Комбинаторика в геометрии чисел

Райгородский Андрей Михайлович

13 мая 2020 г. — 16 мая 2020 г.

Будем говорить про решётки в пространстве.

Определение 1. Решётка Λ в пространстве $\mathbb{R}^n$ — множество точек $X \in \mathbb{R}^n$, которые задаются в виде целочисленной комбинации векторов $\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n}$. То есть все точки $X = \sum a_i \overline{b_i}, a_i \in \mathbb{Z}$. (эти вектора фиксированы для Λ)

Определение 2. Решётка в $\mathbb{R}^n$ — дискретная абелева (коммутативная) подгруппа по сложению векторов, заполняющая всё пространство.

Рассмотрим какой-то вектор с рациональными координатами

$$\overline{a} = \{\frac{a_1}{q}, \frac{a_2}{q}, \ldots, \frac{a_n}{q}\}, a_i \in \mathbb{Z}, q \in \mathbb{N}, (a_1, \ldots, a_n, q) = 1$$

и рассмотрим *центрировку a*

$$\Lambda_a = \langle \mathbb{Z}^n, \overline{a} \rangle_{\mathbb{Z}} = \{\overline{a}l + \overline{b} : l \in \mathbb{Z}, b \in \mathbb{Z}^n\}.$$

Пример. Пусть $n = 2, \overline{a} = \{\frac{1}{2}, \frac{1}{2}\}$. Тогда получим решётку, порождаемую $\overline{a}$ и $\{0, 1\}$.

Пример. Пусть $n = 2, \overline{a} = \{\frac{1}{2}, \frac{1}{3}\} = \{\frac{3}{6}, \frac{2}{6}\}$. Тогда $2\overline{a} = \{1, \frac{2}{3}\}$, значит, в решётке есть вектор $\{0, \frac{1}{3}\}$. Аналогично можно получить $\{\frac{1}{2}, 0\}$.

Назовём $\mathcal{E}$ — *каноническим базисом* $\mathbb{R}^n$ n векторов вида $\{0, 0, 0 \ldots 0, 1, 0, 0, \ldots, 0\}$, где в каждом векторе $n - 1$ координаты нулевые,

Определение 3. Дефект решётки $d(\mathcal{E}, \Lambda)$ — минимальное количество векторов, которые надо заменить в $\mathcal{E}$, чтобы получить базис в Λ (это минимальное множество может быть не единственным). **Пример**: $d(\mathcal{E}_2, \Lambda_{\{\frac{1}{2}, \frac{1}{2}\}}) = 1$, $d(\mathcal{E}_2, \Lambda_{\{\frac{1}{2}, \frac{1}{3}\}}) = 2$.

Лемма 1. В $\mathbb{R}^n$ существует $\overline{a}$ такой, что $d(\mathcal{E}_n, \Lambda_a) = k$ при любом $0 \le k \le n$.

Доказательство. Рассмотрим вектор $\overline{a} = \{\frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{p_k}, 0, \ldots, 0\}$. Докажем, что дефект этого вектора равен k. Действительно, для любого $j \le k$ вектор $\overline{a}$ можно умножить на $\prod_{i \neq j} p_i$ и получить вектор, у которого координата j не целочисленная. Значит, в решётке есть какой-то вектор $\{0, 0, \ldots, 0, t, 0, \ldots, 0\}$, где t находится на месте j и не целое. Значит, нам придётся удалить $\overline{e_j}$. С другой стороны, вектора с номерами $j + 1$ и больше можно не удалять. ■

Пусть q из канонической записи $\overline{a}$ равно $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Рассмотрим такие $M_1, \ldots, M_s \subset \{1, \ldots, n\}$: $M_i = \{\nu : (a_\nu, p_i) = 1\}$ (неформально, это номера тех дробей, у которых числитель не кратен p_i). Теперь рассмотрим все такие $S \subset \{1, \ldots, n\}$, что $\forall i : S \cap M_i \neq \emptyset$ (*систему общих представителей* M_i)

Теорема 2. $d(\mathcal{E}, \Lambda_a) = \min\{|S|\}$.

Пример. Если $a = \{\frac{1}{2}, \frac{1}{2}\}$, то $q = 2, s = 1, M_1 = \{1, 2\}$, тогда минимальная система общих представителей имеет мощность 1.

