

ON ZEROS OF MULTILINEAR POLYNOMIALS

MAXWELL FORST AND LENNY FUKSHANSKY

ABSTRACT. We consider multivariable polynomials over a fixed number field, linear in some of the variables. For a system of such polynomials satisfying certain technical conditions we prove the existence of search bounds for simultaneous zeros with respect to height. For a single such polynomial, we prove the existence of search bounds with respect to height for zeros lying outside of a prescribed algebraic set. We also obtain search bounds in the case of homogeneous multilinear polynomials, which are related to a so-called “sparse” version of Siegel’s lemma. Among the tools we develop are height inequalities that are of some independent interest.

1. INTRODUCTION AND STATEMENT OF RESULTS

Hilbert’s 10th problem asks for an algorithm to decide whether a given Diophantine equation has an integer solution. By a celebrated result of Matiyasevich [15], such an algorithm does not exist in general. On the other hand, for linear Diophantine equations solutions are classically given by the Euclidean algorithm. Further, there are also known algorithms for quadratic polynomials (see, for instance [11]). An important approach to the problem of finding such algorithms for different classes of polynomials is through the use of *search bounds*, as described in [14]. Suppose we can prove that a given equation has integer solutions if and only if it has a solution of norm bounded by some explicit function of the coefficients of this equation. Then a search through a finite set of all integer points with norm bounded by this function provides an algorithm that decides whether a solution exists and finds at least one such solution if it exists.

In fact, search bounds for zeros of polynomial equations have been studied quite extensively over more general rings and fields as well: in these more general situation the role of norm guaranteeing the finiteness of a searchable set is played by an appropriate *height function* (we recall the definitions and properties of related height functions H , \mathcal{H} and h in Section 2). Search bounds with respect to height over different fields and rings of arithmetic interest for a collection of linear forms are given by various forms of Siegel’s lemma: we recall it in Section 3 and prove a certain “sparse” version of it (Theorem 3.3). The subject of search bounds for quadratic polynomials has been started by a classical theorem of Cassels [6]; see [8] for a detailed overview of a large body of work on various extensions and generalizations of this important theorem. Additionally, there are search bounds for integral cubic forms in a sufficient number of variables [4], as well as for systems of integral forms under certain technical non-singularity conditions [13].

2020 *Mathematics Subject Classification*. Primary: 11G50, 11D99.

Key words and phrases. multilinear polynomial, Siegel’s lemma, height, search bound.

Fukshansky was partially supported by the Simons Foundation grant #519058.

The main goal of this paper is to investigate bounds on height of “small” solutions to polynomial equations, linear in some of the variables, over number fields. From here on, let K be a number field of degree d and discriminant Δ_K . Let $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ and let $1 \leq k < n$. Let $[n] = \{1, \dots, n\}$, $I = \{i_1, \dots, i_k\} \subset [n]$, and $I' = [n] \setminus I$. Let $\mathbf{x}_{I'} = (x_j)_{j \in I'}$. We will say that F is linear in I -separated variables if

$$(1) \quad F(x_1, \dots, x_n) = \sum_{j=1}^k x_{i_j} F_j(\mathbf{x}_{I'}) + F_{k+1}(\mathbf{x}_{I'}),$$

where $F_j(\mathbf{x}_{I'}) \in K[\mathbf{x}_{I'}]$ for $1 \leq j \leq k+1$ are any polynomials in $n-k$ variables indexed by I' with coefficients in K . For a polynomial $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, we define its zero-set over K

$$Z_K(F) = \{\mathbf{z} \in K^n : F(\mathbf{z}) = 0\}.$$

We also write $\mathcal{N}(F)$ for the number of nonzero monomials of F . With this notation, we can state our first main result.

Theorem 1.1. *Let I be as above and let*

$$F_l(x_1, \dots, x_n) = \sum_{j=1}^k x_{i_j} F_{l,j}(\mathbf{x}_{I'}) + F_{l,k+1}(\mathbf{x}_{I'}), \quad 1 \leq l \leq k$$

be polynomials over K of respective degrees m_1, \dots, m_k linear in I -separated variables as in (1). Consider the inhomogeneous system

$$(2) \quad \left. \begin{aligned} F_1(x_1, \dots, x_n) &= \sum_{j=1}^k x_{i_j} F_{1,j}(\mathbf{x}_{I'}) + F_{1,k+1}(\mathbf{x}_{I'}) &= 0 \\ &\vdots \\ F_k(x_1, \dots, x_n) &= \sum_{j=1}^k x_{i_j} F_{k,j}(\mathbf{x}_{I'}) + F_{k,k+1}(\mathbf{x}_{I'}) &= 0 \end{aligned} \right\}$$

of linear equations in the variables x_{i_1}, \dots, x_{i_k} with coefficients $F_{l,j}(\mathbf{x}_{I'})$, $1 \leq l \leq k$, $1 \leq j \leq k+1$. Assume that the matrix $\mathcal{F} := (F_{l,j}(\mathbf{x}_{I'}))_{1 \leq l \leq k, 1 \leq j \leq k}$ of the corresponding homogeneous system has the same rank as the coefficient matrix of inhomogeneous system, i.e., \mathcal{F} augmented by the column $(F_{l,k+1}(\mathbf{x}_{I'}))_{1 \leq l \leq k}$. Then $\bigcap_{l=1}^k Z_K(F_l) \neq \emptyset$ and there exists a point $\mathbf{z} \in \bigcap_{l=1}^k Z_K(F_l)$ with

$$h(\mathbf{z}) \leq k^{k+1} |\Delta_K|^{\frac{1}{d}} \left(\frac{D+2}{2} \right)^{2km+1} (\mathcal{N}\mathfrak{H})^{2k},$$

where

$$D = \sum_{l=1}^k m_l, \quad m = \max_{1 \leq l \leq k} m_l,$$

$$\mathcal{N} = \max_{1 \leq l \leq k} \mathcal{N}(F_l), \quad \mathfrak{H} = \max_{1 \leq l \leq k} h(F_l).$$

We prove this theorem in Section 4, where we also show how our method of proof leads to an explicit algorithm for finding a simultaneous zero of the polynomial system in question. Our main tools are the Bombieri–Vaaler Siegel’s lemma (Theorem 3.1), a non-vanishing lemma for polynomials related to Alon’s Combinatorial Nullstellensatz (Lemma 2.6) and a collection of height inequalities that we discuss in Section 2. One of these height inequalities that we prove, a bound on the height of the inverse of a nonsingular matrix (Lemma 2.3), is of some independent interest and may have other applications in Diophantine geometry.

In the case of a single polynomial, we can prove a similar result but with additional avoidance conditions.

