Heights and effective theory of quadratic forms over global fields

Lenny Fukshansky
Claremont McKenna College

Workshop on the Arithmetic of Quadratic Forms and Integral Lattices

December 13-14, 2010

Cassels' Theorem

Let $N \geq 2$, 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 $\mathbb{Z}$. Define its associated quadratic form

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

In **1955, J. W. S. Cassels** proved that if F is isotropic, then there exists $\boldsymbol{x} \in \mathbb{Z} \setminus \{\boldsymbol{0}\}$ such that $F(\boldsymbol{x}) = 0$, and

$$(1) \qquad \max_{1 \leq i \leq N} |x_i| \leq \left(3 \sum_{i=1}^{N} \sum_{j=1}^{N} |f_{ij}| \right)^{\frac{N-1}{2}}.$$

The expressions on the left and right hand sides of (1) are examples of **heights** of a vector and of a quadratic form, respectively. Since sets of integral points with explicitly bounded height are always finite, (1) provides an explicit **search bound** for non-trivial zeros of F. The exponent $\frac{N-1}{2}$ in the upper bound is sharp, as shown by an example due to **M. Knesser**.

What about heights?

The notion of height as above can be extended to number fields and function fields.

Height functions are fundamental tools of arithmetic geometry – they measure the *arithmetic complexity* of objects in much the same way that *degree* in algebraic geometry measures *geometric complexity*.

An especially important property of heights over number fields and function fields with finite coefficient fields is –

Northcott's finiteness property: For each real constant B the set of projective points with height bounded above by B is finite.

This finiteness property makes statements on the existence of objects of bounded height *effective*.

Over global fields

Analogues of Cassels' theorem over a global field K with respect to appropriately defined height functions have been obtained:

- In 1975 by **S. Raghavan** when K is a number field

- In 1987 by **A. Prestel** when K is a rational function field

- In 1997 by **A. Pfister** when K is an algebraic function field

The exponent on height of F in the upper bounds is again $\frac{N-1}{2}$.

In addition, Raghavan produced an analogous result for zeros of **hermitian forms** over CM number fields, where the exponent in the upper bound is $\frac{2N-1}{2}$.

Additional extensions of Cassels' theorem have been obtained by

- **Birch & Davenport**, 1958
- **Chalk**, 1980
- **Davenport**, 1957 & 1971
- **Schulze-Pillot**, 1983
- **Watson**, 1956

and others. In particular, results of Chalk, Davenport (1971) and Schulze-Pillot established existence theorems for collections of linearly independent isotropic vectors of bounded height.

Notation and heights

A more general effective theory followed these results. To survey it we need some notation.

Let K be either a number field, a function field, or algebraic closure of one or the other; we write $\overline{K}$ for the algebraic closure of K, so it may be that $K = \overline{K}$. In fact, until further notice assume that $K \neq \overline{K}$.

By a function field we will always mean a finite algebraic extension of the field $\mathfrak{K} = \mathfrak{K}_0(t)$ of rational functions in one variable over a field $\mathfrak{K}_0$, where $\mathfrak{K}_0$ can be any field.

In the number field case, we write $d = [K : \mathbb{Q}]$ for the global degree of K over $\mathbb{Q}$; in the function field case, the degree is $d = [K : \mathfrak{K}]$.

Let $M(K)$ be the set of places of K. For each place $v \in M(K)$, write K_v for the completion of K at v and let d_v be the local degree of K at v, which is $[K_v : \mathbb{Q}_v]$ in the number field case, and $[K_v : \mathfrak{K}_v]$ in the function field case.

For each place u of the ground field, be it $\mathbb{Q}$ or $\mathfrak{K}$, we have

$$\sum_{v \in M(K), v|u} d_v = d. \tag{2}$$

If K is a number field, then 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.

If K is a function field, then all absolute values on K are non-archimedean. For each $v \in M(K)$, let $\mathcal{O}_v$ be the valuation ring of v in K_v and $\mathfrak{M}_v$ the unique maximal ideal in $\mathcal{O}_v$. We choose the unique corresponding absolute value $| \ |_v$ such that:

(i) if $1/t \in \mathfrak{M}_v$, then $|t|_v = e$,

(ii) if an irreducible polynomial $p(t) \in \mathfrak{M}_v$, then $|p(t)|_v = e^{-\deg(p)}$.

