

Siegel's Lemma with Additional Conditions

Lenny Fukshansky

University of Texas at Austin

The name Siegel's Lemma is usually used to denote results about non-trivial small-height solutions of a system of homogeneous linear equations, or (which is the same) about non-zero points of small height in a given vector space. Such a result in a simple form was first proved by Thue in 1909 using the Dirichlet's box principle. Siegel in 1929 was the first to formally state this principle in the classical case. His result can be interpreted in the following manner:

If W is a subspace of \mathbb{Q}^N of dimension $1 \leq w \leq N$, then there exists a non-zero point \mathbf{x} in W such that

$$H(\mathbf{x}) \ll_{N,w} H(W)^{1/w}$$

for appropriately defined notions of height and with an explicit constant which depends only on N and w .

This principle has been vastly generalized since Siegel. An important version of such a general principle was produced in 1983 by Bombieri and Vaaler. A consequence of their theorem is a direct extension of the above statement to a number field K with the constant in the upper bound now depending on K, N, w . The full power of their result produces a whole basis of small height for W .

We consider the following extension of this problem. Let K be a number field, N, M positive integers. Let W be a subspace of K^N of dimension $1 \leq w \leq N$ and let V_1, \dots, V_M be a collection of proper subspaces of W . We prove the existence of a point \mathbf{x} of small height in W outside of the union of subspaces V_1, \dots, V_M .

We first need to set some notation.

K - number field

O_K - ring of algebraic integers of K

$d = [K : \mathbb{Q}]$ - degree of K over \mathbb{Q}

$M(K)$ - set of all places of K

\mathcal{D}_K - discriminant of K

K_v - completion of K at v for each $v \in M(K)$

$d_v = [K_v : \mathbb{Q}_v]$ - local degree of K at v

For each place $v \in M(K)$ we define the absolute value $\|\cdot\|_v$ 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 $|\cdot|_v$ 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

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

We extend absolute values to vectors by defining the *local heights*. For each $v \in M(K)$ define a local height H_v on K_v^N by

$$H_v(\mathbf{x}) = \max_{1 \leq i \leq N} |x_i|_v, \quad (2)$$

for each $\mathbf{x} \in K_v^N$.

Then we have a *global height function* on K^N :

$$H(\mathbf{x}) = \prod_{v \in M(K)} H_v(\mathbf{x}) \quad (3)$$

We extend the height to polynomials by viewing it as height function of the coefficient vector of a given polynomial. Finally, we also talk of heights of subspaces of K^N . Let $V \subseteq K^N$ be a subspace of dimension J , $1 \leq J \leq N$. Choose a basis $\mathbf{x}_1, \dots, \mathbf{x}_J$ for V in K^N . Then we define

$$H(V) = H(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_J),$$

where \wedge stands for the wedge product of vectors (here we identify an element of $\bigwedge^J K^N$ with its image in $K^{\binom{N}{J}}$ under the standard (lexicographic) isomorphism). This definition is legitimate, since (by product formula) it does not depend on the choice of the basis.

Theorem 1 (F.). *Let K be a number field of degree d with discriminant \mathcal{D}_K and r_2 complex places. Let $N \geq 2$ be an integer, and let W be a subspace of K^N of dimension w , $1 \leq w \leq N$. Let $V_1, \dots, V_M \subseteq W$ be proper subspaces of W of corresponding dimensions $l_1, \dots, l_M \geq 1$. There exists a point $\mathbf{x} \in W \setminus \bigcup_{i=1}^M V_i$ such that*

$$H(\mathbf{x}) \leq (\mathcal{C}_{K,N}^1(W)H(W) + 1) \times \left\{ \left(\sum_{i=1}^M \frac{\mathcal{C}_{K,N}^2(V_i)}{H(V_i)^d} \right)^{\frac{1}{d}} + M^{\frac{1}{d+1}} \right\}, \quad (4)$$

where

$$\mathcal{C}_{K,N}^1(W) = 2^{w - \frac{(wr_2 - 1)}{d}} (wd)^w |\mathcal{D}_K|^{w/2d} \binom{N}{w}^{1/2}, \quad (5)$$

$$\mathcal{C}_{K,N}^2(V_i) = \frac{2^{l_i r_2} \binom{Nd}{l_i d}^{1/2}}{|\mathcal{D}_K|^{l_i/2}}. \quad (6)$$

As a consequence of the method (when $M = 0$), we also can produce a simple version of Siegel's Lemma over a number field. The upper bound exhibits the best possible exponent on $H(W)$. This is an alternative way to produce a Siegel's Lemma over a number field using an elementary construction.

