SEARCH BOUNDS FOR ZEROS OF POLYNOMIALS OVER THE ALGEBRAIC CLOSURE OF $\mathbb{Q}$

LENNY FUKSHANSKY

Abstract. We discuss existence of explicit search bounds for zeros of polynomials with coefficients in a number field. Our main result is a theorem about the existence of polynomial zeros of small height over the field of algebraic numbers outside of unions of subspaces. All bounds on the height are explicit.

1. Introduction

Let $F_1, ..., F_k$ be a collection of nonzero polynomials in N variables of respective degrees $M_1, ..., M_k$ with coefficients in a number field K of degree d over $\mathbb{Q}$. Consider a system of equations

$$F_1(X_1, ..., X_N) = ... = F_k(X_1, ..., X_N) = 0. \tag{1}$$

There are two fundamental questions one can ask about this system: does (1) have nonzero solutions over K, and, if yes, how do we find them? In [8], D. W. Masser poses these general questions for a system of equations with integer coefficients, and suggests an alternative approach to both of them simultaneously by introducing *search bounds* for solutions. We start by generalizing this approach over K.

We write $\overline{\mathbb{Q}}$ for the algebraic closure of $\mathbb{Q}$, and write $\mathbb{P}(\overline{\mathbb{Q}}^N)$ for the projective space over $\overline{\mathbb{Q}}^N$. If H is a height function defined over $\overline{\mathbb{Q}}$, then by Northcott's theorem [10] a set of the form

$$S_D(C) = \{\boldsymbol{x} \in \mathbb{P}(\overline{\mathbb{Q}}^N) : H(\boldsymbol{x}) \leq C,\ \deg(\boldsymbol{x}) \leq D\} \tag{2}$$

has finite cardinality for any $C, D \in \mathbb{R}$, where $\deg(\boldsymbol{x})$ is degree of the field extension generated by the coordinates of $\boldsymbol{x}$ over $\mathbb{Q}$. Suppose that we were able to prove that if (1) has a nonzero solution $\boldsymbol{x} \in K^N$, then it has such a solution with $H(\boldsymbol{x}) \leq C$ for some explicit C. This means that we can restrict the search for a solution to a subset of the finite set $S_d(C)$ as in (2). We will call a constant C like this a *search bound* for (1). If a search bound like this exists, it will clearly depend on heights of polynomials $F_1, ..., F_k$. As in [8], we can now replace the two questions above by the following problem.

Problem 1. *Find an explicit search bound for a nonzero solution of (1) over K.*

This problem has been solved for arbitrary N only in very few cases. First suppose that $k < N$, and $M_1 = ... = M_k = 1$. If $F_1, ..., F_k$ are homogeneous, a solution to Problem 1 is provided by Siegel's Lemma (see [2]). In the case when $F_1, ..., F_k$ are inhomogeneous linear polynomials, this problem has been solved in [11]. Another instance of (1) for which the general solution to Problem 1 is known

1991 *Mathematics Subject Classification.* Primary 11G50, 11E76; Secondary 11D72, 14G40.
Key words and phrases. polynomials, height, search bounds.

is that of one quadratic polynomial. If $k = 1$, $M_1 = 2$, and F_1 is a quadratic form in $N \geq 2$ variables with coefficients in K, a solution to Problem 1 is presented in [3] in case $K = \mathbb{Q}$, and generalized to an arbitrary number field in [13]. If F_1 is an inhomogeneous quadratic polynomial, a general solution to Problem 1 over $\mathbb{Q}$ can be found in [7], and its generalization to an arbitrary number field in [5]. For a review of further advances in this subject and a detailed bibliography, see [8].

A general solution to Problem 1 even for one polynomial of arbitrary degree in an arbitrary number of variables seems to be completely out of reach at the present time. In fact, if $K = \mathbb{Q}$ and $F_1, ..., F_k$ are homogeneous, a solution to Problem 1 would provide an algorithm to decide whether a system of homogeneous Diophantine equations has an integral solution, and so would imply a positive answer to Hilbert's 10th problem in this case. However, by the famous theorem of Matijasevich [9] Hilbert's 10th problem is undecidable. This means that in general search bounds do not exist over $\mathbb{Q}$; in fact, they are unlikely to exist over any fixed number field. Moreover, it is known they do not exist over $\mathbb{Q}$ even for a single quartic polynomial or for a system of quadratics (see [8] for details).

