1-1-2008

Small Zeros of Quadratic Forms over the Algebraic Closure of Q

Lenny Fukshansky
Claremont McKenna College

SMALL ZEROS OF QUADRATIC FORMS OVER $\overline{\mathbb{Q}}$

LENNY FUKSHANSKY

ABSTRACT. Let $N \geq 2$ be an integer, F a quadratic form in N variables over $\overline{\mathbb{Q}}$, and $Z \subseteq \overline{\mathbb{Q}}^N$ an L-dimensional subspace, $1 \leq L \leq N$. We prove the existence of a small-height maximal totally isotropic subspace of the bilinear space (Z, F). This provides an analogue over $\overline{\mathbb{Q}}$ of a well-known theorem of Vaaler proved over number fields. We use our result to prove an effective version of Witt decomposition for a bilinear space over $\overline{\mathbb{Q}}$. We also include some related effective results on orthogonal decomposition and structure of isometries for a bilinear space over $\overline{\mathbb{Q}}$. This extends previous results of the author over number fields. All bounds on height are explicit.

1. INTRODUCTION

Let

$$F(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i Y_j \tag{1}$$

be a symmetric bilinear form in $N \geq 2$ variables with coefficients in a number field K. We will also write

$$F(\boldsymbol{X}) = F(\boldsymbol{X}, \boldsymbol{X})$$

for the associated quadratic form and $F = (f_{ij})_{1 \leq i,j \leq N}$ for the symmetric $N \times N$ coefficient matrix of F. We say that the quadratic form F is *isotropic* over K if it has a non-trivial zero with coordinates in K. A classical theorem of Cassels [3] states that if $K = \mathbb{Q}$ and F is isotropic over $\mathbb{Q}$, then there exists $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Q}^N$ such that $F(\boldsymbol{x}) = 0$ and

$$H(\boldsymbol{x}) \ll_N \mathcal{H}(F)^{\frac{N-1}{2}}, \tag{2}$$

for appropriate notions of heights H and $\mathcal{H}$ to be defined below and an explicit constant. Cassels' theorem has been generalized to any number field K by Raghavan [9]; the bound remained the same as in (2), except that the explicit constant in the upper bound now depends on the number field as well.

Further generalizations and extensions of Cassels' theorem have been considered by a number of authors. A few words of notation are required before we can review some of them. Let $Z \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$, then F is defined on Z, and we write (Z, F) for the corresponding symmetric bilinear space. A subspace W of (Z, F) is called totally isotropic if for all $\boldsymbol{x}, \boldsymbol{y} \in W$, $F(\boldsymbol{x}, \boldsymbol{y}) = 0$. All maximal totally isotropic subspaces of (Z, F) have the same dimension. It is called the Witt index of (Z, F) and we denote it by k. A subspace U of (Z, F) is called regular if for each $\mathbf{0} \neq \boldsymbol{x} \in U$ there exists $\boldsymbol{y} \in U$ so that $F(\boldsymbol{x}, \boldsymbol{y}) \neq 0$. For

1991 *Mathematics Subject Classification.* Primary 11E12, 11G50, 11H55, 11D09.
Key words and phrases. quadratic and bilinear forms, heights.

each subspace U of (Z,F) we define $U^{\perp} = \{\boldsymbol{x} \in Z : F(\boldsymbol{x},\boldsymbol{y}) = 0 \ \forall \ \boldsymbol{y} \in U\}$. If two subspaces U_1 and U_2 of (Z,F) are orthogonal, we write $U_1 \perp U_2$ for their orthogonal sum. If U is a regular subspace of (Z,F), then $Z = U \perp U^{\perp}$ and $U \cap U^{\perp} = \{\boldsymbol{0}\}$.

If F is defined over $\mathbb{Q}$, and the bilinear space $(\mathbb{Q}^N, F)$ has nonzero Witt index, then Schlickewei [13] (see also Schmidt and Schlickewei [14]) proved the existence of a maximal totally isotropic subspace of $(\mathbb{Q}^N, F)$ of bounded height. This result has been generalized to an arbitrary number field K by Vaaler [16]. In particular, Vaaler proved that if an L-dimensional bilinear space (Z,F) over K has Witt index $k \geq 1$, then there exists a maximal totally isotropic subspace V of (Z,F) such that

$$H(V) \ll_{K,L,k} \mathcal{H}(F)^{\frac{L-k}{2}} H(Z). \tag{3}$$

The main goal of this paper is to prove a theorem analogous to Vaaler's over $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. We use a new method to prove such a result, since Vaaler's argument relies on the fact that the number of subspaces of given dimension and explicitly bounded height over a number field is finite, which is no longer true over $\overline{\mathbb{Q}}$. From now on let (Z,F) be an L-dimensional regular bilinear space over $\overline{\mathbb{Q}}$, $1 \leq L \leq N$. It is a well known fact (see for instance [11]) that Witt index of (Z,F) in this case is $\left[\frac{L}{2}\right]$. We can now state the main result of this paper.

Theorem 1.1. *Let F be a quadratic form in N variables as above. Let $Z \subseteq \overline{\mathbb{Q}}^N$ be an L-dimensional subspace, $1 \leq L \leq N$, so that the quadratic space (Z,F) is regular. Let $k = \left[\frac{L}{2}\right]$ be the Witt index of (Z,F). There exists a maximal totally isotropic subspace V of (Z,F) with*

$$H(V) \leq 24 \times 2^{\frac{k-1}{4}} 3^{\frac{k^2(k+1)^2}{4}} \mathcal{H}(F)^{\frac{k^2}{2}} H(Z)^{\frac{k^2+k+2}{2k}}, \tag{4}$$

if L is even, and

$$H(V) \leq 3^{2k(k+1)^3} \mathcal{H}(F)^{k^2} H(Z)^{\frac{4k}{3}}, \tag{5}$$

if L is odd.

Of course given an L-dimensional regular bilinear space (Z,F) which is defined over a number field K, it is possible to find an extension E of K large enough so that (Z,F) has Witt index $k = \left[\frac{L}{2}\right]$ over E, and then apply Vaaler's theorem with bound (3) to it. The constant in (3), however, will depend on the discriminant of E, which can be quite large. In this case Theorem 1.1 can produce a stronger bound than (3).

Theorem 1.1 is a statement in the general spirit of "absolute" results, in particular it parallels the development of the problem about small-height solutions for a system of homogeneous linear equations, ordinarily known under the name of Siegel's lemma. A version of Siegel's lemma over a number field K asserting the existence of a small-height basis for a subspace of K^N has been proved by Bombieri and Vaaler [1]. Roy and Thunder [10] proved a version of Siegel's lemma over $\overline{\mathbb{Q}}$. More specifically, here is a slightly simplified formulation of the "absolute" Siegel's lemma.

Theorem 1.2 ([10])**.** *Let $Z \subseteq \overline{\mathbb{Q}}^N$ be an L-dimensional subspace, $1 \leq L < N$. Then there exists a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ for Z over $\overline{\mathbb{Q}}$ such that*

$$\prod_{i=1}^{L} H(\boldsymbol{x}_i) \leq \prod_{i=1}^{L} h(\boldsymbol{x}_i) \leq 3^{\frac{L(L-1)}{2}} H(Z). \tag{6}$$

In (6), h stand for inhomogeneous height on vectors to be defined below. Notice that an important common feature distinguishing Theorem 1.1 and Theorem 1.2 from their number field analogues is that the constants in the upper bounds bear no dependence on any number field.

The proof of Theorem 1.1 is split into two cases: L is even and L is odd. The argument in the odd case is essentially a reduction to the even case. In the even case we argue by induction on $k = L/2$, the Witt index. We apply the induction hypothesis to the bilinear space (Z_1, F), where Z_1 is a codimension two subspace of Z of bounded height guaranteed by the "absolute" Siegel's lemma of Roy and Thunder [10], and hence has Witt index $k-1$. This way we obtain a small-height maximal totally isotropic subspace U of (Z_1, F) guaranteed by the induction hypothesis, and consider its orthogonal dual W in Z. We then prove that the intersection of the projective space over W with the quadratic projective variety defined by F over $\overline{\mathbb{Q}}$ is a projective intersection cycle whose affine support is a union of two maximal totally isotropic subspaces of (Z, F). Product of their heights can be bounded using a version of arithmetic Bezout's theorem due to Bost, Gillet, and Soulé [2].

This paper is structured as follows. In section 2 we set the notation and define the height functions. In section 3 we review a few technical lemmas on properties of heights. In section 4 we prove Theorem 1.1. In section 5 we use Theorem 1.1 to prove an effective version of Witt decomposition theorem for a bilinear space over $\overline{\mathbb{Q}}$. We also explain how our results can be extended to bilinear spaces with singular points. In section 6 we derive some related results for quadratic spaces over $\overline{\mathbb{Q}}$, including an "orthogonal" version of Siegel's lemma and an effective version of Cartan-Dieudonné theorem; these are direct analogues of results of [4] over a number field, methods of proof are the same.

