1-1-2004

Small Zeros of Quadratic Forms with Linear Conditions

Lenny Fukshansky
Claremont McKenna College

SMALL ZEROS OF QUADRATIC FORMS WITH LINEAR CONDITIONS

Lenny Fukshansky

Abstract. Given a quadratic form and M linear forms in $N+1$ variables with coefficients in a number field K, suppose that there exists a point in K^{N+1} at which the quadratic form vanishes and all the linear forms do not. Then we show that there exists a point like this of relatively small height. This generalizes a result of D.W. Masser.

§1. Introduction and notation.

Let

$$F(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{i=0}^{N} \sum_{j=0}^{N} f_{ij} X_i Y_j$$

be a symmetric bilinear form in $N+1$ variables with coefficients $f_{ij} = f_{ji}$. We write $F = (f_{ij})$ for the associated $(N+1) \times (N+1)$ matrix, and $F(\boldsymbol{X}) = F(\boldsymbol{X}, \boldsymbol{X})$ for the associated quadratic form. First assume that the coefficients f_{ij} are in $\mathbb{Q}$. Suppose there exists a point $\boldsymbol{x} \in \mathbb{Q}^{N+1}$ such that $x_0 \neq 0$ and $F(\boldsymbol{x}) = 0$. In [4] Masser shows that in this case there exists such a point $\boldsymbol{x}$ with

$$H(\boldsymbol{x}) \ll_N H(F)^{(N+1)/2},$$

where H here stands for height of $\boldsymbol{x}$ and F, respectively. This generalizes a well known result of Cassels [2] about the existence of small zeros of quadratic forms with rational coefficients to the existence of small zeros of quadratic polynomials with rational coefficients.

We generalize Masser's result in the following way. Let K be a number field of degree d over $\mathbb{Q}$. Let the coefficients f_{ij} be in K. Let M be a positive integer. Let $L_1(\boldsymbol{X}), ..., L_M(\boldsymbol{X})$ be linear forms in $N+1$ variables with coefficients in K. Suppose there exists a point $\boldsymbol{t} \in K^{N+1}$ such that $F(\boldsymbol{t}) = 0$, and $L_i(\boldsymbol{t}) \neq 0$ for each $1 \leq i \leq M$. Then we prove that there exists such a point of bounded height. The bound on height is in terms of the heights of quadratic and linear forms, and reduces (up to a constant) to Masser's type result over a number field in case $M = 1$ and $L_1(\boldsymbol{X}) = X_0$.

First we set some notation. For a number field K of degree d over $\mathbb{Q}$, we write O_K for the ring of algebraic integers of K and Δ_K for the discriminant of K. Write $M(K)$ for the set of all places of K, and for each $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree, where K_v and $\mathbb{Q}_v$ are completions of K and $\mathbb{Q}$ respectively at the place v. Then if $u \in M(\mathbb{Q})$, let $M_u = \{v \in M(K) : v|u\}$, and we have

$$\sum_{v \in M_u} d_v = d.$$

We normalize our absolute values for $v \in M(K)$ as in [6]:

(1) if $v|p$ then $|p|_v = p^{-d_v/d}$,
(2) if $v|\infty$ then $|\alpha|_v = |\alpha|^{d_v/d}$, where $|\ |$ is the usual Euclidean absolute value on $\mathbb{R}$ or $\mathbb{C}$.

1991 *Mathematics Subject Classification*. Primary 11D09, 11E12; Secondary 11H46.

Then for every $\alpha \in K$, $\alpha \neq 0$, the product formula reads

$$\prod_v |\alpha|_v = 1.$$

For each $v \in M(K)$, we define a local height over K_v by

$$H_v(\boldsymbol{x}) = \max_{0 \leq i \leq N} |x_i|_v,$$

for each $\boldsymbol{x} \in K_v^{N+1}$. Then we have the *homogeneous* global height function on K^{N+1}

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

and the *inhomogeneous height*

$$h(\boldsymbol{x}) = \prod_{v \in M(K)} \max\{1, H_v(\boldsymbol{x})\},$$

for each $\boldsymbol{x} \in K^{N+1}$. We now state a basic well-known property of height functions. Let $\boldsymbol{x}, \boldsymbol{y} \in K^N$, and α, β be positive integers, then

$$H(\alpha \boldsymbol{x} \pm \beta \boldsymbol{y}) \leq h(\alpha \boldsymbol{x} \pm \beta \boldsymbol{y}) \leq (\alpha + \beta) h(\boldsymbol{x}) h(\boldsymbol{y}). \tag{1.1}$$

We define the height of a polynomial to be the height of its coefficient vector.

Let j be a positive integer. Let

(1) $r_v(j) = \pi^{-1/2}\Gamma(j/2+1)^{1/j}$, if $v|\infty$ is real,
(2) $r_v(j) = (2\pi)^{-1/2}\Gamma(j+1)^{1/2j}$, if $v|\infty$ is complex,
(3) $r_v(j) = 1$, if $v \nmid \infty$.

For each j, define a field constant

$$A_K(j) = \left\{ 2^{5j}(j+1)^j |\Delta_K|^{\frac{j+1}{d}} \right\}^{1/2} \prod_{v \in M(K)} r_v(j)^{\frac{jd_v}{d}}. \tag{1.2}$$

Now we can rigorously state the main result of this paper.

