Bounding linear forms on a lattice away from zero

Lenny Fukshansky
Claremont McKenna College

Arithmetic Theory of Quadratic Forms
Seoul National University
January 7 - 11, 2019

The basic problem

Let

$$L_1(x_1, \ldots, x_n), \ldots, L_t(x_1, \ldots, x_n)$$

be linear forms in n variables, and let $\Lambda \subset \mathbb{R}^n$ be a lattice.

The basic problem

Let

$$L_1(x_1, \dots, x_n), \dots, L_t(x_1, \dots, x_n)$$

be linear forms in n variables, and let $\Lambda \subset \mathbb{R}^n$ be a lattice.

Problem 1

Obtain a bound of the form

$$\min \{|L_1(\boldsymbol{x})|, \dots, |L_t(\boldsymbol{x})| : \boldsymbol{x} \in \Lambda \setminus \{\mathbf{0}\}\} \geq C$$

for some appropriate C, which may depend on the linear forms and the lattice.

The basic problem

Let

$$L_1(x_1, \dots, x_n), \dots, L_t(x_1, \dots, x_n)$$

be linear forms in n variables, and let $\Lambda \subset \mathbb{R}^n$ be a lattice.

Problem 1

Obtain a bound of the form

$$\min \{|L_1(\boldsymbol{x})|, \dots, |L_t(\boldsymbol{x})| : \boldsymbol{x} \in \Lambda \setminus \{\mathbf{0}\}\} \geq C$$

for some appropriate C, which may depend on the linear forms and the lattice.

Of course, this is not always possible, but this general problem has many interesting applications. The purpose of this talk is to describe two different directions where some variations of this question naturally come up.

A consequence of Liouville's inequality

Let K be a number field of degree d with real algebraic numbers

$$1 = \alpha_1, \alpha_2, \ldots, \alpha_d \in K$$

forming a $\mathbb{Q}$-basis for K. Let $L(x_1, \ldots, x_n) = \sum_{i=1}^{n} \alpha_i x_i$.

A consequence of Liouville's inequality

Let K be a number field of degree d with real algebraic numbers

$$1 = \alpha_1, \alpha_2, \ldots, \alpha_d \in K$$

forming a $\mathbb{Q}$-basis for K. Let $L(x_1, \ldots, x_n) = \sum_{i=1}^{n} \alpha_i x_i$.

Then for any $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^d$,

$$\|L(\boldsymbol{x})\| > \frac{1}{C|\boldsymbol{x}|^d},$$

where $\| \ \|$ stands for distance to the nearest integer, C is an explicit constant depending on d and $\alpha_1, \ldots, \alpha_d$, and $| \ |$ is the sup-norm.

A consequence of Liouville's inequality

Let K be a number field of degree d with real algebraic numbers

$$1 = \alpha_1, \alpha_2, \ldots, \alpha_d \in K$$

forming a $\mathbb{Q}$-basis for K. Let $L(x_1, \ldots, x_n) = \sum_{i=1}^{n} \alpha_i x_i$.

Then for any $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^d$,

$$\|L(\boldsymbol{x})\| > \frac{1}{C|\boldsymbol{x}|^d},$$

where $\| \ \|$ stands for distance to the nearest integer, C is an explicit constant depending on d and $\alpha_1, \ldots, \alpha_d$, and $| \ |$ is the sup-norm.

In particular, this is an instance of Problem 1 for one linear form with lower bound depending on $\boldsymbol{x}$.

Kronecker's Approximation Theorem

Let us write $\{\ \}$ for the fractional part function, and let $1, \theta_1, \ldots, \theta_t$ be $\mathbb{Q}$-linearly independent real numbers for $t \geq 1$.

Theorem 1 (L. Kronecker, 1884)

The sequence of points $(\{q\theta_1\}, \ldots, \{q\theta_t\})$ *as* q *ranges over* $\mathbb{Z}$ *is dense in the torus* $\mathbb{R}^t/\mathbb{Z}^t$.

Kronecker's Approximation Theorem

Let us write $\{\ \}$ for the fractional part function, and let $1, \theta_1, \ldots, \theta_t$ be $\mathbb{Q}$-linearly independent real numbers for $t \geq 1$.

Theorem 1 (L. Kronecker, 1884)

The sequence of points $(\{q\theta_1\}, \ldots, \{q\theta_t\})$ *as* q *ranges over* $\mathbb{Z}$ *is dense in the torus* $\mathbb{R}^t/\mathbb{Z}^t$.

In fact, for any $\varepsilon > 0$ and $(a_1, \ldots, a_t) \in \mathbb{R}^t$ there exists a $q \in \mathbb{Z}$ such that

$$\|q\theta_j - a_j\| \leq \varepsilon, \ \forall\ 1 \leq j \leq t. \tag{1}$$

Kronecker's Approximation Theorem

Let us write $\{\ \}$ for the fractional part function, and let $1, \theta_1, \ldots, \theta_t$ be $\mathbb{Q}$-linearly independent real numbers for $t \geq 1$.

Theorem 1 (L. Kronecker, 1884)

The sequence of points $(\{q\theta_1\}, \ldots, \{q\theta_t\})$ *as* q *ranges over* $\mathbb{Z}$ *is dense in the torus* $\mathbb{R}^t/\mathbb{Z}^t$.

In fact, for any $\varepsilon > 0$ and $(a_1, \ldots, a_t) \in \mathbb{R}^t$ there exists a $q \in \mathbb{Z}$ such that

$$\|q\theta_j - a_j\| \leq \varepsilon, \ \forall\ 1 \leq j \leq t. \tag{1}$$

Question 1

Can we produce an effective version of this theorem, i.e. how big does q *have to be in* (1)*?*

Kronecker's Approximation Theorem

Let us write $\{\ \}$ for the fractional part function, and let $1, \theta_1, \ldots, \theta_t$ be $\mathbb{Q}$-linearly independent real numbers for $t \geq 1$.