2. Notation and heights

We start with some notation. Let K be a number field of degree d over $\mathbb{Q}$, O_K its ring of integers, and $M(K)$ its set of places. 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 $u \in M(\mathbb{Q})$

$$\sum_{v \in M(K), v|u} d_v = d. \tag{7}$$

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. We also define the second absolute value $|\ |_v$ for each place v by $|a|_v = \|a\|_v^{d_v/d}$ for all $a \in K$. Then for each non-zero $a \in K$ the *product formula* reads

$$\prod_{v \in M(K)} |a|_v = 1. \tag{8}$$

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

$$H_v(\boldsymbol{x}) = \begin{cases} \max_{1 \le i \le N} |x_i|_v & \text{if } v \nmid \infty \\ \left(\sum_{i=1}^N \|x_i\|_v^2 \right)^{d_v/2d} & \text{if } v|\infty \end{cases}$$

for each $\boldsymbol{x} \in K_v^N$. We define the following global height function on K^N:

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} H_v(\boldsymbol{x}), \tag{9}$$

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

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

$$h(\boldsymbol{x}) = H(1, \boldsymbol{x}), \tag{10}$$

hence $h(\boldsymbol{x}) \geq H(\boldsymbol{x})$ for each $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$. A basic property of heights that we will use states that for $a_1, ..., a_L \in \overline{\mathbb{Q}}$ and $\boldsymbol{x}_1, ..., \boldsymbol{x}_L \in \overline{\mathbb{Q}}^N$,

$$H\left(\sum_{i=1}^{L} a_i \boldsymbol{x}_i\right) \leq h\left(\sum_{i=1}^{L} a_i \boldsymbol{x}_i\right) \leq H(\boldsymbol{a}) \prod_{i=1}^{L} h(\boldsymbol{x}_i), \tag{11}$$

where $\boldsymbol{a} = (a_1, ..., a_L) \in \overline{\mathbb{Q}}^L$.

We can extend height to polynomials in the following way: for every $N \geq 1$, if $G(X_1, \ldots, X_N) \in K[X_1, \ldots, X_N]$ we will write $H_v(G)$ and $H(G)$ for the local and global height of the coefficient vector of G, respectively. It is convenient to also introduce a slightly different height $\mathcal{H}$ for our quadratic form F: we define $\mathcal{H}_v(F)$ and $\mathcal{H}(F)$ to be the local and global heights, respectively, of the symmetric matrix $(f_{ij})_{1 \leq i,j \leq N}$ viewed as a vector in K^{N^2}. It is then easy to see that

$$H_v(F) \leq \begin{cases} \mathcal{H}_v(F) & \text{if } v \nmid \infty \\ 2^{\frac{d_v}{2d}} \mathcal{H}_v(F) & \text{if } v | \infty, \end{cases}$$

and so $H(F) \leq \sqrt{2}\mathcal{H}(F)$.

We also define height on matrices, which is the same as height function on subspaces of $\overline{\mathbb{Q}}^N$. Let $V \subseteq \overline{\mathbb{Q}}^N$ be a subspace of dimension J, $1 \leq J \leq N$, defined over a number field K. Choose a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$ for V over K, and write $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_J)$ for the corresponding $N \times J$ basis matrix. Then

$$V = \{X\boldsymbol{t} : \boldsymbol{t} \in \overline{\mathbb{Q}}^J\}.$$

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

$$V = \{\boldsymbol{x} \in \overline{\mathbb{Q}}^N : A\boldsymbol{x} = 0\}.$$

Let $\mathcal{I}$ be the collection of all subsets I of $\{1, ..., N\}$ of cardinality J. 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

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

For each $I \in \mathcal{I}$, write X_I for the $J \times J$ sub-matrix of X consisting of all those rows of X which are indexed by I, and ${}_{I'}A$ for the $(N - J) \times (N - J)$ sub-matrix of A consisting of all those columns of A which are indexed by I'. By the duality principle of Brill-Gordan [6] (also see Theorem 1 on p. 294 of [7]), there exists a non-zero constant $\gamma \in K$ such that

$$\det(X_I) = (-1)^{\varepsilon(I')} \gamma \det({}_{I'}A), \tag{12}$$

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

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

Define

$$H(X) = H(Gr(X)), \quad H(A) = H(Gr(A)),$$

and so by (12) and (8)

$$H(X) = H(A).$$

Define height of V denoted by $H(V)$ to be this common value. Hence the height of a matrix is the height of its row (or column) space, which is equal to the height of its null-space. Also notice that $Gr(X)$ can be identified with $\boldsymbol{x}_1 \wedge \ ... \ \wedge \boldsymbol{x}_J$, where $\wedge$ stands for the wedge product, viewed under the canonical lexicographic embedding into $K^{\binom{N}{J}}$. Therefore we can also write

$$H(V) = H(\boldsymbol{x}_1 \wedge \ ... \ \wedge \boldsymbol{x}_J).$$

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

$$\boldsymbol{y}_1 \wedge \ ... \ \wedge \boldsymbol{y}_J = (\det C)\ \boldsymbol{x}_1 \wedge \ ... \ \wedge \boldsymbol{x}_J,$$

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

Finally, for a point $\boldsymbol{z} = (z_1, ..., z_N) \in \overline{\mathbb{Q}}^N$, we write $\deg_K(\boldsymbol{z})$ to mean the degree of the extension $K(z_1, ..., z_N)$ over K, i.e. $\deg_K(\boldsymbol{z}) = [K(z_1, ..., z_N) : K]$.

3. Preliminary lemmas

Here we present some technical lemmas that we will use. The first one is a consequence of Laplace's expansion, and can be found as Lemma 4.7 of [10] (also see pp. 15-16 of [1]).

Lemma 3.1. *Let X be a $N \times J$ matrix over $\overline{\mathbb{Q}}$ with column vectors $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$. Then*

$$H(X) = H(\boldsymbol{x}_1 \wedge \boldsymbol{x}_1 \ ... \ \wedge \boldsymbol{x}_J) \leq \prod_{i=1}^{J} H(\boldsymbol{x}_i). \tag{13}$$

More generally, if the $N \times J$ matrix X can be partitioned into blocks as $X = (X_1 \ X_2)$, then

$$H(X) \leq H(X_1)H(X_2). \tag{14}$$

The next one is an obvious adaptation of Lemma 2.3 of [4] over $\overline{\mathbb{Q}}$.

Lemma 3.2. *Let X be a $N \times J$ matrix over $\overline{\mathbb{Q}}$ with column vectors $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$, and let F be a symmetric bilinear form in N variables, as above (we also write F for its $N \times N$ coefficient matrix). Then*

$$H(FX) \leq \mathcal{H}(F)^J \prod_{i=1}^{J} H(\boldsymbol{x}_i). \tag{15}$$

The following well known fact is an immediate corollary of Theorem 1 of [15] adapted over $\overline{\mathbb{Q}}$.

Lemma 3.3. *Let U_1 and U_2 be subspaces of $\overline{\mathbb{Q}}^N$. Then*

$$H(U_1 \cap U_2) \le H(U_1)H(U_2).$$

The following simple lemma can be viewed as an analogue of Cassels' bound (2) over $\overline{\mathbb{Q}}$. It is a special case of Proposition 3.1 of [5]; we include a proof here for the purposes of self-containment.

Lemma 3.4. *Let F be a quadratic form in N variables as above. Then there exists $\mathbf{0} \neq \boldsymbol{x} \in \overline{\mathbb{Q}}^N$ such that $F(\boldsymbol{x}) = 0$, and*

$$H(\boldsymbol{x}) \le 2\sqrt{\mathcal{H}(F)}. \tag{16}$$

Proof. If F is identically zero, then we are done. So assume F is non-zero. Write $\boldsymbol{e}_1, ..., \boldsymbol{e}_N$ for the standard basis vectors for $\overline{\mathbb{Q}}^N$ over $\overline{\mathbb{Q}}$. Assume that for some $1 \le i \le N$, $\deg_{X_i} F < 2$, then it is easy to see that $F(\boldsymbol{e}_i) = 0$, and $H(\boldsymbol{e}_i) = 1$. If $N > 2$, let

$$F_1(X_1, X_2) = F(X_1, X_2, 0, ..., 0),$$

and a point $\boldsymbol{x} = (x_1, x_2) \in \overline{\mathbb{Q}}^2$ is a zero of F_1 if and only if $(x_1, x_2, 0, ..., 0)$ is a zero of F, and $H(x_1, x_2) = H(x_1, x_2, 0, ..., 0)$. In particular, if $F_1(X_1, X_2) = 0$, then $F(\boldsymbol{e}_1) = 0$. Hence we can assume that $N = 2$, $F(X_1, X_2) \neq 0$, and $\deg_{X_1} F = \deg_{X_2} F = 2$. Write

$$F(X_1, X_2) = f_{11}X_1^2 + 2f_{12}X_1X_2 + f_{22}X_2^2,$$

where $f_{11}, f_{22} \neq 0$. Let

$$g(X_1) = F(X_1, 1) = f_{11}X_1^2 + 2f_{12}X_1 + f_{22},$$

be a quadratic polynomial in one variable. Notice that since coefficients of g are those of F, we have $H(g) = H(F) \le \sqrt{2}\mathcal{H}(F)$. By Lemma 2 of [8] (see also Lemma 2.1 of [5]), there must exist $\alpha \in \overline{\mathbb{Q}}$ such that $g(\alpha) = 0$, and

$$H(\alpha, 1) \le \sqrt{2H(g)} \le 2\sqrt{\mathcal{H}(F)}.$$

Taking $\boldsymbol{x} = (\alpha, 1)$ completes the proof. □

Next we present a lemma on effective decomposition of a quadratic space into regular and singular components. This is an adaptation of Lemma 3.2 of [4] over $\overline{\mathbb{Q}}$, although the inequality (18) is slightly weaker than its number field analogue; this, however, makes essentially no difference for our purposes.

