

SMALL REPRESENTATIONS OF INTEGERS BY INTEGRAL QUADRATIC FORMS

WAI KIU CHAN AND LENNY FUKSHANSKY

ABSTRACT. Given an isotropic quadratic form over a number field which assumes a value t , we investigate the distribution of points at which this value is assumed. Building on the previous work about the distribution of small-height zeros of quadratic forms, we produce bounds on height of points outside of some algebraic sets in a quadratic space at which the form assumes the value t . Our bounds on height are explicit in terms of the heights of the form, the space, the algebraic set and the value t .

1. INTRODUCTION AND STATEMENT OF RESULTS

The question of effective distribution of zeros of quadratic forms has a long history. In particular, the famous Cassels' theorem (1955) asserts that an isotropic rational quadratic form has zeros of bounded height with effective bounds depending on the height of this form, [2]. By height here we mean a height function, a standard tool of Diophantine geometry, measuring the arithmetic complexity of an object; we provide a brief overview of height functions in Section 2. There have been many extensions and generalizations of Cassels theorem over the years, see [7] for a survey of this lively area. In particular, in the recent years there have been several results assessing the distribution of small-height zeros by proving that they cannot be easily “cut-out” by any finite union of linear subspaces or even projective varieties not completely containing the quadratic hypersurface in question. Specifically, results of [6], [5], [3], [8] prove existence of zeros of bounded height of an isotropic quadratic form outside of a union of projective varieties. One may wonder if the same type of results hold for other values of a quadratic form. Namely, if K is a number field, Q is a nonzero quadratic form on a subspace V of K^n and t is an element of K represented by (V, Q) , can the small-height points $z \in V$ with $Q(z) = t$ be efficiently “cut-out” by sufficiently simple algebraic sets? This question can be viewed as an inhomogeneous analogue of the problem about small-height zeros. To state our results, let us start with some notation.

Let K be a number field and \mathcal{O}_K its ring of integers. Let $j \geq 1$ be an integer. For each $1 \leq i \leq j$, let \mathcal{S}_i be a finite set of polynomials in $K[X_1, \dots, X_n]$ and $Z_K(\mathcal{S}_i)$ be its zero set in K^n , that is,

$$Z_K(\mathcal{S}_i) = \{\mathbf{x} \in K^n : P(\mathbf{x}) = 0 \text{ for all } P \in \mathcal{S}_i\}.$$

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

Key words and phrases. heights, quadratic forms.

The second author was partially supported by the Simons Foundation grant #519058.

For the collection $\mathbf{s} := \{\mathcal{S}_1, \dots, \mathcal{S}_j\}$ of finite sets of polynomials, define

$$(1) \quad \mathcal{Z}_{\mathbf{s}} := \bigcup_{i=1}^j Z_K(\mathcal{S}_i),$$

and

$$(2) \quad M_{\mathbf{s}} := \sum_{i=1}^j \max\{\deg P : P \in \mathcal{S}_i\}.$$

The set $\mathcal{Z}_{\mathbf{s}}$ defined in (1) is said to be *homogeneous* if all the polynomials in the sets $\mathcal{S}_1, \dots, \mathcal{S}_j$ are homogeneous polynomials. When $\mathcal{Z}_{\mathbf{s}}$ is not homogeneous, we will sometimes need the *homogenization* of $\mathcal{Z}_{\mathbf{s}}$, defined as follows. Introducing one more variable X_{n+1} , we define the homogenization $P^*(X_1, \dots, X_{n+1}) \in K[X_1, \dots, X_{n+1}]$ of each polynomial $P(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ to be the unique homogeneous polynomial such that $\deg P^* = \deg P$ and

$$P(X_1, \dots, X_n) = P^*(X_1, \dots, X_n, 1),$$

and for each $1 \leq i \leq j$, let $\mathcal{S}_i^* = \{P^* : P \in \mathcal{S}_i\}$. Then define $\mathbf{s}^* = \{\mathcal{S}_1^*, \dots, \mathcal{S}_j^*\}$ and, as above, let $Z_K(\mathcal{S}_i^*) = \{\mathbf{x} \in K^{n+1} : P^*(\mathbf{x}) = 0 \text{ for all } P \in \mathcal{S}_i\}$, as well as

$$(3) \quad \mathcal{Z}_{\mathbf{s}^*} := \bigcup_{i=1}^j Z_K(\mathcal{S}_i^*).$$

Then $\mathcal{Z}_{\mathbf{s}^*}$ is a homogeneous algebraic set in K^{n+1} , while clearly

$$M_{\mathbf{s}^*} := \sum_{i=1}^j \max\{\deg P^* : P \in \mathcal{S}_i\} = M_{\mathbf{s}}.$$

