Effective decompositions of quadratic spaces

Lenny Fukshansky

Texas A&M University

April 2, 2005

Quadratic forms

Let K be a number field of degree d over $\mathbb{Q}$, $N \geq 2$ be an integer, and 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 with coefficients in K. We write

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

for the associated quadratic form in N variables. We say that F is **isotropic** over K if there exists a non-zero $\boldsymbol{x} \in K^N$ such that $F(\boldsymbol{x}) = 0$.

Question 1: *How do we decide whether F is isotropic over K?*

Question 2: *Assuming it is, how do we find a non-trivial zero of F over K?*

We will introduce an approach that allows to answer both question simultaneously. For this we first need some notation.

Height functions

Let $M(K)$ be the set of places of K. For each place $v \in M(K)$ let K_v be the completion of K at v and $d_v = [K_v : \mathbb{Q}_v]$ be the local degree. 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 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

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

We extend absolute values to vectors by defining the local heights. For each $v \in M(K)$ define a local height H_v for each $\boldsymbol{x} \in K_v^N$ by

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

We define the following global height function on K^N:

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} H_v(\boldsymbol{x}), \tag{2}$$

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

Heights can be extended to polynomials: if

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

we write $H(F)$ to mean the height of its coefficient vector. We can also define height on elements of $GL_N(K)$ by viewing them as vectors in K^{N^2}. Finally, we define height on subspaces of K^N. Let $V \subseteq K^N$ be a J-dimensional subspace, and let $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$ be a basis for V. Then

$$\boldsymbol{x}_1 \wedge ... \wedge \boldsymbol{x}_J \in K^{\binom{N}{J}}$$

under the standard embedding. Define

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

This definition is legitimate, i.e. does not depend on the choice of the basis.

A fundamental property of height is the following.

Northcott's theorem: *The set*

$$\{\boldsymbol{x} \in K^N : H(\boldsymbol{x}) \leq B\}$$

is finite for every positive real number B.

Now suppose that our quadratic form F is isotropic over K. If we can prove that F has a non-trivial zero of bounded height over K with an explicit bound, we reduce the search for a non-trivial zero to a finite set. Hence we answer both questions 1 and 2 simultaneously.

Theorem 1. *Suppose that F is isotropic over K. Then there exists a non-zero point $\boldsymbol{x} \in K^N$ such that $F(\boldsymbol{x}) = 0$, and*

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

where C_1 is an explicit constant that depends on K and N.

This theorem has first been proved over $\mathbb{Q}$ by Cassels in 1955, and generalized to number fields by S. Raghavan in 1975.

Effective structure theorems

We start with some notation. Let F be a symmetric bilinear form with associated quadratic form on K^N, as above. Let $Z \subseteq K^N$ be a subspace of dimension L, $2 \leq L \leq N$. Then Z equipped with F is a symmetric bilinear space over K, we write (Z, F) to denote it. A subspace W of Z is said to be **totally isotropic** if $F(W) = \{0\}$. All maximal totally isotropic subspaces of (Z, F) have the same dimension, called **Witt index** of (Z, F).

Theorem 2 (Vaaler, 1987). *Let $M \geq 1$ be the Witt index of (Z, F) over K. Then there exists a maximal totally isotropic subspace W of (Z, F) such that*

$$H(W) \leq C_2 H(F)^{\frac{L-M}{2}} H(Z)$$

where C_2 is an explicit constant that depends on K, L, and M.

More generally, I have recently shown that (Z, F) has a whole orthogonal decomposition into special subspaces of bounded height, where **orthogonality** denoted by $\perp$ is always meant with respect to the symmetric bilinear form F. First we continue with some more notation.

A subspace U of (Z, F) is **anisotropic** if $F(\boldsymbol{x}) \neq 0$ for all $\mathbf{0} \neq \boldsymbol{x} \in U$. A subspace V 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 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 $U \cap U^{\perp} = \{\mathbf{0}\}$.

Two vectors $\boldsymbol{x}, \boldsymbol{y} \in Z$ are called a **hyperbolic pair** if $F(\boldsymbol{x}) = F(\boldsymbol{y}) = 0$, $F(\boldsymbol{x}, \boldsymbol{y}) = 1$.

The subspace

$$\mathbb{H}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{span}_K\{\boldsymbol{x}, \boldsymbol{y}\}$$

is regular and is called a **hyperbolic plane**. An orthogonal sum of hyperbolic planes is called a hyperbolic space. Every hyperbolic space is regular.

A classical theorem of Witt states that there exists an orthogonal decomposition of (Z, F) of the form

$$Z = Z^\perp \perp \mathbb{H}_1 \perp \; \dots \; \perp \mathbb{H}_M \perp V$$

where $Z^\perp = \{\boldsymbol{x} \in Z : F(\boldsymbol{x}, \boldsymbol{z}) = 0 \; \forall \; \boldsymbol{z} \in Z\}$ is the **singular component**, $\mathbb{H}_i$ are hyperbolic planes, and V is **anisotropic component**.

Theorem 3 (F., 2005). *Let (Z, F) be as above, and let r be rank of F on Z, $1 \leq r \leq L$. There exists a Witt decomposition of (Z, F) with*

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

and

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

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

Using a similar method, I am also proving a related result on the small-height orthogonal decompsoition of (Z, F) into one-dimensional subspaces, i.e. an "orthogonal" version of **Siegel's lemma** for Z with respect to F.

Theorem 4 (F., 2005). *Let (Z, F) be as above. Then there exists a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_L \in K^N$ for Z such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $i \neq j$, and*

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

where $\mathcal{D}_K$ is the discriminant of the number field K.

Isometry group

The classical version of Witt decomposition theorem can be deduced from the 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

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

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

$$\sigma = \tau_1 ... \tau_l$$

where $0 \leq l \leq L$.

The following is a slightly weaker effective version of Cartan-Dieudonné theorem.

Theorem 5 (F., 2004). *Let (Z, F) be a regular symmetric bilinear 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 $\tau_1, ..., \tau_l \in \mathcal{O}(Z, F)$ such that*

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

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.