Siegels's lemma is sharp for almost all linear systems

R. Baker and D. Masser

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2019-12
October 2019

www.math.unibas.ch

SIEGEL'S LEMMA IS SHARP FOR ALMOST ALL LINEAR SYSTEMS

ROGER BAKER† AND DAVID MASSER

ABSTRACT. The well-known Siegel Lemma gives an upper bound $cU^{m/(n-m)}$ for the size of the smallest non-zero integral solution of a linear system of $m \geq 1$ equations in $n > m$ unknowns whose coefficients are integers of absolute value at most $U \geq 1$; here $c = c(m, n) \geq 1$. In this paper we show that a better upper bound $U^{m/(n-m)}/B$ is relatively rare for large $B \geq 1$; for example there are $\theta = \theta(m, n) > 0$ and $c' = c'(m, n)$ such that this happens for at most $c'U^{mn}/B^{\theta}$ out of the roughly $(2U)^{mn}$ possible such systems.

1. INTRODUCTION

Siegel's Lemma concerns the existence of a small solution $\boldsymbol{x}$ of a system of m linear equations in n variables, $1 \leq m < n$, with integer coefficients. Let $U \geq 1$. Let

$$\sum_{j=1}^{n} a_{ij} x_j = 0 \quad (1 \leq i \leq m) \tag{1.1}$$

be a linear system such that

$$a_{ij} \in [-U, U] \cap \mathbb{Z} \quad \text{for all } i, j. \tag{1.2}$$

These had occurred in the groundbreaking work of Thue, and Siegel in 1929 (see [16] for references and an English translation) had formulated as a lemma the fact that there exists a solution $\boldsymbol{x} \in \mathbb{Z}^n$ such that

$$0 < \|\boldsymbol{x}\| := \max_{1 \leq j \leq n} |x_j| \leq 1 + (nU)^{\frac{m}{n-m}} \tag{1.3}$$

(if U is an integer, even 0).

2010 *Mathematics Subject Classification.* 11J13.

Key words and phrases. Siegel's lemma, lattices in subspaces, heights of subspaces, determinantal congruences.

†Research supported in part by Collaboration Grant 412557 from the Simons Foundation.

This lemma and its variants are key tools in diophantine approximation and transcendence theory, where they are used to construct functions with many zeroes.

Pretty soon (1.3) was improved to $\|\boldsymbol{x}\| \leq (nU)^{m/(n-m)}$ (for all real $U \geq 1$); but not until 1982 did van der Poorten and Vaaler [14] obtain $(\sqrt{n+1}U)^{m/(n-m)}$. The record so far is

$$(\sqrt{n}U)^{\frac{m}{n-m}}$$

found by Bombieri and Vaaler [4] in 1983 (see also Schmidt 1991 [12] and Bombieri and Gubler 2006 [3] as well as some remarks below). See also Beck 2017 [1] for a proof (along completely different lines) with $(70\sqrt{n}U)^{m/(n-m)}$.

It is known that hardly any more improvements are possible.

Thus Schmidt 1991 [12] (p.2) proved that the exponent $m/(n-m)$ is sharp for every m and n.

Then Bombieri and Cohen 1997 [2] (p.159) considered from a similar viewpoint certain situations where m, n and $\log U$ all grow at comparable rates (with emphasis on m close to n).

And Beck 2017 [1] (p.170) proved that the factor $\sqrt{n}$ is sharp for every m and n with $n \geq 3m/2$; more precisely the upper bound $2^{-98}e^{-4}(\sqrt{n}U)^{m/(n-m)}$ cannot hold even for $U = 1$ (provided n is sufficiently large).

It should be remarked that Beck's work is specific to the supremum norm in (1.3) and implicit in (1.2). Indeed that is the main source of difficulty. For results specific to the euclidean norm see Vaaler [13].

The above proofs all construct linear systems that are somewhat special: thus Schmidt uses coefficients a_{ij} that are products of few primes, Beck has coefficients $a_{ij} = \pm 1$, while Bombieri and Cohen go back to the problem of functions with many zeroes.

In the present paper we are interested in the totality of the

$$(2[U]+1)^{mn}$$

linear systems with (1.2). We show that for a large positive B and 'almost all' matrices

$$A = (a_{ij})_{1\leq i\leq m,\, 1\leq j\leq n} \tag{1.4}$$

with (1.2), there is no solution in integers of (1.1) with

$$0 < \|\boldsymbol{x}\| \leq \frac{U^{\frac{m}{n-m}}}{B}. \tag{1.5}$$

The precise statement of our results is as follows. We assume throughout the paper that m, n are integers with $1 \le m \le n$ ($n = m$ is allowed in Proposition 2 below) and that $U \ge 1$.

Theorem 1. *Let $n > m$, $1 \le B \le U^{m/(n-m)}$. There are at most*

$$c_1(n)\frac{U^{mn}(\log 3U)^\delta}{B^{n-m}}$$

$m \times n$ matrices A with (1.2), such that there is a solution $\boldsymbol{x} = (x_1, \ldots, x_n)$ of the system (1.1) for which (1.5) holds. Here $\delta = 0$ for $n > m+1$, $\delta = 1$ for $n = m+1$.

Theorem 2. *Let $n = m+1$, $1 \le B \le U/\log 3U$. There are at most*

$$c_2(n)\frac{U^{n^2-n}}{B}$$

$(n-1) \times n$ matrices A with (1.2), such that there is a solution $\boldsymbol{x} = (x_1, \ldots, x_n)$ of the system (1.1) for which (1.5) holds.

These imply the assertion in the abstract. Namely, if $n > m+1$ then we get $\theta = n-m$ at least for $B \le U^{m/(n-m)}$; but if $B > U^{m/(n-m)}$ then (1.5) is impossible so there are no A at all. Similarly if $n = m+1$ we get $\theta = 1$ for $B \le U/\log 3U$; but if $B > U/\log 3U$ then we can assume $B < U^m$ and we get the bound

$$c_2(n)U^{n^2-n-1}\log 3U \le c_3(n,\theta)\frac{U^{mn}}{B^\theta}$$

for any $\theta < 1/m$.

