# Дискретные структуры

МФТИ, весна 2014

Александр Дайняк

www.dainiak.com

# Как мы получали нижнюю оценку чисел Рамсея (общая идея)

- Чтобы доказать оценку вида $R(s,s) > n$, достаточно доказать, что существует граф на $n$ вершинах, в котором *нет* ни клик, ни независимых множеств размера $s$.
- Мы фиксировали множество вершин и строили на них *случайный граф*, проводя каждое ребро независимо от других с вероятностью $1/2$.

# Вероятностный метод

- Пусть нам нужно доказать существование «хорошего» объекта.
- Разбиваем определение «хорошести» на отдельные свойства: чтобы объект был хорошим, нужно, чтобы в нём не было плохих частей вида $\mathrm{bad}_1, \mathrm{bad}_2, \ldots$
- Доказываем, что при случайном выборе объекта $\Pr[\text{в объекте оказалось } \mathrm{bad}_i]$ мала для каждого $i$.
- Делаем отсюда вывод, что
$$\Pr[\text{в объекте есть плохие части}] < 1$$
- Значит, $\Pr[\text{случайный объект хороший}] > 0$

# Маловероятность vs. независимость

При оценке $R(s, s)$ вероятности $A_i$ того, что в графе есть клика или н.м., были очень малыми, поэтому мы оценивали довольно грубо:

$$\Pr\left[\bigcap_i \overline{A_i}\right] = 1 - \Pr\left[\bigcup_i A_i\right] \geq 1 - \sum_i \Pr[A_i] > 0$$

Зачастую $\Pr A_i$ не так малы. Если бы $A_i$ были *независимы*, нам хватало бы оценки $\Pr[A_i] < 1$, так как тогда мы могли бы написать

$$\Pr\left[\bigcap_i \overline{A_i}\right] = \prod_i \Pr[\overline{A_i}] = \prod_i (1 - \Pr[A_i]) > 0$$

# Маловероятность vs. независимость

Зачастую $\Pr A_i$ не очень малы. Если бы $A_i$ были *независимы*, нам хватало бы оценки $\Pr[A_i] < 1$, так как тогда мы могли бы написать

$$\Pr\left[\bigcap_i \overline{A_i}\right] = \prod_i \Pr[\overline{A_i}] = \prod_i (1 - \Pr[A_i]) > 0$$

Проблема возникает, если одновременно

- вероятности плохих событий не слишком малы,
- и плохие события не являются независимыми.

Но и в этом случае выход может найтись:

- **Локальная лемма Ловаса**: балансирует между независимостью и маловероятностью.

# Свойства условных вероятностей (упражнения)

Для любых $A, B$ выполнено $\Pr[\bar{A} \mid B] = 1 - \Pr[A \mid B]$

Для любых $A, B, C$ выполнено

$$\Pr[A \mid BC] = \frac{\Pr[AB \mid C]}{\Pr[B \mid C]}$$

Для любых $A, B, C$ выполнено

$$\Pr[AB \mid C] \leq \Pr[A \mid C]$$

Для любых $A_1, \dots, A_n$ выполнено

$$\Pr[A_1 \dots A_n] = \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1 A_2] \times \cdots \times \Pr[A_n \mid A_1 \dots A_{n-1}]$$

Для любых $A_1, \dots, A_n, B$ выполнено

$$\Pr[A_1 \dots A_n \mid B] = \Pr[A_1 \mid B] \cdot \Pr[A_2 \mid BA_1] \cdot \Pr[A_3 \mid BA_1 A_2] \times \cdots \times \Pr[A_n \mid BA_1 \dots A_{n-1}]$$

# Независимые события

События $A$ и $B$ *независимы*, если

$$\Pr[A \mid B] = \Pr[A]$$
$$\Pr[B \mid A] = \Pr[B]$$

Более симметричное определение, корректное и для событий с нулевой вероятностью: $A$ и $B$ независимы, если

$$\Pr[AB] = \Pr[A] \cdot \Pr[B]$$

**Важно понимать:**

независимость $\neq$ несовместность

Наоборот, если события никогда не происходят одновременно, то они «*сильно*» зависимы.

# Независимые события

**Пример:**
Рассмотрим случайный граф на фиксированном множестве вершин $\{v_1, \dots, v_n\}$.

Пусть

$$A \coloneqq \text{«вершины } v_1, \dots, v_k \text{ образуют клику»}$$
$$B \coloneqq \text{«вершины } v_{k+1}, \dots, v_{2k} \text{ образуют клику»}$$

Тогда $A$ и $B$ независимы, так как наличие/отсутствие клики на вершинах $v_1, \dots, v_k$ ничего не говорит о том, что происходит на вершинах $v_{k+1}, \dots, v_{2k}$ в нашей модели.