In this paper we deal with the case of a single polynomial. Let us relax the condition that a solution must lie over a fixed number field K, but instead search for a solution of bounded height and bounded degree over $\overline{\mathbb{Q}}$. In other words, given an equation of the form

$$F(X_1, ..., X_N) = 0,$$

we want to prove the existence of a nonzero solution $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$ such that $H(\boldsymbol{x}) \leq C$ and $\deg_K(\boldsymbol{x}) \leq D$ for explicit constants C and D, where $\deg_K(\boldsymbol{x})$ stands for the degree of the field extension over K generated by the coordinates of $\boldsymbol{x}$. This problem is easily tractable as we will show in section 3, and still provides an explicit search bound since the set $S_D(C)$ is finite. In fact, we can prove a stronger statement by requiring the point $\boldsymbol{x}$ in question to satisfy some additional arithmetic conditions. Write $\mathbb{G}_m^N$ for the multiplicative torus $(\overline{\mathbb{Q}}^{\times})^N$. Here is the main result of this paper.

Theorem 1.1. *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 $\boldsymbol{x} \in A\mathbb{G}_m^N$ with $\deg_K(\boldsymbol{x}) \leq M$ such that $F(\boldsymbol{x}) = 0$, and

$$H(\boldsymbol{x}) \leq C_1(N, M) H(A)^2 H(F)^{1/M}, \tag{4}$$

where

$$C_1(N, M) = 2^{N-1} \binom{M+2}{2}^{\frac{(4M+1)(N-2)}{2M}} \binom{M+N}{N}^{\frac{1}{2M}} \prod_{j=2}^{N} \binom{M+j-2}{j-2}^{\frac{1}{2M}}. \tag{5}$$

In other words, Theorem 1.1 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}; for instance, if $A = I_N$ this means that there exists a small-height zero of F with all coordinates non-zero.

Notice that our approach of searching for small-height polynomial zeros over $\overline{\mathbb{Q}}$ is analogous in spirit to the so called "absolute" results, like the absolute Siegel's

Lemma of Roy and Thunder, [14]. The difference however is that we also keep a bound on the degree of a solution over the base field K.

This paper is organized as follows. In section 2 we set the notation and introduce the height functions that we will use. In section 3 we talk about the basic search bounds for zeros of a given polynomial over $\overline{\mathbb{Q}}$. In section 4 we prove Theorem 1.1. Results of this paper also appear as a part of [4].

2. Notation and heights

We start with some notation. Let K be a number field of degree d over $\mathbb{Q}$, O_K its ring of integers, and $M(K)$ its set of places. For each place $v \in M(K)$ we write K_v for the completion of K at v and let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree of K at v, so that for each $u \in M(\mathbb{Q})$

$$\sum_{v \in M(K), v|u} d_v = d. \tag{6}$$

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

$$\prod_{v \in M(K)} |a|_v = 1. \tag{7}$$

For each $v \in M(K)$ define a local height H_v on K_v^N by

$$H_v(\boldsymbol{x}) = \begin{cases} \max_{1 \le i \le N} |x_i|_v & \text{if } v \nmid \infty \\ \left(\sum_{i=1}^N \|x_i\|_v^2 \right)^{d_v/2d} & \text{if } v|\infty \end{cases}$$

for each $\boldsymbol{x} \in K_v^N$. We define the following global height function on K^N:

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} H_v(\boldsymbol{x}), \tag{8}$$

for each $\boldsymbol{x} \in K^N$. Notice that due to the normalizing exponent $1/d$, our global height function is absolute, i.e. for points over $\overline{\mathbb{Q}}$ its value does not depend on the field of definition. This means that if $\boldsymbol{x} \in \overline{\mathbb{Q}}^N$ then $H(\boldsymbol{x})$ can be evaluated over any number field containing the coordinates of $\boldsymbol{x}$.

We also define a height function on algebraic numbers. Let $\alpha \in \overline{\mathbb{Q}}$, and let K be a number field containing α. Then define

$$h(\alpha) = \prod_{v \in M(K)} \max\{1, |\alpha|_v\}. \tag{9}$$

We define the height of a polynomial to be the height of the corresponding coefficient vector. We also define height on $GL_N(K)$ by viewing matrices as vectors in K^{N^2}. On the other hand, if $M < N$ are positive integers and A is an $M \times N$ matrix with row vectors $\boldsymbol{a}_1, ..., \boldsymbol{a}_M$, we let

$$H(A) = H(\boldsymbol{a}_1 \wedge ... \wedge \boldsymbol{a}_M), \tag{10}$$

and if V is the nullspace of A over K, we define $H(V) = H(A)$. This is well defined, since multiplication by an element of $GL_M(K)$ does not change the height.

In other words, for a subspace V of K^N its height is defined to be the height of the corresponding point on a Grassmannian.