Here is a curious application of our results. In 1949 Feldman and Gelfond [7] obtained what are probably the first effective results on linear forms

$$b_1 \log\alpha_1 + b_2\log\alpha_2 + b_3\log\alpha_3 \tag{1.6}$$

in three logarithms of algebraic numbers. But they had a condition on $\boldsymbol{b} = (b_1, b_2, b_3) \ne 0$ in $\mathbb{Z}^3$: that for some fixed $\lambda > 0$ there should be $\boldsymbol{a} = (a_1, a_2, a_3)$ in $\mathbb{Z}^3$ with $0 < \|\boldsymbol{a}\| \le \|\boldsymbol{b}\|^{1/2}/(\log 3\|\boldsymbol{b}\|)^\lambda$ and $a_1b_1 + a_2b_2 + a_3b_3 = 0$ (which they use to eliminate b_3 in (1.6) and reduce to two logarithms).

Thus from Theorem 1 we see that the order of magnitude of the number of $\boldsymbol{b}$ with $\|\boldsymbol{b}\| \le U$ to which their result applies is at most $U^3/(\log 3U)^{2\lambda}$.

For the proof of Theorem 1, the work of Schmidt [11] on heights of subspaces of $\mathbb{Q}^n$ plays a key role (note that Schmidt treats K^n rather than $\mathbb{Q}^n$, where K is an algebraic number field of finite degree over $\mathbb{Q}$).

The proof of Theorem 2 is longer, which seems paradoxical because when A has maximal rank m the smallest non-zero solution is unique (up to sign) and can be written down explicitly. In fact we require two subsidiary results, Proposition 1 on the number of solutions of determinantal congruences, and Proposition 2 on the number of matrices A satisfying (1.2) for which a certain generalized determinant is small.

For any matrix A, let

$$A^{(i_1,\ldots,i_r)}\ ,\ A_{(j_1,\ldots,j_s)}$$

denote the matrix obtained by deleting rows $i_1,\ldots,i_r$, respectively columns $j_1,\ldots,j_s$, of A; similarly for $A^{(i_1,\ldots,i_r)}_{(j_1,\ldots,j_s)}$. We write $\#S$ for the number of elements in a finite set S and $\det E$ for the determinant of a square matrix E.

Proposition 1. *Let ϱ be the multiplicative function defined by*

$$\varrho(p) = 1 + \frac{2}{p},\ \ \varrho(p^k) = (k+1)^{n-2} \quad (k \geq 2)$$

for all primes p. Let $T_n(d)$ be the set of $(n-1)\times n$ matrices $A \pmod d$ for which the maximal minors $\det(A_{(j)})$ satisfy

$$\det(A_{(j)}) \equiv 0 \pmod d \quad (j = 1,\ldots,n).$$

Then for $d = 1, 2, \ldots,$

$$\#\ T_n(d) \leq \varrho(d) d^{n^2-n-2}.$$

The generalized determinant mentioned above is (for any real $m \times n$ matrix A)

$$D(A) = \sqrt{\det(AA^t)}$$

for the transpose A^t; the expression under the square root is non-negative due to the classical identity (Cauchy-Binet - see also [12] p.15)

$$\det(AA^t) = \sum \left(\det A_{(j_1,\ldots,j_s)}\right)^2 \tag{1.7}$$

where $s = n - m$ and the sum is over all (distinct) $j_1,\ldots,j_s$. It makes sense even if $n = m$ (which we allow in the next result), when it is just $|\det A|$.

In fact the result of Bombieri and Vaaler implies the upper bound $D(A)^{1/(n-m)}$ on the right of (1.3) provided A has maximal rank m. By Fischer's inequality $D(A)$ is at most the product of the euclidean lengths of the row vectors of A, and so

$$D(A) \le (\sqrt{n}U)^m. \tag{1.8}$$

This gives the required bound, which extends to rank $\tilde{m} < m$ simply by throwing away $m - \tilde{m}$ equations.

Proposition 2. *Let d be a positive integer and C a positive number such that*

$$U \ge d\,C. \tag{1.9}$$

Let A_0 be a given $m \times n$ integer matrix. The number of $m \times n$ matrices A satisfying (1.2) *together with*

$$A \equiv A_0 \pmod{d} \tag{1.10}$$

and

$$D(A) \le \frac{U^m}{C} \tag{1.11}$$

is at most

$$c_4(n)\frac{U^{mn}}{d^{mn}C^{n-m+1}}.$$

For fixed p and large k, it is reasonable to hope that the factor $(k+1)^{n-2}$ in Proposition 1 can be improved using the theory of local zeta functions (see also the end of Section 3). See Igusa [8] for the background and Meuser [10] for the rationality of the relevant zeta function. However, such an improvement does not lead to a sharpening of Theorem 2, because it is $k = 1$ that carries the most weight.

In relation to the case $m = n$, $d = 1$ of Proposition 2, there are results on the distribution of matrices with a particular value of the determinant which we mention for completeness. Duke, Rudnick, and Sarnak [6] (p.147) obtained asymptotics for the number of $n \times n$ matrices having determinant $\Delta \ne 0$; however they use a euclidean norm, so *a priori* their result implies only that the number with (1.2) lies between positive multiples of U^{n^2-n}. For $\Delta = 0$ Katznelson [9] (p.122) worked with more general norms and his result gives the asymptotics $cU^{n^2-n}\log U$ for (1.2).

We thank Arulsaravana Jeyaraj in the Computer Science Department at UCLA for correspondence (about a single linear form of a

particular shape coming from his theoretical investigations in computational number theory with consequences in computer science) which prompted the investigations of our paper.

2. Proof of Theorem 1

We require some preliminaries from the theory of heights of subspaces and generalized determinants, which we take from Schmidt's [11] and [12].

Let S be a subspace of $\mathbb{Q}^n$ of dimension m. If $m = 0$ or $m = n$ we define $H(S) = 1$. If $0 < m < n$ then

$$\Lambda = S \cap \mathbb{Z}^n$$

is a lattice in the space spanned by S over $\mathbb{R}$ (see [12] p.9) and we define

$$H(S) = \det \Lambda$$

for the determinant of the lattice. If $\Lambda = \mathbb{Z}\boldsymbol{a}_1 + \cdots + \mathbb{Z}\boldsymbol{a}_m$ and we interpret $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ as rows of a matrix A then this determinant is just $D(A)$ (see [12] p.4).

As in [12] p.10 we have

$$H(S) = H(S^\perp), \tag{2.1}$$

where

$$S^\perp = \{\boldsymbol{y} \in \mathbb{Q}^n : \boldsymbol{x} \cdot \boldsymbol{y} := x_1 y_1 + \cdots + x_n y_n = 0 \quad \forall\, \boldsymbol{x} \in S\}$$

is the orthogonal complement of S. (In Section 4 we use this notation for the orthogonal complement of a subspace of $\mathbb{R}^n$.) It will be convenient for us sometimes to use the euclidean length $|\boldsymbol{x}| = \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}$.

