

Спецкурс 2020/2021: “Геометрические и комбинаторные свойства матриц и аппроксимация”
Блок лекций “Сложность матриц и аппроксимация”
Лекция 8: “Сложность булевых функций, матриц и графов”

5 декабря 2020 г.

Функции, матрицы и графы

Напомним обозначение $[n] := \{1, 2, \dots, n\}$.

- Функция $f: [M] \times [N] \rightarrow \{0, 1\}$.
- Матрица $M_f \in \{0, 1\}^{M \times N}$, где $M_f(x, y) = f(x, y)$.

Нижние оценки $\text{rank } M_f$, $\text{rank}_{\pm} M_f$, $\text{rank}_{\varepsilon} M_f$ дают оценки снизу для различных вариантов коммуникационной сложности f . Используются методы линейной алгебры: нормы (Шаттена, операторные, γ_2), SVD, умножение Шура и Кронекера.

- Двудольный граф G_f с долями $X = [M]$, $Y = [N]$ и ребрами $x \rightarrow y$ для $f(x, y) = 1$.

Применим методы теории графов для получения оценок сложности G_f и ассоциированных с ним объектов f , M_f .

Матрица инцидентности

Вначале поговорим о связи между графами и матрицами. Пусть $G = (V, E)$ — произвольный неориентированный граф. Пронумеруем вершины: $V = \{v_1, \dots, v_n\}$.

Матрицей инцидентности графа G называется матрица $A = A(G)$ размера $n \times n$, такая что $A_{i,j} = 1$ тогда и только тогда, когда в графе есть ребро $v_i - v_j$.

Рассмотрим свойства матрицы инцидентности. Во-первых, $A(G)$ по определению симметрична и обладает вещественным спектром $\{\lambda_i(A)\}$. Отметим, что спектр не зависит от способа нумерации вершин; можно говорить о спектре графа: $\lambda_i(G)$.

Напомним, что степенью вершины в графе называется количество рёбер, которые из неё выходят: $\deg(v) = |\{e \in E : v \in e\}|$.

Свойства матрицы инцидентности

Утверждение

Пусть $G = (V, E)$ — неориентированный граф из n вершин, A — его матрица инцидентности. Выполнены свойства:

- $|\lambda_i(G)| \leq \max \deg(v)$;
- если G — двудольный граф и λ — собственное значение G , то $(-\lambda)$ тоже собственное значение, той же кратности;
- $\min \deg(v) \leq \lambda_{\max} \leq \max \deg(v)$;
- для индуцированного подграфа H имеем

$$\lambda_{\min}(G) \leq \lambda_{\min}(H) \leq \lambda_{\max}(H) \leq \lambda_{\max}(G).$$

Доказательство свойств

Докажем, что $|\lambda| \leq \max \deg(v)$ для всех собственных значений. Пусть x — собственный вектор с этим собственным значением. Считаем, что координата $|x_p|$ максимальна по модулю.

$$|(Ax)_p| = |\lambda| \cdot |x_p|,$$

$$|(Ax)_p| = \left| \sum_j A_{p,j} x_j \right| \leq \sum_j A_{p,j} |x_j| \leq \deg(v_p) |x_p| \leq \max \deg(v) \cdot |x_p|.$$

Докажем теперь симметричность спектра двудольного графа с долями V_1 и V_2 . Пусть $b_i = 1$ для $v_i \in V_1$ и $b_i = -1$ для $v_i \in V_2$. Рассмотрим изоморфизм $x \mapsto bx$. Пусть $Ax = \lambda x$, вычислим $A(bx)$.

