10-12-2008

Siegel's Lemma Outside of a Union of Varieties

Lenny Fukshansky
Claremont McKenna College

Siegel's lemma outside of a union of varieties

Lenny Fukshansky
Claremont McKenna College

October 12, 2008

Thue (1909) and Siegel (1929)

Let

$$A\boldsymbol{x} = \mathbf{0} \tag{1}$$

be an $M \times N$ linear system of rank $M < N$ with integer entries. Define the **height** of a vector $\boldsymbol{x} \in \mathbb{Z}^N$ to be

$$|\boldsymbol{x}| = \max_{1 \le i \le N} |x_i|,$$

and similarly let the height of the matrix

$$A = (a_{ij})_{1 \le i \le M, 1 \le j \le N}$$

be

$$|A| = \max\{|a_{ij}| : 1 \le i \le M, 1 \le j \le N\}.$$

Siegel's Lemma: There exists a non-trivial integral solution $\boldsymbol{x}$ to (1) with

$$|\boldsymbol{x}| \le (1 + N|A|)^{\frac{M}{N-M}}, \tag{2}$$

and the exponent $\frac{M}{N-M}$ in (2) is sharp.

This principle can be generalized and extended over global fields.

Notation and heights

Throughout this talk, K will be either a number field, a function field, or algebraic closure of one or the other; in any case, we write $\overline{K}$ for the algebraic closure of K, so it may be that $K = \overline{K}$. In fact, until further notice assume that $K \neq \overline{K}$.

By a function field we will always mean a finite algebraic extension of the field $\mathfrak{K} = \mathfrak{K}_0(t)$ of rational functions in one variable over a field $\mathfrak{K}_0$, where $\mathfrak{K}_0$ can be any field.

In the number field case, we write $d = [K : \mathbb{Q}]$ for the global degree of K over $\mathbb{Q}$; in the function field case, the degree is $d = [K : \mathfrak{K}]$.

Let $M(K)$ be the set of places of K. For each place $v \in M(K)$, write K_v for the completion of K at v and let d_v be the local degree of K at v, which is $[K_v : \mathbb{Q}_v]$ in the number field case, and $[K_v : \mathfrak{K}_v]$ in the function field case.

For each place u of the ground field, be it $\mathbb{Q}$ or $\mathfrak{K}$, we have

$$\sum_{v \in M(K), v|u} d_v = d. \tag{3}$$

If K is a number field, then 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.

If K is a function field, then all absolute values on K are non-archimedean. For each $v \in M(K)$, let $\mathfrak{O}_v$ be the valuation ring of v in K_v and $\mathfrak{M}_v$ the unique maximal ideal in $\mathfrak{O}_v$. We choose the unique corresponding absolute value $|\ |_v$ such that:

(i) if $1/t \in \mathfrak{M}_v$, then $|t|_v = e$,

(ii) if an irreducible polynomial $p(t) \in \mathfrak{M}_v$, then $|p(t)|_v = e^{-\deg(p)}$.

In both cases, for each non-zero $a \in K$ the product formula reads

$$\prod_{v \in M(K)} |a|_v^{d_v} = 1. \tag{4}$$

We can now define local norms on each K_v^N:

$$|\boldsymbol{x}|_v = \max_{1 \leq i \leq N} |x_i|_v,$$

and for all archimedean places v also define

$$\|\boldsymbol{x}\|_v = \left(\sum_{i=1}^{N} |x_i|_v^2 \right)^{1/2},$$

for each $\boldsymbol{x} = (x_1, ..., x_N) \in K_v^N$. Then define a **projective height function** on K^N by

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} |\boldsymbol{x}|_v^{d_v/d}$$

for each $\boldsymbol{x} \in K^N$. The normalizing exponent $1/d$ in the definition ensures that H is **absolute**, i.e. does not depend on the field of definition. H is defined on the projective space $\mathbb{P}^{N-1}(K)$:

$$H(a\boldsymbol{x}) = H(\boldsymbol{x}),\ \forall\ 0 \neq a \in K,\ \boldsymbol{x} \in K^N,$$

which is true by the product formula.

