

Спецкурс 2020/2021: “Геометрические и
комбинаторные свойства матриц и аппроксимация”
Блок лекций “Сложность матриц и аппроксимация”
Лекция 1: “Коммуникационная сложность”

24 ноября 2020 г.

Коммуникационная сложность (Yao, 1979)

Пусть \mathcal{X}, \mathcal{Y} — два конечных множества, $f: \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$.

Рассмотрим задачу коммуникации. Есть два участника, Анна и Борис, их задача: по выданным x и y вычислить $f(x, y)$. Трудность в том, что x известно только Анне, а y — только Борису. Им разрешается обмениваться сообщениями: Анна посыпает $a_1 = A_1(x)$, Борис в ответ $b_1 = B_1(y, a_1)$, и т.д. Правило составления сообщений — протокол — должно гарантировать восстановление $f(x, y) = b_t$ на некотором шаге. Через $C(P)$ обозначим суммарную длину (в битах) сообщений в худшем случае, если используется протокол P . Минимально возможное значение $C(P)$ по всем протоколам называется **коммуникационной сложностью** f и обозначается через $C(f)$:

$$C(f) := \min_P \max_{(x,y) \in \mathcal{X} \times \mathcal{Y}} \sum_{i \leq t(P; x, y)} \text{len}(a_i(P; x, y)) + \text{len}(b_i(P; x, y)).$$

Формализации понятия протокола могут немного отличаться. Для нас это не играет роли, т.к. мы интересуемся величиной C с точностью до мультипликативной постоянной. Один из вариантов определения протокола: бинарное дерево, в каждой из вершин либо $A_v: \mathcal{X} \rightarrow \{0, 1\}$, либо $B_v: \mathcal{Y} \rightarrow \{0, 1\}$, в листе ответ.

Тривиальная оценка:

$$C(f) \leq \lceil \log_2 |\mathcal{X}| \rceil + 1.$$

Действительно, Анна кодирует элемент $x \in \mathcal{X}$ с помощью $\lceil \log_2 |\mathcal{X}| \rceil$ бит и отправляет Борису. Борис восстанавливает x и отправляет Анне $f(x, y)$.

Одноцветные прямоугольники

Получим оценку снизу на $C(f)$. Введём понятие *истории* сообщений: $h = (a_1, b_1, a_2, \dots)$. Для оптимального протокола всего не более $2^{C(f)}$ историй(*). Пусть $R_h = \{(x, y) \mapsto h\}$.

- f на R_h либо всюду 1, либо 0 (т.е. множество R_h “одноцветно”);
- R_h не пересекаются и их объединение есть $\mathcal{X} \times \mathcal{Y}$.
- R_h есть прямоугольник, т.е. имеет вид $I \times J$.

Поясним последнее свойство. Пара (x, y) попадает в историю $h = (a_1, b_1, \dots)$, когда выполнены условия:

$$A_1(x) = a_1, \quad B_1(y, a_1) = b_1, \quad A_2(x, a_1, b_1) = a_2, \dots$$

Т.е. условия распадаются на зависящие только от x (нечётные) и от y (чётные).

Через $\chi(f)$ обозначим минимальное количество f -одноцветных прямоугольников, на которые можно разбить $\mathcal{X} \times \mathcal{Y}$. Из вышесказанного следует:

$$\chi(f) \leq 2^{C(f)}.$$

Пример: EQ

Пусть $\mathcal{X} = \mathcal{Y}$ и $|X| = N$. Положим $\text{EQ}_N(x, y) = 1$, если $x = y$ и 0 иначе. Утверждение: $C(\text{EQ}_N) \asymp \log N$.

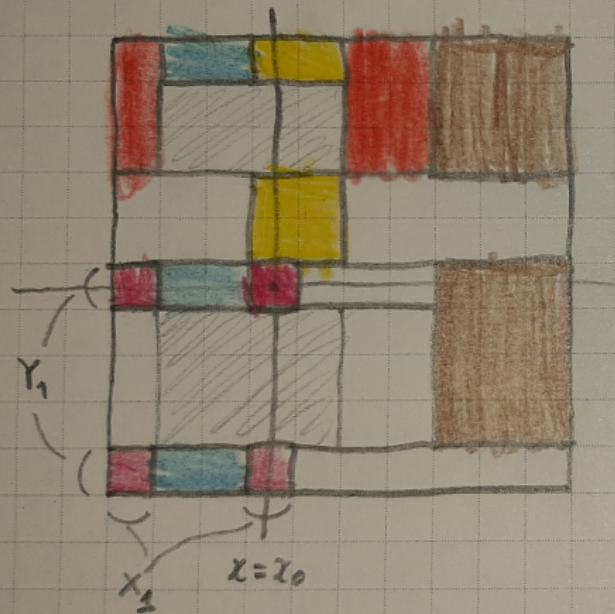
Оценка сверху тривиальна. Оценка снизу следует из $C(f) \geq \log_2 \chi(f)$. Рассмотрим разбиение на одноцветные прямоугольники.

