Диаметры орбитальных графов аффинных групп

Скресанов Савелий Вячеславович

15 июня 2022 г.

Проблема Варинга

Верно ли, что для каждого k существует такое m, что всякое $n \in \mathbb{N}$ раскладывается в сумму m штук k-ых степеней, т.е.

$$n = x_1^k + \cdots + x_m^k, \text{ где } x_1, \ldots, x_m \in \mathbb{N}.$$

Лагранж (1770)	$k = 2$	$m = 4$
Гильберт (1909)	любое k	$m = ?$
...		
Малер (1957)	почти все k	$m = 2^k + \lceil (\frac{3}{2})^k \rceil - 2$

Проблема Варинга для конечных полей

p — простое число, $\mathbb{Z}_p$ — поле вычетов по модулю p.

Верно ли, что для каждого k существует такое m, что всякое $n \in \mathbb{Z}_p$ раскладывается в сумму m штук k-ых степеней, т.е.

$$n = x_1^k + \cdots + x_m^k, \text{ где } x_1, \ldots, x_m \in \mathbb{Z}_p.$$

Ответ: да, верно для любого k, т.к. проблема Варинга для $\mathbb{Z}$ решена положительно. Можно ли лучше?

Коши (1813), Дэвенпорт (1935)	k любое	$m \leq k$
...		
Глибичук (2006)	$k < \sqrt{p}$	$m \leq 16$
Глибичук, Конягин (2007)	$k < p^{1-\epsilon}$	$m \leq C \cdot 4^{1/\epsilon}$

Формулировка в терминах графов

$G = \{x^k \mid x \in \mathbb{Z}_p^*\}$ — группа (ненулевых) k-ых степеней.
$|G| = (p-1)/k$.
Вершины: $V = \mathbb{Z}_p$, рёбра: $E = \{(v, v+g) \mid v \in V, g \in G\}$.

Если $n = x_1^k + \cdots + x_m^k$, то имеем путь из 0 в n длины m:

$$(0, x_1^k),\ (x_1^k, x_1^k + x_2^k),\ \ldots,\ (x_1^k + \cdots + x_{m-1}^k, x_1^k + \cdots + x_m^k)$$

В проблеме Варинга требуется оценить диаметр графа:

$$\max_n \operatorname{dist}(0, n) = \max_{u,v} \operatorname{dist}(u, v) = \operatorname{diam}(V, E).$$

Результат Глибичука и Конягина:
Если $G \leq \mathbb{Z}_p^*$ *и* $|G| > p^\epsilon$, $\epsilon > 0$, *то* $\operatorname{diam}(V, E) \leq C \cdot 4^{1/\epsilon}$.

Формулировка в терминах графов

$G = \{x^k \mid x \in \mathbb{Z}_p^*\}$ — группа (ненулевых) k-ых степеней.
$|G| = (p-1)/k$.
Вершины: $V = \mathbb{Z}_p$, рёбра: $E = \{(v, v+g) \mid v \in V, g \in G\}$.

Если $n = x_1^k + \cdots + x_m^k$, то имеем путь из 0 в n длины m:

$$(0, x_1^k),\ (x_1^k, x_1^k + x_2^k),\ \ldots,\ (x_1^k + \cdots + x_{m-1}^k, x_1^k + \cdots + x_m^k)$$

В проблеме Варинга требуется оценить диаметр графа:

$$\max_n \operatorname{dist}(0, n) = \max_{u,v} \operatorname{dist}(u, v) = \operatorname{diam}(V, E).$$

Результат Глибичука и Конягина:
Если $G \leq \mathbb{Z}_p^*$ *и* $|G| > p^\epsilon$, $\epsilon > 0$, *то* $\operatorname{diam}(V, E) \leq C \cdot 4^{1/\epsilon}$.

Орбитальные графы

$V = \mathbb{Z}_p^d$ — векторное пространство над $\mathbb{Z}_p$.
$G \le \mathrm{GL}_d(p)$ — неприводимая группа матриц.
Вершины: V, рёбра: $E_u = \{(v, v + Au) \mid v \in V,\ A \in G\}$, $u \ne 0$.

Графы (V, E_u), $u \ne 0$, наз. орбитальными, они связны. Таких графов столько, сколько орбит у G на $V \setminus \{0\}$.

$VG = \{u \mapsto v + Au \mid v \in V,\ A \in G\}$ называется аффинной группой подстановок.