In both cases, for each nonzero $a \in K$ the **product formula** reads

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

We can now define local norms on each K_v^N:

$$|\boldsymbol{x}|_v = \max_{1 \le i \le N} |x_i|_v,$$

and for all archimedean places v also define

$$\|\boldsymbol{x}\|_v = \left(\sum_{i=1}^N |x_i|_v^2 \right)^{1/2},$$

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

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

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

H is defined on the projective space $\mathbb{P}^{N-1}(K)$:

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

which is true by the product formula.

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

We also define height on subspaces of K^N. Let $V \subseteq K^N$ be an L-dimensional subspace, and let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L$ be a basis for V. Then

$$\boldsymbol{y} := \boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_L \in K^{\binom{N}{L}}$$

under the standard embedding. Define

$$\mathcal{H}(V) := \prod_{v \nmid \infty} |\boldsymbol{y}|_v^{d_v/d} \times \prod_{v \mid \infty} \|\boldsymbol{y}\|_v^{d_v/d}.$$

This definition is independent of the choice of the basis by the product formula.

The normalizing exponent $1/d$ in the definition of H and $\mathcal{H}$ ensures that our heights are **absolute**, i.e. do not depend on the field of definition.

Isotropic subspaces of bounded height

In **1985, Schlickewei** showed that if F is an isotropic rational quadratic form in $N \geq 2$ variables, and $M < N$ is the dimension of a maximal totally isotropic subspace of the quadratic space $(\mathbb{Q}^N, F)$, then there exists such a subspace W with

$$\mathcal{H}(W) \ll_N H(F)^{\frac{N-M}{2}}.$$

In **1987, Vaaler** generalized this result and extended it to number fields. Specifically, let K be a number field, $N \geq 2$ and $1 \leq L \leq N$ integers, $V \subseteq K^N$ an L-dimensional subspace, F a quadratic form over K in N variables, and (V, F) a quadratic space. Let $M \leq L/2$ be the Witt index of (V, F) and λ dimension of the radical. Then there exists a maximal totally isotropic subspace $W \subset V$ of dimension $M+\lambda$ such that

$$\mathcal{H}(W) \ll_{K,L,M,\lambda} H(F)^{\frac{L-M-\lambda}{2}} \mathcal{H}(V).$$

Analogous result over $\overline{\mathbb{Q}}$

For quadratic spaces over $\overline{\mathbb{Q}}$, we have:

(F., 2008) Let $V \subseteq \overline{\mathbb{Q}}^N$, $\dim V = L$, and consider the quadratic space (V, F). Let $V^{\perp}$ be the radical of V, so that $\dim V^{\perp} = \lambda$, and $M = \left[\frac{L-\lambda}{2}\right]$ is the Witt index of V. Then

$$V = V^{\perp} \perp U,$$

where U is regular, $\dim U = L - \lambda$, and

$$\mathcal{H}(V^{\perp}) \ll_L H(F)^{L-\lambda}\mathcal{H}(V)^2,\ \mathcal{H}(U) \ll_L \mathcal{H}(V).$$

There also exists a maximal totally isotropic subspace W of U so that $\dim W = M$ and

$$\mathcal{H}(W) \ll_M \begin{cases} H(F)^{\frac{M^2}{2}}\mathcal{H}(U)^{\frac{M^2+M+2}{2M}} & \text{if } 2 \mid L-\lambda \\ H(F)^{M^2}\mathcal{H}(U)^{\frac{4M}{3}} & \text{if } 2 \nmid L-\lambda. \end{cases}$$

Then $W' := \operatorname{span}_{\overline{\mathbb{Q}}}\{V^{\perp}, W\}$ is a maximal totally isotropic subspace of V, $\dim W' = M + \lambda$, and

$$\mathcal{H}(W') \leq \mathcal{H}(V^{\perp})\mathcal{H}(W).$$

Families of isotropic subspaces

In **1989, Vaaler** proved the following result over number fields, building on previous work by **Schlickewei and Schmidt (1987)** over $\mathbb{Q}$:

