

# Orthogonal Siegel's lemma

Lenny Fukshansky  
Claremont McKenna College

Illinois Number Theory Conference  
May 21-22, 2010

## Thue (1909) and Siegel (1929)

Let

$$Ax = 0 \quad (1)$$

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

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

and similarly let the height of the matrix

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

be

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

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

$$|x| \leq (1 + N|A|)^{\frac{M}{N-M}}, \quad (2)$$

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  $\mathbb{R}$ , we have

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

If  $K$  is a number field, then 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.

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  $|\cdot|_v$  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

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

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

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

and for all archimedean places  $v$  also define

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

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

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

for each  $\mathbf{x} \in K^N$ . 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  $\mathbb{P}^{N-1}(K)$ :

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

which is true by the product formula.

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

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

under the standard embedding. Define

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

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  $K$ .

Finally, for a polynomial  $F(\mathbf{X})$  in  $N$  variables with coefficients in  $K$ , we define its height  $H(F)$  to be the height of its coefficient vector.

## Generalized Siegel's lemma

A general version of Siegel's lemma was obtained 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  $v_1, \dots, v_L$  for  $V$  over  $K$  such that*

$$\prod_{i=1}^L H(v_i) \leq C_K(L) \mathcal{H}(V),$$

where  $C_K(L)$  is an explicit field constant.

## Orthogonal Siegel's lemma for a quadratic space

Theorem 1 can be used to produce a small-height orthogonal basis for a subspace of a symmetric bilinear space. Specifically, we can prove the following theorem.

**Theorem 2** (F., 2007). *Let  $V \subseteq K^N$  be a subspace of dimension  $L$ ,  $1 \leq L \leq N$ , and let  $F$  be a symmetric bilinear form on  $K^N$ . Then there exists a basis  $\mathbf{x}_1, \dots, \mathbf{x}_L \in K^N$  for  $V$  such that  $F(\mathbf{x}_i, \mathbf{x}_j) = 0$  for all  $i \neq j$ , and*

$$\prod_{i=1}^L H(\mathbf{x}_i) \leq C_K^1(L, N) H(F)^{\frac{L(L+1)}{2}} \mathcal{H}(V)^L,$$

where  $C_K^1(L, N)$  is an explicit field constant.

The argument here has to be more delicate than just an application of Gram-Schmidt, which would produce exponential bounds.

## The case of symplectic spaces

Let  $V \subseteq K^N$  be a subspace of dimension  $L = 2k$ ,  $1 \leq k \leq N/2$ , and let  $F$  be an **alternating** bilinear form on  $K^N$ , which is **nonsingular** on  $V$ . A basis  $\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{y}_1, \dots, \mathbf{y}_k \in K^N$  for  $V$  is called **symplectic** with respect to  $F$  if

$$F(\mathbf{x}_i, \mathbf{x}_j) = F(\mathbf{y}_i, \mathbf{y}_j) = F(\mathbf{x}_i, \mathbf{y}_j) = 0$$

$$\forall 1 \leq i \neq j \leq k \text{ and } F(\mathbf{x}_i, \mathbf{y}_i) = 1 \quad \forall 1 \leq i \leq k.$$

**Theorem 3** (F., 2009). *There exists a symplectic basis for  $V$  such that*

$$\prod_{i=1}^{2k} H(\mathbf{x}_i)H(\mathbf{y}_i) \leq C_K^2(k, N)H(F)^{a_k}\mathcal{H}(V)^{b_k},$$

where  $C_K^2(k, N)$  is an explicit field constant,

$$a_k = \begin{cases} \frac{2k^3+9k^2-14k}{12} & \text{if } 2|k \\ \frac{2k^3+9k^2-14k+3}{12} & \text{if } 2 \nmid k, \end{cases}$$

and

$$b_k = \begin{cases} \frac{k^2+4k}{4} & \text{if } 2|k \\ \frac{k^2+4k-1}{4} & \text{if } 2 \nmid k. \end{cases}$$

## Symplectic spaces: the proof

The proof of Theorem 3 is based on Siegel's lemma (Theorem 1), the fact that any maximal totally isotropic subspace of a nonsingular  $2k$ -dimensional symplectic space (called **Lagrangian**) has dimension  $k$ , and the following combinatorial lemma.

**Lemma 4.** *Let  $G$  be a graph on  $2k$  vertices,  $k \geq 1$ , such that a maximal complete subgraph of  $G$  has at most  $k$  vertices. Then there exist at least  $\left\lceil \frac{k+1}{2} \right\rceil$  disjoint pairs of disconnected vertices. This bound is sharp, meaning that there are such graphs in which any maximal (with respect to cardinality) set of disjoint pairs of disconnected vertices has cardinality precisely  $\left\lceil \frac{k+1}{2} \right\rceil$ .*

## Symplectic spaces: Witt decomposition

The symplectic space  $(V, F)$  can always be decomposed as the orthogonal direct sum (with respect to  $F$ ) of  $k$  **hyperbolic planes**:

$$V = \mathbb{H}_1 \perp \cdots \perp \mathbb{H}_k.$$

Such a representation for  $V$  is called a **Witt decomposition**, and is not unique. As an immediate consequence of Theorem 3, we can obtain such a decomposition of bounded height.

**Corollary 5.** *Let  $\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{y}_1, \dots, \mathbf{y}_k$  be the small-height symplectic basis for  $V$  as guaranteed by Theorem 3. For each  $1 \leq i \leq k$ , define a hyperbolic plane  $\mathbb{H}_i = \text{span}_K\{\mathbf{x}_i, \mathbf{y}_i\}$ . This gives a Witt decomposition for  $(V, F)$  with*

$$\prod_{i=1}^{2k} H(\mathbb{H}_i) \leq C_K^2(k, N) H(F)^{a_k} \mathcal{H}(V)^{b_k}.$$

## Symplectic spaces: small-height flags

As another corollary of Theorem 3, we establish the existence of flags of totally isotropic subspaces of bounded height, whose union generates  $V$ .

**Corollary 6.** *Let the notation be as in Theorem 3. For each  $1 \leq n \leq k$ , there exist totally isotropic subspaces  $U_n$  and  $W_n$  of  $(V, F)$  such that  $\dim_K U_n = \dim_K W_n = n$ ,  $U_n \cap W_n = \{0\}$ ,*

$$U_1 \subset U_2 \subset \cdots \subset U_k, \quad W_1 \subset W_2 \subset \cdots \subset W_k,$$

and

$$H(U_n)H(W_n) \leq \left( C_K^2(k, N) H(F)^{a_k} \mathcal{H}(V)^{b_k} \right)^{\frac{n}{k}}.$$

*In particular,  $(V, F)$  is generated by the two small-height Lagrangians  $U_k$  and  $W_k$ , i.e.  $V = \text{span}_K \{U_k, W_k\}$ .*

It should be noted that analogous results for quadratic spaces (i.e. the form is symmetric bilinear) are more difficult to obtain; in particular, they do not follow from the analogous orthogonal version of Siegel's lemma, Theorem 2 - it only happens so in the symplectic case because of its very "linear" nature.