Theorem 1.2. *Let $n \geq 2$ and $F(\mathbf{x})$ and $P(\mathbf{x})$ be polynomials in n variables over K of degrees g and m , respectively. Assume further that F is linear in at least one of the variables and $Z_K(F) \not\subseteq Z_K(P)$. Then there exists a point $\mathbf{z} \in Z_K(F) \setminus Z_K(P)$ such that*

$$(3) \quad h(\mathbf{z}) \leq \mathcal{N}(F) \left(\frac{m(2g-1)+2}{2} \right)^{g+1} h(F),$$

where $\mathcal{N}(F)$ is the number of monomials of F .

We prove this theorem in Section 5. Finally, we separately discuss the case of homogeneous multilinear polynomials. We refer to a homogeneous polynomial $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ of degree g but linear in every variable as an (n, g) -multilinear form over K . Such forms have many zeros; in particular, they vanish on all sufficiently sparse vectors, specifically on vectors with no more than $g-1$ nonzero coordinates. We use this observation to obtain the following search bounds which we prove in Section 6.

Theorem 1.3. *Let $V \subseteq K^n$ be an m -dimensional subspace and F a multilinear (n, g) -form over K . Assume that $m+g-1 > n$ and $g > 1$. Then V contains a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$ of vectors such that $F(\mathbf{x}_1) = \dots = F(\mathbf{x}_m) = 0$ and*

$$H(\mathbf{x}_i) \leq \sqrt{2m} |\Delta_K|^{\frac{m+1}{2d}} \mathcal{H}(V).$$

for each $1 \leq i \leq m$. Further, suppose that $P(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ is a polynomial such that the dimension of the subspace of V that $Z_K(P, V) := Z_K(P) \cap V$ spans is

$$D(P, V) := \dim \text{span}_K Z_K(P, V) < m.$$

Then there exists a point $\mathbf{z} \in V \setminus Z_K(P, V)$ such that $F(\mathbf{z}) = 0$ and

$$H(\mathbf{z}) \leq \sqrt{2m} |\Delta_K|^{\frac{m+1}{2d}} \mathcal{H}(V).$$

This theorem is a direct consequence of our ‘‘sparse’’ Siegel’s lemma (Theorem 3.3). For completeness purposes, we present the bounds analogous to Theorem 1.3 in the simple case of linear forms ($g = 1$) separately in Lemma 6.5. We are now ready to proceed.

2. NOTATION AND HEIGHTS

Let K be a number field of degree $d := [K : \mathbb{Q}] \geq 1$ and let r_1, r_2 be the numbers of real and conjugate pairs of complex embeddings, respectively, so that

$$d = r_1 + 2r_2.$$

Let Δ_K be the discriminant of K , and write $M(K)$ for the set of places of K . For each $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree, then for each $u \in M(\mathbb{Q})$, $\sum_{v|u} d_v = d$. We normalize the absolute values so that for each nonzero $x \in K$ the product formula reads

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

Let $n \geq 2$, and for any place $v \in M(K)$ and $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ define the corresponding sup-norm

$$|\mathbf{x}|_v = \max\{|x_1|_v, \dots, |x_n|_v\}.$$

If $v \mid \infty$, we also define Euclidean norm

$$\|\mathbf{x}\|_v = \left(\sum_{i=1}^n |x_i|_v^2 \right)^{1/2}.$$

Then we define two projective height functions $H, \mathcal{H} : K^n \rightarrow \mathbb{R}_{\geq 0}$ as follows:

$$H(\mathbf{x}) = \left(\prod_{v \in M(K)} |\mathbf{x}|_v^{d_v} \right)^{1/d}, \quad \mathcal{H}(\mathbf{x}) = \left(\prod_{v \nmid \infty} |\mathbf{x}|_v^{d_v} \times \prod_{v \mid \infty} \|\mathbf{x}\|_v^{d_v} \right)^{1/d}.$$

These heights are absolute, meaning that they are the same when computed over any number field K containing coordinates of \mathbf{x} : this is due to the normalizing exponent $1/d$ in the definition. Further, for each nonzero $\mathbf{x} \in K^n$,

$$(4) \quad 1 \leq H(\mathbf{x}) \leq \mathcal{H}(\mathbf{x}) \leq \sqrt{n}H(\mathbf{x}).$$

The inhomogeneous (Weil) height $h : K^n \rightarrow \mathbb{R}_{\geq 1}$ is defined by

$$h(\mathbf{x}) = H(1, \mathbf{x}) \geq H(\mathbf{x})$$

for every $n \geq 1$, thus including a height on algebraic numbers. We also write $H(A)$ and $h(A)$ for the projective and inhomogeneous heights, respectively, of an $m \times n$ matrix A viewed as a vector in K^{mn} and $H(F)$, $h(F)$ for the respective heights of the coefficient vector of a polynomial F over K .

We can also define Schmidt height on the subspaces of K^n as follows. Let $V = \text{span}_K\{\mathbf{x}_1, \dots, \mathbf{x}_m\}$ be an m -dimensional subspace of K^n , $1 \leq m \leq n$, with a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$. The wedge product of these basis vectors $\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_m$ can be viewed as a vector in $K^{\binom{n}{m}}$ under lexicographic embedding: this is a vector of Grassmann (or Plücker) coordinates of V , which is uniquely defined up to a constant multiple. Define

$$\mathcal{H}(V) = \mathcal{H}(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_m).$$

The product formula guarantees that this definition is independent of the choice of a basis for V . We also define Schmidt height on matrices: for an $n \times m$ matrix A over K , $1 \leq m \leq n$ we let

$$\mathcal{H}(A) = \mathcal{H}(\text{span}_K\{\mathbf{a}_1, \dots, \mathbf{a}_m\}),$$

where $\mathbf{a}_1, \dots, \mathbf{a}_m$ are column vectors of A . If $m > n$, we define $\mathcal{H}(A)$ to be $\mathcal{H}(A^\top)$. Suppose the m -dimensional vector subspace $V \subset K^n$ is described as

$$V = \{A\mathbf{x} : \mathbf{x} \in K^m\} = \{\mathbf{y} \in K^n : B\mathbf{y} = \mathbf{0}\}$$

for the $n \times m$ matrix A and $(n - m) \times n$ matrix B over K , respectively. Then the Brill–Gordan duality principle [10] (also see Theorem 1 on page 294 of [12]) states that

$$(5) \quad \mathcal{H}(A) = \mathcal{H}(B) = \mathcal{H}(V).$$

We also review here several properties of height functions that we will need. The first one is a well known fact, which is an immediate corollary of Theorem 1 of [19].

Lemma 2.1. *Let U_1 and U_2 be subspaces of K^n . Then*

$$\mathcal{H}(U_1 \cap U_2) \leq \mathcal{H}(U_1)\mathcal{H}(U_2).$$

The second one is Lemma 4.7 of [17].

