Searching for rational points on varieties over global fields

Lenny Fukshansky
Claremont McKenna College

CCMS Colloquium
February 26, 2014

Hilbert's Tenth Problem

Consider a system of M Diophantine equations in N variables, i.e.

$$\left.\begin{array}{l} P_1(X_1,\ldots,X_N)=0 \\ \vdots \\ P_M(X_1,\ldots,X_N)=0 \end{array}\right\} \tag{1}$$

where $P_1,\ldots,P_M$ are polynomials with integer coefficients.

Hilbert's Tenth Problem

Consider a system of M Diophantine equations in N variables, i.e.

$$\left.\begin{array}{l} P_1(X_1,\dots,X_N)=0 \\ \vdots \\ P_M(X_1,\dots,X_N)=0 \end{array}\right\} \qquad (1)$$

where $P_1,\dots,P_M$ are polynomials with integer coefficients.

Question 1

Does this system have a nontrivial integral solution?

Hilbert's Tenth Problem

Consider a system of M Diophantine equations in N variables, i.e.

$$\left.\begin{array}{l} P_1(X_1, \ldots, X_N) = 0 \\ \vdots \\ P_M(X_1, \ldots, X_N) = 0 \end{array}\right\} \qquad (1)$$

where $P_1, \ldots, P_M$ are polynomials with integer coefficients.

Question 1

Does this system have a nontrivial integral solution?

Question 2

Assuming it does, how do we find such a solution?

Hilbert's Tenth Problem

Consider a system of M Diophantine equations in N variables, i.e.

$$\left.\begin{array}{l} P_1(X_1,\dots,X_N)=0 \\ \vdots \\ P_M(X_1,\dots,X_N)=0 \end{array}\right\} \tag{1}$$

where $P_1,\dots,P_M$ are polynomials with integer coefficients.

Question 1

Does this system have a nontrivial integral solution?

Question 2

Assuming it does, how do we find such a solution?

The famous result of **Y. Matijasevich** (1970; building on the previous work by **M. Davis, H. Putnam** and **J. Robinson** - 1961) implies that Question 1 in general is undecidable.

But what if . . .

Suppose that we could prove a theorem of the following kind:

But what if ...

Suppose that we could prove a theorem of the following kind:

If the system (1) *has a nontrivial solution vector* $\mathbf{x} \in \mathbb{Z}^N$*, then there exists such a solution vector with*

$$|\mathbf{x}| := \max_{1 \leq i \leq N} |x_i| \leq B \tag{2}$$

for some explicit constant $B = B(P_1, \dots, P_M)$*.*

But what if ...

Suppose that we could prove a theorem of the following kind:

If the system (1) *has a nontrivial solution vector* $\mathbf{x} \in \mathbb{Z}^N$, *then there exists such a solution vector with*

$$|\mathbf{x}| := \max_{1 \leq i \leq N} |x_i| \leq B \tag{2}$$

for some explicit constant $B = B(P_1, \dots, P_M)$.

Then to answer Question 1, it would be enough to check whether any of the vectors in the finite set

$$\left\{ \mathbf{x} \in \mathbb{Z}^N : \max_{1 \leq i \leq N} |x_i| \leq B \right\}$$

is a solution to (1), reducing it to a finite search algorithm.

Search bounds

Moreover, if Question 1 is answered affirmatively, then this finite search algorithm simultaneously provides an answer to Question 2.

Search bounds

Moreover, if Question 1 is answered affirmatively, then this finite search algorithm simultaneously provides an answer to Question 2.

We will refer to a constant B satisfying (2) as an explicit **search bound** (with respect to $| \ |$) for the polynomial system $P_1, \dots, P_M$. Hence Questions 1 and 2 can be replaced by -

Search bounds

Moreover, if Question 1 is answered affirmatively, then this finite search algorithm simultaneously provides an answer to Question 2.