Нас интересует наибольший диаметр, т.е.

$$\mathrm{diam}(V, G) = \max_{u \ne 0} \mathrm{diam}(V, E_u).$$

Примеры

$V = \mathbb{Z}_p,\ G = \{x^k \mid x \in \mathbb{Z}_p^*\} \implies \mathrm{diam}(V, G) = m$ (пр. Варинга)

$V = \mathbb{Z}_p^d,\ d \ge 2,\ G = \mathrm{SL}_d(p) \implies \mathrm{diam}(V, G) = 1$ (полный гр.)

Орбитальные графы

$V = \mathbb{Z}_p^d$ — векторное пространство над $\mathbb{Z}_p$.
$G \leq \mathrm{GL}_d(p)$ — неприводимая группа матриц.
Вершины: V, рёбра: $E_u = \{(v, v + Au) \mid v \in V,\ A \in G\}$, $u \neq 0$.

Графы (V, E_u), $u \neq 0$, наз. орбитальными, они связны. Таких графов столько, сколько орбит у G на $V \setminus \{0\}$.

$VG = \{u \mapsto v + Au \mid v \in V,\ A \in G\}$ называется аффинной группой подстановок.

Нас интересует наибольший диаметр, т.е.

$$\mathrm{diam}(V, G) = \max_{u \neq 0} \mathrm{diam}(V, E_u).$$

Примеры

$V = \mathbb{Z}_p$, $G = \{x^k \mid x \in \mathbb{Z}_p^*\} \implies \mathrm{diam}(V, G) = m$ (пр. Варинга)

$V = \mathbb{Z}_p^d$, $d \geq 2$, $G = \mathrm{SL}_d(p) \implies \mathrm{diam}(V, G) = 1$ (полный гр.)

Основной результат

Теорема (Мароти, С., 2022)

Существует функция $f(d)$ такая, что для любого в.п. $V = \mathbb{Z}_p^d$ и неприводимой группы $G \leq \mathrm{GL}_d(p)$ с $|G| \geq f(d)$, $|G| > p^\epsilon$, $\epsilon > 0$, верно

$$\mathrm{diam}(V, G) \leq 2^{22d^3} \cdot 64^{d^2/\epsilon}.$$

Если подставить $d = 1$, то получится $\mathrm{diam}(V, G) \leq C \cdot 64^{1/\epsilon}$, т.е. результат Глибичука–Конягина (с худшими константами).

Функцию $f(d)$ из условия убрать нельзя (есть примеры).

Основной результат

Теорема (Мароти, С., 2022)

Существует функция $f(d)$ такая, что для любого в.п. $V = \mathbb{Z}_p^d$ и неприводимой группы $G \leq \mathrm{GL}_d(p)$ с $|G| \geq f(d)$, $|G| > p^\epsilon$, $\epsilon > 0$, верно

$$\mathrm{diam}(V, G) \leq 2^{22d^3} \cdot 64^{d^2/\epsilon}.$$

Если подставить $d = 1$, то получится $\mathrm{diam}(V, G) \leq C \cdot 64^{1/\epsilon}$, т.е. результат Глибичука–Конягина (с худшими константами).

Функцию $f(d)$ из условия убрать нельзя (есть примеры).

Про доказательство

Теоретико-групповая часть
Используется теорема Ларсена–Пинка (2011) и строение групп лиева типа, чтобы найти в G большую абелеву подгруппу.

Комбинаторная часть
Используется обобщение теоремы Глибичука–Конягина на произвольные конечные поля, полученное Кокрейном и Ципрой (2012).

Функция $f(d)$ возникает из теоремы Ларсена–Пинка.
Если использовать классификацию конечных простых групп, то можно взять $f(d) \simeq (d!)^2$.

Нижние оценки

$V = \mathbb{Z}_p$, $G = \{-1, 1\}$, орбитальные графы — циклы длины p, т.е. $\mathrm{diam}(V, G) = (p-1)/2$.

Нами построены серии групп $G \leq \mathrm{GL}_d(p)$, $V = \mathbb{Z}_p^d$ с $\mathrm{diam}(V, G) \geq (p-1)d/4$, причём G может быть как циклической, так и простой неабелевой группой.

$H \leq \mathrm{Sym}(\Omega)$. Орбитальный граф: вершины Ω, рёбра

$$E_{u,v} = \{(h(u), h(v)) \mid h \in H\},\ u \neq v.$$

Группа H примитивна, если нет нетривиального отношения эквивалентности на Ω, сохр.-го H ($u \simeq v \iff h(u) \simeq h(v)$).

Гипотеза Пибера

Диаметры орбитальных графов конечных примитивных групп подстановок на Ω ограничены сверху $(\log |\Omega|)^c$, кроме случая аффинных групп.

Нижние оценки

$V = \mathbb{Z}_p$, $G = \{-1, 1\}$, орбитальные графы — циклы длины p, т.е. $\operatorname{diam}(V, G) = (p-1)/2$.

