)}k.$$

From now on we will write $x^{(n)}$ for $\sigma_n(x)$. Then the local norm at each archimedean place is also a positive definite quadratic form over the respective real completion K_{v_n}:

$$\begin{aligned} &\mathrm{N}^{(n)}(x) = x^{(n)}\overline{x}^{(n)} \\ &= \left(x(0)^{(n)}\right)^2 - \alpha^{(n)}\left(x(1)^{(n)}\right)^2 - \beta^{(n)}\left(x(2)^{(n)}\right)^2 + \alpha^{(n)}\beta^{(n)}\left(x(3)^{(n)}\right)^2, \end{aligned}$$

for each $1 \leq n \leq d$. We now have archimedean absolute values on D, corresponding to the infinite places $v_1, \dots, v_d$ of K: for each $x \in D$, define

$$|x|_{v_n} = \sqrt{\mathrm{N}^{(n)}(x)},$$

for every $1 \leq n \leq d$. It will be convenient to define

$$\begin{aligned} s_{v_n}(\alpha,\beta) &= \max\{1, |\alpha|_{v_n}, |\beta|_{v_n}, |\alpha\beta|_{v_n}\}^{\frac{1}{2}}, \\ t_{v_n}(\alpha,\beta) &= \min\{1, |\alpha|_{v_n}, |\beta|_{v_n}, |\alpha\beta|_{v_n}\}^{\frac{1}{2}}, \end{aligned} \tag{17}$$

for each $1 \leq n \leq d$, and also let

$$s(\alpha,\beta) = \prod_{n=1}^{d} s_{v_n}(\alpha,\beta),\ t(\alpha,\beta) = \prod_{n=1}^{d} t_{v_n}(\alpha,\beta). \tag{18}$$

Since local norm forms are positive definite, we immediately have the following inequalities:

$$t_{v_n}(\alpha,\beta) \max_{0\leq m\leq 3} |x(m)|_{v_n} \leq\ |x|_{v_n} \leq 2 s_{v_n}(\alpha,\beta) \max_{0\leq m\leq 3} |x(m)|_{v_n}. \tag{19}$$

Now, generalizing notation of [18], we can define an infinite homogeneous height on D^N by

$$H_{\mathrm{inf}}(\boldsymbol{x}) = \left(\prod_{n=1}^{d} \max_{1\leq l\leq N} |x_l|_{v_n} \right)^{1/d}, \tag{20}$$

and define an infinite inhomogeneous height on D^N by

$$h_{\mathrm{inf}}(\boldsymbol{x}) = H_{\mathrm{inf}}(1, \boldsymbol{x}), \tag{21}$$

for every $\boldsymbol{x} \in D^N$. Clearly, $H_{\mathrm{inf}}(\boldsymbol{x}) \leq h_{\mathrm{inf}}(\boldsymbol{x})$. The infinite height takes into account the contributions at the archimedean places. As in [18], we also define its counterpart, the finite height. Let us once and for all fix an order $\mathcal{O}$ in D; our definition will be with respect to the order $\mathcal{O}$, and this height will be denoted by $H^{\mathcal{O}}_{\mathrm{fin}}$. Specifically, for each $\boldsymbol{x} \in \mathcal{O}^N$, let

$$H^{\mathcal{O}}_{\mathrm{fin}}(\boldsymbol{x}) = [\mathcal{O} : \mathcal{O}x_1 + \dots + \mathcal{O}x_N]^{-1/4d}. \tag{22}$$

This is well defined, since $\mathcal{O}x_1 + \dots + \mathcal{O}x_N$ is a left submodule of $\mathcal{O}$. Now we can define the global homogeneous height on $\mathcal{O}^N$ by

$$H^{\mathcal{O}}(\boldsymbol{x}) = H_{\mathrm{inf}}(\boldsymbol{x}) H^{\mathcal{O}}_{\mathrm{fin}}(\boldsymbol{x}), \tag{23}$$

and the global inhomogeneous height by

$$h(\boldsymbol{x}) := H_{\mathrm{inf}}(1,\boldsymbol{x}) H^{\mathcal{O}}_{\mathrm{fin}}(1,\boldsymbol{x}) = h_{\mathrm{inf}}(\boldsymbol{x}) \geq H^{\mathcal{O}}(\boldsymbol{x}), \tag{24}$$

since $\mathcal{O} + \mathcal{O}x_1 + \dots + \mathcal{O}x_N = \mathcal{O}$. To extend this definition to D^N, notice that for each $\boldsymbol{x} \in D^N$ there exists $a \in O_K$ such that $a\boldsymbol{x} \in \mathcal{O}^N$, and define $H^{\mathcal{O}}(\boldsymbol{x})$ to be $H^{\mathcal{O}}(a\boldsymbol{x})$ for any such a. This is well defined by the product formula, and $H^{\mathcal{O}}(\boldsymbol{x}t) = H^{\mathcal{O}}(\boldsymbol{x})$ for all $t \in D^{\times}$.

We will now define height on the set of proper right D-subspaces of D^N, again following [18]. Recall that D splits over $E = K(\sqrt{\alpha})$, meaning that there exists a K-algebra homomorphism $\rho : D \to \mathrm{Mat}_{22}(E)$, given by

$$\rho(x(0) + x(1)i + x(2)j + x(3)k) = \begin{pmatrix} x(0) + x(1)\sqrt{\alpha} & x(2) + x(3)\sqrt{\alpha} \\ \beta(x(2) - x(3)\sqrt{\alpha}) & x(0) - x(1)\sqrt{\alpha} \end{pmatrix}, \tag{25}$$

so that $\rho(D)$ spans $\mathrm{Mat}_{22}(E)$ as an E-vector space (see Proposition 13.2a (p. 238) and Exercise 1 (p. 240) of [24]). This map extends naturally to matrices over D. Let $Z \subseteq D^N$ be an L-dimensional right vector subspace of D^N, $1 \leq L < N$. Then there exists an $(N-L) \times N$ matrix C over D with left row rank $N-L$ such that Z is the solution space of the linear system $C\boldsymbol{X} = \boldsymbol{0}$. Define

$$H_{\mathrm{inf}}(C) = \left(\prod_{n=1}^{d} \left| \det\left(\rho(CC^*)\right) \right|_{v_n} \right)^{1/4d}, \tag{26}$$

where C^* is the conjugate transpose of C. The analogue of Cauchy-Binet formula works here as well (see (2.7) and (2.8) of [18], as well as Corollary 1 of [19]), and so we have an alternative formula:

$$H_{\mathrm{inf}}(C) = \left(\prod_{n=1}^{d} \sum_{C_0} \left| \det\left(\rho(C_0)\right) \right|^2_{v_n} \right)^{1/2d}, \tag{27}$$

where the sum is taken over all $(N-L) \times (N-L)$ minors C_0 of C. Also define

$$H^{\mathcal{O}}_{\mathrm{fin}}(C) = [\mathcal{O}^{N-L} : C(\mathcal{O}^N)]^{-1/4d}, \tag{28}$$

where C is viewed as a linear map $\mathcal{O}^N \to \mathcal{O}^{N-L}$. Then we can define

$$H^{\mathcal{O}}(Z) = H^{\mathcal{O}}(C) := H_{\mathrm{inf}}(C) H^{\mathcal{O}}_{\mathrm{fin}}(C). \tag{29}$$

This definition does not depend on the specific choice of such matrix C. By the duality principle proved in [20],

$$H^{\mathcal{O}}(Z) = H^{\mathcal{O}}(Z^{\perp}), \tag{30}$$

where $Z^{\perp} = \{\boldsymbol{y} \in D^N : \boldsymbol{x}^* \boldsymbol{y} = 0 \ \forall \ \boldsymbol{x} \in Z\}$. This means that if $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L$ is a basis for Z over D and $X = (\boldsymbol{x}_1 \dots \boldsymbol{x}_L)$ is the corresponding basis matrix, then

$$H^{\mathcal{O}}(Z) = H^{\mathcal{O}}(X) := \left([\mathcal{O}^L : X^t(\mathcal{O}^N)]^{-1} \prod_{n=1}^{d} \left| \det\left(\rho(X^*X)\right) \right|_{v_n} \right)^{1/4d}, \tag{31}$$

completely analogous to the definition of the height $H^{\mathcal{O}}(C)$ in (29); here X^t is viewed as a linear map $\mathcal{O}^N \to \mathcal{O}^{N-L}$.

