

# On a new version of Siegel's lemma

Lenny Fukshansky  
Claremont McKenna College  
*(joint work with Maxwell Forst)*

Diophantine Approximation, Dynamical Systems and Related  
Topics

*Tsinghua Sanya International Mathematics Forum (TSIMF)*

January 29 - February 2, 2024

## Thue & Siegel

The following observation was first made by A. Thue (1909) and then formally proved by C. L. Siegel (1929).

### Theorem 1 (Siegel's Lemma)

Let  $A$  be a nonzero integer  $m \times n$  matrix,  $1 \leq m < n$ . Then there exists  $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^n$  such that  $A\mathbf{x} = \mathbf{0}$  and

$$|\mathbf{x}| \leq 1 + (n|A|)^{\frac{m}{n-m}}, \quad (1)$$

where  $|\cdot|$  is the sup-norm (maximum of the absolute values of the coordinates) of the vector  $\mathbf{x}$  and the matrix  $A$ , respectively.

## Thue & Siegel

The following observation was first made by A. Thue (1909) and then formally proved by C. L. Siegel (1929).

### Theorem 1 (Siegel's Lemma)

Let  $A$  be a nonzero integer  $m \times n$  matrix,  $1 \leq m < n$ . Then there exists  $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^n$  such that  $A\mathbf{x} = \mathbf{0}$  and

$$|\mathbf{x}| \leq 1 + (n|A|)^{\frac{m}{n-m}}, \quad (1)$$

where  $|\cdot|$  is the sup-norm (maximum of the absolute values of the coordinates) of the vector  $\mathbf{x}$  and the matrix  $A$ , respectively.

This result is used in transcendental number theory and Diophantine approximation for construction of auxiliary polynomials with small integer coefficients which vanish with prescribed multiplicity at given algebraic points. The exponent  $\frac{m}{n-m}$  in (2) is sharp.

## Invariant version

The bound (2) lacks invariance under linear transformations: for any  $m \times m$  integer matrix  $U$ ,

$$(UA)\mathbf{x} = A\mathbf{x} = \mathbf{0},$$

however  $|UA|$  and  $|A|$  can be very different.

## Invariant version

The bound (2) lacks invariance under linear transformations: for any  $m \times m$  integer matrix  $U$ ,

$$(UA)\mathbf{x} = A\mathbf{x} = \mathbf{0},$$

however  $|UA|$  and  $|A|$  can be very different. The first *invariant* version of Siegel's lemma was obtained by E. Bombieri and J. Vaaler.

### Theorem 2 (Bombieri-Vaaler, 1983)

Let  $A$  be a nonzero integer  $m \times n$  matrix,  $1 \leq m < n$ . Then there exists  $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^n$  such that  $A\mathbf{x} = \mathbf{0}$  and

$$|\mathbf{x}| \leq \left( D^{-1} \sqrt{\det(A^T A)} \right)^{\frac{1}{n-m}}, \quad (2)$$

where  $D = \gcd$  of the determinants of all  $m \times m$  minors of  $A$ .

## Absolute values

There is interest in extending this theory to the more general setting of *algebraic numbers*. For this, we need some notation.

## Absolute values

There is interest in extending this theory to the more general setting of *algebraic numbers*. For this, we need some notation.

$K$  = number field,  $M(K)$  = its set of places,  $\Delta_K$  = its discriminant

$d = r_1 + 2r_2 = [K : \mathbb{Q}]$ , where  $r_1$  = number of real embeddings and  $r_2$  = number of pairs of complex conjugate embeddings of  $K$

$\forall v \in M(K)$ ,  $d_v = [K_v : \mathbb{Q}_v]$ , and  $|\cdot|_v$  extends the usual archimedean or the usual  $p$ -adic absolute value on  $\mathbb{Q}$

**Product Formula:**  $\prod_{v \in M(K)} |a|_v^{d_v} = 1$ ,  $\forall 0 \neq a \in K$

## Height function

Let  $n \geq 2$ , and define *local norms*

$$|\mathbf{x}|_v = \max_{1 \leq i \leq n} |x_i|_v \quad \forall v \in M(K), \quad \|\mathbf{x}\|_v = \left( \sum_{i=1}^n |x_i|_v^2 \right)^{1/2} \quad \forall v \mid \infty,$$

where  $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ .



