Квадратичные формы и высоты

Леня Фукшанский
Claremont McKenna College, USA

Независимый Московский Университет
Спецсеминар: Диофантовы приближения
11 Мая, 2024

Десятая проблема Гильберта

Рассмотрим систему m Диофантовых уравнений в n переменных

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

где $P_1, \ldots, P_m$ многочлены с целыми коэффициентами.

Десятая проблема Гильберта

Рассмотрим систему m Диофантовых уравнений в n переменных

$$\left.\begin{aligned} P_1(X_1, \ldots, X_n) &= 0 \\ &\vdots \\ P_m(X_1, \ldots, X_n) &= 0 \end{aligned}\right\} \tag{1}$$

где $P_1, \ldots, P_m$ многочлены с целыми коэффициентами.

Вопрос 1

Есть ли у этой системы нетривиальные целые решения?

Десятая проблема Гильберта

Рассмотрим систему m Диофантовых уравнений в n переменных

$$\left.\begin{aligned} P_1(X_1, \ldots, X_n) &= 0 \\ &\vdots \\ P_m(X_1, \ldots, X_n) &= 0 \end{aligned}\right\} \qquad (1)$$

где $P_1, \ldots, P_m$ многочлены с целыми коэффициентами.

Вопрос 1

Есть ли у этой системы нетривиальные целые решения?

Вопрос 2

Если да, то как найти такое решение?

Десятая проблема Гильберта

Рассмотрим систему m Диофантовых уравнений в n переменных

$$\left.\begin{aligned} P_1(X_1, \ldots, X_n) &= 0 \\ &\vdots \\ P_m(X_1, \ldots, X_n) &= 0 \end{aligned}\right\} \qquad (1)$$

где $P_1, \ldots, P_m$ многочлены с целыми коэффициентами.

Вопрос 1

Есть ли у этой системы нетривиальные целые решения?

Вопрос 2

Если да, то как найти такое решение?

Знаменитый результат Матиясевича (1970; базирующийся на предыдущих работах Davis, Putnam и Robinson) установил **неразрешимость Вопроса 1** в общем виде.

Но что если...

Предположим теорему следующего типа:

Но что если...

Предположим теорему следующего типа:

Если система (1) *имеет нетривиальное решение* $\boldsymbol{x} \in \mathbb{Z}^n$, *то существует такое решение с*

$$|\boldsymbol{x}| := \max_{1 \leqslant i \leqslant n} |x_i| \leqslant B, \tag{2}$$

для некоторой константы $B = B(P_1, \ldots, P_m)$.

Но что если...

Предположим теорему следующего типа:

Если система (1) *имеет нетривиальное решение* $\boldsymbol{x} \in \mathbb{Z}^n$, *то существует такое решение с*

$$|\boldsymbol{x}| := \max_{1 \leqslant i \leqslant n} |x_i| \leqslant B, \tag{2}$$

для некоторой константы $B = B(P_1, \ldots, P_m)$.

Тогда, чтобы ответить на Вопрос 1, будет достаточно проверить является ли каждый вектор в конечном множестве

$$\left\{ \boldsymbol{x} \in \mathbb{Z}^n : \max_{1 \leqslant i \leqslant n} |x_i| \leqslant B \right\}$$

решением нашей системы (1), таким образом сводя Вопрос 1 к **конечному поисковому алгоритму.**

Поисковые границы

Более того, если мы поиском получаем положительный ответ на Вопрос 1, то конечный поисковый алгоритм также дает ответ на Вопрос 2.

Поисковые границы

Более того, если мы поиском получаем положительный ответ на Вопрос 1, то конечный поисковый алгоритм также дает ответ на Вопрос 2.

Таким образом, мы называем константу B, удовлетворяющую (2) явной **поисковой границей** (по отношению к норме $|\ |$) к полиномиальной системе $P_1, \ldots, P_M$. Тогда Вопросы 1 и 2 могут быть заменены на -

Поисковые границы

Более того, если мы поиском получаем положительный ответ на Вопрос 1, то конечный поисковый алгоритм также дает ответ на Вопрос 2.

Таким образом, мы называем константу B, удовлетворяющую (2) явной **поисковой границей** (по отношению к норме $|\ |$) к полиномиальной системе $P_1, \ldots, P_M$. Тогда Вопросы 1 и 2 могут быть заменены на -

Вопрос 3

Предположим, что полиномиальная система $P_1, \ldots, P_M$ имеет нетривиальное целое решение. Можем ли мы найти явную поисковую границу?