Theorem 1.1. *Suppose there exists a point $\boldsymbol{t} \in K^{N+1}$ such that $F(\boldsymbol{t}) = 0$, and $L_i(\boldsymbol{t}) \neq 0$ for each $1 \leq i \leq M$. Then there exists $\boldsymbol{u} \in K^{N+1}$ such that $F(\boldsymbol{u}) = 0$, $L_i(\boldsymbol{u}) \neq 0$ for each $1 \leq i \leq M$, and*

$$H(\boldsymbol{u}) \leq B_K(N,M) H(F)^{\frac{N+2M}{2} + (M-1)(N+2)}, \tag{1.3}$$

as well as

$$H(\boldsymbol{u}) \leq B_K(N,M) H(F)^{\frac{N+1}{2} + (M-1)(N+2)} \prod_{i=1}^{M} H(L_i)^{\frac{(2M-1)N}{M}}, \tag{1.4}$$

and finally

$$H(\boldsymbol{u}) \leq B_K(N,M) H(F)^{\frac{2N+2M+1}{4} + (M-1)(N+2)} \prod_{i=1}^{M} H(L_i)^{\frac{(2M-1)N}{2M}}, \tag{1.5}$$

where the constant $B_K(N,M)$ is given by

$$B_K(N,M) = \frac{1}{192}(N+1)^2 A_K(N) \left\{ 486\ (N+1)^6 A_K(N)^2 \right\}^{M-1} (M+2)! \{(M+3)!\}^2, \tag{1.6}$$

with $A_K(N)$ as in (1.2).

The following result is a simple, but useful corollary of Theorem 1.1 in the case $M = 1$.

Corollary 1.2. *Let $F(\boldsymbol{X})$ be a quadratic form in $N+1$ variables with coefficients in the number field K, as above. Let*

$$\mathcal{V}_K(F) = \left\{ \boldsymbol{t} \in K^{N+1} : F(\boldsymbol{t}) = 0 \right\}.$$

Suppose that there exists a non-singular point $\mathbf{0} \neq \boldsymbol{x} \in \mathcal{V}_K(F)$. Then there exists a non-singular point $\mathbf{0} \neq \boldsymbol{s} \in \mathcal{V}_K(F)$ such that

$$H(\boldsymbol{s}) \leq \max\{3, A_K(N)\}\ H(F)^{\frac{N}{2}}.$$

The structure of this paper is the following. In §2 we produce a solution to the problem in case there is only one linear form, obtaining upper bounds for the inhomogeneous height of the point in question, and proving Corollary 1.2. Our line of argument here follows that of Masser [4]. In the process of proof we state a generalization of Cassels' result on small zeros of quadratic forms, that we use to construct auxiliary points. In §3 we produce an upper bound for the height of a point outside of the collection of subspaces. In §4 we prove Theorem 1.1. It is derived from a slightly more technical result of Theorem 4.1. Our argument is by induction on the number of linear forms, so we use the results of §2 for the base case of the induction, and we use the result of §3 to construct certain auxiliary points. Then we compute bounds on the height. We also remark that one can assume the point $\boldsymbol{u}$ of Theorem 1.1 to be in O_K^{N+1}.

§2. The problem with one linear form. Let $L(\boldsymbol{X})$ be a linear form in $N+1$ variables with coefficients in K, and suppose there exists a point $\boldsymbol{t} \in K^{N+1}$ so that $F(\boldsymbol{t}) = 0$ and $L(\boldsymbol{t}) \neq 0$. We want to show an existence of such a point of small height. The argument of this section parallels that of Masser [4]. We argue by induction on N.

First suppose that $N = 1$, then

$$F(X_0, X_1) = aX_0^2 + bX_0X_1 + cX_1^2,$$

$$L(X_0, X_1) = q_0X_0 + q_1X_1,$$

where $a, b, c, q_0, q_1 \in K$. Since $L(\boldsymbol{X})$ is not identically zero, we can assume without loss of generality that $q_0 \neq 0$. If $a = c = 0$, then $\alpha\{(1,0),(0,1)\}$, $\alpha \in K$, is the zero set of F consisting of two projective points of height 1, and L must not vanish at one of them. Then assume $a \neq 0$. Let $\boldsymbol{x} = (x_0, x_1) \in K^2$ be a non-trivial zero of F, so $x_0, x_1 \neq 0$. Then

$$(x_0, x_1) = x_1 \left(\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, 1 \right),$$

so again the zero set of F consists of only two projective points, and hence L must not vanish at one them. Thus we just have to estimate the heights of these two points. We can assume that $x_1 = 1$, therefore $h(\boldsymbol{x}) = H(\boldsymbol{x})$. A straightforward calculation shows that

$$h(\boldsymbol{x}) \leq 3H(F), \tag{2.1}$$

and this finishes the proof in case $N = 1$.

Now we state a generalized form of Cassels' theorem on small zeros of quadratic forms, that we will use in the proof. The following version is due to Vaaler.

Theorem 2.1. *If a quadratic form F has a nontrivial zero in K^{N+1}, then there exists $\mathbf{0} \neq \boldsymbol{x} \in O_K^{N+1}$ such that $F(\boldsymbol{x}) = 0$, and*

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq A_K(N) H(F)^{N/2}, \tag{2.2}$$

where $A_K(N)$ is as in (1.2).

This follows by combining Theorem 1, Corollary 2 and remark after it of [6] with Corollary 11 of [1].