## Height function

Let  $n \geq 2$ , and define *local norms*

$$|\mathbf{x}|_v = \max_{1 \leq i \leq n} |x_i|_v \quad \forall v \in M(K), \quad \|\mathbf{x}\|_v = \left( \sum_{i=1}^n |x_i|_v^2 \right)^{1/2} \quad \forall v \nmid \infty,$$

where  $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ .

A **height function**  $H : K^n \rightarrow \mathbb{R}_{\geq 0}$  is then given by

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

## Height function

Let  $n \geq 2$ , and define *local norms*

$$|\mathbf{x}|_v = \max_{1 \leq i \leq n} |x_i|_v \quad \forall v \in M(K), \quad \|\mathbf{x}\|_v = \left( \sum_{i=1}^n |x_i|_v^2 \right)^{1/2} \quad \forall v \mid \infty,$$

where  $\mathbf{x} = (x_1, \dots, x_n) \in K^n$ .

A **height function**  $H : K^n \rightarrow \mathbb{R}_{\geq 0}$  is then given by

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

By product formula,  $H(a\mathbf{x}) = H(\mathbf{x})$  for every  $0 \neq a \in K$ , hence  $H$  is *projectively defined*. Further,  $H$  is *absolute*, i.e.  $H(\mathbf{x})$  is the same computed over any number field containing coordinates of  $\mathbf{x}$ . We define  $H(\mathbf{0}) = 0$ .

## Schmidt's height on subspaces

We can also talk about height of subspaces of  $K^n$ , as first introduced by **W. M. Schmidt** (1967). Let  $V \subseteq K^n$  be an  $m$ -dimensional subspace, and let  $\mathbf{x}_1, \dots, \mathbf{x}_m$  be a basis for  $V$ .

## Schmidt's height on subspaces

We can also talk about height of subspaces of  $K^n$ , as first introduced by **W. M. Schmidt** (1967). Let  $V \subseteq K^n$  be an  $m$ -dimensional subspace, and let  $\mathbf{x}_1, \dots, \mathbf{x}_m$  be a basis for  $V$ .

Write  $\wedge$  for the usual wedge product of vectors, and let

$$\mathbf{y} := \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_m \in K \binom{n}{m}$$

under the standard lexicographic embedding.

## Schmidt's height on subspaces

We can also talk about height of subspaces of  $K^n$ , as first introduced by **W. M. Schmidt** (1967). Let  $V \subseteq K^n$  be an  $m$ -dimensional subspace, and let  $\mathbf{x}_1, \dots, \mathbf{x}_m$  be a basis for  $V$ .

Write  $\wedge$  for the usual wedge product of vectors, and let

$$\mathbf{y} := \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_m \in K \binom{n}{m}$$

under the standard lexicographic embedding. Define

$$H(V) := H(\mathbf{y}).$$

## Schmidt's height on subspaces

We can also talk about height of subspaces of  $K^n$ , as first introduced by **W. M. Schmidt** (1967). Let  $V \subseteq K^n$  be an  $m$ -dimensional subspace, and let  $\mathbf{x}_1, \dots, \mathbf{x}_m$  be a basis for  $V$ .

Write  $\wedge$  for the usual wedge product of vectors, and let

$$\mathbf{y} := \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_m \in K \binom{n}{m}$$

under the standard lexicographic embedding. Define

$$H(V) := H(\mathbf{y}).$$

This definition does not depend on the choice of the basis.

## Schmidt's height on subspaces

We can also talk about height of subspaces of  $K^n$ , as first introduced by **W. M. Schmidt** (1967). Let  $V \subseteq K^n$  be an  $m$ -dimensional subspace, and let  $\mathbf{x}_1, \dots, \mathbf{x}_m$  be a basis for  $V$ .

Write  $\wedge$  for the usual wedge product of vectors, and let

$$\mathbf{y} := \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_m \in K^{\binom{n}{m}}$$

under the standard lexicographic embedding. Define

$$H(V) := H(\mathbf{y}).$$

This definition does not depend on the choice of the basis.