Theorem 1 (L. Kronecker, 1884)

The sequence of points $(\{q\theta_1\}, \ldots, \{q\theta_t\})$ *as* q *ranges over* $\mathbb{Z}$ *is dense in the torus* $\mathbb{R}^t/\mathbb{Z}^t$.

In fact, for any $\varepsilon > 0$ and $(a_1, \ldots, a_t) \in \mathbb{R}^t$ there exists a $q \in \mathbb{Z}$ such that

$$\|q\theta_j - a_j\| \leq \varepsilon, \ \forall\ 1 \leq j \leq t. \tag{1}$$

Question 1

Can we produce an effective version of this theorem, i.e. how big does q *have to be in* (1)*?*

There are several different results in the literature addressing this question. We present ours.

Effective version of Kronecker's Theorem

Theorem 2 (F., Moshchevitin, 2017)

Let $1, \theta_1, \dots, \theta_t \in \overline{\mathbb{Q}} \cap \mathbb{R}$ *be* $\mathbb{Q}$*-linearly independent with height*

$$h(\theta_j) \le H \ \forall\ 1 \le j \le t \text{ and } e = [\mathbb{Q}(\theta_1, \dots, \theta_t) : \mathbb{Q}].$$

Let $\varepsilon > 0$. *Then* $\forall\ (a_1, \dots, a_t) \in \mathbb{R}^t\ \exists\ q \in \mathbb{Z} \setminus \{0\}$ *with*

$$|q| \le \left(2^{et(e-1)}(t+1)^{3e-1}(t!)^{2e} H^{e^2(t+1)-e}\right) \varepsilon^{-e+1},$$

such that

$$\|q\theta_j - a_j\| \le \varepsilon,\ 1 \le j \le t. \tag{2}$$

Proof of Theorem 2

Liouville inequality implies that for any $\mathbf{0} \neq \boldsymbol{m} \in \mathbb{Z}^t$ with sup-norm $|\boldsymbol{m}| \leq Y$,

$$\|m_1\theta_1 + \cdots + m_t\theta_t\| \geq C_1 Y^{-e+1}$$

for an explicit constant C_1 depending on $\theta_1, \ldots, \theta_t$.

Proof of Theorem 2

Liouville inequality implies that for any $\mathbf{0} \neq \boldsymbol{m} \in \mathbb{Z}^t$ with sup-norm $|\boldsymbol{m}| \leq Y$,

$$\|m_1\theta_1 + \cdots + m_t\theta_t\| \geq C_1 Y^{-e+1}$$

for an explicit constant C_1 depending on $\theta_1, \ldots, \theta_t$.

Now a homogeneous-inhomogeneous transference principle implies that for every $(a_1, \ldots, a_t) \in \mathbb{R}^t$ there exists $q \in \mathbb{Z} \setminus \{0\}$ with $|q|$ appropriately bounded from above in terms of C_1 and Y so that

$$\max_{1 \leq j \leq t} \|q\theta_j - a_j\| \leq C_2 Y^{-1},$$

where C_2 is again explicitly computable in terms of C_1.

Proof of Theorem 2

Liouville inequality implies that for any $\mathbf{0} \neq \boldsymbol{m} \in \mathbb{Z}^t$ with sup-norm $|\boldsymbol{m}| \leq Y$,

$$\|m_1\theta_1 + \cdots + m_t\theta_t\| \geq C_1 Y^{-e+1}$$

for an explicit constant C_1 depending on $\theta_1, \ldots, \theta_t$.

Now a homogeneous-inhomogeneous transference principle implies that for every $(a_1, \ldots, a_t) \in \mathbb{R}^t$ there exists $q \in \mathbb{Z} \setminus \{0\}$ with $|q|$ appropriately bounded from above in terms of C_1 and Y so that

$$\max_{1 \leq j \leq t} \|q\theta_j - a_j\| \leq C_2 Y^{-1},$$

where C_2 is again explicitly computable in terms of C_1.

Hence for a given $\varepsilon > 0$ we simply need to compute the appropriate Y so that $C_2 Y^{-1} \leq \varepsilon$.

Density of images of linear forms

A quick corollary of Kronecker's theorem is density of the image of $\mathbb{Z}^n$ in the torus $\mathbb{R}^t/\mathbb{Z}^t$ under a collection of linear forms

$$L_1(x_1, \ldots, x_n), \ldots, L_t(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n].$$

Specifically, if 1 and coefficients of $L_1, \ldots, L_t$ are $\mathbb{Q}$-linearly independent, then $\forall\ \varepsilon > 0,\ (a_1, \ldots, a_t) \in \mathbb{R}^t\ \exists\ \boldsymbol{x} \in \mathbb{Z}^n$ such that

$$\|L_i(\boldsymbol{x}) - a_i\| < \varepsilon\ \forall\ 1 \leq i \leq t.$$

We effectively extend this result in two different ways:

Density of images of linear forms

A quick corollary of Kronecker's theorem is density of the image of $\mathbb{Z}^n$ in the torus $\mathbb{R}^t/\mathbb{Z}^t$ under a collection of linear forms

$$L_1(x_1, \ldots, x_n), \ldots, L_t(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n].$$