We will need the following basic property of heights, which can be easily derived from Lemma 2 of [12] (see Lemma 4.1.1 of [4] for details).

Lemma 2.1. *Let $g(X) \in K[X]$ be a polynomial of degree M in one variable with coefficients in K. There exists $\alpha \in \overline{\mathbb{Q}}$ of degree at most M over K such that $g(\alpha) = 0$, and*

$$h(\alpha) \leq H(g)^{1/M}. \tag{11}$$

Throughout this paper, let M, N be positive integers, and define

$$\mathcal{M}(N,M) = \left\{ (i_1,...,i_N) \in \mathbb{Z}_+^N : \sum_{j=1}^N i_j = M \right\}, \tag{12}$$

where $\mathbb{Z}_+$ is the set of all non-negative integers. Then any homogeneous polynomial F in N variables of degree M with coefficients in K can be written as

$$F(X_1,...,X_N) = \sum_{\boldsymbol{i} \in \mathcal{M}(N,M)} f_{\boldsymbol{i}} X_1^{i_1} \dots X_N^{i_N} \in K[X_1,...,X_N].$$

For a point $\boldsymbol{z} = (z_1,...,z_N) \in \overline{\mathbb{Q}}^N$, we write $\deg_K(\boldsymbol{z})$ to mean the degree of the extension $K(z_1,...,z_N)$ over K, i.e. $\deg_K(\boldsymbol{z}) = [K(z_1,...,z_N) : K]$. We are now ready to proceed.

3. Basic bounds for one polynomial

We start by exhibiting a basic bound for zeros of polynomials over $\overline{\mathbb{Q}}$.

Proposition 3.1. *Let $M \geq 1$, $N \geq 2$, and $F(X_1,...,X_N)$ be a homogeneous polynomial in N variables of degree M with coefficients in a number field K. There exists $\boldsymbol{0} \neq \boldsymbol{z} \in \overline{\mathbb{Q}}^N$ with $\deg_K(\boldsymbol{z}) \leq M$ such that $F(\boldsymbol{z}) = 0$ and*

$$H(\boldsymbol{z}) \leq \sqrt{2}\ H(F)^{1/M}. \tag{13}$$

Proof. If F is identically zero, then we are done. So assume F is non-zero. Write $\boldsymbol{e}_1,...,\boldsymbol{e}_N$ for the standard basis vectors for $\overline{\mathbb{Q}}^N$ over $\overline{\mathbb{Q}}$. Assume that for some $1 \leq i \leq N$, $\deg_{X_i} F < M$, then it is easy to see that $F(\boldsymbol{e}_i) = 0$, and $H(\boldsymbol{e}_i) = 1$. If $N > 2$, let

$$F_1(X_1,X_2) = F(X_1,X_2,0,...,0),$$

and a point $\boldsymbol{x} = (x_1,x_2) \in \overline{\mathbb{Q}}^2$ is a zero of F_1 if and only if $(x_1,x_2,0,...,0)$ is a zero of F, and $H(x_1,x_2) = H(x_1,x_2,0,...,0)$. In particular, if $F_1(X_1,X_2) = 0$, then $F(\boldsymbol{e}_1) = 0$. Hence we can assume that $N = 2$, $F(X_1,X_2) \neq 0$, and $\deg_{X_1} F = \deg_{X_2} F = M$. Write

$$F(X_1,X_2) = \sum_{i=0}^M f_i X_1^i X_2^{M-i},$$

where $f_0, f_M \neq 0$. Let

$$g(X_1) = F(X_1,1) = \sum_{i=0}^M f_i X_1^i \in K[X_1],$$

be a polynomial in one variable of degree M with coefficients in K. Notice that since coefficients of g are those of F, we have $H(g) = H(F)$. By Lemma 2.1, there must exist $\alpha \in \overline{\mathbb{Q}}$ with $\deg_K(\alpha) \leq M$ such that $g(\alpha) = 0$, and

$$H(\alpha, 1) \leq \sqrt{2}\ h(\alpha) \leq \sqrt{2}\ H(g)^{1/M} = \sqrt{2}\ H(F)^{1/M}.$$

Taking $\boldsymbol{z} = (\alpha, 1)$, completes the proof. □

Notice that if $N = 2$, then the bound (13) is best possible with respect to the exponent. Take

$$F(X_1, X_2) = X_1^M - CX_2^M,$$

for some $0 \neq C \in K$. Then zeros of F are of the form $(\alpha C^{1/M}, \alpha)$ for $\alpha \in \overline{\mathbb{Q}}$, and it is easy to see that $H(\alpha C^{1/M}, \alpha) \geq \frac{1}{\sqrt{2}} H(F)^{1/M}$.