**Duality:** If  $A = (\mathbf{a}_1 \dots \mathbf{a}_{n-m})^\top$  is an  $(n-m) \times n$  matrix over  $K$  such that

$$V = \{\mathbf{x} \in K^n : A\mathbf{x} = \mathbf{0}\},$$

then

$$H(V) = H(A) := H(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_{n-m}).$$

# Finiteness property

An important property that height functions satisfy, by analogy with  $|\cdot|$  or  $\|\cdot\|$  over  $\mathbb{Z}$  is *finiteness*.



## Finiteness property

An important property that height functions satisfy, by analogy with  $|\cdot|$  or  $\|\cdot\|$  over  $\mathbb{Z}$  is *finiteness*.

**Northcott's theorem:** For every  $d, B \in \mathbb{R}_{>0}$  the set

$$\left\{ [\mathbf{x}] \in \mathbb{P}(\overline{\mathbb{Q}}^n) : \deg_{\mathbb{Q}}(\mathbf{x}) \leq d, H(\mathbf{x}) \leq B \right\}$$

is finite.

## Finiteness property

An important property that height functions satisfy, by analogy with  $|\cdot|$  or  $\|\cdot\|$  over  $\mathbb{Z}$  is *finiteness*.

**Northcott's theorem:** For every  $d, B \in \mathbb{R}_{>0}$  the set

$$\left\{ [\mathbf{x}] \in \mathbb{P}(\overline{\mathbb{Q}}^n) : \deg_{\mathbb{Q}}(\mathbf{x}) \leq d, H(\mathbf{x}) \leq B \right\}$$

is *finite*.

More generally, height measures *arithmetic complexity* (by analogy with *degree* in algebraic geometry measuring *geometric complexity*), and so a point of relatively small height is *arithmetically simple*.

## Bombieri – Vaaler

The following generalized and powerful *subspace version* of Siegel's lemma was proved by Bombieri and Vaaler.

### Theorem 3 (Bombieri-Vaaler, 1983)

Let  $K$  be a number field of degree  $d$  with  $r_2$  pairs of complex conjugate embeddings and discriminant  $\Delta_K$ , and 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  $V$  over  $K$  such that

$$\prod_{i=1}^m H(\mathbf{x}_i) \leq n^{m/2} \left( \left( \frac{2}{\pi} \right)^{r_2} |\Delta_K| \right)^{\frac{m}{2d}} H(V). \quad (3)$$

## Bombieri – Vaaler

The following generalized and powerful *subspace version* of Siegel's lemma was proved by Bombieri and Vaaler.

### Theorem 3 (Bombieri-Vaaler, 1983)

Let  $K$  be a number field of degree  $d$  with  $r_2$  pairs of complex conjugate embeddings and discriminant  $\Delta_K$ , and 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  $V$  over  $K$  such that

$$\prod_{i=1}^m H(\mathbf{x}_i) \leq n^{m/2} \left( \left( \frac{2}{\pi} \right)^{r_2} |\Delta_K| \right)^{\frac{m}{2d}} H(V). \quad (3)$$

In situations when  $|\Delta_K|$  is very large, it may overpower  $H(V)$  in the upper bound. This calls for an *absolute* version that would not depend on a number field.

## Roy – Thunder

An absolute version of Siegel's lemma was established by Roy & Thunder (a similar result was independently obtained by S. Zhang (1995)).

### Theorem 4 (Roy-Thunder, 1996)

Let  $V \subseteq \overline{\mathbb{Q}}^n$  be an  $m$ -dimensional subspace,  $1 \leq m \leq n$ . There exists a basis  $\mathbf{x}_1, \dots, \mathbf{x}_m$  for  $V$  over  $\overline{\mathbb{Q}}$  such that

$$\prod_{i=1}^m H(\mathbf{x}_i) \leq \left( e^{\frac{m(m-1)}{4}} + \varepsilon \right) H(V), \quad (4)$$

for any  $\varepsilon > 0$  (the choice of the basis depends on  $\varepsilon$ ).

## Roy – Thunder

An absolute version of Siegel's lemma was established by Roy & Thunder (a similar result was independently obtained by S. Zhang (1995)).