Lemma 3.5. *Let F have rank r on Z, and assume that $1 \le r < L$. Then the bilinear space (Z, F) can be represented as*

$$Z = Z^{\perp} \perp W, \tag{17}$$

where $Z^{\perp} = \{\boldsymbol{z} \in Z : F(\boldsymbol{z}, \boldsymbol{x}) = 0 \ \forall \ \boldsymbol{x} \in Z\}$ is the $(L-r)$-dimensional singular component, and W is a regular subspace of Z, with $\dim_{\overline{\mathbb{Q}}} W = r$ and

$$H(Z^{\perp}) \le 3^{\frac{L(L-1)}{2}} \mathcal{H}(F)^r H(Z)^2, \tag{18}$$

and

$$H(W) \le 3^{\frac{L(L-1)}{2}} H(Z). \tag{19}$$

Proof. Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L$ be the basis for Z guaranteed by Theorem 1.2, and write $X = (\boldsymbol{x}_1 \dots \boldsymbol{x}_L)$ for the corresponding $N \times L$ basis matrix. Notice that

$$Z^{\perp} = \mathbb{N}(FX) \cap Z,$$

where $\mathbb{N}(FX) = \{\boldsymbol{z} \in \overline{\mathbb{Q}}^N : \boldsymbol{z}FX = 0\}$ is the null-space of the matrix FX. Since the matrix $FX = (F\boldsymbol{x}_1 \dots F\boldsymbol{x}_L)$ has rank $r < L$, only r of its columns can be linearly independent. In other words, there exist $\boldsymbol{x}_{i_1}, ..., \boldsymbol{x}_{i_r} \in \{\boldsymbol{x}_1, ..., \boldsymbol{x}_L\}$ such that the $N \times r$ matrix $FX' = (F\boldsymbol{x}_{i_1} \dots F\boldsymbol{x}_{i_L})$ has rank r, and $\mathbb{N}(FX) = \{\boldsymbol{z} \in \overline{\mathbb{Q}}^N : \boldsymbol{z}FX' = 0\}$. Then, combining Lemmas 3.2 and 3.3 with Theorem 1.2, we obtain

$$\begin{aligned} H(Z^{\perp}) &\leq H(\mathbb{N}(FX))H(Z) = H(FX')H(Z) \leq H(Z)\mathcal{H}(F)^r \prod_{j=1}^{r} H(\boldsymbol{x}_{i_j}) \\ &\leq H(Z)\mathcal{H}(F)^r \prod_{i=1}^{L} H(\boldsymbol{x}_i) \leq 3^{\frac{L(L-1)}{2}} \mathcal{H}(F)^r H(Z)^2, \end{aligned}$$

which is precisely (18). The proof of (19) is identical to the argument in the proof of Lemma 3.2 of [4], but we use Theorem 1.2 instead of Bombieri-Vaaler version of Siegel's lemma. □

Finally, we will need the following result on the existence of a small-height vector in a subspace $Z \subseteq \overline{\mathbb{Q}}^N$ at which the quadratic form F does not vanish, satisfying one additional condition. An *isometry* of the quadratic space (Z, F) is an isomorphism $\sigma : Z \to Z$ such that $F(\sigma(\boldsymbol{x}), \sigma(\boldsymbol{y})) = F(\boldsymbol{x}, \boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y} \in Z$. It is easy to see that isometries of (Z, F) form a group under function composition, which we denote by $\mathcal{O}(Z, F)$; isometries will be discussed in more details in section 6. The following is a direct analogue of Lemma 5.2 of [4] over $\overline{\mathbb{Q}}$.

Lemma 3.6. *Let (Z, F) be an L-dimensional regular bilinear space in N variables over $\overline{\mathbb{Q}}$, as above, and let $\sigma \in \mathcal{O}(Z, F)$. There exists an anisotropic vector $\boldsymbol{y}$ in Z such that $\sigma(\boldsymbol{y}) \pm \boldsymbol{y}$ is also anisotropic for some choice of $\pm$, and*

$$H(\boldsymbol{y}) \leq h(\boldsymbol{y}) \leq 2\sqrt{L}\ 3^{\frac{(L+2)(L-1)}{4}} H(Z)^{\frac{L+2}{2L}}. \tag{20}$$

Proof. The argument is identical to that in the proof of Lemma 5.2 of [4] with Bombieri-Vaaler version of Siegel's lemma [1] replaced with the absolute version of Roy and Thunder (Theorem 1.2). □

We are now ready to proceed.

4. Proof of Theorem 1.1

Let F be a quadratic form in $N \geq 2$ variables, as above. Let $Z \subseteq \overline{\mathbb{Q}}^N$ be an L-dimensional subspace, $1 \leq L \leq N$, such that the bilinear space (Z, F) is regular. We start by proving a lemma about the existence of a small-height zero of F in Z.

Lemma 4.1. *Let $2 \leq L \leq N$. There exists $\mathbf{0} \neq \boldsymbol{y} \in Z$ such that $F(\boldsymbol{y}) = 0$ and*

$$H(\boldsymbol{y}) \leq 8 \times 3^{2(L-1)} \mathcal{H}(F)^{\frac{1}{2}} H(Z)^{\frac{4}{L}}. \tag{21}$$

Proof. Let $\boldsymbol{z}_1, \dots, \boldsymbol{z}_L$ be the basis for Z guaranteed by Theorem 1.2 ordered so that

$$H(\boldsymbol{z}_1) \leq \dots \leq H(\boldsymbol{z}_L).$$

Then, by (6),

$$H(\boldsymbol{z}_1)H(\boldsymbol{z}_2) \le \left(3^{\frac{L(L-1)}{2}}H(Z)\right)^{\frac{2}{L}} = 3^{L-1}H(Z)^{\frac{2}{L}}. \tag{22}$$

We will now construct $a_1, a_2 \in \overline{\mathbb{Q}}$ such that $\boldsymbol{y} = a_1\boldsymbol{z}_1 + a_2\boldsymbol{z}_2$ is a zero of F. In other words, we want

$$0 = F(\boldsymbol{y}) = F(\boldsymbol{z}_1)a_1^2 + 2F(\boldsymbol{z}_1, \boldsymbol{z}_2)a_1a_2 + F(\boldsymbol{z}_2)a_2^2 = G(a_1, a_2). \tag{23}$$

The right hand side of (23) is a quadratic form G in the variables a_1, a_2 with coefficients $F(\boldsymbol{z}_1), 2F(\boldsymbol{z}_1, \boldsymbol{z}_2), F(\boldsymbol{z}_2)$. By Lemma 3.4, there must exist such a pair (a_1, a_2) with

$$H(a_1, a_2) \le 2\sqrt{\mathcal{H}(G)}. \tag{24}$$

Let E be the field extension generated over K by coefficients of G. By (2.6) of [17], for each $v \in M(E)$ and each $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \in E_v^N$

$$|F(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2)|_v \le \mathcal{H}_v(F)H_v(\boldsymbol{\alpha}_1)H_v(\boldsymbol{\alpha}_2).$$

Therefore, if $v \nmid \infty$, we have

$$\begin{aligned} \mathcal{H}_v(G) &\le \max\{|F(\boldsymbol{z}_1)|_v, |2|_v|F(\boldsymbol{z}_1, \boldsymbol{z}_2)|_v, |F(\boldsymbol{z}_2)|_v\} \\ &\le \mathcal{H}_v(F)\max\{H_v(\boldsymbol{z}_1)^2, H_v(\boldsymbol{z}_1)H_v(\boldsymbol{z}_2), H_v(\boldsymbol{z}_2)^2\} \\ &\le \mathcal{H}_v(F)\max\{1, H_v(\boldsymbol{z}_1)\}^2\max\{1, H_v(\boldsymbol{z}_2)\}^2. \end{aligned} \tag{25}$$