Ну так что, можем?

Существование поисковых границ для полиномиальных систем как (1) в общем виде противоречит теореме Матиясевича, так что в общем случае поисковые границы существовать не могут.

Ну так что, можем?

Существование поисковых границ для полиномиальных систем как (1) в общем виде противоречит теореме Матиясевича, так что в общем случае поисковые границы существовать не могут.

Более того, **J. P. Jones** (1980) доказал, что вопрос существования *положительных* целых решений неразрешим даже для одного полинома четвертой степени в достаточно большом количестве переменных.

Ну так что, можем?

Существование поисковых границ для полиномиальных систем как (1) в общем виде противоречит теореме Матиясевича, так что в общем случае поисковые границы существовать не могут.

Более того, **J. P. Jones** (1980) доказал, что вопрос существования *положительных* целых решений неразрешим даже для одного полинома четвертой степени в достаточно большом количестве переменных.

Соотвественно, существование поисковых границ для общих уравнений степени $\geqslant 4$ выглядит маловероятным, и даже про уравнения степени 3 не много известно (хотя некоторые результаты есть). В линейном и квадратичном случаях существуют достаточно развитые теории. Мы сконцентрируемся на квадратичном случае.

Квадратичные формы: Теорема Касселса

Определим симметричную билинейную форму в $2n$ переменных, $n \geqslant 2$, с целыми коэффициентами

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

а также сопряженную с ней квадратичную форму $F(\boldsymbol{X}) = F(\boldsymbol{X}, \boldsymbol{X})$. F называется **изотропной** над множеством S если она имеет нетривиальные нули в S.

Квадратичные формы: Теорема Касселса

Определим симметричную билинейную форму в $2n$ переменных, $n \geqslant 2$, с целыми коэффициентами

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

а также сопряженную с ней квадратичную форму $F(\boldsymbol{X}) = F(\boldsymbol{X}, \boldsymbol{X})$. F называется **изотропной** над множеством S если она имеет нетривиальные нули в S.

Теорема 1 (J. W. S. Cassels - 1955)

Если F изотропна над $\mathbb{Z}$, то существует $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$ такой что $F(\boldsymbol{x}) = 0$ и

$$|\boldsymbol{x}| \ll_n |F|^{\frac{n-1}{2}},$$

где $|F| := \max_{1 \leqslant i,j \leqslant n} |f_{ij}|$ и константа в верхней границе может быть представлена в явном виде.

Квадратичные формы: Теорема Касселса

Определим симметричную билинейную форму в $2n$ переменных, $n \geqslant 2$, с целыми коэффициентами

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

а также сопряженную с ней квадратичную форму $F(\boldsymbol{X}) = F(\boldsymbol{X}, \boldsymbol{X})$. F называется **изотропной** над множеством S если она имеет нетривиальные нули в S.

Теорема 1 (J. W. S. Cassels - 1955)

Если F изотропна над $\mathbb{Z}$, то существует $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$ такой что $F(\boldsymbol{x}) = 0$ и

$$|\boldsymbol{x}| \ll_n |F|^{\frac{n-1}{2}},$$

где $|F| := \max_{1 \leqslant i,j \leqslant n} |f_{ij}|$ и константа в верхней границе может быть представлена в явном виде.

Степень $\frac{n-1}{2}$ в верхней границе оптимальна

Пример (M. Kneser)

Рассмотрим $F(\boldsymbol{X}) = X_1^2 - \sum_{i=2}^{n}(X_i - cX_{i-1})^2 =$

$$(1-c^2)X_1^2 - (1+c^2)\sum_{i=2}^{n-1} X_i^2 - X_n^2 + 2c\sum_{i=2}^{n} X_{i-1}X_i,$$

где c большое целое; тогда $|F| = 1 + c^2$. Если $F(\boldsymbol{x}) = 0$ для какого-то $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$, то

$$0 \neq x_1^2 = \sum_{i=2}^{n}(x_i - cx_{i-1})^2 = y_2^2 + \cdots + y_n^2,$$

где $y_i = x_i - cx_{i-1}$ для каждого $2 \leqslant i \leqslant n$. Запишем

$$x_n = y_n + cy_{n-1} + \cdots + c^{n-1}y_2 + c^{n-1}x_1.$$

Тогда наименьшее возможное значение модуля x_n будет

$$(c^{n-1} - c^{n-2})|x_1| > \frac{1}{2}c^{n-1} = \frac{1}{2}\left(|F| - 1\right)^{\frac{n-1}{2}}.$$