We also write H and h for the homogeneous and inhomogeneous height function, respectively, to be defined in Section 2. Further, if $V \subseteq K^n$ and $Q(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ is a quadratic form in n variables, we refer to the pair (V, Q) as a quadratic space (over K). This quadratic space is called isotropic if there exists $\mathbf{0} \neq \mathbf{x} \in V$ such that $Q(\mathbf{x}) = 0$. A totally isotropic subspace of V is a subspace of V on which Q vanishes identically. A maximal totally isotropic subspace of V is the largest totally isotropic subspace of V with respect to inclusion. The orthogonal complement of V in K^n is defined to be

$$\perp_Q(V) := \{\mathbf{x} \in K^n : Q(\mathbf{x}, \mathbf{y}) = 0 \text{ for all } \mathbf{y} \in V\},$$

where $Q(\mathbf{x}, \mathbf{y})$ is the associated symmetric bilinear form. It is easy to see that $\perp_Q(V)$ is a subspace of K^n . The radical V^\perp of (V, Q) is defined to be the subspace of singular points in V with respect to Q , i.e.

$$V^\perp := \{\mathbf{x} \in V : Q(\mathbf{x}, \mathbf{y}) = 0 \text{ for all } \mathbf{y} \in V\}.$$

Then $\dim(V) + \dim(\perp_Q(V)) - \dim(V^\perp) = n$. The quadratic space (V, Q) is called regular if $V^\perp = \{\mathbf{0}\}$; we may also say that Q is regular on V , or simply that Q is regular if $V = K^n$. The dimension of a maximal totally isotropic subspace of a regular quadratic space V is called the Witt index of V . With this notation and terminology, here is a simplified version of a result of [8] (which is an improvement of the previous similar results [3], [5], [6]), adapted to our purposes.

Theorem 1.1 ([8], Theorem 7.1). *Let Q be a nonzero quadratic form in n variables over K , V be an m -dimensional subspace of K^n , and w be the dimension of a maximal totally isotropic subspace of the quadratic space (V, Q) . Let \mathcal{Z}_s be a homogeneous algebraic set as in (1) such that Q has a nontrivial zero in $V \setminus \mathcal{Z}_s$. Then there exists a nontrivial zero $\mathbf{x} \in (V \cap \mathcal{O}_K^n) \setminus \mathcal{Z}_s$ of Q such that*

$$(4) \quad H(\mathbf{x}) \ll H(Q)^{\frac{m-w+1}{2}} H(V)^2,$$

where the implied constant depends only on K , m and M_s .

Remark 1.1. Here and in the rest of the paper we choose not to explicitly specify the dimensional and field constants: their importance is marginal while their form often gets complicated. This being said, all the results of this paper are effective in that these constants can be explicitly computed.

Results like Theorem 1.1 are usually stated with the point \mathbf{x} in question having coordinates in K . It is however always possible to find some $a \in \mathcal{O}_K$ such that $a\mathbf{x} \in \mathcal{O}_K^n$; since $Q(a\mathbf{x}) = a^2Q(\mathbf{x}) = 0$ and the homogeneous height $H(a\mathbf{x}) = H(\mathbf{x})$, we can simply assume that $\mathbf{x} \in \mathcal{O}_K^n$. On the other hand, the distinction between points in K^n and \mathcal{O}_K^n is more subtle in the inhomogeneous situations. For any $0 \neq t \in Q(V)$, let $Q_t(X_1, \dots, X_n) := Q(X_1, \dots, X_n) - t$ and $Q_t^*(X_1, \dots, X_{n+1})$ be its homogenization as defined earlier. Here is the first ‘‘inhomogeneous’’ observation, which we derive from Theorem 1.1 in Section 3.

Theorem 1.2. *Let Q be a nonzero quadratic form in n variables over K and let $V \subseteq K^n$ be an m -dimensional subspace, $m \leq n$. Let $w \geq 0$ be the dimension of a maximal totally isotropic subspace of the quadratic space (V, Q) . Let $0 \neq t \in Q(V)$ and \mathcal{Z}_s be an algebraic set as in (1) which does not contain the zero set of the polynomial $Q_t(X_1, \dots, X_n)$. Then there exists a point $\mathbf{z} \in V \setminus \mathcal{Z}_s$ such that $Q(\mathbf{z}) = t$ and*

$$(5) \quad h(\mathbf{z}) \ll H(Q_t^*)^{\frac{m-w+2}{2}} H(V)^2.$$

The implied constant in the inequality depends only on K , m , n and M_s .

The idea of the proof here is to consider $Q_t^*(X_1, \dots, X_{n+1})$ under the condition $X_{n+1} \neq 1$, apply Theorem 1.1 and then divide out by this new variable.

One conceptual difference between Theorem 1.1 and Theorem 1.2 is that in the homogeneous case the small-height point in question has coordinates in \mathcal{O}_K whereas in the inhomogeneous setting it does not. In fact, the problem of obtaining an inhomogeneous result over \mathcal{O}_K instead of K is substantially more difficult. Some state-of-the-art results for integer solutions to inhomogeneous integral quadratic equations without any avoidance conditions can be found in [4]. Theorem 1.3 below is a version of the main result of [4], which addresses the special case $K = \mathbb{Q}$, stated in terms of our notation. A quadratic form in $\mathbb{Z}[X_1, \dots, X_n]$ is said to be integral if its Gram matrix has integer entries.

