Конспект к лекции 1. (Санкт-Петербург, 8 апреля 2017 г.)

1 Используемые обозначения

Для неориентрированных графов мы используем обозначение $G = (V, E)$, где V есть множество вершин, а E — множество рёбер. При этом мы допускаем графы с петлями и с кратными (параллельными) рёбрами[1].

Если A и B являются подмножествами (возможно, пересекающимися) вершин графа, мы обозначаем $E(A, B)$ множество рёбер, у которых один из концов принадлежит A, а второй B. Также мы обозначаем $\Gamma(v)$ множество соседей вершины v (множество всех вершин w, соединённых с v ребром). Аналогичное обозначение используется для множеств вершин: если A есть подмножество вершин графа, то $\Gamma(A)$ обозначает множество всех соседей A, т.е.,

$$\Gamma(A) = \bigcup_{v \in A} \Gamma(v).$$

Векторы-строки мы обозначаем $\mathbf{x} = (x_1, \ldots, x_n)$. Транспонирование матрицы M мы обозначаем $M^\perp$; в частности, если $\mathbf{x} = (x_1, \ldots, x_n)$, то соответствующий вектор-столбец обозначается

$$\mathbf{x}^\perp = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

2 Двудольные экспандеры.

В этой главе мы рассмотрим самый простой вариант экспандера (расширяющего графа) — мы дадим определение двудольного экспандера и докажес существование таких графов (при некотором соотношении парамтеров).

Определение 2.1 *Двудольный граф $G = (L, R, E)$ (L и R — левая и правая доли графов, E — множество рёбер) называется двудольным $(n, m, d, k, \varepsilon)$-экспандером, если $|L| = n$, $|R| = m$, степень всех вершин в левой доле L равна d, и выполняется следующее свойство* расширения*: для любого множества $S \subset L$, $|S| \leqslant k$ множество соседей (соседи S лежат в R) достаточно велико: $|\Gamma(S)| > (1 - \varepsilon)d|S|$.*

Замечание: Чем меньше значение ε в этом определении, тем сильнее требование к графу. В приложениях как правило используют двудольные экспандеры с $\varepsilon < 1/2$. А для применения в теории кодирования (для построения

[1] Для графа с кратными рёбрами правильнее называть E не множеством, а *мультимножеством* рёбер, поскольку для каждой пары вершин в E может содержаться больше одного ребра с данными концами.

экспандерных кодов) часто требуются двудольные экспандеры с ещё меньшими значениями ε.

Теорема 2.1 *Пусть ε – некоторое положительное число. Тогда для любых n и $k \leqslant n$ найдется $d = O(\log n)$ и $m = O(dk)$ такие, что существует двудольный $(n, m, d, k, \varepsilon)$-экспандер.*

Замечание: Константы в $O(\cdot)$-обозначения в этой теореме зависят от ε.

Доказательство: Выберем граф случайно. Это значит, что для каждой вершины в L мы случайно и независимо выбираем d соседей в R (таким образом, разрешаются кратные рёбра). Покажем, что с большой вероятностью такой граф оказывается экспандером.

Граф *не* является экспандером, если некоторое множество вершин из левой доли графа $S \subset L$ (размера не более k) имеет не больше $(1-\varepsilon)d|S|$ соседей. Другими словами, все соседи S содержатся в некотором подмножестве правой доли графа $T \subset R$, состоящем из $(1-\varepsilon)d|S|$ вершин.

Поскольку при случайном выборе графа мы проводим все nd рёбер случайно и независимо, то для каждого ребра вероятность того, что его правый конец окажется в фиксированном множестве T, равна $|T|/m$. Следовательно,

$$\text{Prob[свойство экспандерности графа нарушено]} \leqslant \sum_{S,T} \left(\frac{|T|}{m}\right)^{sd},$$

где суммирование происходит по всем множествам $S \subset L$ размера не более k и по всем множествам $T \subset R$ размера $(1-\varepsilon)d|S|$. Оценим данную сумму сверху:

$$\sum_{s=1}^{k} C_n^s \cdot C_m^{(1-\varepsilon)sd} \cdot \left(\frac{(1-\varepsilon)sd}{m}\right)^{sd} \tag{1}$$

Оценивая биномиальные коэффициенты, получаем, что сумма не превосходит

$$\sum_{s=1}^{k} \left(\frac{ne}{s}\right)^{s} \cdot \left(\frac{me}{(1-\varepsilon)sd}\right)^{(1-\varepsilon)sd} \cdot \left(\frac{(1-\varepsilon)sd}{m}\right)^{sd} \leqslant$$
$$\leqslant \sum_{s=1}^{k} \left[\frac{ne}{s} \cdot \left(\frac{e^{(1-\varepsilon)/\varepsilon}(1-\varepsilon)sd}{m}\right)^{\varepsilon d}\right]^{s}. \tag{2}$$