We also define the **inhomogeneous height** on K^N by

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

for all $\boldsymbol{x} \in K^N$, $N \geq 1$. It is easy to see that

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

for all non-zero $\boldsymbol{x} \in K^N$.

While the advantage of H is its projective nature, h is more sensitive when measuring the "arithmetic complexity" of a specific vector, not just the corresponding projective point.

We also define height on subspaces of K^N. Let $V \subseteq K^N$ be an L-dimensional subspace, and let $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ be a basis for V. Then

$$\boldsymbol{y} := \boldsymbol{x}_1 \wedge ... \wedge \boldsymbol{x}_L \in K^{\binom{N}{L}}$$

under the standard embedding. Define

$$\mathcal{H}(V) := \prod_{v \nmid \infty} |\boldsymbol{y}|_v^{d_v/d} \times \prod_{v | \infty} \|\boldsymbol{y}\|_v^{d_v/d}.$$

This definition is legitimate, i.e. does not depend on the choice of the basis. Hence we have defined a height on points of a Grassmanian over K.

Generalized Siegel's lemma

The following general version of Siegel's lemma was proved by Bombieri and Vaaler (1983) if K is a number field, by Thunder (1995) if K is a function field, and by Roy and Thunder (1996) if K is the algebraic closure of one or the other.

Theorem 1. *Let K be a number field, a function field, or the algebraic closure of one or the other. Let $V \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$. Then there exists a basis $\boldsymbol{v}_1, ..., \boldsymbol{v}_L$ for V over K such that*

$$\prod_{i=1}^{L} H(\boldsymbol{v}_i) \leq C_K(L)\mathcal{H}(V), \tag{5}$$

where $C_K(L)$ is an explicit field constant. In fact, if K is a number field or $\overline{\mathbb{Q}}$, then even more is true: there exists such a basis with

$$\prod_{i=1}^{L} H(\boldsymbol{v}_i) \leq \prod_{i=1}^{L} h(\boldsymbol{v}_i) \leq C_K(L)\mathcal{H}(V). \tag{6}$$

It is interesting to note that the transition from projective height H to inhomogeneous height h in Theorem 1 is quite straightforward over number fields (in other words, (6) is a fairly direct corollary of (5) in the number field case and over $\overline{\mathbb{Q}}$). In the function field case, however, such a transition is quite non-trivial. In fact, it seems unlikely that a direct analogue of (6) would hold over an arbitrary function field. On the other hand, it is possible to produce such a bound over function fields of genus 0 or 1.

Theorem 2 (F., 2008). *Let $\mathfrak{K}_0$ be any perfect field and let Y be a smooth projective curve over $\mathfrak{K}_0$ of genus $g = 0$ or 1, i.e. Y is either a rational or an elliptic curve. Let $K = \mathfrak{K}_0(Y)$ be the field of rational functions on Y over $\mathfrak{K}_0$, and let $V \subseteq K^N$ be an L-dimensional subspace, $1 \leq L \leq N$. Then there exists a basis $\boldsymbol{u}_1, ..., \boldsymbol{u}_L$ for V over K such that*

$$\prod_{i=1}^{L} H(\boldsymbol{u}_i) \leq \prod_{i=1}^{L} h(\boldsymbol{u}_i) \leq e^{gL} C_K(L) \mathcal{H}(V). \quad (7)$$

where $C_K(L)$ is as above.

The proof of Theorem 2 involves an application of Theorem 1, a weak form of Riemann-Roch theorem, and a special representation for degree zero divisors, which is the underlying reason for the existence of group structure on elliptic curves.

The bounds of (5) - (7) are sharp in the sense that the exponents on $H(V)$ are smallest possible.

For many applications it is also important to have refinements of Siegel's lemma with some additional algebraic conditions. One such example is the so called **Faltings' version of Siegel's lemma**, which guarantees the existence of a point of bounded norm in a vector space $V \subseteq \mathbb{R}^N$ outside of a subspace $U \subsetneq V$. It was proved by Gerd Faltings (1992) and applied in his famous work on Diophantine approximation on abelian varieties.

