Конспект к лекции 5. (Санкт-Петербург, 9 апреля 2017 г.)

12 Спектральные экспандеры: теорема о существовании

Мы изучили разные свойства спектральных экспандеров, однако до сих пор не задавались вопросом о существовании таких графов. Напомним, что мы хотели бы иметь графы, у которых второе по абсолютной величине собственное число мало по сравнению с d. В этой главе мы докажем утверждение о существовании таких графов, хотя и не в самой сильной форме. (Теоремы о существовании, которую мы докажем, достаточно для большинства приложений).

Теорема 12.1 *Пусть $\gamma > 0$ — произвольное число. Тогда для достаточно больших d существует граф с $n = d^4$ вершинами степени d, у которого все собственные числа, кроме первого d, не превосходят по модулю γd.*

Доказательство: Мы докажем, что при определённом соотношении между числом вершин и числом рёбер *почти все* однородные графы обладают таким свойством. Слова «почти все» здесь означают, что при некотором естественном распределении вероятностей случайно выбранный граф оказывается спектральным экспандером (с нужными нам параметрами) с вероятностью близкой к единице.

Прежде всего опишем распределение вероятностей, которое мы будем использовать. Оно будет отличаться от распределения, использованного на первой лекции. Будем считать, что n (число вершин) чётно. Если n чётно, мы имеем право рассмотреть на n вершинах *совершенные паросочетания*. (Совершенное паросочетание есть такой набор из $n/2$ рёбер, что каждая из n вершин является концом ровно одного ребра. Другими словами, совершенное паросочетание на n вершинах есть граф степени 1, состоящий из $n/2$ рёбер.) Мы выбираем на n вершинах d случайных паросочетаний $P_1, \ldots, P_d$ (каждое из d паросочетантий выбирается равномерно; все d выборов делаются независимо). Объединением выбранных паросочетаний мы и будем считать графом G. Отметим, что в таком графе не может быт петель, однако могут быть кратные рёбра (поскольку одно и то же ребро может входить в несколько паросочетаний).

Мы обозначаем собственные числа полученного графа λ_i и считаем, что

$$d = |\lambda_1| \geqslant |\lambda_2| \geqslant \ldots \geqslant |\lambda_n|.$$

Теперь нам нужно оценить λ_2 — второе (по абсолютной величине) собственное число этого графа. При возведении матрицы в степень (мы выберем десятую степень) все собственные числа возводятся в ту же степень и след матрицы станет равным $\lambda_1^{10} + \lambda_2^{10} + \ldots + \lambda_n^{10}$. Первое слагаемое равно d^{10}; если для какой-то матрицы вся сумма близка к d^{10}, то все слагаемые кроме первого малы. А существование такой матрицы будет доказано, если мы убедимся что *среднее* значение следа матрицы M^{10} (для матрицы графа, выбранного случайно описанным выше способом) близко к d^{10}.

В нашем распределении вероятностей все вершины графа равноправны. След M^{10} равен сумме диагональных элементов, поэтому его среднее значение равно среднему значению одного элемента, умноженному на n. А среднее значение одного элемента равно среднему числу путей длины 10, начинающихся и заканчивающихся в данной вершине. Так что нам нужно доказать, что среднее число таких путей чуть больше, чем d^{10}/n.

Подсчёт удобно интерпретировать в терминах вероятностей. Будем считать, что помимо d паросочетаний $P_1, \ldots, P_d$ (напомним, что каждое из которых выбирается независимо, причём все паросочетания равновероятны) мы отдельно (и независимо) выбираем набор из 10 чисел $\omega = (\omega_1, \ldots, \omega_{10})$, каждое число от 1 до d. После этого мы (для фиксированной вершины графа) строим путь длины 10, выходящий из этой вершины. На первом шаге он идёт вдоль паросочетания P_{ω_1}, на втором — вдоль P_{ω_2}, и так далее. Нас интересует вероятность того, что после 10 шагов мы вернёмся в исходную точку. Точнее, мы хотим показать, что она равна $\frac{1}{n} \cdot (1 + o(1))$.

Поменяем порядок усреднения. Если усреднять сначала по выбору ω_i, то получается число петель длины 10 (делённое на d^{10}), которое затем можно усреднять по выбору P_i. Мы же проведём усреднение в другом порядке: сначала для каждого фиксированного набора ω_i мы усредняем по всем графам, и лишь потом усредняем по всевозможным наборам ω_i.