Обобщения: над глобальными полями

Аналоги теоремы Касселса над глобальным полем K были получены в следующих случаях:

Обобщения: над глобальными полями

Аналоги теоремы Касселса над глобальным полем K были получены в следующих случаях:

- В 1975, **S. Raghavan**, когда K числовое поле
- В 1987, **A. Prestel**, когда K поле рациональных функций над конечным полем
- В 1997, **A. Pfister**, когда K алгебраическое расширение поля рациональных функций над конечным полем
- А также некоммутативный вариант для эрмитовой формы на кватернионовой алгебре над полностью вещественным числовым полем – в 2010, **W.K. Chan, L.F.**

Обобщения: над глобальными полями

Аналоги теоремы Касселса над глобальным полем K были получены в следующих случаях:

- В 1975, **S. Raghavan**, когда K числовое поле
- В 1987, **A. Prestel**, когда K поле рациональных функций над конечным полем
- В 1997, **A. Pfister**, когда K алгебраическое расширение поля рациональных функций над конечным полем
- А также некоммутативный вариант для эрмитовой формы на кватернионовой алгебре над полностью вещественным числовым полем – в 2010, **W.K. Chan, L.F.**

В каждом из этих случаев, суп-норма $|\ |$ заменена соответствующей *функцией высоты*, измеряющей *арифметическую сложность* решений. Во всех коммутативных случаях, степень на высоте квадратичной формы F в верхней границе по-прежнему $\frac{n-1}{2}$, как у Касселса.

Обобщения: больше одного вектора

- В 1971, **H. Davenport**, "маленькая" пара линейно независимых нулей квадратичной формы в решетке (обобщено над числовым полем – **J. H. H. Chalk**, 1980)
- В 1983/1985 **R. Schulze-Pillot / H. P. Schlickewei**, "маленький" базис решетки состоящий из нулей квадратичной формы (обобщено над числовым полем – **J. D. Vaaler, 1987**; над функциональным полем – **H. Loher**, 1997)
- В 1987, **H. P. Schickewei, W. M. Schmidt**, полностью изотропные подпространства малой высоты в квадратичном пространстве (обобщено над числовым полем – **J. D. Vaaler, 1987**; над $\overline{\mathbb{Q}}$ – **L. F., 2008**; над функциональным полем – **W. K. Chan, L. F., G. Henshaw, 2014**)
- В 2007, **L. F.**, разложение Витта малой высоты для квадратичного пространства над любым глобальным полем

Неоднородный квадратичный случай

Теперь предположим, что неоднородное квадратичное уравнение в $n \geqslant 3$ переменных с целыми коэффицентами

$$F(\boldsymbol{X}) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_{ij} X_i X_j + \sum_{i=1}^{n} f_{i0} X_i + f_{00} = 0$$

имеет целочисленное решение.

Неоднородный квадратичный случай

Теперь предположим, что неоднородное квадратичное уравнение в $n \geqslant 3$ переменных с целыми коэффицентами

$$F(\boldsymbol{X}) = \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}X_iX_j + \sum_{i=1}^{n} f_{i0}X_i + f_{00} = 0$$

имеет целочисленное решение.

R. Dietmann (2003), продолжая предыдущие работы **Siegel** (1972) и **Kornhauser** (1990), доказал, что в этом случае существует решение $\boldsymbol{x} \in \mathbb{Z}^n$ с

$$|\boldsymbol{x}| \ll_n |F|^{p(n)}, \tag{3}$$

где степень $p(n)$ линейна в n $(\approx 5n + c)$.

Неоднородный квадратичный случай

Теперь предположим, что неоднородное квадратичное уравнение в $n \geqslant 3$ переменных с целыми коэффицентами

$$F(\boldsymbol{X}) = \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}X_iX_j + \sum_{i=1}^{n} f_{i0}X_i + f_{00} = 0$$

имеет целочисленное решение.

R. Dietmann (2003), продолжая предыдущие работы **Siegel** (1972) и **Kornhauser** (1990), доказал, что в этом случае существует решение $\boldsymbol{x} \in \mathbb{Z}^n$ с

$$|\boldsymbol{x}| \ll_n |F|^{p(n)}, \tag{3}$$

где степень $p(n)$ линейна в n ($\approx 5n + c$).