We will refer to a constant B satisfying (2) as an explicit **search bound** (with respect to $|\ |$) for the polynomial system $P_1, \dots, P_M$. Hence Questions 1 and 2 can be replaced by -

Question 3

Assuming the polynomial system $P_1, \dots, P_M$ has a nontrivial integral solution, can we find an explicit search bound?

Well, can we?

Existence of search bounds for general polynomial systems like (1) would contradict Matijasevich's theorem, and hence search bounds in general cannot exist.

Well, can we?

Existence of search bounds for general polynomial systems like (1) would contradict Matijasevich's theorem, and hence search bounds in general cannot exist.

Moreover, it was proved by **J. P. Jones** (1980) that the question whether a single Diophantine equation of degree four or larger has a solution in positive integers is already undecidable.

Well, can we?

Existence of search bounds for general polynomial systems like (1) would contradict Matijasevich's theorem, and hence search bounds in general cannot exist.

Moreover, it was proved by **J. P. Jones** (1980) that the question whether a single Diophantine equation of degree four or larger has a solution in positive integers is already undecidable.

This suggests that search bounds for equations of degree ≥ 4 may be out of reach, and relatively little is known even for degree 3 (although some work has been done, especially in the recent years). There is however a wealth of results for degree 1 and 2, which will be the main focus of this talk.

The homogeneous linear case

Let

$$A\mathbf{x} = \mathbf{0} \tag{3}$$

be an $M \times N$ linear system of rank $M < N$ with integer entries.

The homogeneous linear case

Let

$$A\mathbf{x} = \mathbf{0} \tag{3}$$

be an $M \times N$ linear system of rank $M < N$ with integer entries. As above, we will write

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

for the **height** of a vector $\mathbf{x} \in \mathbb{Z}^N$. Similarly, we define the **height** of the coefficient matrix $A = (a_{ij})_{1 \leq i \leq M, 1 \leq j \leq N}$ by

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

The homogeneous linear case

Let

$$A\mathbf{x} = \mathbf{0} \tag{3}$$

be an $M \times N$ linear system of rank $M < N$ with integer entries. As above, we will write

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

for the **height** of a vector $\mathbf{x} \in \mathbb{Z}^N$. Similarly, we define the **height** of the coefficient matrix $A = (a_{ij})_{1 \leq i \leq M, 1 \leq j \leq N}$ by

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

Question 4

What is the smallest height of a nontrivial integral solution to (3)?

The homogeneous linear case

Let

$$A\mathbf{x} = \mathbf{0} \tag{3}$$

be an $M \times N$ linear system of rank $M < N$ with integer entries. As above, we will write

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

for the **height** of a vector $\mathbf{x} \in \mathbb{Z}^N$. Similarly, we define the **height** of the coefficient matrix $A = (a_{ij})_{1 \leq i \leq M, 1 \leq j \leq N}$ by

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

Question 4

What is the smallest height of a nontrivial integral solution to (3)?

It is natural to expect that there must exist a solution vector $\mathbf{x}$ with $|\mathbf{x}|$ not too large, compared to $|A|$.

Siegel's lemma

In 1929 **Carl Ludwig Siegel** proved that there exists a non-trivial integral solution $\mathbf{x}$ to (3) with

$$|\mathbf{x}| \leq (1 + N|A|)^{\frac{M}{N-M}}. \tag{4}$$

Siegel's lemma

In 1929 **Carl Ludwig Siegel** proved that there exists a non-trivial integral solution $\mathbf{x}$ to (3) with

$$|\mathbf{x}| \leq (1 + N|A|)^{\frac{M}{N-M}}. \tag{4}$$

The proof uses Dirichlet box principle. In fact, a similar result was at least informally observed by **Axel Thue** as early as 1909. This result is best possible in the sense that the exponent $\frac{M}{N-M}$ in (4) cannot be improved.

