Searching for rational points on varieties over global fields

Lenny Fukshansky
Claremont McKenna College

Uppsala Universitet
Matematiska kollokviet
November 19, 2010

Hilbert's Tenth Problem

Consider a system of M Diophantine equations in N variables, i.e.

$$\left.\begin{array}{l} P_1(X_1,\ldots,X_N) = 0 \\ \vdots \\ P_M(X_1,\ldots,X_N) = 0 \end{array}\right\} \qquad (1)$$

where $P_1,\ldots,P_M$ are polynomials with integer coefficients.

Question 1. *Does this system have a non-trivial integral solution?*
Question 2. *Assuming it does, how do we find such a solution?*

Both questions are very difficult. The famous result of **Y. Matijasevich** (1970; building on the previous work by **M. Davis, H. Putnam** and **J. Robinson** - 1961) implies that Question 1 in general is undecidable.

But what if. . .

Suppose that we could prove a theorem of the following kind:

If the system (1) *has a nontrivial solution vector* $\boldsymbol{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$*, then there exists such a solution vector with*

$$|\boldsymbol{x}| := \max_{1 \le i \le N} |x_i| \le B \tag{2}$$

for some explicit constant $B = B(P_1, \ldots, P_M)$*. We refer to* $|\boldsymbol{x}|$ *as the* **height** *of* $\boldsymbol{x}$*.*

Then to answer Question 1, it would be enough to check whether any of the vectors in the finite set

$$\left\{ \boldsymbol{x} \in \mathbb{Z}^N : \max_{1 \le i \le N} |x_i| \le B \right\}$$

is a solution of (1). In other words, this would reduce Question 1 to a finite search algorithm.

Search bounds

Moreover, if the Question 1 is answered affirmatively, then this finite search algorithm simultaneously provides an answer to Question 2.

We will refer to a constant B satisfying (2) as an explicit **search bound** (with respect to height $|\ |$) for the polynomial system $P_1, \dots, P_M$. Hence Questions 1 and 2 can be replaced by -

Question 3. *Assuming the polynomial system $P_1, \dots, P_M$ has a nontrivial integral solution, can we find an explicit search bound?*

Well, can we?

Existence of search bounds for general polynomial systems like (1) would contradict Matijasevich's theorem, and hence search bounds in general cannot exist.

Moreover, it was proved by **J. P. Jones** (1980) that the question whether a single Diophantine equation of degree four or larger has a solution in positive integers is already undecidable.

This suggests that search bounds for equations of degree ≥ 4 may be out of reach, and relatively little is known even for degree 3 (although some work has been done, especially in the recent years). There is however a wealth of results for degree 1 and 2, which will be the main focus of this talk.

The homogeneous linear case

Let

$$A\boldsymbol{x} = \boldsymbol{0} \qquad (3)$$

be an $M \times N$ linear system of rank $M < N$ with integer entries. As above, we will write

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

for the height of a vector $\boldsymbol{x} \in \mathbb{Z}^N$. Similarly, we define the height of the coefficient matrix

$$A = (a_{ij})_{1 \leq i \leq M, 1 \leq j \leq N}$$

by

$$|A| := \max\{|a_{ij}| : 1 \leq i \leq M, 1 \leq j \leq N\}.$$

Question 4. *What is the smallest height of a nontrivial integral solution to (3)?*

Indeed, it is natural to expect that there must exist a solution vector $\boldsymbol{x}$ with $|\boldsymbol{x}|$ not too large, compared to $|A|$.

Siegel's lemma

In 1929 **Carl Ludwig Siegel** proved that there exists a non-trivial integral solution $\boldsymbol{x}$ to (3) with

$$|\boldsymbol{x}| \leq (1 + N|A|)^{\frac{M}{N-M}}. \tag{4}$$

The proof uses Dirichlet box principle. In fact, a similar result was at least informally observed by **Axel Thue** as early as 1909. This result is best possible in the sense that the exponent $\frac{M}{N-M}$ in (4) cannot be improved.

Results of this sort are known under the general name of **Siegel's lemma**, and are very important in transcendental number theory.

In the recent years Siegel's lemma was studied by many authors in Diophantine approximations for its own sake as well: as the simplest case of an **effective** existence result for rational points on varieties.