Remark. A theorem like this has first been proved for the case $K = \mathbb{Q}$ by Cassels in [2], and later generalized to number fields by Raghavan [5] (various other important generalizations of Cassels' result were also carried out by Birch, Davenport, Chalk, Schmidt, Schlickewei, and Vaaler, just to name a few; see [6] for a more detailed account and bibliography).

We return to the proof. Now assume that $N \geq 2$. Then

$$L(\boldsymbol{X}) = \boldsymbol{q} \cdot \boldsymbol{X} = \sum_{i=0}^{N} q_i X_i \in K[X_0, ..., X_N]. \tag{2.3}$$

By Theorem 2.1, there exists $\mathbf{0} \neq \boldsymbol{x} \in K^{N+1}$ such that $F(\boldsymbol{x}) = 0$ and

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq A_K(N) H(F)^{N/2}. \tag{2.4}$$

If $L(\boldsymbol{x}) \neq 0$, we are done, so assume $L(\boldsymbol{x}) = 0$. Again, since $L(\boldsymbol{X})$ is not identically zero, we can assume that for instance $q_0 \neq 0$. This implies that

$$x_0 = -\frac{1}{q_0} \sum_{i=1}^{N} q_i x_i,$$

hence

$$0 = F(\boldsymbol{x}) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} x_i x_j + 2 \sum_{i=1}^{N} f_{0i} x_0 x_i + f_{00} x_0^2 = \sum_{i=1}^{N} \sum_{j=1}^{N} g_{ij} x_i x_j,$$

where for each $1 \leq i, j \leq N$, $g_{ij} = f_{ij} - \frac{2q_j}{q_0} f_{0i} + \frac{f_{00}}{q_0^2} q_i q_j$. Then define a quadratic form G in N variables:

$$G(\boldsymbol{X}) = \sum_{i=1}^{N} \sum_{j=1}^{N} g_{ij} X_i X_j.$$

Notice that $\mathbf{0} \neq (x_1, ..., x_N) \in K^N$, and $G(x_1, ..., x_N) = 0$, hence by Theorem 2.1, there exists $\mathbf{0} \neq \boldsymbol{z} \in K^N$ such that $G(\boldsymbol{z}) = 0$ and

$$H(\boldsymbol{z}) \leq h(\boldsymbol{z}) \leq A_K(N-1) H(G)^{(N-1)/2}.$$

We need a bound on $H(G)$ in terms of $H(F)$ and $H(L)$. Using the fact that $H_v(L) \geq |q_0|_v$ for each $v \in M(K)$ along with ultrametric inequality in the non-archimedean case and triangle inequality in the archimedean case, we obtain

$$H(G) \leq 6 H(F) H(L)^2,$$

therefore

$$H(\boldsymbol{z}) \leq h(\boldsymbol{z}) \leq 6 A_K(N-1) H(F)^{(N-1)/2} H(L)^{N-1}. \tag{2.5}$$

Define

$$y_0 = -\frac{1}{q_0} \sum_{i=1}^{N} q_i z_i,$$

and let $\mathbf{0} \neq \boldsymbol{y} = (y_0, \boldsymbol{z}) \in K^{N+1}$. By construction, $F(\boldsymbol{y}) = L(\boldsymbol{y}) = 0$. Then using (2.5), we obtain

$$H(\boldsymbol{y}) \leq h(\boldsymbol{y}) \leq N \prod_{v \in M(K)} \frac{H_v(L)}{|q_0|_v} \max\{1, H_v(\boldsymbol{z})\} \tag{2.6}$$

$$\leq 6NA_K(N-1)H(F)^{(N-1)/2}H(L)^N.$$

Since the bilinear form F is not identically zero, there must exist a coefficient $f_{ij} \neq 0$. Then without loss of generality, assume $f_{00} = 1$, which implies that

$$\max\{1, H_v(F)\} = H_v(F), \tag{2.7}$$

for each $v \in M(K)$.

Next let $\mathbf{0} \neq \boldsymbol{t}_1, \boldsymbol{t}_2 \in K^{N+1}$, and define

$$\boldsymbol{u}_1 = F(\boldsymbol{t}_1)\boldsymbol{x} - 2F(\boldsymbol{t}_1, \boldsymbol{x})\boldsymbol{t}_1, \tag{2.8}$$

and

$$\boldsymbol{u}_2 = F(\boldsymbol{t}_2)\boldsymbol{y} - 2F(\boldsymbol{t}_2, \boldsymbol{y})\boldsymbol{t}_2. \tag{2.9}$$

It is easy to check that $F(\boldsymbol{u}_1) = F(\boldsymbol{u}_2) = 0$. Let

$$\mathcal{V}_K(F) = \left\{\boldsymbol{t} \in K^{N+1} : F(\boldsymbol{t}) = 0\right\}.$$

Lemma 2.2. *Suppose that $\boldsymbol{x}, \boldsymbol{y}$ are non-singular points in the variety $\mathcal{V}_K(F)$. Then there exist $\mathbf{0} \neq \boldsymbol{t}_1, \boldsymbol{t}_2 \in K^{N+1}$ with coordinates $0, \pm 1$ such that $L(\boldsymbol{u}_1), L(\boldsymbol{u}_2) \neq 0$.*

Proof. We will go through the construction of $\boldsymbol{t}_1$, and the construction of $\boldsymbol{t}_2$ is identical. Since $L(\boldsymbol{x}) = 0$, we want to construct $\boldsymbol{t}_1 \in K^{N+1}$ such that the following holds:

(1) $t_{10} \neq -\frac{1}{q_0}\sum_{i=1}^N q_i t_{1i}$,
(2) $F(\boldsymbol{t}_1, \boldsymbol{x}) \neq 0$,
(3) $t_{1i} = 0, \pm 1 \ \ \forall \ \ 0 \leq i \leq N$.