It will also be convenient to define a map $[\ ] : D \to K^4$, given by

$$[x] = (x(0), x(1), x(2), x(3)),$$

for each $x = x(0) + x(1)i + x(2)j + x(3)k \in D$. This map obviously extends to $[\ ] : D^N \to K^{4N}$, given by $[\boldsymbol{x}] = ([x_1], \dots, [x_N])$ for each $\boldsymbol{x} = (x_1, \dots, x_N) \in D^N$. Clearly this is a bijection; in fact, it is an isomorphism of K-vector spaces, and we will write $[\ ]^{-1}$ for its inverse.

By analogy with heights over D, we will also write

$$H_{\mathrm{inf}}(\boldsymbol{x}) = \prod_{v | \infty} H_v(\boldsymbol{x})^{d_v/d}, \ H_{\mathrm{fin}}(\boldsymbol{x}) = \prod_{v \nmid \infty} H_v(\boldsymbol{x})^{d_v/d},$$

for every $\boldsymbol{x} \in K^N$. Then by Lemma 2.1 of [18], for every $\boldsymbol{x} \in O_K^N$ we have

$$H_{\mathrm{fin}}(\boldsymbol{x}) = \left[O_K : O_K x_1 + \dots + O_K x_N \right]^{-1/d}. \tag{32}$$

Also, if V is an L-dimensional subspace of K^N and C is any $(N-L)\times N$ matrix over O_K of rank $1 \leq L < N$, viewed as a linear map $O_K^N \to O_K^{N-L}$, such that $V = \{\boldsymbol{x} \in K^N : C\boldsymbol{x} = \boldsymbol{0}\}$, let us write

$$H_{\text{inf}}(C) = \prod_{v \mid \infty} \mathcal{H}_v(C)^{d_v/d},\ H_{\text{fin}}(C) = \prod_{v \nmid \infty} H_v(C)^{d_v/d},$$

and then by Lemma 2.1 and Proposition 2.4 of [18], we have

$$H_{\text{fin}}(C) = \left[O_K^{N-L} : C(O_K^N)\right]^{-1/d}. \tag{33}$$

This means that the definitions over K and over D are really analogous.

Now let $F(\boldsymbol{X},\boldsymbol{Y}) \in D[\boldsymbol{X},\boldsymbol{Y}]$ be a hermitian form in $2N$ variables with coefficients in D, so that $F(a\boldsymbol{x},\boldsymbol{y}) = \bar{a}F(\boldsymbol{x},\boldsymbol{y})$ and $F(\boldsymbol{y},\boldsymbol{x}) = \overline{F(\boldsymbol{x},\boldsymbol{y})}$ for each $a \in D$ and $\boldsymbol{x},\boldsymbol{y} \in D^N$. We also write $F(\boldsymbol{X})$ for $F(\boldsymbol{X},\boldsymbol{X})$, then $F(\boldsymbol{x}) \in K$ for any $\boldsymbol{x} \in D^N$. Let us also write $\mathbb{F} = (f_{ml})$ for the $N \times N$ coefficient matrix of F, then $f_{ml} = \overline{f_{lm}}$ for each $1 \leq l,m \leq N$, and $F(\boldsymbol{X},\boldsymbol{Y}) = \boldsymbol{X}^t\mathbb{F}\boldsymbol{Y}$. In the same way as for quadratic and bilinear forms over K, we will talk about the height of the hermitian form F over D, where by $H^{\mathcal{O}}(F)$ (respectively, $H_{\text{inf}}(F)$, $H^{\mathcal{O}}_{\text{fin}}(F)$) we will always mean $H^{\mathcal{O}}(\mathbb{F})$ (respectively, $H_{\text{inf}}(\mathbb{F})$, $H^{\mathcal{O}}_{\text{fin}}(\mathbb{F})$), viewing $\mathbb{F}$ as a vector in D^{N^2}. We define the corresponding bilinear form B over K by taking the trace of F, i.e. $B([\boldsymbol{X}],[\boldsymbol{Y}]) = \text{Tr}(F(\boldsymbol{X},\boldsymbol{Y}))$. The associated quadratic form

$$Q([\boldsymbol{X}]) := B([\boldsymbol{X}],[\boldsymbol{X}]) \tag{34}$$

in $4N$ variables over K is equal to $2F(\boldsymbol{X})$. Therefore $F(\boldsymbol{x}) = 0$ for some $\boldsymbol{x} \in D^N$ if and only if $Q([\boldsymbol{x}]) = 0$. Write $\mathbb{B}$ for the $4N \times 4N$ symmetric matrix of B over K, then each entry of $\mathbb{F}$ corresponds to a 4×4 block in $\mathbb{B}$. Specifically, if $f_{ml} = f_{ml}(0) + f_{ml}(1)i + f_{ml}(2)j + f_{ml}(3)k \in D$, then the corresponding block in $\mathbb{B}$ is of the form

$$\mathbb{B}(f_{ml}) := \begin{pmatrix} 2f_{ml}(0) & 2\alpha f_{ml}(1) & 2\beta f_{ml}(2) & -2\alpha\beta f_{ml}(3) \\ -2\alpha f_{ml}(1) & -2\alpha f_{ml}(0) & -2\alpha\beta f_{ml}(3) & 2\alpha\beta f_{ml}(2) \\ -2\beta f_{ml}(2) & 2\alpha\beta f_{ml}(3) & -2\beta f_{ml}(0) & -2\alpha\beta f_{ml}(1) \\ 2\alpha\beta f_{ml}(3) & -2\alpha\beta f_{ml}(2) & 2\alpha\beta f_{ml}(1) & 2\alpha\beta f_{ml}(0) \end{pmatrix}, \tag{35}$$

so $\mathbb{B} = (\mathbb{B}(f_{ml}))_{1\leq m,l\leq N}$, and $Q(\boldsymbol{z}) = \boldsymbol{z}^t\mathbb{B}\boldsymbol{z}$ for each $\boldsymbol{z} \in K^{4N}$. As defined before, we will write $H(Q)$ (respectively, $H_{\text{inf}}(Q)$, $H_{\text{fin}}(Q)$) for $H(\mathbb{B})$ (respectively, $H_{\text{inf}}(\mathbb{B})$, $H_{\text{fin}}(\mathbb{B})$), viewed as a vector in K^{16N^2}.

Finally, we define the constants that appear in our inequalities over quaternion algebras. Define a special order $\mathcal{O}_D$ in D:

$$\mathcal{O}_D = O_K + O_K i + O_K j + O_K k. \tag{36}$$

For our fixed order $\mathcal{O}$, define

$$c_{\mathcal{O}}(Z) = \min\left\{h(a) : a \in K \text{ such that } aZ \cap \mathcal{O}^N \subset \mathcal{O}_D^N\right\}, \tag{37}$$

as well as

$$z_{\mathcal{O}}(Z) = \min\left\{h(a)h(a^{-1}) : a \in K \text{ such that } aZ \cap \mathcal{O}^N \subset \mathcal{O}_D^N\right\}. \tag{38}$$

Let $\Delta_{\mathcal{O}}$ be the discriminant of the order $\mathcal{O}$, which is the ideal in O_K generated by all the elements of the form

$$\det\left(\text{Tr}(\omega_h\omega_n)\right)_{0\leq h,n\leq 3} \in O_K,$$

where $\omega_0, \dots, \omega_3$ are in $\mathcal{O}$. Now the constants used in the statement of Theorem 1.2 are given by

$$\mathcal{E}_3(D, \mathcal{O}, Z, d, L) = 2^{\frac{4L(d-2)+3}{2}} Ld\ s(\alpha, \beta) z_{\mathcal{O}}(Z) c_{\mathcal{O}}(Z)^{4Ld-1} \mathbb{N}(\Delta_{\mathcal{O}})^{\frac{L}{2}}, \tag{39}$$

where $\mathbb{N}$ stands for the norm from K to $\mathbb{Q}$, and

$$\mathcal{E}_4(D, \mathcal{O}, Z, d, L) = \frac{c_{\mathcal{O}}(Z)}{2\sqrt{2}Ld\ s(\alpha, \beta) z_{\mathcal{O}}(Z)}. \tag{40}$$

We also define the constant that appears in the upper bound of Theorem B.2. Let

$$\mathfrak{M}(\mathcal{O}) := \max \left\{ \frac{\mathbb{N}(\Delta_{\mathcal{O}})^{1/2}}{\mathbb{N}(4\alpha\beta)}, \frac{\mathbb{N}(4\alpha\beta)}{\mathbb{N}(\Delta_{\mathcal{O}})^{1/2}} \right\}, \tag{41}$$

and define

$$\mathcal{A}_{K,\mathcal{O}}(L, M, J, \alpha, \beta) = \frac{2^{\frac{9L+13}{2}} s(\alpha, \beta)^{9L+12}}{t(\alpha, \beta)^{\frac{9L+11}{2}}} \mathfrak{M}(\mathcal{O})^{4(N-L)(9L+12)} T_K(L, M + 2J + 1), \tag{42}$$

where the field constant $T_K(\ell, j)$ is defined in (16) and $s(\alpha, \beta)$, $t(\alpha, \beta)$ are defined in (18). We are now ready to proceed.