В случае $n = 2$, **Kornhauser** (1990) доказал, что степень в верхней границе не может быть лучше экпоненциальной.

Неоднородный случай над $\mathbb{Q}$

Рассмотрим то же неоднородное квадратичное уравнение над $\mathbb{Q}$. **D.W. Masser** в 1998 доказал, что если F имеет решение над $\mathbb{Q}$, то существует такое решение $\boldsymbol{x}$ с

$$|\boldsymbol{x}| \ll_n |F|^{\frac{n+1}{2}}.$$

Степень $\frac{n+1}{2}$ в теореме Массера опять же оптимальна (он приводит пример, похожий по сути на пример Кнесера).

Неоднородный случай над $\mathbb{Q}$

Рассмотрим то же неоднородное квадратичное уравнение над $\mathbb{Q}$. **D.W. Masser** в 1998 доказал, что если F имеет решение над $\mathbb{Q}$, то существует такое решение $\boldsymbol{x}$ с

$$|\boldsymbol{x}| \ll_n |F|^{\frac{n+1}{2}}.$$

Степень $\frac{n+1}{2}$ в теореме Массера опять же оптимальна (он приводит пример, похожий по сути на пример Кнесера).
Метод доказательства основан на введении новой переменной X_{n+1}, с помощью которой многочлен F превращается в квадратичную форму:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}X_iX_j + \sum_{i=1}^{n} f_{i0}X_iX_{n+1} + f_{00}X_{n+1}^2.$$

Неоднородный случай над $\mathbb{Q}$

Теперь можно следовать методу Касселса, но с дополнительным условием: решение

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

должно иметь $x_{n+1} \neq 0$. Так как мы работаем над полем $\mathbb{Q}$, получаем решение:

$$F\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) = 0.$$

Неоднородный случай над $\mathbb{Q}$

Теперь можно следовать методу Касселса, но с дополнительным условием: решение

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

должно иметь $x_{n+1} \neq 0$. Так как мы работаем над полем $\mathbb{Q}$, получаем решение:

$$F\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) = 0.$$

Условие $x_{n+1} \neq 0$ значит, что мы ищем решения, не содержащиеся в заданном подпространстве нашего пространства.

Неоднородный случай над $\mathbb{Q}$

Теперь можно следовать методу Касселса, но с дополнительным условием: решение

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

должно иметь $x_{n+1} \neq 0$. Так как мы работаем над полем $\mathbb{Q}$, получаем решение:

$$F\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) = 0.$$

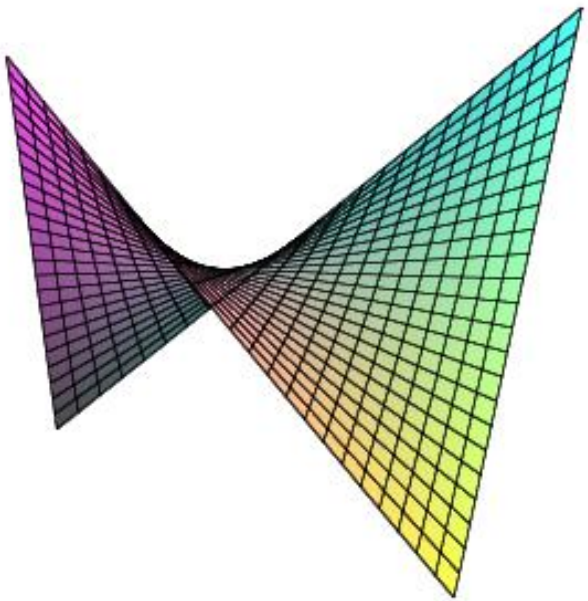
Условие $x_{n+1} \neq 0$ значит, что мы ищем решения, не содержащиеся в заданном подпространстве нашего пространства.Этот подход можно обобщить, сформулировав так называемую *задачу избежания*: **при условии, что квадратичная форма имеет нетривиальные нули лежащие вне заданной алгебраической гиперповерхности, найти такой ноль малой высоты**.

Вопрос распределения

Задачу избежания можно также рассматривать как вопрос распределения. Как точки малой высоты распределены на квадратичной гиперповерхности? Насколько легко их можно "вырезать" полиномами?