Given a quadratic space (V,F) over a number field K, as above, there exists a family

$$U_0,\dots,U_{L-M} \subseteq V$$

of maximal totally isotropic subspaces of V such that

$$V = \text{span}_K\{W_0,\dots,W_{L-M}\}$$

and for each $0 \leq i \leq L-M$,

$$\mathcal{H}(W_0)\mathcal{H}(W_i) \ll_{K,L,M} H(F)^{L-M}\mathcal{H}(V)^2.$$

In joint work **(W. K. Chan, L. F., G. Henshaw; in progress)**, we show that in fact there exists an infinite sequence of families of maximal totally isotropic subspaces

$$\{W_{n1}, \dots, W_{nJ}\}_{n=1}^{\infty} \subseteq V,$$

where $J = M(L - 2M - \lambda)$, such that for each $n \geq 1$,

$$\text{span}_K \{W_{n1}, \dots, W_{nJ}\} = V,$$

and for each $1 \leq j \leq J$,

$$\mathcal{H}(W_{nj}) \ll H(F)^{\mathsf{p}(L,M)} \mathcal{H}(V)^{\mathsf{q}(M)},$$

where the constant in the upper bound depends on K, N, L, M, λ, n, and $\mathsf{p}(L, M)$, $\mathsf{q}(M)$ are polynomials: $\mathsf{p}(L, M)$ is linear in L, quartic in M, and $\mathsf{q}(M)$ is cubic in M.

We have also obtained an analogous result over $\overline{\mathbb{Q}}$, and are working on the function field case.

Witt decomposition (F., 2007-2008)

Let K be a number field or $\overline{\mathbb{Q}}$, and let (V, F) be an L-dimensional quadratic space in N variables over K, as above. Let $r := L - \lambda$ be the rank of F on V. There exists an orthogonal decomposition of the quadratic space (V, F) of the form

$$V = V^{\perp} \perp \mathbb{H}_1 \perp \ \cdots \perp \mathbb{H}_M \perp U,$$

where $\mathbb{H}_1, \dots, \mathbb{H}_M$ are hyperbolic planes and U is anisotropic component, with all components of bounded height. Specifically, if K is a number field, then

$$\mathcal{H}(V^{\perp}) \ll_{K,L,r} H(F)^{r/2} \mathcal{H}(V),$$

as proved by **Vaaler (1989)**, and

$$\max\{\mathcal{H}(\mathbb{H}_i), \mathcal{H}(U)\} \ll \left\{ H(F)^{\frac{L+2M}{4}} \mathcal{H}(V) \right\}^{e_1(M)},$$

for each $1 \leq i \leq M$, where

$$e_1(M) = \frac{(M+1)(M+2)}{2}$$

and the constant depends on N, L, M.

If $K = \overline{\mathbb{Q}}$, then

$$\mathcal{H}(V) \ll_{L,r} H(F)^r \mathcal{H}(V)^2,$$

and

$$\mathcal{H}(\mathbb{H}_i) \ll \left\{ H(F)^{M^2+1} \mathcal{H}(V)^{\frac{6M+5}{4M+2}} \right\}^{e_2(M)},$$

where

$$e_2(M) = \frac{(M+1)(M+2)}{2} \left(\frac{3}{2}\right)^M$$

and the constant depends on L, M, r, and $U = \{\mathbf{0}\}$ if $L = 2M$, or $U = \overline{\mathbb{Q}}\boldsymbol{y}$ with

$$\mathcal{H}(U) \ll_{L,M,r} \mathcal{H}(V)^{\frac{2M+3}{4M+2}},$$

if $L = 2M + 1$.

In a joint project **(W. K. Chan, F., G. Henshaw; in progress)** we are working to obtain function field analogue of these results.