Lemma 2.2. *Let V be an m -dimensional subspace of K^n , $1 \leq m \leq n$, and let $\mathbf{x}_1, \dots, \mathbf{x}_m$ be any basis for V . Then*

$$\mathcal{H}(V) \leq \mathcal{H}(\mathbf{x}_1) \cdots \mathcal{H}(\mathbf{x}_m).$$

The next lemma gives a bound on the height H of the inverse of a square nonsingular matrix (viewed as a vector) in terms of the height of the matrix itself.

Lemma 2.3. *Let $A \in \text{GL}_n(K)$, then*

$$(6) \quad H(A^{-1}) \leq (\sqrt{n}H(A))^{n-1},$$

and

$$(7) \quad h(A^{-1}) \leq n^n |\Delta_K|^{\frac{1}{2}} h(A)^{2n-1}.$$

Proof. Let us write $\mathbf{a}_1, \dots, \mathbf{a}_n$ for the row vectors of A , and for each $1 \leq j \leq n$ let A_j be the $(n-1) \times n$ submatrix of A obtained by deleting the j -th row \mathbf{a}_j . For each j ,

$$V_j = \{\mathbf{x} \in K^n : A_j \mathbf{x} = \mathbf{0}\}$$

is a 1-dimensional subspace. Let \mathbf{x}_j be any nonzero point in V_j and notice that $\mathbf{a}_j \mathbf{x}_j \neq 0$: if it was equal to 0, then $A \mathbf{x}_j = \mathbf{0}$, contradicting the assumption that A is nonsingular. Then take $\mathbf{b}_j = \frac{1}{\mathbf{a}_j \mathbf{x}_j} \mathbf{x}_j$, then $\mathbf{a}_i \mathbf{b}_j = 0$ for every $i \neq j$ and $\mathbf{a}_j \mathbf{b}_j = 1$. Take B to be the $n \times n$ matrix whose columns are the vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$, then AB is the identity matrix, so $B = A^{-1}$. Notice also that for every j ,

$$(8) \quad H(\mathbf{b}_j) \leq \mathcal{H}(\mathbf{b}_j) = \mathcal{H}(V_j) = \mathcal{H}(A_j) \leq \prod_{i=1, i \neq j}^n \mathcal{H}(\mathbf{a}_i) \leq n^{\frac{n-1}{2}} \prod_{i=1, i \neq j}^n H(\mathbf{a}_i),$$

by (5) combined with Lemma 2.2 and (4). Since $H(B) = \max_{1 \leq j \leq n} H(\mathbf{b}_j)$ and $H(\mathbf{a}_i) \leq H(A)$ for every $1 \leq i \leq n$, (6) follows.

To obtain the second inequality, we will use Siegel's lemma (see Theorem 3.1 below) to choose a specific vector $\mathbf{x}_j \in V_j$ such that

$$(9) \quad h(\mathbf{x}_j) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{1/2d} \mathcal{H}(V_j) \leq |\Delta_K|^{\frac{1}{2d}} \mathcal{H}(V_j).$$

Now take $\mathbf{b}_j = \frac{1}{\mathbf{a}_j \mathbf{x}_j} \mathbf{x}_j$, then

$$(10) \quad \begin{aligned} h(\mathbf{b}_j) &\leq h \left(\sum_{l=1}^n a_{jl} x_{jl}, \mathbf{x}_j \right) \leq h \left(\sum_{l=1}^n a_{jl} x_{jl} \right) h(\mathbf{x}_j) \leq n h(\mathbf{a}_j) h(\mathbf{x}_j)^2 \\ &\leq n |\Delta_K|^{\frac{1}{2d}} h(\mathbf{a}_j) \mathcal{H}(V_j)^2, \end{aligned}$$

where the last inequality follows by (9). Combining (10) with (8) and observing that $h(B) = \max_{1 \leq j \leq n} h(\mathbf{b}_j)$ and $h(\mathbf{a}_i) \leq h(A)$ for every $1 \leq i \leq n$, we obtain (7). \square

Next we present a useful bound on the height of a vector whose coordinates are images of a given point under a collection of polynomials.

Lemma 2.4. *Let F_1, \dots, F_k be polynomials of respective degrees m_1, \dots, m_k in $K[x_1, \dots, x_n]$ and $\mathbf{z} \in K^n$. Then*

$$(11) \quad h(F_1(\mathbf{z}), \dots, F_k(\mathbf{z})) \leq \mathcal{N} \mathfrak{H} h(\mathbf{z})^m,$$

where $\mathcal{N} = \max_{1 \leq i \leq k} \mathcal{N}(F_i)$, $\mathfrak{H} = \max_{1 \leq i \leq k} h(F_i)$ and $m = \max_{1 \leq i \leq k} m_i$.

Proof. For each $1 \leq i \leq k$, let us write

$$F_i(\mathbf{x}) = \sum_J f_J \mathbf{x}^J,$$

where $J = (j_1, \dots, j_n)$ is a multi-index with $0 \leq j_l \leq m_i$ for each $1 \leq l \leq n$. Let $\mathbf{z} \in K^n$, then for every $v \nmid \infty$ in $M(K)$,

$$|F_i(\mathbf{z})|_v \leq \max_J \left\{ |f_J|_v \prod_{l=1}^n |z_l|_v^{j_l} \right\} \leq \max_J \{|f_J|_v\} \max\{1, |z_1|_v, \dots, |z_n|_v\}^{m_i},$$

and for $v \mid \infty$ in $M(K)$,

$$|F_i(\mathbf{z})|_v \leq \mathcal{N}(F_i) \max_J \left\{ |f_J|_v \prod_{l=1}^n |z_l|_v^{j_l} \right\} \leq \mathcal{N}(F_i) \max\{|f_J|_v\} \max\{1, |z_1|_v, \dots, |z_n|_v\}^{m_i}.$$

Then

$$\begin{aligned} h(F_1(\mathbf{z}), \dots, F_k(\mathbf{z})) &\leq \prod_{v \in M(K)} \max\{1, |F_1(\mathbf{z})|_v, \dots, |F_k(\mathbf{z})|_v\}^{\frac{d_v}{d}} \\ &\leq \left(\max_{1 \leq i \leq k} \mathcal{N}(F_i) \right) \left(\max_{1 \leq i \leq k} h(F_i) \right) h(\mathbf{z})^{\max_{1 \leq i \leq k} m_i}. \end{aligned}$$

This is precisely (11). \square

The next lemma bounds the height of a polynomial under a linear transformation.