Положим $m := Const \cdot kd$ (с достаточно большим значением $Const$), чтобы для всех возможных s выполнялось неравенство $\frac{e^{(1-\varepsilon)/\varepsilon}(1-\varepsilon)sd}{m} \leqslant 1/2$. Тогда выражение в квадратных скобках в правой части (2) не превосходит $ne \cdot (1/2)^{\varepsilon d}$. Остаётся выбрать d большим $\frac{1}{\varepsilon}\log(2en)$, и мы получаем

$$ne \cdot (1/2)^{\varepsilon d} < 1/2.$$

Таким образом, для выбранных значений параметров суммы (1) и (2) не превосходят 1. Это и означает, что с положительной вероятностью случайный двудольный граф является $(n, m, k, d, \varepsilon)$-экспандером. Теорема доказана.

Упражнение 2.1 *Докажите несколько более сильный вариант теоремы 2.1:*

(а) Gпри заданных параметрах n и k ($k \leqslant n$) существует существует двудольный $(n, m, d, k, \varepsilon)$-экспандер с $d = O(\log \frac{n}{k})$ и $m = O(\log dk)$ (усиление состоит в более точной оценке для степени графа d). Указание: выражение в квадратных скобках в правой части (2) можно оценить более точно.

(б) Докажите, что существует двудольный $(n, m, d, k, \varepsilon)$-экспандер с $d = O(\log \frac{n}{k})$ и $m = O(\log dk)$, в котором степени всех вершин в правой доле не превосходят $O(dn/m)$.

(в) Докажите, что существует двудольный $(n, m, d, k, \varepsilon)$-экспандер с $d = O(\log \frac{n}{k})$ и $m = O(\log dk)$, в котором все вершины в правой доле имеют одинаковую степень.

Упражнение 2.2 *Оцените асимптотику зависимости d и m от ε в теореме 2.1: как зависят степень графа и размер правой доли от параметра расширения ε?*

3 Однородный комбинаторный экспандер

В этой главе мы рассматриваем ещё один вариант комбинаторного определение экспандера. Мы определяем экспандер как однородный граф со свойством вершинного расширения — требуем, чтобы у каждого не сишком большого множества вершин графа имелось достаточно много соседей.

Определение 3.1 *Граф $G = (V, E)$ называется однородным комбинаторным (n, d, ε)-экспандером (расширяющим графом), если $|V| = n$ (в графе n вершин), степени всех вершин равны d (допускаются кратные ребра и петли), и выполняется следующее свойство* вершинного расширения*: для любого множества $S \subset V$, $|S| \leqslant n/2$ множество соседей S достаточно велико: $|\Gamma(S)| > (1 + \varepsilon)|A|$.*

Замечание 1: Чем больше значение ε в определении 3.1, тем более сильное свойство требуется от графа.

Замечание 2: Степень вершины графа — это число рёбер, для которых данная вершина является концом. Это определение распространяется и на петли (ребра, у которых концы совпадают). Таким образом, если некоторой вершине инцидентны d_1 рёбер, не являющихся петлями, и ещё d_2 петель, то степень этой вершины равна $d_1 + d_2$ (каждая петля учитывается с кратностью один, как и всякое другое ребро).

Теорема 3.1 *Пусть ε – некоторое положительное число меньшее 1. Тогда для всех достаточно больших четных d и всех n существует однородный (n, d, ε)-экспандер.*

Доказательство: Мы выберем граф случайно и покажем, что с положительной (и даже довольно близкой к 1) вероятностью такой граф оказывается экспандером. Отсюда будет следовать, что экспандеры существуют.

Прежде всего, нам нужно уточнить, что означает *случайный выбор графа*. Другими словами, нужно зафиксировать распределение вероятностей на графах. Мы выберем случайно $d/2$ перестановок π_i на множестве вершин графа,

$$\pi_i \ : \ \{1,\dots,n\} \to \{1,\dots,n\},\ i = 1,\dots,d/2.$$

(Каждая перестановка π_i выбирается среди $n!$ равновероятных вариантов; при этом все $d/2$ перестановок выбираются незамисимо друг от друга.) Ребрами графа будем считать все (неупорядоченные) пары вершин $\{v, \pi_i(v)\}$. Таким образом, из каждой вершины v выходит $d/2$ рёбер $\{v, \pi_i(v)\}$ и ещё $d/2$ рёбер $\{v, \pi_i^{-1}(v)\}$. У перестановок могут быть неподвижные точки (перестановка может оставлять некоторые вершины на месте), так что в случае $v = \pi_i(v)$ мы получаем петлю — ребро, оба конца которой совпадают с v. Чтобы степень каждой вершины была равна d, мы будем учитывать каждую петлю дважды.