Theorem 1.3 ([4], Theorem 1). *Let $Q(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ be a regular integral quadratic form. Suppose that an integer t is integrally represented by Q . Then there is a vector $\mathbf{z} \in \mathbb{Z}^n$ such that $Q(\mathbf{z}) = t$ and*

$$h(\mathbf{z}) \ll h(Q_t)^{\ell(n)},$$

where the implied constant depends only on n and

$$\ell(n) = \begin{cases} 2100 & \text{if } n = 3, \\ 84 & \text{if } n = 4, \\ 5n + 19 + 74/(n - 4) & \text{if } n \geq 5. \end{cases}$$

The following corollary is a subspace version of Theorem 1.3. We postpone its proof to the next section after all the height functions are defined.

Corollary 1.4. *Let $Q(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ be an integral quadratic form and (V, Q) be an m -dimensional regular subspace of \mathbb{Q}^n , $m \geq 3$. Suppose that $t \in Q(V \cap \mathbb{Z}^n)$. Then there exists $\mathbf{z} \in V \cap \mathbb{Z}^n$ such that $Q(\mathbf{z}) = t$ and*

$$(6) \quad h(\mathbf{z}) \ll h(Q_t)^{\ell(m)} H(V)^{2\ell(m)+1}.$$

As for integer solutions to inhomogeneous integral quadratic equations with avoidance conditions, we have the following result in this direction. Its proof will be given in Section 4.

Theorem 1.5. *Let $Q(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ be an integral quadratic form. Let $V \subseteq \mathbb{Q}^n$ be an m -dimensional subspace, $3 \leq m \leq n$, such that the quadratic space (V, Q) is regular and isotropic of Witt index w . Let W_1, \dots, W_k be distinct hyperplanes of V . Then for any $0 \neq t \in Q(V \cap \mathbb{Z}^n)$, there exists $\mathbf{z} \in (V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$ such that $Q(\mathbf{z}) = t$ and*

$$h(\mathbf{z}) \ll \begin{cases} h(Q_t)^{(1+\frac{2}{m-2})\ell(m)+m+2+\frac{m+4}{m-2}} H(V)^{(2+\frac{4}{m-2})\ell(m)+5+\frac{8}{m-2}} & \text{if } w = 1; \\ h(Q_t)^{2\ell(m)+\frac{m-w+5}{2}} H(V)^{2\ell(m)+3} & \text{if } w \geq 2, \end{cases}$$

where the implied constant depends only on m , n , and k .

Remark 1.2. Notice that Theorem 1.5 cannot be true when the dimension of V is equal to 2, since in that case the number of representations of an integer by Q on $V \cap \mathbb{Z}^n$ is always finite, and hence all the representing vectors can easily be cut out by a finite union of hyperplanes.

2. NOTATION AND TOOLS

We start with some notation and technical lemmas, following [3]. Let K be a number field and $d := [K : \mathbb{Q}]$ the global degree of K over \mathbb{Q} . Let $M(K)$ be the set of all places of K . For each place $v \in M(K)$, we write K_v for the completion of K at v , and let $d_v := [K_v : \mathbb{Q}_v]$ be the local degree of K at v . For each place $v \in M(K)$ we define the absolute value $|\cdot|_v$ to be the unique absolute value on K_v that extends either the usual absolute value on \mathbb{R} or \mathbb{C} if $v|\infty$, or the usual p -adic absolute value on \mathbb{Q}_p if $v|p$, where p is a prime. For each non-zero $a \in K$ the following product formula is satisfied:

$$(7) \quad \prod_{v \in M(K)} |a|_v^{d_v} = 1, \quad \text{for all } a \in K^\times.$$

For each $v \in M(K)$, we define a local height H_v on K_v^n by

$$H_v(\mathbf{x}) = \max_{1 \leq i \leq n} |x_i|_v^{d_v}, \quad \text{for each } \mathbf{x} \in K_v^n,$$

and take a product to define a global height function on K^n :

$$(8) \quad H(\mathbf{x}) = \left(\prod_{v \in M(K)} H_v(\mathbf{x}) \right)^{1/d}$$

for each $\mathbf{x} \in K^n$. This height function is *homogeneous*, in the sense that it is defined on the projective space over K^n , thanks to the product formula (7). We also define the *inhomogeneous* height

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

which generalizes the Weil height on algebraic numbers. Clearly, $h(\mathbf{x}) \geq H(\mathbf{x})$ for each $\mathbf{x} \in K^n$. We extend the height functions H and h to polynomials by evaluating the height of their coefficient vectors. Finally, we define the height of an m -dimensional subspace $V \subseteq K^n$ as

$$H(V) := H(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_m),$$

where $\mathbf{x}_1, \dots, \mathbf{x}_m$ is a basis for V and $\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_m$ is viewed as a vector in $K^{\binom{n}{m}}$ under the standard Plücker coordinate embedding. Due to the product formula, this global height does not depend on the choice of the basis, and $H(K^n) = 1$.

Now we review some basic tools that we will need for our main arguments.

Lemma 2.1 ([3], Lemma 2.1). *For $\xi_1, \dots, \xi_\ell \in K$ and $\mathbf{x}_1, \dots, \mathbf{x}_\ell \in K^n$,*

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

where $\boldsymbol{\xi} = (\xi_1, \dots, \xi_\ell) \in K^\ell$.