3. Counting points of bounded height

Here we discuss counting estimates for the cardinality of sets of points of bounded height over number fields and quaternion algebras, as discussed above. In particular, we prove Theorems 1.1, 1.2 and 1.3.

Our main tool is a basic counting mechanism for lattice points in cubes, which is a consequence of results of [11] and [12]. Let us write $C_n(R)$ for the closed cube of side-length $2R$ centered at the origin in $\mathbb{R}^n$, i.e.

$$C_n(R) = \left\{ \boldsymbol{x} \in \mathbb{R}^n : \max_{1 \leq m \leq n} |x_m| \leq R \right\}. \tag{43}$$

Lemma 3.1. *Let $\Lambda \subset \mathbb{R}^N$ be a lattice of rank $L \leq N$ so that for every $\mathbf{0} \neq \boldsymbol{x} \in \Lambda$,*

$$|\boldsymbol{x}| := \max_{1 \leq n \leq N} |x_n| \geq c \tag{44}$$

for some $c \in \mathbb{R}_{>0}$ independent of $\boldsymbol{x}$. Then for any $R \in \mathbb{R}_{>0}$,

$$|\Lambda \cap C_N(R)| \leq \begin{cases} \left(\frac{2Rc^{N-1}}{\det(\Lambda)} + 1\right) \left(\frac{2R}{c} + 1\right)^{N-1} & \text{if } L = N \\ \left(\frac{2R}{c} + 1\right)^{N-1} & \text{if } L < N \\ \left(\frac{2\binom{N}{L}^{1/2} R}{\det(\Lambda)} + 1\right) (2R + 1)^{L-1} & \text{if } \Lambda \subseteq \mathbb{Z}^N \end{cases} \tag{45}$$

In addition, if $R \geq \frac{L}{2} \max\left\{\frac{\det(\Lambda)}{c^{L-1}}, c\right\}$, then

$$|\Lambda \cap C_N(R)| \geq \left(\frac{2Rc^{L-1}}{L \det(\Lambda)} - 1\right) \left(\frac{2R}{Lc} - 1\right)^{L-1}. \tag{46}$$

Proof. We start by obtaining the upper bound of (45). If $L = N$, then (45) follows from Lemma 2.1 of [12]. Assume that $L < N$ and let

$$V = \left\{ \boldsymbol{x} \in \mathbb{R}^N : \boldsymbol{x} \cdot \boldsymbol{y} = 0 \ \forall \ \boldsymbol{y} \in \Lambda \right\}$$

be the $(N-L)$-dimensional subspace of $\mathbb{R}^N$ orthogonal to Λ. Let $\Lambda' \subseteq V$ be a full-rank lattice in V spanned by an orthogonal basis of unit vectors, then $\det(\Lambda') = 1$ and a shortest nonzero vector in Λ' has norm 1. Now let $R \in \mathbb{R}_{>0}$ and let $R_* \geq \max\left\{ 2\sqrt{N}R, \frac{c\sqrt{N}}{\min\{|\boldsymbol{x}| : \boldsymbol{0} \neq \boldsymbol{x} \in \Lambda'\}} \right\}$, and define

$$\Lambda''(R_*) = \Lambda \oplus R_* \Lambda'.$$

Notice that every $\boldsymbol{x} \in \Lambda''(R_*)$ is of the form $\boldsymbol{x} = \boldsymbol{x}_1 + R_* \boldsymbol{x}_2$ for some $\boldsymbol{x}_1 \in \Lambda$, $\boldsymbol{x}_2 \in \Lambda'$ and $\|\boldsymbol{x}\|^2 = \|\boldsymbol{x}_1\|^2 + R_*^2 \|\boldsymbol{x}_2\|^2$ since $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are orthogonal. Therefore

$$|\boldsymbol{x}| \geq \frac{1}{\sqrt{N}} \|\boldsymbol{x}\| = \frac{1}{\sqrt{N}} \sqrt{\|\boldsymbol{x}_1\|^2 + R_*^2 \|\boldsymbol{x}_2\|^2} \geq \max\{2R, c\}, \tag{47}$$

which in particular means that if $\boldsymbol{x} \in \Lambda''(R_*) \cap C_N(R)$, then $\boldsymbol{x}_2 = \boldsymbol{0}$ and so $\boldsymbol{x} \in \Lambda$. Hence $|\Lambda \cap C_N(R)| = |\Lambda''(R_*) \cap C_N(R)|$ and

$$\det(\Lambda''(R_*)) = R_*^{N-L} \det(\Lambda) \geq (2NR)^{N-L} \det(\Lambda). \tag{48}$$

Since rank of $\Lambda''(R_*)$ is N, combining (47) and (48) with Lemma 2.1 of [12] produces the bound

$$|\Lambda \cap C_N(R)| \leq \left(\frac{2Rc^{N-1}}{R_*^{N-L} \det(\Lambda)} + 1 \right) \left(\frac{2R}{c} + 1 \right)^{N-1},$$

and the bound of (45) in case $L < N$ follows by taking the limit as $R_* \to \infty$.

Next, following [12], let X be a basis matrix for Λ and for each $I \subset \{1, \dots, N\}$ with $|I| = L$ write X_I for the $L \times L$ submatrix of X whose columns are indexed by the elements of I. Let $J \subset \{1, \dots, N\}$ with $|J| = L$ be such that

$$|\det(X_J)| = \max_{|I|=L} |\det(X_I)|,$$

and let Ω be the lattice of full rank in $\mathbb{R}^L$ spanned over $\mathbb{Z}$ by the column vectors of X_J. Then $\det(\Omega) = |\det(X_J)|$ is maximum of absolute values of Grassmann coordinates of Λ, and Cauchy-Binet formula (see, for instance (18) of [12]) implies that

$$\det(\Omega) \leq \det(\Lambda) \leq \binom{N}{L}^{1/2} \det(\Omega). \tag{49}$$

The bound of (45) in case $\Lambda \subseteq \mathbb{Z}^N$ follows by combining (49) with Theorem 4.2 of [11].

Now we derive the lower bound of (46). By Corollary 1 on p. 13 of [4], it is possible to select a basis for Ω such that the basis matrix A is upper triangular, all of its nonzero entries are positive, and the maximum entry of each row occurs on the diagonal. By (44) above, each of these entries is at least c, since each column of A is a linear combination of columns of X_J. The lattice Ω now satisfies the conditions of Lemma 2.1 of [12], and so if $2R \geq \max\left\{ \frac{\det(\Omega)}{c^{L-1}}, c \right\}$, then

$$|\Omega \cap C_L(R)| \geq \left(\frac{2Rc^{L-1}}{\det(\Omega)} - 1 \right) \left(\frac{2R}{c} - 1 \right)^{L-1}, \tag{50}$$

where the condition on R simply ensures that every term in the product on the right hand side of the inequality is positive. Now Theorem 4.3 (equation (31)) of [11] implies that

$$|\Lambda \cap C_N(R)| \geq \left| \Omega \cap C_L\left(\frac{R}{L}\right) \right|, \tag{51}$$

and combining this observation with (49) and (50), we obtain (46). □

We now use Lemma 3.1 to prove Theorem 1.1, producing an estimate on the number of points of bounded height in a fixed torsion-free O_K-module for an arbitrary number field K.