Corollary 3.2. *Let the notation be as in Proposition 3.1. Then there exist vectors* $\boldsymbol{x}_{ij} \in \overline{\mathbb{Q}}^N$ *with non-zero coordinates i-th and j-th coordinates,* $1 \leq i \neq j \leq N$, *and the rest of the coordinates equal to zero such that* $F(\boldsymbol{x}_{ij}) = 0$, $\deg_K(\boldsymbol{x}_{ij}) \leq M$, *and each* $\boldsymbol{x}_{ij}$ *satisfies (13). Notice that* $\overline{\mathbb{Q}}^N = \operatorname{span}_{\overline{\mathbb{Q}}}\{\boldsymbol{x}_{ij} : 1 \leq i \neq j \leq N\}$.

Proof. In the proof of Proposition 3.1 instead of setting all but X_1 and X_2 equal to zero, set all but X_i and X_j equal to zero. □

4. Proof of Theorem 1.1

Notice that Proposition 3.1 only proves the existence of 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? To answer this question, we consider the problem of Proposition 3.1 with additional arithmetic conditions. We wonder what can be said about zeros of a polynomial over $\overline{\mathbb{Q}}$ outside of a collection of subspaces? For instance, under which conditions does a polynomial F vanish at a point with nonzero coordinates? Here is a simple effective criterion.

Proposition 4.1. *Let* $N \geq 2$, *and let* $F(X_1, ..., X_N) \in K[X_1, ..., X_N]$ *have degree* $M \geq 1$. *If F is not a monomial, then there exists* $\boldsymbol{z} \in \overline{\mathbb{Q}}^N$ *with* $\deg_K(\boldsymbol{z}) \leq M$ *such that* $F(\boldsymbol{z}) = 0$, $z_i \neq 0$ *for all* $1 \leq i \leq N$, *and*

$$H(\boldsymbol{z}) \leq M^M \sqrt{N-1} H(F). \tag{14}$$

Proof. Since F is not a monomial, there must exist a variable which is present to different powers in at least two different monomials, we can assume without loss of generality that it is X_1. Then we can write

$$F(X_1, ..., X_N) = \sum_{i=0}^{M} F_i(X_2, ..., X_N) X_1^i,$$

where each F_i is a polynomial in $N-1$ variables of degree at most $M-i$. At least two of these polynomials are not identically zero, say F_j and F_k for some $0 \leq j < k \leq M$. Let

$$F_{jk}(X_2, ..., X_N) = F_j(X_2, ..., X_N) F_k(X_2, ..., X_N),$$

then F_{jk} has degree at most $2M-1$. By Lemma 2.2 of [6], there exists $\boldsymbol{a} \in \mathbb{Z}^{N-1}$ such that $a_i \neq 0$ for all $2 \leq i \leq N-1$, $F_{jk}(\boldsymbol{a}) \neq 0$, and

$$\max_{1 \leq i \leq N-1} |a_i| \leq M,$$

hence $H(\boldsymbol{a}) \leq M\sqrt{N-1}$. Then $g(X_1) = F(X_1, a_2, ..., a_N)$ is a polynomial in one variable of degree at most M with at least two nonzero monomials. If $v \in M(K)$, $v \nmid \infty$, then $H_v(g) \leq H_v(F)$. If $v|\infty$, then for each $0 \leq i \leq M$ we have $\|F_i(\boldsymbol{a})\|_v \leq M^{M-i} H_v(F_i)$, and so

$$H(g) \leq M^{M-1} H(F). \tag{15}$$

By factoring a power of X_1, if necessary, we can assume that g is a polynomial of degree at least one with coefficients in K such that $g(0) \neq 0$. Then, combining Lemma 2.1 with (15), we see that there exists $0 \neq \alpha \in \overline{\mathbb{Q}}$ such that $[K(\alpha):K] \leq M$, $g(\alpha) = 0$, and

$$h(\alpha) \leq H(g) \leq M^{M-1} H(F).$$

Let $\boldsymbol{z} = (\alpha, \boldsymbol{a})$, then $F(\boldsymbol{z}) = 0$, $\deg_K(\boldsymbol{z}) \leq M$, $z_i \neq 0$ for each $1 \leq i \leq N$, and

$$H(\boldsymbol{z}) \leq h(\alpha) H(\boldsymbol{a}) \leq M^M \sqrt{N-1} H(F).$$

□

Under stronger conditions we can find a zero of F of smaller height, all coordinates of which are non-zero.