# Независимость групп событий

События $A_1, \dots, A_t$ *независимы в совокупности*, если $\forall s, \forall i_1, \dots, \forall i_s$ выполнено равенство

$$\Pr\left[A_{i_1} \dots A_{i_s}\right] = \Pr\left[A_{i_1}\right] \cdot \dots \cdot \Pr\left[A_{i_s}\right]$$

Событие $A$ *не зависит от группы событий* $B_1, \dots, B_t$, если $\forall s, \forall i_1, \dots, \forall i_s$ при условии $\Pr\left[B_{i_1} \dots B_{i_s}\right] > 0$ выполняется равенство

$$\Pr\left[A \mid B_{i_1} \dots B_{i_s}\right] = \Pr[A]$$

Иначе говоря, $\forall s, \forall i_1, \dots, \forall i_s$ выполнено

$$\Pr\left[AB_{i_1} \dots B_{i_s}\right] = \Pr[A] \cdot \Pr\left[B_{i_1} \dots B_{i_s}\right]$$

# Независимость события от группы других событий

Событие $A$ *не зависит от группы событий* $B_1, \dots, B_t$, если $\forall s \forall i_1, \dots, i_s$ при условии $\Pr\left[B_{i_1} \dots B_{i_s}\right] > 0$ выполняется равенство

$$\Pr\left[A \mid B_{i_1} \dots B_{i_s}\right] = \Pr[A]$$

**Утверждения-упражнения:**

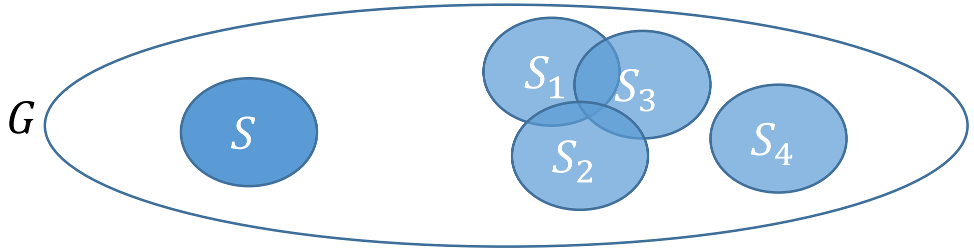
- События $A_1, \dots, A_t$ независимы в совокупности т. и т.т., когда $\forall i$ событие $A_{i+1}$ не зависит от группы событий $A_1, \dots, A_i$.
- Если событие $A$ не зависит от группы событий $B_1, \dots, B_t$, то $A$ не зависит и от группы событий $B_1, \dots, B_t, \overline{B_1}, \dots, \overline{B_t}$.
(Доказательство можно провести индукцией по длине набора индексов $i_1, \dots, i_s$ в определении.)

# Независимость события от группы других событий

Событие $A$ *не зависит от группы событий* $B_1, \dots, B_t$, если $\forall s \forall i_1, \dots, i_s$ при условии $\Pr\left[B_{i_1} \dots B_{i_s}\right] > 0$ выполняется равенство

$$\Pr\left[A \mid B_{i_1} \dots B_{i_s}\right] = \Pr[A]$$

**Пример.**
В нашей модели графа $G$ со «случайно проводимыми рёбрами», если картина такая:




События $A, B_1, \dots, B_4$ = появление клики/н.м. на множестве вершин $S, S_1, \dots, S_4$

поскольку множества вершин, на которых «живёт» событие $A$ и остальные события, не пересекаются. При этом сами $B_1, \dots, B_t$ необязательно независимы!

# Орграф зависимостей

*Орграф зависимостей* $(V, D)$ для набора событий $A_1, \ldots, A_t$ определяется так:

- $V := \{1, \ldots, t\}$
- $D$ таково, что если $(i_1, k), \ldots, (i_s, k) \notin D$, то $A_k$ не зависит от группы $A_{i_1}, \ldots, A_{i_s}$.

Содержательно, в орграфе *нет* дуги из $i$ в $k$, если $A_i$ «*никак не влияет*» на $A_k$.

Замечание: если дуга проведена, это не значит, что есть зависимость между событиями!