Siegel's lemma

In 1929 **Carl Ludwig Siegel** proved that there exists a non-trivial integral solution $\mathbf{x}$ to (3) with

$$|\mathbf{x}| \leq (1 + N|A|)^{\frac{M}{N-M}}. \tag{4}$$

The proof uses Dirichlet box principle. In fact, a similar result was at least informally observed by **Axel Thue** as early as 1909. This result is best possible in the sense that the exponent $\frac{M}{N-M}$ in (4) cannot be improved.

Results of this sort are known under the general name of **Siegel's lemma**, and are very important in transcendental number theory.

Siegel's lemma

In 1929 **Carl Ludwig Siegel** proved that there exists a non-trivial integral solution $\mathbf{x}$ to (3) with

$$|\mathbf{x}| \leq (1 + N|A|)^{\frac{M}{N-M}}. \tag{4}$$

The proof uses Dirichlet box principle. In fact, a similar result was at least informally observed by **Axel Thue** as early as 1909. This result is best possible in the sense that the exponent $\frac{M}{N-M}$ in (4) cannot be improved.
Results of this sort are known under the general name of **Siegel's lemma**, and are very important in transcendental number theory. In the recent years Siegel's lemma was studied by many authors in Diophantine approximations for its own sake as well: as the simplest case of an **effective** existence result for rational points on varieties.

The inhomogeneous linear case

Instead of (3), consider now an inhomogeneous $M \times N$ linear system

$$A\mathbf{x} = \mathbf{b}, \tag{5}$$

where $\mathbf{b} \in \mathbb{Z}^M$.

The inhomogeneous linear case

Instead of (3), consider now an inhomogeneous $M \times N$ linear system

$$Ax = \mathbf{b}, \tag{5}$$

where $\mathbf{b} \in \mathbb{Z}^M$. Define

$$\mathcal{D}(A) := \gcd\{\det C : C \text{ is an } M \times M \text{ minor of } A\}.$$

The inhomogeneous linear case

Instead of (3), consider now an inhomogeneous $M \times N$ linear system

$$A\mathbf{x} = \mathbf{b}, \tag{5}$$

where $\mathbf{b} \in \mathbb{Z}^M$. Define

$$\mathcal{D}(A) := \gcd\{\det C : C \text{ is an } M \times M \text{ minor of } A\}.$$

Then a classical result of **I. Heger** (1856) states that (5) has a solution in $\mathbb{Z}^N$ if and only if

$$\mathcal{D}(A) = \mathcal{D}((A\ \mathbf{b})).$$

The inhomogeneous linear case

Instead of (3), consider now an inhomogeneous $M \times N$ linear system

$$A\mathbf{x} = \mathbf{b}, \tag{5}$$

where $\mathbf{b} \in \mathbb{Z}^M$. Define

$$\mathcal{D}(A) := \gcd\{\det C : C \text{ is an } M \times M \text{ minor of } A\}.$$

Then a classical result of **I. Heger** (1856) states that (5) has a solution in $\mathbb{Z}^N$ if and only if

$$\mathcal{D}(A) = \mathcal{D}((A\ \mathbf{b})).$$

When this is the case, a result of **Borosh, Flahive, Rubin,** and **Treybig** (1989) states that there exists such a solution $\mathbf{x} \in \mathbb{Z}^N$ with

$$|\mathbf{x}| \leq \max\{|\det C| : C = M \times M \text{ minor of } (A\ \mathbf{b})\}.$$

One quadratic form

Let

$$F(\mathbf{X}, \mathbf{Y}) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i Y_j$$

be a symmetric bilinear form in $2N$ variables, $N \geq 2$, with integer coefficients, and let

$$F(\mathbf{X}) = F(\mathbf{X}, \mathbf{X})$$

be the associated quadratic form.

One quadratic form

Let

$$F(\mathbf{X},\mathbf{Y}) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i Y_j$$

be a symmetric bilinear form in $2N$ variables, $N \geq 2$, with integer coefficients, and let

$$F(\mathbf{X}) = F(\mathbf{X},\mathbf{X})$$

be the associated quadratic form. A famous result of **J. W. S. Cassels** (1955) states that if F has a nontrivial rational zero, then there exists $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^N$ such that $F(\mathbf{x}) = 0$ and

$$|\mathbf{x}| \ll_N |F|^{\frac{N-1}{2}}, \tag{6}$$

where $|F| := \max_{1 \leq i,j \leq N} |f_{ij}|$, and the constant in the upper bound is explicit. The exponent $\frac{N-1}{2}$ in the upper bound is best possible.