From a theorem of Minkowski (see [12] p.6), we can estimate the *successive minima* $\lambda_1, \ldots, \lambda_m$ of Λ, where λ_j is the least positive number such that Λ contains j linearly independent points of length at most λ_j. We have

$$\frac{2^m}{m! V_m} d(\Lambda) \le \lambda_1 \ldots \lambda_m \le \frac{2^m}{V_m} d(\Lambda) \tag{2.2}$$

where V_m is the volume of the unit ball in $\mathbb{R}^m$.

It follows that

$$H(S) \le \frac{m! V_m}{2^m} |\boldsymbol{\ell}_1| \ldots |\boldsymbol{\ell}_m| \tag{2.3}$$

for any linearly independent vectors $\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_m$ in Λ; this we see by ordering them by increasing length.

Let $\mathcal{S}(n, m, H)$ denote the set of subspaces of $\mathbb{Q}^n$ of dimension m with height at most H. Schmidt proved the following satisfying estimates for its cardinality, where henceforth in this paper the (positive) constants implicit in $\ll$ (and $\gg$) depend only on n.

Lemma 1. *For $H \geq 1$ and $1 \leq m \leq n-1$ we have*

$$H^n \ll \# \mathcal{S}(n, m, H) \ll H^n.$$

Proof. See Theorem 3 of [11] (p.440) for $K = \mathbb{Q}$. In fact we will use only the upper bound. □

Here is another cardinality estimate.

Lemma 2. *Let $R > 0$. Let $\lambda_1, \ldots, \lambda_m$ be the successive minima of the m-dimensional lattice Λ in $\mathbb{Q}^n$. Then the number of points of Λ satisfying $|\boldsymbol{x}| \leq R$ is*

$$\ll 1 + \sum_{i=1}^{m} \frac{R^i}{\lambda_1 \ldots \lambda_i}.$$

Proof. For $m = n$, see Theorem 5.4 of Widmer [15] (p.4808), noting (2.2) and that the Lipschitz parameters $M \ll 1$ and $L \ll R$. We can deduce the general case by remarking that balls centred at the origin intersect subspaces in balls of the same radius. □

Proof of Theorem 1. Let $X = U^{m/(n-m)}/B$. For $\boldsymbol{x} \in \mathbb{Z}^n$ we define $\mathcal{M}(\boldsymbol{x}, U)$ to be the number of vectors $\boldsymbol{a} = (a_1, \ldots, a_n)$ in $\mathbb{Z}^n$ satisfying

$$\|\boldsymbol{a}\| \leq U, \quad \boldsymbol{x} \cdot \boldsymbol{a} = 0.$$

If there is a solution of (1.1) satisfying (1.5) for a given matrix A, then there is a primitive solution $\boldsymbol{x}$ satisfying (1.5), that is,

$$\boldsymbol{x} \in \mathbb{Z}^n, \ \gcd(x_1, \ldots, x_n) = 1.$$

The number of $m \times n$ matrices A satisfying (1.2) associated to a particular vector $\boldsymbol{x}$ is $\mathcal{M}(\boldsymbol{x}, U)^m$. Hence it suffices to show that

$$\sum_{\substack{\boldsymbol{x} \text{ primitive} \\ \|\boldsymbol{x}\| \leq X}} \mathcal{M}(\boldsymbol{x}, U)^m \ll \frac{U^{mn} (\log 3U)^\delta}{B^{n-m}}.$$

By Lemma 2 we have

$$\mathcal{M}(\boldsymbol{x}, U) \ll 1 + \sum_{j=1}^{n-1} \frac{U^j}{\lambda_1 \dots \lambda_j}, \tag{2.4}$$

where $\lambda_1, \dots, \lambda_{n-1}$ are the successive minima of the lattice $\langle \boldsymbol{x} \rangle^\perp \cap \mathbb{Z}^n$ for $\langle \boldsymbol{x} \rangle = \mathbb{Q}\boldsymbol{x}$. Let $\boldsymbol{\ell}_1, \dots, \boldsymbol{\ell}_{n-1}$ be linearly independent vectors in $\langle \boldsymbol{x} \rangle^\perp \cap \mathbb{Z}^n$ with $|\boldsymbol{\ell}_j| = \lambda_j$. By (2.2) and (2.1)

$$\lambda_1 \dots \lambda_{n-1} \ll d(\langle x \rangle^\perp \cap \mathbb{Z}^n) = H(\langle \boldsymbol{x} \rangle^\perp) = H(\langle \boldsymbol{x} \rangle) = |\boldsymbol{x}|.$$

Let T^j be the subspace of $\langle \boldsymbol{x} \rangle^\perp$ generated by $\boldsymbol{\ell}_1, \dots, \boldsymbol{\ell}_j$; then using (2.3) we get

$$H(T^j) \ll \lambda_1 \dots \lambda_j \le (\lambda_1 \dots \lambda_{n-1})^{\frac{j}{n-1}} \le c|\boldsymbol{x}|^{j/(n-1)} \tag{2.5}$$

for c depending only on n. Thus from (2.4)

$$\mathcal{M}(\boldsymbol{x}, U) \ll 1 + \sum_{j=1}^{n-1} \frac{U^j}{H(T^j)}$$

and indeed

$$\mathcal{M}(\boldsymbol{x}, U)^m \ll 1 + \sum_{j=1}^{n-1} \frac{U^{jm}}{H(T^j)^m}. \tag{2.6}$$

From (2.5) and (2.6), we deduce that

$$\sum_{\substack{\boldsymbol{x} \text{ primitive} \\ \|\boldsymbol{x}\| \le X}} \mathcal{M}(\boldsymbol{x}, U)^m \ll X^m + \sum_{j=1}^{n-1} Y_j$$

for

$$Y_j = U^{jm} \sum_{\substack{0 < \|\boldsymbol{x}\| \le X \\ \boldsymbol{x} \in \mathbb{Z}^n}} \sum_{\substack{T \in \mathcal{S}(n, j, c|\boldsymbol{x}|^{j/(n-1)}) \\ T \subset \langle \boldsymbol{x} \rangle^\perp}} H(T)^{-m}.$$