Lemma 2.5. *Let $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ be a polynomial of degree m and let A be an $n \times k$ matrix over K . For a variable vector $\mathbf{y} = (y_1, \dots, y_k)$, define $G(\mathbf{y}) = F(A\mathbf{y}^\top)$, then G is a polynomial in k variables over K of degree $\leq m$. Further,*

$$h(G) \leq k^m \mathcal{N}(F) h(F) h(A)^m.$$

Proof. Write $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq k}$ and notice that

$$A\mathbf{y}^\top = \left(\sum_{j=1}^k a_{1j} y_j, \dots, \sum_{j=1}^k a_{nj} y_j \right)^\top.$$

Then $G(\mathbf{y}) = F\left(\sum_{j=1}^k a_{1j} y_j, \dots, \sum_{j=1}^k a_{nj} y_j\right)$. Each linear form $\sum_{j=1}^k a_{ij} y_j$ has coefficient vector of inhomogeneous height $\leq h(A)$, and F has $\mathcal{N}(F)$ monomials each of degree no bigger than m and height no bigger than $h(F)$. Therefore

$$h(G) \leq \mathcal{N}(F) h(F) (kh(A))^m,$$

where k^m is an upper bound on the binomial coefficients which occur when taking m -th power of a linear form. This is precisely the result of the lemma. \square

Next, we introduce the notion of “sparsity” of vectors. We say that a vector $\mathbf{x} \in K^n$ is s -sparse for some $1 \leq s \leq n$ if \mathbf{x} has no more than s nonzero coordinates. Let $\mathbf{e}_1, \dots, \mathbf{e}_n$ be the standard basis for K^n , and for an indexing subset $I \subseteq \{1, \dots, n\}$ of cardinality t let

$$(12) \quad \mathbb{H}_I = \text{span}_K \{\mathbf{e}_i : i \in I\}$$

be the corresponding t -dimensional coordinate subspace of K^n . Then every vector in \mathbb{H}_I is t -sparse and $\mathcal{H}(\mathbb{H}_I) = 1$.

The following lemma that will be quite important to us is a rigorous form of the basic principle that a polynomial which is not identically zero cannot vanish “too much”. Somewhat different formulations of this principle can be found in [5] (Lemma 1 on p. 261) as well as in the context of N. Alon’s celebrated Combinatorial Nullstellensatz [1]. The following formulation, which is most convenient for our purposes follows easily from Lemma 2.2 of [9].

Lemma 2.6. *Suppose $P(\mathbf{x}) \in K[x_1, \dots, x_n]$ is a polynomial of degree m which is not identically 0. There exists a point $\mathbf{z} \in \mathbb{Z}^n$ such that $P(\mathbf{z}) \neq 0$ and*

$$h(\mathbf{z}) \leq \frac{m+2}{2}.$$

3. ON SIEGEL’S LEMMA

Let us recall the classical Siegel’s lemma over a number field K as proved in [2] by Bombieri and Vaaler (see also Theorem 1.1 of [7] for a generalized formulation over different choices of the ground field).

Theorem 3.1. *Let $V \subseteq K^n$ be an m -dimensional subspace, $1 \leq m \leq n$. There exists a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$ for V such that*

$$(13) \quad \prod_{i=1}^m h(\mathbf{x}_i) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{m/2d} \mathcal{H}(V).$$

Our main goal in this section to establish a “sparse” version of Siegel’s lemma, i.e., existence of a small-height basis of sparse vectors for V . One can ask if a sparse basis necessarily exists. Suppose $\mathbf{x}_1, \dots, \mathbf{x}_m$ is some basis for V and write $X = (\mathbf{x}_1 \dots \mathbf{x}_m)$ for the corresponding $n \times m$ basis matrix, so that $V = XK^m$. Let Y be the reduced column-echelon form of X . Then $V = YK^m$ so column vectors of Y again form a basis for V . Further, the first column of Y has the fewest number of zero coordinates, and this number is at least equal to the number of remaining columns, which is $m - 1$, since all the entries to the left of the leading 1 in each column are 0’s. Hence the column vectors of Y provide a basis of $(n - m + 1)$ -sparse vectors for V . On the other hand, it is not so easy to produce a bound on the height of these basis vectors, since it is tricky to keep track of the coefficients used in the column-echelon reduction. To do this, we need a certain version of Siegel’s lemma with avoidance conditions established in [7] (Corollary 1.5).

Theorem 3.2. *Let $V \subseteq K^n$ be an m -dimensional subspace, $1 \leq m \leq n$, and $U_1, \dots, U_k \subset K^n$ be subspaces such that $V \not\subseteq \bigcup_{i=1}^k U_i$. Then there exists $\mathbf{x} \in V \setminus \left(\bigcup_{i=1}^k U_i \right)$ such that*

$$h(\mathbf{x}) \leq \sqrt{2m} |\Delta_K|^{\frac{m+1}{2d}} k^{\frac{1}{d}} \mathcal{H}(V).$$

With this in mind, we can prove the following result.

Theorem 3.3. *Let $V \subseteq K^n$ be an m -dimensional subspace, $1 \leq m \leq n$. Then V contains a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$ of $(n - m + 1)$ -sparse vectors such that*

$$(14) \quad h(\mathbf{x}_i) \leq \sqrt{2}m|\Delta_K|^{\frac{m+1}{2d}} \mathcal{H}(V).$$

for each $1 \leq i \leq m$.

Proof. Take $t = n - m + 1$. First suppose that V is contained in some t -dimensional coordinate subspace. Then the basis guaranteed by Theorem 3.1 is $(n - m + 1)$ -sparse and satisfies the bound (14). Hence we can assume that V is not contained in any such \mathbb{H}_I . Let

$$\mathcal{J}(n, t) = \{I \subset \{1, \dots, n\} : |I| = t\}.$$

Then cardinality of $\mathcal{J}(n, t)$ is equal to $\binom{n}{t}$. Pick some $I_1 \in \mathcal{J}(n, t)$ and let m_1 be the dimension of the subspace $V \cap \mathbb{H}_{I_1} \subsetneq V$. Since $\dim V + \dim \mathbb{H}_{I_1} > n$, we must have $1 \leq m_1 < m$. Let \mathbf{x}_1 be a vector of smallest height from a basis for $V \cap \mathbb{H}_{I_1}$ guaranteed by Theorem 3.1, then \mathbf{x}_1 is an $(n - m + 1)$ -sparse vector satisfying

$$(15) \quad h(\mathbf{x}_1) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{1}{2d}} \mathcal{H}(V \cap \mathbb{H}_{I_1})^{\frac{1}{m_1}} \leq |\Delta_K|^{\frac{1}{2d}} \mathcal{H}(V),$$

since $\mathcal{H}(V \cap \mathbb{H}_{I_1}) \leq \mathcal{H}(V)\mathcal{H}(\mathbb{H}_{I_1}) = \mathcal{H}(V)$ by Lemma 2.1. Let $V_1 = K\mathbf{x}_1$. Now, by our column-echelon form argument above, we know that V has a basis of $(n - m + 1)$ -sparse vectors, hence there must exist some $I_2 \in \mathcal{J}(n, t)$ such that $V \cap \mathbb{H}_{I_2} \not\subseteq V_1$. Every vector in $V \cap \mathbb{H}_{I_2}$ is again $(n - m + 1)$ -sparse, so let $\mathbf{x}_2 \in (V \cap \mathbb{H}_{I_2}) \setminus V_1$ be a vector guaranteed by Theorem 3.2, then