The inhomogeneous linear case

Instead of (3), consider now an inhomogeneous $M \times N$ linear system

$$A\boldsymbol{x} = \boldsymbol{b}, \tag{5}$$

where $\boldsymbol{b} \in \mathbb{Z}^M$. Define

$$\mathcal{D}(A) := \text{gcd} \ \{ \ \det C : \\ C \text{ is an } M \times M \text{ minor of } A\}.$$

Then a classical result of **I. Heger** (1856) states that (5) has a solution in $\mathbb{Z}^N$ if and only if

$$\mathcal{D}(A) = \mathcal{D}((A \ \boldsymbol{b})).$$

When this is the case, a result of **Borosh, Flahive, Rubin,** and **Treybig** (1989) states that there exists such a solution $\boldsymbol{x} \in \mathbb{Z}^N$ with

$$|\boldsymbol{x}| \leq \max \ \{ \ |\det C| : \\ C = M \times M \text{ minor of } (A \ \boldsymbol{b})\}.$$

One quadratic form

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 $2N$ variables, $N \geq 2$, with integer coefficients, and let

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

be the associated quadratic form. A famous result of **J. W. S. Cassels** (1955) states that if F has a nontrivial rational zero, then there exists $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^N$ such that $F(\boldsymbol{x}) = 0$ and

$$|\boldsymbol{x}| \ll_N |F|^{\frac{N-1}{2}}, \tag{6}$$

where

$$|F| := \max_{1 \leq i,j \leq N} |f_{ij}|,$$

and the constant in the upper bound is explicit. The exponent $\frac{N-1}{2}$ in the upper bound is best possible.

The inhomogeneous quadratic case

Now assume that an inhomogeneous quadratic equation in $N \geq 3$ variables with integer coefficients

$$\sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i X_j + \sum_{i=1}^{N} f_{i0} X_i + f_{00} = 0$$

has an integral solution. **R. Dietmann** (2003), building on previous work by **Siegel** (1972) and **Kornhauser** (1990), showed that in this case there exists a solution $\boldsymbol{x} \in \mathbb{Z}^N$ with

$$|\boldsymbol{x}| \ll_N |F|^{p(N)}, \tag{7}$$

where $p(N)$ is a linear polynomial ($\approx 5N+C$).

In case $N = 2$, **Kornhauser** (1990) showed that only exponential bounds are possible.

Generalizing to global fields

From now on we will work with homogeneous polynomials only, and so we can work over fields instead of rings, which is more convenient.

Let K be a **global field**, i.e. a number field, function field (= finite algebraic extension of $E(t)$, where E is any perfect coefficient field), or the algebraic closure of one or the other. Let $\mathcal{X}_K$ be a projective variety over K.

Problem 1. *Find a search bound $B = B(\mathcal{X}_K)$ such that if $\mathcal{X}_K$ is not empty, then it contains a point $\boldsymbol{x}$ with*

$$H(\boldsymbol{x}) \ll B,$$

where H is an appropriately defined height function.

Absolute values

First let K be a number field or a function field and let $\mathfrak{K}$ be the **ground field**, i.e. $\mathfrak{K} = \mathbb{Q}$ or $\mathfrak{K}_0(t)$, respectively, then $K \subset \overline{K}$, the algebraic closure of $\mathfrak{K}$. Let $d = [K : \mathfrak{K}]$ be the **global degree** of K over $\mathfrak{K}$.

There are infinitely many **absolute values** on K: those that satisfy the triangle inequality

$$|a + b| \leq |a| + |b|,$$

but not the ultrametric inequality

$$|a + b| \leq \max\{|a|, |b|\},$$

are called **archimedean**, and those that satisfy the ultrametric inequality are called **non-archimedean**. We can define an equivalence relation on absolute values: $| \ |_1$ and $| \ |_2$ are said to be equivalent if there exists a real number θ such that

$$|a|_1 = |a|_2^{\theta}$$

for all $a \in K$.

Places

We write $M(K)$ for the set of all equivalence classes of absolute values (called **places**) of K. We write $v \mid u$ if the place $v \in M(K)$ **lies over** (i.e. extends) the place $u \in M(\mathfrak{K})$. All archimedean places of K lie over the same place $\infty \in M(\mathbb{Q})$ if K is a number field (i.e. they are all equivalent); function fields have no archimedean places.