Specifically, if 1 and coefficients of $L_1, \ldots, L_t$ are $\mathbb{Q}$-linearly independent, then $\forall\ \varepsilon > 0,\ (a_1, \ldots, a_t) \in \mathbb{R}^t\ \exists\ \boldsymbol{x} \in \mathbb{Z}^n$ such that

$$\|L_i(\boldsymbol{x}) - a_i\| < \varepsilon\ \forall\ 1 \leq i \leq t.$$

We effectively extend this result in two different ways:

1. allow for the approximating vector $\boldsymbol{x}$ above to come from an algebraic lattice Λ, not just $\mathbb{Z}^n$,

Density of images of linear forms

A quick corollary of Kronecker's theorem is density of the image of $\mathbb{Z}^n$ in the torus $\mathbb{R}^t/\mathbb{Z}^t$ under a collection of linear forms

$$L_1(x_1, \ldots, x_n), \ldots, L_t(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n].$$

Specifically, if 1 and coefficients of $L_1, \ldots, L_t$ are $\mathbb{Q}$-linearly independent, then $\forall\ \varepsilon > 0,\ (a_1, \ldots, a_t) \in \mathbb{R}^t\ \exists\ \boldsymbol{x} \in \mathbb{Z}^n$ such that

$$\|L_i(\boldsymbol{x}) - a_i\| < \varepsilon\ \forall\ 1 \leq i \leq t.$$

We effectively extend this result in two different ways:

1. allow for the approximating vector $\boldsymbol{x}$ above to come from an algebraic lattice Λ, not just $\mathbb{Z}^n$,
2. exclude vectors from a prescribed union $\mathcal{Z}$ of projective varieties or sublattices not containing this lattice, that is we are interested in approximation vectors $\boldsymbol{x} \in \Lambda \setminus \mathcal{Z}$. This provides information on distribution of such approximating vectors.

The setup

1. The lattice: $\Lambda_K(\mathcal{M}) \subset \mathbb{R}^{wd}$ be the lattice of rank sd, which is the image of an $\mathcal{O}_K$-module $\mathcal{M} \subset K^w$ of rank s under the standard Minkowski embedding, where K is a number field of degree d.

The setup

1. The lattice: $\Lambda_K(\mathcal{M}) \subset \mathbb{R}^{wd}$ be the lattice of rank sd, which is the image of an $\mathcal{O}_K$-module $\mathcal{M} \subset K^w$ of rank s under the standard Minkowski embedding, where K is a number field of degree d.

2. The projective varieties: $\mathcal{Z}$ is a union of a finite collection of intersections of projective hypersurfaces of total degree M, or $\{\mathbf{0}\}$.

The setup

1. The lattice: $\Lambda_K(\mathcal{M}) \subset \mathbb{R}^{wd}$ be the lattice of rank sd, which is the image of an $\mathcal{O}_K$-module $\mathcal{M} \subset K^w$ of rank s under the standard Minkowski embedding, where K is a number field of degree d.

2. The projective varieties: $\mathcal{Z}$ is a union of a finite collection of intersections of projective hypersurfaces of total degree M, or $\{\mathbf{0}\}$.

3. The linear forms: Let

- $K_1 = K(\Lambda_K(\mathcal{M}))$,
- $1, b_{11}, \ldots, b_{t(wd)} \in \overline{\mathbb{Q}}$ linearly independent over K_1; let $h(B) = \max_{i,j} h(b_{ij})$, $\ell = [K(b_{11}, \ldots, b_{t(wd)}) : \mathbb{Q}]$,
- $L_i(x_1, \ldots, x_{wd})$ linear forms with coefficients $b_{i1}, \ldots, b_{i(wd)}$ for all $1 \leq i \leq t$,

The setup

1. The lattice: $\Lambda_K(\mathcal{M}) \subset \mathbb{R}^{wd}$ be the lattice of rank sd, which is the image of an $\mathcal{O}_K$-module $\mathcal{M} \subset K^w$ of rank s under the standard Minkowski embedding, where K is a number field of degree d.

2. The projective varieties: $\mathcal{Z}$ is a union of a finite collection of intersections of projective hypersurfaces of total degree M, or $\{\mathbf{0}\}$.

3. The linear forms: Let

- $K_1 = K(\Lambda_K(\mathcal{M}))$,
- $1, b_{11}, \ldots, b_{t(wd)} \in \overline{\mathbb{Q}}$ linearly independent over K_1; let $h(B) = \max_{i,j} h(b_{ij})$, $\ell = [K(b_{11}, \ldots, b_{t(wd)}) : \mathbb{Q}]$,
- $L_i(x_1, \ldots, x_{wd})$ linear forms with coefficients $b_{i1}, \ldots, b_{i(wd)}$ for all $1 \leq i \leq t$,

Define also $\mathfrak{K} = \ell^2(t+1) - \ell$ and

$$h(\mathcal{M}) = \min\left\{ h(\alpha)^{(\mathfrak{K}+1)sd-1} h(\alpha^{-1})^{\mathfrak{K}} \ : \ \alpha \in K, \alpha\mathcal{M} \subseteq \mathcal{O}_K^w \right\}.$$

Avoidance results - I

With this notation, we have our first effective version of Kronecker's theorem with avoidance conditions.

Theorem 3 (F., Moshchevitin, 2017)

Let $\boldsymbol{a} = (a_1, \dots, a_t) \in \mathbb{R}^t$ *and* $\varepsilon > 0$. *There exist* $\boldsymbol{x} \in \Lambda_K(\mathcal{M}) \setminus \mathcal{Z}$ *such that*

$$\|L_i(\boldsymbol{x}) - a_i\| < \varepsilon$$

and

$$|\boldsymbol{x}| \le \mathcal{C}_3 \left(\det \Lambda_K(\mathcal{M})\right)^{\mathfrak{K}+1} h(B)^{\mathfrak{K}} h(\mathcal{M})\ \varepsilon^{-\ell+1},$$

where $\mathcal{C}_3$ *is an explicit constant depending on* K, t, ℓ, s, M.