We first verify that

$$X^m \ll \frac{U^{mn}}{B^{n-m}}, \tag{2.7}$$

that is,

$$B^{n-2m} \ll U^{mn-\frac{m^2}{n-m}}. \tag{2.8}$$

Since $m^2/(n-m) \le mn$, it suffices to prove (2.8) for $n > 2m$. Since $B < U^{m/(n-m)}$, this follows from the simple inequality

$$\frac{m(n-2m)}{n-m} \le mn - \frac{m^2}{n-m}.$$

It now suffices to show for a fixed j, $1 \le j \le n-1$ that

$$Y_j \ll \frac{U^{mn}(\log 3U)^\delta}{B^{n-m}}. \tag{2.9}$$

Since the relation $T^j \subset \langle \boldsymbol{x} \rangle^\perp$ may be rewritten as $\boldsymbol{x} \in (T^j)^\perp$, a reversal of the order of summation gives

$$Y_j \ll U^{jm} \sum_{T \in \mathcal{S}(n,j,cX^{\frac{j}{n-1}})} H(T)^{-m} \sum_{\substack{\boldsymbol{x} \in T^\perp \cap \mathbb{Z}^n \\ |\boldsymbol{x}| \le X}} 1. \tag{2.10}$$

Given T as in (2.10), let $\Lambda_T = T^\perp \cap \mathbb{Z}^n$, so that

$$d(\Lambda_T) = H(T^\perp) = H(T)$$

from (2.1). Since $X \ge 1$, it follows at once from Lemma 2 that

$$\#\{x \in \Lambda_T : |\boldsymbol{x}| \le X\} \ll \frac{X^{n-j}}{d(\Lambda_T)} + X^{n-j-1} \ll \frac{X^{n-j}}{H(T)}, \tag{2.11}$$

where in the last step we use $H(T) \ll X^{j/(n-1)} \ll X$.

From (2.10), (2.11),

$$Y_j \ll U^{jm} X^{n-j} \sum_{T \in \mathcal{S}(n,j,cX^{\frac{j}{n-1}})} H(T)^{-m-1}.$$

The contribution to the last sum from $2^k \le H(T) < 2^{k+1}$ (where $1 \le 2^k \ll X^{j/(n-1)}$) is $\ll 2^{k(n-m-1)}$ from Lemma 1. It follows that

$$Y_j \ll U^{jm} X^{n-j} (\log 3U)^\delta X^{j\left(\frac{n-m-1}{n-1}\right)}. \tag{2.12}$$

The ratio of terms with successive j on the right hand side is

$$U^m X^{-\frac{m}{n-1}} \ge U^{m-\frac{m^2}{(n-1)(n-m)}} \ge 1.$$

Hence (2.12) yields

$$Y_j \ll U^{m(n-1)} X^{1+(n-m-1)} (\log 3U)^{\delta} = U^{mn} (\log 3U)^{\delta} B^{-(n-m)}.$$

This completes the proof of Theorem 1. $\square$

3. Proof of Proposition 1

By the Chinese remainder theorem, we need only show that

$$\# T_n(p) \leq \left(1 + \frac{2}{p}\right) p^{n^2-n-2} \quad (n = 2, 3, \ldots) \tag{3.1}$$

and, including $k = 0, 1$ for convenience,

$$\# T_n(p^k) \leq (k+1)^{n-2} p^{k(n^2-n-2)} \quad (n = 2, 3, \ldots; k \geq 0) \tag{3.2}$$

where p is prime.

For (3.1) we are counting the number of $(n-1) \times n$ matrices of rank $\leq n-2$, where $n \geq 2$, over the field $\mathbb{Z}/p\mathbb{Z}$ with p elements. For $n = 2$ only the zero matrix is counted.

Now let $n \geq 3$. We divide the matrices counted as follows:

(i) A has zero first row. Since the other rows are arbitrary, there are $p^{n(n-2)}$ of these matrices.

(ii) For some i, $3 \leq i \leq n$, the rows $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-2}$ are linearly independent, while $\boldsymbol{a}_{i-1}$ is in the linear span of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-2}$. There are

$$(p^n - 1)(p^n - p) \ldots (p^n - p^{i-3})$$

possibilities for $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-2}$; then p^{i-2} possibilities for $\boldsymbol{a}_{i-1}$; and $\boldsymbol{a}_i, \ldots, \boldsymbol{a}_n$ are arbitrary. This yields

$$(p^n - 1) \ldots (p^n - p^{i-3}) p^{i-2} p^{n(n-i)}$$

matrices.

In total we obtain

$$\# T_n(p) = p^{n(n-2)} + \sum_{i=3}^{n} p^{n(n-i)} p^{i-2} \prod_{j=0}^{i-3} (p^n - p^j)$$

which is at most (ignoring subtracted terms)

$$p^{n(n-2)} + \sum_{i=3}^{n} p^{n^2-2n+i-2} = p^{n(n-2)} + p^{n^2-n-2} \, \frac{1 - p^{-(n-2)}}{1 - p^{-1}}$$

and so at most

$$p^{n^2-n-2}\left(1+\frac{1}{p-1}\right) \le p^{n^2-n-2}\left(1+\frac{2}{p}\right).$$

We prove (3.2) *for all* $k \ge 0$ by induction on n. Let $0 \le j \le k$. We shall use the notation $p^j \mid\mid (a_1, \dots, a_n)$, where a_i is in $\mathbb{Z}/p^k\mathbb{Z}$, to mean $p^j \mid a_i$ $(i = 1, \dots, n)$ and $p^{j+1} \nmid a_i$ for *some* i; except when $j = k$, when $p^k \mid\mid (a_1, \dots, a_n)$ means $p^k \mid a_i$ for $i = 1, \dots, n$. Thus for any $(a_1, \dots, a_n)$ and $k \ge 0$, there is exactly one j with $0 \le j \le k$ and $p^j \mid\mid (a_1, \dots, a_n)$.

The first step of the induction, $n = 2$, is easy, since for $A \in T_2(p^k)$ we have

$$A = (a_{11}\, a_{12})\ ,\ a_{1j} \equiv 0 \pmod{p^k}\ (j = 1, 2),$$

and $\# T_2(p^k) = 1$.