Proof of Theorem 1.1. Let all the notation be as in the statement of the theorem. Since $\mathcal{M} \subset K^N$, it must be torsion-free, hence projective. By the structure theorem for finitely generated projective modules over Dedekind domains (see, for instance [17]),

$$\mathcal{M} = \left\{ \sum_{n=1}^{L} \beta_n \boldsymbol{y}_n : \boldsymbol{y}_n \in O_K^N,\ \beta_n \in \mathcal{I}_n \right\}$$

for some O_K-fractional ideals $\mathcal{I}_1, \dots, \mathcal{I}_L$ in K. By Proposition 13 on p.66 of [17], the discriminant of $\mathcal{M}$ is then

$$\mathcal{D}_K(\mathcal{M}) := \mathcal{D}_K \prod_{n=1}^{L} \mathbb{N}(\mathcal{I}_n)^2, \tag{52}$$

where $\mathbb{N}(\mathcal{I}_n)$ is the norm of the fractional ideal $\mathcal{I}_n$. Define $\mathfrak{U}_K(\mathcal{M})$, a fractional O_K-ideal in K, to be

$$\mathfrak{U}_K(\mathcal{M}) = \left\{ \alpha \in K : \alpha\mathcal{M} \subseteq O_K^N \right\}, \tag{53}$$

then

$$c_K(\mathcal{M}) = \min\{h(\alpha) : \alpha \in \mathfrak{U}_K(\mathcal{M})\}.$$

Let

$$\sigma_1, \dots, \sigma_{r_1}, \tau_1, \dots, \tau_{r_2}, \dots, \tau_{2r_2}$$

be the embeddings of K into $\mathbb{C}$ with $\sigma_1, \dots, \sigma_{r_1}$ being the real embeddings and $\tau_n, \tau_{r_2+n} = \bar{\tau}_n$ for each $1 \leq n \leq r_2$ being the pairs of complex conjugate embeddings. For each $\alpha \in K$ and each complex embedding τ_n, write $\tau_{n1}(\alpha) = \Re(\tau_n(\alpha))$ and $\tau_{n2}(\alpha) = \Im(\tau_n(\alpha))$, where $\Re$ and $\Im$ stand respectively for real and imaginary parts of a complex number. Then $d = r_1 + 2r_2$, and we define an embedding

$$\sigma^N = (\sigma_1^N, \dots, \sigma_{r_1}^N, \tau_{11}^N, \tau_{12}^N, \dots, \tau_{r_2 1}^N, \tau_{r_2 2}^N) : K^N \to \mathbb{R}^{Nd}.$$

Let $\alpha \in \mathfrak{U}_K(\mathcal{M})$. Since $\alpha\boldsymbol{x} \in O_K^N$ for every $\boldsymbol{x} \in \mathcal{M}$, we have

$$\max\{|\sigma_1(\alpha x_n)|, \dots, |\sigma_{r_1}(\alpha x_n)|, |\tau_{11}(\alpha x_n)|, |\tau_{12}(\alpha x_n)|, \dots, |\tau_{r_2 1}(\alpha x_n)|, |\tau_{r_2 2}(\alpha x_n)|\}$$
$$\geq \frac{1}{\sqrt{2}},$$

for every $1 \leq n \leq N$, as indicated in [12], and therefore

$$\begin{aligned} & \max\{|\sigma_1(x_n)|, \dots, |\sigma_{r_1}(x_n)|, |\tau_{11}(x_n)|, |\tau_{12}(x_n)|, \dots, |\tau_{r_21}(x_n)|, |\tau_{r_22}(x_n)|\} \\ \geq \quad & \frac{1}{\sqrt{2}} \max\{|\sigma_1(\alpha)|, \dots, |\sigma_{r_1}(\alpha)|, |\tau_{11}(\alpha)|, |\tau_{12}(\alpha)|, \dots, |\tau_{r_21}(\alpha)|, |\tau_{r_22}(\alpha)|\}^{-1} \\ \geq \quad & \frac{1}{\sqrt{2}} \prod_{l=1}^{r_1} \max\{1, |\sigma_l(\alpha)|\}^{-1} \times \prod_{m=1}^{r_2} \max\{1, |\tau_m(\alpha)|\}^{-1} \\ \geq \quad & \frac{1}{\sqrt{2}} h(\alpha)^{-1}. \end{aligned}$$

Since the choice of $\alpha \in \mathfrak{U}_K(\mathcal{M})$ was arbitrary, we can pick such an α with $h(\alpha) = c_K(\mathcal{M})$, and so

$$\begin{aligned} & \max\{|\sigma_1(x_n)|, \dots, |\sigma_{r_1}(x_n)|, |\tau_{11}(x_n)|, |\tau_{12}(x_n)|, \dots, |\tau_{r_21}(x_n)|, |\tau_{r_22}(x_n)|\} \\ & \geq \frac{1}{\sqrt{2}} c_K(\mathcal{M})^{-1} \end{aligned} \tag{54}$$

for every $1 \leq n \leq N$, $\boldsymbol{x} \in \mathcal{M}$. Notice that $\Lambda_K(\mathcal{M}) := \sigma^N(\mathcal{M})$ is a lattice of rank Ld in $\mathbb{R}^{Nd}$, and a direct adaptation of Lemma 2 on p.115 of [17] implies that the determinant of $\Lambda_K(\mathcal{M})$ is

$$\det(\Lambda_K(\mathcal{M})) = 2^{-Lr_2} |\mathcal{D}_K(\mathcal{M})|^{\frac{L}{2}} = 2^{-Lr_2} |\mathcal{D}_K|^{\frac{L}{2}} \prod_{n=1}^{L} \mathbb{N}(\mathcal{I}_n), \tag{55}$$

where the last identity follows by (52) above. Combining (54) and (55) with Lemma 3.1, we see that the cardinality of the set $\Lambda_K(\mathcal{M}) \cap C_{Nd}(R)$ is

$$\geq \left(\frac{R}{2^{\frac{Lr_1-3}{2}} Ld \; c_K(\mathcal{M})^{Ld-1} |\mathcal{D}_K(\mathcal{M})|^{\frac{L}{2}}} - 1 \right) \left(\frac{2^{\frac{3}{2}} c_K(\mathcal{M}) R}{Ld} - 1 \right)^{Ld-1}. \tag{56}$$

For any $\alpha \in \mathfrak{U}_K(\mathcal{M})$, $\alpha\boldsymbol{x} \in O_K^N$ for every $\boldsymbol{x} \in \mathcal{M}$, and so

$$\prod_{v \in M(K), v \nmid \infty} \max\{1, |\alpha x_1|_v, \dots, |\alpha x_N|_v\} = 1,$$

and so

$$\begin{aligned} h(\alpha\boldsymbol{x})^d \quad = \quad & \prod_{m=1}^{r_1} \max\{1, |\sigma_m(\alpha x_1)|, \dots, |\sigma_m(\alpha x_N)|\} \times \\ & \times \prod_{n=1}^{r_2} \max\{1, \tau_{n1}(\alpha x_1)^2 + \tau_{n2}(\alpha x_1)^2, \dots, \tau_{n1}(\alpha x_N)^2 + \tau_{n2}(\alpha x_N)^2\} \\ \leq \quad & h(\alpha)^d |\sigma^N(\boldsymbol{x})|^d, \end{aligned}$$

where $|\boldsymbol{y}| = \max_{1 \leq n \leq Nd} |y_n|$ for each vector $\boldsymbol{y} \in \mathbb{R}^{Nd}$, and so

$$h(\boldsymbol{x}) = h(\alpha^{-1}(\alpha\boldsymbol{x})) \leq h(\alpha^{-1}) h(\alpha\boldsymbol{x}) \leq h(\alpha^{-1}) h(\alpha) |\sigma^N(\boldsymbol{x})|.$$

Notice that

$$z_K(\mathcal{M}) = \min\left\{ h(\alpha) h(\alpha^{-1}) : \alpha \in \mathfrak{U}_K(\mathcal{M}) \right\},$$

and choose α with $h(\alpha)h(\alpha^{-1}) = z_K(\mathcal{M})$, then

$$h(\boldsymbol{x}) \leq z_K(\mathcal{M}) |\sigma^N(\boldsymbol{x})| \tag{57}$$

for every $\boldsymbol{x} \in \mathcal{M}$. Therefore

$$\Lambda_K(\mathcal{M}) \cap C_{Nd}(R) \subseteq \sigma^N(S_{\mathcal{M}}(z_K(\mathcal{M})R)).$$

Combining this observation with (56) yields (1). □

We will now apply the bound of Theorem 1.1 to obtain a lower bound on the number of points of bounded height in a right D-vector space which are integral over a fixed order $\mathcal{O}$ in D.