# Лемма Ловаса (общий случай)

**Теорема. (Локальная лемма Ловаса)**
Пусть $D$ — множество дуг некоторого орграфа зависимостей для набора событий $A_1, \dots, A_n$.
Допустим, что нашлись такие $x_1, \dots, x_n \in (0,1)$, что $\forall k \in \{1, \dots, n\}$ выполнено неравенство

$$\Pr[A_k] \leq x_k \cdot \prod_{i:\ (i,k) \in D} (1 - x_i)$$

Тогда

$$\Pr[\overline{A_1} \dots \overline{A_n}] \geq (1 - x_1) \cdot \dots \cdot (1 - x_n) > 0$$

# Доказательство леммы Ловаса

- $\forall k \quad \Pr[A_k] \le x_k \cdot \prod_{i:(i,k)\in D}(1-x_i)$

Индукцией по $|S|$ докажем, что для любого $S \subseteq \{1,\dots,n\}$ и любого $A_k$

$$\Pr\left[A_k \mid \bigcap_{i\in S} \overline{A_i}\right] \le x_k$$

База: $|S| = 0$. Тогда $S = \emptyset$ и мы получаем

$$\Pr\left[A_k \mid \bigcap_{i\in S} \overline{A_i}\right] = \Pr[A_k] \le x_k$$

- $\forall k \quad \Pr[A_k] \le x_k \cdot \prod_{i:(i,k)\in D}(1 - x_i)$
- $\forall k \forall S' \quad |S'| < |S| \Rightarrow \Pr\left[A_k \mid \bigcap_{i\in S'} \overline{A_i}\right] \le x_k$

Положим

$$S_{\text{bad}} \coloneqq \{i \in S \text{ т. что } (i,k) \in D\}$$
$$S_{\text{good}} \coloneqq S \setminus S_{\text{bad}}$$

Если $S_{\text{bad}} = \emptyset$, то всё сразу получается:

$$\Pr\left[A_k \mid \bigcap_{i\in S} \overline{A_i}\right] = \Pr[A_k] \le x_k$$

Поэтому дальше будем рассматривать только случай $|S_{\text{bad}}| > 0$.

- $\forall k \quad \Pr[A_k] \leq x_k \cdot \prod_{i:\,(i,k)\in D}(1 - x_i)$
- $\forall k \forall S' \quad |S'| < |S| \Rightarrow \Pr\left[A_k \mid \bigcap_{i\in S'} \overline{A_i}\right] \leq x_k$
- $S_{\text{bad}} \coloneqq \{i \in S \text{ т. что } (i,k) \in D\} \neq \emptyset, \qquad S_{\text{good}} \coloneqq S \setminus S_{\text{bad}}$

Имеем

$$\Pr\left[A_k \mid \bigcap_{i\in S} \overline{A_i}\right] = \frac{\Pr\left[\ A_k \cap \bigcap_{i\in S_{\text{bad}}} \overline{A_i} \quad \mid \quad \bigcap_{i\in S_{\text{good}}} \overline{A_i}\ \right]}{\Pr\left[\ \bigcap_{i\in S_{\text{bad}}} \overline{A_i} \quad \mid \quad \bigcap_{i\in S_{\text{good}}} \overline{A_i}\ \right]}$$

В этой дроби

$$\text{числитель} \leq \Pr\left[A_k \mid \bigcap_{i\in S_{\text{good}}} \overline{A_i}\right] = \Pr[A_k]$$

Достаточно теперь доказать, что

$$\text{знаменатель} \geq \prod_{i:\,(i,k)\in D} (1 - x_i)$$

- $\forall k \quad \Pr[A_k] \le x_k \cdot \prod_{i:\,(i,k)\in D}(1-x_i)$
- $\forall k \forall S' \quad |S'| < |S| \Rightarrow \Pr\left[A_k \mid \cap_{i\in S'} \overline{A_i}\right] \le x_k$
- $S_{\text{bad}} \coloneqq \{i \in S \text{ т. что } (i,k) \in D\} \neq \emptyset, \qquad S_{\text{good}} \coloneqq S \setminus S_{\text{bad}}$

Пусть $S_{\text{bad}} = \{i_1, \dots, i_l\}$. Имеем

$$\Pr\left[\bigcap_{i\in S_{\text{bad}}} \overline{A_i} \mid \bigcap_{i\in S_{\text{good}}} \overline{A_i}\right] =$$

$$= \Pr\left[\overline{A_{i_1}} \mid \bigcap_{i\in S_{\text{good}}} \overline{A_i}\right] \cdot \Pr\left[\overline{A_{i_2}} \mid \overline{A_{i_1}} \cap \bigcap_{i\in S_{\text{good}}} \overline{A_i}\right] \cdot \Pr\left[\overline{A_{i_3}} \mid \overline{A_{i_1}}\,\overline{A_{i_2}} \cap \bigcap_{i\in S_{\text{good}}} \overline{A_i}\right] \times \cdots$$

$$\times \Pr\left[\overline{A_{i_l}} \mid \overline{A_{i_1}} \dots \overline{A_{i_{l-1}}} \cap \bigcap_{i\in S_{\text{good}}} \overline{A_i}\right] \ge \left(1 - x_{i_1}\right) \cdot \left(1 - x_{i_2}\right) \cdot \dots \cdot \left(1 - x_{i_l}\right) \ge \prod_{i:\,(i,k)\in D} (1 - x_i)$$

что и требовалось.