Lemma 2.2. *Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$, then $h(\mathbf{x}) = |\mathbf{x}|$, where $|\mathbf{x}|$ is the sup-norm of \mathbf{x} , and $H(\mathbf{x}) = h(\mathbf{x})$ if \mathbf{x} is primitive, i.e. $\gcd(x_1, \dots, x_n) = 1$. Moreover, for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$, $h(\mathbf{x} + \mathbf{y}) \leq h(\mathbf{x}) + h(\mathbf{y})$.*

Proof. Let $\mathbf{x} \in \mathbb{Z}^n$. Then $H_p(\mathbf{x}, 1) = 1$ for all finite primes p and $H_\infty(\mathbf{x}, 1) = \max\{|x_1|, \dots, |x_n|\}$ which is the sup-norm $|\mathbf{x}|$. Therefore, $h(\mathbf{x}) = H(\mathbf{x}, 1) = |\mathbf{x}|$. Furthermore, $|\mathbf{x}| = H_\infty(\mathbf{x})$, while the product over p -adic absolute values

$$\prod_{v \nmid \infty} H_v(\mathbf{x}) = \gcd(x_1, \dots, x_n)^{-1}.$$

Thus, $H(\mathbf{x}) = |\mathbf{x}| / \gcd(x_1, \dots, x_n)$ and hence $H(\mathbf{x}) = h(\mathbf{x})$ if \mathbf{x} is primitive. The last assertion is clear because h is just the sup-norm. \square

Lemma 2.3 ([3], Lemma 2.2). *Let V be a subspace of K^n , $n \geq 2$, and let subspaces $U_1, \dots, U_k \subseteq V$ and vectors $\mathbf{x}_1, \dots, \mathbf{x}_\ell \in V$ be such that*

$$V = \text{span}_K\{U_1, \dots, U_k, \mathbf{x}_1, \dots, \mathbf{x}_\ell\}.$$

Then

$$H(V) \ll H(U_1) \cdots H(U_k) H(\mathbf{x}_1) \cdots H(\mathbf{x}_\ell),$$

where the constant in the upper bound depends on n and ℓ .

Lemma 2.4 ([3], Lemma 2.4). *Let U_1, U_2 be subspaces of K^n , then*

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

Lemma 2.5. *Let Q be a nonzero quadratic form in n variables over K and let $V \subsetneq K^n$ be an m -dimensional subspace, $1 \leq m < n$. Then*

$$H(\perp_Q(V)) \ll H(Q)^m H(V),$$

where the constant in the upper bound depends on n , m , and K .

Proof. Let $\mathbf{x}_1, \dots, \mathbf{x}_m$ be a small-height basis for V guaranteed by Siegel's lemma (see [1]), so

$$(9) \quad \prod_{i=1}^m h(\mathbf{x}_i) \ll H(V),$$

where the constant in the upper bound depends on K and m . By Lemma 2.3 of [3],

$$(10) \quad H(\perp_Q(V)) \ll H(Q)^m \prod_{i=1}^m H(\mathbf{x}_i),$$

where the constant in the upper bound depends only on n and m . The conclusion follows by combining (9) with (10). \square

We conclude this section by presenting the proof of Corollary 1.4. From now on, for a string of parameters I , we will write " $f \ll_I g$ " to mean that $f \leq Cg$ for some constant C depending only on the parameters in I .

Proof of Corollary 1.4. As in the proof of Lemma 2.5, V has a basis $\mathbf{y}_1, \dots, \mathbf{y}_m$ satisfying

$$(11) \quad \prod_{i=1}^m h(\mathbf{y}_i) \ll_m H(V).$$

But the version of Siegel's lemma in [1, Theorem 9] says more: $\mathbf{y}_1, \dots, \mathbf{y}_m$ can be chosen to be in $V \cap \mathbb{Z}^n$. For every $\mathbf{y} \in V \cap \mathbb{Z}^n$, $h(\mathbf{y})$ is simply the sup-norm of the integral vector \mathbf{y} which is comparable to the Euclidean length of \mathbf{y} . Then by the Hadamard Inequality [9, Theorem 2.1.1], the Hermite Inequality [9, Theorem 2.2.1], and (11) together, the \mathbb{Z} -lattice $V \cap \mathbb{Z}^n$ has a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$ such that

$$(12) \quad \prod_{i=1}^m h(\mathbf{x}_i) \ll_m H(V).$$

Let T be the $n \times m$ matrix $[\mathbf{x}_1 \cdots \mathbf{x}_m]$ and $Q'(X_1, \dots, X_m)$ be the integral quadratic form with Gram matrix $T^t Q T$. Then Q' is a regular integral quadratic form in m variables and t is integrally represented by Q' . By Theorem 1.3, there exists $\mathbf{u} \in \mathbb{Z}^m$ such that $Q'(\mathbf{u}) = t$ and $h(\mathbf{u}) \ll_m h(Q'_t)^{\ell(m)}$. If $\mathbf{u} = (u_1, \dots, u_m)$, then $\mathbf{z} := u_1 \mathbf{x}_1 + \cdots + u_m \mathbf{x}_m$ is a vector in $V \cap \mathbb{Z}^n$ such that $Q(\mathbf{z}) = t$.