Theorem 4.2. *Let $F(X_1, ..., X_N)$ be a homogeneous polynomial in $N \geq 2$ variables of degree $M \geq 1$ with coefficients in 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 $\boldsymbol{z} \in \overline{\mathbb{Q}}^N$ with $\deg_K(\boldsymbol{z}) \leq M$ such that $F(\boldsymbol{z}) = 0$, $z_i \neq 0$ for all $1 \leq i \leq N$, and*

$$H(\boldsymbol{z}) \leq C_2(N,M)\ H(F)^{1/M}, \tag{16}$$

where

$$C_2(N,M) = 2^{N-1} \binom{M+2}{2}^{\frac{(4M+1)(N-2)}{2M}} \prod_{j=2}^{N} \binom{M+j-2}{j-2}^{\frac{1}{2M}}. \tag{17}$$

Proof. We argue by induction on N. If $N = 2$, then the result follows from the argument in the proof of Proposition 3.1. Assume $N > 2$. Let β be a positive integer, and let

$$F'_{\pm\beta}(X_1, ..., X_{N-1}) = F(X_1, ..., X_{N-1}, \pm\beta X_{N-1}),$$

in other words set $X_N = \pm\beta X_{N-1}$, where the choice of $\pm\beta$ is to be specified later. Let $\boldsymbol{e}'_1, ..., \boldsymbol{e}'_{N-1}$ be the standard basis vectors for $\overline{\mathbb{Q}}^{N-1}$. Notice that if $F'_{\pm\beta}$ vanishes at $\boldsymbol{e}'_i$ for $1 \leq i \leq N-2$, then F vanishes at $\boldsymbol{e}_i$, which is a contradiction. In particular, $F'_{\pm\beta}$ cannot be a monomial and cannot be identically zero. Suppose that $F'_{\pm\beta}(\boldsymbol{e}'_{N-1}) = 0$. This means that $F'_{\pm\beta}(0, ..., 0, X_{N-1})$ is identically zero. Write $\boldsymbol{u}_i = (0, ..., 0, i, M-i) \in \mathbb{Z}^N$ for each $0 \leq i \leq M$. Let

$$G(X_{N-1}, X_N) = F(0, ..., 0, X_{N-1}, X_N) = \sum_{i=0}^{M} f_{\boldsymbol{u}_i} X_{N-1}^i X_N^{M-i},$$

then

$$F'_{\pm\beta}(0,...,0,X_{N-1}) = G(X_{N-1}, \pm\beta X_{N-1}) = \left(\sum_{i=0}^{M} f_{\boldsymbol{u}_i} (\pm\beta)^{M-i} \right) X_{N-1}^M = 0,$$

that is

$$\sum_{i=0}^{M} f_{\boldsymbol{u}_i} (\pm\beta)^{M-i} = 0. \tag{18}$$

Notice that $f_{\boldsymbol{u}_0} \neq 0$ and $f_{\boldsymbol{u}_M} \neq 0$, since otherwise $F(\boldsymbol{e}_N) = 0$ or $F(\boldsymbol{e}_{N-1}) = 0$. Therefore the left hand side of (18) is a non-zero polynomial of degree M in β, and 0 is not one of its roots, so it has M non-zero roots. Therefore for the appropriate choice of $\pm$ we can select $\beta \in \mathbb{Z}_+$ such that (18) is *not* true and

$$0 < \beta \leq \frac{M}{2} + 1 = \frac{M+2}{2}. \tag{19}$$

Then for this choice of $\pm\beta$, $F'_{\pm\beta}$ is a polynomial in $N-1$ variables of degree M which does not vanish at any of the standard basis vectors. From now on we will write F'_β instead of $F'_{\pm\beta}$ for this fixed choice of $\pm\beta$.

Next we want to estimate height of such F'_β. Let $\boldsymbol{l} \in \mathbb{Z}_+^{N-1}$ be such that $\sum_{i=1}^{N-1} l_i = M$. There exist $l_{N-1} + 1 \leq M + 1$ vectors $\boldsymbol{m}_j \in \mathbb{Z}_+^N$ such that $m_{ji} = l_i$ for each $1 \leq i \leq N-2$ and $m_{j(N-1)} + m_{jN} = l_{N-1}$, where $0 \leq j \leq l_{N-1}$. Therefore the monomial of F'_β which is indexed by $\boldsymbol{l}$ will have coefficient

$$\alpha_{\boldsymbol{l}} = \sum_{j=0}^{l_{N-1}} f_{\boldsymbol{m}_j} (\pm\beta)^{l_{N-1}-j}. \tag{20}$$

