

Heights and Diophantine problems

Lenny Fukshansky

Texas A&M University

September 30, 2004

Diophantine equations

The study of solutions to Diophantine equations is a very old subject. Suppose we have a system of M equations

$$\begin{aligned} P_1(X_1, \dots, X_N) &= 0 \\ &\vdots \\ P_M(X_1, \dots, X_N) &= 0 \end{aligned}$$

where P_1, \dots, 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 Matijasevich implies that Question 1 in general is undecidable. We will concentrate on Question 2.

Search bounds

Suppose that the system above has a non-trivial integral solution. Suppose we were able to prove that there exists a solution $\mathbf{x} = (x_1, \dots, x_N) \in \mathbb{Z}^N$ with

$$\max_{1 \leq i \leq N} |x_i| \leq B$$

for some explicit constant B . This means that we can restrict the search for a non-trivial solution to a finite set

$$\{\mathbf{x} \in \mathbb{Z}^N : \max_{1 \leq i \leq N} |x_i| \leq B\}.$$

We will refer to a constant B like this as an explicit **search bound** for the polynomial system P_1, \dots, P_M . Hence Question 2 can be replaced by the following.

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

A general answer to this question is currently known only for systems of linear equations and for one quadratic equation, where the known search bounds, as one would expect, depend on the coefficients of polynomials.

The discussion above can be generalized to \mathbb{Q} . Let P_1, \dots, P_M be polynomials with rational coefficients such that they have a common non-trivial rational zero. We want to find a search bound B such that there exists a non-trivial solution $\mathbf{x} = \left(\frac{x_1}{x_0}, \dots, \frac{x_N}{x_0} \right) \in \mathbb{Q}^N$ with

$$\max_{0 \leq i \leq N} |x_i| \leq B.$$

Notice that the set

$$\left\{ \left(\frac{x_1}{x_0}, \dots, \frac{x_N}{x_0} \right) \in \mathbb{Q}^N : \max_{0 \leq i \leq N} |x_i| \leq B \right\}$$

is again finite, so B is in fact a search bound.

Height functions

Now let K be a number field, i.e. a finite extension of \mathbb{Q} , of degree d . Let P_1, \dots, P_M be polynomials with coefficients in K such that they have a common non-trivial zero over K . How can we define search bounds in this context? Namely, we want to come up with a function

$$H : K^N \longrightarrow \mathbb{R}_+$$

that would measure “size” or, more accurately, “arithmetic complexity” of vectors so that for every $B \in \mathbb{R}_+$ the set

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

is finite. Functions like this are called **height functions**. We define an example of height.

There are infinitely many **absolute values** on K : those that extend the usual absolute value on \mathbb{Q} are called **archimedean** and those that extend p -adic ones on \mathbb{Q} are called **non-archimedean**.

We can define an equivalence relation on absolute values: $|\cdot|_1$ and $|\cdot|_2$ are said to be equivalent if there exists a real number θ such that

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

for all $a \in K$. Equivalence classes of absolute values are called **places**, and we write $M(K)$ for the set of all places of K . For each place $v \in M(K)$ we pick representatives $|\cdot|_v$ and we write $v|\infty$ if v is archimedean, and $v \nmid \infty$ otherwise. Here is an important property.

Artin-Whaples product formula: *For each $a \in K, a \neq 0,$*

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

Equivalent absolute values define the same metric topology, and so we can talk about **completion** of K with respect to the metric defined by v , call this completion K_v . We can define local norms on each K_v^N by

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

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

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

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. Also notice that because of the product formula, H is well defined on the projective space $\mathbb{P}^{N-1}(K)$. 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*

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

is finite for every positive real number B .

Hence we have successfully generalized the discussion of search bounds to systems of polynomials over a number field.

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. Indeed, if $\mathbf{y}_1, \dots, \mathbf{y}_J$ is another basis for V , then there exists $U \in GL_J(K)$ such that

$$Y = XU$$

where $Y = (\mathbf{y}_1 \dots \mathbf{y}_J)$ and $X = (\mathbf{x}_1 \dots \mathbf{x}_J)$ are $N \times J$ basis matrices. Hence

$$\mathbf{y}_1 \wedge \dots \wedge \mathbf{y}_J = (\det U) \mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_J.$$

Therefore

$$\begin{aligned}
 H(\mathbf{y}_1 \wedge \dots \wedge \mathbf{y}_J) &= H(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_J) \times \\
 &\times \prod_{v \in M(K)} |\det U|_v \\
 &= H(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_J).
 \end{aligned}$$

by the product formula. Hence we have defined a height on points of a Grassmanian over K . It satisfies the following important property.