- $\forall k \quad \Pr[A_k] \le x_k \cdot \prod_{i:\,(i,k)\in D}(1-x_i)$
- $\forall k \forall S \quad \Pr\left[A_k \mid \bigcap_{i\in S'} \overline{A_i}\right] \le x_k$ — доказали!

Теперь легко вывести утверждение теоремы:

$$\Pr[\overline{A_1} \cap \dots \cap \overline{A_n}] = \Pr[\overline{A_1}] \cdot \Pr[\overline{A_2} \mid \overline{A_1}] \cdot \ldots \cdot \Pr[\overline{A_n} \mid \overline{A_1} \cap \dots \cap \overline{A_{n-1}}] \ge$$
$$\ge (1-x_1)(1-x_2) \cdot \ldots \cdot (1-x_n)$$

Лемма Ловаса доказана.

# Лемма Ловаса (симметричный случай)

**Теорема. (Локальная лемма Ловаса — с.с.)**
Пусть события $A_1, \ldots, A_n$ таковы, что

- $\forall i$ событие $A_i$ не зависит от группы всех остальных, кроме не более $d$, событий (т.е. в орграфе зависимостей $d^-(i) \leq d$)
- $\forall i \Pr[A_i] \leq \frac{1}{(d+1)e}$, где $e = 2.718 \ldots$

Тогда

$$\Pr[\overline{A_1} \ldots \overline{A_n}] > 0$$

# Доказательство симметричного случая: сведение к общему

Если $d = 0$, то все события независимы в совокупности, и $\Pr[\overline{A_1} \ldots \overline{A_n}] > 0$.

Пусть $d \geq 1$. Положим $x_1, \ldots, x_n \coloneqq \frac{1}{d+1}$.
Замечаем, что выполнены требования общего случая Локальной Леммы:

$$\Pr[A_k] \leq \frac{1}{(d+1)e} < \frac{1}{d+1} \cdot \left(1 - \frac{1}{d+1}\right)^d \leq x_k \cdot \prod_{i:\ (i,k) \in D} (1 - x_i)$$

Остаётся лишь применить Локальную лемму.

# Применение к оценке чисел Рамсея: напоминание модели

Пусть $n := \lfloor 2^{0.5\,s} \rfloor$, и пусть $V := \{v_1, \ldots, v_n\}$ — фиксированное множество вершин.

Построим на этих вершинах *случайный граф*, проводя каждое из $\binom{n}{2}$ рёбер независимо от других с вероятностью $1/2$.

Вероятность получить при этом любой конкретный граф на вершинах $v_1, \ldots, v_n$ равна

$$2^{-\binom{n}{2}}$$

# Оценка чисел Рамсея: применение Локальной Леммы

Для каждого множества $U \subset V$ размера $s$ рассмотрим события

$$A_U := «U — \text{н. м. или клика}»$$

Для каждого $U$ имеем

$$\Pr[A_U] = 2^{1-\binom{s}{2}}$$

На каждое $A_U$ могут влиять только такие $A_{U'}$, что $|U \cap U'| \geq 2$. Значит, $A_U$ не зависит от всех, кроме, как максимум, $\binom{s}{2}\binom{n-2}{s-2}$ других событий.

# Оценка чисел Рамсея: применение Локальной Леммы

- $A_U \coloneqq$ «$U$ — н. м. или клика»
- $\Pr[A_U] = 2^{1-\binom{s}{2}}$
- $A_U$ не зависит от всех, кроме, как максимум, $\binom{s}{2}\binom{n-2}{s-2}$ других событий.

Если $2^{1-\binom{s}{2}} \leq \frac{1}{\binom{s}{2}\binom{n-2}{s-2}\cdot e}$, то $R(s,s) > n$.