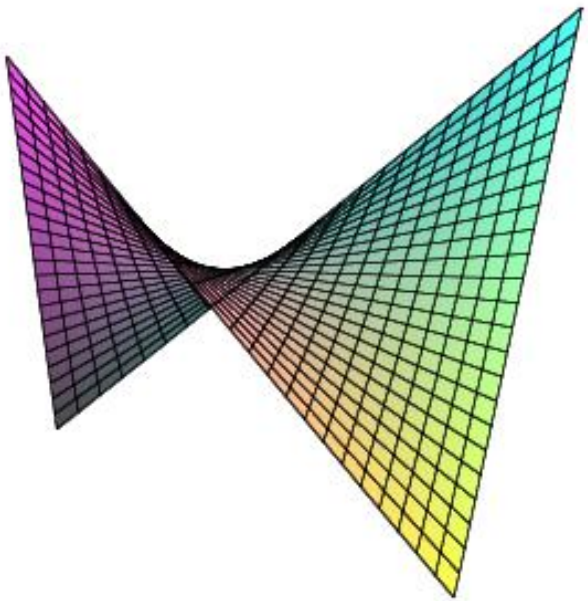
Вопрос распределения

Задачу избежания можно также рассматривать как вопрос распределения. Как точки малой высоты распределены на квадратичной гиперповерхности? Насколько легко их можно "вырезать" полиномами?



Вопрос распределения

Задачу избежания можно также рассматривать как вопрос распределения. Как точки малой высоты распределены на квадратичной гиперповерхности? Насколько легко их можно "вырезать" полиномами?



Нормирования

Чтобы представить эту теорию в общем арифметическом контексте, нам придется ввести дополнительные обозначения.

Нормирования

Чтобы представить эту теорию в общем арифметическом контексте, нам придется ввести дополнительные обозначения.

K = числовое поле, $M(K)$ = множество всех нормирований, Δ_K = дискриминант

$d = r_1 + 2r_2 = [K : \mathbb{Q}]$, где r_1 = количество вещественных вложений, r_2 = количество пар сопряженных комплексных вложений K

$\forall v \in M(K)$, $d_v = [K_v : \mathbb{Q}_v]$, и $|\cdot|_v$ продолжает обыкновенное архимедово или обыкновенное p-адическое нормирование на $\mathbb{Q}$

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

Функция высоты

Для $n \geqslant 2$ определим *локальные нормы*

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

где $\boldsymbol{x} = (x_1, \ldots, x_n) \in K^n$.

Функция высоты

Для $n \geqslant 2$ определим *локальные нормы*

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

где $\boldsymbol{x} = (x_1, \ldots, x_n) \in K^n$.
Функция высоты $H : K^n \to \mathbb{R}_{\geqslant 0}$ определяется как

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

Функция высоты

Для $n \geqslant 2$ определим *локальные нормы*

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

где $\boldsymbol{x} = (x_1, \ldots, x_n) \in K^n$.
Функция высоты $H : K^n \to \mathbb{R}_{\geqslant 0}$ определяется как

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

По формуле произведения, $H(a\boldsymbol{x}) = H(\boldsymbol{x})$ для каждого $0 \neq a \in K$, так что H *проэктивно определена*. Кроме того, H *абсолютная высота*, т.е. $H(\boldsymbol{x})$ не зависит от поля в котором лежат коэффициенты $\boldsymbol{x}$. Мы также определяем $H(\boldsymbol{0}) = 0$.

Высота Шмидта на подпространствах

Мы также можем определить высоту на подпространствах K^n (**W. M. Schmidt, 1967**). Пусть $V \subseteq K^n$ это m-мерное подпространство, и пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ это базис для V.

Высота Шмидта на подпространствах

Мы также можем определить высоту на подпространствах K^n (**W. M. Schmidt, 1967**). Пусть $V \subseteq K^n$ это m-мерное подпространство, и пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ это базис для V.

Мы обозначаем $\wedge$ обычное внешнее произведение векторов, и определяем

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

под стандартным лексикографическим вложением.

Высота Шмидта на подпространствах

Мы также можем определить высоту на подпространствах K^n (**W. M. Schmidt, 1967**). Пусть $V \subseteq K^n$ это m-мерное подпространство, и пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ это базис для V.

Мы обозначаем $\wedge$ обычное внешнее произведение векторов, и определяем

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

под стандартным лексикографическим вложением. Определим

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

Высота Шмидта на подпространствах

Мы также можем определить высоту на подпространствах K^n (**W. M. Schmidt, 1967**). Пусть $V \subseteq K^n$ это m-мерное подпространство, и пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ это базис для V.
Мы обозначаем $\wedge$ обычное внешнее произведение векторов, и определяем

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

под стандартным лексикографическим вложением. Определим

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

Это определение не зависит от выбора базиса.