The inhomogeneous quadratic case

Now assume that an inhomogeneous quadratic equation in $N \geq 3$ variables with integer coefficients

$$\sum_{i=1}^{N}\sum_{j=1}^{N} f_{ij}X_iX_j + \sum_{i=1}^{N} f_{i0}X_i + f_{00} = 0$$

has an integral solution.

The inhomogeneous quadratic case

Now assume that an inhomogeneous quadratic equation in $N \geq 3$ variables with integer coefficients

$$\sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i X_j + \sum_{i=1}^{N} f_{i0} X_i + f_{00} = 0$$

has an integral solution.
R. Dietmann (2003), building on previous work by **Siegel** (1972) and **Kornhauser** (1990), showed that in this case there exists a solution $\mathbf{x} \in \mathbb{Z}^N$ with

$$|\mathbf{x}| \ll_N |F|^{p(N)}, \tag{7}$$

where $p(N)$ is a linear polynomial ($\approx 5N + C$).

The inhomogeneous quadratic case

Now assume that an inhomogeneous quadratic equation in $N \geq 3$ variables with integer coefficients

$$\sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i X_j + \sum_{i=1}^{N} f_{i0} X_i + f_{00} = 0$$

has an integral solution.
R. Dietmann (2003), building on previous work by **Siegel** (1972) and **Kornhauser** (1990), showed that in this case there exists a solution $\mathbf{x} \in \mathbb{Z}^N$ with

$$|\mathbf{x}| \ll_N |F|^{p(N)}, \tag{7}$$

where $p(N)$ is a linear polynomial ($\approx 5N + C$).
In case $N = 2$, **Kornhauser** (1990) showed that only exponential bounds are possible.

Generalizing to global fields

From now on we will work with homogeneous polynomials only, and so we can work over fields instead of rings, which is more convenient.

Generalizing to global fields

From now on we will work with homogeneous polynomials only, and so we can work over fields instead of rings, which is more convenient.

Let K be a **global field**, that is a number field or global function field (i.e., a finite algebraic extension of $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is any finite coefficient field), or the algebraic closure of a global field.

Let $\mathcal{X}_K$ be a projective variety over K.

Generalizing to global fields

From now on we will work with homogeneous polynomials only, and so we can work over fields instead of rings, which is more convenient.

Let K be a **global field**, that is a number field or global function field (i.e., a finite algebraic extension of $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is any finite coefficient field), or the algebraic closure of a global field. Let $\mathcal{X}_K$ be a projective variety over K.

Problem 1

Find a search bound $B = B(\mathcal{X}_K)$ such that if $\mathcal{X}_K$ is not empty, then it contains a point $\mathbf{x}$ with

$$H(\mathbf{x}) \ll B,$$

where H is an appropriately defined height function.

Height functions

Let $N \geq 2$, then a **height function** $H : K^N \to \mathbb{R}_{\geq 0}$ is a *measure of arithmetic complexity* of points, which naturally generalizes the sup-norm height $|\ |$ defined over $\mathbb{Z}$.