Avoidance results - I

With this notation, we have our first effective version of Kronecker's theorem with avoidance conditions.

Theorem 3 (F., Moshchevitin, 2017)

Let $\boldsymbol{a} = (a_1, \dots, a_t) \in \mathbb{R}^t$ *and* $\varepsilon > 0$. *There exist* $\boldsymbol{x} \in \Lambda_K(\mathcal{M}) \setminus \mathcal{Z}$ *such that*

$$\|L_i(\boldsymbol{x}) - a_i\| < \varepsilon$$

and

$$|\boldsymbol{x}| \leq \mathcal{C}_3 \left(\det \Lambda_K(\mathcal{M})\right)^{\mathfrak{K}+1} h(B)^{\mathfrak{K}} h(\mathcal{M})\ \varepsilon^{-\ell+1},$$

where $\mathcal{C}_3$ *is an explicit constant depending on* K, t, ℓ, s, M.

One special case of this theorem is when $\mathcal{Z}$ is a union of linear spaces, which means that the point $\boldsymbol{x}$ in question is in $\Lambda_K(\mathcal{M})$ but outside of a union of sublattices of smaller rank than $\Lambda_K(\mathcal{M})$. What if the rank of such sublattices is equal to the rank of $\Lambda_K(\mathcal{M})$? The next theorem addresses this situation.

Avoidance results - II

Theorem 4 (F., Moshchevitin, 2017)

Let $\boldsymbol{a} = (a_1, \dots, a_t) \in \mathbb{R}^t$ *and* $\varepsilon > 0$. *Let* $m > 0$ *and*

$$\Gamma_1, \dots, \Gamma_m \subset \Lambda_K(\mathcal{M})$$

be proper sublattices of full rank and respective determinants $\mathcal{D}_1, \dots, \mathcal{D}_m$, *and let* $\mathcal{D} = \mathcal{D}_1 \cdots \mathcal{D}_m$. *Then there exists* $\boldsymbol{x} \in \Lambda_K(\mathcal{M}) \setminus \bigcup_{i=1}^m \Gamma_i$ *such that*

$$\|L_i(\boldsymbol{x}) - a_i\| < \varepsilon$$

and

$$|\boldsymbol{x}| \le \mathcal{C}_4 \left(\sum_{i=1}^m \frac{\mathcal{D}}{\mathcal{D}_i} \right)^{\mathfrak{K}+2} (\det \Lambda_K(\mathcal{M}))^{\mathfrak{K}-m+1} h(B)^{\mathfrak{K}} h(\mathcal{M})\ \varepsilon^{-\ell+1},$$

where $\mathcal{C}_4$ *is an explicit constant depending on* K, t, ℓ, s, m.

Proof of Theorems 3 and 4

- We first construct a point $\boldsymbol{y} \in \Lambda_K(\mathcal{M})$ of controlled sup-norm, which is outside of $\mathcal{Z}$ or $\bigcup_{i=1}^{m} \Gamma_i$, respectively.

Proof of Theorems 3 and 4

- We first construct a point $\boldsymbol{y} \in \Lambda_K(\mathcal{M})$ of controlled sup-norm, which is outside of $\mathcal{Z}$ or $\bigcup_{i=1}^{m} \Gamma_i$, respectively.
  1. In the first case, we use the classical Minkowski's Successive Minima Theorem and a version of Alon's Combinatorial Nullstellensatz.

Proof of Theorems 3 and 4

- We first construct a point $\boldsymbol{y} \in \Lambda_K(\mathcal{M})$ of controlled sup-norm, which is outside of $\mathcal{Z}$ or $\bigcup_{i=1}^{m} \Gamma_i$, respectively.
  1. In the first case, we use the classical Minkowski's Successive Minima Theorem and a version of Alon's Combinatorial Nullstellensatz.
  2. In the second case we employ a recent result of Henk and Thiel on points of small norm in a lattice outside of a union of full-rank sublattices.

Proof of Theorems 3 and 4

- We first construct a point $\boldsymbol{y} \in \Lambda_K(\mathcal{M})$ of controlled sup-norm, which is outside of $\mathcal{Z}$ or $\bigcup_{i=1}^{m} \Gamma_i$, respectively.
  1. In the first case, we use the classical Minkowski's Successive Minima Theorem and a version of Alon's Combinatorial Nullstellensatz.
  2. In the second case we employ a recent result of Henk and Thiel on points of small norm in a lattice outside of a union of full-rank sublattices.
- We use $\boldsymbol{y}$ to construct an infinite sequence of points $n\boldsymbol{y}$ satisfying the above conditions, and use our Theorem 2 to obtain a value of the index n (depending on $\varepsilon > 0$) for which the required inequalities on values of linear forms are satisfied.

Proof of Theorems 3 and 4

In other words, our avoidance strategy is to follow the line $n\mathbf{y}$ until a necessary point is found.

Proof of Theorems 3 and 4

In other words, our avoidance strategy is to follow the line $n\mathbf{y}$ until a necessary point is found.

One may wish to use a similar strategy, but following a higher dimensional subspace of the ambient space in the hope of a better bound, however it is difficult to guarantee avoiding our fixed algebraic set with such strategy.

Proof of Theorems 3 and 4

In other words, our avoidance strategy is to follow the line $n\boldsymbol{y}$ until a necessary point is found.

One may wish to use a similar strategy, but following a higher dimensional subspace of the ambient space in the hope of a better bound, however it is difficult to guarantee avoiding our fixed algebraic set with such strategy.