Прямоугольник с $\text{EQ}_N = 1$ может содержать только одну точку (x, x) , следовательно, их не меньше N и $\chi(\text{EQ}_N) \geq N$.

Имеет место обратное неравенство (Aho, Ullman, Yannakakis, 1983):

$$C(f) \ll \log^2 \chi(f).$$

Упражнение. Докажите неравенство. (Анна и Борис должны определить прямоугольник, в котором находятся.)



$$R_i = X_i \times Y_i$$

$$i = 1, \dots, \gamma(f)$$

$$C(f) \ll \log^2 \gamma(f).$$

Связь с рангом

Занумеруем множества: $\mathcal{X} = \{x_1, \dots, x_M\}$ и $\mathcal{Y} = \{y_1, \dots, y_N\}$. Тогда функцию f можно отождествить с матрицей из $\{0, 1\}^{M \times N}$:

$$f \longleftrightarrow (f(x_i, y_j))_{\substack{1 \leq i \leq M \\ 1 \leq j \leq N}}.$$

Мы будем пользоваться матричной терминологией, не оговаривая этого особо.

Утверждение: $\chi(f) \geq \text{rank } f$. Действительно, матрица f представляется в виде суммы матриц $f|_{R_h}$. Каждая из них имеет ранг 1 в силу того, что R_h — одноцветный прямоугольник. Следствие:

$$C(f) \geq \log_2 \chi(f) \geq \log_2 \text{rank } f.$$

Пример. Для любой невырожденной $N \times N$ матрицы имеем $C(f) \asymp \log N$.

Нерешенные проблемы

Итак, $\log \chi(f) \ll C(f) \ll (\log \chi(f))^2$.

Проблема 1. Верно ли, что $C(f) \ll \log \chi(f)$?

Гипотеза. Верно ли, что $\log \chi(f) \ll \log \text{rank } f$?

Гипотеза была опровергнута в серии публикаций (Alon-Seymour, Raz-Spieker, Razborov).

Проблема 2 (log-rank гипотеза). Верно ли, что $\log \chi(f) \ll (\log \text{rank } f)^C$?

Вероятностные модели

Предположим, Анна и Борис имеют доступ к последовательностям случайных бит (достаточно большой длины) и могут использовать эти биты во время исполнения протокола (или: подбрасывать монету). Тогда результат работы протокола Q на входе (x, y) это случайная величина $Q(x, y)$.

Скажем, что протокол Q вычисляет f с ошибкой ε , если

$$\forall (x, y) \in \mathcal{X} \times \mathcal{Y} \quad P(Q(x, y) \neq f(x, y)) \leq \varepsilon.$$

(Ясно, что можно обеспечить $\varepsilon = 1/2$, просто бросая монетку.)

Минимальная сложность протокола, вычисляющего f с ошибкой $\leq 1/3$, обозначается $R(f)$ и называется *вероятностной коммуникационной сложностью* f в модели с ограниченной ошибкой. Ошибку $\varepsilon = 1/3$ можно превратить в $\varepsilon = 10^{-100}$, повторив действия достаточно большое количество раз.

Сложность вычисления EQ_N с ограниченной ошибкой

Theorem (Yao, Rabin)

$$R(\text{EQ}_N) \ll \log \log N.$$

Доказательство. Закодируем элементы \mathcal{X} двоичными векторами $x \in \{0, 1\}^n$, где $n = \lceil \log_2 N \rceil$. Вектор x отождествим с многочленом $x_1 + x_2\xi + \dots + x_n\xi^{n-1}$. Таким образом, у Анны и Бориса есть многочлены $g(\xi)$ и $h(\xi)$ и они хотят определить, равны ли эти многочлены.

Заранее фиксируется простое число $p \in [3n, cn]$. Анна выбирает случайное $\xi \in \{0, 1, \dots, p - 1\}$ и отправляет пару $(\xi, g(\xi) \bmod p)$ Борису. Борис вычисляет $h(\xi) \bmod p$ и выдаёт “1”, если значения совпали и “0” в противном случае.

По протоколу передаётся $\asymp \log p \asymp \log \log N$ бит, как и требовалось. Какова вероятность успеха?

Сложность вычисления EQ_N (продолжение)

Если $g = h$, то выдаётся “1” безо всякой ошибки.