If $v|\infty$, then

$$\begin{aligned} \mathcal{H}_v(G)^{\frac{2d}{d_v}} &\le \|F(\boldsymbol{z}_1)\|_v^2 + 2\|F(\boldsymbol{z}_1, \boldsymbol{z}_2)\|_v^2 + \|F(\boldsymbol{z}_2)\|_v^2 \le \mathcal{H}_v(F)^{\frac{2d}{d_v}} \times \\ &\times \left(H_v(\boldsymbol{z}_1)^{\frac{4d}{d_v}} + 2\left(H_v(\boldsymbol{z}_1)H_v(\boldsymbol{z}_2)\right)^{\frac{2d}{d_v}} + H_v(\boldsymbol{z}_2)^{\frac{4d}{d_v}}\right) \\ &\le \mathcal{H}_v(F)^{\frac{2d}{d_v}}\left(1 + H_v(\boldsymbol{z}_1)^{\frac{2d}{d_v}}\right)^2\left(1 + H_v(\boldsymbol{z}_2)^{\frac{2d}{d_v}}\right)^2. \end{aligned} \tag{26}$$

Combining (24) with (25) and (26), we see that

$$H(a_1, a_2) \le 2\mathcal{H}(F)^{\frac{1}{2}}h(\boldsymbol{z}_1)h(\boldsymbol{z}_2). \tag{27}$$

Combining (27) and (11), we see that there exists a zero of F of the form $\boldsymbol{y} = a_1\boldsymbol{z}_1 + a_2\boldsymbol{z}_2 \in Z$ so that

$$H(\boldsymbol{y}) \le 2\mathcal{H}(F)^{\frac{1}{2}}h(\boldsymbol{z}_1)^2h(\boldsymbol{z}_2)^2. \tag{28}$$

Notice that for each $l = 1, 2$, $\boldsymbol{z}_l$ is a non-zero vector. If $\boldsymbol{z}_l$ has just one non-zero coordinate, let it for instance be i-th coordinate, then clearly we can take $\boldsymbol{z}_l$ to be i-th standard basis vector $\boldsymbol{e}_i$, and so $h(\boldsymbol{z}_l) = \sqrt{2}$. If $\boldsymbol{z}_l$ has more than one non-zero coordinates, then we can assume without loss of generality that at least one of them is equal to 1, and then it is easy to see that $h(\boldsymbol{z}_l) \le \sqrt{2}H(\boldsymbol{z}_l)$. Therefore (28) can be rewritten as

$$H(\boldsymbol{y}) \le 8\mathcal{H}(F)^{\frac{1}{2}}\left(H(\boldsymbol{z}_1)H(\boldsymbol{z}_2)\right)^2 \le 8 \times 3^{2(L-1)}\mathcal{H}(F)^{\frac{1}{2}}H(Z)^{\frac{4}{L}}, \tag{29}$$

where the last inequality follows by (22). This completes the proof. □

We are now ready to prove the theorem.

Proof of Theorem 1.1. First suppose that L is even, say $L = 2k$ for some integer $k \geq 1$. We argue by induction on k, the Witt index of (Z, F). Suppose that $k = 1$. Let $\boldsymbol{y} \in Z$ be the point guaranteed by Lemma 4.1. Then

$$H(\boldsymbol{y}) \leq 72\ \mathcal{H}(F)^{\frac{1}{2}} H(Z)^2, \tag{30}$$

and $V = \operatorname{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{y}\}$ is the desired maximal totally isotropic subspace of (Z, F).

Next suppose $k > 1$. Let $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_L$ be the basis for Z guaranteed by Theorem 1.2 ordered so that

$$H(\boldsymbol{z}_1) \leq \cdots \leq H(\boldsymbol{z}_L).$$

Let $Z_1 = \operatorname{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{z}_1, ..., \boldsymbol{z}_{L-2}\}$, so that

$$H(Z_1) \leq \prod_{i=1}^{L-2} H(\boldsymbol{z}_i) \leq \left(3^{\frac{L(L-1)}{2}} H(Z)\right)^{\frac{L-2}{L}} \leq 3^{(2k-1)(k-1)} H(Z)^{\frac{k-1}{k}}. \tag{31}$$

Let U be the maximal totally isotropic subspace of bounded height of (Z_1, F) guaranteed by the induction hypothesis, so that

$$\begin{aligned} H(U) &\leq 24 \times 2^{\frac{k-2}{4}} 3^{\frac{k^2(k-1)^2}{4}} \mathcal{H}(F)^{\frac{(k-1)^2}{2}} H(Z_1)^{\frac{k^2-k+2}{2(k-1)}} \\ &\leq 24 \times 2^{\frac{k-2}{4}} 3^{\frac{(2k-1)(k^2-k+2)}{2} + \frac{k^2(k-1)^2}{4}} \mathcal{H}(F)^{\frac{(k-1)^2}{2}} H(Z)^{\frac{k^2-k+2}{2k}}, \end{aligned} \tag{32}$$

by (31). Since $\dim_{\overline{\mathbb{Q}}}(U) = k - 1$, let $\boldsymbol{x}_1, ..., \boldsymbol{x}_{k-1}$ be the basis for U guaranteed by Theorem 1.2, and let $X = (\boldsymbol{x}_1\ ...\ \boldsymbol{x}_{k-1})$ be the corresponding $N \times (k-1)$ basis matrix. Define a $(k+1)$-dimensional subspace of Z

$$W = \{\boldsymbol{y} \in Z : \boldsymbol{y}FX = 0\} = Z \cap \{\boldsymbol{y} \in \overline{\mathbb{Q}} : \boldsymbol{y}FX = 0\}.$$

Combining Lemma 3.2, Lemma 3.3, and Theorem 1.2, we see that

$$\begin{aligned} H(W) \leq H(Z)H(FX) &\leq H(Z)\mathcal{H}(F)^{k-1} \prod_{i=1}^{k-1} H(\boldsymbol{x}_i) \\ &\leq \left\{3^{\frac{k}{2}} \mathcal{H}(F)\right\}^{k-1} H(U)H(Z). \end{aligned} \tag{33}$$

It is easy to see that $U \subset W$. Let $\boldsymbol{w}_1, ..., \boldsymbol{w}_{k+1}$ be a basis for W. Then at least two of these basis vectors are not in U, we can assume without loss of generality that these are $\boldsymbol{w}_1$ and $\boldsymbol{w}_2$. Since $W = \operatorname{span}_{\overline{\mathbb{Q}}}\{U, \boldsymbol{w}_1, \boldsymbol{w}_2\}$, and $\dim_{\overline{\mathbb{Q}}}(W) = \dim_{\overline{\mathbb{Q}}}(U) + 2$, it must be true that $U \cap \operatorname{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{w}_1, \boldsymbol{w}_2\} = \{\boldsymbol{0}\}$. Consider a binary quadratic form G in two variables a, b given by

$$G(a, b) = F(\boldsymbol{w}_1)a^2 + 2F(\boldsymbol{w}_1, \boldsymbol{w}_2)ab + F(\boldsymbol{w}_2)b^2.$$

Let $a = 1$, then there exist $b_1, b_2 \in \overline{\mathbb{Q}}$ such that $G(1, b_1) = G(1, b_2) = 0$, i.e. the zero-set of G consists, up to multiplicity, of two projective points. Let $\boldsymbol{y}_i = \boldsymbol{w}_1 + b_i\boldsymbol{w}_2$ for each $i = 1, 2$, and so $F(\boldsymbol{y}_1) = F(\boldsymbol{y}_2) = 0$ and $\boldsymbol{y}_1, \boldsymbol{y}_2 \notin U$. Define $V_i = \operatorname{span}_{\overline{\mathbb{Q}}}\{U, \boldsymbol{y}_i\}$ for each $i = 1, 2$, then $V_1, V_2 \subset W$ are maximal totally isotropic subspaces of (Z, F). Now suppose that $\boldsymbol{x} \in W$, then $\boldsymbol{x} = \boldsymbol{x}' + \beta_1\boldsymbol{w}_1 + \beta_2\boldsymbol{w}_2$, where $\boldsymbol{x}' \in U$. Therefore

$$F(\boldsymbol{x}) = F(\beta_1\boldsymbol{w}_1 + \beta_2\boldsymbol{w}_2) = G(\beta_1, \beta_2).$$

Hence $F(\boldsymbol{x}) = 0$ if and only if (β_1, β_2) is a multiple of either $(1, b_1)$ or $(1, b_2)$. In other words, $\boldsymbol{x} \in W$ is such that $F(\boldsymbol{x}) = 0$ if and only if $\boldsymbol{x} \in V_1 \cup V_2$.