Proof of Theorem 1.2. Define $Z_{\mathcal{O}} = Z \cap \mathcal{O}^N$ and let $\mathcal{M}_Z = [Z_{\mathcal{O}}] \subset K^{4N}$, which is an O_K-module such that $\mathcal{M}_Z \otimes_K K \cong K^{4L}$. Suppose that $\boldsymbol{y} \in \mathcal{M}_Z$ satisfies $h(\boldsymbol{y}) \leq R$, then $\boldsymbol{x} := [\boldsymbol{y}]^{-1} \in Z_{\mathcal{O}}$ and

$$h(\boldsymbol{x}) \leq 2s(\alpha,\beta)h(\boldsymbol{y}) \leq 2s(\alpha,\beta)R,$$

by Lemma 3.1 of [5]. Therefore

$$|S_{D,N}(Z,\mathcal{O},R)| \geq \left| \left\{ \boldsymbol{y} \in \mathcal{M}_Z : h(\boldsymbol{y}) \leq \frac{R}{2s(\alpha,\beta)} \right\} \right|. \tag{58}$$

Therefore we can apply Theorem 1.1 to $\mathcal{M}_Z$, obtaining a lower bound on the number of points of bounded height in $\mathcal{M}_Z$. To derive (3) from this bound, we need to relate invariants of $\mathcal{M}_Z$ which appear in (1) to corresponding invariants of $Z_{\mathcal{O}}$ and then apply the height comparison lemmas of [5].

Let $\Lambda_K(\mathcal{M}_Z) = \sigma^N(\mathcal{M}_Z)$, as in the proof of Theorem 1.1 above. Then Lemma 3.2 of [18] (also see the proof of Lemma 3.5 of [5]) combined with equation (55) above asserts that

$$|\mathcal{D}_K(\mathcal{M}_Z)|^{\frac{4L}{2}} = \det(\Lambda_K(\mathcal{M}_Z)) = \left(\sqrt{\mathbb{N}(\Delta_{\mathcal{O}})}/16\right)^L H^{\mathcal{O}}(Z)^{4d}. \tag{59}$$

Also notice that $aZ_{\mathcal{O}} \subseteq \mathcal{O}_D^N$ for some $a \in K$ if and only $a\mathcal{M}_Z \subseteq O_K^{4N}$, which means that $c_{\mathcal{O}}(Z) = c_K(\mathcal{M}_Z)$ and $z_{\mathcal{O}}(Z) = z_K(\mathcal{M}_Z)$, where $c_K(\mathcal{M}_Z)$ and $z_K(\mathcal{M}_Z)$ are defined as in (12) and (13) above. Now combining (1) with (58) and (59), we see that $|S_{D,N}(Z,\mathcal{O},R)| \geq$

$$\begin{aligned} &\geq \left(\frac{R}{\mathcal{E}_3(D,\mathcal{O},Z,d,L)H^{\mathcal{O}}(Z)^{4d}} - 1 \right) (\mathcal{E}_4(D,\mathcal{O},Z,d,L)R - 1)^{4Ld-1} \\ &= \mathcal{E}_3'(D,\mathcal{O},Z,d,L)\frac{R^{4Ld}}{H^{\mathcal{O}}(Z)^{4d}} + O(R^{4Ld-1}), \end{aligned} \tag{60}$$

where

$$\mathcal{E}_3'(D,\mathcal{O},Z,d,L) = \left(2^{4L(2d-1)}(Ld\ s(\alpha,\beta)z_{\mathcal{O}}(Z))^{4Ld}\mathbb{N}(\Delta_{\mathcal{O}})^{\frac{L}{2}} \right)^{-1}.$$

This finishes the proof. □

Finally, we apply the counting estimate of [21] over number fields to prove Theorem 1.3.

Proof of Theorem 1.3. Since $[\ ] : D \to K^4$ is a vector space isomorphism,

$$|S_{D,N}(R)| = |[S_{D,N}(R)]|.$$

Now Lemma 3.1 (or, more precisely, inequality (18)) of [5] guarantee that for every $\boldsymbol{x} \in D^N$,

$$t(\alpha,\beta)h([\boldsymbol{x}]) \leq h(\boldsymbol{x}) \leq s(\alpha,\beta)h([\boldsymbol{x}]), \tag{61}$$

and hence

$$[S_{D,N}(R)] \subseteq S_{K,4N}(R/t(\alpha,\beta)) := \left\{ \boldsymbol{y} \in K^{4N} : h(\boldsymbol{y}) \leq \frac{R}{t(\alpha,\beta)} \right\}.$$

An upper bound on cardinality of the set $S_{K,4N}(R/t(\alpha,\beta))$ follows from Theorem 4 of [21]:

$$|S_{K,4N}\left(R/t(\alpha,\beta)\right)| \leq (1088 d \log d)^{4N} \left(\frac{R}{t(\alpha,\beta)} \right)^{(4N+1)d}. \tag{62}$$

□

Remark 3.1. On the other hand, (61) implies that

$$S_{K,4N}(R/s(\alpha,\beta)) := \left\{ \boldsymbol{y} \in K^{4N} : h(\boldsymbol{y}) \leq \frac{R}{s(\alpha,\beta)} \right\} \subseteq [S_{D,N}(R)].$$

Equation (1.5) of [26] implies that

$$|S_{K,4N}\left(R/s(\alpha,\beta)\right)| \gg_{K,N} \left(\frac{R}{s(\alpha,\beta)} \right)^{4N+1}. \tag{63}$$

Then (5) follows by combining (62) with (63). In fact, as long as we have *any* upper or lower bounds on the number of points of bounded height over K, we can "transfer" them to obtain analogous bounds for the number of points of bounded height over D.

Appendix A. Further counting estimates over global fields

Here we show some further applications of Lemma 3.1, obtaining estimates on the number of S-units of bounded height in an arbitrary number field as well as number of rational functions of bounded height supported on a given curve over a fixed finite field.

We start with the number field situation. Let K be any number field, and write S_∞ for the set of all archimedean places of K. Let S_1 be a finite (possibly empty) set of non-archimedean places of K, and let $S = S_\infty \cup S_1$. The group of S-units of K is

$$O_S^* = \{a \in K : |a|_v = 1 \ \forall \ v \notin S\}.$$

Define the logarithmic S-height function on $K^\times$ by

$$H_S(a) = \max_{v \in S} \{ \left|\log |a|_v\right|, \left|\log |a^{-1}|_v\right| \}, \tag{64}$$

i.e., $H_S(a)$ measures the extent of divisibility of numerator and denominator of a at the places in S, and let

$$H_{S,K} = \min\{H_S(a) : a \in O_S^* \setminus \mu_K\} > 0, \tag{65}$$

where μ_K is the group of roots of unity in K. Let $d = [K : \mathbb{Q}]$, h_K be the class number and R_K the regulator of K.

