Integral Points of Small Height outside of a Hypersurface

Lenny Fukshansky

University of Texas at Austin

We study "non-solutions" of polynomial equations. Let

$$F(\boldsymbol{X}) = F(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$$

be a homogeneous polynomial in $N \geq 2$ variables of degree $M \geq 1$ with integer coefficients. If F is not identically zero, there must exist a point with integer coordinates at which F does not vanish, in other words an integral point that lies outside of the hypersurface defined by F over $\mathbb{Q}$. How does one find such a point? Here is a strategy.

For a point $\boldsymbol{x} = (x_1, ..., x_N) \in \mathbb{Z}^N$, define its *height* and *length* respectively by

$$H(\boldsymbol{x}) = \max_{1 \leq i \leq N} |x_i|, \quad \boldsymbol{\mathcal{L}}(\boldsymbol{x}) = \sum_{i=1}^{N} |x_i|.$$

It is easy to see that a set of points with height or length bounded by some fixed constant is finite. In fact, for a positive real number R,

$$\left|\{\boldsymbol{x} \in \mathbb{Z}^N : H(\boldsymbol{x}) \leq R\}\right| = (2[R]+1)^N,$$

and

$$\left|\{\boldsymbol{x} \in \mathbb{Z}^N : \boldsymbol{\mathcal{L}}(\boldsymbol{x}) \leq R\}\right| = \sum_{k=0}^{\min([R],N)} 2^k \binom{N}{k} \binom{[R]}{k},$$

where $[R]$ is the integer part of R. Therefore if we were able to prove the existence of a point $\boldsymbol{x} \in \mathbb{Z}^N$ with $H(\boldsymbol{x}) \leq R$ or $\boldsymbol{\mathcal{L}}(\boldsymbol{x}) \leq R$ for some explicitly determined value of R, then the problem of finding this point would reduce to a finite search.

Thus we will consider the following problem.

Problem 1. *Given a homogeneous polynomial $F(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$ in $N \geq 2$ variables of degree $M \geq 1$, prove the existence of a point $\boldsymbol{x} \in \mathbb{Z}^N$ of small height (length) such that $F(\boldsymbol{x}) \neq 0$ with an explicit upper bound on the height (length).*

The following basic bound is not difficult to prove.

Lemma 1. *Let F be as above. There exists $\boldsymbol{x} \in \mathbb{Z}^N$ with $\boldsymbol{x}_i \neq 0$ for all $1 \leq i \leq N$, $F(\boldsymbol{x}) \neq 0$, and*

$$H(\boldsymbol{x}) \leq \frac{M+1}{2}, \tag{1}$$

and there exists $\boldsymbol{x} \in \mathbb{Z}^N$ such that $F(\boldsymbol{x}) \neq 0$, and

$$\mathcal{L}(\boldsymbol{x}) \leq \left[\frac{(M+2)}{2} \; \min\left\{ N, \frac{M+2}{4} \right\} \right]. \tag{2}$$

The bound of Lemma 1 depends only on N and M, not on the "nature" of polynomial F. We can do better in a special case that we consider next. It is closely related to an important trend in Diophantine approximations. Suppose that $F(\boldsymbol{X})$ is decomposable into a product of integral linear forms, i.e. suppose that

$$F(X_1, ..., X_N) = \prod_{i=1}^{M} L_i(X_1, ..., X_M),$$

where $L_i(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$ is a linear form for each $1 \leq i \leq M$. Write

$$\Lambda_i = \{\boldsymbol{y} \in \mathbb{Z}^N : L_i(\boldsymbol{y}) = 0\},$$

for each $1 \leq i \leq M$. Then each such Λ_i is a lattice of rank $N-1$ in $\mathbb{R}^N$, and the statement that $F(\boldsymbol{x}) \neq 0$ for some $\boldsymbol{x} \in \mathbb{Z}^N$ is equivalent to the statement that $\boldsymbol{x} \in \mathbb{Z}^N \setminus \bigcup_{i=1}^{M} \Lambda_i$.

In this case Problem 1 can be restated as follows.

Problem 2. *Let* $\Lambda_1, ..., \Lambda_M$ *be sublattices of* $\mathbb{Z}^N$ *of rank* $N-1$*. Prove the existence of a point* $\boldsymbol{x} \in \mathbb{Z}^N \setminus \bigcup_{i=1}^M \Lambda_i$ *of small height with an explicit bound on height.*

More generally, suppose that $\Omega \subseteq \mathbb{Z}^N$ is a lattice of rank J, $2 \leq J \leq N$, and let $\Lambda_1, ..., \Lambda_M$ be proper sublattices of Ω of respective ranks $l_1, ..., l_M$, $1 \leq l_i \leq J-1$ for each $1 \leq i \leq M$. We can state the following generalization of Problem 2.

