

Effective structure theorems for quadratic spaces via height

Lenny Fukshansky
Claremont McKenna College

December 2007

Quadratic forms

Let K be a **number field**, i.e. a finite extension of \mathbb{Q} . Let

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

be a symmetric bilinear form in $N \geq 2$ variables with coefficients in K . Write

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

for the associated quadratic form. We will also write F for the symmetric coefficient matrix $(f_{ij})_{1 \leq i, j \leq N}$. Notice that

$$F(\mathbf{X}, \mathbf{Y}) = \mathbf{X}^t F \mathbf{Y}.$$

Clearly,

$$F(\mathbf{0}) = 0.$$

We will say that F is **isotropic** over K if it has a *non-trivial* zero with coordinates in K .

How can we tell if F is isotropic over K ?

A criterion is provided by the famous Hasse-Minkowski theorem: F is isotropic over K if and only if it is isotropic over every completion of K .

This is an example of a *non-effective* statement: it provides no information about non-trivial zeros of F over K , only a criterion for their existence. We will be interested in *effective* questions, such as the following.

Question 1. *Assuming F is isotropic over K , how do we find a non-trivial zero of F over K ?*

More generally, let $Z \subseteq K^N$ be a subspace of K^N of dimension L , $1 \leq L \leq N$. We write (Z, F) for the quadratic space defined on Z by F .

We say that (Z, F) is **isotropic** if there exists $0 \neq x \in Z$ such that $F(x) = 0$; we call (Z, F) **anisotropic** otherwise. A subspace V of (Z, F) is called **totally isotropic** if

$$F(V) = 0.$$

All maximal totally isotropic subspaces have the same dimension, called **Witt index** of (Z, F) .

Question 2. *If (Z, F) is isotropic, how do we find a maximal totally isotropic subspace of (Z, F) ?*

We generalize further. Two points $x, y \in Z$ are said to be **orthogonal** with respect to F if

$$F(x, y) = 0.$$

In the same manner, we can talk about orthogonal subspaces of Z , where orthogonality will always be meant with respect to F .

If two subspaces, V and W of Z are orthogonal, we will write

$$V \perp W$$

for their orthogonal direct sum.

The **singular** component of (Z, F) is the subspace

$$Z^\perp = \{x \in Z : F(x, y) = 0 \forall y \in Z\},$$

so Z^\perp is orthogonal to every subspace of Z .

The **rank** of F on Z is

$$r = L - \dim_K Z^\perp.$$

If $Z^\perp = \{0\}$, we say that (Z, F) is **nonsingular** or **regular**: in this case $r = L$.

A subspace $\mathbb{H} = \text{span}_K\{x, y\}$, where $x, y \in Z$ are such that

$$F(x) = F(y) = 0, \quad F(x, y) = 1,$$

is called a **hyperbolic plane**.

Witt Decomposition: Let k be the Witt index of (Z, F) . There exist hyperbolic planes $\mathbb{H}_1, \dots, \mathbb{H}_k$ and an anisotropic subspace W of Z such that

$$Z = Z^\perp \perp \mathbb{H}_1 \perp \dots \perp \mathbb{H}_k \perp W.$$

Witt decomposition for a quadratic space is not unique.

Question 3. *How do we find a Witt decomposition for a quadratic space?*

In what follows we demonstrate an approach to Questions 1, 2, and 3 which not only suggests a search algorithm for objects in question, but also proves the existence of such objects with special nice arithmetic properties.

For this we need to introduce the machinery of height functions.

Absolute values

Let K be a number field of degree

$$d = [K : \mathbb{Q}]$$

over \mathbb{Q} . We will write $M(K)$ for the set of places of K , and for each $v \in M(K)$, let

$$d_v = [K_v : \mathbb{Q}_v]$$

be the local degree of K at v , where K_v and \mathbb{Q}_v are the completions of K and \mathbb{Q} at v , respectively. If absolute values from $v \in M(K)$ extend absolute values from $u \in M(\mathbb{Q})$, we write $v|u$. Then for each $u \in M(\mathbb{Q})$,

$$\sum_{v \in M(K), v|u} d_v = d = [K : \mathbb{Q}].$$

We choose a representative $|\cdot|_v$ so that it extends either $|\cdot|_\infty$ on \mathbb{Q} , if $v \in M_\infty(K)$, or some p -adic absolute value $|\cdot|_p$ if $v \in M_0(K)$.