We write K_v for the completion of K at v and let $d_v = [K_v : \mathfrak{K}_v]$ be the local degree of K at v. For each place $u \in M(\mathfrak{K})$, we have

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

If K is a number field, then for each place $v \in M(K)$ pick a representative $|\ |_v$ to be the unique absolute value on K_v that extends either the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$ if $v \mid \infty$, or the usual p-adic absolute value on $\mathbb{Q}_p$ if $v \mid p$, 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 $\mathfrak{O}_v$ be the valuation ring of v in K_v and $\mathfrak{M}_v$ the unique maximal ideal in $\mathfrak{O}_v$. 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 **Artin-Whaples product formula** reads

$$\prod_{v \in M(K)} |a|_v^{d_v} = 1. \tag{8}$$

Height functions

We can define local norms on each K_v^N by

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

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 $\boldsymbol{x} = (x_1, \dots, x_N) \in K_v^N$. 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 $\boldsymbol{x} \in K^N$. This product is convergent because only finitely many of the local norms for each vector $\boldsymbol{x} \in K^N$ 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. H is called projective because it is well defined on the projective space $\mathbb{P}^{N-1}(K)$, i.e.

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

which is true by the product formula.

Schmidt's height on subspaces

We can also talk about height of subspaces of K^N, as first introduced by **W. M. Schmidt** (1967). 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

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

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 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.

Finiteness property

A very important property that both of these heights satisfy is –

Northcott's theorem: *If K is a number field or a function field over a finite coefficient field, then for every $B \in \mathbb{R}_{>}0$ the sets*

$$\left\{ [\boldsymbol{x}] \in \mathbb{P}(K^N) : H(\boldsymbol{x}) \leq B \right\}$$

and

$$\left\{ \mathbb{P}(V) \subseteq \mathbb{P}(K^N) : \mathcal{H}(V) \leq B \right\}$$

are finite.

More generally, height measures arithmetic complexity, and so a point of relatively small height is "arithmetically simple". This makes search bounds on height interesting even when Northcott's theorem fails.

We are now ready to apply this machinery.

Generalized Siegel's lemma

The following result has been obtained by **E. Bombieri** and **J. Vaaler** (1983) if K is a number field, by **J. Thunder** (1995) if K is a function field, and by **D. Roy** and **J. Thunder** (1996) if K is the algebraic closure of one or the other.

Theorem 1. *Let K be a number field, a function field, or the algebraic closure of one or the other. Let $V \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$. Then there exists a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_L$ for V over K such that*

$$\prod_{i=1}^{L} H(\boldsymbol{v}_i) \ll_{K,L} \mathcal{H}(V). \tag{9}$$

The exponent 1 on $\mathcal{H}(V)$ in this bound is smallest possible.

Corollaries

An immediate consequence of Theorem 1 is the existence of a nonzero point $\boldsymbol{v}_1 \in V$ such that

$$H(\boldsymbol{v}_1) \ll_{K,L} \mathcal{H}(V)^{1/L}. \tag{10}$$

Moreover, a standard property of heights is that for any basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L$ for V,

$$\mathcal{H}(V) \ll_L \prod_{i=1}^{L} H(\boldsymbol{x}_i). \tag{11}$$

Hence Theorem 1 implies that for each $M \leq L$, there exists an M-dimensional subspace $U_M \subseteq V$ such that

$$\mathcal{H}(U_M) \ll_{K,L,M} \mathcal{H}(V)^{M/L}.$$

This is a statement about the existence of search bounds on Grassmanians of a vector space over any global field.

Faltings' version

In 1992 **Gerd Faltings** proved a refinement of Siegel's lemma, which guaranteed the existence of a small-height point in a vector space outside of a proper subspace, all over $\mathbb{Q}$. Here is a generalization of Faltings' result.

Theorem 2 (F. (2010))**.** *Let K be a number field, function field, or $\overline{\mathbb{Q}}$. Let $N \geq 2$ be an integer, and let V be an L-dimensional subspace of K^N, $1 \leq L \leq N$. Let $\mathcal{Z}_K$ be a union of algebraic varieties defined over K such that $V \not\subseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. Then there exists a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_L \in V \setminus \mathcal{Z}_K$ for V over K such that for each $1 \leq n \leq L$,*

$$H(\boldsymbol{x}_n) \ll_{K,L,M} \mathcal{H}(V). \tag{12}$$

The exponent 1 on $\mathcal{H}(V)$ in the bound of (12) is sharp in general. As above, Theorem 2 along with (11) establishes the existence of small-height points on the Grassmanians of V outside of $\mathcal{Z}_K$.

Back to quadratic forms

Cassels' theorem has been generalized over number fields by **S. Raghavan (1975)** (also for inhomogeneous quadratic polynomials by **D. Masser** (1998)), over rational function fields by **A. Prestel (1987)**, and over algebraic function fields by **A. Pfister (1997)**.