Let $n \ge 3$. For the induction step, we partition $T_n(p^k)$ into subsets $\mathcal{C}_\ell$ $(\ell = 0, 1, \dots, k)$, where $A \in \mathcal{C}_\ell$ if

$$p^\ell \mid\mid \left(\det A^{(1)}_{(1,n)}, \dots, \det A^{(n-1)}_{(1,n)}\right).$$

By the induction hypothesis applied to the transpose of $A_{(1,n)}$, for $A \in \mathcal{C}_\ell$ there are at most

$$J_\ell := p^{\ell((n-1)(n-2)-2)}(\ell+1)^{n-3}$$

possibilities $\pmod{p^\ell}$ for $A_{(1,n)}$. Modulo p^k, of course, the number of possible $A_{(1,n)}$ is

$$\le p^{(n-1)(n-2)(k-\ell)} J_\ell \le (k+1)^{n-3} p^{k(n-1)(n-2)-2\ell}. \tag{3.3}$$

For $A \in \mathcal{C}_\ell$, if we fix $A_{(1,n)}$, it will suffice to show that there are at most

$$p^{k(n-2)+\ell} \tag{3.4}$$

possibilities for the first column, and the same number of possibilities for the last column. For

$$\sum_{\ell=0}^{k} (k+1)^{n-3} p^{k(n-1)(n-2)-2\ell} p^{k(2n-4)+2\ell} = (k+1)^{n-2} p^{k(n^2-n-2)}.$$

We need only treat the first column. There is a $\det(A^{(i)}_{(1,n)})$ divisible by p^ℓ, but not $p^{\ell+1}$ (if $\ell < k$), and by p^k (if $\ell = k$). For simplicity of writing we suppose that $i = 1$.

The number of possible vectors $(a_{2,1}, \ldots, a_{n-1,1}) \pmod{p^k}$ is $p^{k(n-2)}$. Fix one of these vectors. We expand $\det A_{(n)}$ by the first column. Modulo p^k the vanishing $\det A_{(n)}$ is

$$a_{11} \det\left(A^{(1)}_{(1,n)}\right) - a_{21} \det\left(A^{(2)}_{(1,n)}\right) + \cdots + (-1)^{n-2} a_{n-1,1} \det\left(A^{(n-1)}_{(1,n)}\right).$$

Every quantity in this congruence except a_{11} has been fixed. Clearly there are at most p^ℓ possibilities for $a_{11} \pmod{p^k}$, both for $\ell < k$ and $\ell = k$. Combining this with the factor $p^{k(n-2)}$ yields the bound (3.4) and completes the induction step. This finishes the proof of Proposition 1.

We found by direct computation that

$$\#T_3(p^k) = p^{4k} + p^{4k-1} + p^{4k-2} - p^{3k-1} - p^{3k-2}.$$

This is at most $p^{4k}(1 + 2/p)$ and so

$$\#T_3(d) \le \rho_3(d) d^4$$

for ρ_3 defined as in Proposition 1 but with $\rho_3(p^k) = 1 + 2/p$ $(k \ge 2)$.

We did not succeed in computing $\#T_4(p^k)$ or in finding such things in the literature. A naive application of Igusa Theory leads to $\#T_n(p^k) \le p^{c(n)} p^{k(n^2-n-2)}$ in place of (3.2); but this would not suffice for us.

4. Distribution of matrices with small determinant

We note a bound for the number of lattice points in a compact subset E of $\mathbb{R}^n$ that is simpler than Lemma 2. Let

$$E' = \left\{ \boldsymbol{x} : \min_{\boldsymbol{y} \in E} \|\boldsymbol{x} - \boldsymbol{y}\| \le \frac{1}{2} \right\},$$

then

$$\# \, E \cap \mathbb{Z}^n \le \mu(E') \tag{4.1}$$

where $\mu(\ldots)$ is Lebesgue measure. For the left-hand side of (4.1) is

$$\sum_{\boldsymbol{a} \in E \cap \mathbb{Z}^n} \mu\left(\boldsymbol{a} + \left[-\frac{1}{2}, \frac{1}{2}\right)^n\right).$$

This sum is at most $\mu(E')$ because the $\boldsymbol{a} + [-1/2, 1/2)^n$ are pairwise disjoint subsets of E'.

It is now convenient to write $D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ for $D(A)$ when the matrix A has rows $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$, even in $\mathbb{R}^n$. We note that this is $\det(\boldsymbol{a}_i \cdot \boldsymbol{a}_{i'})_{1 \le i, i' \le m}$.

Lemma 3. *Let $1 \le m < n$. Let $d \ge 1$ and $\boldsymbol{c} \in \mathbb{R}^n$, $\|\boldsymbol{c}\| < d$. Let $W \ge 0$ and let Z, U be positive numbers with*

$$U \gg d \ , \ Z \gg Wd. \tag{4.2}$$

Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \mathbb{R}^n$ with $D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) = W$. Let E be the set of $\boldsymbol{y}$ in $\mathbb{R}^n$ with $\|d\boldsymbol{y} + \boldsymbol{c}\| \le U$ and

$$D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \ , d\boldsymbol{y} + \boldsymbol{c}) \le Z. \tag{4.3}$$

Then in the above notation

$$\mu(E') \ll \min\left(\frac{U^n}{d^n} \ , \ \frac{U^m Z^{n-m}}{d^n W^{n-m}}\right). \tag{4.4}$$

We interpret the right-hand side of (4.4) as U^n/d^n when $W = 0$.

Proof. Clearly $\mu(E') \ll U^n/d^n$. Hence we may assume that $W > 0$ and

$$\frac{Z}{W} < U.$$

For $\boldsymbol{y} \in E$ and $\boldsymbol{x} = d\boldsymbol{y} + \boldsymbol{c}$, we write

$$\boldsymbol{x} = \boldsymbol{x}_V + \boldsymbol{x}_{V^\perp} \qquad \boldsymbol{x}_V \in V, \ \boldsymbol{x}_{V^\perp} \in V^\perp$$

when $V := \mathbb{R}\boldsymbol{a}_1 + \cdots + \mathbb{R}\boldsymbol{a}_m$ has dimension m. We have

$$D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \ , d\boldsymbol{y} + \boldsymbol{c}) = D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)\, |\boldsymbol{x}_{V^\perp}| \le Z,$$

hence

$$|\boldsymbol{x}_{V^\perp}| \le \frac{Z}{W}.$$

Now take any $\boldsymbol{h}$ with $\|\boldsymbol{h}\| \le 1/2$, then decomposing $\boldsymbol{h}$ as $\boldsymbol{h}_V + \boldsymbol{h}_{V^\perp}$ as above, and recalling (4.2), we have

$$\|\boldsymbol{x}_V + d\boldsymbol{h}_V\| \ll U \ , \ \|\boldsymbol{x}_{V^\perp} + d\boldsymbol{h}_{V^\perp}\| \ll \frac{Z}{W}.$$

