Лекция 3. Вероятностный метод. Примеры его применения в комбинаторной теории чисел

Лектор — Нагорный Александр Степанович
anagorny@list.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Множества, свободные от сумм

Определение 1. Подмножество A абелевой группы по сложению G называется **свободным от сумм**, если $(A + A) \cap A = \emptyset$, т. е. не существует трёх элементов $a_1, a_2, a_3 \in A$ таких, что $a_1 + a_2 = a_3$.

Пример. Множество всех нечётных целых чисел является множеством, свободным от сумм (относительно обычного сложения) в $\mathbb{Z}$.

Теорема 1. ([4] Эрдёш, 1965). Каждое множество $B = \{b_1, \dots, b_n\}$, состоящее из n целых чисел, отличных от нуля, содержит множество A, свободное от сумм, такое, что $|A| > \frac{1}{3}n$.

Множества, свободные от сумм

Доказательство. Выберем простое вида $p = 3k + 2$ так, чтобы выполнялось $p > 2 \max\limits_{1 \le i \le n} |b_i|$. Пусть $C = \{k + 1,\ k + 2, \dots, 2k + 1\}$.

Заметим, что C является подмножеством циклической группы $\mathbb{Z}_p$, свободным от сумм, и что $\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}$. Выберем случайным образом натуральное число x, $1 \le x < p$, согласно равномерному распределению на множестве $\{1, 2, \dots, p - 1\}$.

Пусть числа $d_1, \dots,\ d_n$ удовлетворяют следующим сравнениям: $d_i \equiv x b_i (\mathrm{mod}\, p),\ 0 \le d_i < p$. Очевидно, что если x пробегает числа $1, 2, \dots, p - 1$, то для любого фиксированного i, $1 \le i \le n$ величина d_i пробегает все ненулевые элементы группы $\mathbb{Z}_p$.

Множества, свободные от сумм

Доказательство (окончание). Значит, $\Pr[d_i \in C] = \frac{|C|}{p-1} > \frac{1}{3}$. Таким образом, математическое ожидание числа элементов b_i, таких, что $d_i \in C$, превосходит $\frac{n}{3}$. Следовательно, существуют x, $1 \leq x < p$, и подпоследовательность A последовательности B, такая, что $|A| > \frac{n}{3}$ и $d_i \equiv xa (\mathrm{mod}\, p) \in C$ для всех $a \in A$. Ясно, что множество A свободно от сумм. Действительно, если бы для некоторых $a_1, a_2, a_3 \in A$ выполнялось $a_1 + a_2 = a_3$, то тогда обязательно было бы верно сравнение $xa_1 + xa_2 \equiv xa_3 (\mathrm{mod}\, p)$, а это противоречило бы тому, что C является подмножеством группы $\mathbb{Z}_p$, свободным от сумм. ■

Множества, свободные от сумм

В работе **[3]** показано, что в любом подмножестве мощности n абелевой группы, не содержащем нейтрального элемента, существует более чем $2n/7$ элементов, образующих множество, свободное от сумм. Причём константа $2/7$ не улучшаемая. Наилучшая константа в утверждении теоремы 1 неизвестна.

Пары с пустым пересечением

Определение 2. Пусть $\boldsymbol{\mathcal{F}}$ является семейством из m различных подмножеств множества $X = \{1, 2, \dots, n\}$. Обозначим через $d(\boldsymbol{\mathcal{F}})$ количество непересекающихся пар в семействе $\boldsymbol{\mathcal{F}}$, т. е.,

$$d(\boldsymbol{\mathcal{F}}) = |\{(F', F'') : F', F'' \in \boldsymbol{\mathcal{F}}, F' \cap F'' = \emptyset\}|.$$

Дайкин и Эрдёш выдвинули гипотезу, что если $m = 2^{\left(\frac{1}{2} + \delta\right)n}$, то $d(\boldsymbol{\mathcal{F}}) = o(m^2)$ для любого фиксированного $\delta > 0$ и $n \to \infty$. Справедливость данной гипотезы следует из следующей теоремы, доказанной Алоном и Франклом в 1985 году.

Пары с пустым пересечением

Теорема 2 ([2] Alon and Frankl, 1985). Пусть $\boldsymbol{\mathcal{F}}$ — произвольное семейство, состоящее из $m = 2^{\left(\frac{1}{2}+\delta\right)n}$ подмножеств множества $X = \{1, 2, \dots, n\}$, где $\delta > 0$. Тогда

$$d(\boldsymbol{\mathcal{F}}) < m^{2-\frac{\delta^2}{2}}. \qquad (1)$$

Доказательство. Предположим, что неравенство (1) неверно. Выберем (в качестве элементов семейства $\boldsymbol{\mathcal{F}}$) случайно и независимо t множеств $A_1, A_2, \dots, A_t$, где t — большое натуральное число, которое будет определено позже.