Высота Шмидта на подпространствах

Мы также можем определить высоту на подпространствах K^n (**W. M. Schmidt, 1967**). Пусть $V \subseteq K^n$ это m-мерное подпространство, и пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ это базис для V.
Мы обозначаем $\wedge$ обычное внешнее произведение векторов, и определяем

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

под стандартным лексикографическим вложением. Определим

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

Это определение не зависит от выбора базиса.
Дуальность: Если $A = (\boldsymbol{a}_1 \ldots \boldsymbol{a}_{n-m})^\top$ это $(n-m) \times n$ матрица над K, такая что

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

то

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

Еще высоты

Для многочлена F с коэффицентами в K, $H(F)$ это высота вектора коэффицентов.

Еще высоты

Для многочлена F с коэффицентами в K, $H(F)$ это высота вектора коэффицентов.

Также определим **неоднородную высоту** на K^n:

$$h(\boldsymbol{x}) = H(1, \boldsymbol{x})$$

для каждого $\boldsymbol{x} \in K^n$.

Еще высоты

Для многочлена F с коэффицентами в K, $H(F)$ это высота вектора коэффицентов.

Также определим **неоднородную высоту** на K^n:

$$h(\boldsymbol{x}) = H(1, \boldsymbol{x})$$

для каждого $\boldsymbol{x} \in K^n$.

Следовательно,

$$H(\boldsymbol{x}) \leqslant h(\boldsymbol{x})$$

для всех $\boldsymbol{x} \in K^n$.

Свойство конечности множеств

Важное свойство, которому удовлетворяют функции высоты над числовым полем K, по аналогии с нормой над $\mathbb{Z}$, это *конечность:*

Свойство конечности множеств

Важное свойство, которому удовлетворяют функции высоты над числовым полем K, по аналогии с нормой над $\mathbb{Z}$, это *конечность:*

Теорема Норткотта: *Для всех* $d, B \in \mathbb{R}_{>0}$ *множество*

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

конечно.

Свойство конечности множеств

Важное свойство, которому удовлетворяют функции высоты над числовым полем K, по аналогии с нормой над $\mathbb{Z}$, это *конечность:*

Теорема Норткотта: *Для всех* $d, B \in \mathbb{R}_{>0}$ *множество*

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

конечно.

Более того, высота меряет *арифметическую сложность* (по аналогии со *степенью* в алгебраической геометрии, которая меряет *геометрическую сложность*).

Избегаем многообразия: однородный случай

Теорема 2 (Gaudron, Remond - 2017)

Пусть K числовое поле, F не идентично нулевая квадратичная форма в n переменных над K, V – m-мерное подпространство K^n, и пусть $w \geqslant 1$ это размерность максимального полностью изотропного подпространства квадратичного пространства (V, F). Пусть $\mathcal{Z}$ это проэктивное алгебраическое многообразие степени M, такое что F имеет нетривиальные нули в $V \backslash \mathcal{Z}$. Тогда существует ноль $\boldsymbol{x} \in V \backslash \mathcal{Z}$ формы F, такой что

$$H(\boldsymbol{x}) \ll_{K,m,M} H(F)^{\frac{m-w+1}{2}} H(V)^2.$$

Избегаем многообразия: однородный случай

Теорема 2 (Gaudron, Remond - 2017)

Пусть K числовое поле, F не идентично нулевая квадратичная форма в n переменных над K, V – m-мерное подпространство K^n, и пусть $w \geqslant 1$ это размерность максимального полностью изотропного подпространства квадратичного пространства (V, F). Пусть $\mathcal{Z}$ это проэктивное алгебраическое многообразие степени M, такое что F имеет нетривиальные нули в $V \backslash \mathcal{Z}$. Тогда существует ноль $\boldsymbol{x} \in V \backslash \mathcal{Z}$ формы F, такой что

$$H(\boldsymbol{x}) \ll_{K,m,M} H(F)^{\frac{m-w+1}{2}} H(V)^2.$$

Первый результат такого плана, но с несколько более слабой верхней границей был получен в статье **Chan, F., Henshaw (2014)**. Там же, мы доказываем аналогичные результаты над любым глобальным функциональным полем и $\overline{\mathbb{Q}}$.