Since a typical point of E' has the form $\boldsymbol{x} + d\boldsymbol{h}$, it follows that

$$\mu(dE' + \boldsymbol{c}) \ll U^m \left(\frac{Z}{W}\right)^{n-m},$$

and then at once

$$\mu(E') \ll \frac{U^m}{d^n} \left(\frac{Z}{W}\right)^{n-m}. \qquad \square$$

Corollary. *Let $1 \leq m \leq n$. Let $d \geq 1$ be in $\mathbb{Z}$, let $W \geq 0$, and let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ be in $\mathbb{R}^n$ with $D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) = W$. Let C, U be positive numbers with*

$$C \gg 1\ ,\ U \gg dC. \tag{4.5}$$

Suppose further that $\|\boldsymbol{a}_i\| \leq U$ for $1 \leq i \leq m$. Let $\boldsymbol{c}_{m+1} \in \mathbb{Z}^n$. Then the number of $\boldsymbol{a}_{m+1}$ in $[-U, U]^n \cap \mathbb{Z}^n$ satisfying

$$\boldsymbol{a}_{m+1} \equiv \boldsymbol{c}_{m+1} \pmod{d}$$

and

$$D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{a}_{m+1}) \leq \frac{U^{m+1}}{C} \tag{4.6}$$

is

$$\ll d^{-n} \min\left(U^n, \frac{U^{(m+1)n-m^2}}{C^{n-m} W^{n-m}}\right).$$

Proof. We can assume $\|\boldsymbol{c}_{m+1}\| < d$. We combine Lemma 3 and (4.1), taking $Z = U^{m+1}/C$. We need only verify that $Z \gg Wd$, that is, $U^{m+1} \gg WdC$. Since $W \ll U^m$, this follows from the hypothesis (4.5). $\square$

Proof of Proposition 2. We may assume $C > (\sqrt{n})^{-m}$, because otherwise (1.11) holds for all A by (1.8) and the number of such A with (1.10) is trivially $\ll U^{mn}/d^{mn}$.

Now we use induction on m. Denote the rows of A_0 by $\boldsymbol{c}_i$ ($i = 1, \ldots, m$), with $0 \leq c_{ij} < d$. When $m = 1$, the condition $D(\boldsymbol{a}_1) \leq U/C$ implies $|a_{1j}| \leq U/C$ ($j = 1, \ldots, n$). There are

$$\ll \frac{U}{Cd} + 1 \ll \frac{U}{Cd}$$

possible a_{1j} with $a_{1j} \equiv c_{1j} \pmod{d}$, giving $\ll (U/Cd)^n$ possible vectors $\boldsymbol{a}_1$.

Suppose we have proved the result for a given $m < n$. Consider a value of W with

$$W \in \left[\frac{U^m}{C}, (\sqrt{n}\,U)^m\right].$$

We give an upper bound for N_W, the number of sets of vectors $\boldsymbol{a}_1, \dots \boldsymbol{a}_m, \boldsymbol{a}_{m+1}$ in $[-U, U]^n \cap \mathbb{Z}^n$ such that

$$\boldsymbol{a}_i \equiv \boldsymbol{c}_i \pmod{d} \quad (i = 1, \dots, m+1) \tag{4.7}$$

and

$$W \le D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m) < 2W.$$

Let us write $W = U^m/C_1$, then $1 \ll C_1 \le C$. By the induction hypothesis, the number of possibilities for $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$ is

$$\ll \frac{U^{mn}}{d^{mn} C_1^{n-m+1}}$$

since $dC_1 \le dC \le U$. Given $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$, the number of possibilities for $\boldsymbol{a}_{m+1}$ with (4.6) is

$$\ll \frac{U^{(m+1)n-m^2}}{d^n C^{n-m} W^{n-m}} = \frac{U^n C_1^{n-m}}{d^n C^{n-m}}$$

by the Corollary.

Overall for this W, the number of possibilities for $\boldsymbol{a}_1, \dots \boldsymbol{a}_{m+1}$ is

$$N_W \ll \frac{U^{(m+1)n} C_1^{-1}}{d^{(m+1)n} C^{n-m}}.$$

We now take $C_1 = 2^k$ with $1 \ll 2^k \le C$. Summing over k we obtain a total of

$$\ll \frac{U^{(m+1)n}}{d^{(m+1)n} C^{n-m}} = \frac{U^{(m+1)n}}{d^{(m+1)n} C^{n-(m+1)+1}} \tag{4.8}$$

sets of vectors $\boldsymbol{a}_1, \dots, \boldsymbol{a}_{m+1}$ with $\boldsymbol{a}_i \in [-U, U]^n \cap \mathbb{Z}^n$ $(i = 1, \dots, m+1)$, (4.7), and

$$D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m) \ge \frac{U^m}{C}$$

again by (1.8).

It remains to count those $\boldsymbol{a}_1, \dots, \boldsymbol{a}_{m+1}$ with $\boldsymbol{a}_i \in [-U, U]^n \cap \mathbb{Z}^n$ $(i = 1, \dots, m+1)$, (4.6), (4.7) and

$$D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m) < \frac{U^m}{C}.$$

We use the bounds

$$\ll \frac{U^{mn}}{d^{mn}C^{n-m+1}}\ ,\ \frac{U^n}{d^n}$$

(again by induction) for the respective number of possible $\boldsymbol{a}_1, \dots \boldsymbol{a}_m$ and possible $\boldsymbol{a}_{m+1}$. This leads to a stronger upper bound than (4.8), and the proof of the induction step is complete. This finishes the proof of Proposition 2. $\square$

5. Proof of Theorem 2

We first note a consequence of Proposition 2. Recall from (1.7) that for an $(n-1) \times n$ matrix A with rows $\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}$, we have

$$D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1})^2 = \sum_{j=1}^{n} \det A_{(j)}^2. \tag{5.1}$$

Lemma 4. *Let $n \geq 2$, $C \gg 1$, $d \in \mathbb{N}$, $U \gg dC$. Let A_0 be an $(n-1) \times n$ integer matrix. The number of $(n-1) \times n$ matrices A with entries in $[-U, U] \cap \mathbb{Z}$ and*

$$A \equiv A_0 \pmod{d}$$

such that

$$|(\det A_{(1)}, \dots, \det A_{(n)})| \leq \frac{U^{n-1}}{C}$$

is

$$\ll \frac{U^{n^2-n}}{d^{n^2-n}C^2}.$$

Proof. In view of (5.1), this is a restatement of Proposition 2 in the case $m = n - 1$. $\square$