Отметим, что в случайно выбранном графе с положительной вероятностью появляются кратные рёбра (поскольку одно и то же ребро $\{v, \pi_i(v)\}$ может получаться из нескольких перестановок π_i).

Теперь оценим вероятность того, что полученный в результате граф *не* окажется экспандером. Согласно определению, граф не является экспандером, если найдется множество вершин S (состоящее из не более, чем $n/2$ вершин), все соседи которого лежат в некотором множестве T, состоящем из $\lfloor (1+\varepsilon)|S| \rfloor$ вершин.

Зафиксируем некоторые множества вершин S и T. Зафиксируем номер перестановки π_i. Вероятность того, что для каждой вершины $v \in S$ второй конец ребра $\{v, \pi_i(v)\}$ попадёт в T, равна

$$\frac{|T|}{n} \cdot \frac{|T|-1}{n-1} \cdot \ldots \cdot \frac{|T|-|S|+1}{n-|S|+1} \leqslant \left(\frac{|T|}{n}\right)^{|S|}.$$

Поскольку мы выбираем $d/2$ перестановок независимо, вероятность того, что данное событие произойдёт для всех i, не превосходит $\left(\frac{|T|}{n}\right)^{(d/2)\cdot|S|}$. Таким образом,

$$\text{Prob[свойство экспандерности графа нарушено]} \leqslant \sum_{S,T} \left(\frac{|T|}{n}\right)^{(d/2)\cdot|S|},$$

где суммирование происходит по всем множествам вершин S размера не более $n/2$ и по всем множествам T размера $\lfloor (1+\varepsilon)|S| \rfloor$.

На самом деле интересующая нас вероятностью ещё меньше — чтобы свойство экспандерности нарушилось, для каждой вершины $v \in S$ все рёбра вида $\{v, \pi_i^{-1}(v)\}$ также должны попасть в T. Но мы не будем этого учитывать; рёбер вида $\{v, \pi_i(v)\}$ уже достаточно, чтобы получить нужную нам оценку на вероятность «неприятного» события.

Оценим интересующую нас сумму:

$$\sum_{S,T} \left(\frac{|T|}{n}\right)^{(d/2)\cdot|S|} \leqslant \sum_{s=1}^{n/2} C_n^s \cdot C_n^{(1+\varepsilon)s} \cdot \left(\frac{(1+\varepsilon)s}{n}\right)^{sd/2}. \tag{3}$$

Каждый биномиальный коэффициент C_n^k можно оценить сверху величиной $\left(\frac{ne}{k}\right)^k$ (см. упражнение 3.1 ниже). Таким образом, сумма (3) не превосходит

$$\sum_{s=1}^{n/2} \left(\frac{ne}{s}\right)^s \cdot \left(\frac{ne}{(1+\varepsilon)s}\right)^{(1+\varepsilon)s} \cdot \left(\frac{(1+\varepsilon)s}{n}\right)^{sd/2} =$$

$$= \sum_{s=1}^{n/2} \left[(s/n)^{d/2-2-\varepsilon} \cdot (1+\varepsilon)^{d/2} \cdot \frac{e^{1+\varepsilon}}{(1+\varepsilon)^{1+\varepsilon}}\right]^s. \tag{4}$$

Остаётся заметить, что $s \leqslant n/2$, а $1+\varepsilon < 2$. Таким образом, можно подобрать такое $d = d(\varepsilon)$, чтобы выражение в квадратных скобках в правой части (4) было меньше $1/2$ при всех значениях s. Следовательно, сумма (3) меньше единицы. А это и означает, что с положительной вероятностью случайный граф является (n, d, ε)-экспандером. Теорема доказана.

Упражнение 3.1 *Докажите оценку для биномиальных коэффициентов, которую мы использовали в доказательстве теоремы 3.1:*

$$C_n^k \leqslant \left(\frac{ne}{k}\right)^k,$$

где e — основание натурального логарифма.

Упражнение 3.2 *Оцените асимптотику зависимости $d = d(\varepsilon)$ в теореме 1: насколько большой должна быть степень графа, чтобы гарантировать существование экспандера с данным параметром расширения ε?*

Упражнение 3.3 *Докажите , что утверждение теоремы 3.1 выполнено для графов без петель: для любого $\varepsilon < 1$, для всех достаточно больших чётных d и всех n существует однородный комбинаторный (n, d, ε)-экспандер без петель.*

Следующее упражнение показывает, что $d = 3$ есть минимальная степень графа, для которой определение однородного комбинаторного экспандера имеет смысл.