Then for each $v \nmid \infty$

$$|\alpha_{\boldsymbol{l}}|_v \leq H_v(F), \tag{21}$$

and for each $v | \infty$

$$\begin{aligned}
\|\alpha_{\boldsymbol{l}}\|_v^2 &\leq \sum_{i=0}^{l_{N-1}} \sum_{j=0}^{l_{N-1}} \beta^{2l_{N-1}-i-j} \|f_{\boldsymbol{m}_i}\|_v \|f_{\boldsymbol{m}_j}\|_v \\
&\leq \left(\frac{\beta^{2l_{N-1}}}{2} \right) \sum_{i=0}^{l_{N-1}} \sum_{j=0}^{l_{N-1}} (\|f_{\boldsymbol{m}_i}\|_v^2 + \|f_{\boldsymbol{m}_j}\|_v^2) \\
&\leq \left(\frac{\beta^{2l_{N-1}}(l_{N-1}+1)}{2} \right) \left(\sum_{i=0}^{l_{N-1}} \|f_{\boldsymbol{m}_i}\|_v^2 + \sum_{j=0}^{l_{N-1}} \|f_{\boldsymbol{m}_j}\|_v^2 \right) \\
&\leq \beta^{2M}(M+2) H_v(F)^2 \leq 2 \left(\frac{M+2}{2} \right)^{2M+1} H_v(F)^2,
\end{aligned} \tag{22}$$

where the last inequality follows by (19). Therefore, by (21) and (22), we have for each $v \nmid \infty$,

$$H_v(F'_\beta) \leq H_v(F), \tag{23}$$

and for each $v|\infty$,

$$\begin{aligned} H_v(F'_\beta) &= \left(\sum_{\boldsymbol{l} \in \mathcal{M}(N-1,M)} \|\alpha_{\boldsymbol{l}}\|_v^2 \right)^{1/2} \\ &\leq \sqrt{2}\ |\mathcal{M}(N-1,M)|^{1/2} \left(\frac{M+2}{2} \right)^{\frac{2M+1}{2}} H_v(F) \\ &\leq \sqrt{2} \binom{M+N-2}{N-2}^{1/2} \left(\frac{M+2}{2} \right)^{\frac{2M+1}{2}} H_v(F) \end{aligned} \tag{24}$$

Putting (23) and (24) together implies that

$$H(F'_\beta) \leq \sqrt{2} \binom{M+N-2}{N-2}^{1/2} \left(\frac{M+2}{2} \right)^{\frac{2M+1}{2}} H(F). \tag{25}$$

By induction hypothesis, there exists $\boldsymbol{x} \in \overline{\mathbb{Q}}^{N-1}$ with $\deg_K(\boldsymbol{x}) \leq M$ such that $F'_\beta(\boldsymbol{x}) = 0$, $x_i \neq 0$ for all $1 \leq i \leq N-1$, and

$$\begin{aligned} H(\boldsymbol{x}) &\leq C_2(N-1,M)\ H(F'_\beta)^{\frac{1}{M}} \\ &\leq C_2(N-1,M)\ 2^{\frac{1}{2M}} \binom{M+N-2}{N-2}^{\frac{1}{2M}} \left(\frac{M+2}{2} \right)^{\frac{2M+1}{2M}} H(F)^{\frac{1}{M}}. \end{aligned} \tag{26}$$

Let $E = K(x_1, ..., x_{N-1})$. Set $\boldsymbol{z} = (\boldsymbol{x}, \pm\beta x_{N-1}) \in E^N$, then $\deg_K(\boldsymbol{z}) = [E:K] \leq M$, $F(\boldsymbol{z}) = 0$, $z_i \neq 0$ for all $1 \leq i \leq N$, and applying (19) and (26) we have

$$\begin{aligned} H(\boldsymbol{z}) &\leq \prod_{v \nmid \infty} H_v(\boldsymbol{x}) \times \prod_{v | \infty} \left(\beta^2 \|x_{N-1}\|_v^2 + H_v(\boldsymbol{x})^2 \right)^{\frac{d'_v}{2d'}} \leq \sqrt{\beta^2+1}\ H(\boldsymbol{x}) \\ &\leq 2^{\frac{M+1}{2M}} \binom{M+N-2}{N-2}^{\frac{1}{2M}} \left(\frac{M+2}{2} \right)^{\frac{4M+1}{2M}} C_2(N-1,M)\ H(F)^{\frac{1}{M}}, \end{aligned} \tag{27}$$

where the product in (27) is taken over all places in $M(E)$, and d'_v, d' stand for local and global degrees of E over $\mathbb{Q}$ respectively. The result follows. □

Proof of Theorem 1.1. Let $K[\boldsymbol{X}]_M$ be the space of homogeneous polynomials of degree M in N variables over K. For an element $A \in GL_N(K)$ define a map $\rho_A : K[\boldsymbol{X}]_M \longrightarrow K[\boldsymbol{X}]_M$ (compare with [1]), given by $\rho_A(F)(\boldsymbol{X}) = F(A\boldsymbol{X})$ for each $F \in K[\boldsymbol{X}]_M$. It is easy to see that the map $A \longmapsto \rho_A$ is a representation of $GL_N(K)$ in $GL(K[\boldsymbol{X}]_M)$.