It should be remarked that the most important feature of approximation results such as our Theorems 3 and 4 is the exponent on ε in the bounds for $|\boldsymbol{x}|$. As we show, this exponent is the same as in the corresponding bound of the effective version of Kronecker's theorem that we use.

A problem from compressed sensing

The following optimization problem is motivated by applications in *compressed sensing*, an area of applied mathematics concerned with robust reconstruction of sparse signals from few measurements.

A problem from compressed sensing

The following optimization problem is motivated by applications in *compressed sensing*, an area of applied mathematics concerned with robust reconstruction of sparse signals from few measurements.
Let

$$\mathbb{Z}_m^d := \left\{ \boldsymbol{x} \in \mathbb{Z}^d : |\{i : x_i \neq 0\}| \leq m \right\}.$$

Problem 2

Construct an $m \times d$ matrix A with $m < d$ such that

$$|A| := \max\{|a_{ij}| : 1 \leq i \leq m, 1 \leq j \leq d\} \leq C_1,$$

and for every nonzero $\boldsymbol{x} \in \mathbb{Z}_m^d$,

$$\|A\boldsymbol{x}\| \geq C_2,$$

where $C_1, C_2 > 0$, and $\| \ \|$ now stands for Euclidean norm.

Liouville's inequality again

This is an optimization problem with the goal of making d as large as possible in comparison to m.

Liouville's inequality again

This is an optimization problem with the goal of making d as large as possible in comparison to m.

Using Liouville's inequality as before, we can take $m = 1$, arbitrary d, and

$$A = \begin{pmatrix} 1 & \alpha_2 & \dots & \alpha_d \end{pmatrix},$$

with real algebraic $1 = \alpha_1, \alpha_2, \dots, \alpha_d$ forming a $\mathbb{Q}$-basis for a number field of degree d. Then for any $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^d$,

$$|A\boldsymbol{x}| > \frac{1}{C|\boldsymbol{x}|^d}$$

for an explicit constant C depending on d and $\alpha_1, \dots, \alpha_d$: here $\boldsymbol{x}$ does not even have to be sparse.

Liouville's inequality again

This is an optimization problem with the goal of making d as large as possible in comparison to m.

Using Liouville's inequality as before, we can take $m = 1$, arbitrary d, and

$$A = \begin{pmatrix} 1 & \alpha_2 & \dots & \alpha_d \end{pmatrix},$$

with real algebraic $1 = \alpha_1, \alpha_2, \dots, \alpha_d$ forming a $\mathbb{Q}$-basis for a number field of degree d. Then for any $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^d$,

$$|A\boldsymbol{x}| > \frac{1}{C|\boldsymbol{x}|^d}$$

for an explicit constant C depending on d and $\alpha_1, \dots, \alpha_d$: here $\boldsymbol{x}$ does not even have to be sparse.

However, this lower bound depends on $\boldsymbol{x}$ and d, which is not sufficiently good for applications. We want an absolute lower bound C_2 in Problem 2.

Existence of such matrices

Theorem 5 (F., Needell, Sudakov – 2017)

There exist $m \times d$ integer matrices A with $m < d$ and bounded $|A|$ such that for any nonzero $\boldsymbol{x} \in \mathbb{Z}_m^d$,

$$\|A\boldsymbol{x}\| \geq 1. \tag{3}$$

In fact, for sufficiently large m, there exist such matrices with

$$|A| = 1 \text{ and } d = 1.2938\, m,$$

and there also exist such matrices with

$$|A| = k \text{ and } d = \Omega(\sqrt{k}\, m).$$

Proof of Theorem 5

We use two powerful results of Bourgain, Vu and Wood (2010):

Let M_m be an $m \times m$ random matrix whose entries are 0 with probability $1/2$ and ± 1 with probability $1/4$ each. Then the probability that matrix M_m is singular is at most $(1/2 - o(1))^m$.

Proof of Theorem 5

We use two powerful results of Bourgain, Vu and Wood (2010):

Let M_m be an $m \times m$ random matrix whose entries are 0 with probability $1/2$ and ± 1 with probability $1/4$ each. Then the probability that matrix M_m is singular is at most $(1/2 - o(1))^m$.

If N_m is an $m \times m$ random matrix whose entries come from the set $\{-k, \cdots, k\}$ with equal probability, then the probability that N_m is singular is at most $(1/\sqrt{2k} - o(1))^m$.

Proof of Theorem 5

We use two powerful results of Bourgain, Vu and Wood (2010):

Let M_m be an $m \times m$ random matrix whose entries are 0 with probability $1/2$ and ± 1 with probability $1/4$ each. Then the probability that matrix M_m is singular is at most $(1/2 - o(1))^m$.

If N_m is an $m \times m$ random matrix whose entries come from the set $\{-k, \cdots, k\}$ with equal probability, then the probability that N_m is singular is at most $(1/\sqrt{2k} - o(1))^m$.

We combine these with the union bound to obtain an estimate on d in terms of m that guarantees positive probability of all $m \times m$ submatrices of A being non-singular.

How much bigger than m can d be?

Theorem 6 (F., Needell, Sudakov – 2017)

For any integers $m \geq 3$, $k \geq 1$ and $m \times d$ integer matrix A with $|A| = k$ satisfying (3) for all $s \leq m$, we must have

$$d \leq (2k^2 + 2)(m - 1) + 1.$$

How much bigger than m can d be?