$$(16) \quad h(\mathbf{x}_2) \leq \sqrt{2}m|\Delta_K|^{\frac{m+1}{2d}} \mathcal{H}(V),$$

since $k = 1$ in this case, dimension of $V \cap \mathbb{H}_{I_2}$ is $\leq m$ and again $\mathcal{H}(V \cap \mathbb{H}_{I_2}) \leq \mathcal{H}(V)\mathcal{H}(\mathbb{H}_{I_2}) = \mathcal{H}(V)$. Let $V_2 = \text{span}_K\{V_1, \mathbf{x}_2\}$, then either $V_2 = V$ or, again, there must exist some $I_3 \in \mathcal{J}(n, t)$ such that $V \cap \mathbb{H}_{I_3} \not\subseteq V_2$, and hence we can use Theorem 3.2 to obtain $\mathbf{x}_3 \in (V \cap \mathbb{H}_{I_3}) \setminus V_2$ with height bounded the same way as in (16). Continuing in the same manner m times, we obtain an $(n - m + 1)$ -sparse basis satisfying (14), since the bound of (15) is less than the bound of (16). \square

4. ZEROS OF MULTIPLE POLYNOMIALS

The main goal of this section is to prove Theorem 1.1. Let the notation be as in the statement of the theorem.

Proof of Theorem 1.1. Let r be the rank of the linear system (2), which is the same as the rank of the homogeneous system as in the statement of the theorem. If $r < k$, then $k - r$ equations of (2) are dependent on the rest of them, and so every solution to the rest of the equations is automatically a solution to the whole system. Since r equations are linearly independent, there must exist some $r \times r$ submatrix of the coefficient matrix of these equations with entries $F_{ij}(\mathbf{x}_{I'})$ which is nonsingular for some $\mathbf{x}_{I'} \in K^{n-k}$, and hence the determinant of this matrix is not identically zero as a polynomial in the variables of $\mathbf{x}_{I'}$. We can set all the $k - r$ variables x_{i_j} not corresponding to the columns of this submatrix equal to 0, and hence reduce to the

case of r equations in r variables. Hence we can assume without loss of generality that $r = k$.

Let us rewrite (2) as

$$(17) \quad \mathcal{F}(\mathbf{x}_{I'})\mathbf{x}_I = \mathbf{f}(\mathbf{x}_{I'}),$$

where $\mathcal{F}(\mathbf{x}_{I'})$ is the $k \times k$ matrix with entries $F_{ij}(\mathbf{x}_{I'})$, $\mathbf{f}(\mathbf{x}_{I'})$ is the k -dimensional column vector with coordinates $-F_{i(k+1)}(\mathbf{x}_{I'})$ and $\mathbf{x}_I = (x_{i_1}, \dots, x_{i_k})^\top$ is the variable vector. Then $\mathcal{F}(\mathbf{x}_{I'})$ is nonsingular for some choice of $\mathbf{x}_{I'} \in K^{n-k}$, hence $P(\mathbf{x}_{I'}) := \det(\mathcal{F}(\mathbf{x}_{I'}))$ is not identically zero as a polynomial in the variables $\mathbf{x}_{I'}$. Notice that $\deg(P) \leq \sum_{i=1}^k \deg(F_i) = D$, and hence by Lemma 2.6 there exists a point $\mathbf{z}_{I'} \in \mathbb{Z}^{n-k}$ such that $P(\mathbf{z}_{I'}) \neq 0$ and

$$(18) \quad h(\mathbf{z}_{I'}) \leq \frac{D+2}{2}.$$

Plugging in $\mathbf{z}_{I'}$ for $\mathbf{x}_{I'}$ into (17), we obtain a nonsingular linear system of k equations in k variables, and hence have a unique solution $\mathbf{z}_I = \mathcal{F}(\mathbf{z}_{I'})^{-1}\mathbf{f}(\mathbf{z}_{I'})$. Combining \mathbf{z}_I with $\mathbf{z}_{I'}$ into appropriately indexed coordinates, we obtain a vector $\mathbf{z} \in \bigcap_{j=1}^k Z_K(F_j)$ and $H(\mathbf{z}) = H(\mathbf{z}_I, \mathbf{z}_{I'})$.

We now estimate the height of \mathbf{z}_I . First notice that, by Lemma 2.3,

$$(19) \quad h(\mathcal{F}(\mathbf{z}_{I'})^{-1}) \leq k^k |\Delta_K|^{\frac{1}{d}} h(\mathcal{F}(\mathbf{z}_{I'}))^{2k-1}.$$

On the other hand,

$$(20) \quad h(\mathcal{F}(\mathbf{z}_{I'})) = H(1, F_{11}(\mathbf{z}_{I'}), \dots, F_{kk}(\mathbf{z}_{I'})) \leq \mathcal{N}h(\mathbf{z}_{I'})^m \max_{1 \leq i \leq k} h(F_i),$$

as well as

$$(21) \quad h(\mathbf{f}(\mathbf{z}_{I'})) = H(1, -F_{1(k+1)}(\mathbf{z}_{I'}), \dots, -F_{k(k+1)}(\mathbf{z}_{I'})) \leq \mathcal{N}h(\mathbf{z}_{I'})^m \max_{1 \leq i \leq k} h(F_i),$$

both by Lemma 2.4. Combining (19), (20), (21) and (18), we obtain:

$$(22) \quad \begin{aligned} h(\mathbf{z}_I) &= h(\mathcal{F}(\mathbf{z}_{I'})^{-1}\mathbf{f}(\mathbf{z}_{I'})) \leq kh(\mathcal{F}(\mathbf{z}_{I'})^{-1})h(\mathbf{f}(\mathbf{z}_{I'})) \\ &\leq k^{k+1} |\Delta_K|^{\frac{1}{d}} h(\mathcal{F}(\mathbf{z}_{I'}))^{2k-1} h(\mathbf{f}(\mathbf{z}_{I'})) \\ &\leq k^{k+1} |\Delta_K|^{\frac{1}{d}} \left(\mathcal{N}h(\mathbf{z}_{I'})^m \max_{1 \leq i \leq k} h(F_i) \right)^{2k} \\ &\leq k^{k+1} |\Delta_K|^{\frac{1}{d}} \left(\mathcal{N} \left(\frac{D+2}{2} \right)^m \max_{1 \leq i \leq k} h(F_i) \right)^{2k}. \end{aligned}$$

Now notice that

$$\begin{aligned} h(\mathbf{z}) &= H(1, \mathbf{z}_I, \mathbf{z}_{I'}) = \prod_{v \in M(K)} \max \{1, |\mathbf{z}_I|_v, |\mathbf{z}_{I'}|_v\}^{\frac{d_v}{d}} \\ &\leq \prod_{v \in M(K)} \left(\max \{1, |\mathbf{z}_I|_v\}^{\frac{d_v}{d}} \max \{1, |\mathbf{z}_{I'}|_v\}^{\frac{d_v}{d}} \right) = h(\mathbf{z}_I)h(\mathbf{z}_{I'}), \end{aligned}$$

and hence the theorem follows from (18) and (22). \square

Remark 4.1. Our argument leads to an algorithm for finding a simultaneous zero \mathbf{z} of the polynomial system (2) under the assumption that it exists:

- (1) Compute $P(\mathbf{x}_{I'}) = \det(\mathcal{F}(\mathbf{x}_{I'}))$ as a polynomial in the variables $\mathbf{x}_{I'}$.

