О ПОПЕРЕЧНИКАХ ОКТАЭДРОВ

Б. С. Кашин

В работе [3] нами была получена оценка поперечника $d_m(l_1^n, l_\infty^n)$ (все обозначения см. в работе [3])

$$d_m(l_1^n, l_\infty^n) \leqslant \frac{2\ln^{1/2} n}{\sqrt{m}}. \tag{1}$$

При этом использовались соображения вероятностного характера. Оценка (1) при $2m=n$ неточна, точный по порядку результат в этом случае такой:

$$d_m(l_1^{2m}, l_\infty^{2m}) \asymp \frac{1}{\sqrt{m}}.$$

Здесь доказывается, что множитель $\ln^{1/2} n$ можно отбросить и в том случае, когда

$$n^\lambda < m < n, \qquad 0<\lambda<1, \tag{2}$$

точнее, при условии (2)

$$d_m(l_1^n, l_\infty^n) \leqslant \frac{c_\lambda}{\sqrt{m}}, \tag{3}$$

где постоянная c_λ зависит только от λ. Используя известные оценки для поперечника $d_m(l_1^n, l_2^n)$ (см. [4]), легко показать, что при $m<n\theta\,(\theta<1)$ $d_m(l_1^n, l_\infty^n) > c_\theta/\sqrt{m}$; таким образом, оценка (3) не улучшаема по порядку. В работе [3] использовался тот факт, что задача об оценке поперечника $d_m(l_1^n, l_\infty^n)$ тесно связана с задачей о равномерном распределении на m-мерной сфере. В частности, рассуждая так же как в [3], мы получим оценку (3) из следующего утверждения.

Пусть k — натуральное число, тогда в пространстве R^m найдутся m^k векторов $\{e_i\}_{i=1}^{m^k}$ таких, что

$$\|e_i\|_{l_2} = \sqrt{m}, \qquad 1 \leqslant i \leqslant m^k, \tag{а}$$

$$|(e_i, e_j)| \leqslant c_k\sqrt{m} \quad \text{при} \quad i \neq j \tag{б}$$

(постоянная c_k зависит только от k). Учитывая, что при больших m всегда найдется такое простое число p, что $m/2 \leqslant p \leqslant m$, последнее утверждение без труда выводится из следующей леммы.

Лемма. *Пусть p — простое число $(p \geqslant 3)$, k — натуральное, $k \leqslant \sqrt{p}$. Тогда найдется система $\{e_\alpha\}$ из C_p^k векторов (C_p^k — число сочетаний из p по k) пространства R^p такая, что*

1) *при любом α $\|e_\alpha\|_{l_2} = \sqrt{p}$,*

2) *при $\alpha \neq \beta$ $|(e_\alpha, e_\beta)| \leqslant 2k\sqrt{p}\,(p/(p-k)) < 5k\sqrt{p}$.*

Построим искомую систему векторов. Пусть $\alpha=\{\alpha_1, \ldots, \alpha_k\}$ — такой набор целых чисел, что $0 \leqslant \alpha_1 < \ldots < \alpha_k < p$. Всего таких наборов C_p^k штук. Каждому такому набору сопоставим вектор p-мерного пространства e_α

$$e_\alpha = \{e_{\alpha,0}, e_{\alpha,1}, \ldots, e_{\alpha,p-1}\},$$

где

$$e_{\alpha,j} = \left(\frac{(j+\alpha_1)(j+\alpha_2)\ldots(j+\alpha_k)}{p}\right)\sqrt{\frac{p}{p-k}} \qquad (j=0, 1, \ldots, p-1),$$

а (s/p) обозначает символ Лежандра (см. [1], стр. 66).

Докажем, что система $\{e_\alpha\}$ искомая. В самом деле, так как $|(s/p)|=1$ при s, не делящемся на p, и $(s/p)=0$ в противном случае, то при любом α у вектора e_α все координаты, кроме k, по модулю равны $(p/(p-k))^{1/2}$, а остальные k координат равны нулю; следовательно, $\left(\sum_{j=0}^{p-1} e^2_{\alpha,\,j}\right)^{1/2} = \sqrt{\frac{p}{p-k}}\sqrt{p-k} = \sqrt{p}$, что доказывает 1).

Далее пусть набор α не равен набору β; тогда

$$|(e_\alpha, e_\beta)| = \frac{p}{p-k}\left(\sum_{j=0}^{p-1}\left(\frac{(j+\alpha_1)\ldots(j+\alpha_k)}{p}\right)\left(\frac{(j+\beta_1)\ldots(j+\beta_k)}{p}\right)\right);$$

в силу того, что $\left(\frac{s}{p}\right)\left(\frac{s'}{p}\right) = \left(\frac{s\cdot s'}{p}\right)$ при любых s и s' (см. [1], стр. 68), имеем

$$(4)\qquad |(e_\alpha, e_\beta)| = \frac{p}{p-k}\left|\sum_{j=0}^{p-1}\left(\frac{(j+\alpha_1)\ldots(j+\alpha_k)(j+\beta_1)\ldots(j+\beta_k)}{p}\right)\right| = \frac{p}{p-k}\left|\sum_{j=0}^{p-1}\left(\frac{Q(j)}{p}\right)\right|,$$

где

$$(5)\qquad Q(x) = (x+\alpha_1)\ldots(x+\alpha_k)(x+\beta_1)\ldots(x+\beta_k),$$

причем, так как набор α не равен набору β, то в разложении (5) многочлена $Q(x)$ на линейные множители найдется одночлен $(x+\alpha_r)$, который входит в (5) только в первой степени. Отсюда легко следует, что ни при каком многочлене $p(x)$

$$(6)\qquad Q(x) \not\equiv p^2(x) \pmod p$$

для суммы $\sum_{j=0}^{p-1}\left(\frac{Q(j)}{p}\right)$ при условии (6) справедлива известная оценка А. Вейля (см., например [2], стр. 221)

$$\left|\sum_{j=0}^{p-1}\left(\frac{Q(j)}{p}\right)\right| \leqslant 2k\sqrt{p}.$$

Подставляя последнюю оценку в равенство (4), получаем, что $|(e_\alpha, e_\beta)| \leqslant 2k\sqrt{p}\left(\frac{p}{p-k}\right)$, что доказывает 2). Лемма доказана.

ЛИТЕРАТУРА

[1] И. М. Виноградов, Основы теории чисел, М., «Наука», 1972.
[2] А. О. Гельфонд, Ю. В. Линник, Элементарные методы в аналитической теории чисел, М. «Наука», 1962.
[3] Б. С. Кашин, О колмогоровских поперечниках октаэдров, ДАН 214:5 (1974).
[4] С. Б. Стечкин, О наилучшем приближении заданных классов функций любыми полиномами, УМН 9: 1 (1954).

Поступило в Правление общества 4 июня 1974 г.