Для $i: v_i \in V_1$ имеем

$$\begin{aligned} (A(bx))_i &= \sum_j A_{i,j} b_j x_j = \sum_{v_j \in V_1} A_{i,j} x_j - \sum_{v_j \in V_2} A_{i,j} x_j = - \sum_{v_j \in V_2} A_{i,j} x_j = \\ &= - \sum_{j=1}^n A_{i,j} x_j = -\lambda x_i = -\lambda (bx)_i. \end{aligned}$$

Доказательство свойств

Докажем, что $\min \deg(v) \leq \lambda_{\max} \leq \max \deg(v)$. Оценка сверху уже была доказана. Для оценки снизу заметим, что $\langle Ax, x \rangle \leq \lambda_{\max}$ для любого единичного x . Подставим $x = n^{-1/2}(1, 1, \dots, 1)$:

$$\frac{1}{n} \langle A\mathbf{1}, \mathbf{1} \rangle = \frac{1}{n} \sum_{k,l=1}^n A_{k,l} = \frac{1}{n} \sum_{k=1}^n \deg(v_k) \geq \min \deg(v).$$

Для доказательства $\lambda_{\max}(H) \leq \lambda_{\max}(G)$ нужно взять вектор, максимизирующий $\langle A_H x, x \rangle$.

Хроматическое число

Из доказанных свойств вытекает следствие.

Утверждение

Хроматическое число графа G оценивается величиной
 $\chi(G) \leq \lambda_{\max}(G) + 1$.

Действительно, для любого индуцированного подграфа H имеем $\min_{v \in V_H} \deg(v) \leq \lambda_{\max}(H) \leq \lambda_{\max}(G)$. Докажем, что если всегда $\min \deg \leq K$, то граф можно покрасить в $K + 1$ цвет.

Пусть x_n — вершина G степени не выше K . Положим $H_{n-1} = G - \{x_n\}$ и возьмём в нём вершину x_{n-1} , и т.д. В последовательности x_1, x_2, \dots, x_n каждый x_j соединяется не более чем с K вершинами перед ним. Значит, можно красить их жадным образом.

Сложность формул

Пусть $f: \{0, 1\}^n \rightarrow \{0, 1\}$ — булева функция от n переменных. Схемой, реализующей функцию f , называется ациклический ориентированный граф с n входными узлами (соответствующими переменным x_i), вычислительными узлами ($y_i \& y_j$, $y_i \vee y_j$, $\neg y_i$) и выходом, в котором должно вычисляться значение f .

Схема называется *формулой*, если промежуточные узлы нельзя переиспользовать — из каждого идёт только одно выходное ребро.

Сложностью $L(f)$ реализации f в виде формулы назовём минимальный размер формулы, вычисляющей f .

Сложность двудольных графов

Рассматриваем двудольные графы с фиксированными долями X и Y .
Граф отождествим со множеством его рёбер: $G \subset X \times Y$.

При определении сложности графа нужно задать “начальные” элементы, из которых он собирается, и элементарные операции (которые происходят в вычислительных узлах).

- операции: объединение и пересечение множества рёбер, т.е. для G_1 и G_2 можно вычислить $G_1 \cap G_2$ и $G_1 \cup G_2$;
- начальные элементы: графы вида $A \times Y$ и $X \times B$, множество таких графов обозначим \mathcal{B} ;

Аналогично булевым функциям, определяются схемы и формулы, вычисляющие данный граф. Будем обозначать $L_{\mathcal{B}}(G)$ сложность реализации графа в виде формулы с начальными элементами из \mathcal{B} .

Связь между сложностью функции и графа

Пусть f — булева функция от $2n$ переменных. Запишем её в виде $f: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ и рассмотрим соответствующий граф G_f .

Сравните функции и графы:

- Какие графы соответствуют функциям $f_1 \& f_2$, $f_1 \vee f_2$? Графы $G_{f_1 \cap f_2}$ и $G_{f_1 \cup f_2}$, соответственно.
- Какой граф у функции $f(x_1, \dots, x_n, y_1, \dots, y_n) = x_i$? А у функции y_j ? В первом случае это полный двудольный подграф вида $K_{N/2, N}$, $N = 2^N$.
- Как соотносятся сложности функции $L(f)$ и графа $L_B(G_f)$?

$$L_B(G_f) \leq L(f).$$

Что делать с отрицаниями? Поскольку это формула, то можно их загнать в переменные.