New refinements

Let us say that a field K is **admissible** if it is a number field, $\overline{\mathbb{Q}}$, or the field of rational functions on a smooth projective curve of genus 0 or 1 over a perfect field.

Theorem 3 (F., 2008)**.** *Let K be an admissible field. Let $N \geq 2$ be an integer, and let V be an L-dimensional subspace of K^N, $1 \leq L \leq N$. Let $\mathcal{Z}_K$ be a union of algebraic varieties defined over K such that $V \nsubseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. Then there exists a point $\boldsymbol{x} \in V \setminus \mathcal{Z}_K$ such that*

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq A_K(L, M)\mathcal{H}(V), \qquad (8)$$

where $A_K(L, M)$ is an explicit field constant.

The exponent 1 on $\mathcal{H}(V)$ in the bound of (8) is best possible.

Sketch of the proof of Theorem 3

- Reduction to the case of one polynomial

- Combinatorial Nullstellensatz on a subspace

- Siegel's lemma (Theorems 1 and 2)

- Inhomogeneous height inequality:

$$h\left(\sum_{i=1}^{L} \xi_i \boldsymbol{v}_i\right) \leq L^{\delta} H(\boldsymbol{\xi}) \prod_{i=1}^{L} h(\boldsymbol{x}_i), \qquad (9)$$

where $\boldsymbol{\xi} \in K^L$, $\boldsymbol{v}_1, \dots, \boldsymbol{v}_L \in K^N$, and

$$\delta = \begin{cases} 1 & \text{if } K \text{ is a number field or } \overline{\mathbb{Q}} \\ 0 & \text{otherwise.} \end{cases}$$

It should be remarked that the inequality (9) no longer holds if the inhomogeneous height h in the upper bound is replaced with the projective height H.

- Assuming we have a bound on $H(\boldsymbol{\xi})$, we can combine (9) with Siegel's lemma to finish the proof.

We want to construct a set $S \subseteq K$ with $|S| > M$ so that $H(\boldsymbol{\xi})$ is small for every $\boldsymbol{\xi} \in S^L$.

If K is a number field with the number of roots of unity $\omega_K > M$, $\overline{\mathbb{Q}}$, or function field with either an infinite field of constants or a finite field of constants $\mathbb{F}_q$ so that $q > M$, then there exists such a set S with $H(\boldsymbol{\xi}) = 1$ for every $\boldsymbol{\xi} \in S^L$.

The main difficulty arises if K is a number field with $\omega_K \leq M$ or if K is a function field over a finite field $\mathbb{F}_q$ with $q \leq M$.

In both cases the construction of S comes from a certain lattice in Euclidean space. In the number field case, this lattice is the image of the ring of algebraic integers O_K under the standard embedding of K into $\mathbb{R}^d$.

In the function field case, this lattice is the image of the ring of rational functions with all zeros and poles on the curve over which K is defined under the principal divisor map.

Lattice point counting estimates are then used to construct S.

Algebraic integers of small height

As a corollary of the proof of Theorem 3, we produce a uniform lower bound on the number of algebraic integers of bounded height in a number field K. The subject of counting *algebraic numbers* of bounded height has been started by the famous asymptotic formula of Schanuel. Some explicit upper and lower bounds have also been produced later, for instance by Schmidt. Recently a new sharp upper bound has been given by Loher and Masser. We produce the following estimate for the number of *algebraic integers*.

Corollary 4 (F., 2008). *Let K be a number field of degree d over $\mathbb{Q}$ with discriminant $\mathcal{D}_K$ and r_1 real embeddings. Let O_K be its ring of integers. For all $R \geq (2^{r_1}|D_K|)^{1/2}$,*

$$(2^{r_1}|\mathcal{D}_K|)^{-1/2} R^d < |\{x \in O_K \ : \ h(x) \leq R\}| .$$