Artin-Whaples Product Formula: For each $0 \neq a \in K$,

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

Height functions

We can define local norms on each K_v^N by

$$|\mathbf{x}|_v = \begin{cases} \max_{1 \leq i \leq N} |x_i|_v & \text{if } v \in M_0(K) \\ \left(\sum_{i=1}^N |x_i|_v^2 \right)^{1/2} & \text{if } v \in M_\infty(K) \end{cases}$$

for each $\mathbf{x} = (x_1, \dots, x_N) \in K_v^N$. Then define a global height function on K^N by

$$H(\mathbf{x}) = \prod_{v \in M(K)} |\mathbf{x}|_v^{d_v/d}$$

for each $\mathbf{x} \in K^N$. This product is convergent because only finitely many of the local norms for each vector $\mathbf{x} \in K^N$ are different from 1. Moreover, because of the normalizing power $1/d$ in the definition, H is *absolute*, i.e. does not depend on the field of definition. Also notice that because of the product formula, H is well defined on the projective space $\mathbb{P}^{N-1}(K)$, i.e.

$$H(a\mathbf{x}) = H(\mathbf{x}), \quad \forall 0 \neq a \in K, \quad \mathbf{x} \in K^N.$$

In general, one can define a variety of different height functions by selecting different local norms while making sure that the defining product is still convergent. For our purposes this height function turns out to be convenient. It is easy to see that $H(\mathbf{x}) \geq 1$ for all non-zero $\mathbf{x} \in K^N$. The main property, for our purposes, that all height functions satisfy is

Northcott's theorem: *For a height function H on K^N the set*

$$\{\mathbf{x} \in \mathbb{P}^{N-1}(K) : H(\mathbf{x}) \leq B\}$$

is finite for every positive real number B .

Heights can be extended to polynomials: if

$$F(X_1, \dots, X_N) \in K[X_1, \dots, X_N]$$

we write $H(F)$ to mean the height of its coefficient vector.

We can also talk about height of subspaces of K^N . Let $V \subseteq K^N$ be a J -dimensional subspace, and let $\mathbf{x}_1, \dots, \mathbf{x}_J$ be a basis for V . Then

$$\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_J \in K^{\binom{N}{J}}$$

under the standard embedding. Define

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

This definition is legitimate, i.e. does not depend on the choice of the basis. Hence we have defined a height on points of a Grassmanian over K .

Finally, define height on elements of $GL_N(K)$ by viewing them as vectors in K^{N^2} .

Northcott's theorem has the following most important consequence.

Suppose we want to find a point satisfying some arithmetic condition, and assume that we can prove the existence of a point of height $\leq B$ satisfying this condition. But there are only finitely many such points. This suggests a search algorithm, and so B is a **search bound**.

Moreover, height measures arithmetic complexity, and so a point of relatively small height is “arithmetically simple”, which makes it even more interesting.

We are now ready to apply this machinery to quadratic forms.

Effective theory

As discussed above, one way to approach Questions 1, 2, and 3 is to prove the existence of objects in question of bounded height with explicit bounds. Here we demonstrate such results. The subject begins with the following classical result in the direction of Question 1.

Theorem 1 (Cassels 1955, Raghavan 1975). *If F is isotropic over K , then there exists $0 \neq \mathbf{x} \in K^N$ such that $F(\mathbf{x}) = 0$, and*

$$H(\mathbf{x}) \leq C_1(K, N)H(F)^{\frac{N-1}{2}},$$

where $C_1(K, N)$ is an explicit constant.

This theorem has been generalized and extended in a variety of ways by a number of different authors. We only review two such generalizations.