Итак, сложность двудольного графа даёт нижнюю оценку обычной сложности булевых функций.

Пример: функция чётности

Рассмотрим

$$f(x_1, \dots, x_n, y_1, \dots, y_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n \oplus y_1 \oplus \dots \oplus y_n.$$

Известно, что эту функцию нельзя вычислить схемой константной глубины, используя полиномиальное число узлов вида $\&$ и \vee (даже с произвольным кол-вом входов). Используя обычный базис, можно сделать формулу глубины $\asymp \log n$.

Какой вид имеет граф G_f ? Оцените его сложность.

$G_f = (A \times \bar{A}) \cup (\bar{A} \times A)$, где A это множество векторов $\{0, 1\}^n$ с чётным числом единиц.

Пример: матрица Адамара

Пусть H_n — матрица Уолша–Адамара размера $N \times N$, $N = 2^n$. Пусть G — соответствующий граф (проводим ребро $x - y$, если $H_n(x, y) = 1$).

Матрица Адамара сложные с точки зрения коммуникационной сложности (Forster: $\text{rank}_{\pm} H \geq \sqrt{N}$). Что можно сказать про граф?

Соответствующая булева функция имеет вид

$$f(x_1, \dots, x_n, y_1, \dots, y_n) = x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n.$$

Она вычисляется формулой с $O(n)$ элементами глубины $O(\log n)$.

Упражнение: придумайте схему константной глубины для вычисления графа.

Проективная и аффинная размерности графа

Дадим различные оценки сложности графов. Пусть $G = (V, E)$ — произвольный неориентированный граф.

Говорят, что задана *проективная реализация* графа $G = (V, E)$ в линейном пространстве U над полем \mathbb{F} , если для каждой вершины $v \in V$ задано линейное пространство $U_v \subset U$, так что

$$(v, w) \in E \iff U_v \cap U_w \neq \{0\}.$$

Проективной размерностью графа $\text{pdim}_{\mathbb{F}}(G)$ назовём минимальную размерность пространства U , в котором существует его проективная реализация.

Аналогично определяется *аффинная размерность*, только линейные пространства U_v заменяются на аффинные, а требование $U_v \cap U_w \neq \{0\}$ заменяется на $U_v \cap U_w \neq \emptyset$.

Связь между размерностями

Утверждение

- Для произвольного поля имеем $\text{adim}_{\mathbb{F}}(G) \leq \text{pdim}_{\mathbb{F}}(G)^2$.
- Над полем \mathbb{R} имеем $\text{adim}_{\mathbb{R}}(G) \leq \text{pdim}_{\mathbb{R}}(G) - 1$.

Известные оценки в обратную сторону намного слабее.

Пусть $\{U_v\}$, $U_v \subset \mathbb{F}^d$ — проективная реализация. Построим аффинную реализацию в пространстве матриц $\mathbb{F}^{d \times d}$.

Полагаем

$$W_v := \{A \in \mathbb{F}^{d \times d} : \text{строки } A \text{ лежат в } U_v \text{ и } \text{tr}(A) = 1\}.$$

Если $x \in U_{v_1} \cap U_{v_2}$, то можно взять матрицу с одной строкой, пропорциональной x , и остальными нулевыми. Если $A \in W_{v_1} \cap W_{v_2}$, то в A найдётся ненулевая строка, она принадлежит U_{v_1} и U_{v_2} .

Как получить из проективной реализации аффинную? Нужно пересечь всё с гиперплоскостью общего положения.

Theorem (Pudlák, Rödl, 1992)

Если булева функция f от $2n$ переменных вычислима программой с ветвлением размера S , то $\text{pdim}_{\mathbb{F}}(G_f) \leq S + 2$.

Программы с ветвлением (рисуем картинку!) по силе между булевыми формулами и булевыми схемами.

Theorem (Разборов, 1990)

Для любого двудольного графа имеем $L_B(G) \geq \text{adim}_{\mathbb{F}}(G)$.