Height functions

Let $N \geq 2$, then a **height function** $H : K^N \to \mathbb{R}_{\geq 0}$ is a *measure of arithmetic complexity* of points, which naturally generalizes the sup-norm height $|\ |$ defined over $\mathbb{Z}$.
For instance, every point in $\mathbf{0} \neq \mathbf{x} \in \mathbb{Q}^N$ can be written as

$$\mathbf{x} = \left(\frac{x_1}{x_0}, \dots, \frac{x_N}{x_0} \right).$$

Height functions

Let $N \geq 2$, then a **height function** $H : K^N \to \mathbb{R}_{\geq 0}$ is a *measure of arithmetic complexity* of points, which naturally generalizes the sup-norm height $|\ |$ defined over $\mathbb{Z}$.
For instance, every point in $\mathbf{0} \neq \mathbf{x} \in \mathbb{Q}^N$ can be written as

$$\mathbf{x} = \left(\frac{x_1}{x_0}, \dots, \frac{x_N}{x_0} \right).$$

Define $d = \gcd(x_1, \dots, x_N)$, then

$$H(\mathbf{x}) := \frac{1}{d} \max \left\{ |x_1|, \dots, |x_N| \right\},$$

and so $H(a\mathbf{x}) = H(\mathbf{x})$ for every $0 \neq a \in \mathbb{Q}$. Hence H is *projectively defined*. 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 L-dimensional subspace, and let $\mathbf{x}_1, \dots, \mathbf{x}_L$ 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 L-dimensional subspace, and let $\mathbf{x}_1, \dots, \mathbf{x}_L$ be a basis for V. Let

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

under the standard 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 L-dimensional subspace, and let $\mathbf{x}_1, \dots, \mathbf{x}_L$ be a basis for V. Let

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

under the standard 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 L-dimensional subspace, and let $\mathbf{x}_1, \dots, \mathbf{x}_L$ be a basis for V. Let

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

under the standard embedding. Define

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

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

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 L-dimensional subspace, and let $\mathbf{x}_1, \dots, \mathbf{x}_L$ be a basis for V. Let

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

under the standard embedding. Define

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

This definition does not depend on the choice of the basis. Hence we have defined a height on points of a Grassmanian over K.
Duality: If $A = (\mathbf{a}_1 \dots \mathbf{a}_L)^t$ is an $L \times N$ matrix over K such that

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

then

$$H(V) = H(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_L).$$

Finiteness property

A crucial property that height functions satisfy, by analogy with $| \ |$ over $\mathbb{Z}$ is *finiteness*.

Finiteness property

A crucial property that height functions satisfy, by analogy with $|\ |$ over $\mathbb{Z}$ is *finiteness*.

Northcott's theorem: *If K is a number field or a function field over a finite coefficient field, then for every $B \in \mathbb{R}_{>0}$ the set*

$$\left\{[\mathbf{x}] \in \mathbb{P}(K^N) : H(\mathbf{x}) \leq B\right\}$$

is finite.

Finiteness property

A crucial property that height functions satisfy, by analogy with $|\ |$ over $\mathbb{Z}$ is *finiteness*.

Northcott's theorem: *If K is a number field or a function field over a finite coefficient field, then for every $B \in \mathbb{R}_{>0}$ the set*

$$\left\{ [\mathbf{x}] \in \mathbb{P}(K^N) : H(\mathbf{x}) \leq B \right\}$$

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*. This makes search bounds on height interesting even when Northcott's theorem fails.

Finiteness property

A crucial property that height functions satisfy, by analogy with $| \ |$ over $\mathbb{Z}$ is *finiteness*.

Northcott's theorem: *If K is a number field or a function field over a finite coefficient field, then for every $B \in \mathbb{R}_{>0}$ the set*

$$\left\{ [\mathbf{x}] \in \mathbb{P}(K^N) : H(\mathbf{x}) \leq B \right\}$$

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*. This makes search bounds on height interesting even when Northcott's theorem fails.
We are now ready to apply this machinery.

Generalized Siegel's lemma

The following result has been obtained by **E. Bombieri** and **J. Vaaler** (1983) if K is a number field, by **J. Thunder** (1995) if K is a function field, and by **D. Roy** and **J. Thunder** (1996) if K is the algebraic closure of one or the other.

Theorem 1

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

$$\prod_{i=1}^{L} H(\mathbf{v}_i) \ll_{K,L} H(V). \tag{8}$$

The exponent 1 on $H(V)$ in this bound is smallest possible.