As before, let (Z, F) be an L -dimensional quadratic space in N variables, $1 \leq L \leq N$, of rank r and Witt index k . In the direction of Question 2 we have:

Theorem 2 (Schlickewei 1985, Vaaler 1987). *There exists a maximal totally isotropic subspace $V \subseteq Z$ with*

$$H(V) \leq C_2(K, L, k)H(F)^{\frac{L-k}{2}}H(Z),$$

where $C_2(K, L, k)$ is an explicit constant.

Building on Theorem 2, we can prove the following effective version of Witt decomposition for (Z, F) .

Theorem 3 (F. 2005). *There exists a decomposition for (Z, F) of the form*

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

where Z^\perp is the singular component, $\mathbb{H}_1, \dots, \mathbb{H}_k$ are hyperbolic planes, and W is anisotropic component with

$$H(Z^\perp) \leq C_3 H(F)^{\frac{r}{2}} H(Z)$$

and

$$\begin{aligned} & \max\{H(\mathbb{H}_i), H(W)\} \\ & \leq C_4 \left\{ H(F)^{\frac{L+2k}{4}} H(Z) \right\}^{\frac{(k+1)(k+2)}{2}}, \end{aligned}$$

for each $1 \leq i \leq k$, where the constants are explicit and depend on K, r, N, L , and k .

Effective theory over $\overline{\mathbb{Q}}$

From now on assume that (Z, F) is defined over $\overline{\mathbb{Q}}$, and is **regular**, meaning that

$$Z^\perp = \{0\},$$

and so $r = L$. Then the Witt index is

$$k = \left\lfloor \frac{L}{2} \right\rfloor,$$

and we can prove the following analogue of Schlickewei-Vaaler theorem.

Theorem 4 (F. 2005). *There exists a maximal totally isotropic subspace V of (Z, F) with*

$$H(V) \leq 12\sqrt{2} \ 3^{\frac{k^2(k+1)^2}{4}} H(F)^{\frac{k^2}{2}} H(Z)^{\frac{k^2+k+2}{2k}},$$

if L is even, and

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

if L is odd.

- If (Z, F) 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 $k = \left\lfloor \frac{L}{2} \right\rfloor$ over E , and then apply Vaaler's theorem to it. The constant in Vaaler's bound, however, will depend on the discriminant of E , which can be quite large. In this case the bounds of Theorem 4 can be better.
- Theorem 4 is a statement in the general spirit of "absolute" results, in particular it parallels the development of Siegel's lemma (results on existence of points of bounded height in a given vector space), the number field version of which was proved in 1983 by Bombieri and Vaaler, and the $\overline{\mathbb{Q}}$ "absolute" version in 1996 by Roy and Thunder.

- The Schlickewei-Vaaler method relies on Northcott's theorem about finiteness of projective points of bounded height over a number field; this is no longer true over $\overline{\mathbb{Q}}$, which does not allow to extend this method.
- Our argument uses the Roy-Thunder absolute Siegel's lemma along with a version of arithmetic Bezout's theorem due to Bost, Gillet, and Soulé, which provides a bound on the height of a projective intersection cycle in terms of the heights of intersecting projective varieties.

Witt decomposition for a regular space (Z, F) over $\overline{\mathbb{Q}}$ becomes

$$Z = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k \perp W, \quad (1)$$

where W is zero if $L = 2k$, and is a one-dimensional anisotropic subspace if $L = 2k + 1$. Then we obtain the following effective version of Witt decomposition over $\overline{\mathbb{Q}}$.

Theorem 5 (F. 2005). *There exists an orthogonal decomposition as in (1) such that for each $1 \leq i \leq k = \lfloor \frac{L}{2} \rfloor$*

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

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

$$H(W) = H(\mathbf{y}) \leq 2\sqrt{2k+1} 3^{\frac{(2k+3)k}{2}} H(Z)^{\frac{2k+3}{4k+2}},$$

if $L = 2k + 1$.