Используя оценку Warren-а (см. лекцию 2), можно показать, что существуют графы с $\text{pdim}_{\mathbb{R}}(G) \geq c\sqrt{n/\log n}$.

Связь сложность графа и аппроксимативного ранга

В ряде случаев можно показать, что матрица инцидентности двудольного графа малой сложности имеет низкий аппроксимативный ранг. Рассмотрим пример.

Утверждение

Предположим, двудольный $N \times N$ граф G имеет вид

$$G = \bigcup_{i=1}^n A_i \times B_i, \quad A_i \subset X, B_i \subset Y.$$

Тогда для любого $\varepsilon \in (0, 1/2)$ найдётся матрица $M \in \mathbb{R}^{N \times N}$, такая что

- для всех $(x, y) \in X \times Y$ имеем $|G(x, y) - M(x, y)| \leq \varepsilon$,
- $\text{rank } M \leq \exp(C\sqrt{n} \log(2/\varepsilon) \log n)$.

Мы отождествляем граф G с его матрицей. Пусть $G_i = A_i \times B_i$. Ясно, что $G = G_1 \cup G_2 \cup \dots \cup G_n$ и $\text{rank } G_i = 1$. Для получения из G матрицы M нужно аппроксимировать функцию $y_1 \vee y_2 \vee \dots \vee y_n$.

Аппроксимация дизъюнкции

Для $x \in \{0, 1\}^n$ обозначим через $\text{OR}(x)$ функцию $x_1 \vee x_2 \vee \dots \vee x_n$.

Утверждение (в качестве упражнения)

Для любого $\varepsilon \in (0, 1/2)$ найдётся вещественный многочлен p от n булевых переменных степени не выше $Cn^{1/2} \log(2/\varepsilon)$, такой что для всех $x \in \{0, 1\}^n$, $|p(x) - \text{OR}(x)| \leq \varepsilon$.

Аппроксимация булевых функций многочленами — отдельная важная тема. Для $f: \{0, 1\}^n$ через $\deg_\varepsilon(f)$ обозначим минимальную степень полинома $p(x_1, \dots, x_n)$, аппроксимирующего f с точностью ε :

$$\|p - f\|_\infty \leq \varepsilon.$$

Определение $\deg_\varepsilon(f)$ вполне аналогично определению ε -ранга матрицы. Более того, есть и прямая связь. Скажем, если f — булева функция от $2n$ переменных, $d = \deg_\varepsilon(f)$, то матрица $M(x, y) = f(x, y)$, $x, y \in \{0, 1\}^n$, приближается матрицей $p(x, y)$, $\deg p \leq d$. Отсюда

$$\text{rank}_\varepsilon(M) \leq \sum_{k=0}^d \binom{2n}{k}.$$

Вернёмся к доказательству утверждения про $G = \cup A_i \times B_i$. Имеем $G = \cup G_i$, или $f_G = f_{G_1} \vee f_{G_2} \vee \dots \vee f_{G_n}$ в терминах функций.

Пусть полином p аппроксимирует $\text{OR}(y_1, \dots, y_n)$ с погрешностью ε , $\deg p \ll n^{1/2} \log(2/\varepsilon)$.

Подставим в p вместо y_i матрицу G_i , заменяя произведение на поэлементное умножение, т.е. $y_i y_j$ заменяется на $G_i \circ G_j$. Если матрицы A и B имеют ранг 1, то и $\text{rank}(A \circ B) = 1$. Следовательно, вместо монома $y_{i_1} \cdots y_{i_s}$ возникнет матрица $G_{i_1} \circ \cdots \circ G_{i_s}$ ранга 1.

Положим $M = p(G_1, \dots, G_n)$. Из вышесказанного следует, что $\|M - G\|_\infty \leq \varepsilon$ и

$$\text{rank } M \leq \sum_{j=0}^{\deg p} \binom{n}{j} \leq (en / \deg p)^{\deg p}.$$



P. Pudlák, V. Rödl, “A combinatorial approach to complexity”,
Combinatorica, 1992.