Если $g \neq h$, то $g - h$ это ненулевой многочлен степени не выше n , он имеет не более n корней в \mathbb{F}_p , то есть количество ξ , таких что $g(\xi) = h(\xi)$, не превосходит $n \leq p/3$. Значит, вероятность ошибиться не больше $1/3$.

Дискрепанс

В детерминированной модели мы рассматривали f -одноцветные прямоугольники (и доказывали, что их должно быть много, т.к. они в том или ином смысле малы). В вероятностной модели нужно рассматривать произвольные прямоугольники R . Пусть $N_0(f, R)$ — количество точек в R , для которых $f = 0$, а $N_1(f, R)$ — количество точек с $f = 1$. Для нижних оценок сложности нам нужно доказать, что если прямоугольник большой, то он “сбалансированный”, то есть N_0 и N_1 близки друг к другу.

Дискрепансом функции $f: \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$ назовём величину

$$\text{disc}_u(f) = \max_R \frac{|N_0(f, R) - N_1(f, R)|}{|\mathcal{X}| \times |\mathcal{Y}|}.$$

Эта величина измеряет отклонение f от равномерного распределения, для семейства комбинаторных прямоугольников. Возможно обобщение на другие распределения μ на множестве $\mathcal{X} \times \mathcal{Y}$:

$$\text{disc}_\mu(f) = \max_R |\mu(R \cap \{f = 0\}) - \mu(R \cap \{f = 1\})|$$

(нам встретится эта величина позже).

Дискрепанс

$$\text{disc}_u(f) = \max_R \frac{|N_0(f, R) - N_1(f, R)|}{|\mathcal{X}| \times |\mathcal{Y}|}.$$

Если R — одноцветный прямоугольник, то $\text{disc}_u(f) \geq |R|/|\mathcal{X} \times \mathcal{Y}|$.
Суммируя по одноцветным прямоугольникам, получим
 $\chi(f)\text{disc}_u(f) \geq 1$, то есть

$$\chi(f) \geq 1/\text{disc}_u(f), \quad C(f) \geq \log_2(1/\text{disc}_u(f)).$$

Оказывается, имеет место намного более сильный результат:

$$R(f) \gg \log(1/\text{disc}_u(f)).$$

Пример: $\text{IP}_n(x, y) = \sum x_i y_i \bmod 2$, $x, y \in \{0, 1\}^n$.

Пусть M — матрица из $\{\pm 1\}^{N \times N}$. Дискрепанс определяется аналогично, как максимум по комбинаторным прямоугольникам R величины $N^{-2} |\sum_{(i,j) \in R} M_{i,j}|$. Применим линейную алгебру! Пусть $R = A \times B$, тогда дискрепанс равен

$$\begin{aligned} N^{-2} \left| \sum_{(i,j) \in R} M_{i,j} \right| &= N^{-2} |\mathbf{1}_A^t M \mathbf{1}_B| \leqslant \\ &\leqslant N^{-2} \|\mathbf{1}_A\|_2 \cdot \|\mathbf{1}_B\|_2 \cdot \|M\|_{2 \rightarrow 2} \leqslant N^{-2} |A|^{1/2} |B|^{1/2} \|M\|_{2 \rightarrow 2}. \end{aligned}$$

Следовательно, $\text{disc}_u(M) \leqslant N^{-1} \|M\|_{2 \rightarrow 2}$.

Рассмотрим матрицу W_n , соответствующую $2 \cdot \text{IP}_n - 1$ (т.е. значения $\{0, 1\}$ заменили на $\{-1, 1\}$). Получится так называемая матрица Уолша–Адамара. Нетрудно видеть, что строки матрицы ортогональны и их длина равна $2^{n/2}$. Следовательно, $\|W_n\|_{2 \rightarrow 2} = 2^{n/2}$. Значит, $\text{disc}_u(\text{IP}_n) = \text{disc}_u(W_n) \leqslant 2^{-n/2}$, откуда $R(\text{IP}_n) \gg n$.

В отличие от EQ_N , функция IP_n осталась сложной даже с разрешенной ограниченной ошибкой.

Таблица результатов

$U(f)$ — сложность с “неограниченной ошибкой” (вероятность успеха $> 1/2$).

f	$C(f)$	$R(f)$	$U(f)$
EQ	$\asymp \log N$	$O(\log \log N)$	$O(1)$
DISJ	$\asymp \log N$	$\asymp \log N$	$O(\log \log N)$
IP	$\asymp \log N$	$\asymp \log N$	$\asymp \log N$ (Forster)

Список литературы

- А.А. Разборов, “Коммуникационная сложность”.
- E. Kushilevitz, N. Nisan, “Communication complexity”.
- S. Arora, B. Barak, “Computational Complexity: A Modern Approach”.