Symplectic spaces (F., 2009)

Let K be a number field, function field, or the algebraic closure of one or the other. Let

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

be an alternating bilinear form in $N \geq 2$ variables with coefficients in K. Let $V \subseteq K^N$ be a $2M$-dimensional subspace, $1 \leq M \leq N/2$, such that (V, F) is a regular symplectic space over K. Define

$$a(M) = \begin{cases} \frac{M^2+4M}{4} & \text{if } 2 \mid M \\ \frac{M^2+4M-1}{4} & \text{if } 2 \nmid M, \end{cases}$$

and

$$b(M) = \begin{cases} \frac{2M^3+9M^2-14M}{12} & \text{if } 2 \mid M \\ \frac{2M^3+9M^2-14M+3}{12} & \text{if } 2 \nmid M. \end{cases}$$

For each $1 \leq n \leq M$, there exist totally isotropic subspaces U_n and W_n of (V, F) such that

$$\dim_K U_n = \dim_K W_n = n, \; U_n \cap W_n = \{\mathbf{0}\}$$

and

$$U_1 \subset U_2 \subset \cdots \subset U_M, \; W_1 \subset W_2 \subset \cdots \subset W_M,$$

so that $V = \text{span}_K\{U_M, W_M\}$, and

$$\mathcal{H}(V_n)\mathcal{H}(W_n) \ll_{K,N,M} \left(\mathcal{H}(V)^{a(M)}\mathcal{H}(F)^{b(M)}\right)^{\frac{n}{M}}.$$

Moreover,

$$V = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_M,$$

where for each $1 \leq i \leq M$, $\mathbb{H}_i$ is a hyperbolic plane, and

$$\prod_{i=1}^{M} \mathcal{H}(\mathbb{H}_i) \ll_{K,N,M} \mathcal{H}(V)^{a(M)} H(F)^{b(M)}.$$

Hermitian forms (Chan, F., 2010)

Let K be a **totally real** number field of degree d, and let $\alpha, \beta \in O_K$ be **totally negative**. Let $D = \binom{\alpha,\beta}{K}$ be a positive definite quaternion algebra over K, generated by the elements i, j, k which satisfy the relations $i^2 = \alpha,\ j^2 = \beta,\ ij = -ji = k,\ k^2 = -\alpha\beta$. Let $\mathcal{O}$ be an order in D. Let $N \geq 2$ be an integer, and let $V \subseteq D^N$ be an L-dimensional right D-subspace, $1 \leq L \leq N$. Let $F(\boldsymbol{X}, \boldsymbol{Y}) \in D[\boldsymbol{X}, \boldsymbol{Y}]$ be a hermitian form in $2N$ variables, and assume that F is isotropic on V. Then there exists a basis $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$ for V over D such that $F(\boldsymbol{y}_n) := F(\boldsymbol{y}_n, \boldsymbol{y}_n) = 0$ for all $1 \leq n \leq L$, $h(\boldsymbol{y}_1) \leq \dots \leq h(\boldsymbol{y}_L)$, and

$$h(\boldsymbol{y}_1)h(\boldsymbol{y}_L) \ll_{K,\mathcal{O},N,L,\alpha,\beta} H_{\mathsf{inf}}(F)^{4L-1} H^{\mathcal{O}}(V)^8,$$

for appropriately defined height functions h, H_{inf}, and $H^{\mathcal{O}}$, following the approach of **C. Liebendorfer (2004)**.

This is an analogue of a result of **Vaaler (1989)** over number fields.

Further work

Some of the additional work done includes investigation of small zeros of quadratic forms over a field K outside of unions of subspaces and varieties:

- In 1998 by **D. Masser:** $K = \mathbb{Q}$, outside of one hyperplane
- In 2004 by **L. F.:** K is a number field, union of m hyperplanes
- In 2009 by **R. Dietmann:** better bound when $m > 1$
- In progress by **W. K. Chan, L. F., G. Henshaw:** K is a number field or $\overline{\mathbb{Q}}$, in a vector space missing a union of varieties

In a joint project **(W. K. Chan, F., G. Henshaw; in progress)** we are working to obtain function field analogue of these results.