Some effective Diophantine results over $\overline{\mathbb{Q}}$

Lenny Fukshansky

Texas A&M University, USA

July 2005

Introduction

Let $F(X_1, ..., X_N) \in K[X_1, ..., X_N]$ be a homogeneous polynomial of degree $M \geq 1$ in $N \geq 2$ variables with coefficients in a number field K with $[K : \mathbb{Q}] = d$.

Question 1: *Does F have a non-trivial zero over K?*

Question 2: *Assuming it does, how do we find such a zero?*

Both questions are very difficult. The famous result of Matijasevich implies that (at least in case $K = \mathbb{Q}$) Question 1 is undecidable.

One can consider both questions simultaneously. Following D. W. Masser, we introduce **search bounds**. We start by defining height functions.

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}.

Notice that because of the normalizing exponent $1/d$ our height is absolute (i.e. defined over $\overline{\mathbb{Q}}$) in the sense that it does not depend on the field of definition; hence K can be any number field which contains coordinates of a vector whose height we want to compute.

Search bounds

For each vector $\boldsymbol{x} = (x_1, ..., x_N) \in \overline{\mathbb{Q}}^N$, let

$$\deg_K(\boldsymbol{x}) = [K(x_1, ..., x_N) : K].$$

A fundamental property of height is the following.

Northcott's theorem: *Let $C, D \in \mathbb{R}_+$. The set*

$$S(C, D) = \{\boldsymbol{x} \in \overline{\mathbb{Q}}^N : H(\boldsymbol{x}) \leq C,\ \deg_{\mathbb{Q}}(\boldsymbol{x}) \leq D\}$$

is finite for all C, D.

Now suppose that our polynomial F has a non-trivial zero over K. If we can prove that F has such a zero of bounded height over K with an explicit bound, call it $C_K(F)$, we reduce the search for a non-trivial zero to a finite set. Hence we answer both questions 1 and 2 simultaneously. We will call $C_K(F)$ a **search bound** for F over K.

Problem 1. *Given a polynomial F as above, find a search bound for it over K.*

For a general N, search bounds have only been found in the following cases:

1. F is a linear form (Siegel's Lemma: Bombieri-Vaaler 1983)

2. F is an inhomogeneous linear polynomial (Vaaler-O'Leary 1993, etc.)

3. F is a quadratic form (Cassels 1955, Raghavan 1975, etc.)

4. F is an inhomogeneous quadratic polynomial (Masser 1998, F. 2004)

In general, search bounds over a fixed number field probably do not exist. However, we can relax the requirement that zero of F has to lie over K.

Problem 2. *Given a polynomial F as above, find a pair $(C, D) = (C(F), D(F))$ independent of K such that there exists a non-trivial zero $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$ of F with $\deg_K(\boldsymbol{x}) \leq D$ and $H(\boldsymbol{x}) \leq C$.*

By Northcott's theorem, this would still be an effective search bound for F.

Basic bounds

The following is an easy observation.

Proposition 1. *Let $N \geq 2$, and let*

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

be a homogeneous polynomial of degree $M \geq 1$. There exists $\mathbf{0} \neq \boldsymbol{x} \in \overline{\mathbb{Q}}^N$ such that $F(\boldsymbol{x}) = 0$, $\deg_K(\boldsymbol{x}) \leq M$*, and*

$$H(\boldsymbol{x}) \leq \sqrt{2}\ H(F)^{1/M}.$$

Proof. Let

$$G(X_1, X_2) = F(X_1, X_2, 0, ..., 0).$$

If G is identically 0, take $\boldsymbol{x} = (1, 0, ..., 0)$. If not, then either $G(1, 0) = 0$, $G(0, 1) = 0$, or $g(X_1) = G(X_1, 1)$ is a polynomial of degree M, all of whose roots are not equal to 0. Then

$$H(F) \geq H(g) \geq \mu(g) \geq \prod_{i=1}^{M} \left(\frac{H(1, \alpha_i)}{\sqrt{2}} \right),$$

where $\mu(g)$ is the global absolute Mahler's measure of g, and $\alpha_1, ..., \alpha_M$ are roots of g. $\square$

Notice that Proposition 1 produces a small-height zero of F which is *degenerate* in the sense that it really is a zero of a binary form to which F is trivially reduced. Do there necessarily exist *non-degenerate* zeros of F? Here is another simple observation.