With notation as in the statement of the theorem, let $G(\boldsymbol{X}) = \rho_A(F)(\boldsymbol{X})$. First suppose that $G(\boldsymbol{e}_i) = F(A\boldsymbol{e}_i) = 0$ for some $1 \leq i \leq N$. Since $\boldsymbol{0} \neq \boldsymbol{y} = A\boldsymbol{e}_i \in K^N$ is a row of A, it is easy to see that

$$H(\boldsymbol{y}) \leq H(A),$$

which is (3). Next assume that $G(\boldsymbol{e}_i) \neq 0$ for each $1 \leq i \leq N$. By Theorem 4.2, there exists $\boldsymbol{z} \in \mathbb{G}_m^N$ such that $G(\boldsymbol{z}) = 0$, $\deg_K(\boldsymbol{z}) \leq M$, and

$$H(\boldsymbol{z}) \leq C_2(N,M)\ H(G)^{1/M}.$$

Then $\boldsymbol{x} = A\boldsymbol{z}$ is such that $F(\boldsymbol{x}) = 0$, $\deg_K(\boldsymbol{x}) \leq M$, and $\boldsymbol{x} = A\boldsymbol{z} \in A\mathbb{G}_m^N$. It is easy to see that

$$H(\boldsymbol{x}) \leq H(A)H(\boldsymbol{z}) \leq C_2(N,M)\ H(A)H(G)^{1/M}. \tag{28}$$

We now want to estimate $H(G)$. Let $v \in M(K)$. If $v \nmid \infty$, then

$$H_v(G) \leq H_v(A)^M H_v(F), \tag{29}$$

and if $v|\infty$, then

$$H_v(G) \leq \binom{N+M}{N}^{d_v/2d} H_v(A)^M H_v(F). \tag{30}$$

These bounds on local heights are well-known. Essentially identical estimates for a bihomogeneous polynomial in two pairs of variables follow from Lemmas 6, 7, and formula (2.2) of [1]. The proofs of (29) and (30) are similar to the proofs of Lemmas 6 and 7 of [1], so we do not include them here to maintain the brevity of exposition. Combining (29) and (30), we obtain

$$H(G) \leq \binom{N+M}{N}^{1/2} H(A)^M H(F). \tag{31}$$

The result follows by combining (28) and (31). □

Corollary 4.3. *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 $\boldsymbol{z} \in \overline{\mathbb{Q}}^N$ with $\deg_K(\boldsymbol{z}) \leq M$ such that $F(\boldsymbol{z}) = 0$, $z_i \neq 0$ for all $1 \leq i \leq N$, and*

$$H(\boldsymbol{z}) \leq C_2(N+1,M)\ H(F)^{1/M}, \tag{32}$$

where the constant $C_2(N+1,M)$ is defined by (17) of Theorem 4.2.

Proof. Homogenize F using the variable X_0 and denote the resulting homogeneous polynomial in $N+1$ variables by $F'(X_0,...,X_N)$. Then F' has degree M, its coefficients are in K, and

$$F(X_1,...,X_N) = F'(1,X_1,...,X_N),$$

hence $H(F') = H(F)$. There exists $\boldsymbol{x} = (x_0,...,x_N) \in \overline{\mathbb{Q}}^{N+1}$ so that $x_0 \neq 0$, and

$$F'(x_0,...,x_N) = F(x_1/x_0,...,x_N/x_0) = 0.$$

Notice that

$$H(x_1/x_0,...,x_N/x_0) = H(x_1,...,x_N) \leq H(x_0,...,x_N) = H(\boldsymbol{x}),$$

hence it is sufficient to prove that there exists a zero $\boldsymbol{z} \in \overline{\mathbb{Q}}^{N+1}$ of F' so that $z_0 \neq 0$ and $\boldsymbol{z}$ is of bounded height. Notice that since the variable X_0 was introduced to homogenize F, we have $\deg(F) = \deg(F') = M$, and so $X_0 \nmid F'(X_0,...,X_N)$.