### Theorem 4 (Roy-Thunder, 1996)

Let  $V \subseteq \overline{\mathbb{Q}}^n$  be an  $m$ -dimensional subspace,  $1 \leq m \leq n$ . There exists a basis  $\mathbf{x}_1, \dots, \mathbf{x}_m$  for  $V$  over  $\overline{\mathbb{Q}}$  such that

$$\prod_{i=1}^m H(\mathbf{x}_i) \leq \left( e^{\frac{m(m-1)}{4}} + \varepsilon \right) H(V), \quad (4)$$

for any  $\varepsilon > 0$  (the choice of the basis depends on  $\varepsilon$ ).

While the Roy-Thunder bound does not depend on any number field, the vectors  $\mathbf{x}_1, \dots, \mathbf{x}_m$  are also not guaranteed to lie over a fixed number field and their degrees over  $\mathbb{Q}$  are not bounded.

## Monotone basis

A vector is  $s$ -sparse if it has no more than  $s$  nonzero coordinates.

### Theorem 5 (Forst-F., 2023)

Let  $K$  be a number field and  $V = AK^m \subseteq K^n$  be an  $m$ -dimensional subspace,  $1 \leq m < n$ , where  $A$  is an  $n \times m$  basis matrix for  $V$ . Let  $B$  be a full rank  $m \times m$  submatrix of  $A$ , and write  $\{\mathbf{x}_1, \dots, \mathbf{x}_m\}$  for the column vectors of the matrix  $AB^{-1}$ . Then  $\mathbf{x}_1, \dots, \mathbf{x}_m$  is another basis for  $V$  over  $K$ , which consists of  $(n - m + 1)$ -sparse vectors satisfying the following property: if  $I \subseteq \{1, \dots, m\}$  is a nonempty subset, and

$$W_I = \text{span}_K \{\mathbf{x}_i : i \in I\},$$

then

$$H(W_I) \leq H(V).$$

## Monotone basis

### Theorem 5, continuation

*In particular,*

$$\max_{1 \leq i \leq m} H(\mathbf{x}_i) \leq H(V). \quad (5)$$

*Moreover, if  $I_1 \subsetneq I_2 \subseteq \{1, \dots, m\}$ , then*

$$H(W_{I_1}) \leq H(W_{I_2}). \quad (6)$$

*Equality is attained in (6) if and only if  $\mathbf{x}_i$  is a standard basis vector for each  $i \in I_2 \setminus I_1$ .*



## Idea of proof

We outline a construction of a basis  $\mathbf{x}_1, \dots, \mathbf{x}_m$  for  $V$  with

$$H(\mathbf{x}_j) \leq H(V) \quad \forall 1 \leq j \leq m.$$

## Idea of proof

We outline a construction of a basis  $\mathbf{x}_1, \dots, \mathbf{x}_m$  for  $V$  with

$$H(\mathbf{x}_j) \leq H(V) \quad \forall 1 \leq j \leq m.$$

Since  $\dim_K V = m$ , there exists an  $(n - m) \times n$  matrix  $A$  of rank  $n - m$  with entries in  $K$  so that

$$V = \{\mathbf{x} \in K^n : A\mathbf{x} = \mathbf{0}\},$$

then  $H(A) = H(V)$  by the duality principle. Since  $\text{rk}(A) = n - m$ , there must exist standard basis vectors  $\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_m} \in K^n$  so that the matrix  $B := \begin{pmatrix} A \\ E \end{pmatrix}$  with  $E := (\mathbf{e}_{i_1} \dots \mathbf{e}_{i_m})^\top$  is in  $\text{GL}_n(K)$ .

## Idea of proof

We outline a construction of a basis  $\mathbf{x}_1, \dots, \mathbf{x}_m$  for  $V$  with

$$H(\mathbf{x}_j) \leq H(V) \quad \forall 1 \leq j \leq m.$$

Since  $\dim_K V = m$ , there exists an  $(n - m) \times n$  matrix  $A$  of rank  $n - m$  with entries in  $K$  so that

$$V = \{\mathbf{x} \in K^n : A\mathbf{x} = \mathbf{0}\},$$

then  $H(A) = H(V)$  by the duality principle. Since  $\text{rk}(A) = n - m$ , there must exist standard basis vectors  $\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_m} \in K^n$  so that the matrix  $B := \begin{pmatrix} A \\ E \end{pmatrix}$  with  $E := (\mathbf{e}_{i_1} \dots \mathbf{e}_{i_m})^\top$  is in  $\text{GL}_n(K)$ .