By Lemma 2.1 and (12), we have

$$(13) \quad h(\mathbf{z}) \ll_m h(\mathbf{u}) \prod_{i=1}^m h(\mathbf{x}_i) \ll_m h(\mathbf{u}) H(V) \ll_m h(Q'_t)^{\ell(m)} H(V).$$

Since the matrices T and Q have integral entries, (12) implies that

$$(14) \quad h(Q'_t) \ll_m h(Q_t) h(T)^2 \leq h(Q_t) \left(\prod_{i=1}^m h(\mathbf{x}_i) \right)^2 \ll_m h(Q_t) H(V)^2,$$

where by $h(T)$ we mean height of T viewed as a vector. Combining (13) and (14) we obtain (6) in the Corollary. \square

3. PROOF OF THEOREM 1.2

Starting with an algebraic set $\mathcal{Z}_s \subset K^n$ as in (1), let us consider its homogenization $\mathcal{Z}_{s^*} \subset K^{n+1}$ as in (3). Given the m -dimensional subspace V of K^n , let $V^* = V \oplus K\mathbf{e}_{n+1} \subseteq K^{n+1}$, where \mathbf{e}_{n+1} is the last standard basis vector in K^{n+1} . Then V^* is an $(m+1)$ -dimensional subspace of K^{n+1} , and by Lemma 2.3,

$$(15) \quad H(V^*) \ll_n H(V)H(\mathbf{e}_{n+1}) = H(V),$$

since the height of V does not change after the embedding $V \rightarrow (V, 0)$ into K^{n+1} . Let $t \neq 0$ be an element of $Q(V)$, and $Q_t^* \in K[X_1, \dots, X_{n+1}]$ be the homogenization of the quadratic polynomial $Q(X_1, \dots, X_{n+1}) - t$, i.e.

$$Q_t^*(X_1, \dots, X_{n+1}) = Q(X_1, \dots, X_n) - tX_{n+1}^2.$$

Then for any $\mathbf{x} \in V$, $Q(\mathbf{x}) = t$ if and only if $Q_t^*(\mathbf{x}, 1) = 0$. The hypothesis of the theorem implies that there exists $\mathbf{z} \in V \setminus \mathcal{Z}_s$ such that $Q(\mathbf{z}) = t$. Let

$$\mathcal{Z}'_s = \mathcal{Z}_{s^*} \cup \{(\mathbf{x}, 0) : \mathbf{x} \in K^n\} \subset K^{n+1}.$$

Then $Q_t^*(\mathbf{z}, 1) = 0$ and $(\mathbf{z}, 1) \in V^* \setminus \mathcal{Z}'_s$, meaning that the quadratic form Q_t^* on K^{n+1} has a nontrivial zero in $V^* \setminus \mathcal{Z}'_s$. Notice also that for every maximal totally isotropic subspace W of (V, Q) , $(W, 0)$ is a totally isotropic subspace of (V^*, Q_t^*) , and hence the dimension w^* of a maximal totally isotropic subspace of (V^*, Q_t^*) is at least w . Further, if $w = 0$, i.e. if (V, Q) is anisotropic, then $w^* = 1$. Then, by Theorem 1.1, there must exist $\mathbf{y} \in V^* \setminus \mathcal{Z}'_s$ such that $Q_t^*(\mathbf{y}) = 0$ and

$$H(\mathbf{y}) \ll_{m, M_s} H(Q_t^*)^{\frac{(m+1)-w^*+1}{2}} H(V^*)^2 \ll_n H(Q_t^*)^{\frac{m-w+2}{2}} H(V)^2,$$

by (15). Since $\mathbf{y} \notin \mathcal{Z}'_s$, $y_{n+1} \neq 0$, so define

$$\mathbf{y}' = \frac{1}{y_{n+1}} \mathbf{y} = \left(\frac{y_1}{y_{n+1}}, \dots, \frac{y_n}{y_{n+1}}, 1 \right),$$

and let $\mathbf{z} = \left(\frac{y_1}{y_{n+1}}, \dots, \frac{y_n}{y_{n+1}} \right) \in V$, i.e. $\mathbf{y}' = (\mathbf{z}, 1)$. Then, by the product formula,

$$(16) \quad h(\mathbf{z}) = H(\mathbf{y}') = H(\mathbf{y}) \ll_{m, n, M_s} H(Q_t^*)^{\frac{m-w+2}{2}} H(V)^2,$$

and $Q_t^*(\mathbf{y}') = Q_t^*(\mathbf{y}) = 0$, which means that $Q(\mathbf{z}) = t$. This completes the proof of Theorem 1.2.

Remark 3.1. Notice that the argument in the proof of Theorem 1.2 does not necessarily produce a point with coordinates in \mathcal{O}_K , since we divided by y_{n+1} . In the next section we produce weaker versions of such a result over \mathcal{O}_K when $K = \mathbb{Q}$.