Theorem 6 (F., Needell, Sudakov – 2017)

For any integers $m \geq 3$, $k \geq 1$ and $m \times d$ integer matrix A with $|A| = k$ satisfying (3) for all $s \leq m$, we must have

$$d \leq (2k^2 + 2)(m - 1) + 1.$$

Theorem 7 (Konyagin – 2018)

If $m \geq 2(\log k + 1)$, then

$$d < 144k(\log k + 1)m.$$

How much bigger than m can d be?

Theorem 6 (F., Needell, Sudakov – 2017)

For any integers $m \geq 3$, $k \geq 1$ and $m \times d$ integer matrix A with $|A| = k$ satisfying (3) for all $s \leq m$, we must have

$$d \leq (2k^2 + 2)(m - 1) + 1.$$

Theorem 7 (Konyagin – 2018)

If $m \geq 2(\log k + 1)$, then

$$d < 144k(\log k + 1)m.$$

Theorem 8 (Sudakov – 2018)

For sufficiently large m,

$$d = O(k\sqrt{\log k}\ m).$$

Question and example

Question 2

What is the optimal upper bound on d in terms of k and m? In particular, is it true that $d = O(km)$?

Question and example

Question 2

What is the optimal upper bound on d in terms of k and m? In particular, is it true that $d = O(km)$?

Here is a low-dimensional example.

Example 1

Let $m = 3$, $d = 6$, $k = 1$, and define a 3×6 matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & -1 & -1 \\ 1 & 0 & 1 & -1 & 0 & -1 \end{pmatrix}.$$

This matrix has $|A| = 1$ and any three of its columns are linearly independent. Then for $s \leq 3$ and any $\boldsymbol{x} \in \mathbb{Z}_s^6$, $\|A\boldsymbol{x}\| \geq 1$.

Algebraic matrices

While our Theorem 5 gives the image vector $A\boldsymbol{x}$ bounded away from 0, many of its coordinates may still be 0. A variation of our original Problem 1 would ask for a matrix A with $A\boldsymbol{x}$ bounded away from 0 **and** nonzero coordinates.

Algebraic matrices

While our Theorem 5 gives the image vector $A\boldsymbol{x}$ bounded away from 0, many of its coordinates may still be 0. A variation of our original Problem 1 would ask for a matrix A with $A\boldsymbol{x}$ bounded away from 0 **and** nonzero coordinates.

Corollary 9 (F., Needell, Sudakov – 2017)

Let B be the $d \times m$-transpose of a matrix satisfying (3) as guaranteed by Theorem 5. Let θ be an algebraic integer of degree m, and let $\theta = \theta_1, \theta_2, \ldots, \theta_m$ be its algebraic conjugates. For each $1 \leq i \leq m$, let $\boldsymbol{\theta}_i = (1 \ \theta_i \ \ldots \theta_i^{m-1})^\top$, compute the $d \times m$ matrix

$$B\left(\boldsymbol{\theta}_1 \quad \ldots \quad \boldsymbol{\theta}_m\right),$$

and let A be its transpose. Then $|A| = O\left(|B|m\right)$, for any $\boldsymbol{x} \in \mathbb{Z}_s^d$, $0 < s \leq m$, $\|A\boldsymbol{x}\| \geq \sqrt{m}$ and the vector $A\boldsymbol{x}$ has **all nonzero coordinates**.

Proof of Corollary 9

We use the AM-GM inequality:

$$\begin{aligned}\frac{1}{m}\|A\boldsymbol{x}\|^2 &= \frac{1}{m}\sum_{i=1}^{m}|(B\boldsymbol{\theta}_i)\boldsymbol{x}|^2 \\ &\geq \left(\prod_{i=1}^{m}|(B\boldsymbol{\theta}_i)\boldsymbol{x}|^2\right)^{1/m} \\ &= |\mathbb{N}_K((B\boldsymbol{\theta}_1)\boldsymbol{x})|^{2/m},\end{aligned}$$

where $\mathbb{N}_K$ is the field norm, which is $\geq$ since $(B\boldsymbol{\theta}_1)\boldsymbol{x}$ is an algebraic integer.

Proof of Corollary 9

We use the AM-GM inequality:

$$\begin{aligned}\frac{1}{m}\|A\boldsymbol{x}\|^2 &= \frac{1}{m}\sum_{i=1}^{m}|(B\boldsymbol{\theta}_i)\boldsymbol{x}|^2 \\ &\geq \left(\prod_{i=1}^{m}|(B\boldsymbol{\theta}_i)\boldsymbol{x}|^2\right)^{1/m} \\ &= |\mathbb{N}_K((B\boldsymbol{\theta}_1)\boldsymbol{x})|^{2/m},\end{aligned}$$

where $\mathbb{N}_K$ is the field norm, which is $\geq$ since $(B\boldsymbol{\theta}_1)\boldsymbol{x}$ is an algebraic integer.

Since $(B\boldsymbol{\theta}_1)\boldsymbol{x} \neq 0$, its algebraic conjugates, which are the rest of the coordinates of the vector $A\boldsymbol{x}$ must all be nonzero.

Algebraic matrix example

Let $m = 3$, $d = 6$, and take $K = \mathbb{Q}(\theta)$, where $\theta = 2^{1/3}$, then

$$\boldsymbol{\theta} = \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix}.$$

Algebraic matrix example

Let $m = 3$, $d = 6$, and take $K = \mathbb{Q}(\theta)$, where $\theta = 2^{1/3}$, then

$$\boldsymbol{\theta} = \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix}.$$

Let $k = 1$ and take B to be the transpose of the matrix from Example 1, i.e.