We employ here the standard logarithmic lattice construction used in the proof of Dirichlet's Unit Theorem (see, for instance, p.104 of [17] and pp.575–578 of [27]). Let $n = |S| = d + t$, where $t = |S_1|$, and define the map $\varphi_S : O_S^* \to \mathbb{R}^n$ by

$$\varphi_S(a) = (\log |a|_v)_{v \in S}.$$

Then $\operatorname{Ker}\varphi_S = \mu_K$ and $L_S := \varphi(O_S^*)$ is a lattice of rank $(n-1)$ in $\mathbb{R}^n$, which is contained in the hyperplane $V = \{\boldsymbol{x} \in \mathbb{R}^n : \sum_{m=1}^n x_m = 0\}$, and so L_S is a lattice of full rank in V. The S-regulator of K is defined to be

$$R_{S,K} := \det L_S,$$

which is just R_K if $S_1 = \emptyset$. If $S_1 \neq \emptyset$, let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be the prime ideals in K corresponding to the places in S_1, and let P be the largest rational prime lying below these prime ideals. In Lemma 3 of [2], the following bounds on $R_{S,K}$ are produced (see also Lemma 3 of [3] and Proposition 5.4.7 of [27]):

$$R_{S,K} \leq R_K h_K \prod_{m=1}^{t} \log \mathbb{N}(\mathfrak{p}_m) \leq R_K h_K (d \log^* P)^t \tag{66}$$

and

$$R_{S,K} \geq R_K \prod_{m=1}^{t} \log \mathbb{N}(\mathfrak{p}_m) \geq 0.2052 (\log 2)^d (\log^* P), \tag{67}$$

where $\log^* P = \max\{\log P, 1\}$. Observe also that for any $\boldsymbol{x} \in L_S \setminus \{\boldsymbol{0}\}$,

$$|\boldsymbol{x}| = \max_{1 \leq m \leq n} |x_m| \geq H_{S,K} > 0. \tag{68}$$

We are now ready to state and prove our estimate.

Lemma A.1. *Let $B \in \mathbb{R}_{>0}$ and let*

$$O_S^*(B) = \{a \in O_S^* : H_S(a) \leq B\}.$$

Then, with notation as above,

$$\omega_K \left(\frac{2BH_{S,K}^{n-2}}{(n-1)R_{S,K}} - 1 \right) \left(\frac{2B}{(n-1)H_{S,K}} - 1 \right)^{n-2} \leq |O_S^*(B)| \leq \omega_K \left(\frac{2B}{H_{S,K}} + 1 \right)^{n-1}, \tag{69}$$

where $\omega_K = |\mu_K|$; the lower bound of (69) *holds for $B \geq \frac{n-1}{2} \max \left\{ \frac{R_{S,K}}{H_{S,K}^{n-2}}, H_{S,K} \right\}$.*

Proof. Given a positive real number B, let $C_n(B)$ be as in (43). It is then an easy observation that $O_S^*(B) = \varphi_S^{-1}(C_n(B) \cap L_S)$. Notice that for each $\boldsymbol{x} \in L_S$, $|\varphi_S^{-1}(\boldsymbol{x})| = \omega_K$, therefore

$$|O_S^*(B)| = \omega_K \; |C_n(B) \cap L_S|, \tag{70}$$

and (69) follows by combining (68) and (70) with Lemma 3.1. □

Remark A.1. Inequalities (66) and (67) can now be used to make estimates of Lemma A.1 more explicit, if necessary. Comparable asymptotic estimates on the number of units and S-units of bounded height (with somewhat different heights used) were previously obtained in [8] (see also Theorem 5.2 on p.70 of [16]) and [9] (Lemma 1). In contrast, our estimates are explicit upper and lower bounds.

Next we discuss an analogous construction over function fields, following pp.578–581 of [27]. Let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. Let X be a smooth projective curve defined over $\mathbb{F}_q$, and let $K = \mathbb{F}_q(X)$ be the field of rational functions on X over $\mathbb{F}_q$. For every $f \in K^\times$, we write $\operatorname{Supp}(f)$ for the support of f, i.e., the set of all points at which X has zeros or poles. Let $X(\mathbb{F}_q)$ be the set of points of X which are rational over $\mathbb{F}_q$. Let $\mathcal{P} \subseteq X(\mathbb{F}_q)$, and define

$$O^*_{\mathcal{P}} = \{f \in K^\times : \operatorname{Supp}(f) \subseteq \mathcal{P}\}$$

to be the group of all rational functions in K supported on $\mathcal{P}$. Let $n = |\mathcal{P}|$, say $\mathcal{P} = \{p_1, \dots, p_n\}$, and write $a_m(f) \in \mathbb{Z}$ for the order of zero or pole that $f \in K^\times$ has at $p_m \in \mathcal{P}$. We can define the $\mathcal{P}$-height on $K^\times$ by

$$H_{\mathcal{P}}(f) = \max_{1 \le m \le n} |a_m(f)|, \tag{71}$$

which is a direct function-field analogue of the S-height function defined in (64) above. The principal divisor of any $f \in O^*_{\mathcal{P}}$ is

$$\operatorname{div}(f) = a_1(f)p_1 + \cdots + a_n(f)p_n,$$

so that $\sum_{m=1}^n a_m(f) = 0$. We can then define a map $\varphi_{\mathcal{P}} : O^*_{\mathcal{P}} \to \mathbb{R}^n$ by

$$\varphi_{\mathcal{P}}(f) = (a_1(f), \dots, a_n(f)),$$

and so $\operatorname{Ker}(\varphi_{\mathcal{P}}) = \mathbb{F}_q^\times$ and $L_{\mathcal{P}} := \varphi_{\mathcal{P}}(O^*_{\mathcal{P}})$ is a finite-index sublattice of the root lattice

$$A_{n-1} = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \sum_{m=1}^n x_m = 0 \right\},$$

which has determinant $= \sqrt{n}$. We need some more notation to give a formula for the determinant of $L_{\mathcal{P}}$, following [27]. Let $\operatorname{Div}^0(X)$ be the group of divisors of degree 0 on X and $P(X)$ the subgroup of principal divisors, then $J(X) = \operatorname{Div}^0(X)/P(X)$ is the Jacobian of X, and we write $J_X(\mathbb{F}_q)$ for the set of $\mathbb{F}_q$-rational points on the Jacobian. Let also $\operatorname{Div}^0_{\mathcal{P}}(X) \subset \operatorname{Div}^0(X)$ be the subgroup of degree 0 divisors supported on $\mathcal{P}$ and $P_{\mathcal{P}}(X) = \operatorname{Div}^0_{\mathcal{P}}(X) \cap P(X)$. Define the restricted $\mathcal{P}$-Jacobian to be $J_{X,\mathcal{P}} := \operatorname{Div}^0_{\mathcal{P}}(X)/P_{\mathcal{P}}(X)$, then Theorem 5.4.9 of [27] states that

$$\det(L_{\mathcal{P}}) = \det(A_{n-1})|A_{n-1} : L_{\mathcal{P}}| = \sqrt{n}\,|J_{X,\mathcal{P}}|, \tag{72}$$

and so

$$\sqrt{n} \le \det(L_{\mathcal{P}}) \le \sqrt{n}|J_X(\mathbb{F}_q)| \le \sqrt{n}\left(1 + q + \frac{|X(\mathbb{F}_q)| - q - 1}{g}\right)^g, \tag{73}$$

where g is the genus of X. Further, the same theorem guarantees that for every $\boldsymbol{x} \in L_{\mathcal{P}} \setminus \{\boldsymbol{0}\}$,

$$|\boldsymbol{x}| \ge \max\left\{1, \frac{1}{n}\sqrt{\frac{2|X(\mathbb{F}_q)|}{q+1}}\right\}. \tag{74}$$

We are now ready to state and prove the function-field analogue of Lemma A.1.

Lemma A.2. *Let $B \in \mathbb{R}_{>0}$ and let*

$$O^*_{\mathcal{P}}(B) = \{f \in O^*_{\mathcal{P}} : H_{\mathcal{P}}(f) \le B\}.$$

Then, with notation as above,

$$\begin{aligned} &(q-1)\left(\frac{2B}{(n-1)\sqrt{n}\,|J_{X,\mathcal{P}}|} - 1\right)\left(\frac{2B}{(n-1)} - 1\right)^{n-2} \\ &\le |O^*_{\mathcal{P}}(B)| \le (q-1)\left(\frac{2B}{|J_{X,\mathcal{P}}|} + 1\right)(2B+1)^{n-2} \end{aligned} \tag{75}$$

where the lower bound of (69) *holds for* $B \geq \frac{(n-1)\sqrt{n}|J_{X,\mathcal{P}}|}{2}$.

Proof. Given a positive real number B, let $C_n(B)$ be as in (43). It is then an easy observation that $O^*_{\mathcal{P}}(B) = \varphi_{\mathcal{P}}^{-1}(C_n(B) \cap L_{\mathcal{P}})$. Notice that for each $\boldsymbol{x} \in L_{\mathcal{P}}$, $|\varphi_{\mathcal{P}}^{-1}(\boldsymbol{x})| = q-1$, therefore

$$|O^*_{\mathcal{P}}(B)| = (q-1)\ |C_n(B) \cap L_{\mathcal{P}}|, \tag{76}$$

and (75) follows by combining (74) and (76) with Lemma 3.1. □

Remark A.2. Formulas (72) and (73) can be used to make estimates of Lemma A.2 more explicit, if necessary.