Нами построены серии групп $G \leq \mathrm{GL}_d(p)$, $V = \mathbb{Z}_p^d$ с $\operatorname{diam}(V, G) \geq (p-1)d/4$, причём G может быть как циклической, так и простой неабелевой группой.

$H \leq \mathrm{Sym}(\Omega)$. Орбитальный граф: вершины Ω, рёбра

$$E_{u,v} = \{(h(u), h(v)) \mid h \in H\},\ u \neq v.$$

Группа H примитивна, если нет нетривиального отношения эквивалентности на Ω, сохр.-го H ($u \simeq v \iff h(u) \simeq h(v)$).

Гипотеза Пибера

Диаметры орбитальных графов конечных примитивных групп подстановок на Ω ограничены сверху $(\log |\Omega|)^c$, кроме случая аффинных групп.

Связь с теорией моделей

$H \leq \mathrm{Sym}(\Omega)$ — группа подстановок на Ω.

Либек, Макферсон, Тент (2009) начали изучение бесконечных примитивных групп подстановок H со свойствами:

- Если формула верна на H, то она верна и на какой-то конечной группе подстановок.
- Если на группе выполняются все формулы, верные в H, то эта группа тоже примитивна.

На языке теории моделей: примитивные счётно насыщенные псевдоконечные группы подстановок.

Примитивность — свойство второго порядка (для любого отношения эквивалентности выполнено ...).

Орбитальные графы: $(\Omega, E_{u,v})$, $u \neq v$.
Орбитальных графов может быть бесконечно много.

Т. модельное свойство $\iff$ $\mathrm{diam}(\Omega, E_{u,v})$ ограничены одной константой для всех $u, v \in \Omega$.

Теорема (Либек, Макферсон, Тент, 2009)

Описаны все конечные примитивные группы подстановок, у которых $\mathrm{diam}(\Omega, E_{u,v})$ ограничены одной константой, кроме случая аффинных групп.

Аффинные группы:
$VG = \{u \mapsto v + Au \mid v \in V, A \in G\}$, где $G \leq \mathrm{GL}_d(p)$, $V = \mathbb{Z}_p^d$.

Орбитальные графы: $(\Omega, E_{u,v})$, $u \neq v$.
Орбитальных графов может быть бесконечно много.

Т. модельное свойство $\iff$ $\mathrm{diam}(\Omega, E_{u,v})$ ограничены одной константой для всех $u, v \in \Omega$.

Теорема (Либек, Макферсон, Тент, 2009)

Описаны все конечные примитивные группы подстановок, у которых $\mathrm{diam}(\Omega, E_{u,v})$ ограничены одной константой, кроме случая аффинных групп.

Аффинные группы:
$VG = \{u \mapsto v + Au \mid v \in V, A \in G\}$, где $G \leq \mathrm{GL}_d(p)$, $V = \mathbb{Z}_p^d$.

Л.-М.-Т. получили необходимое условие для аффинных групп, которое нетривиально только при $\dim V \to \infty$.

Следствие основного результата (Мароти, С., 2022)

Существует функция $f(d)$ такая, что для любой примитивной аффинной гр. подстановок VG, где $1 < G \leq \mathrm{GL}_d(p)$, $V = \mathbb{Z}_p^d$ верно

$$\frac{\log |V|}{3 \log |G|} \leq \operatorname{diam}(V, G) \leq f(d)^{\frac{\log |V|}{\log |G|}}.$$

То есть если $\dim V = d$ фиксировано, то $\operatorname{diam}(V, G)$ ограничен тогда и только тогда, когда $\frac{\log |V|}{\log |G|}$ ограничено.

Связь с экспоненциальными суммами

$G \le \mathrm{GL}_d(p)$, $u \in \mathbb{Z}_p^d$, $u \ne 0$.
$O_u = \{Au \mid A \in G\}$ — окрестность нуля в графе (V, E_u).

Теорема (Пелюзе, 2016)

Пусть $\epsilon > 0$, $\alpha > 0$. Если $|O_u| \ge p^\epsilon$ и $|O_u \cap P| \le |O_u|^{1-\alpha}$ для всех гиперплоскостей $P \subseteq \mathbb{Z}_p^d$, то

$$\max_{x \in \mathbb{Z}_p^d \setminus 0} \left| \sum_{v \in O_u} \exp\left(2\pi i \frac{x_1 v_1 + \dots + x_d v_d}{p}\right) \right| \le p^{-\delta} |O_u|,$$

где δ зависит от ϵ и α.

Из оценки на экспоненциальную сумму следует, что диаметр графа (V, E_u) ограничен в терминах ϵ и α.