Brill-Gordan duality: *If V as above is the nullspace of an $(N - J) \times N$ matrix A with row vectors $\mathbf{a}_1, \dots, \mathbf{a}_{N-J}$, then*

$$H(V) = H(\mathbf{a}_1 \wedge \dots \wedge \mathbf{a}_{N-J}).$$

Finally, define height on elements of $GL_N(K)$ by viewing them as vectors in K^{N^2} . We are now ready to talk about known results on search bounds for systems of polynomial equations over K .

Siegel's lemma

The first case, which is well understood by now, is the existence of search bounds for a system of linear forms. Results on this subject are usually referred to by the common name of Siegel's lemma. Here is a version of it over K .

Theorem 1 (Bombieri - Vaaler, 1983). *Let A be an $M \times N$ matrix of rank $M < N$ with coefficients in K . Let V be the nullspace of A . Then the linear system*

$$A\mathbf{x} = \mathbf{0}$$

has a non-trivial solution $\mathbf{x} \in V$ such that

$$H(\mathbf{x}) \leq C_1 H(V)^{\frac{1}{N-M}}$$

where the constant C_1 is explicit and depends on K and N .

There has been a large amount of further work done in this direction since 1983, for instance by Aliev, Chaladus, Fukshansky, O’Leary, Roy, Schinzel, Thunder, Vaaler, just to name a few.

Among these, I would like to mention the following two. First a result analogous to Theorem 1, producing a search bound for solutions of an inhomogeneous linear system over K , by O’Leary and Vaaler. Second, a so-called “absolute” version of Siegel’s lemma, i.e. a version of Theorem 1 over $\overline{\mathbb{Q}}$, by Roy and Thunder; namely, they prove that there exists a solution over $\overline{\mathbb{Q}}$ to a homogeneous linear system whose height is bounded above by an expression not depending on a number field. This, however, is not an actual search bound, since Northcott’s theorem only applies to sets of points of bounded height AND degree over \mathbb{Q} .

Quadratic forms

The only other case that is known is that of one quadratic polynomial. 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 with coefficients in K . We write

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

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

Theorem 2. *Suppose that F is isotropic over K . Then there exists a non-zero point $\mathbf{x} \in K^N$ such that $F(\mathbf{x}) = 0$, and*

$$H(\mathbf{x}) \leq C_2 H(F)^{\frac{N-1}{2}}$$

where C_2 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.

A large amount of further work in this direction has also been done by Birch, Chalk, Davenport, Fukshansky, Knesser, Masser, Schlickewei, Schmidt, and Vaaler, among others.

Masser in 1998 proved an analogue of Theorem 2 for an inhomogeneous quadratic polynomial over \mathbb{Q} . I have extended Masser's result to number fields and generalized it by considering an additional set of arithmetic conditions on point in question.

Nothing is known about search bounds for polynomials of higher degree, or for a system of quadratic polynomials. Quadratic spaces have a very rich and symmetrical structure that seems to be lacking in higher degree. We next demonstrate some further results on the effective structure of quadratic spaces.

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 3 (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*

$$H(W) \leq C_3 H(F)^{\frac{L-M}{2}} H(Z)$$

where C_3 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 $F(\mathbf{x}) \neq 0$ for all $\mathbf{0} \neq \mathbf{x} \in U$. A subspace V of (Z, F) is called **regular** if for each $\mathbf{0} \neq \mathbf{x} \in U$ there exists $\mathbf{y} \in U$ so that $F(\mathbf{x}, \mathbf{y}) \neq 0$. For each subspace U of (Z, F) we define

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

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

The subspace

$$\mathbb{H}(\mathbf{x}, \mathbf{y}) = \text{span}_K \{\mathbf{x}, \mathbf{y}\}$$

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

Theorem 4 (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*

$$H(Z^\perp) \leq C_4 H(F)^{\frac{r}{2}} H(Z)$$

and

$$\begin{aligned} & \max\{H(\mathbb{H}_i), H(V)\} \\ & \leq C_5 \left\{ H(F)^{\frac{L+2M}{4}} H(Z) \right\}^{\frac{(M+1)(M+2)}{2}}, \end{aligned}$$

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

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

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

for all $\mathbf{x}, \mathbf{y} \in Z$. 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.