4. PROOF OF THEOREM 1.5

In this section we give the proof of Theorem 1.5. We start with the following lemma, which is essentially Case 1 in the proof of the main theorem in [5]. We extract its proof from [5] and present it here for the convenience of the reader.

Lemma 4.1. *Let K be a number field and $Q(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ be a nonzero quadratic form. Suppose that (V, Q) is a regular isotropic subspace of K^n of dimension ≥ 3 . If W_1, \dots, W_k are hyperplanes of V , then V has an isotropic vector outside of the union $\bigcup_{i=1}^k W_i$.*

Proof. After fixing a choice of basis for V , we may assume that $V = K^n$ with $n \geq 3$. For $i = 1, \dots, k$, let L_i be a nonzero linear form in $K[X_1, \dots, X_n]$ whose kernel is W_i . Let \mathbf{u} be an isotropic vector in K^n . For every $\mathbf{x} \in K^n$, let

$$T_{\mathbf{u}}(\mathbf{x}) = Q(\mathbf{x})\mathbf{u} - 2Q(\mathbf{x}, \mathbf{u})\mathbf{x}.$$

It is straightforward to check that $Q(T_{\mathbf{u}}(\mathbf{x})) = 0$ for all $\mathbf{x} \in K^n$.

Fix an index i . We claim that $L_i(T_{\mathbf{u}}(X_1, \dots, X_n))$ is not the zero polynomial. Assume the contrary that $L_i(T_{\mathbf{u}}(X_1, \dots, X_n))$ is indeed the zero polynomial. Suppose first that $L_i(\mathbf{u}) \neq 0$. Then

$$Q(\mathbf{x}) = \frac{2Q(\mathbf{u}, \mathbf{x})L_i(\mathbf{x})}{L_i(\mathbf{u})}$$

for all $\mathbf{x} \in K^n$, which means that $Q(X_1, \dots, X_n)$ is a product of two linear forms which is impossible since (K^n, Q) is a regular quadratic space of dimension ≥ 3 . Now, if $L_i(\mathbf{u}) = 0$, then $Q(\mathbf{u}, \mathbf{x})L_i(\mathbf{x}) = 0$ for all $\mathbf{x} \in K^n$, which is impossible again since both L_i and $\mathbf{x} \mapsto Q(\mathbf{u}, \mathbf{x})$ are not the zero linear functional on K^n .

So, the polynomial

$$F(X_1, \dots, X_n) := L_1(T_{\mathbf{u}}(X_1, \dots, X_n)) \cdots L_k(T_{\mathbf{u}}(X_1, \dots, X_n))$$

is not the zero polynomial in $K[X_1, \dots, X_n]$. We can then take a vector $\mathbf{x} \in K^n$ such that $F(\mathbf{x}) \neq 0$. Then $T_{\mathbf{u}}(\mathbf{x})$ is an isotropic vector in K^n outside of $\bigcup_{i=1}^k W_i$. \square

Lemma 4.2. *Let $Q(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ be an integral quadratic form. Let $V \subseteq \mathbb{Q}^n$ be an m -dimensional subspace, $3 \leq m \leq n$, such that the quadratic space (V, Q) is regular and isotropic of Witt index w . Let W_1, \dots, W_k be distinct hyperplanes of V . Then for every anisotropic vector $\mathbf{y} \in V \cap \mathbb{Z}^n$, there exists a point $\mathbf{z} \in (V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$ such that $Q(\mathbf{z}) = Q(\mathbf{y})$ and*

$$h(\mathbf{z}) \ll_{m,n,k} \begin{cases} h(\mathbf{y})^{1+\frac{2}{m-2}} h(Q)^{m+2+\frac{m+4}{m-2}} H(V)^{4+\frac{6}{m-2}} & \text{if } w = 1; \\ h(\mathbf{y})^2 h(Q)^{\frac{m-w+5}{2}} H(V)^2 & \text{if } w \geq 2. \end{cases}$$

Proof. If $\mathbf{y} \notin \bigcup_{i=1}^k W_i$, then we are done; so we assume from now on that $\mathbf{y} \in \bigcup_{i=1}^k W_i$.

Case 1: Assume that w , the Witt index of V , is at least 2. Let $V_{\mathbf{y}}$ be the orthogonal complement of \mathbf{y} in V , which is an $(m-1)$ -dimensional regular isotropic subspace of V such that $V = \mathbb{Q}[\mathbf{y}] \perp V_{\mathbf{y}}$. We have two cases to consider, according to whether $V_{\mathbf{y}}$ is one of the W_i or not.