Все наборы $\omega = \omega_1, \ldots, \omega_{10}$ мы разделим на три категории:

1. гарантированно приводящие в исходную точку (независимо от выбора P_d); к этой категории относятся наборы, в которые после сокращений идущих подряд равных чисел ничего не остаётся;

2. наборы, состоящие из десяти разных чисел.

3. наборы, которые сокращаются не полностью, но в которых присутствуют равные числа (мы идём несколько раз по одному и тому же паросочетанию, но не обязательно подряд).

Для каждого из этих трёх типов наборов ω мы оцениваем количество таких наборов, а также (для каждого фиксированного набора) вероятность получить замкнутый путь при случайном выборе паросочетаний.

1. Количество наборов первого типа не превосходит $O(d^5)$. В самом деле, есть некоторое (фиксированное, так как длина цепочки — число 10 — фиксировано) число способов сокращения, и для каждого способа сокращения имеется не более d^5 способов его реализации (пять сокращающихся пар). Для каждого такого ω вероятность получить замкнутый путь равна 1 — какой бы граф мы не выбрали, путь с пометками ω обязательно приведет в исходную вершину.

2. Наборы без повторений составляют большинство из общего числа d^{10} (при достаточно больших значениях d). При этом вероятность того, что на последнем шаге цикл замкнётся, и мы вернемся в исходную вершину, не превосходит $1/(n-1) = \frac{1}{n} \cdot (1 + o(1))$, поскольку последнее ω_{10} число в наборе ранее не встречалось и соответствующее ω_{10} паросочетание независимо с предыдущими 9 шагами нашего пути.

3. Количество наборов второго типа есть $O(d^9)$, где константа в O-обозначении соответствует числу возможных пар позиций, где происходит совпадение (то есть $C_{10}^2 = 10 \cdot 9/2$).

   Докажем, что вероятность вернуться в исходную точку для такого набора есть $O(1/n)$. Разобьём это событие на случаи в зависимости от того, когда путь в первый раз возвращается в уже пройденную вершину и того, какой эта вершина была по счёту. Разных случаев снова будет не больше C_{10}^2, так что достаточно рассмотреть вероятность одного из них.

   В момент перед назначенным возвращением в уже пройденную вершину уже фиксированы некоторые рёбра некоторых паросочетаний (те, что использованы в пути), а следующее ребро (по которому мы должны попасть в уже посещённую вершину) ещё не фиксировано. Поэтому для его конца остаётся не менее $n - 10$ вариантов, и вероятность выбрать один из них не больше $1/(n-10) = O(1/n)$.

Осталось сложить оценки вероятности из трёх разобранных случаев. Получаем для среднего числа замкнутых путей оценку сверху

$$O\left(\frac{d^5}{d^{10}}\right) \cdot 1 + \frac{1}{n} \cdot (1 + o(1)) + O\left(\frac{d^9}{d^{10}}\right) \cdot O\left(\frac{1}{n}\right).$$

Если $n = d^4$, то второй член в этой сумме будет основным, и потому среднее значение следа есть

$$n \cdot d^{10} \cdot \frac{1}{n}(1 + o(1)) = d^{10}(1 + o(1)).$$

Следовательно, существуют и даже образуют большинство графы, у которых след десятой степени матрицы близок к d^{10} и потому все собственные числа (кроме первого) равны $o(d)$. Таким образом, теорема доказана.

Упражнение 12.1 *Докажите аналогичное утверждение для $n = d^8$.*

13 Спектр индуцированного подграфа и случайное блуждание на экспандерах

Мы уже видели, что спектральные экспандеры обладают свойствами «хорошего перемешивания». Даже один шаг случайного блуждания на спектральном экспандере заметно приближает исходное распределение вероятностей на вершинах к равномерному (см. лемму о перемешивании). В этом параграфе мы изучим свойства многошагового случайного блуждания на спектральном экспандере.