Proposition 2. *Let F be as above. If F is not a monomial, then there exists $\boldsymbol{x} \in \left(\overline{\mathbb{Q}}^{\times}\right)^N$ such that $F(\boldsymbol{x}) = 0$ with $\deg_K(\boldsymbol{x}) \leq M$, and*

$$H(\boldsymbol{x}) \leq M^M \sqrt{N-1}\ H(F).$$

Under slightly stronger assumptions we can produce a considerably better search bound for non-degenerate zeros of F.

Main results

Our first result looks as follows.

Theorem 3. *Let* $F(X_1, ..., X_N)$ *be a homogeneous polynomial in* $N \geq 2$ *variables of degree* $M \geq 1$ *over a number field* K*. Suppose that* F *does not vanish at any of the standard basis vectors* $\boldsymbol{e}_1, ..., \boldsymbol{e}_N$*. Then there exists* $\boldsymbol{x} \in \left(\overline{\mathbb{Q}}^{\times}\right)^N$ *with* $\deg_K(\boldsymbol{x}) \leq M$ *such that* $F(\boldsymbol{x}) = 0$*, and*

$$H(\boldsymbol{x}) \leq C_1(N, M)\ H(F)^{1/M},$$

with an explicit constant $C_1(N, M)$*.*

As a corollary of Theorem 3, we also produce the following search bound for zeros of *inhomogeneous* polynomials.

Corollary 4. *Let* $F(X_1, ..., X_N) \in K[X_1, ..., X_N]$ *be an inhomogeneous polynomial of degree* $M \geq 1$, $N \geq 2$. *Suppose that* F *does not vanish at any of the standard basis vectors* $\boldsymbol{e}_1, ..., \boldsymbol{e}_N$. *Then there exists* $\boldsymbol{x} \in \left(\overline{\mathbb{Q}}^{\times}\right)^N$ *with* $\deg_K(\boldsymbol{x}) \leq M$ *such that* $F(\boldsymbol{x}) = 0$, *and*

$$H(\boldsymbol{x}) \leq C_1(N+1, M)\ H(F)^{1/M},$$

where the constant $C_1(N+1, M)$ *is that of Theorem 3.*

We can also prove the following generalization of Theorem 3.

Theorem 5. *Let $F(X_1, ..., X_N)$ be a homogeneous polynomial in $N \geq 2$ variables of degree $M \geq 1$ over a number field K, and let $A \in GL_N(K)$. Then either there exists $\mathbf{0} \neq \boldsymbol{x} \in K^N$ such that $F(\boldsymbol{x}) = 0$ and*

$$H(\boldsymbol{x}) \leq H(A), \tag{3}$$

or there exists $\boldsymbol{x} \in A\left(\overline{\mathbb{Q}}^{\times}\right)^N$ with $\deg_K(\boldsymbol{x}) \leq M$ such that $F(\boldsymbol{x}) = 0$, and

$$H(\boldsymbol{x}) \leq C_2(N, M) H(A)^2 H(F)^{1/M},$$

with an explicit constant $C_2(N, M)$.

In other words, Theorem 5 asserts that for each element A of $GL_N(K)$ either there exists a zero of F over K whose height is bounded by $H(A)$, or there exists a small-height zero of F over $\overline{\mathbb{Q}}$ which lies outside of the union of nullspaces of row vectors of A^{-1}.

Conjecture

If F is a homogeneous polynomial in $N > 2$ variables of degree $M \geq 1$ with coefficients in K, then we conjecture that there exists $\boldsymbol{0} \neq \boldsymbol{x} \in \overline{\mathbb{Q}}^N$ such that $F(\boldsymbol{x}) = 0$ and

$$H(\boldsymbol{x}) \leq C_3(N,M) H(F)^{\frac{1}{M\beta(N)}},$$

for an explicit constant $C_3(N,M)$ and an appropriate function $\beta(N)$.

A bound as above may come at the expense of $\deg_K(\boldsymbol{x})$ not being bounded any longer, so it may not be an explicit search bound in the above sense. In fact, if

$$F = f_1 X_1^M + \cdots + f_N X_N^M$$

is a diagonal form, then such a bound with

$$\beta(N) = N-1, \quad C_3(N,M) = 3^{\frac{N-2}{2M}}$$

follows as an easy corollary of the absolute Siegel's lemma of Roy and Thunder.