Suppose first that $V_{\mathbf{y}}$ is not equal to any of the W_i . Then $V_{\mathbf{y}} \cap W_i$ is a hyperplane of $V_{\mathbf{y}}$ for each i . By Lemma 4.1, $V_{\mathbf{y}} \setminus \bigcup_{i=1}^k W_i$ has an isotropic vector. Then,

by Theorem 1.1 and Lemmas 2.3, 2.4, 2.5 there exists an isotropic vector $\mathbf{u} \in (V_{\mathbf{y}} \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$ with

$$(17) \quad h(\mathbf{u}) \ll_{m,n,k} h(Q)^{\frac{m-w+1}{2}} H(V_{\mathbf{y}})^2 \ll_{m,n,k} h(\mathbf{y})^2 h(Q)^{\frac{m-w+5}{2}} H(V)^2.$$

Note that $H(Q) = h(Q)$ because Q has integer coefficients. For $1 \leq r \leq k+1$, let $\mathbf{z}_r := \mathbf{y} + r\mathbf{u}$ which is in $(V \cap \mathbb{Z}^n)$. Suppose that all of these \mathbf{z}_r are in $\bigcup_{i=1}^k W_i$. By the Pigeon-Hole Principle, there must be $1 \leq r \neq s \leq k+1$ and $1 \leq j \leq k$ such that \mathbf{z}_r and \mathbf{z}_s are in W_j . Then $\mathbf{z}_r - \mathbf{z}_s$ is in W_j , implying that \mathbf{u} is also in W_j which is a contradiction. Thus, there must be an r such that $\mathbf{z} := \mathbf{z}_r$ is not in $\bigcup_{i=1}^k W_i$ and $Q(\mathbf{z}) = Q(\mathbf{y})$. Moreover,

$$(18) \quad h(\mathbf{z}) \leq h(\mathbf{y}) + rh(\mathbf{u}) \ll_{m,n,k} h(\mathbf{y})^2 h(Q)^{\frac{m-w+5}{2}} H(V)^2.$$

Now, suppose that $V_{\mathbf{y}}$ is one of the W_i , say $V_{\mathbf{y}} = W_1$. Then $V_{\mathbf{y}} \cap W_i$ is a hyperplane in $V_{\mathbf{y}}$ for every $i \geq 2$. As is done in the last paragraph, we have an isotropic vector $\mathbf{u} \in (V_{\mathbf{y}} \cap \mathbb{Z}^n) \setminus \bigcup_{i=2}^k W_i$ and $h(\mathbf{u})$ is bounded above as in (17). Since \mathbf{u} is in W_1 but \mathbf{y} is not, all of the \mathbf{z}_r defined as in the last paragraph are not in W_1 . Suppose that all of these \mathbf{z}_r are in $\bigcup_{i=2}^k W_i$. As is argued before, there will be two different indices $r, s \in \{1, \dots, k+1\}$ and $j \in \{2, \dots, k\}$ such that $\mathbf{z}_r - \mathbf{z}_s \in W_j$. This means that \mathbf{u} is in W_j for some $j \geq 2$, which is impossible. We may now argue as in the last paragraph to obtain an $\mathbf{z} \in (V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$ with $Q(\mathbf{z}) = Q(\mathbf{y})$ and $h(\mathbf{z})$ bounded above as in (18).

Case 2: Suppose that $w = 1$. The space V itself is regular and isotropic. By Lemma 4.1 and Theorem 1.1, there exists an isotropic vector $\mathbf{u} \in (V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$ with

$$(19) \quad h(\mathbf{u}) \ll_{m,n,k} h(Q)^{\frac{m}{2}} H(V)^2.$$

Suppose first that $Q(\mathbf{u}, \mathbf{y}) = 0$. We could argue as in Case 1 and obtain a vector $\mathbf{z} \in (V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$ such that $Q(\mathbf{z}) = Q(\mathbf{y})$ and

$$(20) \quad h(\mathbf{z}) \leq h(\mathbf{y}) + rh(\mathbf{u}) \ll_{m,n,k} h(\mathbf{y})h(Q)^{\frac{m}{2}} H(V)^2.$$

Note that this upper bound is better than the one in the statement of the lemma.

Now, let us suppose that $Q(\mathbf{u}, \mathbf{y}) \neq 0$. Then $\mathbb{Q}[\mathbf{u}, \mathbf{y}]$ is a 2-dimensional regular subspace of V , and its orthogonal complement G in V is an $(m-2)$ -dimensional anisotropic subspace of V . By Siegel's lemma [1, Theorem 9], there exist vectors $\mathbf{x}_1, \dots, \mathbf{x}_s$ in \mathbb{Z}^n which form a basis for G and

$$(21) \quad \prod_{i=1}^{m-2} h(\mathbf{x}_i) \ll_m H(G).$$

Let \mathbf{x} be a vector among the \mathbf{x}_i that has the smallest height. Then, combining this with (19) and using Lemmas 2.3, 2.4, and 2.5, we have

$$(22) \quad h(\mathbf{x}) \ll_m H(G)^{\frac{1}{m-2}} \ll_{m,n} h(\mathbf{y})^{\frac{1}{m-2}} h(Q)^{\frac{m+4}{2(m-2)}} H(V)^{\frac{3}{m-2}}.$$

This \mathbf{x} is necessarily an anisotropic vector in $V \cap \mathbb{Z}^n$. By replacing \mathbf{x} with $2\mathbf{x}$ if necessary, we may assume that $Q(\mathbf{x})$ is a nonzero even integer.