Problem 3. *Prove the existence of a point* $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^M \Lambda_i$ *of small height with an explicit bound on height.*

Notice that this can be viewed as a certain extension of a classical Siegel's Lemma, which guarantees the existence of a non-zero point of small height in Ω. Then Problem 3 is a version of Siegel's Lemma with additional linear conditions, and Problem 2 can be thought of as a problem inverse to Siegel's Lemma.

Our main result is a bound for Problem 3 which depends on the "nature" of lattices Ω and $\Lambda_1, ..., \Lambda_M$, namely on their *heights*. Before we can proceed, we need to extend the height function to lattices.

Let $\Lambda \subseteq \mathbb{Z}^N$ be a lattice of rank J, $1 \leq J \leq N$. Let $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$ be a basis for Λ. Let

$$G = G(\boldsymbol{x}_1, ..., \boldsymbol{x}_J) = \boldsymbol{x}_1 \wedge ... \wedge \boldsymbol{x}_J \in \mathbb{Z}^{\binom{N}{J}},$$

where $\wedge$ stands for the wedge product on vectors.

Define

$$H(\Lambda) = H(G) = \max_{1 \le i \le \binom{N}{J}} |G_i|.$$

This definition is legitimate, since it does not depend on the choice of the basis. We are now ready to state the main result, which is a solution of Problem 3.

Theorem 2 (F.). *Let* $\Omega \subseteq \mathbb{Z}^N$ *be a sublattice of rank* J*,* $1 \le J \le N$*. Let* $\Lambda_1, ..., \Lambda_M$ *be proper non-zero sublattices of* Ω*. Then there exists* $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^M \Lambda_i$ *such that*

$$H(\boldsymbol{x}) \le \left(\frac{3}{2}\right)^{J-1} J^J \left\{ \sum_{i=1}^M \frac{1}{H(\Lambda_i)} + \sqrt{M} \right\} H(\Omega).$$

There are some interesting consequences of this theorem.

First of all, as a corollary of the method we can produce the following simple version of Siegel's Lemma.

Corollary 3. *Let $\Omega \subseteq \mathbb{Z}^N$ be a sublattice of rank J, $1 \leq J \leq N$. There exists a non-zero point $\boldsymbol{x} \in \Omega$ such that*

$$H(\boldsymbol{x}) \leq \left(\frac{J}{2^{\frac{J-1}{J}}} \right) H(\Omega)^{1/J}.$$

The exponent in the bound is best possible, and the method of proof is classical. We write down a lower bound for a function that counts the number of points of Ω in a homogeneously expanding cube centered at the origin in $\mathbb{R}^N$. If this function is at least two, there must be a non-zero point in the section of the cube by Ω, and so we are done.

Another interesting corollary is a solution of Problem 2: we produce a point of small height *outside* of a union of sublattices of $\mathbb{Z}^N$.

Corollary 4. *Let* $L_1(\boldsymbol{X}), ..., L_M(\boldsymbol{X})$ *be non-zero linear forms with relatively prime integer coordinates. Then there exists* $\boldsymbol{x} \in \mathbb{Z}^N$ *such that* $L_i(\boldsymbol{x}) \neq 0$ *for every* $i = 1, ..., M$ *and*

$$H(\boldsymbol{x}) \leq \sum_{i=1}^{M} \frac{1}{H(L_i)} + \sqrt{M}.$$

In other words, if for each $1 \leq i \leq M$, Λ_i is the "null-lattice" of L_i, then the point $\boldsymbol{x}$ of Corollary 4 is in $\mathbb{Z}^N \setminus \bigcup_{i=1}^{M} \Lambda_i$. By a well known duality principle, $H(L_i) = H(\Lambda_i)$. Hence Theorem 2 can be thought of as a combination of Siegel's Lemma and its inverse problem.

In fact, in case $M = 1$ we can deduce a formulation of Faltings' version of Siegel's Lemma in our setting from Theorem 2.

Corollary 5. *Let* V *and* W *be real vector spaces of respective dimensions* d_1 *and* d_2*. Let* $\Omega_1 = V \cap \mathbb{Z}^{d_1}$ *and* $\Omega_2 = W \cap \mathbb{Z}^{d_2}$*. Let* $\rho : V \longrightarrow W$ *be a linear map such that* $\rho(\Omega_1) \subseteq \Omega_2$*. Let* $U = \ker(\rho)$*, and let* $\Omega = U \cap \Omega_1$*. Let* J *be the rank of* Ω*. Then for any proper subspace* U_0 *of* U *there exists a point* $\boldsymbol{x} \in \Omega \setminus U_0$ *such that*

$$H(\boldsymbol{x}) \leq 2J^J \left(\frac{3}{2}\right)^{J-1} H(\Omega).$$

Faltings' lemma is more general (works for any lattices and any norms - our height is the sup-norm), but produces a worse upper bound.