Let $\mathcal{Z}_F$ be the projective closure of the affine set $\{\boldsymbol{x} \in \overline{\mathbb{Q}}^N : F(\boldsymbol{x}) = 0\}$, i.e. the projective variety defined by F over $\overline{\mathbb{Q}}$. Write $\mathbb{P}(W)$ for the projective space over

W. Let $\mathcal{Z}_F \centerdot \mathbb{P}(W)$ be the intersection cycle of these two projective varieties, so that up to multiplicity

$$\mathcal{Z}_F \centerdot \mathbb{P}(W) = \mathbb{P}(V_1) + \mathbb{P}(V_2),$$

i.e. its support is $\mathbb{P}(V_1) \cup \mathbb{P}(V_2)$. Notice that from our construction above it is possible that $V_1 = V_2$, then we write $\mathcal{Z}_F \centerdot \mathbb{P}(W) = 2\mathbb{P}(V_1)$, so that 2 is the multiplicity of the component V_1 in this intersection cycle. In any case, the height of this intersection cycle is defined by

$$H(\mathcal{Z}_F \centerdot \mathbb{P}(W)) = H(V_1)H(V_2). \tag{34}$$

See [2] for the details on arithmetic intersection theory and heights, keeping in mind that in case of a linear space or a hypersurface their height reduces to an additive height given by $\log(H^d)$ (see (3.1.6) on p. 947 and remark after Proposition 4.1.2 on p. 965 of [2]). Then applying a version of Arithmetic Bezout's Theorem presented by Theorem 5.4.4 (i) of [2], we obtain

$$H(\mathcal{Z}_F \centerdot \mathbb{P}(W)) \le \sqrt{2} H(W)^2 \mathcal{H}(F). \tag{35}$$

Therefore, combining (34), (35), and (33), we have

$$\begin{aligned} \min\{H(V_1), H(V_2)\} &\le \sqrt{H(V_1)H(V_2)} = \sqrt{H(\mathcal{Z}_F \centerdot \mathbb{P}(W))} \\ &\le 2^{\frac{1}{4}} H(W)\mathcal{H}(F)^{\frac{1}{2}} \le 2^{\frac{1}{4}} 3^{\frac{k(k-1)}{2}} \mathcal{H}(F)^{k-\frac{1}{2}} H(U)H(Z). \end{aligned} \tag{36}$$

Write V for V_i with $H(V_i)$ being the smaller of the two, $i = 1, 2$. Combining (32) and (36) yields (4).

Next suppose that L is odd, say $L = 2k + 1$ for some $k \ge 0$. We again argue by induction on k, which is the Witt index of (Z, F). If $k = 0$, then $L = 1$, and so $Z = \overline{\mathbb{Q}}\boldsymbol{y}$ for some anisotropic vector $\boldsymbol{y} \in \overline{\mathbb{Q}}^N$ since (Z, F) is regular. Hence $\{\mathbf{0}\}$ is the maximal totally isotropic subspace of (Z, F), so there is nothing to prove. Assume $k \ge 1$. Let $\boldsymbol{z}_1, \dots, \boldsymbol{z}_L$ be the basis for Z guaranteed by Theorem 1.2 ordered so that

$$H(\boldsymbol{z}_1) \le \cdots \le H(\boldsymbol{z}_L),$$

and define $Z_1 = \mathrm{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{z}_1, ..., \boldsymbol{z}_{L-1}\}$. By Theorem 1.2

$$H(Z_1) \le 3^{2k^2} H(Z)^{\frac{2k}{2k+1}}. \tag{37}$$

Then (Z_1, F) is a bilinear space over $\overline{\mathbb{Q}}$ of dimension $L - 1 = 2k$. Notice that maximal totally isotropic subspaces of (Z_1, F) are also maximal totally isotropic subspaces of (Z, F), hence have dimension k. Let

$$Z_1^{\perp} = \{\boldsymbol{x} \in Z_1 : F(\boldsymbol{x}, \boldsymbol{z}) = 0 \ \forall \ \boldsymbol{z} \in Z_1\}$$

be the singular component of Z_1, and suppose it has dimension l. Then $Z_1 = Z_1^{\perp} \perp W$ for some $(2k - l)$-dimensional subspace W of Z_1 such that (W, F) is regular. Witt index of (W, F) is therefore equal to $\left[\frac{2k-l}{2}\right]$, so let V be a maximal totally isotropic subspace of W. Then $Z_1^{\perp} \perp V$ is a maximal totally isotropic subspace of Z_1, and so has dimension k. On the other hand, $Z_1^{\perp} \cap V = \{\mathbf{0}\}$, hence $\dim_{\overline{\mathbb{Q}}}(Z_1^{\perp} \perp V) = l + \left[\frac{2k-l}{2}\right]$. Therefore we must have

$$l + \left[\frac{2k-l}{2}\right] = k,$$

which means that either $l = 0$ or $l = 1$. If $l = 0$, then (Z_1, F) is regular, and so by the argument in the even case above there exists a maximal totally isotropic

subspace V of (Z_1, F) of bounded height. Moreover, by combining (4) and (37), we obtain

$$H(V) \le 24 \times 2^{\frac{k-1}{4}} 3^{\frac{k(k+1)^2(k+4)}{4}} \mathcal{H}(F)^{\frac{k^2}{2}} H(Z)^{\frac{k^2+k+2}{2k+1}}, \tag{38}$$

which is smaller than the bound in (5).

Assume $l = 1$. Then (W, F) is a regular $(2k-1)$-dimensional bilinear space of Witt index $k-1$ with

$$H(W) \le 3^{k(4k-1)} H(Z)^{\frac{2k}{2k+1}}, \tag{39}$$

where this bound is obtained by combining (19) with (37). By induction hypothesis, there exists a maximal totally isotropic subspace U of (W, F) with

$$H(U) \le 3^{2(k-1)k^3} \mathcal{H}(F)^{(k-1)^2} H(W)^{\frac{4(k-1)}{3}}. \tag{40}$$

Notice that F has rank $2k-1$ on Z_1. Combining Lemma 3.5 and (40), and applying (14) of Lemma 3.1, we see that the maximal totally isotropic subspace $V = Z_1^{\perp} \perp U$ of (Z_1, F) satisfies

$$H(V) \le H(Z_1^{\perp}) H(U) \le 3^{k(6k-1)} \mathcal{H}(F)^{2k-1} H(Z)^{\frac{4k}{2k+1}} H(U), \tag{41}$$

where the last inequality follows by combining (18) and (37). Combining (39), (40), and (41) produces (5), and so finishes the proof. □

5. Corollaries

In this section we use Theorem 1.1 to prove an effective version of Witt decomposition theorem over $\overline{\mathbb{Q}}$. First let us recall that a *hyperbolic plane* in (Z, F) is a two-dimensional subspace of the form

$$\mathbb{H} = \mathrm{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{x}, \boldsymbol{y} \in Z : F(\boldsymbol{x}) = F(\boldsymbol{y}) = 0,\ F(\boldsymbol{x}, \boldsymbol{y}) = 1\}.$$

A classical theorem of Witt (1937) for a regular L-dimensional bilinear space (Z, F) over $\overline{\mathbb{Q}}$ states that there exists a decomposition of Z into an orthogonal direct sum with respect to F of the form

$$Z = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k \perp W, \tag{42}$$

where $k = \left[\frac{L}{2}\right]$ is Witt index of (Z, F), $\mathbb{H}_1, \ldots, \mathbb{H}_k$ are hyperbolic planes, and W is zero if $L = 2k$, and is a one-dimensional anisotropic component if $L = 2k+1$, i.e. is of the form $\mathrm{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{y}\}$ for some $\boldsymbol{y} \in Z$ such that $F(\boldsymbol{y}) \neq 0$ (see for instance Corollary 5.11 on p.17 of [12]). An effective version of Witt decomposition theorem for bilinear spaces over a number field is proved in [4]. Here we obtain the following effective analogue of Witt's theorem over $\overline{\mathbb{Q}}$.

Theorem 5.1. *Let (Z, F) be a regular L-dimensional bilinear space in N-variables over $\overline{\mathbb{Q}}$. There exists an orthogonal decomposition of (Z, F) as in (42) such that for each $1 \le i \le k = \left[\frac{L}{2}\right]$*

$$H(\mathbb{H}_i) \le 3^{12k^4(k+1)\left(\frac{3}{2}\right)^k} \left\{\sqrt{k}\ \mathcal{H}(F)^{k^2+1} H(Z)^{\frac{6k+5}{4k+2}}\right\}^{\frac{(k+1)(k+2)}{2}\left(\frac{3}{2}\right)^k}, \tag{43}$$

and $W = \{\mathbf{0}\}$ if $L = 2k$, or $W = \overline{\mathbb{Q}}\boldsymbol{y}$ with

$$H(W) = H(\boldsymbol{y}) \le 2\sqrt{2k+1}\ 3^{\frac{(2k+3)k}{2}} H(Z)^{\frac{2k+3}{4k+2}}, \tag{44}$$

if $L = 2k+1$.