Неоднородный случай над полем

Теорема 3 (Chan, F. - 2019)

Пусть K числовое поле, F не идентично нулевая квадратичная форма в n переменных над K, V – m-мерное подпространство K^n, и пусть $w \geqslant 0$ это размерность максимального полностью изотропного подпространства квадратичного пространства (V, F). Допустим $0 \neq t \in F(V)$ и $\mathcal{Z}$ алгебраическое многообразие степени M, которое не содержит в себе все множество нулей полинома

$$F_t(X_1, \ldots, X_n) := F(X_1, \ldots, X_n) - t.$$

Тогда существует точка $\boldsymbol{z} \in V \backslash \mathcal{Z}$, такая что $F(\boldsymbol{z}) = t$ и

$$h(\boldsymbol{z}) \ll_{K,n,m,M} H(F_t)^{\frac{m-w+2}{2}} H(V)^2.$$

Избегаем объединение гиперплоскостей над $\mathbb{Z}$

Теорема 4 (Chan, F. - 2019)

Рассмотрим целочисленую квадратичную форму $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$. *Пусть* $V \subseteq \mathbb{Q}^n$ *будет* m*-мерное подпространство,* $3 \leqslant m \leqslant n$, *на котором* F *несингулярна и изотропна. Предположим, что* $w \geqslant 1$ *это размерность максимального полностью изотропного подпространства* V. *Допустим, что* $W_1, \ldots, W_k$ *это гиперплоскости в* V. *Тогда для каждого* $0 \neq t \in F(V \cap \mathbb{Z}^n)$ *существует* $\boldsymbol{z} \in (V \cap \mathbb{Z}^n) \setminus \bigcup_{i=1}^{k} W_i$ *такой что* $F(\boldsymbol{z}) = t$ *и, если* $w = 1$,

$$h(\boldsymbol{z}) \ll_{m,n,k} h(F_t)^{(1+\frac{2}{m-2})p(m)+m+2+\frac{m+4}{m-2}} H(V)^{(2+\frac{4}{m-2})p(m)+5+\frac{8}{m-2}},$$

а если $w \geqslant 2$, $h(\boldsymbol{z}) \ll_{m,n,k} h(F_t)^{2p(m)+\frac{m-w+5}{2}} H(V)^{2p(m)+3}$.
Степень $p(m) \approx 5m + c$ *как в теореме Dietmann.*

Система квадратичных форм

Обобщений теоремы Касселса для общей системы квадратичных форм над фиксированным числовым полем не известно. Более того, не очевидно, что такое обобщение возможно.

Система квадратичных форм

Обобщений теоремы Касселса для общей системы квадратичных форм над фиксированным числовым полем не известно. Более того, не очевидно, что такое обобщение возможно.

Редукция Сколема позволяет обратить вопрос о решаемости общей системы Диофантовых уравнений в вопрос о решаемости (большей) системы линейных и квадратичных уравнений (в большем количестве переменных). Поэтому существование общей поисковой границы для квадратичной системы противоречил бы теореме Матиясевича.

Система квадратичных форм

Обобщений теоремы Касселса для общей системы квадратичных форм над фиксированным числовым полем не известно. Более того, не очевидно, что такое обобщение возможно.

Редукция Сколема позволяет обратить вопрос о решаемости общей системы Диофантовых уравнений в вопрос о решаемости (большей) системы линейных и квадратичных уравнений (в большем количестве переменных). Поэтому существование общей поисковой границы для квадратичной системы противоречил бы теореме Матиясевича.

Впрочем, над $\overline{\mathbb{Q}}$ границы на высоту решений возможны.

Система квадратичных форм над $\overline{\mathbb{Q}}$

Теорема 5 (F. - 2015)

Пусть $k \geqslant 2$ целое число, $F_1, \ldots, F_k$ квадратичные формы в n переменных над $\overline{\mathbb{Q}}$. Допустим также, что $V \subseteq \overline{\mathbb{Q}}^n$ это ℓ-мерное подпространство, $n \geqslant \ell \geqslant \frac{k(k+1)}{2} + 1$. Тогда существует точка $\mathbf{0} \neq \boldsymbol{z} \in V$, такая что $F_m(\boldsymbol{z}) = 0$ для всех $1 \leqslant m \leqslant k$ и

$$h(\boldsymbol{z}) \leqslant \left(3^{\frac{\ell^2}{2}} n^{\frac{3(\ell+1)}{2}} H(V)\right)^{20B_k^2/81} \left(\prod_{m=1}^{k-1} H(F_m)\right)^{B_k} H(F_k)^2,$$

где $B_2 = 9$ и

$$B_k = \frac{1}{4} \times 36^{2^{k-2}} \prod_{m=3}^{k} m^{2^{k-m+1}}$$

для всех $k \geqslant 3$.