Corollaries

An immediate consequence of Theorem 1 is the existence of a nonzero point $\mathbf{v}_1 \in V$ such that

$$H(\mathbf{v}_1) \ll_{K,L} H(V)^{1/L}. \tag{9}$$

Corollaries

An immediate consequence of Theorem 1 is the existence of a nonzero point $\mathbf{v}_1 \in V$ such that

$$H(\mathbf{v}_1) \ll_{K,L} H(V)^{1/L}. \tag{9}$$

Moreover, a standard property of heights is that for any basis $\mathbf{x}_1, \dots, \mathbf{x}_L$ for V,

$$H(V) \ll_L \prod_{i=1}^{L} H(\mathbf{x}_i). \tag{10}$$

Corollaries

An immediate consequence of Theorem 1 is the existence of a nonzero point $\mathbf{v}_1 \in V$ such that

$$H(\mathbf{v}_1) \ll_{K,L} H(V)^{1/L}. \tag{9}$$

Moreover, a standard property of heights is that for any basis $\mathbf{x}_1, \dots, \mathbf{x}_L$ for V,

$$H(V) \ll_L \prod_{i=1}^{L} H(\mathbf{x}_i). \tag{10}$$

Hence Theorem 1 implies that for each $M \leq L$, there exists an M-dimensional subspace $U_M \subseteq V$ such that

$$H(U_M) \ll_{K,L,M} H(V)^{M/L}.$$

This proves existence of search bounds on Grassmanians of a vector space over a global field.

Back to quadratic forms: isotropic subspaces

Let F be a quadratic form in N variables over a field K and $V \subseteq K^N$ be an L-dimensional subspace such that F is **isotropic** on V (i.e. has a nontrivial zero on V).

Back to quadratic forms: isotropic subspaces

Let F be a quadratic form in N variables over a field K and $V \subseteq K^N$ be an L-dimensional subspace such that F is **isotropic** on V (i.e. has a nontrivial zero on V). A subspace $U \subseteq V$ is called **totally isotropic** if $F(U) = 0$. All maximal totally isotropic subspaces of V over K have the same dimension, we denote it by $\omega = \omega(V)$.

Back to quadratic forms: isotropic subspaces

Let F be a quadratic form in N variables over a field K and $V \subseteq K^N$ be an L-dimensional subspace such that F is **isotropic** on V (i.e. has a nontrivial zero on V). A subspace $U \subseteq V$ is called **totally isotropic** if $F(U) = 0$. All maximal totally isotropic subspaces of V over K have the same dimension, we denote it by $\omega = \omega(V)$. The following theorem was proved by **Schlickewei & Schmidt (1987)** when $K = \mathbb{Q}$ and by **Vaaler (1989)** when K is a number field.

Theorem 2

There exists a collection of $L - \omega + 1$ maximal totally isotropic subspaces $U_0, \dots, U_{L-\omega} \subseteq V$ such that $V = \operatorname{span}_K \{U_0, \dots, U_{L-\omega}\}$, and for each $0 \leq i \leq L - \omega$,

$$H(U_0)H(U_i) \ll_{K,L,\omega} H(F)^{L-\omega} H(V)^2,$$

where $H(F)$ is height of the coefficient vector of F.

Infinite family

Here is an extension of the Schlickewei-Schmidt-Vaaler theorem, although with weaker bounds, which holds over **any global field**.

Theorem 3 (Chan, F., Henshaw (2010/2014))

There exists an infinite family of collections of maximal totally isotropic subspaces $\{U_{n1}, \dots, U_{nJ}\}_{n=1}^{\infty} \subseteq V$*, for an appropriately defined* J*, such that for each* $n \geq 1$*,* $\operatorname{span}_K \{U_{n1}, \dots, U_{nJ}\} = V$*, and for each* $1 \leq j \leq J$*,*

$$H(U_{nj}) \ll H(F)^{\varphi(L,\omega)} H(V)^{\psi(\omega)},$$

where the constant in the upper bound depends on $K, N, L, \omega, \lambda, n$*, and* $\varphi(L,\omega)$*,* $\psi(\omega)$ *are polynomials:* $\varphi(L,\omega)$ *is linear in* L*, quartic in* ω*, and* $\psi(\omega)$ *is cubic in* ω*.*

Fano varieties

As a set, the **Fano variety** of m-planes on a projective variety $\mathcal{X}_K$ defined over a field K, which we denote by $\mathcal{F}_m(\mathcal{X}_K)$, is the set of $(m+1)$-dimensional vector spaces over K which are contained in $\mathcal{X}_K$; this is a subvariety of the Grassmannian.