For each  $1 \leq j \leq m$  define the vector

$$\mathbf{x}_j = B^{-1} \mathbf{e}_{j+n-m},$$

which is the  $(j + n - m)$ -th column vector of the matrix  $B^{-1}$ . Then for every  $1 \leq j \leq m$ ,  $A\mathbf{x}_j = 0$ , i.e.  $\mathbf{x}_j \in V$ .

## Idea of proof

Further, these vectors are linearly independent since they are columns of a nonsingular matrix  $B^{-1}$ , and so they form a basis for  $V$ . We will now estimate their heights.

## Idea of proof

Further, these vectors are linearly independent since they are columns of a nonsingular matrix  $B^{-1}$ , and so they form a basis for  $V$ . We will now estimate their heights.

Let us write  $B_j$  for the  $(n-1) \times n$  submatrix of  $B$  without the  $(j+n-m)$ -th row, then  $B_j \mathbf{x}_j = \mathbf{0}$  since the  $(j+n-m)$ -th is the only row of  $B$  whose dot-product with the  $(j+n-m)$ -th column of  $B^{-1}$  is nonzero.

## Idea of proof

Further, these vectors are linearly independent since they are columns of a nonsingular matrix  $B^{-1}$ , and so they form a basis for  $V$ . We will now estimate their heights.

Let us write  $B_j$  for the  $(n-1) \times n$  submatrix of  $B$  without the  $(j+n-m)$ -th row, then  $B_j \mathbf{x}_j = \mathbf{0}$  since the  $(j+n-m)$ -th is the only row of  $B$  whose dot-product with the  $(j+n-m)$ -th column of  $B^{-1}$  is nonzero.

Using some standard height inequalities, we obtain:

$$H(\mathbf{x}_j) = H(B_j) \leq H(A) \prod_{\substack{k=1 \\ k \neq j+n-m}}^m H(\mathbf{e}_k) = H(A) = H(V),$$

since height of a standard basis vector is equal to 1. This completes the proof.

## Some remarks

- Our result does not imply Bombieri-Vaaler or Roy-Thunder, but is also not implied by them. Our bound is sharp.

## Some remarks

- Our result does not imply Bombieri-Vaaler or Roy-Thunder, but is also not implied by them. Our bound is sharp.
- Our bound is absolute with basis vectors lying over  $K$ .



## Some remarks

- Our result does not imply Bombieri-Vaaler or Roy-Thunder, but is also not implied by them. Our bound is sharp.
- Our bound is absolute with basis vectors lying over  $K$ .
- In situations when height of the subspace  $V$  is dominated by the constant depending on  $n$  and  $K$  in Bombieri-Vaaler (3) or on  $m$  in Roy-Thunder (4) our bound (5) may be better. Additionally, our bound can be preferable in some applications due to its simplicity.

## Some remarks

- Our result does not imply Bombieri-Vaaler or Roy-Thunder, but is also not implied by them. Our bound is sharp.
- Our bound is absolute with basis vectors lying over  $K$ .
- In situations when height of the subspace  $V$  is dominated by the constant depending on  $n$  and  $K$  in Bombieri-Vaaler (3) or on  $m$  in Roy-Thunder (4) our bound (5) may be better. Additionally, our bound can be preferable in some applications due to its simplicity.
- Bombieri-Vaaler and Roy-Thunder arguments rely on sophisticated tools from the geometry of numbers. Ours uses only linear algebra.

## Some remarks

- Our result does not imply Bombieri-Vaaler or Roy-Thunder, but is also not implied by them. Our bound is sharp.
- Our bound is absolute with basis vectors lying over  $K$ .
- In situations when height of the subspace  $V$  is dominated by the constant depending on  $n$  and  $K$  in Bombieri-Vaaler (3) or on  $m$  in Roy-Thunder (4) our bound (5) may be better. Additionally, our bound can be preferable in some applications due to its simplicity.
- Bombieri-Vaaler and Roy-Thunder arguments rely on sophisticated tools from the geometry of numbers. Ours uses only linear algebra.
- Our result produces a small-height basis with additional *sparse* and *monotone* properties, which can also be valuable in potential applications.