Appendix B. Points of small height

Classical Diophantine results on existence of points of bounded height on linear and quadratic spaces, such as Siegel's lemma and Cassels' theorem, have enjoyed much attention, including a number of papers by various authors in the recent years. In particular, some of the recent work has been devoted to extending these results to the non-commutative situation (see [18], [19], [20], [30], [5], and others). On the other hand, the non-commutative situation presents various obstacles that do not exist over fields, which makes it difficult to push the theory much further even over quaternion algebras. It is however possible to "transfer" some of the existent results in the context of number fields to quaternion algebras, using appropriate height comparison inequalities. Here we demonstrate this transfer principle on several examples in the hope that it can also prove to be useful in a variety of other situations. As above, let K be a totally real number field of degree d over $\mathbb{Q}$, and let $D = \left(\frac{\alpha,\beta}{K}\right)$ be a positive definite quaternion algebra over K. Suppose we want to prove the existence of a nonzero point $\boldsymbol{x} \in D^N$ of explicitly bounded height which would satisfy a certain set of algebraic conditions. We suggest the use of the following basic method:

Suppose we know that there exists a point $\boldsymbol{y} \in K^{4N}$ of bounded height such that $[\boldsymbol{y}]^{-1} \in D^N$ satisfies the desired algebraic conditions. Use the height comparison lemmas developed in Section 3 of [5] *to produce the necessary bounds on the height of $\boldsymbol{x} := [\boldsymbol{y}]^{-1} \in D^N$.*

In other words, the results on points of bounded height over D can be obtained by "transferring" the analogous results over K with the use of height comparison inequalities. The first instance of this method at work has been demonstrated in [5], where a result on existence of a small-height basis for a hermitian space over D consisting of zeros of the corresponding quadratic form has been obtained by the transfer of an analogous result over K, due to Vaaler [29]. We also used this same method above to derive Theorem 1.2 from Theorem 1.1. Here we take this principle further, proving the analogues of some recent results of [6] and [13].

Theorem B.1. *Let $D = \left(\frac{\alpha,\beta}{K}\right)$ be a positive definite quaternion algebra over a totally real number field K, where α, β are totally negative algebraic integers in K. Let $\mathcal{O}$ be an order in D. Let $N \geq 2$ be an integer, and let $Z \subseteq D^N$ be an L-dimensional right D-subspace, $1 \leq L \leq N$. Let $U_1, \dots, U_M \subset D^N$ be proper right D-subspaces, let*

$$G_1(\boldsymbol{X}, \boldsymbol{Y}), \dots, G_J(\boldsymbol{X}, \boldsymbol{Y}) \in D[\boldsymbol{X}, \boldsymbol{Y}]$$

be a hermitian forms in $2N$ variables, and let

$$W_l = \{\boldsymbol{x} \in D^N : G_l(\boldsymbol{x}) := G_l(\boldsymbol{x}, \boldsymbol{x}) = 0\} \tag{77}$$

for each $1 \leq l \leq J$. Suppose that $Z \not\subseteq \left(\bigcup_{m=1}^{M} U_m\right) \left(\bigcup_{l=1}^{J} W_l\right)$. Then there exists a basis

$$\boldsymbol{y}_1, \dots, \boldsymbol{y}_L \in Z \setminus \left(\left(\bigcup_{m=1}^{M} U_m \right) \left(\bigcup_{l=1}^{J} W_l \right) \right) \tag{78}$$

for Z over D, such that

$$\begin{aligned} h(\boldsymbol{y}_1) &\leq h(\boldsymbol{y}_2) \leq \cdots \leq h(\boldsymbol{y}_L) \\ &\leq 4L(M+2J+1)^{\frac{1}{d}} |\mathcal{D}_K|^{\frac{L+1}{2d}} s(\alpha,\beta) \mathfrak{M}(\mathcal{O})^{4(N-L)} H^{\mathcal{O}}(Z)^4. \end{aligned} \tag{79}$$

Proof. For an L-dimensional right D-subspace $Z \subseteq D^N$, $[Z]$ is a $4L$-dimensional subspace of K^{4N}. Recall from the definitions in Section 2 that for a hermitian form $F(\boldsymbol{X}, \boldsymbol{Y}) \in D[\boldsymbol{X}, \boldsymbol{Y}]$ in $2N$ variables, its associated trace form

$$Q_F([\boldsymbol{X}]) = \operatorname{Tr}(F(\boldsymbol{X})) = F(\boldsymbol{X}) + \overline{F(\boldsymbol{X})}, \tag{80}$$

which is a quadratic form in $4N$ variables over K, and $F(\boldsymbol{x}) = 0$ for some $\boldsymbol{x} \in D^N$ if and only if $Q_F([\boldsymbol{x}]) = 0$. Then for each W_l as in (77), define

$$[W_l] := \{[\boldsymbol{y}] \in K^{4N} : \boldsymbol{y} \in D^N,\ G_l(\boldsymbol{y}) = 0\} = \{\boldsymbol{x} \in K^{4N} : Q_{G_l}(\boldsymbol{x}) = 0\}.$$

Now Theorem A.1 of [6] guarantees that there exists a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{4L}$ for $[Z]$ over K such that

$$\boldsymbol{x}_1, \dots, \boldsymbol{x}_{4L} \in [Z] \setminus \left(\left(\bigcup_{m=1}^{M} [U_m] \right) \left(\bigcup_{l=1}^{J} [W_l] \right) \right)$$

and

$$H(\boldsymbol{x}_1) \leq H(\boldsymbol{x}_2) \leq \cdots \leq H(\boldsymbol{x}_{4L}),\ h(\boldsymbol{x}_1) \leq h(\boldsymbol{x}_2) \leq \cdots \leq h(\boldsymbol{x}_{4L}), \tag{81}$$

and for each $1 \leq n \leq 4L$,

$$H(\boldsymbol{x}_n) \leq h(\boldsymbol{x}_n) \leq 2L(M+2J+1)^{\frac{1}{d}} |\mathcal{D}_K|^{\frac{L+1}{2d}} H([Z]). \tag{82}$$

Moreover, these vectors can be taken with coordinates in O_K. Notice that there exist

$$1 = l_1 < l_2 < \cdots < l_L < 4L$$

such that $[\boldsymbol{x}_{l_1}]^{-1}, \dots, [\boldsymbol{x}_{l_L}]^{-1}$ is a basis for Z as a right D-vector space, which satisfies (78); we will write $\boldsymbol{y}_n = [\boldsymbol{x}_{l_n}]^{-1}$ for each $1 \leq n \leq L$. Notice that in fact $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L \in \mathcal{O}_D^N$, where $\mathcal{O}_D$ is defined in (36). Combining Lemmas 3.4 and 3.5 of [5], we see that

$$H([Z]) = H^{\mathcal{O}_D}(Z)^4 \leq \mathfrak{M}(\mathcal{O})^{4(N-L)} H^{\mathcal{O}}(Z)^4, \tag{83}$$

while Lemma 3.1 of [5] implies that for each $1 \leq n \leq 4L$

$$h([\boldsymbol{x}_n]^{-1}) \leq 2s(\alpha,\beta) h(\boldsymbol{x}_n). \tag{84}$$

Combining (82) with (83) and (84) yields

$$h(\boldsymbol{y}_n) \leq 4L(M+2J+1)^{\frac{1}{d}} |\mathcal{D}_K|^{\frac{L+1}{2d}} s(\alpha,\beta) \mathfrak{M}(\mathcal{O})^{4(N-L)} H^{\mathcal{O}}(Z)^4$$

for each $1 \leq n \leq L$. Arranging $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$ in the non-decreasing height order yields (79) and completes the proof of Theorem B.1. □

Remark B.1. Theorem B.1 is a version of Theorem A.1 of [6] over a quaternion algebra. It constitutes a non-commutative version of Sielgel's lemma missing a union of varieties and hence generalizes a non-commutative version of Siegel's lemma first established by Liebendörfer in [18].