Write $\boldsymbol{e}'_0,...,\boldsymbol{e}'_N$ for the standard basis vectors in $\overline{\mathbb{Q}}^{N+1}$. First suppose that $F'(\boldsymbol{e}'_i) \neq 0$ for all $0 \leq i \leq N$, then by Theorem 4.2 there exists $\boldsymbol{z} \in \overline{\mathbb{Q}}^{N+1}$ satisfying (32) with $\deg_K(\boldsymbol{z}) \leq M$ such that $z_i \neq 0$ for each $0 \leq i \leq N$, and $F'(\boldsymbol{z}) = 0$, hence we are done. Next suppose that $F'(\boldsymbol{e}'_0) = F(\boldsymbol{0}) = 0$. Then let

$$G(X_1,...,X_N) = F'(X_1,X_1,...,X_N),$$

that is set $X_0 = X_1$ in F'. Notice that for each $1 \leq i \leq N$, $G(\boldsymbol{e}_i) = F(\boldsymbol{e}_i) \neq 0$, and $H(G) = H(F') = H(F)$. Again, by Theorem 4.2 there exists $\boldsymbol{z} \in \overline{\mathbb{Q}}^N$ satisfying (32) with $\deg_K(\boldsymbol{z}) \leq M$ such that $z_i \neq 0$ for each $1 \leq i \leq N$, and $G(\boldsymbol{z}) = F'(z_1,\boldsymbol{z}) = 0$, and so we are done. Finally suppose that $F'(\boldsymbol{e}'_i) = 0$ for some $1 \leq i \leq N$. Since $X_0 \nmid F(X_0, ..., X_N)$, we can write

$$F'(X_0, \dots, X_N) = G_1(X_1, \dots, X_N) + X_0 G_2(X_0, \dots, X_N),$$

where G_1 and G_2 are both non-zero homogeneous polynomials of degrees M and $M-1$ respectively. Then $F'(\boldsymbol{e}'_i) = G_1(\boldsymbol{e}_i) = 0$, which means that the coefficient of the term X_i^M in G_1 is zero, and hence it is zero in F' and thus in F. This implies that $F(\boldsymbol{e}_i) = 0$ contradicting our original assumption. Hence $F'(\boldsymbol{e}'_i) \neq 0$ for every $1 \leq i \leq N$, and so we are done. □

In case $N = 2$, the exponent in the bound of Corollary 4.3 is best possible. Take

$$F(X_1, X_2) = X_1 - C X_2^M,$$

for some $0 \neq C \in K$. Then by the same argument as in the remark after the proof of Proposition 3.1 every non-trivial zero of F has height $\geq O(H(F)^{1/M})$.

Acknowledgment. I would like to thank Professors Paula Tretkoff and Jeff Vaaler for their helpful comments on the subject of this paper.

References

[1] E. Bombieri, A. J. Van Der Poorten, and J. D. Vaaler. Effective measures of irrationality for cubic extensions of number fields. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 23(2):211–248, 1996.

[2] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[3] J. W. S. Cassels. Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 51:262–264, 1955.

[4] L. Fukshansky. *Algebraic points of small height with additional arithmetic conditions*. PhD thesis, University of Texas at Austin, 2004.

[5] L. Fukshansky. Small zeros of quadratic forms with linear conditions. *J. Number Theory*, 108(1):29–43, 2004.

[6] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatsh. Math.*, 147(1):25–41, 2006.

[7] D. W. Masser. How to solve a quadratic equation in rationals. *Bull. London Math. Soc.*, 30(1):24–28, 1998.

[8] D. W. Masser. Search bounds for Diophantine equations. *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 247–259, 2002.

[9] Yu. V. Matijasevich. The diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[10] D. G. Northcott. An inequality in the theory of arithmetic on algebraic varieties. *Proc. Camb. Phil. Soc.*, 45:502–509 and 510–518, 1949.

[11] R. O'Leary and J. D. Vaaler. Small solutions to inhomogeneous linear equations over number fields. *Trans. Amer. Math. Soc.*, 336(2):915–931, 1993.

[12] C. G. Pinner and J. D. Vaaler. The number of irreducible factors of a polynomial. I. *Trans. Amer. Math. Soc.*, 339(2):809–834, 1993.

[13] S. Raghavan. Bounds of minimal solutions of diophantine equations. *Nachr. Akad. Wiss. Gottingen, Math. Phys. Kl.*, 9:109–114, 1975.

[14] D. Roy and J. L. Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.

Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, Texas 77843-3368

E-mail address: `lenny@math.tamu.edu`