- (2) Search through the set of integer points of sup-norm $\leq \deg(P)$ to find $\mathbf{z}_{I'}$ such that $P(\mathbf{z}_{I'}) \neq 0$.
- (3) For this choice of $\mathbf{z}_{I'}$, compute $\mathcal{F}(\mathbf{z}_{I'})$ and $\mathbf{f}(\mathbf{z}_{I'})$.
- (4) Compute $\mathcal{F}(\mathbf{z}_{I'})^{-1}$.
- (5) Compute $\mathbf{z}_I = \mathcal{F}(\mathbf{z}_{I'})^{-1}\mathbf{f}(\mathbf{z}_{I'})$.
- (6) Combine \mathbf{z}_I and $\mathbf{z}_{I'}$ according to the indices of the coordinates to obtain the vector \mathbf{z} .

5. ZEROS OF ONE POLYNOMIAL

In this section, we prove existence of a zero of bounded height for a polynomial F , linear in at least one variable, outside of an algebraic set not containing the entire zero locus of F . Our main goal is to prove Theorem 1.2.

Proof of Theorem 1.2. Assume without loss of generality that F is linear in x_n . Define $\mathbf{x}' := (x_1, \dots, x_{n-1})$, so $\mathbf{x} = (\mathbf{x}', x_n)$. We can write

$$F(x_1, \dots, x_n) = x_n F_1(x_1, \dots, x_{n-1}) + F_2(x_1, \dots, x_{n-1}),$$

where $\deg F_1 \leq g - 1$, $\deg F_2 \leq g$ and both of them are polynomials in $n - 1$ variables \mathbf{x}' with at least F_1 not identically zero. Then we can describe $Z_K(F)$ as the union $Z_K^1(F) \cup Z_K^2(F)$, where

$$(23) \quad \begin{aligned} Z_K^1(F) &= \{\mathbf{z} \in K^n : F_1(\mathbf{z}') = F_2(\mathbf{z}') = 0\}, \\ Z_K^2(F) &= \{\mathbf{z} \in K^n : F_1(\mathbf{z}') \neq 0, z_n = -F_2(\mathbf{z}')/F_1(\mathbf{z}')\}. \end{aligned}$$

Let $Z_K^2(F)' = \{\mathbf{z}' : \mathbf{z} \in Z_K^2(F)\}$, and define

$$Q(\mathbf{x}') = P\left(x_1, \dots, x_{n-1}, -\frac{F_2(\mathbf{x}')}{F_1(\mathbf{x}')}\right) F_1(\mathbf{x}')^m.$$

Since the degree of P is m , Q is a polynomial in $n - 1$ variables \mathbf{x}' on $Z_K^2(F)'$. Let us show that Q is not identically 0. Suppose it is, then $P(Z_K^2(F)) = 0$. For each $\mathbf{z}' \in Z_K^2(F)'$ view $P(\mathbf{z}', x_n)$ as a polynomial in one variable x_n . Since

$$x_n = -F_2(\mathbf{z}')/F_1(\mathbf{z}')$$

is a root of this polynomial, the linear factor $x_n + F_2(\mathbf{z}')/F_1(\mathbf{z}')$ must divide it, and since we are working over a field, we can say that $F_1(\mathbf{z}')x_n + F_2(\mathbf{z}')$ divides $P(\mathbf{z}', x_n)$ for every $\mathbf{z}' \in Z_K^2(F)'$. This implies that $P(\mathbf{x})$ must be divisible by $x_n F_1(\mathbf{x}') + F_2(\mathbf{x}') = F(\mathbf{x})$, and therefore $Z_K(F) \subseteq Z_K(P)$. This is a contradiction, and hence there exists $\mathbf{z}' \in Z_K^2(F)'$ such that $Q(\mathbf{z}') \neq 0$. We want to find such \mathbf{z}' of bounded height. Notice that

$$\deg Q \leq m \deg F_2 + m \deg F_1 \leq m(g + g - 1) = m(2g - 1).$$

By Lemma 2.6, there exists $\mathbf{z}' \in \mathbb{Z}^{n-1}$ such that $Q(\mathbf{z}') \neq 0$ and

$$(24) \quad h(\mathbf{z}') \leq \frac{\deg Q + 1}{2} = \frac{m(2g - 1) + 2}{2}.$$

Then we can estimate the height of the corresponding point $\mathbf{z} = \left(\mathbf{z}', -\frac{F_2(\mathbf{z}')}{F_1(\mathbf{z}')}\right)$. Notice that

$$\begin{aligned}
h(\mathbf{z}) &\leq H(1, F_1(\mathbf{z}')\mathbf{z}', F_2(\mathbf{z}')) \\
&= \prod_{v \in M(K)} \max\{1, |F_1(\mathbf{z}')z_{1v}|, \dots, |F_1(\mathbf{z}')z_{n-1v}|, |F_2(\mathbf{z}')|_v\}^{\frac{d_v}{d}} \\
&\leq \prod_{v \in M(K)} (\max\{1, |F_1(\mathbf{z}')|_v, |F_2(\mathbf{z}')|_v\} \max\{1, |z_{1v}|, \dots, |z_{n-1v}|\})^{\frac{d_v}{d}} \\
(25) \quad &\leq H(1, F_1(\mathbf{z}'), F_2(\mathbf{z}')) h(\mathbf{z}') \leq \mathcal{N}(F)h(F)h(\mathbf{z}')^g h(\mathbf{z}'),
\end{aligned}$$

where the last inequality follows by Lemma 2.4. Combining (24) and (25) yields (3). \square

Remark 5.1. Notice that description (23) immediately implies that $Z_K(F)$ is not empty, and therefore taking P to be a nonzero constant polynomial we see that F has a zero $\mathbf{z} \in K^n$ with $h(\mathbf{z}) \leq \mathcal{N}(F)h(F)$. Further, our argument allows for an explicit algorithm to find the point \mathbf{z} in question, similar to the procedure described in Remark 4.1 for Theorem 1.1: here, we just need to do a finite search for an integer point \mathbf{z}' so that $Q(\mathbf{z}') \neq 0$ and define $\mathbf{z} = \left(\mathbf{z}', -\frac{F_2(\mathbf{z}')}{F_1(\mathbf{z}')}\right)$.