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \\ 1 & -1 & -1 \end{pmatrix}.$$

Algebraic matrix example

The number field K has three embeddings into $\mathbb{C}$, given by

$$\theta \mapsto \theta, \ \theta \mapsto \xi\theta, \ \theta \mapsto \xi^2\theta,$$

where $\xi = e^{\frac{2\pi i}{3}}$ is a third root of unity, i.e. θ is mapped to roots of its minimal polynomial by injective field homomorphisms that fix $\mathbb{Q}$.

Algebraic matrix example

The number field K has three embeddings into $\mathbb{C}$, given by

$$\theta \mapsto \theta,\ \theta \mapsto \xi\theta,\ \theta \mapsto \xi^2\theta,$$

where $\xi = e^{\frac{2\pi i}{3}}$ is a third root of unity, i.e. θ is mapped to roots of its minimal polynomial by injective field homomorphisms that fix $\mathbb{Q}$.

Hence we get the following 3×6 matrix:

$$A = \begin{pmatrix} 1+\theta+\theta^2 & 1+\theta & 1+\theta^2 & 1-\theta^2 & 1-\theta & 1-\theta-\theta^2 \\ 1+\xi\theta+\xi^2\theta^2 & 1+\xi\theta & 1+\xi^2\theta^2 & 1-\xi^2\theta^2 & 1-\xi\theta & 1-\xi\theta-\xi^2\theta^2 \\ 1+\xi^2\theta+\xi\theta^2 & 1+\xi^2\theta & 1+\xi\theta^2 & 1-\xi\theta^2 & 1-\xi^2\theta & 1-\xi^2\theta-\xi\theta^2 \end{pmatrix}$$

with $|A| \leq 3\sqrt[3]{2}$ and $\|A\boldsymbol{x}\| \geq \sqrt{3}$ for every $\boldsymbol{x} \in \mathbb{Z}_3^6$.

Upper bound on $\|A\boldsymbol{x}\|$

While these results show the existence of matrices A such that $\|A\boldsymbol{x}\|$ is bounded away from $\mathbf{0}$ on sparse vectors, it is also clear that for any $m \times d$ matrix A there exist sparse vectors with $\|A\boldsymbol{x}\|$ not too large: for instance, if $\boldsymbol{x} \in \mathbb{Z}^d$ is a standard basis vector, then

$$\|A\boldsymbol{x}\| \leq \sqrt{m}\ |A|. \tag{4}$$

Upper bound on $\|A\boldsymbol{x}\|$

While these results show the existence of matrices A such that $\|A\boldsymbol{x}\|$ is bounded away from $\mathbf{0}$ on sparse vectors, it is also clear that for any $m \times d$ matrix A there exist sparse vectors with $\|A\boldsymbol{x}\|$ not too large: for instance, if $\boldsymbol{x} \in \mathbb{Z}^d$ is a standard basis vector, then

$$\|A\boldsymbol{x}\| \leq \sqrt{m}\ |A|. \tag{4}$$

We prove a determinantal upper bound on $\|A\boldsymbol{x}\|$ in the spirit of Minkowski's Geometry of Numbers, which is often better.

Theorem 10 (F., Needell, Sudakov – 2017)

Let A be an $m \times d$ real matrix of rank $m \leq d$, and let A' be the $d \times m$ real matrix so that AA' is the $m \times m$ identity matrix. There exists a nonzero point $\boldsymbol{x} \in \mathbb{Z}_m^d$ such that

$$\|A\boldsymbol{x}\| \leq \sqrt{m}\ \left|\det\left((A')^\top A'\right)\right|^{-1/2m}. \tag{5}$$

Upper bound examples

Example 2

Let $d = 5$, $m = 3$, and let

$$A = \begin{pmatrix} 15 & 15 & 4 & 13 & 15 \\ 2 & -1 & -15 & 2 & -13 \\ -13 & 2 & 1 & -15 & 4 \end{pmatrix},$$

then

$$A' = \begin{pmatrix} 3392/3905 & 23/355 & 3021/3905 \\ -1949/2130 & 3/710 & -1697/2130 \\ -6409/9372 & -19/284 & -5647/9372 \\ -6407/9372 & -17/284 & -6353/9372 \\ 13869/15620 & 1/1420 & 12047/15620 \end{pmatrix},$$

and so the bound of (5) is 8.375..., which is better than 25.980..., the bound given by (4).

Upper bound examples

Example 3

Let $d = 6$, $m = 3$, and let

$$A = \begin{pmatrix} 50000 & 20 & 40 & 3 & -50000 & 30 \\ -1 & -50000 & 20 & 40 & 4 & -50000 \\ -50000 & -1 & -50000 & -50000 & 20 & 40 \end{pmatrix},$$

then the bound of (5) is 7651.170... and (4) is 86602.540...

Upper bound examples

Example 3

Let $d = 6$, $m = 3$, and let

$$A = \begin{pmatrix} 50000 & 20 & 40 & 3 & -50000 & 30 \\ -1 & -50000 & 20 & 40 & 4 & -50000 \\ -50000 & -1 & -50000 & -50000 & 20 & 40 \end{pmatrix},$$

then the bound of (5) is 7651.170... and (4) is 86602.540...
Let $d = 8$, $m = 4$, and let

$$A = \begin{pmatrix} 6 & 13 & 13 & 11 & 6 & 12 & 11 & 10 \\ 7 & 12 & 6 & 13 & 7 & 11 & 11 & 9 \\ 8 & 11 & 12 & 9 & 12 & 12 & 12 & 11 \\ 13 & 10 & 7 & 8 & 13 & 13 & 13 & 13 \end{pmatrix},$$

then the bound of (5) is 2.412... and (4) is 26.

Sparse Geometry of Numbers

Let us now sketch the strategy of proof of Theorem 10. For this, we develop sparse analogues of some classical theorems in Minkowski's Geometry of Numbers. We start with a result of J. D. Vaaler (1979).