Notice that (1) is equivalent to $L(\boldsymbol{t}_1) \neq 0$, and (2) is possible since $\boldsymbol{x}$ is non-singular in $\mathcal{V}_K(F)$. Write $\boldsymbol{e}_0, ..., \boldsymbol{e}_N$ for the standard basis vectors. Each $\boldsymbol{e}_i$ satisfies (3). There exists $\boldsymbol{e}_i$ satisfying (1). If $\boldsymbol{e}_i$ satisfies (2), let $\boldsymbol{t}_1 = \boldsymbol{e}_i$. Otherwise, there exists $\boldsymbol{e}_j$ satisfying (2), and $i \neq j$. If $\boldsymbol{e}_j$ satisfies (1), let $\boldsymbol{t}_1 = \boldsymbol{e}_j$. If not, then let $\boldsymbol{t}_1 = \boldsymbol{e}_i + \boldsymbol{e}_j$, and we are done. □

Assume $\boldsymbol{x}, \boldsymbol{y}$ are non-singular points in the variety $\mathcal{V}_K(F)$. Make the choice of $\boldsymbol{t}_1, \boldsymbol{t}_2$ in (2.8), (2.9) as in Lemma 2.2. Then $F(\boldsymbol{u}_1) = F(\boldsymbol{u}_2) = 0$, $L(\boldsymbol{u}_1), L(\boldsymbol{u}_2) \neq 0$. We want to estimate heights of $\boldsymbol{u}_1, \boldsymbol{u}_2$.

Lemma 2.3. *If $\boldsymbol{t}, \boldsymbol{w} \in K^{N+1}$, and $\boldsymbol{u} = F(\boldsymbol{t})\boldsymbol{w} - 2F(\boldsymbol{t}, \boldsymbol{w})\boldsymbol{t}$, then*

$$H(\boldsymbol{u}) \leq h(\boldsymbol{u}) \leq 3(N+1)^2 H(F)h(\boldsymbol{w})h(\boldsymbol{t})^2. \tag{2.10}$$

Proof. If $v \nmid \infty$, then $|2|_v \leq 1$, and so

$$\max\{1, H_v(\boldsymbol{u})\} \leq \max\left\{1, |F(\boldsymbol{t})|_v H_v(\boldsymbol{w}), |2|_v |F(\boldsymbol{t}, \boldsymbol{w})|_v H_v(\boldsymbol{t})\right\}$$

$$\leq \max\{1, H_v(F)H_v(\boldsymbol{w})H_v(\boldsymbol{t})^2\} \leq \max\{1, H_v(F)\}\max\{1, H_v(\boldsymbol{w})\}\max\{1, H_v(\boldsymbol{t})\}^2$$

$$= H_v(F)\max\{1, H_v(\boldsymbol{w})\}\max\{1, H_v(\boldsymbol{t})\}^2,$$

where the last equality follows by (2.7). If $v|\infty$, then

$$H_v(\boldsymbol{u}) \leq |F(\boldsymbol{t})|_v H_v(\boldsymbol{w}) + 2|F(\boldsymbol{t}, \boldsymbol{w})|_v H_v(\boldsymbol{t}) \leq \{3(N+1)^2\}^{d_v/d} H_v(F)H_v(\boldsymbol{w})H_v(\boldsymbol{t})^2,$$

and so

$$\max\{1, H_v(\boldsymbol{u})\} \le \{3(N+1)^2\}^{d_v/d} \max\{1, H_v(F)H_v(\boldsymbol{w})H_v(\boldsymbol{t})^2\}$$
$$\le \{3(N+1)^2\}^{d_v/d} \max\{1, H_v(F)\} \max\{1, H_v(\boldsymbol{w})\} \max\{1, H_v(\boldsymbol{t})\}^2$$
$$= \{3(N+1)^2\}^{d_v/d} H_v(F) \max\{1, H_v(\boldsymbol{w})\} \max\{1, H_v(\boldsymbol{t})\}^2,$$

where the last equality follows by (2.7). Then (2.10) follows by taking a product. □

By Lemma 2.2, $h(\boldsymbol{t}_1) = h(\boldsymbol{t}_2) = 1$, and so by Lemma 2.3, (2.4), and (2.6) we have

$$h(\boldsymbol{u}_1) \le 3(N+1)^2 H(F) h(\boldsymbol{x}) \le 3(N+1)^2 A_K(N) H(F)^{(N+2)/2}, \tag{2.11}$$

and

$$h(\boldsymbol{u}_2) \le 3(N+1)^2 H(F) h(\boldsymbol{y}) \le 18N(N+1)^2 A_K(N-1) H(F)^{(N+1)/2} H(L)^N. \tag{2.12}$$

Next we consider the "singular" case.