Fano varieties

As a set, the **Fano variety** of m-planes on a projective variety $\mathcal{X}_K$ defined over a field K, which we denote by $\mathcal{F}_m(\mathcal{X}_K)$, is the set of $(m+1)$-dimensional vector spaces over K which are contained in $\mathcal{X}_K$; this is a subvariety of the Grassmannian.

We will also write $\mathcal{F}_m(\mathcal{Z}_K)$ for the set of $(m+1)$-dimensional vector spaces contained in any union of algebraic varieties $\mathcal{Z}_K$, defined over K.

Fano varieties

As a set, the **Fano variety** of m-planes on a projective variety $\mathcal{X}_K$ defined over a field K, which we denote by $\mathcal{F}_m(\mathcal{X}_K)$, is the set of $(m+1)$-dimensional vector spaces over K which are contained in $\mathcal{X}_K$; this is a subvariety of the Grassmannian.

We will also write $\mathcal{F}_m(\mathcal{Z}_K)$ for the set of $(m+1)$-dimensional vector spaces contained in any union of algebraic varieties $\mathcal{Z}_K$, defined over K.

Let

$$\mathcal{X}_K(V, F) = \{[\mathbf{x}] \in \mathbb{P}(V) : F(\mathbf{x}) = 0\}, \tag{11}$$

then Theorems 2 and 3 can be interpreted as statements about the existence of points of bounded height on $\mathcal{F}_{\omega-1}(\mathcal{X}_K(V, F))$.

Fano varieties

As a set, the **Fano variety** of m-planes on a projective variety $\mathcal{X}_K$ defined over a field K, which we denote by $\mathcal{F}_m(\mathcal{X}_K)$, is the set of $(m+1)$-dimensional vector spaces over K which are contained in $\mathcal{X}_K$; this is a subvariety of the Grassmannian.

We will also write $\mathcal{F}_m(\mathcal{Z}_K)$ for the set of $(m+1)$-dimensional vector spaces contained in any union of algebraic varieties $\mathcal{Z}_K$, defined over K.

Let

$$\mathcal{X}_K(V, F) = \{[\mathbf{x}] \in \mathbb{P}(V) : F(\mathbf{x}) = 0\}, \tag{11}$$

then Theorems 2 and 3 can be interpreted as statements about the existence of points of bounded height on $\mathcal{F}_{\omega-1}(\mathcal{X}_K(V, F))$.

Moreover, Siegel's lemma combined with Theorems 2 and 3 immediately produces the analogous results for points on $\mathcal{F}_m(\mathcal{X}_K(V, F))$ for any $0 \leq m \leq \omega - 1$.

Questions of distribution

How are points of small height distributed on hypersurfaces?

Questions of distribution

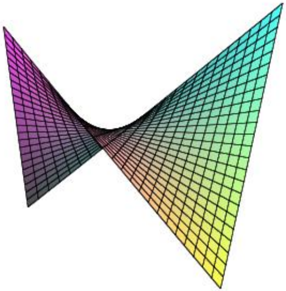
How are points of small height distributed on hypersurfaces? Are they *evenly spread out* or *bunched together*?

Questions of distribution

How are points of small height distributed on hypersurfaces? Are they *evenly spread out* or *bunched together*? For instance, can they be easily *cut out* by polynomial maps?