Theorem B.2. *Let all the notation be as in Theorem B.1, and let* $F(\boldsymbol{X},\boldsymbol{Y}) \in D[\boldsymbol{X},\boldsymbol{Y}]$ *be a hermitian form in* $2N$ *variables. Suppose that there exists a point* $\boldsymbol{y} \in Z \setminus \left(\left(\bigcup_{m=1}^{M} U_m \right) \left(\bigcup_{l=1}^{J} W_l \right) \right)$ *such that* $F(\boldsymbol{y}) := F(\boldsymbol{y},\boldsymbol{y}) = 0$, *then there exists such a point with*

$$h(\boldsymbol{y}) \leq \mathcal{A}_{K,\mathcal{O}}(L,M,J,\alpha,\beta) H_{\inf}(F)^{\frac{9L+11}{2}} H^{\mathcal{O}}(Z)^{4(9L+12)}, \tag{85}$$

where the constant $\mathcal{A}_{K,\mathcal{O}}(L,M,J,\alpha,\beta)$ *given by* (42) *above. Furthermore, there exists a point* $\boldsymbol{z} \in D^N \setminus \left(\bigcup_{m=1}^{M} U_m \right)$ *such that* $F(\boldsymbol{z}) = 0$ *and*

$$h(\boldsymbol{z}) \ll_{K,N,M} 2s(\alpha,\beta) \left(\frac{2s(\alpha,\beta)^2}{t(\alpha,\beta)} H_{\inf}(F) \right)^{\frac{N+1}{2}}. \tag{86}$$

Proof. Notice that

$$[\boldsymbol{y}] \in [Z] \setminus \left(\left(\bigcup_{m=1}^{M} [U_m] \right) \left(\bigcup_{l=1}^{J} [W_l] \right) \right)$$

and $Q_F([\boldsymbol{y}]) = 0$. Let ω be the Witt index and λ the dimension of the radical of the quadratic space $([Z], Q_F)$ over K, so that a maximal totally isotropic subspace of $([Z], Q_F)$ has dimension $\mu := \omega + \lambda$, then Theorem 1.1 of [6] guarantees that there exist μ linearly independent vectors

$$\boldsymbol{x}_1, \dots, \boldsymbol{x}_\mu \in [Z] \setminus \left(\left(\bigcup_{m=1}^{M} [U_m] \right) \left(\bigcup_{l=1}^{J} [W_l] \right) \right)$$

such that for each $1 \leq n \leq \mu$

$$h(\boldsymbol{x}_n) \leq T_K(L, M+2J+1) H(Q_F)^{\frac{9L+11}{2}} H([Z])^{9L+12}, \tag{87}$$

where $T_K(L,M)$ is a dimensional field constant, given by equation (43) of [6]; its technical definition is somewhat complicated, so we do not present here in the interest of the brevity of exposition. Now, combining (87) with (83), (84) and Lemma 3.2 of [5], we obtain

$$h([\boldsymbol{x}_n]^{-1}) \leq \mathcal{A}_{K,\mathcal{O}}(L,M,J,\alpha,\beta) H_{\inf}(F)^{\frac{9L+11}{2}} H^{\mathcal{O}}(Z)^{4(9L+12)} \tag{88}$$

for each $1 \leq n \leq \mu$. Since

$$[\boldsymbol{x}_1]^{-1}, \dots, [\boldsymbol{x}_\mu]^{-1} \in Z \setminus \left(\left(\bigcup_{m=1}^{M} U_m \right) \left(\bigcup_{l=1}^{J} W_l \right) \right),$$

and $\mu \geq 1$, we can take, for instance, $\boldsymbol{y} = [\boldsymbol{x}_1]^{-1}$, and obtain (85).

Finally, to obtain (86), we can combine Theorem of [7] with (84) and Lemma 3.1 of [5] in the same manner as above. This completes the proof of Theorem B.2. □

Remark B.2. Inequality (85) of Theorem B.2 is a version of Theorem 1.1 of [6] and (86) is a version of the main theorem of [7] (see also [10]), both over a quaternion algebra. The bound of (86) demonstrates better dependence on $H_{\inf}(F)$ when $Z = D^N$, although it only provides a point missing a collection of linear subspaces.

One can continue applying our "transfer method" in the similar manner to obtain analogues of results on Siegel's lemma outside of linear subspaces with an additional dependence on the height of these subspaces (see [12], [14]).

References

[1] F. Barroero. Algebraic integers of fixed degree and bounded height. *preprint; arXiv:1305.0482v2.*

[2] Y. Bugeaud. Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107(2):187–219, 1997.

[3] Y. Bugeaud and K. Győry. Bounds for the solutions of unit equations. *Acta Arith.*, 74(1):67–80, 1996.

[4] J. W. S. Cassels. *An Introduction to the Geometry of Numbers.* Springer, Berlin, 1959.

[5] W. K. Chan and L. Fukshansky. Small zeros of hermitian forms over quaternion algebras. *Acta Arith.*, 142(3):251–266, 2010.

[6] W. K. Chan, L. Fukshansky, and G. Henshaw. Small zeros of quadratic forms missing a union of varieties. preprint, `http://math.cmc.edu/lenny/papers/quad_zero-1.pdf`, 2012.

[7] R. Dietmann. Small zeros of quadratic forms avoiding a finite number of prescribed hyperplanes. *Canad. Math. Bull.*, 52(1):63–65, 2009.

[8] G. R. Everest and J. H. Loxton. Counting algebraic units with bounded height. *J. Number Theory*, 44(2):222–227, 1993.

[9] C. Fuchs, R. Tichy, and V. Ziegler. On quantitative aspects of the unit sum number problem. *Arch. Math. (Basel)*, 93(3):259–268, 2009.

[10] L. Fukshansky. Small zeros of quadratic forms with linear conditions. *J. Number Theory*, 108(1):29–43, 2004.

[11] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatshefte für Mathematik*, 147(1):25–41, 2006.

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

[13] L. Fukshansky. Algebraic points of small height missing a union of varieties. *J. Number Theory*, 130(10):2099–2118, 2010.

[14] E. Gaudron. Géométrie des nombres adélique et lemmes de Siegel généralisés. *Manuscripta Math.*, 130(2):159182, 2009.

[15] P. Gritzmann and J. M. Wills. Lattice points. In *Handbook of Convex Geometry, Vol. A, B*, pages 765–797. North-Holland, Amsterdam, 1993.

[16] S. Lang. *Fundamentals of Diophantine geometry.* Springer-Verlag, 1983.

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

[18] C. Liebendörfer. Linear equations and heights over division algebras. *J. Number Theory*, 105(1):101–133, 2004.

[19] C. Liebendörfer. Heights and determinants over quaternion algebras. *Comm. Algebra*, 33(10):3699–3717, 2005.

[20] C. Liebendörfer and G. Rémond. Duality of heights over quaternion algebras. *Monatsh. Math.*, 145(1):61–72, 2005.

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

[22] D. Masser and J. D. Vaaler. Counting algebraic numbers with large height. II. *Trans. Amer. Math. Soc.*, 359(1):427–445, 2007.

[23] D. G. Northcott. An inequality in the theory of arithmetic on algebraic varieties. *Proc. Camb. Phil. Soc.*, 45:502–509 and 510–518, 1949.

[24] R. S. Pierce. *Associative Algebras.* Springer-Verlag, 1982.

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

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

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

[28] J. D. Vaaler. Small zeros of quadratic forms over number fields. *Trans. Amer. Math. Soc.*, 302(1):281–296, 1987.

[29] J. D. Vaaler. Small zeros of quadratic forms over number fields, II. *Trans. Amer. Math. Soc.*, 313(2):671–686, 1989.

[30] T. Watanabe. Minkowski's second theorem over a simple algebra. *Monatsh. Math.*, 149(2):155–172, 2006.

[31] M. Widmer. Integral points of fixed degree and bounded height. *preprint*.

[32] M. Widmer. Counting points of fixed degree and bounded height. *Acta Arith.*, 140(2):145–168, 2009.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
E-mail address: lenny@cmc.edu

Department of Mathematics, California State University at Channel Islands, One University Drive, Camarillo, CA 93012
E-mail address: glenn.henshaw@csuci.edu