## Example

We demonstrate Theorem 5 on a simple example. Let  $K = \mathbb{Q}$ ,  $n = 4$ ,  $m = 3$ , and take

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 3 & 1 \\ 5 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}.$$

The corresponding vector of Grassmann coordinates is  $-18 \cdot (1, 1, 1, 1)$ , and hence the height of the subspace  $V = A\mathbb{Q}^3 \subset \mathbb{Q}^4$  is  $H(V) = 2$ . Take the indexing set  $I = \{1, 2, 3\}$  and consider the corresponding nonsingular minor

$$A_I = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 3 & 1 \\ 5 & 2 & 1 \end{pmatrix}.$$

## Example

Then we obtain the new basis matrix

$$X = AA_I^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}.$$

The column vectors  $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$  of  $X$  are 2-sparse and of height  $\sqrt{2}$  each. Further, the 2-dimensional subspace spanned by any two of these column vectors has height  $\sqrt{3}$ . For instance, take

$$W_{\{1\}} = \text{span}_{\mathbb{Q}}\{\mathbf{x}_1\}, \quad W_{\{1,2\}} = \text{span}_{\mathbb{Q}}\{\mathbf{x}_1, \mathbf{x}_2\},$$

and observe that

$$H(W_{\{1\}}) = \sqrt{2} < H(W_{\{1,2\}}) = \sqrt{3} < H(V) = 2.$$

## Many bases

We also obtain the following generalization:

### Theorem 6 (Forst-F., 2023)

Let  $V \subseteq K^n$  be a subspace of dimension  $m$  where  $1 \leq m < n$ . For each integer  $\ell > m$  there exists a collection of vectors

$$S(\ell) = \{\mathbf{y}_1, \dots, \mathbf{y}_\ell\} \subset V$$

with the following properties:

1. Every subset of  $m$  vectors from  $S(\ell)$  forms a basis for  $V$ ,
2. For every  $\mathbf{y}_i \in S(\ell)$ ,

$$H(\mathbf{y}_i) \leq m^{3/2} (2\ell)^{\frac{m-1}{m}} \min \left\{ H(V)^m, \gamma_K(m)^{m/2} H(V) \right\},$$

where  $\gamma_K(m)^{1/2}$  is the generalized Hermite's constant.

# Proof ingredients

The proof of Theorem 6 uses the following ingredients:

- Our Theorem 5
- A version of Bombieri-Vaaler theorem with an improved constant (due to Vaaler, 2003)
- A construction of small-norm integer sensing matrices (due to Konyagin & Sudakov, 2020)

## Proof ingredients

The proof of Theorem 6 uses the following ingredients:

- Our Theorem 5
- A version of Bombieri-Vaaler theorem with an improved constant (due to Vaaler, 2003)
- A construction of small-norm integer sensing matrices (due to Konyagin & Sudakov, 2020)

The idea is to multiply a small-height basis matrix by an integer sensing matrix with controlled coefficients: every maximal minor of such a matrix is nonsingular.



## References

- E. Bombieri, J. Vaaler. [On Siegel's lemma](#), *Invent. Math.* 73 (1983), no. 1, 11–32
- M. Forst, L. Fukshansky. [On a new absolute version of Siegel's lemma](#), to appear in *Res. Math. Sci.*, (arXiv:2308.05827)
- D. Roy, J. Thunder. [An absolute Siegel's lemma](#), *J. Reine Angew. Math.* 476 (1996), 1–26

## References

- E. Bombieri, J. Vaaler. [On Siegel's lemma](#), *Invent. Math.* 73 (1983), no. 1, 11–32
- M. Forst, L. Fukshansky. [On a new absolute version of Siegel's lemma](#), to appear in *Res. Math. Sci.*, (arXiv:2308.05827)
- D. Roy, J. Thunder. [An absolute Siegel's lemma](#), *J. Reine Angew. Math.* 476 (1996), 1–26

# Thank you!