Lemma 5. *Define the multiplicative function ϱ as in Proposition 1. Then for $x \geq 1$ we have*

$$\sum_{d \leq x} \varrho(d) \ll x.$$

Proof. Let $\mathcal{A}$ be the set of squarefull natural numbers, $\mathcal{B}$ the set of squarefree natural numbers. A natural number d can be written uniquely as

$$d = uv\ ,\ u \in \mathcal{A}\ ,\ v \in \mathcal{B}\ ,\ (u,v) = 1,$$

so that

$$\sum_{d \le x} \rho(d) = \sum_{\substack{u \le x \\ u \in \mathcal{A}}} \rho(u) \sum_{\substack{v \le x/u \\ v \in \mathcal{B} \\ (v,u)=1}} \rho(v). \tag{5.2}$$

We next prove that

$$\sum_{\substack{v \le y \\ v \in \mathcal{B}}} \rho(v) \ll y \quad (y \ge 1). \tag{5.3}$$

Let $\tau(e)$ denote the number of divisors of r and $\omega(e)$ the number of distinct primes dividing e. The sum on the left of (5.3) is at most

$$\sum_{v \le y} \prod_{p \mid v} \left(1 + \frac{2}{p}\right) \le \sum_{v \le y} \sum_{e \mid v} \frac{2^{\omega(e)}}{e} = \sum_{e \le y} \frac{2^{\omega(e)}}{e} \left[\frac{y}{e}\right] \le y \sum_{e=1}^{\infty} \frac{\tau(e)}{e^2}.$$

This proves (5.3).

By writing $u = w'^2 w''^3$ we see that

$$\sum_{u \in \mathcal{A}} u^{-3/4} \le \zeta\left(\frac{3}{2}\right)\zeta\left(\frac{9}{4}\right). \tag{5.4}$$

Since $\rho(u) = \tau(u)^{n-2}$ for $u \in \mathcal{A}$, the right-hand side of (5.2) is

$$\ll \sum_{\substack{u \le x \\ u \in \mathcal{A}}} u^{1/4} \sum_{\substack{v \le \frac{x}{u} \\ v \in \mathcal{B}}} \rho(v) \ll x \sum_{u \in \mathcal{A}} u^{-3/4}$$

using (5.3), which by (5.4) is $\ll x$. □

Proof of Theorem 2. Let $\mathcal{M}$ be the number of $(n-1) \times n$ matrices with entries in $[-U, U] \cap \mathbb{Z}$ for which the system

$$\sum_{j=1}^{n} a_{ij} x_j = 0 \quad (i = 1, \ldots, n-1) \tag{5.5}$$

has a nontrivial solution $\boldsymbol{x}$ with

$$\|\boldsymbol{x}\| < \frac{U^{n-1}}{B}.$$

The matrices A with $D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}) < U^{n-1}/B$ make a contribution to $\mathcal{M}$ of $\ll U^{n^2-n}/B^2$ by Proposition 2 with $d = 1$, which is acceptable. Let $\mathcal{M}_0$ be the contribution from A with $D(\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}) \geq U^{n-1}/B$. In particular, these A have rank $n-1$; the vector space of solutions of (5.5) has dimension 1 and is spanned by

$$\boldsymbol{x}_A := (\det A_{(1)}, -\det A_{(2)}, \dots, (-1)^{n-1} \det A_{(n)}).$$

To see that this last statement holds, we observe that

$$0 = \det(\boldsymbol{a}_i, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}) = \sum_{j=1}^{n} (-1)^{j-1} a_{ij} \det A_{(j)}$$

for $i = 1, \dots, n-1$. The integer solutions of smallest length are therefore

$$\pm \frac{1}{g_A} \boldsymbol{x}_A$$

where g_A is the greatest common divisor of $\det A_{(1)}, \dots, \det A_{(n)}$.

Thus $\mathcal{M}_0 \leq \mathcal{N}_0$ where $\mathcal{N}_0$ is the number of matrices A with $a_{ij} \in [-U, U] \cap \mathbb{Z}$ and

$$\frac{\|\boldsymbol{x}_A\|}{g_A} < \frac{U^{n-1}}{B}.$$

The contribution to $\mathcal{N}_0$ from matrices with

$$\frac{\|\boldsymbol{x}_A\|}{g_A} < U^{n-2}$$

is 0 for $n = 2$, and is

$$\ll U^{n^2-n} \frac{\log 3U}{U} \ll \frac{U^{n^2-n}}{B}$$

for $n \geq 3$, by Theorem 1. Thus it remains to consider the contribution to $\mathcal{N}_0$ from matrices with

$$U^{n-2} \leq \frac{\|\boldsymbol{x}_A\|}{g_A} < \frac{U^{n-1}}{B}. \tag{5.6}$$

Let $\mathcal{N}_0(l, k)$ be the contribution to $\mathcal{N}_0$ from matrices with

$$U^{n-1} 2^{-k} \leq |\boldsymbol{x}_A| < U^{n-1} 2^{-k+1}$$

(the change in norm will not matter) and

$$2^{l-1} \leq g_A < 2^l.$$

Here $l \geq 1$, $2^k \gg 1$ and moreover

$$U \gg 2^{l+k} \gg B$$

from (5.6).

The contribution to $\mathcal{N}_0(l,k)$ from A for which g_A takes a particular value d and A lies in a particular congruence class (mod d) is

$$\ll \frac{U^{n^2-n}}{d^{n^2-n}2^{2k}}$$

by Lemma 4. The number of congruence classes (mod d) permitted by the condition $g_A \mid \boldsymbol{x}_A$ is at most

$$\varrho(d)d^{n^2-n-2}$$

by Proposition 1. Hence

$$\mathcal{N}_0(l,k) \ll \sum_{2^{l-1}\leq d<2^l} \frac{U^{n^2-n}}{d^{n^2-n}2^{2k}}\,\varrho(d)d^{n^2-n-2} \ll \frac{U^{n^2-n}}{2^{2k+2l}} \sum_{d<2^l} \varrho(d) \ll U^{n^2-n}2^{-l-2k}$$

by Lemma 5.

We now sum over k with

$$2^{-l}U \gg 2^k \gg \max(1, 2^{-l}B),$$

obtaining

$$\sum_k \mathcal{N}_0(l,k) \ll \frac{U^{n^2-n}}{\max(1,2^{-l}B)^2}\,2^{-l}.$$

Finally we sum over l. The contribution from l with $2^l < B$ is

$$\ll \frac{U^{n^2-n}}{B^2} \sum_{2^l<B} 2^l \ll \frac{U^{n^2-n}}{B}.$$

The contribution from l with $2^l \geq B$ is

$$\ll U^{n^2-n} \sum_{2^l\geq B} 2^{-l} \ll \frac{U^{n^2-n}}{B}.$$

This completes the proof of Theorem 2. $\square$

References

[1] J. Beck, Siegel's Lemma is sharp, *A Journey Through Discrete Mathematics*, 165–206, Springer, Cham 2017.