Пример. Если $a = \{\frac{1}{2}, \frac{1}{3}\}$, то $q = 6, s = 2, M_1 = \{1\}, M_2 = \{2\}$, тогда минимальная система общих представителей имеет мощность 2.

Доказательство. Вначале докажем, что $d \le |S|$. Заметим, что $d \le x$ равносильно тому, что $\exists \mathbb{R}^{n-x} \subset \mathbb{R}^n$, в котором все точки решётки Λ_a целые. Рассмотрим $S = \{\sigma_1, \ldots, \sigma_\tau\}$ — систему общих представителей для M_i. Пусть $I = \mathcal{E} \setminus \{\overline{e_i} | i \in S\}$. Рассмотрим такое подпространство N — $\mathbb{R}^{n-\tau}$, натянутое на векторы из I. Допустим, что точка $l\overline{a} + b$ оказалась в N. Мы знаем, что $\forall i \exists j : \sigma_j \in M_i \iff (a_{\sigma_j}, p_i) = 1$. Мы должны сделать τ целых чисел, чтобы потом их сделать равными нулю. То есть мы должны домножить на все простые множители знаменателей этих дробей, но там есть все простые множители, значит, мы умножим на общий знаменатель. Значит, целыми станут и все остальные компоненты вектора, тогда и весь вектор целый. Первая часть доказана. Аналогично можно доказать, что если мы нашли подпространство размерности $n - y$, то его антиподпространство размера y порождено векторами из какой-то системы общих представителей. ■

Теорема 3 (Минковский). Пусть $\omega \in \mathbb{R}^n$ выпукло, симметрично относительно начала координат и $Vol\omega > 2^n$. Тогда $\omega \cap \mathbb{Z}^n \setminus O \neq \emptyset$.

Обозначим $N_p = |\frac{1}{p}\mathbb{Z}^n \cap \omega|$. Тогда $\lim_{p\to\infty} \frac{N_p}{p^n} = Vol\omega \implies \exists P \forall p > P : N_p > (2p)^n$ (первое утверждение верно, потому что так работает объём).

Доказательство теоремы 3. Назовём точки $\frac{\overline{a}}{p}$ и $\frac{\overline{b}}{p}$ в $\frac{1}{p}\mathbb{Z}^n$ одинаковыми, если $2 \mid \overline{a} - \overline{b}$. По принципу Дирихле существуют две «одинаковые» точки. Значит, $\frac{a-b}{2}$ по выпуклости лежит в ω, а это ненулевая целая точка. ■

Пусть Λ — решётка в $\mathbb{R}^n$. Назовём $\det\Lambda$ — определитель матрицы, составленной из базисных векторов Λ (легко показать, что это определение корректное, т.к. не зависит от базиса). Это объём базисного параллелепипеда.

Теорема 4. Пусть $\omega \subset \mathbb{R}^n, \Lambda \subset \mathbb{R}^n$, ω выпукло и симметрично относительно начала координат, кроме того, $Vol\omega > 2^n \det\Lambda$. Тогда $w \cap \Lambda \setminus O \neq \emptyset$.

Доказательство. Аналогично 3. ■

Лемма 5. $\det\Lambda_a = \frac{1}{q}$.

Обозначим за O^n (октаэдр в n-мерном пространстве) тело $|x_1| + |x_2| + \ldots + |x_n| \leq 1$.

Лемма 6. $Vol\ O^n = \frac{2^n}{n!}$.

Дальше мы будем рассматривать только те решётки $\Lambda_{\overline{a*}}$, которые пересекаются с O^n только в целых точках. Обозначим $\mathfrak{f}_c(n) = \frac{cn}{\ln n} \cdot (\ln\ln n)^2$.

Теорема 7. $\max_{\overline{a*}} d(\mathcal{E}, \Lambda_{\overline{a*}}) \leq \mathfrak{f}_c(n)$ для какого-то $c > 0$.

Теорема 8. $\max_{\overline{a*}} d(\mathcal{E}, \Lambda_{\overline{a*}}) \geq \mathfrak{f}_d(n)$ для какого-то $d > 0$. *Задача слишком сложная.*

Лемма 9. $s \leq n$ (s — количество простых в каноническом разложении общего знаменателя координат a).