Sparse Geometry of Numbers

Let us now sketch the strategy of proof of Theorem 10. For this, we develop sparse analogues of some classical theorems in Minkowski's Geometry of Numbers. We start with a result of J. D. Vaaler (1979).

Lemma 11 (Vaaler's Cube Slicing Inequality)

Let $\mathcal{C}^d(1)$ be a cube of sidelength 1 centered at the origin in $\mathbb{R}^d$, i.e.

$$\mathcal{C}^d(1) = \{\boldsymbol{x} \in \mathbb{R}^d : |x_i| \leq 1/2 \ \forall \ 1 \leq i \leq d\}.$$

Let V be an m-dimensional subspace of $\mathbb{R}^d$, $m \leq d$. Then the m-dimensional volume of the section $\mathcal{C}_d(1) \cap V$ is

$$\mathrm{Vol}_m(\mathcal{C}_d(1) \cap V) \geq 1.$$

Sparse Geometry of Numbers

We can use Vaaler's lemma to prove a sparse version of Minkowski's Convex Body Theorem for parallelepipeds.

Proposition 12 (F., Needell, Sudakov – 2017)

Let $m \leq d$ be positive integers. Let $A \in \mathrm{GL}_d(\mathbb{R})$, and let $P_A = A\mathcal{C}^d(1)$. Assume that for some $I \subset [d]$ with $|I| = m$,

$$\sqrt{|\det(A_I^\top A_I)|} \geq 2^m. \tag{6}$$

Then P_A contains a nonzero point of $\mathbb{Z}_m^d$.

Here $[d] := \{1, \ldots, d\}$ and A_I is the $d \times m$ submatrix of A with columns indexed by elements of I.

Sparse Geometry of Numbers

This implies a sparse version of Minkowski's Linear Forms Theorem.

Theorem 13 (F., Needell, Sudakov – 2017)

Let $m \leq d$ be positive integers and $B \in \mathrm{GL}_d(\mathbb{R})$. For each $1 \leq i \leq d$, let $L_i(X_1, \ldots, X_d) = \sum_{j=1}^{d} b_{ij} X_j$ be the linear form with entries of the i-th row of B for its coefficients. Let $c_1, \ldots, c_d$ be positive real numbers such that for some $I = \{1 \leq j_1 < \cdots < j_m \leq d\} \subset [d]$,

$$c_{j_1} \cdots c_{j_m} \geq \left| \det \left((B^{-1})_I^{\top} (B^{-1})_I \right) \right|^{-1/2}. \tag{7}$$

Then there exists a nonzero point $\boldsymbol{x} \in \mathbb{Z}_m^d$ such that

$$|L_{j_i}(\boldsymbol{x})| \leq c_{j_i} \ \forall \ 1 \leq i \leq m. \tag{8}$$

Sparse Geometry of Numbers

Taking $I = \{1, \ldots, m\}$ and

$$c_i = \left|\det\left((B^{-1})_I^\top (B^{-1})_I\right)\right|^{-1/2m}$$

for each $1 \leq i \leq m$ in Theorem 13 implies –

Corollary 14 (F., Needell, Sudakov – 2017)

Let A be an $m \times d$ real matrix of rank $m \leq d$. Let $B \in \mathrm{GL}_d(\mathbb{R})$ be a matrix whose first m rows are the rows of A. Let $I = \{1, \ldots, m\}$. Then there exists a nonzero point $\boldsymbol{x} \in \mathbb{Z}_m^d$ such that

$$\|A\boldsymbol{x}\| \leq \sqrt{m}\left|\det\left((B^{-1})_I^\top (B^{-1})_I\right)\right|^{-1/2m}.$$

Sparse Geometry of Numbers

Taking $I = \{1, \ldots, m\}$ and

$$c_i = \left|\det\left((B^{-1})_I^\top (B^{-1})_I\right)\right|^{-1/2m}$$

for each $1 \le i \le m$ in Theorem 13 implies –

Corollary 14 (F., Needell, Sudakov – 2017)

Let A be an $m \times d$ real matrix of rank $m \le d$. Let $B \in \mathrm{GL}_d(\mathbb{R})$ be a matrix whose first m rows are the rows of A. Let $I = \{1, \ldots, m\}$. Then there exists a nonzero point $\boldsymbol{x} \in \mathbb{Z}_m^d$ such that

$$\|A\boldsymbol{x}\| \le \sqrt{m}\left|\det\left((B^{-1})_I^\top (B^{-1})_I\right)\right|^{-1/2m}.$$

Theorem 10 follows immediately.

References

L. Fukshansky and N. Moshchevitin, *On an effective variation of Kronecker's approximation theorem avoiding algebraic sets*, Proceedings of the American Mathematical Society, vol. 146 no. 10 (2018), pg. 4151–4163.

L. Fukshansky, D. Needell, B. Sudakov, *An algebraic perspective on integer sparse recovery*, Applied Mathematics and Computation, vol. 340 (2019), pg. 31–42

Preprints are available at:

`http://math.cmc.edu/lenny/research.html`

References

L. Fukshansky and N. Moshchevitin, *On an effective variation of Kronecker's approximation theorem avoiding algebraic sets*, Proceedings of the American Mathematical Society, vol. 146 no. 10 (2018), pg. 4151–4163.

L. Fukshansky, D. Needell, B. Sudakov, *An algebraic perspective on integer sparse recovery*, Applied Mathematics and Computation, vol. 340 (2019), pg. 31–42

Preprints are available at:

`http://math.cmc.edu/lenny/research.html`

Thank you!