Теорема 13.1 *Пусть граф G является спектральным (n, d, γ)-экспандером и A — некоторое множество вершин графа, состоящее из αn вершин (для некоторого $\alpha > 0$). Тогда все собственные числа индуцированного подграфа*[1] *на вершинах A не превосходят $(\gamma + \alpha(1-\gamma))d$.*

Замечание: Даже если граф G однороден (все вершины имеют степень d), его индуцированный подграф может быть неоднородным. Однако матрица индуцированного подграфа симметрична, а значит, имеет собственный ортонормированный базис. Собственные числа графа оцениваются сверху максимальным значением отношения Рэлея. При этом нет необходимости отдельно выписывать в явном виде матрицу подграфа — поскольку мы рассматриваем *индуцированный* подграф в G, достаточно ограничить множество ненулевых координат распределения $\mathbf{f}$ на вершинах графа. Таким образом, если нас интересует индуцированный подграф, заданный множеством вершин A, мы должны изучить отношение Рэлея

$$\frac{|\mathbf{f}M\mathbf{f}^{\perp}|}{||\mathbf{f}||^2}$$

для всех ненулевых векторов $\mathbf{f}$, сосредоточенных на вершинах выбранного подграфа (координаты f для вершин, не принадлежащих A, должны быть равны нулю).

Лемма 13.1 *Пусть граф G является спектральным (n, d, γ)-экспандером с матрицей M и $\mathbf{f} = (f_1, \dots, f_n)$ некоторый вектор. Тогда*

$$\mathbf{f}M\mathbf{f}^{\perp} \leqslant \gamma d||f||^2 + \frac{d(1-\gamma)}{n}\left(\sum f_i\right)^2.$$

Доказательство: Обозначим $\mathbf{e}_1, \dots, \mathbf{e}_n$ ортонормрованный собственный базис для M и $\lambda_1, \dots, \lambda_n$ соответствующие собственные числа. При этом, как обычно, мы можем полагать первый собственный вектор $\mathbf{e}_1 = \frac{1}{\sqrt{n}}(1, \dots, 1)$ и первое собственное число $\lambda_1 = d$). Далее, разложим вектор $\mathbf{f}$ в сумму $\mathbf{f} = \mathbf{f}_{||} + \mathbf{f}_{\perp}$, где $\mathbf{f}_{||}$ параллелен, $\mathbf{f}_{\perp}$ перпендикулярен базисному вектору $\mathbf{e}_1$.

Заметим, что

$$\mathbf{f}_{||} = (\mathbf{f}, \mathbf{e}_1) \cdot \mathbf{e}_1 = \frac{\sum f_i}{\sqrt{n}}(1, \dots, 1).$$

Далее,

$$\mathbf{f}M\mathbf{f}^{\perp} = \mathbf{f}_{||}M\mathbf{f}_{||}^{\perp} + \mathbf{f}_{\perp}M\mathbf{f}_{\perp}^{\perp}.$$

[1]В индуцированном подграфе G_S множество вершин совпадает с A (некоторым подмножеством вершин исходного графа G), а в качестве рёбер берутся все рёбра графа G, оба конца которых принадлежат A.

Поскольку $\mathbf{f}_\perp$ лежит в подпространстве, натянутом на собственные векторы, собственные числа для которых не превосходят γd, мы получаем

$$|\mathbf{f}M\mathbf{f}^\perp| \leqslant d||\mathbf{f}_\|||^2 + (\gamma d)||\mathbf{f}_\perp||^2.$$

По теореме Пифагора мы имеем $||\mathbf{f}||^2 = ||\mathbf{f}_\|||^2 + ||\mathbf{f}_\perp||^2$. Следовательно,

$$|\mathbf{f}M\mathbf{f}^\perp| \leqslant d||\mathbf{f}_\|||^2 + (\gamma d)(||\mathbf{f}||^2 - ||\mathbf{f}_\|||^2).$$

Остаётся заметить, что $||\mathbf{f}_\|||^2 = \frac{(\sum f_i)^2}{n}$ (неравенство между средним арифметическим и средним квадратичным), и лемма доказана.