Пары с пустым пересечением

Доказательство (продолжение).
Покажем, что с положительной вероятностью выполняется неравенство $|A_1 \cup A_2 \cup \cdots \cup A_t| > n/2$, и что данное объединение не пересекается более чем с $2^{n/2}$ различными подмножествами множества X. Это противоречие покажет, что неравенство (1) верно. В самом деле,

$$\Pr[|A_1 \cup A_2 \cup \cdots \cup A_t| \le n/2] \le \sum_{S \subset X, |S| \le n/2} \Pr[A_i \subset S, i = 1, \dots, t] \le$$

$$\le 2^n (2^{n/2} / 2^{((1/2+\delta)n)})^t = 2^{n(1-\delta t)}. \qquad (2)$$

Пары с пустым пересечением

Доказательство (продолжение). Введём обозначение

$$v(B)=|\{A \in \mathcal{F} : B \cap A = \emptyset\}|.$$

Ясно, что

$$\sum_{B\in\mathcal{F}} v(B) = 2d(\mathcal{F}) \geq 2m^{2-\frac{\delta^2}{2}}.$$

Пусть Y — случайная величина, значение которой равно числу множеств $B \in \mathcal{F}$, которые не пересекаются с каждым из A_i $(1 \leq i \leq t)$. В силу выпуклости функции z^t математическое ожидание величины Y удовлетворяет условиям

$$\mathbf{E}[Y] = \sum_{B\in\mathcal{F}} (v(B)/m)^t = \frac{1}{m^t} \cdot m \left(\frac{\sum v(B)^t}{m}\right) \geq \frac{1}{m^t} \cdot m \left(\frac{2d(\mathcal{F})}{m}\right)^t \geq 2m^{1-\frac{t\delta^2}{2}}.$$

Пары с пустым пересечением

Доказательство (окончание). Так как $Y \leq m,$ то

$$\Pr\left[Y \geq m^{1-\frac{t\delta^2}{2}}\right] \geq m^{-\frac{t\delta^2}{2}}. \qquad (3)$$

Легко видеть, что при $t = \lceil 1 + 1/\delta \rceil$ выполняется $m^{1-\frac{t\delta^2}{2}} > 2^{n/2}$, и правая часть неравенства (3) больше правой части неравенства (2).

Итак, с положительной вероятностью выполняется неравенство $|A_1 \cup A_2 \cup \cdots \cup A_t| > n/2,$ и это объединение не пересекается с более чем $2^{n/2}$ множествами из семейства $\boldsymbol{\mathcal{F}}$. Это противоречие доказывает неравенство (1).

Теорема 2 доказана. ■

Пересекающиеся семейства множеств

Определение 3. Семейство $\mathcal{F}$ множеств называется **пересекающимся**, если для любых двух множеств $A, B \in \mathcal{F}$ выполняется условие $A \cap B \neq \emptyset$.

Пусть $n \geq 2k$, и $\mathcal{F}$ является пересекающимся семейством k –элементных подмножеств множества мощности n. Для определённости будем считать, что элементы $\mathcal{F}$ являются подмножествами множества $\{0, 1, \dots, n-1\}$.

Лемма 1. Для каждого s, $0 \leq s \leq n-1$, рассмотрим множество $A_s = \{s, \ s+1, \dots, s+k-1\}$, где сумма берётся по модулю n. Тогда $\mathcal{F}$ может содержать не более k множеств A_s.

Доказательство Леммы 1.

Зафиксируем некоторое $A_s \in \mathcal{F}$. Из всех остальных множеств A_t, пересекающих A_s, составим $k-1$ пар $\{A_{s-i}, A_{s+k-i}\}$, $1 \leq i \leq k-1$. Элементы каждой такой пары являются непересекающимися. Утверждение леммы теперь вытекает из того, что $\mathcal{F}$ не может содержать более одного элемента из каждой пары. ■

Теорема Эрдёша — Ко — Радо

Теорема 3 ([5] Katona, 1972).

Пусть $n \geq 2k$, и $\boldsymbol{\mathcal{F}}$ — пересекающееся семейство k–элементных подмножеств множества $\{0, 1, \dots, n-1\}$. Тогда

$$|\boldsymbol{\mathcal{F}}| \geq \binom{n-1}{k-1}.$$

Доказательство. Выберем случайным образом перестановку σ на множестве $\{0, 1, \dots, n-1\}$ и число $i \in \{0, 1, \dots, n-1\}$.

Пусть $A = \{\sigma(i), \sigma(i+1), \dots, \sigma(i+k-1)\}$, где сумма, как и раньше, берётся по модулю n. В силу произвольности выбора σ из леммы вытекает, что $\Pr[A \in \boldsymbol{\mathcal{F}}] \leq k/n$.

Теорема Эрдёша — Ко — Радо

Доказательство (окончание).

Но A выбирается равновероятно из всех k–множеств, поэтому

$$\frac{k}{n} \geq \Pr[A \in \mathcal{F}] = \frac{|\mathcal{F}|}{\binom{n}{k}} \quad \text{и} \quad |\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}. \blacksquare$$

Замечание. Оценка, доказанная в теореме 3, достижима, например, на семействе всех k –элементных подмножеств (множества из n элементов), содержащих какую-то определённую точку.

Литература к лекции

1. Алон Н., Спенсер Дж. Вероятностный метод. М.: БИНОМ. Лаборатория знаний, 2007, С. 27-31.
2. Alon N. and Frankl P. (1985) The maximum number of disjoint pairs in a family of subsets // *Graphs and Combinatorics* **1**: P. 13-21.
3. Alon N. and Kleitman D.J. (1990) Sum-free subsets, in: *A tribute to Paul Erdós* (A. Baker, B.Bollobás and A.Hajnál, eds.) Cambrige Univ. Press, Cambrige, England, P. 13-26.
4. Erdós P. (1965) Extremal problems in number theory // *Proc. Symp. Pure Math. (AMS)* **VIII**, P. 181-189.
5. Katona G.O.H. (1972) A simple proof of the Erdós-Ko-Rado theorem. // *J. Combinatorial Theory. Ser. B* **13:** P. 183-184.

СПАСИБО ЗА ВНИМАНИЕ!