Proof. First assume $L = 2k$. In this case we prove that there exists a decomposition of (Z, F) of the form

$$Z = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k, \tag{45}$$

with

$$H(\mathbb{H}_i) \le 3^{12k^5\left(\frac{3}{2}\right)^k} \left\{\mathcal{H}(F)^{k^2} H(Z)\right\}^{\frac{(k+1)(k+2)}{2}\left(\frac{3}{2}\right)^k}, \tag{46}$$

for each $1 \le i \le k$, which is smaller than the bound in (43). The argument is identical to the proof of Theorem 4.1 of [4], except that instead of Bombieri-Vaaler version of Siegel's lemma over a fixed number field (quoted as Theorem 2.1 in [4]) we use the absolute version of our Theorem 1.2 due to Roy and Thunder, and instead of Vaaler's theorem on the existence of a maximal totally isotropic subspace of bounded height in a bilinear space over a fixed number field (quoted as Theorem 3.1 in [4]) we use the absolute version, i.e. the case $L = 2k$ of our Theorem 1.1 given by the bound in (4). Using the same construction as in the proof of Theorem 4.1 of [4], we first obtain a hyperbolic plane $\mathbb{H}_1 \subseteq Z$ such that

$$H(\mathbb{H}_1) \le 3^{(k+1)^3} \mathcal{H}(F)^{\frac{k}{2}} H(Z)^{\frac{(k+1)(k+2)}{2k^2}}, \tag{47}$$

which is smaller than the bound in (46), and then define

$$Z_1 = \mathbb{H}_1^{\perp} = \{\boldsymbol{z} \in \overline{\mathbb{Q}}^N : F(\boldsymbol{z}, \boldsymbol{x}) = 0 \ \forall \ \boldsymbol{x} \in \mathbb{H}_1\} \cap Z,$$

so that $\dim_{\overline{\mathbb{Q}}}(Z_1) = L - 2 = 2(k-1)$, (Z_1, F) is a regular bilinear space of Witt index $k-1$, and $Z = \mathbb{H}_1 \perp Z_1$. Combining Lemmas 3.2 and 3.3 with (47), we obtain

$$H(Z_1) \le H(\mathbb{H}_1) H(Z) \mathcal{H}(F)^2 \le 3^{(k+1)^3} \mathcal{H}(F)^{\frac{k+4}{2}} H(Z)^{\frac{3k^2+3k+2}{2k^2}}. \tag{48}$$

We proceed by induction on k. If $k = 1$, we are done. If $k \ge 2$, by induction hypothesis there must exist a decomposition for (Z_1, F) of the form

$$Z_1 = \mathbb{H}_2 \perp \cdots \perp \mathbb{H}_k,$$

with

$$H(\mathbb{H}_i) \le 3^{12(k-1)^5\left(\frac{3}{2}\right)^{k-1}} \left\{\mathcal{H}(F)^{(k-1)^2} H(Z_1)\right\}^{\frac{k(k+1)}{2}\left(\frac{3}{2}\right)^{k-1}}, \tag{49}$$

for each $2 \le i \le k$. Then

$$Z = \mathbb{H}_1 \perp Z_1 = \mathbb{H}_1 \perp \mathbb{H}_2 \perp \cdots \perp \mathbb{H}_k,$$

and combining (48) and (49) yields (46).

Next suppose $L = 2k + 1$. Then let $\boldsymbol{y} \in Z$ be the anisotropic vector guaranteed by Lemma 3.6, and define $W = \operatorname{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{y}\}$, so that by (20)

$$H(W) = H(\boldsymbol{y}) \le 2\sqrt{2k+1}\ 3^{\frac{(2k+3)k}{2}} H(Z)^{\frac{2k+3}{4k+2}}. \tag{50}$$

Define

$$Z_1 = W^{\perp} = \{\boldsymbol{z} \in \overline{\mathbb{Q}}^N : F(\boldsymbol{z}, \boldsymbol{y}) = 0\} \cap Z,$$

then $\dim_{\overline{\mathbb{Q}}}(Z_1) = L - 1 = 2k$, and $Z = W \perp Z_1$. Combining Lemmas 3.2 and 3.3 with (50), we obtain

$$H(Z_1) \le H(W) H(Z) \mathcal{H}(F) \le 2\sqrt{2k+1}\ 3^{\frac{(2k+3)k}{2}} \mathcal{H}(F) H(Z)^{\frac{6k+5}{4k+2}}. \tag{51}$$

Suppose there exists $\boldsymbol{x} \in Z_1$ such that $F(\boldsymbol{x}, \boldsymbol{z}) = 0$ for all $\boldsymbol{z} \in Z_1$. By construction $F(\boldsymbol{x}, \boldsymbol{y}) = 0$, and hence $F(\boldsymbol{x}, \boldsymbol{z}) = 0$ for all $\boldsymbol{z} \in Z$. This contradicts the original assumption that (Z, F) is regular, hence (Z_1, F) must also be regular, and thus its Witt index is equal to k. Therefore, by the argument in the even case above, there exists a decomposition into an orthogonal sum of k hyperbolic planes of bounded height like (45) for Z_1. Hence we obtained a decomposition as in (42) for Z. Combining (46) with (51) yields (43), and (44) is precisely (50). □

Remark. Notice that Theorems 1.1 and 5.1 can both be extended to the case when our bilinear space (Z, F) contains singular points. In this case Z can be written as $Z = Z^{\perp} \perp Z_1$, where $Z^{\perp}$ is the singular component and (Z_1, F) is a regular bilinear space. If V is the maximal totally isotropic subspace of (Z_1, F) of bounded height as guaranteed by Theorem 1.1, then $Z^{\perp} \perp V$ is a maximal totally isotropic subspace of (Z, F), and by Lemma 3.1

$$H(Z^{\perp} \perp V) \leq H(Z^{\perp})H(V),$$

where $H(Z^{\perp})$ is bounded by (18) of Lemma 3.5. Witt decomposition for (Z, F) in this case will be of the form

$$Z = Z^{\perp} \perp \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k \perp W,$$

where k is the Witt index of (Z_1, F), and $Z_1 = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k \perp W$ is the small-height decomposition for (Z_1, F) guaranteed by Theorem 5.1.

6. Related Results

In this section we derive some additional structural theorems for bilinear spaces over $\overline{\mathbb{Q}}$, analogous to those in [4]. In particular, all the arguments in this section are completely parallel to their respective analogues over a fixed number field developed in [4]. We include them here for the purposes of self-containment and readability. As above, let F be a quadratic form in $N \geq 2$ variables. We first state a result on an effective decomposition of a bilinear space into an orthogonal sum of one-dimensional subspaces, i.e. a version of Siegel's lemma for a bilinear space.

Theorem 6.1. *Let Z be an L-dimensional subspace of $(\overline{\mathbb{Q}}^N, F)$, $L < N$. Then there exists a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_L \in \overline{\mathbb{Q}}^N$ for Z such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $i \neq j$, and*

$$\prod_{i=1}^{L} H(\boldsymbol{x}_i) \leq 3^{\frac{(L-1)^2(L+2)}{4}} \mathcal{H}(F)^{\frac{L(L+1)}{2}} H(Z)^L. \tag{52}$$

Proof. We argue by induction on L. First suppose that $L = 1$, then pick any $\mathbf{0} \neq \boldsymbol{x}_1 \in Z$, and observe that $H(\boldsymbol{x}_1) = H(Z)$. Now assume that $L > 1$ and the theorem is true for all $1 \leq j < L$. Let $\mathbf{0} \neq \boldsymbol{x}_1 \in Z$ be a vector guaranteed by Theorem 1.2 so that

$$H(\boldsymbol{x}_1) \leq 3^{\frac{L-1}{2}} H(Z)^{\frac{1}{L}}. \tag{53}$$

First assume that $\boldsymbol{x}_1$ is a non-singular point in Z. Then

$$Z_1 = \{\boldsymbol{y} \in Z : \boldsymbol{x}_1^t F \boldsymbol{y} = 0\} = \{\boldsymbol{x}_1\}^{\perp} \cap Z,$$

has dimension $L - 1$; here $\{\boldsymbol{x}_1\}^{\perp} = \{\boldsymbol{y} \in \overline{\mathbb{Q}}^N : \boldsymbol{x}_1^t F \boldsymbol{y} = 0\}$. Then by Lemma 3.3, Lemma 3.2, and (53) we obtain

$$H(Z_1) \leq H(\boldsymbol{x}_1^t F) H(Z) \leq \mathcal{H}(F) H(\boldsymbol{x}_1) H(Z) \leq 3^{\frac{L-1}{2}} \mathcal{H}(F) H(Z)^{\frac{L+1}{L}}. \tag{54}$$

Since $\dim_{\overline{\mathbb{Q}}}(Z_1) = L-1$, the induction hypothesis implies that there exists a basis $\boldsymbol{x}_2, ..., \boldsymbol{x}_L$ for Z_1 such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $2 \le i \ne j \le L$, and

$$\begin{aligned} \prod_{i=2}^{L} H(\boldsymbol{x}_i) &\le 3^{\frac{(L-2)^2(L+1)}{4}} \mathcal{H}(F)^{\frac{L(L-1)}{2}} H(Z_1)^{L-1} \\ &\le 3^{\frac{(L-2)^2(L+1)}{4} + \frac{(L-1)^2}{2}} \mathcal{H}(F)^{\frac{L^2+L-2}{2}} H(Z)^{\frac{L^2-1}{L}}, \end{aligned} \tag{55}$$

where the last inequality follows by (54). Combining (53) and (55) we see that $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ is a basis for Z satisfying (52) such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $1 \le i \ne j \le L$.