One can further ask if a result similar to Theorem 1.2 holds with a restriction to a subspace V of K^n . The problem here is that the restriction of our polynomial F to V may no longer be linear in any of the variables. For example, if $F(x_1, x_2) = x_1x_2$ and $V = K \begin{pmatrix} 1 \\ 1 \end{pmatrix} \subset K^2$, then the restriction of F to V is

$$F_V(x) = F(x, x) = x^2,$$

and hence is not linear. On the other hand, we can prove a simple lemma in case $\dim_K V = 1$.

Lemma 5.1. *Let F, P be as in Theorem 1.2 and suppose V is a one-dimensional subspace of K^n such that*

$$Z_K(F, V) := Z_K(F) \cap V \not\subseteq Z_K(P).$$

Then there exists $\mathbf{z} \in Z_K(F, V) \setminus Z_K(P)$ such that

$$h(\mathbf{z}) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{m+1}{2d}} \mathcal{N}(F)^{\frac{3}{2}} h(F) \mathcal{H}(V)^{m+1}.$$

Proof. Now suppose that V is a one-dimensional subspace of K^n , i.e., $\ell = 1$. Then $V = K\mathbf{y}$ for some vector $\mathbf{y} \in K^n$ and $F(\alpha\mathbf{y}) = 0$ for some $\alpha \in K$ such that $\mathbf{z} := \alpha\mathbf{y} \notin Z_K(P)$, since $Z_K(F, V) \not\subseteq Z_K(P)$. By Theorem 3.1, we can choose \mathbf{y} such that

$$(26) \quad h(\mathbf{y}) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{1}{2d}} \mathcal{H}(V).$$

Then F_V is a polynomial in one variable of degree $\leq m$ with

$$(27) \quad h(F_V) \leq \mathcal{N}(F)h(F)h(\mathbf{y})^m \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{m}{2d}} \mathcal{N}(F)h(F)\mathcal{H}(V)^m,$$

by Lemma 2.5 combined with (26). Let $\alpha_1, \dots, \alpha_k$ be the roots of F_V , $k \leq m$, with repetition if necessary. Then Lemma 2 of [16] combined with (4) guarantees that

$$(28) \quad \prod_{i=1}^k h(\alpha_i) \leq \sqrt{\mathcal{N}(F)} h(F_V).$$

Observing that $\max_{1 \leq i \leq k} h(\alpha_i) \leq \prod_{i=1}^k h(\alpha_i)$ and combining (27) with (28), we obtain

$$\max_{1 \leq i \leq k} h(\alpha_i \mathbf{y}) \leq h(\mathbf{y}) \max_{1 \leq i \leq k} h(\alpha_i) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{m+1}{2d}} \mathcal{N}(F)^{\frac{3}{2}} h(F) \mathcal{H}(V)^{m+1},$$

which is the bound of the lemma. This completes the proof. \square

6. ZEROS OF MULTILINEAR FORMS

In this section we prove Theorem 1.3. For $n \geq 2$, let $n \geq g \geq 1$ and let $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ be a multilinear (n, g) -form, which is not identically zero.

Lemma 6.1. *There exists a nonzero point $\mathbf{z} \in K^n$ such that $F(\mathbf{z}) = 0$ and*

$$(29) \quad H(\mathbf{z}) \leq H(F).$$

Proof. We argue by induction on n . If $n = 2$, then

$$F(x_1, x_2) = ax_1 + bx_2, \text{ or } F(x_1, x_2) = cx_1x_2,$$

for some $a, b, c \in K$. In the first case, $F(-b, a) = 0$, and in the second $F(0, 1) = 0$. In either case, the nontrivial zero $\mathbf{z} = (-b, a)$ or $\mathbf{z} = (0, 1)$ satisfies the bound (29).

Suppose now $n > 2$. If $n = g$, then

$$F(x_1, \dots, x_n) = cx_1 \cdots x_n,$$

and so $F(0, \dots, 0, 1) = 0$. Hence assume $n > g$, then for some $1 \leq i \leq n$ we can write

$$F(x_1, \dots, x_n) = x_i F_1(\mathbf{x}'_i) + F_2(\mathbf{x}'_i),$$

where

$$\mathbf{x}'_i = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$$

is the vector of $n-1$ variables excluding x_i and F_1, F_2 are multilinear forms in $n-1$ variables, not identically zero. By the induction hypothesis, there exists a nonzero point $\mathbf{z}' \in K^{n-1}$ such that $F_2(\mathbf{z}') = 0$ satisfying (29). Define \mathbf{z} by inserting 0 for the i -th coordinate in \mathbf{z}' , then $F(\mathbf{z}) = 0$ and \mathbf{z} satisfies (29). \square

On the other hand, if $V \subseteq K^n$ is a subspace of K^n , then F may not necessarily have nontrivial zeros on V . Indeed, the form $x_1 + x_2$ has no nontrivial zeros on the subspace $\{(a, 2a) : a \in \mathbb{Q}\}$ of \mathbb{Q}^2 . There are, however, some situations when F is guaranteed to have nontrivial zeros on V , and then we can find such zeroes of small height.

Lemma 6.2. *Assume $g > 1$ and let F be a multilinear (n, g) -form over K and $\mathbf{x} \in K^n$ a $(g-1)$ -sparse vector. Then $F(\mathbf{x}) = 0$.*

Proof. The vector \mathbf{x} has no more than $g - 1$ nonzero coordinates. Hence $F(\mathbf{x}) = 0$, since every monomial of F has degree g and is linear in each variable, hence is a product of $g > 1$ distinct variables. \square

Corollary 6.3. *Let $V \subseteq K^n$ be an m -dimensional subspace of K^n and F a multilinear (n, g) -form over K . Assume that $m + g - 1 > n$ and $g > 1$. Then V contains a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$ of vectors such that $F(\mathbf{x}_1) = \dots = F(\mathbf{x}_m) = 0$ and*

$$(30) \quad H(\mathbf{x}_i) \leq \sqrt{2}m |\Delta_K|^{\frac{m+1}{2d}} \mathcal{H}(V).$$

for each $1 \leq i \leq m$.

