Effective theorems for quadratic spaces over $\overline{\mathbb{Q}}$

Lenny Fukshansky
Texas A&M University

January 2006

Notation and heights

- K is a number field of degree d over $\mathbb{Q}$ with the set of places $M(K)$.

- For each $v \in M(K)$, let $d_v = [K_v : \mathbb{Q}_v]$ and let $|\ |_v$ 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.

- Product formula:
$$\prod_{v \in M(K)} |a|_v^{d_v} = 1,$$
for each $0 \neq a \in K$.

- Let $N \geq 2$, and for each $v \in M(K)$ define **local heights** on K_v^N:

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

for each $\boldsymbol{x} \in K_v^N$.

- **Global height** on K^N:

$$H(\boldsymbol{x}) = \left(\prod_{v \in M(K)} H_v(\boldsymbol{x})^{d_v} \right)^{1/d},$$

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 $\boldsymbol{x}$.

- For a polynomial F with coefficients in K, $H(F)$ is the height of its coefficient vector.

- For an L-dimensional subspace $V \subseteq K^N$ with a basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_L$, define

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

  This definition is independent of the choice of the basis.

Quadratic forms

Let

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

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

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

for the associated quadratic form. F is **isotropic** over K if it has a non-trivial zero with coordinates in K.

Cassels (1955); Raghavan (1975):

If F is isotropic over K, then there exists $\boldsymbol{0} \neq \boldsymbol{x} \in K^N$ such that $F(\boldsymbol{x}) = 0$, and

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

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

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, called the **Witt index** of (Z, F).

Schlickewei (1985); Vaaler (1987):

If (Z, F) has Witt index $k \geq 1$, then 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.

Witt decomposition

From here on orthogonality is always with respect to F. We define the **singular component** of (Z, F) to be

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

The **rank** of F on Z is $r = L - \dim_K(Z^{\perp})$.

A subspace $W \subseteq Z$ is called **anisotropic** if $F(\boldsymbol{x}) \neq 0$ for each $\boldsymbol{0} \neq \boldsymbol{x} \in W$.

If $\boldsymbol{x}, \boldsymbol{y} \in Z$ are such that

$$F(\boldsymbol{x}) = F(\boldsymbol{y}) = 0, \ \ F(\boldsymbol{x}, \boldsymbol{y}) = 1,$$

then the subspace $\mathbb{H} = \mathrm{span}_K\{\boldsymbol{x}, \boldsymbol{y}\}$ is called a **hyperbolic plane**.

Witt (1937):

There exists an orthogonal decomposition of (Z, F) *of the form*

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

where W *is anisotropic.*

Theorem 1 (F. (2005)). *There exists a decomposition like (1) with*

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

and

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

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

The proof of this theorem makes use of the Schlickewei-Vaaler theorem on the existence of a small-height maximal totally isotropic subspace of (Z, F).

Quadratic forms over $\overline{\mathbb{Q}}$

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

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

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

$$k = \left[\frac{L}{2}\right],$$

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

Theorem 2 (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 $k = \left[\frac{L}{2}\right]$ 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 2 can be better.

- Theorem 2 is a statement in the general spirit of "absolute" results, in particular it parallels the development of Siegel's lemma, 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

$$Z = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k \perp W, \tag{2}$$

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 3 (F. (2005)). *There exists an orthogonal decomposition as in (2) such that for each* $1 \leq i \leq k = \left[\frac{L}{2}\right]$

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

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

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

if $L = 2k + 1$.

In addition, we prove the following **orthogonal** version of Siegel's lemma for a bilinear space.

Theorem 4 (F. (2005)). *Let (Z, F) be an L-dimensional symmetric bilinear space in N variables, not necessarilly regular, over a number field K with $1 \leq L < N$. Then there exists a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ over K for Z such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $i \neq j$, and*

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

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

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