Now assume that $\boldsymbol{x}_1$ is a singular point in Z. Since $\boldsymbol{x}_1 \ne 0$, it must be true that $x_{1j} \ne 0$ for some $1 \le j \le N$. Let

$$Z_1 = Z \cap \{\boldsymbol{x} \in \overline{\mathbb{Q}}^N : x_j = 0\},$$

then $\boldsymbol{x}_1 \notin Z_1$, $Z = \overline{\mathbb{Q}}\boldsymbol{x}_1 \perp Z_1$, and

$$H(Z_1) \le H(Z), \tag{56}$$

by Lemma 3.3. Since $\dim_{\overline{\mathbb{Q}}}(Z_1) = L-1$, we can apply induction hypothesis to Z_1, and proceed the same way as in the non-singular case above. Since the upper bound of (56) is smaller than that of (54), the result follows. □

Next we discuss the effective structure of the isometry group of a bilinear space over $\overline{\mathbb{Q}}$. For the rest of this section assume that $Z \subseteq \overline{\mathbb{Q}}^N$ is an L-dimensional subspace, $1 \le L \le N$ such that the bilinear space (Z, F) is regular. From here on our notation is the same as in section 5 of [4]; we review it here.

First notice that $\overline{\mathbb{Q}}^N = Z \perp Z^{\perp_{\overline{\mathbb{Q}}^N}}$, where $Z^{\perp_{\overline{\mathbb{Q}}^N}} = \{\boldsymbol{x} \in \overline{\mathbb{Q}}^N : F(\boldsymbol{x}, \boldsymbol{z}) = 0 \ \forall \ \boldsymbol{z} \in Z\}$. Let $\mathcal{O}(Z, F)$ be the group of isometries of (Z, F), and write id_Z for its identity element. Also let $-id_Z$ be the element of $\mathcal{O}(Z, F)$ that takes $\boldsymbol{x}$ to $-\boldsymbol{x}$ for each $\boldsymbol{x} \in Z$. Each element σ of the isometry group $\mathcal{O}(\overline{\mathbb{Q}}^N, F)$ is uniquely represented by an $N \times N$ matrix $A \in GL_N(\overline{\mathbb{Q}})$, and so we can define $\mathcal{H}(\sigma)$ to be the height of A viewed as a vector in $\overline{\mathbb{Q}}^{N^2}$, same way as for the coefficient matrix of F.

Notice that each $\sigma \in \mathcal{O}(Z, F)$ can be extended to an isometry $\hat{\sigma} \in \mathcal{O}(\overline{\mathbb{Q}}^N, F)$ by selecting an isometry $\sigma' \in \mathcal{O}(Z^{\perp_{\overline{\mathbb{Q}}^N}}, F)$. For each $\sigma \in \mathcal{O}(Z, F)$ choose such an extension $\hat{\sigma} : \overline{\mathbb{Q}}^N \to \overline{\mathbb{Q}}^N$ so that $\mathcal{H}(\hat{\sigma})$ is minimal, and define $\mathcal{H}(\sigma) = \mathcal{H}(\hat{\sigma})$ for this choice of $\hat{\sigma}$. This definition of height in particular insures that for each $\sigma \in \mathcal{O}(Z, F)$

$$\mathcal{H}(\sigma) = \mathcal{H}(-\sigma), \tag{57}$$

where $-\sigma = -id_Z \circ \sigma$. Moreover, if A is the matrix of $\hat{\sigma}$, then

$$\det(A) = \det(\hat{\sigma}) = \det(\hat{\sigma} \mid_Z) \det\left(\hat{\sigma} \mid_{Z^{\perp_{\overline{\mathbb{Q}}^N}}}\right) = \det(\sigma)\det(\sigma') = \pm 1. \tag{58}$$

We will also refer to this matrix A as the matrix of σ.

For each $\boldsymbol{x} \in Z$ such that $F(\boldsymbol{x}) \ne 0$ we can define an element of $\mathcal{O}(Z, F)$, $\tau_{\boldsymbol{x}} : Z \longrightarrow Z$, given by

$$\tau_{\boldsymbol{x}}(\boldsymbol{y}) = \boldsymbol{y} - \frac{2F(\boldsymbol{x}, \boldsymbol{y})}{F(\boldsymbol{x})}\boldsymbol{x}, \tag{59}$$

which is a *reflection* in the hyperplane $\{\boldsymbol{x}\}^{\perp} = \{\boldsymbol{z} \in Z : F(\boldsymbol{x}, \boldsymbol{z}) = 0\}$. It is not difficult to see that the matrix of such a reflection is of the form $(\tau_{ij}(\boldsymbol{x}))_{1 \le i,j \le N}$, where

$$\tau_{ij}(\boldsymbol{x}) = \begin{cases} 1 - \frac{2}{F(\boldsymbol{x})} \sum_{k=1}^{N} f_{ik} x_i x_k & \text{if } i = j \\ -\frac{2}{F(\boldsymbol{x})} \sum_{k=1}^{N} f_{jk} x_i x_k & \text{if } i \neq j \end{cases}$$

For each reflection $\tau_{\boldsymbol{x}}$, $\det(\tau_{\boldsymbol{x}}) = -1$. We say that σ is a *rotation* if $\det(\sigma) = +1$.

We can now derive some bounds on height of isometries of (Z, F). We start with a simple result, which is precisely Lemma 5.1 of [4].

Lemma 6.2. *Let $\boldsymbol{x} \in Z$ be anisotropic and $\tau_{\boldsymbol{x}} \in \mathcal{O}(Z, F)$ be the corresponding reflection. Then*

$$\mathcal{H}(\tau_{\boldsymbol{x}}) \le N^3 (N+2) \mathcal{H}(F) H(\boldsymbol{x})^2. \tag{60}$$

An immediate consequence of Lemmas 6.2 and 3.6 is the following statement about the existence of a reflection of relatively small height in $\mathcal{O}(Z, F)$ - this is a direct analogue of Corollary 5.3 of [4].

Corollary 6.3. *There exists a reflection $\tau \in \mathcal{O}(Z, F)$ with*

$$\mathcal{H}(\tau) \le 3^{\frac{(L+2)(L-1)}{2}} 4 L N^3 (N+2) \mathcal{H}(F) H(Z)^{\frac{L+2}{L}}. \tag{61}$$

Proof. Let $\boldsymbol{x}$ be an anisotropic point in Z guaranteed by Lemma 3.6. Let $\tau = \tau_{\boldsymbol{x}}$. The result follows by combining (60) with (20). □

Moreover, every isometry $\sigma \in \mathcal{O}(Z, F)$ can be represented as a product of reflections of bounded height. This is an effective version of the well-known Cartan-Dieudonné theorem. Specifically, we can state the following.

Theorem 6.4. *Let (Z, F) be a regular symmetric bilinear space over $\overline{\mathbb{Q}}$ with $Z \subseteq \overline{\mathbb{Q}}^N$ of dimension L, $1 \le L \le N$, $N \ge 2$. Let $\sigma \in \mathcal{O}(Z, F)$. Then either σ is the identity, or there exist an integer $1 \le l \le 2L-1$ and reflections $\tau_1, ..., \tau_l \in \mathcal{O}(Z, F)$ such that*

$$\sigma = \tau_1 \circ \cdots \circ \tau_l, \tag{62}$$

and for each $1 \le i \le l$,

$$\mathcal{H}(\tau_i) \le \left\{ \left(2 N^2 3^{\frac{L-1}{2}} \right)^{\frac{L^2}{2}} \mathcal{H}(F)^{\frac{L}{3}} H(Z)^{\frac{L}{2}} \mathcal{H}(\sigma) \right\}^{5^{L-1}}. \tag{63}$$

To prove Theorem 6.4 we will need the following two technical lemmas, which are Lemmas 5.4 and 5.6 of [4], respectively.

Lemma 6.5. *Let $A \in GL_N(\overline{\mathbb{Q}})$ be such that $\det(A) = \pm 1$, and write I_N for the $N \times N$ identity matrix. Then*

$$\mathcal{H}(A \pm I_N) \le 2 \mathcal{H}(A). \tag{64}$$

Lemma 6.6. *Let A and B be two $N \times N$ matrices with entries in $\overline{\mathbb{Q}}$. Then*

$$\mathcal{H}(AB) \le \mathcal{H}(A) \mathcal{H}(B). \tag{65}$$

Proof of Theorem 6.4. We argue by induction on L. When $L = 1$, $Z = \overline{\mathbb{Q}}\boldsymbol{x}$ for some anisotropic vector $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$, since (Z, F) is regular. Then $\sigma = \pm id_Z$, where $-id_Z = \tau_{\boldsymbol{x}}$, and $\mathcal{H}(\sigma) = \sqrt{N}$ by (57).