Another orthogonal decomposition that every quadratic space has is decomposition into orthogonal one-dimensional subspaces, i.e. every quadratic space has an orthogonal basis. In fact, using the same approach we can prove the existence of such a basis of bounded height.

Theorem 6 (F. 2005). *Let (Z, F) be an L -dimensional quadratic space in N variables, not necessarily regular, over a number field K with $1 \leq L < N$. Then there exists a basis $\mathbf{x}_1, \dots, \mathbf{x}_L$ over K for Z such that $F(\mathbf{x}_i, \mathbf{x}_j) = 0$ for all $i \neq j$, and*

$$\prod_{i=1}^L H(\mathbf{x}_i) \leq (N|\mathcal{D}_K|)^{\frac{L^2+L-2}{4}} H(F)^{\frac{L(L+1)}{2}} H(Z)^L,$$

where \mathcal{D}_K is the discriminant of K . There also exists a basis $\mathbf{y}_1, \dots, \mathbf{y}_L$ over $\overline{\mathbb{Q}}$ for Z such that $F(\mathbf{y}_i, \mathbf{y}_j) = 0$ for all $i \neq j$, and

$$\prod_{i=1}^L H(\mathbf{y}_i) \leq 3^{\frac{(L-1)^2(L+2)}{4}} H(F)^{\frac{L(L+1)}{2}} H(Z)^L.$$

Isometry group

In this section K will be either a number field or $\overline{\mathbb{Q}}$, and (Z, F) a quadratic space over K , as above.

The classical version of Witt decomposition theorem can be deduced from a variation of the famous theorem of Cartan and Dieudonné on the representation of isometries of a bilinear space. From here on assume that (Z, F) is regular. Let $\mathcal{O}(Z, F)$ be the group of all isometries of (Z, F) , i.e. $\mathcal{O}(Z, F)$ consists of all $\sigma \in GL_N(K)$ such that

$$F(\sigma x, \sigma y) = F(x, y)$$

for all $x, y \in Z$. Let $\sigma \in \mathcal{O}(Z, F)$. There exist **reflections** $\tau_1, \dots, \tau_l \in \mathcal{O}(Z, F)$ such that

$$\sigma = \tau_1 \dots \tau_l$$

where $0 \leq l \leq L$.

The following is a slightly weaker effective version of Cartan-Dieudonné theorem, where by height of an isometry we mean height of the corresponding matrix from $GL_N(K)$ viewed as a vector in K^{N^2} .

Theorem 7 (F. 2005). *Let (Z, F) be a regular quadratic space over K with $Z \subseteq K^N$ of dimension L , $1 \leq L \leq N$, $N \geq 2$. Let $\sigma \in \mathcal{O}(Z, F)$. Then either σ is the identity, or there exist an integer $1 \leq l \leq 2L - 1$ and reflections $\tau_1, \dots, \tau_l \in \mathcal{O}(Z, F)$ such that*

$$\sigma = \tau_1 \circ \dots \circ \tau_l,$$

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

$$H(\tau_i) \leq C_5 \left\{ H(F)^{\frac{L}{3}} H(Z)^{\frac{L}{2}} H(\sigma) \right\}^{5^{L-1}},$$

where C_5 is an explicit constant depending on K , N , and L .

There are two interesting corollaries of the method. One is a bound on the height of the **invariant subspace** of an isometry. The second is a statement about the existence of a reflection of relatively small height.

What is next?

It is interesting to also consider the case of a symplectic space, in other words let $F(\mathbf{X}, \mathbf{Y})$ be an **alternating** bilinear form over the coefficient field K . If Z is an even-dimensional subspace of K^N such that the corresponding symplectic space (Z, F) is regular, the goal is to provide effective decomposition theorems for (Z, F) . In other words, what would be the appropriate analogues of Theorems 3 - 6 in this case?

One distinguishing feature of this situation is that it seems to admit an entirely combinatorial argument, which allows K to be any global field (i.e. any field with a product formula), which is quite different from the symmetric case, where situations over different fields had to be considered separately. This is work in progress.