Proposition 2.4. *Assume that $\boldsymbol{x}$ is a singular point in the variety $\mathcal{V}_K(F)$. Then there exists a point $\boldsymbol{s} \in K^{N+1}$ so that $F(\boldsymbol{s}) = 0$, $L(\boldsymbol{s}) \neq 0$, and*

$$H(\boldsymbol{s}) \le h(\boldsymbol{s}) \le 3H(F)^{N/2}. \tag{2.13}$$

Proof. Here the idea is as in [4], to reduce to fewer variables keeping coefficients under control and to use induction. If $N = 1$, (2.13) is just (2.1). Then assume that $N \ge 2$, and that (2.13) has been proved for $N-1$. Without loss of generality, assume that $x_N \neq 0$. Then $\boldsymbol{x}$ is linearly independent of the first N standard unit vectors $\boldsymbol{e}_0, ..., \boldsymbol{e}_{N-1}$, so we can define new variables $Y_0, ..., Y_N$ by

$$\boldsymbol{X} = (X_0, ..., X_N) = Y_0\boldsymbol{e}_0 + ... + Y_{N-1}\boldsymbol{e}_{N-1} + Y_N\boldsymbol{x}. \tag{2.14}$$

We have

$$F(\boldsymbol{X}) = F\left(\sum_{i=0}^{N-1} Y_i\boldsymbol{e}_i\right) + Y_N^2 F(\boldsymbol{x}) + 2F\left(\sum_{i=0}^{N-1} Y_i\boldsymbol{e}_i, Y_N\boldsymbol{x}\right) = F\left(\sum_{i=0}^{N-1} Y_i\boldsymbol{e}_i\right),$$

since $F(\boldsymbol{x}) = 0$, and $\boldsymbol{x}$ is a singular point in V, i.e. $F(\boldsymbol{t}, \boldsymbol{x}) = 0$ for all $\boldsymbol{t} \in K^{N+1}$. Then define a new quadratic form Q in N variables $Y_0, ..., Y_{N-1}$ by

$$Q(\boldsymbol{Y}) = F\left(\sum_{i=0}^{N-1} Y_i\boldsymbol{e}_i\right),$$

and so $F(\boldsymbol{X}) = Q(\boldsymbol{Y})$. Clearly, the coefficients of Q form a subset of coefficients of F, and hence

$$H(Q) \le H(F). \tag{2.15}$$

There exists a $\boldsymbol{t} \in K^{N+1}$ so that $F(\boldsymbol{t}) = 0$, and $L(\boldsymbol{t}) \neq 0$. Let $\boldsymbol{w} = (w_0, ..., w_{N-1})$ be the vector that corresponds to $\boldsymbol{t}$ under the coordinate change (2.14) and reduction to N variables. Then

$$0 \neq L(\boldsymbol{t}) = L\left(\sum_{i=0}^{N-1} w_i\boldsymbol{e}_i\right) + \frac{t_N}{x_N} L(\boldsymbol{x}) = L\left(\sum_{i=0}^{N-1} w_i\boldsymbol{e}_i\right),$$

since $L(\boldsymbol{x}) = 0$. Then define a new linear form L_1 in N variables $Y_0, ..., Y_{N-1}$ by

$$L_1(\boldsymbol{Y}) = L\left(\sum_{i=0}^{N-1} Y_i \boldsymbol{e}_i\right),$$

and so $L_1(\boldsymbol{w}) \neq 0$, and

$$H(L_1) \leq H(L),$$

since coefficents of L_1 form a subset of coefficients of L. We also know that $Q(\boldsymbol{w}) = F(\boldsymbol{t}) = 0$. Therefore, by induction hypothesis, there exists $\boldsymbol{u} \in K^N$ such that $Q(\boldsymbol{u}) = 0$, $L_1(\boldsymbol{u}) \neq 0$, and

$$h(\boldsymbol{u}) \leq 3H(Q)^{N/2} \leq 3H(F)^{N/2},$$

by (2.15). Define $\boldsymbol{s} = (\boldsymbol{u}, 0) \in K^{N+1}$, and then $F(\boldsymbol{s}) = Q(\boldsymbol{u}) = 0$, $L(\boldsymbol{s}) = L_1(\boldsymbol{u}) \neq 0$, and $h(\boldsymbol{s}) = h(\boldsymbol{u})$. This completes the proof. □

Now notice that if $N \geq 1$, $3(N+1)^2 A_K(N) > 3$, as well as for each $N \geq 2$, $(N+1)^2 A_K(N) \geq N(N+1)^2 A_K(N-1)$. Putting this together with (2.11), (2.12), and (2.13), we have proved the following theorem.

Theorem 2.5. *Let the notation be as above. Suppose there exists a point $\boldsymbol{t} \in K^{N+1}$ such that $F(\boldsymbol{t}) = 0$, and $L(\boldsymbol{t}) \neq 0$. Then there exists $\boldsymbol{u} \in K^{N+1}$ such that $F(\boldsymbol{u}) = 0$, $L(\boldsymbol{u}) \neq 0$, and*

$$H(\boldsymbol{u}) \leq h(\boldsymbol{u}) \leq 18(N+1)^2 A_K(N) H(F)^{(N+1)/2} \min\left\{H(F)^{1/2}, H(L)^N\right\}. \tag{2.16}$$

Proof of Corollary 1.2. Let $\boldsymbol{x}$ be the zero of F guranteed by Theorem 2.1. If $\boldsymbol{x}$ is non-singular, we are done. If $\boldsymbol{x}$ is singular, let $L(\boldsymbol{X}) = \frac{\partial F}{\partial X_i}$ for some $0 \leq i \leq N$, so $L(\boldsymbol{x}) = 0$. Then by Proposition 2.4, there must exist $\boldsymbol{s} \in K^{N+1}$ so that $F(\boldsymbol{s}) = 0$, $L(\boldsymbol{s}) \neq 0$, and

$$H(\boldsymbol{s}) \leq h(\boldsymbol{s}) \leq 3H(F)^{N/2}.$$

□

§**3. Points of small height outside of a collection of subspaces.** Let M, N be positive integers, and let K be a number field of degree d over $\mathbb{Q}$. Keeping all the notation as before, we prove the existence of a point of small height at which none of M linear forms in N variables with coefficients in K vanish.