Then assume $L > 1$. Write A for the $N \times N$ matrix of σ, and I_N for the $N \times N$ identity matrix, so in particular $\mathcal{H}(\sigma) = \mathcal{H}(A)$. Notice that for each $\boldsymbol{x} \in Z$,

$$F(\sigma(\boldsymbol{x}) - \boldsymbol{x}, \sigma(\boldsymbol{x}) + \boldsymbol{x}) = 0. \tag{66}$$

Let $\boldsymbol{x} \in Z$ be the anisotropic vector guaranteed by Lemma 3.6 with $\sigma(\boldsymbol{x}) \pm \boldsymbol{x}$ also anisotropic. For this choice of $\pm$, $\tau_{\sigma(\boldsymbol{x})\pm\boldsymbol{x}}$ fixes $\sigma(\boldsymbol{x}) \mp \boldsymbol{x}$ and maps $\sigma(\boldsymbol{x}) \pm \boldsymbol{x}$ to $-(\sigma(\boldsymbol{x}) \pm \boldsymbol{x})$. Then $2\sigma(\boldsymbol{x}) = (\sigma(\boldsymbol{x})) + (\sigma(\boldsymbol{x}) - \boldsymbol{x})$ will be mapped to $(\sigma(\boldsymbol{x}) \mp \boldsymbol{x}) - (\sigma(\boldsymbol{x}) \pm \boldsymbol{x}) = \mp 2\boldsymbol{x}$. We can therefore observe that if $\sigma(\boldsymbol{x}) - \boldsymbol{x}$ is anisotropic, then

$$\sigma' = \tau_{\sigma(\boldsymbol{x})-\boldsymbol{x}} \circ \sigma \tag{67}$$

fixes $\boldsymbol{x}$. If, on the other hand, $\sigma(\boldsymbol{x}) + \boldsymbol{x}$ is anisotropic, then

$$\sigma' = \tau_{\sigma(\boldsymbol{x})+\boldsymbol{x}} \circ \tau_{\sigma(\boldsymbol{x})} \circ \sigma \tag{68}$$

fixes $\boldsymbol{x}$. In any case, σ' defined either by (67) or (68) is an isometry of the $(L-1)$-dimensional regular bilinear space $(\{\boldsymbol{x}\}^\perp, F)$, where $\{\boldsymbol{x}\}^\perp = \{\boldsymbol{z} \in Z : F(\boldsymbol{x}, \boldsymbol{z}) = 0\}$. Then, by the induction hypothesis,

$$\sigma' = \tau_1 \circ \cdots \circ \tau_l,$$

for some reflections $\tau_1, ..., \tau_l$ with $1 \le l \le 2L - 3$ and

$$\mathcal{H}(\tau_i) \le \left\{ \left(2N^2 3^{\frac{L-2}{2}}\right)^{\frac{(L-1)^2}{2}} \mathcal{H}(F)^{\frac{L-1}{3}} H\left(\{\boldsymbol{x}\}^\perp\right)^{\frac{L-1}{2}} \mathcal{H}(\sigma') \right\}^{5^{L-2}}, \tag{69}$$

for each $1 \le i \le l$, and so

$$\sigma = \sigma'' \circ \tau_1 \circ \cdots \circ \tau_l, \tag{70}$$

for the same $\tau_1, ..., \tau_l$ and $\sigma'' = \tau_{\sigma(\boldsymbol{x})-\boldsymbol{x}}$ or $\sigma'' = \tau_{\sigma(\boldsymbol{x})+\boldsymbol{x}} \circ \tau_{\sigma(\boldsymbol{x})}$, depending on which of $\sigma(\boldsymbol{x}) \pm \boldsymbol{x}$ is anisotropic, so σ is a product of at most $2L - 1$ reflections. Next we are going to produce bounds on their heights. Combining Lemma 6.2 with a bound analogous to that of Lemma 3.2 and with Lemma 3.6, we obtain

$$\mathcal{H}(\tau_{\sigma(\boldsymbol{x})}) \le 4LN^3(N+2)\ 3^{\frac{(L+2)(L-1)}{2}} \mathcal{H}(F) H(Z)^{\frac{L+2}{L}} \mathcal{H}(\sigma)^2. \tag{71}$$

Therefore $\tau_{\sigma(\boldsymbol{x})}$ satisfies (63). Also by Lemma 6.2,

$$\mathcal{H}(\tau_{\sigma(\boldsymbol{x})\pm\boldsymbol{x}}) \le N^3(N+2)\mathcal{H}(F) H(\sigma(\boldsymbol{x}) \pm \boldsymbol{x})^2. \tag{72}$$

Notice that $\sigma(\boldsymbol{x}) \pm \boldsymbol{x} = (A \pm I_N)\boldsymbol{x}$. Then, once again, by a bound analogous to that of Lemma 3.2

$$\mathcal{H}(\sigma(\boldsymbol{x}) \pm \boldsymbol{x}) \le H(\boldsymbol{x})\mathcal{H}(A \pm I_N) \le 2\sqrt{L}\ 3^{\frac{(L+2)(L-1)}{4}} H(Z)^{\frac{L+2}{2L}} \mathcal{H}(A \pm I_N), \tag{73}$$

where the last inequality follows by (20). Combining (73) with Lemma 6.5, we obtain

$$H(\sigma(\boldsymbol{x}) \pm \boldsymbol{x}) \le 4\sqrt{L}\ 3^{\frac{(L+2)(L-1)}{4}} H(Z)^{\frac{L+2}{2L}} \mathcal{H}(A). \tag{74}$$

Combining (72) and (74), we obtain

$$\mathcal{H}(\tau_{\sigma(\boldsymbol{x})\pm\boldsymbol{x}}) \le 16LN^3(N+2)\ 3^{\frac{(L+2)(L-1)}{2}} \mathcal{H}(F) H(Z)^{\frac{L+2}{L}} \mathcal{H}(\sigma)^2, \tag{75}$$

hence $\tau_{\sigma(\boldsymbol{x})\pm\boldsymbol{x}}$ satisfies (63). By combining (67), (68), (57), Lemma 6.6, (71), and

(75), we have

$$\mathcal{H}(\sigma') \le 64L^2N^6(N+2)^2\ 3^{(L+2)(L-1)}\mathcal{H}(F)^2H(Z)^{\frac{2L+4}{L}}\mathcal{H}(\sigma)^5. \tag{76}$$

By Lemma 3.3, Lemma 3.2, and (20)

$$H\left(\{\boldsymbol{x}\}^{\perp}\right) \le \mathcal{H}(F)H(\boldsymbol{x})H(Z) \le 2\sqrt{L}\ 3^{\frac{(L+2)(L-1)}{4}}\mathcal{H}(F)H(Z)^{\frac{3L+2}{2L}}. \tag{77}$$

Then bound (63) follows upon combining (69) with (76) and (77) while keeping in mind that $2 \le L \le N$ and $N+2 \le 2N$. This completes the proof. □

Acknowledgment. I would like to thank Professor Paula Tretkoff for her helpful remarks on the subject of this paper.

References

[1] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.
[2] J.-B. Bost, H. Gillet, and C. Soulé. Heights of projective varieties and positive Green forms. *J. Amer. Math. Soc.*, 7(4):903–1027, 1994.
[3] J. W. S. Cassels. Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 51:262–264, 1955.
[4] L. Fukshansky. On effective Witt decomposition and Cartan-Dieudonné theorem. *to appear in Canad. J. Math., arXiv:math.NT/0501282*.
[5] L. Fukshansky. Search bounds for zeros of polynomials over the algebraic closure of $\mathbb{Q}$. *to appear in Rocky Mountain J. Math., arXiv:math.NT/0512132*.
[6] P. Gordan. Uber den grossten gemeinsamen factor. *Math. Ann.*, 7:443–448, 1873.
[7] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1*. Cambridge Univ. Press, 1947.
[8] C. G. Pinner and J. D. Vaaler. The number of irreducible factors of a polynomial. I. *Trans. Amer. Math. Soc.*, 339(2):809–834, 1993.
[9] S. Raghavan. Bounds of minimal solutions of diophantine equations. *Nachr. Akad. Wiss. Gottingen, Math. Phys. Kl.*, 9:109–114, 1975.
[10] D. Roy and J. L. Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.
[11] L. J. Rylands and D. E. Taylor. Matrix generators for the orthogonal groups. *J. Symbolic Comput.*, 25(3):351–360, 1998.
[12] W. Scharlau. *Quadratic and Hermitian Forms*. Springer-Verlag, 1985.
[13] H. P. Schlickewei. Kleine nullstellen homogener quadratischer gleichungen. *Monatsh. Math.*, 100(1):35–45, 1985.
[14] H. P. Schlickewei and W. M. Schmidt. Quadratic geometry of numbers. *Trans. Amer. Math. Soc.*, 301(2):679–690, 1987.
[15] T. Struppeck and J. D. Vaaler. Inequalities for heights of algebraic subspaces and the Thue-Siegel principle. *Analytic number theory (Allerton Park, IL, 1989), Progr. Math.*, 85:493–528, 1990.
[16] J. D. Vaaler. Small zeros of quadratic forms over number fields. *Trans. Amer. Math. Soc.*, 302(1):281–296, 1987.
[17] J. D. Vaaler. Small zeros of quadratic forms over number fields, II. *Trans. Amer. Math. Soc.*, 313(2):671–686, 1989.

Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, Texas 77843-3368

E-mail address: lenny@math.tamu.edu