However, nothing is known for **systems of quadratic forms** even over $\mathbb{Q}$, not even for simultaneous zeros of two quadratic forms. In fact, it is not at all clear that search bounds exist in this situation, since degree of the intersection of two quadratic hypersurfaces is four; this may come into conflict with Jones' theorem.

While Hilbert's 10-th problem is still open over number fields, it seems unlikely that search bounds for general systems of quadratic forms can exist. In fact, it is known that the question about solvability of any system of Diophantine equations can be reduced to the question of solvability of a system of integral quadratic equations.

Isotropic subspaces

Let K be a number field, and let $V \subset K^N$ be an L-dimensional subspace and $F(\boldsymbol{X})$ a quadratic form over K, which is **isotropic** on V (i.e. has a nontrivial zero on V). A subspace $U \subseteq V$ is called **totally isotropic** if $F(U) = 0$. All maximal totally isotropic subspaces of V over K have the same dimension, called the **Witt index** of V; we denote it by $\mathcal{W} = \mathcal{W}(V)$.

Theorem 3 (Vaaler (1989)). *There exists a collection of $L - \mathcal{W} + 1$ maximal totally isotropic subspaces $U_0, \dots, U_{L-\mathcal{W}} \subseteq V$ such that*

$$\text{span}_K \{U_0, \dots, U_{L-\mathcal{W}}\} = V.$$

and for each $0 \leq i \leq L - \mathcal{W}$,

$$\mathcal{H}(U_0)\mathcal{H}(U_i) \ll_{K,L,\mathcal{W}} H(F)^{L-\mathcal{W}} \mathcal{H}(V)^2,$$

where $H(F)$ is height of the coefficient vector of F.

Infinite family

Here is a generalization of Vaaler's result, although with weaker bounds. Let λ be the dimension of the subspace of all singular points of F on V, called the **radical** of V with respect to F, and define

$$J := \mathcal{W}(L - 2\mathcal{W} - \lambda).$$

Theorem 4 (Chan, F., Henshaw (2010))**.** *There exists an infinite family of collections of maximal totally isotropic subspaces*

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

such that for each $n \geq 1$,

$$\mathrm{span}_K \{U_{n1}, \dots, U_{nJ}\} = V,$$

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

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

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

Fano varieties

As a set, the **Fano variety** of m-planes on a projective variety $\mathcal{X}_K$ defined over a field K, which we denote by $\mathcal{F}_m(\mathcal{X}_K)$, is the set of m-dimensional vector spaces over K which are contained in $\mathcal{X}_K$; this is a subvariety of the Grassmannian. We will also write $\mathcal{F}_m(\mathcal{Z}_K)$ for the set of m-dimensional vector spaces contained in any union of algebraic varieties $\mathcal{Z}_K$, defined over K.

Let

$$\mathcal{X}_K(V,F) = \{[\boldsymbol{x}] \in \mathbb{P}(V) : F(\boldsymbol{x}) = 0\}\,, \quad (13)$$

then Theorems 3 and 4 can be interpreted as statements about the existence of points of bounded height on $\mathcal{F}_{\mathcal{W}}(\mathcal{X}_K(V,F))$.

Moreover, Siegel's lemma combined with Theorems 3 and 4 immediately produces the analogous results for points on $\mathcal{F}_m(\mathcal{X}_K(V,F))$ for any $1 \leq m \leq \mathcal{W}$.

Missing a union of varieties

Finally, we can obtain a result in the spirit of Theorem 2 for quadratic spaces.

Theorem 5 (Chan, F., Henshaw (2010)). *Let (V, F) be an isotropic quadratic space of dimension L in N variables over a number field K, as above, and let $\mathcal{X}_K(F, V)$ be as in* (13). *Let $\mathcal{Z}_K$ be a union of algebraic varieties defined over K such that $\mathcal{X}_K(F, V) \nsubseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. Then for each $1 \leq m \leq \mathcal{W}$, there exists*

$$W_m \in \mathcal{F}_m(\mathcal{X}_K(V, F)) \setminus \mathcal{F}_m(\mathcal{Z}_K),$$

such that

$$\mathcal{H}(W_m) \ll_{K,L,M,m} H(F)^{7L-m+14} \mathcal{H}(V)^{12L+31}.$$

We also obtained analogues of Theorems 4 and 5 over $\overline{\mathbb{Q}}$ with slightly different bounds, and are currently working on the function field case.