Доказательство. Мы знаем, что $\Lambda_a \cap O^n = \{0, \pm\epsilon_i\}$. Значит, $\frac{2^n}{n} = Vol\ O^n \leq 2^n \det\Lambda_a = \frac{2^n}{q}$. Тогда $q \leq n!$.С другой стороны, $q = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \geq s!$ (очевидно). Лемма доказана. ■

Пусть $k_i = |M_i|$ — размеры множеств из 2.

Лемма 10. $k_i! \geq p_i$.

Доказательство. Рассмотрим координатные направления с номерами из M_i. В подпространстве π, которое ими образовано, есть $O^{k_i} \subset O^n$. Часть решётки $\Lambda_a \cap \pi$ содержит точки вида $\frac{1}{q'} \cdot \{a_1, \ldots, a_n\}$, где $q' \geq p_i$ (вектор, сокращённый до нашего подпространства). Тогда $\det(\Lambda_a \cap \pi) \leq \frac{1}{p_i}$. Тогда по теореме Минковского у нас всё получается. ■

Лемма 11. $k! \geq p \implies k \geq \frac{\ln p}{2\ln\ln p}$.

Доказательство. Пусть $k < \frac{\ln p}{2\ln\ln p}$. Тогда

$$k! < k^k = e^{k\ln k} < e^{\frac{\ln p}{2\ln\ln p}\ln k} < e^{\frac{\ln p}{2\ln\ln p}\ln\ln p} = \sqrt{p} < p.\blacksquare$$

Доказательство теоремы 7. Мы знаем следующее: $\{M_1, \ldots, M_s\}; s \leq n; |M_i| \geq \frac{\ln p_i}{2\ln\ln p_i}$. Ищем $d(\mathcal{E}, \Lambda_a) = \tau(\{M_1, \ldots, M_s\})$.

Лемма 12. $\tau(\{M_1, \ldots, M_s\}) \leq \max\{\frac{n}{k}, \frac{n}{k}\ln(\frac{sk}{n})\} + \frac{n}{k} + 1$, где k таково, что $|M_i| \geq k \forall i$.

Доказательство. См. следующую страницу.

Завершение доказательства (через 12). Посмотрим на такие i, что $p_i > n$. Все множества, у которых соответствующие p большие, имеют множества мощности больше, чем $k = \frac{\ln n}{\ln\ln n}$. Воспользуемся 12 для этих множеств. Получится $\tau \leq \frac{2n(\ln\ln n)^2}{\ln n} + \frac{2n\ln\ln n}{\ln n} + 1 < \frac{3n(\ln\ln n)^2}{\ln n}$. Из других множеств возьмём по одному представителю, их будет максимум $\frac{cn}{\ln n}$, а это ещё меньше. ■

Доказательство леммы 12. Можно удалить любой набор элементов из слишком больших множеств, чтобы получилось, что $|M_i| = k$. Рассмотрим несколько случаев:

1. $\frac{sk}{n} < 1 \iff s < \frac{n}{k} \implies$ следует из того, что $\tau \le s$.
2. $\frac{n}{k} \ln \frac{sk}{n} \ge n \implies$ следует из того, что $\tau \le n$.
3. Ни то, ни другое не выполняется. Построим СОП жадным алгоритмом. Будем на i-м шаге брать элемент, который лежит в максимальном количестве множеств, которые не содержат первых $i-1$ элементов. Тогда первый элемент лежит хотя бы в $\rho_1 = \frac{sk}{n}$ множествах (принцип Дирихле); второй элемент лежит хотя бы в $\rho_2 = \frac{(s-\rho_1)k}{n}$ новых множествах; ...

   $$\text{Сделаем } N = \left\lfloor \frac{n}{k} \ln \frac{sk}{n} \right\rfloor + 1 \text{ шагов.}$$

   Мы сделали хотя бы 1 шаг и не больше, чем n. Тогда s_N (количество оставшихся множеств)

   $$s_N = s_{N-1} - \rho_N < s_{N-1}\left(1 - \frac{k}{n}\right) < \ldots < s_0\left(1 - \frac{k}{n}\right)^n = se^{N\ln(1-\frac{k}{n})} \le s^{-\frac{k}{n}N} \le se^{-\frac{k}{n}\frac{n}{k}\ln\frac{sk}{n}} = \frac{sn}{sk} = \frac{n}{k}.$$

   Возьмём из каждого оставшегося множества по элементу, получится утверждение. ■