For each integer $\ell \geq 1$, let $a_\ell = 2^{\ell-1} + \dots + 2 + 1$ and

$$I_\ell = \{(k+1)a_\ell - k, \dots, (k+1)a_\ell\}.$$

For each $r \in I_\ell$, let

$$\mathbf{z}_r := \mathbf{y} + rQ(\mathbf{y}, \mathbf{u})\mathbf{x} - \frac{r^2}{2}Q(\mathbf{x})Q(\mathbf{y}, \mathbf{u})\mathbf{u}.$$

It is easy to check that $\mathbf{z}_r \in V \cap \mathbb{Z}^n$ and $Q(\mathbf{z}_r) = Q(\mathbf{y})$. Suppose that for all $\ell \in \{1, \dots, k+1\}$ and all $r \in I_\ell$, \mathbf{z}_r are in $\bigcup_{i=1}^k W_i$. Fix an ℓ ; by the Pigeon-Hole Principle, there must be two distinct indices $r, s \in I_\ell$ and $i(\ell) \in \{1, \dots, k\}$ such that both \mathbf{z}_r and \mathbf{z}_s are in $W_{i(\ell)}$. Then $\mathbf{z}_r - \mathbf{z}_s$ is in $W_{i(\ell)}$ and hence

$$\mathbf{x} - \frac{1}{2}Q(\mathbf{x})(r+s)\mathbf{u} \in W_{i(\ell)}.$$

By virtue of the Pigeon-Hole Principle one more time, there must be two different indices $\ell_1, \ell_2 \in \{1, \dots, k+1\}$, $i_0 \in \{1, \dots, k\}$, and pairs of distinct integers $r_1, s_1 \in I_{\ell_1}$ and $r_2, s_2 \in I_{\ell_2}$ such that both $\mathbf{z}_{r_1} - \mathbf{z}_{s_1}$ and $\mathbf{z}_{r_2} - \mathbf{z}_{s_2}$ are in W_{i_0} . Then,

$$\frac{1}{2}Q(\mathbf{x})((r_2 + s_2) - (r_1 + s_1))\mathbf{u} \in W_{i_0}.$$

Without loss of generality, we may assume that $\ell_1 < \ell_2$. Then

$$\begin{aligned} r_1 + s_1 &\leq 2(k+1)a_{\ell_1} \\ &= (k+1)a_{\ell_1+1} - (k+1) \\ &\leq (k+1)a_{\ell_2} - k - 1 \\ &< 2(k+1)a_{\ell_2} - 2k \\ &\leq r_2 + s_2, \end{aligned}$$

and hence $\mathbf{u} \in W_{i_0}$, which is impossible. Thus, there must be one of these \mathbf{z}_r in $(V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^k W_i$. Let \mathbf{z} be this \mathbf{z}_r . A crude estimate shows that

$$(23) \quad h(\mathbf{z}) \ll_{m,n,k} h(\mathbf{y})h(Q)^2 h(\mathbf{u})^2 h(\mathbf{x})^2.$$

Using (19), (22), and (23) we obtain

$$(24) \quad h(\mathbf{z}) \ll_{m,n,k} h(\mathbf{y})h(\mathbf{y})^{\frac{2}{m-2}} h(Q)^{m+2+\frac{m+4}{m-2}} H(V)^{4+\frac{6}{m-2}}.$$

The lemma is proved by combining (18), (20), and (24). \square

Proof of Theorem 1.5. The theorem now follows upon combining Corollary 1.4 and Lemma 4.2, noticing that $h(Q) \leq h(Q_t)$. \square

Acknowledgement: We thank the referee for a very careful and thorough reading and many helpful comments which have improved the quality of the paper.

REFERENCES

- [1] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.
- [2] J. W. S. Cassels. Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 51:262–264, 1955.
- [3] W. K. Chan, L. Fukshansky, and G. Henshaw. Small zeros of quadratic forms missing a union of varieties. *Trans. Amer. Math. Soc.*, 366(10):5587–5612, 2014.
- [4] R. Dietmann. Small solutions of quadratic diophantine equations. *Proc. London Math. Soc.*, 86(3):545–582, 2003.
- [5] R. Dietmann. Small zeros of quadratic forms avoiding a finite number of prescribed hyperplanes. *Canad. Math. Bull.*, 52(1):63–65, 2009.

- [6] L. Fukshansky. Small zeros of quadratic forms with linear conditions. *J. Number Theory*, 108(1):29–43, 2004.
- [7] L. Fukshansky. Heights and quadratic forms: on Cassels’ theorem and its generalizations. In W. K. Chan, L. Fukshansky, R. Schulze-Pillot, and J. D. Vaaler, editors, *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, Contemp. Math., 587, pages 77–94. Amer. Math. Soc., Providence, RI, 2013.
- [8] E. Gaudron and G. Rémond. Espaces adéliques quadratiques. *Math. Proc. Cambridge Philos. Soc.*, 162(2):211–247, 2017.
- [9] J. Martinet. *Perfect lattices in Euclidean spaces*. Springer-Verlag, 2003.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, WESLEYAN UNIVERSITY, MIDDLETOWN, CT 06459

E-mail address: `wkchan@wesleyan.edu`

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE, CLAREMONT, CA 91711

E-mail address: `lenny@cmc.edu`