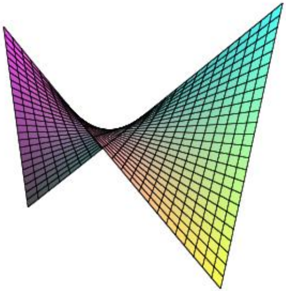
Questions of distribution

How are points of small height distributed on hypersurfaces? Are they *evenly spread out* or *bunched together*? For instance, can they be easily *cut out* by polynomial maps?



Questions of distribution

How are points of small height distributed on hypersurfaces? Are they *evenly spread out* or *bunched together*? For instance, can they be easily *cut out* by polynomial maps?



Missing varieties: Siegel's lemma

Theorem 4 (F. (2010))

Let K be a number field, function field, or $\overline{\mathbb{Q}}$. Let $N \geq 2$, $1 \leq L \leq N$, and $V \subseteq K^N$ be an L-dimensional subspace. Let $\mathcal{Z}_K$ be a union of algebraic varieties over K such that $V \nsubseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. There exists a basis $\mathbf{x}_1, \dots, \mathbf{x}_L \in V \setminus \mathcal{Z}_K$ for V over K such that for each $1 \leq n \leq L$,

$$H(\mathbf{x}_n) \ll_{K,L,M} H(V), \tag{12}$$

where the exponent 1 on $H(V)$ in the bound of (12) is sharp in general.

Missing varieties: Siegel's lemma

Theorem 4 (F. (2010))

Let K be a number field, function field, or $\overline{\mathbb{Q}}$. Let $N \geq 2$, $1 \leq L \leq N$, and $V \subseteq K^N$ be an L-dimensional subspace. Let $\mathcal{Z}_K$ be a union of algebraic varieties over K such that $V \nsubseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. There exists a basis $\mathbf{x}_1, \dots, \mathbf{x}_L \in V \setminus \mathcal{Z}_K$ for V over K such that for each $1 \leq n \leq L$,

$$H(\mathbf{x}_n) \ll_{K,L,M} H(V), \tag{12}$$

where the exponent 1 on $H(V)$ in the bound of (12) is sharp in general.

This result generalizes a result of **G. Faltings (1992)** on the existence of a small-height point in a vector space over $\mathbb{Q}$ outside of a proper subspace.

Missing varieties: quadratic forms

Theorem 5 (Chan, F., Henshaw (2013))

Let (V, F) be an isotropic quadratic space of dimension L in N variables over a global field K, as above, and let $\mathcal{X}_K(F, V)$ the set of projective zeros of F on V, as in (11). Let $\mathcal{Z}_K$ be a union of algebraic varieties defined over K such that $\mathcal{X}_K(F, V) \nsubseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. Then for each $0 \leq m \leq \omega - 1$, there exists

$$W_m \in \mathcal{F}_m(\mathcal{X}_K(V, F)) \setminus \mathcal{F}_m(\mathcal{Z}_K),$$

such that

$$H(W_m) \ll_{K,L,M,m} H(F)^{15(L+1)-m} H(V)^{27L+37}.$$

Missing varieties: quadratic forms

Theorem 5 (Chan, F., Henshaw (2013))

Let (V, F) be an isotropic quadratic space of dimension L in N variables over a global field K, as above, and let $\mathcal{X}_K(F, V)$ the set of projective zeros of F on V, as in (11). Let $\mathcal{Z}_K$ be a union of algebraic varieties defined over K such that $\mathcal{X}_K(F, V) \nsubseteq \mathcal{Z}_K$, and let M be sum of degrees of these varieties. Then for each $0 \leq m \leq \omega - 1$, there exists

$$W_m \in \mathcal{F}_m(\mathcal{X}_K(V, F)) \setminus \mathcal{F}_m(\mathcal{Z}_K),$$

such that

$$H(W_m) \ll_{K,L,M,m} H(F)^{15(L+1)-m} H(V)^{27L+37}.$$

We also have analogues of Theorems 3 and 5 over $\overline{\mathbb{Q}}$ with slightly different bounds.

Thank you!