Corollary 2. *Let $W \subseteq K^N$ be a subspace of dimension w , $1 \leq w \leq N$. There exists a non-zero point $\mathbf{x} \in W \cap O_K^N$ such that*

$$H(\mathbf{x}) \leq \left(\frac{wd}{2^{\frac{wd-1}{wd}}} \right) |\mathcal{D}_K|^{1/2d} \binom{N}{w}^{1/2w} H(W)^{1/w}. \quad (7)$$

Another immediate corollary of Theorem 1 can be viewed as a statement about non-vanishing of decomposable forms at points of small height.

The following basic lemma is not difficult to prove.

Lemma 3. *Let $F(X_1, \dots, X_N)$ be a non-zero polynomial with coefficients in K . There exists $\mathbf{x} \in O_K^N$ such that $F(\mathbf{x}) \neq 0$, and*

$$H(\mathbf{x}) \ll_{K,N} M^{1/d}. \quad (8)$$

It is hard however to determine an explicit constant for the upper bound of (8) in the general case. On the other hand, in case F is a decomposable form over K a value for such a constant easily follows from Theorem 1.

Suppose that $W = K^N$ and V_1, \dots, V_M is a collection of nullspaces of linear forms L_1, \dots, L_M in N variables with coefficients in K (i.e. $w = N$ and $l_i = N - 1$ for each $1 \leq i \leq M$). Let

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

Then Theorem 1 produces a point $\mathbf{x} \in K^N$ of small height outside of the $\bigcup_{i=1}^M V_i$, i.e. a point at which F does not vanish. In fact, the following simple bound on $H(\mathbf{x})$ depending only on K , N , and M follows from Theorem 1 in this case:

$$H(\mathbf{x}) \leq 2^{N(d+1)} (Nd)^N |\mathcal{D}_K|^{1/2d} \binom{Nd}{Nd-d}^{1/2} M^{1/d}.$$

The method of proof of Theorem 1 is the following. For a real number $R \geq 1$ we define the set

$$S_R(W) = \{\mathbf{x} \in W \cap O_K^N : \max_{v|\infty} H_v(\mathbf{x}) \leq R\},$$

and for each $1 \leq i \leq M$, let $S_R(V_i) = S_R(W) \cap V_i$.

Define a counting function

$$\begin{aligned} f_W(R) &= |S_R(W)| - \left| \bigcup_{i=1}^M S_R(V_i) \right| \\ &\geq |S_R(W)| - \sum_{i=1}^M |S_R(V_i)|, \end{aligned}$$

so that if $f_W(R) > 0$ then there exists a point of height at most R in $W \cap O_K^N$ outside of $\bigcup_{i=1}^M V_i$.

Thus we want to find the minimal possible R for which $f_W(R) > 0$. We do this by viewing $W \cap O_K^N$ and each $V_i \cap O_K^N$ as a lattice in an appropriate Euclidean space.

The determinant of such a lattice can be related to height of W or V_i respectively (by a theorem of Schmidt, 1967). Then the quantities $|S_R(W)|$ and $|S_R(V_i)|$ for each i can be estimated by counting the number of points of a corresponding lattice in a closed cube with side length $2R$ centered at the origin in the appropriate Euclidean space. The proofs of these counting lemmas are of combinatorial flavor.

The resulting bound on the counting function $f_W(R)$ is of the form

$$f_W(R) \geq aR^{d+1} - 2^{wd}bR - 2^{wd}M,$$

where the constants a and b are explicit and depend on N, K , and heights and dimensions of subspaces W and V_1, \dots, V_M respectively.