Proof. By Theorem 3.3, V contains a basis $\mathbf{x}_1, \dots, \mathbf{x}_m$ of $(n - m + 1)$ -sparse vectors satisfying (30). Since $m + g - 1 > n$, these vectors have no more than $g - 1 \geq n - m + 1$ nonzero coordinates, and hence $F(\mathbf{x}_i) = 0$ for each $1 \leq i \leq m$. \square

Corollary 6.4. *Let $V \subseteq K^n$ be an m -dimensional subspace of K^n and F a multilinear (n, g) -form over K . Assume that $m + g - 1 > n$ and $g > 1$. Suppose also that $P(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ is a polynomial such that $D(P, V) < m$. Then there exists a point $\mathbf{z} \in V \setminus Z_K(P, V)$ such that $F(\mathbf{z}) = 0$ and*

$$H(\mathbf{z}) \leq \sqrt{2}m |\Delta_K|^{\frac{m+1}{2d}} \mathcal{H}(V).$$

Proof. Let $\mathbf{x}_1, \dots, \mathbf{x}_m$ be the $(n - m + 1)$ -sparse basis for V guaranteed by Theorem 3.3. Since $m + g - 1 > n$, we see that $g > n - m + 1$ and hence $F(\mathbf{x}_i) = 0$ for each $1 \leq i \leq m$, by the same argument as in the proof of Corollary 6.3. Since $D(P, V) < m$, at least one of these vectors is not in $Z_K(P, V)$. Call this vector \mathbf{z} , and the result follows. \square

Proof of Theorem 1.3. The theorem now follows by combining Corollaries 6.3 and 6.4. As such, it is a consequence of the ‘‘sparse’’ Siegel’s lemma (Theorem 3.3). \square

The case $g = 1$ of linear forms has to be considered separately: this is just a simple case of Theorem 1.4 of [7], which we present here in a simplified form. Suppose that

$$F(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i \in K[x_1, \dots, x_n],$$

and $V \subseteq K^n$ is an m -dimensional subspace.

Lemma 6.5. *Let $V \subseteq K^n$ be an m -dimensional subspace with $2 \leq m \leq n$. Then there exists $\mathbf{0} \neq \mathbf{z} \in V$ such that $F(\mathbf{z}) = 0$ and*

$$(31) \quad H(\mathbf{z}) \leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{1}{2d}} (\sqrt{n} \mathcal{H}(V) H(F))^{\frac{1}{m-1}}.$$

Further, if $P(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ is a polynomial such that $D(P, V) < m - 1$, then there exists a point $\mathbf{z} \in V \setminus Z_K(P, V)$ such that $F(\mathbf{z}) = 0$ and

$$(32) \quad H(\mathbf{z}) \leq \sqrt{n} \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{m-1}{2d}} \mathcal{H}(V) H(F).$$

Proof. Define

$$U(F) = \{\mathbf{x} \in K^n : F(\mathbf{x}) = 0\},$$

then, by (5),

$$(33) \quad \mathcal{H}(U(F)) = \mathcal{H}(F) \leq \sqrt{n}H(F),$$

where $\mathcal{H}(F)$ is the \mathcal{H} height applied to the coefficient vector of F , which has n coordinates. This is an $(n-1)$ -dimensional subspace of K^n and $\dim V \geq 2$, hence

$$\ell := \dim(V \cap U(F)) \geq m-1 \geq 1.$$

By Theorem 3.1, there is a basis $\mathbf{x}_1, \dots, \mathbf{x}_\ell \in V \cap U(F)$ such that

$$(34) \quad \begin{aligned} \prod_{i=1}^{\ell} H(\mathbf{x}_i) &\leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{\ell}{2d}} \mathcal{H}(V \cap U(F)) \\ &\leq \left(\left(\frac{2}{\pi} \right)^{2r_2} |\Delta_K| \right)^{\frac{\ell}{2d}} \mathcal{H}(V)\mathcal{H}(U(F)), \end{aligned}$$

by Lemma 2.1. Then (31) follows by combining (33) with (34) and taking \mathbf{z} to be the vector with smallest height among $\mathbf{x}_1, \dots, \mathbf{x}_\ell$. Since $D(P, V) < m-1$, at least one of these vectors is not in $Z_K(P, V)$, and this implies (32). \square

Acknowledgement: We wish to thank Pavel Guerzhoy for some helpful remarks. We are also grateful to the anonymous referee for many thoughtful suggestions that improved the quality of presentation.

REFERENCES

- [1] N. Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8 (1999), no. 1-2, pp. 7–29.
- [2] E. Bombieri and J. D. Vaaler. On Siegel’s lemma. *Invent. Math.*, 73 (1983), no. 1, pp. 11–32.
- [3] A. Böttcher and L. Fukshansky. Representing integers by multilinear polynomials. *Res. Number Theory*, 6 (2020), no. 4, Paper No. 38, 8 pp.
- [4] T. D. Browning, R. Dietmann and P. D. T. A Elliott. Least zero of a cubic form. *Math. Ann.*, 352 (2012) no. 3, pp. 745–778.
- [5] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1959.
- [6] J. W. S. Cassels. Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 51 (1955), pp. 262–264.
- [7] L. Fukshansky. Algebraic points of small height missing a union of varieties. *J. Number Theory*, 130 (2010), no. 10, pp. 2099–2118.
- [8] L. Fukshansky. Heights and quadratic forms: Cassels’ theorem and its generalizations. *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, 77–93, *Contemp. Math.*, 587, Amer. Math. Soc., Providence, RI, 2013.
- [9] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatsh. Math.*, 147 (2006), no. 1, pp. 25–41.
- [10] P. Gordan. Über den grossten gemeinsamen factor. *Math. Ann.*, 7 (1873), pp. 443–448.
- [11] F. J. Grunewald and D. Segal. How to solve a quadratic equation in integers. *Math. Proc. Cambridge Philos. Soc.*, 89 (1981) no. 1, pp. 1–5.
- [12] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry*, Volume 1. Cambridge Univ. Press, 1947.
- [13] J.-W. M. van Ittersum. Quantitative results on Diophantine equations in many variables. *Acta Arith.*, 194 (2020), pp. 219–240.
- [14] D. W. Masser. Search bounds for Diophantine equations. *A panorama of number theory or the view from Baker’s garden (Zürich, 1999)*, 247–259, Cambridge Univ. Press, Cambridge, 2002.

- [15] Y. V. Matiyasevich. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191 (1970), pp. 279–282.
- [16] C. G. Pinner and J. D. Vaaler. The number of irreducible factors of a polynomial. I. *Trans. Amer. Math. Soc.*, 339 (1993) no. 2, pp. 809–834.
- [17] D. Roy and J. L. Thunder. An absolute Siegel’s lemma. *J. Reine Angew. Math.*, 476 (1996), pp. 1–26.
- [18] C. L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.*, (1929), pp. 41–69
- [19] T. Struppeck and J. D. Vaaler. Inequalities for heights of algebraic subspaces and the Thue-Siegel principle. *Analytic number theory (Allerton Park, IL, 1989)*, *Progr. Math.*, 85 (1990), pp. 493–528.
- [20] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135 (1909), pp. 284–305.

INSTITUTE OF MATHEMATICAL SCIENCES, CLAREMONT GRADUATE UNIVERSITY, CLAREMONT, CA 91711

Email address: maxwell.forst@cgu.edu

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE, CLAREMONT, CA 91711

Email address: lenny@cmc.edu