Доказательство теоремы 13.1: Рассмотрим вектор $\mathbf{f}$, у которого все координаты кроме тех, что соответствуют вершинам множества A, равны нулю. Согласно лемме 13.1 имеем

$$\mathbf{f}M\mathbf{f}^\perp \leqslant \gamma d||f||^2 + \frac{d(1-\gamma)}{n}\left(\sum f_i\right)^2.$$

Далее, из неравенства между средним арифметическим и средним квадратичным выкает следующая оценка для суммы $\sum f_i$ (в которой содержится не более αn ненулевых членов):

$$\sum f_i \leqslant \sqrt{[\text{число ненулевых членов в сумме}]} \cdot \sqrt{\sum f_i^2} \leqslant \sqrt{\alpha n}||\mathbf{f}||.$$

Соединяя два последних неравенства, мы получаем

$$\mathbf{f}M\mathbf{f}^\perp \leqslant \gamma d||f||^2 + d\alpha(1-\gamma)||f||^2.$$

Это позволяет нам оценить отношение Рэлея: для всех f с нулевыми координатами за пределами A мы имеем

$$\frac{|\mathbf{f}M\mathbf{f}^\perp|}{||\mathbf{f}||^2} \leqslant (\gamma + \alpha(1-\gamma))\, d,$$

что и даёт требуемое неравенство для собственных чисел индуцированного подграфа.

Теперь мы готовы доказать несколько утверждений о блуждании на экспандере.

Утверждение 13.1 *Пусть граф G является спектральным (n, d, γ)-экспандером и A — некоторое множество вершин графа, состоящее из αn вершин. Рассмотрим случайное блуждание по графу*

$$x_0 - x_1 - \ldots - x_t,$$

где вершина x_0 выбирается случайно (по равномерному распределению), а затем на каждом шаге $i = 1, \ldots, t$ следующая вершина x_i выбирается случайно (также равномерно) среди всех соседей x_{i-1}. Тогда

$$\mathrm{Prob}[x_i \in A \textit{ для всех } i] \leqslant (\alpha + \gamma(1-\alpha))^t.$$

Доказательство: Общее число путей $x_0 - x_1 - \ldots - x_t$, в графе G равно nd^t (имеется n вариантов для выбора первой вершины x_0 и по d вариантов для выбора каждого из t шагов). Нужно подсчитать, сколько из этих путей полностью лежат в A.

Обозначим $\mathbf{f}^{(i)} = (f_1^{(i)}, \ldots, f_n^{(i)})$ такой вектор, где $f_j^{(i)}$ есть число путей длины i, проходящих только по вершинам A и заканчивающимся в j-ой вершине графа G. В частности, в векторе $\mathbf{f}^{(0)}$ в позициях вершин A стоят единицы, а в позициях вершин вне A стоят нули.

Каждый следующий вектор $\mathbf{f}^{(i+1)}$ получается из $\mathbf{f}^{(i)}$ умножением на матрицу индуцированного подграфа. Поскольку собственные числа матрицы этого графа не превосходят $(\alpha + \gamma - \alpha\gamma)d$, мы получаем

$$||\mathbf{f}^{(t)}|| \leqslant ((\alpha + \gamma - \alpha\gamma)d)^t ||\mathbf{f}^{(0)}|| = ((\alpha + \gamma - \alpha\gamma)d)^t \cdot \sqrt{\alpha n}.$$

Применяем неравенство Коши и получаем, что сумма координат (L_1-норма) вектора $\mathbf{f}^{(t)}$ не превосходит

$$\sqrt{n} \cdot ||\mathbf{f}^{(t)}|| \leqslant \alpha(\alpha + \gamma - \alpha\gamma)^t \cdot (d^t n) \leqslant (\alpha + \gamma - \alpha\gamma)^t \cdot (d^t n).$$

Утверждение доказано.

Упражнение 13.1 *Для распределения вероятностей* $\mathbf{p} = (p_1, \ldots, p_n)$ *рассмотрим три варианта меры его «неопределённости»:*

(i) энтропия Шеннона $H(\mathbf{p}) = \sum\limits_{p_i \neq 0} p_i \log \frac{1}{p_i}$,

(ii) энтропия Реньи $H_2(\mathbf{p}) = -\log \left(\sum\limits_{i=1}^{n} p_i^2 \right)$,

(iii) min-энтропия $H_{\min}(\mathbf{p}) = \log \left(\min\limits_{p_i > 0} \frac{1}{p_i} \right)$.

Докажите, что для любого распределения вероятностей на спектральном (n, d, γ)*-экспандере величины энтропий* H*,* H_2 *и* $H_{\min}$ *не убывают на каждом шаге случайного блуждания.*