Неоднородные полиномы над $\overline{\mathbb{Q}}$

Теорема 6 (F. - 2015)

Пусть F и G квадратичные полиномы в $n \geqslant 4$ переменных над $\overline{\mathbb{Q}}$, возможно неоднородные. Пусть m это целое число, $0 \leqslant m \leqslant n-4$, и $\mathcal{L}_1, \dots, \mathcal{L}_m$ это линейные полиномы в n переменных над $\overline{\mathbb{Q}}$, тоже возможно неоднородные; случай $m = 0$ просто значит, что линейных полиномов нет. Предположим, что система уравнений

$$F(\boldsymbol{x}) = G(\boldsymbol{x}) = \mathcal{L}_1(\boldsymbol{x}) = \cdots = \mathcal{L}_m(\boldsymbol{x}) = 0$$

имеет нетривиальное решение над $\overline{\mathbb{Q}}$. Тогда существует точка $\mathbf{0} \neq \boldsymbol{y} \in \overline{\mathbb{Q}}^n$, такая что $F(\boldsymbol{y}) = \mathcal{L}_1(\boldsymbol{y}) = \cdots = \mathcal{L}_m(\boldsymbol{y}) = 0$ и

$$h(\boldsymbol{y}) \leqslant 8(n+1)^{2m} 3^{2(n-m+1)(n-m)} H(F)^{\frac{1}{2}} \prod_{i=1}^{m} H(\mathcal{L}_i)^4.$$

Неоднородные полиномы над $\overline{\mathbb{Q}}$

Theorem 6, continuation

Таке, существует точка $\mathbf{0} \neq \boldsymbol{z} \in \overline{\mathbb{Q}}^n$, *такая что*

$$F(\boldsymbol{z}) = G(\boldsymbol{z}) = \mathcal{L}_1(\boldsymbol{z}) = \cdots = \mathcal{L}_m(\boldsymbol{z}) = 0$$

и

$$h(\boldsymbol{z}) \leqslant \mathcal{M}(m,n) H(F)^{58} H(G)^3 \prod_{i=1}^{m} H(\mathcal{L}_i)^{180},$$

где

$$\mathcal{M}(m,n) = 18 \times 8^{38} (n+1)^{90m+8} (n+1-m)^{36} 3^{90(n-m+1)(n-m)}.$$

Над фиксированным числовым полем

Наш метод также позволяет получить аналог Теорем 5 и 6, где полученные точки имеют ограниченную степень над заданным числовым полем. Благодаря свойству Норткотта, это дает поисковую границу для систем квадратичных и линейных уравнений, как описано выше. С другой стороны, границы на высоту получаются несколько слабее.

Ссылки

Ссылки

Обзор литературы по теореме Касселса и ее обобщениям:

Heights and quadratic forms: on Cassels' theorem and its generalizations, in "Diophantine methods, lattices, and arithmetic theory of quadratic forms"(W. K. Chan, L. Fukshansky, R. Schulze-Pillot, and J. D. Vaaler, eds.), Contemporary Mathematics, AMS vol. 587 (2013), pg. 77–94

Ссылки

Обзор литературы по теореме Касселса и ее обобщениям:

Heights and quadratic forms: on Cassels' theorem and its generalizations, in "Diophantine methods, lattices, and arithmetic theory of quadratic forms"(W. K. Chan, L. Fukshansky, R. Schulze-Pillot, and J. D. Vaaler, eds.), Contemporary Mathematics, AMS vol. 587 (2013), pg. 77–94

А также некоторые более новые результаты с тех пор:

W. K. Chan, L. Fukshansky. *Small representations of integers by integral quadratic forms*, J. Number Theory, vol. 201 (2019) pg. 40–52

L. Fukshansky. *Height bounds on zeros of quadratic forms over* $\overline{\mathbb{Q}}$, Res. Math. Sci., vol. 2 no. 1 (2015), art. 19, 26 pp.

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


Thank You!
СПАСИБО!