In fact, we consider a more general situation and produce a basic result. Let $v \in M(K)$ be any place of K, and let

$$\mathcal{S}_M = \{\boldsymbol{\alpha} \in \mathbb{Z}^N_{\geq 0} : \alpha_1 + ... + \alpha_N \leq M\}.$$

Then let

$$U(X_1, ..., X_N) = \sum_{\boldsymbol{\alpha} \in \mathcal{S}_M} c(\boldsymbol{\alpha}) X_1^{\alpha_1} ... X_N^{\alpha_N} \in K_v[X_1, ..., X_N],$$

be a polynomial in N variables of degree M. If k is a positive integer, then for each vector $\boldsymbol{x} \in \mathbb{Z}^k$ write

$$|\boldsymbol{x}| = \max\{|x_1|, ..., |x_k|\}.$$

The idea for the following argument was suggested to me by Sinnou David, [3].

Theorem 3.1. *Let the notation be as above, and suppose $U(\boldsymbol{X})$ is not identically 0. Then there exists $\boldsymbol{x} \in \mathbb{Z}^N$ such that $U(\boldsymbol{x}) \neq 0$ and $|\boldsymbol{x}| \leq \left[\frac{\deg(U)}{2}\right] + 1 = \left[\frac{M}{2}\right] + 1$.*

Proof. We argue by induction on N. First suppose $N = 1$. Then our polynomial is of the form

$$U(X) = c_M X^M + ... + c_1 X + c_0 \in K_v[X],$$

and U has at most M integer roots. Hence there must exist $x \in \mathbb{Z}$ such that $U(x) \neq 0$ and $|x| \leq \left[\frac{M}{2}\right] + 1$. Now suppose the theorem has been proved for all polynomials in k variables for any $1 \leq k < N$. Notice that for each $1 \leq i \leq N$, $\deg_{X_i}(U) \leq \deg(U) = M$, where $\deg_{X_i}(U)$ is the degree of U in the variable X_i.

There must exist $\boldsymbol{q} \in \mathbb{Z}^{N-1}$ such that $U(\boldsymbol{q}, X_N)$ is not identically 0. Indeed, suppose it is not so. Then U vanishes on all of $\mathbb{Z}^N$, which by continuity implies that U is identically 0.

Since $U(\boldsymbol{q}, X_N)$ is a polynomial in one variable, by the base of induction there exists $q_N \in \mathbb{Z}$ such that $U(\boldsymbol{q}, q_N) \neq 0$ and $|q_N| \leq \left[\frac{M}{2}\right] + 1$. Let

$$P(X_1, ..., X_{N-1}) = U(X_1, ..., X_{N-1}, q_N),$$

then P is not identically 0, and $\deg(P) \leq M$. By induction hypothesis, there exists $\boldsymbol{x} \in \mathbb{Z}^{N-1}$ such that $P(\boldsymbol{x}) \neq 0$ and $|\boldsymbol{x}| \leq \left[\frac{M}{2}\right] + 1$. Then $(\boldsymbol{x}, q_N) \in \mathbb{Z}^N$, $U(\boldsymbol{x}, q_N) = P(\boldsymbol{x}) \neq 0$, and $|(\boldsymbol{x}, q_N)| \leq \left[\frac{M}{2}\right] + 1$. □

Corollary 3.2. *Let the notation and assumptions be as in Theorem 3.1. Then there exists $\boldsymbol{x} \in O_K^N$ such that $U(\boldsymbol{x}) \neq 0$ and $H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq \left[\frac{\deg(U)}{2}\right] + 1 = \left[\frac{M}{2}\right] + 1$.*

Proof. The point $\boldsymbol{x}$ obtained in Theorem 3.1 is in $\mathbb{Z}^N \subseteq O_K^N$, and so

$$h(\boldsymbol{x}) \leq \prod_{v|\infty} \max\{1, |\boldsymbol{x}|_v\} = \prod_{v|\infty} \max\{1, |\boldsymbol{x}|\}^{d_v/d} = |\boldsymbol{x}|.$$

The result follows. □

Considering the special case when $U(\boldsymbol{X}) = \prod_{i=1}^M L_i(\boldsymbol{X})$ is decomposable into a product of M linear forms $L_1, ..., L_M$, we conclude that there exists a point $\boldsymbol{x} \in K^N$ at which none of the linear forms vanish and $h(\boldsymbol{x}) \leq \frac{M+2}{2}$.

§**4. Proof of Theorem 1.1.** Let M and N be positive integers. Let F be a quadratic form in $N+1$ variables with coefficients in a number field K of degree d, as above. Let $L_1, ..., L_M$ be linear forms in $N+1$ variables with coefficients in K.