Упражнение 3.4 *(а) Докажите, что для некоторого $\varepsilon > 0$ и всех достаточно больших чётных n существует однородный комбинаторный $(n, 3, \varepsilon)$-экспандер.*

(б) Докажите, что для всякого $\varepsilon > 0$ найдётся такое n_0, что при $n > n_0$ однородных комбинаторных $(n, 2, \varepsilon)$-экспандеров не существует.

Замечание: Не следует воспринимать определение 3.1 догматически — в некоторых случаях может оказаться удобно его немного подправить. В стандартном определении требуется, чтобы свойство расширения выполнялось для множеств, содержащих не более 50% от всех вершин графа. Выбор границы $n/2$ в определении достаточно произволен и не существенен для построения теории экспандеров. Для приложений иногда бывает удобнее потребовать, чтобы свойство расширения выполнялось лишь для достаточно малых множеств A (например, для множеств, содержащих не более 1% всех вершин графа) или, напротив, даже для достаточно больших множеств (например, для всех множеств, содержащих не более 99% всех вершин графа).

Упражнение 3.5 *Докажите, что для любого целого $d \geqslant 3$, любого $\delta > 0$ найдётся такое $\rho > 0$, что всех достаточно больших n, для большинства d-регулярных графов с n вершинами*

$$\min_{S \subset V,\ |S| \leqslant \rho n} \frac{|\Gamma(S)|}{|S|} \geqslant d - 1 - \delta$$

Объясните, почему оценку $(d - 1 - \delta)$ в правой части неравенства нельзя заменить на величну $d - \delta$.

4 Замечание об эффективных конструкциях

Когда мы говорим о экспандерных свойствах графа — вершинном или рёберном расширении, различных вариантах свойства «сильной связности» или «быстром перемешивании» (мы обсудим эти свойства в следующей главе) — возможные различные постановки вопроса:

1. Типичные свойства графа: каковы свойства «типичного», случайно выбранного графа? Например, что можно утверждать про коэффициент вершинного расширения для 99% графов степени d с n вершинами?

2. Экстремальные свойства графов: насколько сильными экспандерными свойствами может обладать граф? Например, насколько большим может быть коэффициент вершинного расширения для графа степени d с n вершинами?

3. Явные примеры экспандеров: для каких «конкретных», «явно описанных» графов можно оценить их эскадренные свойства? Нередко бывает проще показать, что некоторое комбинаторное свойство выполнено для 99% графов с n вершинам, чем доказать это же свойство для какого-то конкретного графа с простым описанием (например, заданного простой алгебрической формулой).

4. Алгоритмически эффективные конструкции: требуется найти экспандер, для которого не просто имеется «явное описание», но который может можно построить с помощью быстрого алгоритма.

Приведённые выше доказательства Теоремы 3.1 и Теоремы 2.1 неконструктивны. Эти рассуждения показывают, что экспандеры с заданными

параметрами существуют и, более того, *большинство* графов являются такими экспандерами. Однако эти доказательства не дают способа предъявить хотя бы один из экспандеров явно. Разумеется, мы можем перебрать все графы с заданным числом вершин и найти среди них экспандер. Но такой перебор потребует экспоненциального (от числа вершин) времени. Хуже того, даже для одного графа на n вершинах прямая проверка определения экспандера требует экспоненциального перебора (нужно перебрать все подмножества вершин и для каждого из них подсчитать число соседей).

В приложения (в теории сложности вычислений и в теории кодирования) как правило требуются алгоритмически эффективные конструкции экспандеров. При этом эффективность может пониматься в двух разных смыслах.

Конструкции эффективные в слабом смысле: экспандеры с n вершинами, которые можно построить за время $\mathrm{poly}(n)$. В данном случае «построить» граф означает, что мы должны предъявить некоторое стандартное описание этого графа (скажем, матрицу смежности или список всех его рёбер).

Конструкции эффективные в сильном смысле: экспандеры с $N = 2^{\Theta(n)}$ вершинами, простые операции с которыми можно производить за время $\mathrm{poly}(n)$. В таком графе каждая вершина задаётся индексом из $\Theta(n)$ битов; мы требуем, чтобы по индексу вершины можно было найти список всех её соседей (точнее, список *индексов* всех её соседей) за время $\mathrm{poly}(n)$. (Тут стоит напомнить, что мы интересуемся *разреженными* графами, в которых у каждой вершины сравнительно небольшое число соседей. Так что для каждой вершины размер списка её соседей будет очень коротким; трудность лишь в том, чтобы научиться эти списки быстро вычислять.)

Поиск эффективных конструкций экспандеров с параметрами, близкими к оптимальным, является одной из главных задач теории экспандеров.