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 $\tau_1, \dots, \tau_l \in \mathcal{O}(Z, F)$ such that*

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

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

$$H(\tau_i) \leq C_6 \left\{ H(F)^{\frac{L}{3}} H(Z)^{\frac{L}{2}} H(\sigma) \right\}^{5^{L-1}},$$

where C_6 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 existence of a reflection of relatively small height.

What is next?

This last corollary is related to a much more general recent conjecture of Masser on small-height integral equivalences of isometric bilinear spaces.

Namely, if bilinear spaces (K^N, F) and (K^N, G) are isometric, then there should exist an isometry σ between them with coefficients in the ring of algebraic integers of K so that $H(\sigma)$ is effectively bounded by a polynomial expression in $H(F) + H(G)$.

This conjecture currently seems to be far out of reach. I believe that a first step in this direction should be an investigation of the effective structure of bilinear lattices and their isometry groups, analogous to the above results on bilinear spaces.

Bounds over $\overline{\mathbb{Q}}$

What about explicit search bounds for polynomials of higher degree, or even a system of quadratics? It does not look hopeful. If we look for solutions over \mathbb{Z} , Matijasevich's result implies that in general the question of whether a given polynomial system has non-trivial integral solutions is undecidable. Analogous questions over \mathbb{Q} , or rings of integers of number fields are open problems.

A question like this about a polynomial system can always be reduced to a system of quadratics. Hence even for a system of quadratics it does not look good.

However, if one was to relax the condition that a non-trivial solution for a polynomial system P_1, \dots, P_M with coefficients in K has to lie over K , and look over $\overline{\mathbb{Q}}$ instead, the question becomes easily tractable.

It is an immediate consequence of Arithmetic Bezout's Theorem of Bost, Gillet, and Soulé (also Laurent and Roy) that if P_1, \dots, P_M are homogeneous polynomials in $N > M + 1$ variables of respective degrees J_1, \dots, J_M with coefficients in K , then there exists non-zero $\mathbf{x} \in \overline{\mathbb{Q}}^N$ with

$$\deg_K(\mathbf{x}) \leq J_1 \dots J_M$$

such that

$$P_1(\mathbf{x}) = \dots = P_M(\mathbf{x}) = 0$$

and

$$H(\mathbf{x}) \leq C_7 \prod_{i=1}^M H(P_i)^{\frac{1}{J_i}}$$

where the constant C_7 is explicit.

This is still a search bound, since degree of \mathbf{x} is bounded.

In case of just one polynomial more can be said.

Theorem 6 (F., 2003). *Let P be a homogeneous polynomial in $N \geq 2$ variables of degree $J \geq 1$ over K , and let $A \in GL_N(K)$. Then either there exists a non-zero point $\mathbf{y} \in K^N$ such that $P(\mathbf{y}) = 0$ and*

$$H(\mathbf{y}) \leq H(A^{-1})$$

or there exists $\mathbf{x} \in \overline{\mathbb{Q}}^N$ with $\deg_K(\mathbf{x}) \leq J$ such that $P(\mathbf{x}) = 0$, $A\mathbf{x} \in (\overline{\mathbb{Q}}^\times)^N$, and

$$H(\mathbf{x}) \leq C_8 H(A^{-1})^2 H(P)^{\frac{1}{J}}$$

where the constant C_8 is explicit and depends on N and J only.

This means that placing additional arithmetic conditions on the zero in question does not change the exponent in the upper bound, so perhaps this exponent is not best possible.

I believe that it should be possible to prove that if P is a homogeneous polynomial in $N > 2$ variables of degree $J \geq 1$ with coefficients in K , then there exists a non-zero $\mathbf{x} \in \overline{\mathbb{Q}}^N$ such that $P(\mathbf{x}) = 0$ and

$$H(\mathbf{x}) \leq C_9 H(P)^{\frac{1}{J(N-1)}}$$

for an explicit constant C_9 .

A bound as above may come at the expense of $\deg_K(\mathbf{x})$ not being bounded, so it may not be an explicit search bound any longer. Such a result for diagonal forms follows as an immediate consequence of the absolute Siegel's lemma of Roy and Thunder. I hope that further progress can be made on this question in the near future.