Theorem 4.1. *Suppose there exists a point $\boldsymbol{t} \in K^{N+1}$ such that $F(\boldsymbol{t}) = 0$, and $L_i(\boldsymbol{t}) \neq 0$ for each $1 \leq i \leq M$. Then there exists $\boldsymbol{u} \in K^{N+1}$ such that $F(\boldsymbol{u}) = 0$, $L_i(\boldsymbol{u}) \neq 0$ for each $1 \leq i \leq M$, and*

$$H(\boldsymbol{u}) \leq h(\boldsymbol{u}) \leq B_K(N, M) H(F)^{\frac{N+1}{2} + (M-1)(N+2)} \prod_{i=1}^M \mathcal{M}_i^{2 - \frac{1}{M}},$$

where

$$\mathcal{M}_i = \min\left\{H(F)^{1/2}, H(L_i)^N\right\}, \tag{M}$$

and the constant $B_K(N, M)$ is as in (1.6).

Proof. We will actually prove a slightly stronger upper bound:

$$(*) \qquad h(\boldsymbol{u}) \leq B_K(N,M)H(F)^{\frac{N+1}{2}+(M-1)(N+2)}\mathcal{M}_1\prod_{i=2}^{M}\mathcal{M}_i^2.$$

We argue by induction on M. If $M=1$, then Theorem 4.1 follows from Theorem 2.5. So suppose $M\geq 2$, and that theorem has been proved for any subset of $L_1,...,L_M$ of k linear forms, where $1\leq k\leq M-1$. Then there exist points $\boldsymbol{x},\boldsymbol{y}\in K^{N+1}$ such that $F(\boldsymbol{x})=F(\boldsymbol{y})=0$, $L_i(\boldsymbol{x})\neq 0$ for every $1\leq i\leq M-1$, $L_M(\boldsymbol{y})\neq 0$, and

$$h(\boldsymbol{x}) \leq B_K(N,M-1)H(F)^{\frac{N+1}{2}+(M-2)(N+2)}\mathcal{M}_1\prod_{i=2}^{M-1}\mathcal{M}_i^2, \tag{4.1}$$

$$h(\boldsymbol{y}) \leq 18(N+1)^2A_K(N)H(F)^{(N+1)/2}\mathcal{M}_M. \tag{4.2}$$

Notice that if $b<a$ are positive integers, we interpret $\prod_{i=a}^{b}$ as 1. If $L_M(\boldsymbol{x})\neq 0$ or $L_i(\boldsymbol{y})\neq 0$ for all $1\leq i\leq M-1$, then we are done. So assume it is not so. Then there exists a k, such that $1\leq k<M-1$ and by reordering the linear forms if necessary we have

(1) $L_i(\boldsymbol{x})\neq 0$, $L_i(\boldsymbol{y})\neq 0$, for all $1\leq i\leq k$,
(2) $L_i(\boldsymbol{x})\neq 0$, $L_i(\boldsymbol{y})=0$, for all $k<i\leq M-1$,
(3) $L_M(\boldsymbol{x})=0$, $L_M(\boldsymbol{y})\neq 0$.

Notice that for every $k<i\leq M$, $L_i(\boldsymbol{x}+\boldsymbol{y})\neq 0$. In fact, there exists a positive integer β such that for all $1\leq i\leq M$,

$$L_i(\boldsymbol{x}\pm\beta\boldsymbol{y})\neq 0,$$

for the same choice of $\pm$. For this, β needs to be such that for the same choice of $\pm$ none of the linear equations in β

$$L_i(\boldsymbol{x})\pm\beta L_i(\boldsymbol{y})=0, \quad 1\leq i\leq k\leq M-2,$$

are true. There are at most $M-2$ such equations, and since we can also choose $\pm$, there exists such a β so that

$$1\leq\beta\leq\left[\frac{M-2}{2}\right]+1\leq\frac{M}{2}. \tag{4.3}$$

Define

$$\boldsymbol{u}=\boldsymbol{x}\pm\beta\boldsymbol{y},$$

for this choice of $\pm$ and β.

Case 1. Suppose $F(\boldsymbol{x},\boldsymbol{y})=0$. Then

$$F(\boldsymbol{u})=F(\boldsymbol{x})+\beta^2F(\boldsymbol{y})\pm 2\beta F(\boldsymbol{x},\boldsymbol{y})=0,$$

and

$$L_i(\boldsymbol{u})\neq 0, \quad \forall\ 1\leq i\leq M.$$

Combining (1.1) and (4.3) we obtain

$$h(\boldsymbol{u})\leq(\beta+1)h(\boldsymbol{x})h(\boldsymbol{y})\leq\left(\frac{M+2}{2}\right)h(\boldsymbol{y})h(\boldsymbol{x}). \tag{4.4}$$

Case 2. Suppose $F(\boldsymbol{x},\boldsymbol{y}) \neq 0$. By Corollary 3.2, there exists $\boldsymbol{w} \in K^{N+1}$ such that $L_i(\boldsymbol{w}) \neq 0$ for each $1 \leq i \leq M$ and

$$h(\boldsymbol{w}) \leq \frac{M+2}{2}. \tag{4.5}$$

If $F(\boldsymbol{w}) = 0$, we are done. Assume it is not so. Let β be a positive integer, and define

$$\boldsymbol{u} = F(\boldsymbol{y} \pm \beta\boldsymbol{w})\boldsymbol{x} - 2F(\boldsymbol{x}, \boldsymbol{y} \pm \beta\boldsymbol{w})(\boldsymbol{y} \pm \beta\boldsymbol{w}).$$