[2] E. Bombieri and P. Cohen, Siegel's lemma, Padé approximation, and jacobians (with Appendix by U. Zannier), *Ann. Norm. Sup. Pisa* **25** (1997), 155–178.

[3] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, Cambridge 2006.

[4] E. Bombieri and J. Vaaler, On Siegel's Lemma, *Invent. Math.* **73** (1983), 11–32.

[5] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Springer, Berlin-Heidelberg-New York 1971.

[6] W. Duke, Z. Rudnick, and P. Sarnak, Density of integer points on affine homogeneous varieties, *Duke Math. J.* **71** (1993), 143–179.

[7] A.O. Gelfond and N.I. Feldman, On lower bounds for linear forms in three logarithms of algebraic numbers (in Russian), *Vestnik Moscow. Univ.* **5** (1949), 13–16.

[8] J. Igusa, *An introduction to the theory of local zeta functions*, American Mathematical Society, Providence, RI and International Press, Cambridge, MA 2000.

[9] Y. R. Katznelson, Singular matrices and a uniform bound for congruence subgroups of $SL_n(\mathbb{Z})$, *Duke Math. J.* **69** (1993), 121–136.

[10] D. Meuser, On the rationality of certain generating functions, *Math. Ann.* **256** (1981), 303–310.

[11] W. M. Schmidt, On heights of algebraic subspaces and diophantine approximations, *Ann of Math.* (2) **85** (1967), 430–472.

[12] W.M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. **1467**, Springer Berlin-Heidelberg-New York-Tokyo 1991.

[13] J. Vaaler, The best constant in Siegel's Lemma, *Monatsh. Math.* **140** (2003), 71–89.

[14] J. Vaaler and A.J. van der Poorten, Bounds for solutions of systems of linear equations, *Bull. Austral. Math. Soc.* **25** (1982), 125–132.

[15] M. Widmer, Counting primitive points of bounded height, *Trans. Amer. Math. Soc.*, **362** (2010), 4793–4829.

[16] U. Zannier (ed.), *On Some Applications of Diophantine Approximations (with Commentary by C. Fuchs and U. Zannier)*, Edizione della Normale **2**, Scuola Normale Pisa 2014.

Department of Mathematics
Brigham Young University
Provo, UT 84602, U.S.A
Email address: baker@math.byu.edu

Department of Mathematics and Computer Science
University of Basel
Spiegelgasse 1, 4051 Basel, Switzerland
Email address: david.masser@unibas.ch

LATEST PREPRINTS

No.	**Author:** *Title*
2018-01	**H. Harbrecht and P. Zaspel** *On the algebraic construction of sparse multilevel approximations of elliptic tensor product problems*
2018-02	**F. Ghiraldin and X. Lamy** *Optimal Besov differentiability for entropy solutions of the eikonal equation*
2018-03	**H. Harbrecht and M. Schmidlin** *Multilevel quadrature for elliptic problems on random domains by the coupling of FEM and BEM*
2018-04	**M. Bugeanu and H. Harbrecht** *Parametric representation of molecular surfaces*
2018-05	**A. Abdulle, M. J. Grote and O. Jecker** *Finite element heterogeneous multiscale method for Elastic Waves in Heterogeneous Media*
2018-06	**M. J. Grote and J. H. Tang** *On controllability methods for the Helmholtz equation*
2018-07	**H. Harbrecht and M. Moor** *Wavelet boundary element methods — Adaptivity and goal-oriented error estimation*
2018-08	**P. Balazs and H. Harbrecht** *Frames for the solution of operator equations in Hilbert spaces with fixed dual pairing*
2018-09	**R. Brügger, R. Croce and H. Harbrecht** *Solving a Bernoulli type free boundary problem with random diffusion*
2018-10	**J. Dölz, H. Harbrecht and M. D. Multerer** *On the best approximation of the hierarchical matrix product*
2018-11	**H. Harbrecht and P. Zaspel** *A scalable $\mathcal{H}$-matrix approach for the solution of boundary integral equations on multi-GPU clusters*
2018-12	**H. Harbrecht, N. Ilić and M. D. Multerer** *Acoustic scattering in case of random obstacles*
2018-13	**D. H. Baffet, M. J. Grote, S. Imperiale and M. Kachanovska** *Energy decay and stability of a perfectly matched layer for the wave equation*

LATEST PREPRINTS

No.	**Author:** *Title*
2018-14	**D. Baffet and M. J. Grote** *On wave splitting, source separation and echo removal with absorbing boundary conditions*
2019-01	**M. Graff, M. J. Grote, F. Nataf and F. Assous** *How to solve inverse scattering problems without knowing the source term: a three-step strategy*
2019-02	**Z. Gao and P. Habegger** *Heights in families of abelian varieties and the geometric Bogomolov conjecture*
2019-03	**M. J. Grote, F. Nataf, J. H. Tang and P.-H. Tournier** *Parallel Controllability Methods For the Helmholtz Equation*
2019-04	**G. Ciampa, G. Crippa and S. Spirito** *On smooth approximations of rough vector fields and the selection of flows*
2019-05	**M. Colombo, G. Crippa, M. Graff and L. V. Spinolo** *Recent results on the singular local limit for nonlocal conservation laws*
2019-06	**M. Colombo, G. Crippa, M. Graff and L. V. Spinolo** *On the role of numerical viscosity in the study of the local limit of nonlocal conservation laws*
2019-07	**G. Ciampa, G. Crippa and S. Spirito** *Smooth approximation is not a selection principle for the transport equation with rough vector field*
2019-08	**G. Ciampa, G. Crippa and S. Spirito** *Weak solutions obtained by the vortex method for the 2D Euler equations are Lagrangian and conserve the energy*
2019-09	**H. Harbrecht and I. Kalmykov** *Sparse grid approximation of the Riccati operator for closed loop parabolic control problems with Dirichlet boundary control*
2019-10	**J. Dölz, H. Harbrecht, S. Kurz, M. Multerer, S. Schöps, F. Wolf** *Bembel: The Fast Isogeometric Boundary Element C++ Library for Laplace, Helmholtz, and Electric Wave Equation*
2019-11	**Ch. Bürli, H. Harbrecht, P. Odermatt, S. Sayasone, N. Chitnis** *Age dependency in the transmission dynamics of the liver fluke, Opisthorchis viverrini and the effectiveness of interventions*
2019-12	**R. Baker and D. Masser** *Siegel's lemma is sharp for almost all linear systems*