Достаточно, чтобы выполнялось неравенство

$$\frac{s^2}{2}\left(\frac{en}{s-2}\right)^{s-2} \cdot e < 2^{s(s-1)/2-1}$$

# Оценка чисел Рамсея: применение Локальной Леммы

Для оценки $R(s,s) > n$ достаточно неравенства

$$\frac{s^2}{2}\left(\frac{en}{s-2}\right)^{s-2} \cdot e < 2^{s(s-1)/2-1}$$

Берём корень из обеих частей:

$$n < \big(1+o(1)\big) \cdot e^{-1} \cdot s \cdot 2^{(s^2-s)/(2s-4)}$$

$$n < \big(1+o(1)\big) \cdot e^{-1} \cdot s \cdot 2^{\frac{s+1}{2}+\frac{1}{s-2}}$$

Окончательно,

$$R(s,s) \gtrsim \frac{\sqrt{2}}{e} \cdot s\left(\sqrt{2}\right)^{s}$$

Это в 2 раза лучше, чем оценка без ЛЛЛ.

Лучшей оценки на сегодня не известно.

# Внедиагональные числа Рамсея

Оценим $R(s, 3)$ — минимальное $n$, такое, что любой граф на $n$ вершинах содержит клику на трёх вершинах или н.м. на $s$ вершинах.

Построим случайный граф, проводя каждое ребро с вероятностью $p$.

Для каждого множества $U \subset V$ размера $s$ рассмотрим событие

$$A_U \coloneqq \text{«множество } U \text{ независимое»}$$

Для каждого множества $W \subset V$ размера $3$ рассмотрим событие

$$B_W \coloneqq \text{«множество } W \text{ образует клику»}$$

# Внедиагональные числа Рамсея

- $A_U \coloneqq$ «множество $U$ независимое»
- $B_W \coloneqq$ «множество $W$ образует клику»

Имеем

$$\Pr[A_U] = (1-p)^{\binom{s}{2}}, \qquad \Pr[B_W] = p^3$$

- Число событий вида $A_{\dots}$, могущих повлиять на фиксированное $A_U$, не больше $\binom{n}{s}$. Число событий вида $B_{\dots}$, могущих повлиять на фиксированное $A_U$, не больше $\binom{s}{2}(n-2) < \frac{s^2 n}{2}$.
- Число событий вида $A_{\dots}$, могущих повлиять на фиксированное $B_W$, не больше $\binom{n}{s}$. Число событий вида $B_{\dots}$, могущих повлиять на фиксированное $B_W$, не больше $3(n-3) < 3n$.

# Внедиагональные числа Рамсея

- $\Pr[A_U] = (1-p)^{\binom{s}{2}}, \qquad \Pr[B_W] = p^3$
- На $A_U$ могут влиять не больше $\binom{n}{s}$ событий $A_*$ и не больше $\frac{s^2 n}{2}$ событий $B_{\dots}$.
- На $B_W$ могут влиять не больше $\binom{n}{s}$ событий $A_*$ и не больше $3n$ событий $B_{\dots}$.

Если мы сможем подобрать $x, y, p \in (0,1)$ и $n \in \mathbb{N}$, так, чтобы выполнялись условия

$$\begin{cases} (1-p)^{\binom{s}{2}} \le x \cdot (1-x)^{\binom{n}{s}} \cdot (1-y)^{s^2 n/2} \\ p^3 \le y \cdot (1-x)^{\binom{n}{s}} \cdot (1-y)^{3n} \end{cases}$$

то (с помощью ЛЛЛ) мы докажем, что $R(s,3) > n$.

# Внедиагональные числа Рамсея

Если $\begin{cases} (1-p)^{\binom{s}{2}} \leq x \cdot (1-x)^{\binom{n}{s}} \cdot (1-y)^{s^2 n/2} \\ p^3 \leq y \cdot (1-x)^{\binom{n}{s}} \cdot (1-y)^{3n} \end{cases}$

то $R(s,3) > n$.

Вычисления показывают, что можно взять

$$n \coloneqq c_1 \frac{s^2}{(\log s)^2}, \quad p \coloneqq c_2 \frac{\log s}{s},$$

$$x \coloneqq c_3 \binom{n}{s}^{-1}, \quad y \coloneqq c_4 \frac{(\log s)^3}{s^3}$$

для некоторых констант $c_1, c_2, c_3, c_4$. Отсюда

$$R(s,3) = \Omega\left(\frac{s^2}{(\log s)^2}\right).$$

# Внедиагональные числа Рамсея

Исходя из предыдущего,

$$R(s, 3) = \Omega\left(\frac{s^2}{(\log s)^2}\right)$$

**Замечание.**

Как показал J. H. Kim (1995), на самом деле

$$R(s, 3) = \Theta\left(\frac{s^2}{\log s}\right).$$