Notice that $F(\boldsymbol{u}) = 0$. We want to choose $\pm\beta$ in such a way that the following is true:

(1) $F(\boldsymbol{y} \pm \beta\boldsymbol{w}) = \beta(\beta F(\boldsymbol{w}) \pm 2F(\boldsymbol{y},\boldsymbol{w})) \neq 0$,
(2) $F(\boldsymbol{x}, \boldsymbol{y} \pm \beta\boldsymbol{w}) = F(\boldsymbol{x},\boldsymbol{y}) \pm \beta F(\boldsymbol{x},\boldsymbol{w}) \neq 0$,
(3) $L_i(\boldsymbol{u}) = F(\boldsymbol{y} \pm \beta\boldsymbol{w})L_i(\boldsymbol{x}) - 2F(\boldsymbol{x}, \boldsymbol{y} \pm \beta\boldsymbol{w})(L_i(\boldsymbol{y}) \pm \beta L_i(\boldsymbol{w})) \neq 0$, for each $1 \leq i \leq M$.

It is not difficult to see that (1), (2), (3) amount to a total of 2 linear and M quadratic expressions in β. Selecting $\pm$ appropriately we see that there exists a positive integer β such that (1), (2), (3) are satisfied, and

$$\beta \leq M + 2. \tag{4.6}$$

By the same argument as in §2, we can assume without loss of generality that $f_{00} = 1$. Then, for this choice of $\pm\beta$, Lemma 2.3, (1.1), (4.5), and (4.6) imply that

$$\begin{aligned} h(\boldsymbol{u}) &\leq 3(N+1)^2 H(F) h(\boldsymbol{x}) h(\boldsymbol{y} \pm \beta\boldsymbol{w})^2 \\ &\leq 3(N+1)^2(\beta+1)^2 \left(\frac{M+2}{2}\right) H(F) h(\boldsymbol{x}) h(\boldsymbol{y})^2 \\ &\leq \frac{3}{2}(N+1)^2(M+2)(M+3)^2 H(F) h(\boldsymbol{x}) h(\boldsymbol{y})^2. \end{aligned} \tag{4.7}$$

Combining (4.2), (4.4), and (4.7), we have proved that there exists $\boldsymbol{u} \in K^{N+1}$ such that $F(\boldsymbol{u}) = 0$, $L_i(\boldsymbol{u}) \neq 0$ for each $1 \leq i \leq M$, and

$$h(\boldsymbol{u}) \leq 486(N+1)^6 A_K(N)^2 (M+2)(M+3)^2 H(F)^{N+2} \mathcal{M}_M^2 h(\boldsymbol{x}). \tag{4.8}$$

This proves (*). Notice that the ordering of linear forms was arbitrary, so assume that $\mathcal{M}_1 = \max_{1 \leq i \leq M} \mathcal{M}_i$. Then $\mathcal{M}_1 \geq \mathcal{M}_1^{1/M} ... \mathcal{M}_M^{1/M}$, and so

$$\mathcal{M}_1 \prod_{i=2}^{M} \mathcal{M}_i^2 \leq \prod_{i=1}^{M} \mathcal{M}_i^{2-\frac{1}{M}}. \tag{4.9}$$

The theorem follows by combining (4.8) with (4.1) and (4.9). □

To derive Theorem 1.1, notice that for each $1 \leq i \leq M$, the following inequalities hold:

$$\mathcal{M}_i \leq H(F)^{1/2}, \quad \mathcal{M}_i \leq H(L_i)^N, \quad \mathcal{M}_i \leq H(F)^{1/4} H(L_i)^{N/2}.$$

Combining these with the inequality of Theorem 4.1 produces (1.3), (1.4), and (1.5) respectively.

Remark. Let $\boldsymbol{u}$ be the point of Theorem 1.1. Since $H_v(\boldsymbol{u}) = 1$ for all but finitely many places of K, the Strong Approximation Theorem guarantees the existence of $0 \neq \alpha \in K$ such that $\alpha\boldsymbol{u} \in O_K^{N+1}$, and of course $H(\alpha\boldsymbol{u}) = H(\boldsymbol{u})$. From this, it is also an easy exercise to produce an upper bound on $H_\infty(\alpha\boldsymbol{u}) = \prod_{v|\infty} H_v(\alpha\boldsymbol{u})$. The exponents in the upper bound turn out to be the same as in Theorem 1.1, and the constant is only slightly larger.

Aknowledgements. I would like to express my deep gratitude to Professor Jeffrey D. Vaaler for his valuable advice and numerous helpful conversations on the subject of this paper. I would also like to thank Professor Sinnou David for his helpful idea that I used in §4, and the referee for his useful comments and simplifications of some arguments.

References

1. E. Bombieri, J. D. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11–32.
2. J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. **51** (1955), 262–264.
3. S. David, personal communication.
4. D. W. Masser, *How to solve a quadratic equation in rationals*, Bull. London Math. Soc. **30** (1998), 24–28.
5. S. Raghavan, *Bounds of minimal solutions of diophantine equations*, Nachr. Akad. Wiss. Gottingen, Math. Phys. Kl. **9** (1975), 109–114.
6. J. D. Vaaler, *Small zeros of quadratic forms over number fields*, Trans. Amer. Math. Soc. **302** (1987), 281–296.

Department of Mathematics, The University of Texas at Austin, Austin, Texas 78712
E-mail address: lenny@math.utexas.edu