Конспект лекций по курсу
***Алгоритмические задачи теории графов*, А. Ромащенко,**
мехмат МГУ, весенний семестр, 2011.

Лекция 1, 18 февраля.

Часть 1. Определение экспандера и пример его использования.

Мы начнём наш курс с определения 'расширящего графа' – экспандера. Экспандеры являются разреженными графами (т.е., в них сравнительно мало рёбер), но при этом обладают замечательными свойствами 'расширения', 'перемешивания', и т.д. Явные конструкции экспандеров нам потребуются в различных комбинаторных конструкциях. Экспандеры часто используются при дерандомизации — для явного построения комбинаторных объектов, существование которых можно доказать вероятностно.

Определение 1 (комбинаторное определение экспандера) *Мы будем называть $[n, d, \delta]$-экспандером неориентированный однородный граф с n вершинами, со степенью каждой вершины d, и следующим свойством рёберного расширения: для любого множества S, состоящего из не более чем $n/2$ вершин графа, число рёбер, ведущих из множества S в его дополнение, не меньше $\delta d|S|$ (обозначение: $E(S, \bar{S}) \geq \delta d|S|$).*

Иногда мы будем дополнительно требовать, чтобы экспандер имел правильную d-раскраску множества рёбер, т.е., чтобы рёбра графа можно было раскрасить в d цветов таким образом, чтобы любые два ребра с общим концом имели бы разные цвета.

В определении экспандера мы допускаем, чтобы граф имел кратные (параллельные) рёбра, но запрещаем петли.

Теорема 1 *Существует такое $\delta > 0$, что для всех $d \geq 3$, для всех достаточно больших чётных n существует $[n, d, \delta]$-экспандер с правильной d-раскраской рёбер.*

Упражнение 1: Докажите теорему 1. *Указание:* можно доказать, что случайно выбранный граф с большой вероятностью является экспандером. Случайный граф удобно выбирать так: возьмём n вершин и выпустим из каждой из них по d 'висячих' рёбер; при этом раскрасим рёбра, выходящие из каждой вершины, в d цветов. Затем для каждого из d цветов случайно разобъём n 'висячих рёбер' данного цвета на пары и соединим их. Про полученный граф можно доказать, что он с большой вероятностью обладает свойством рёберного расширения.

В данном упраженении нужно лишь доказать, что экспандры существуют. Для большинства применений требуются *явные* конструкции экспандеров, позоволяющие по номеру вершины быстро находить всех её соседей. На следующих лекциях мы рассмотрим эффективные способы построения

экспандеров. А пока рассмотрим простой пример использования таких графов.

Пример применения экспандеров: увеличение вероятности успеха в алгоритмах с датчиком случайных чисел.

Определение 2 *Язык L принадлежит сложностному классу* coRP*, если существует полиномиальный алгоритм A такой что*

1. *для всех $x \in L$ и для всех $r \in \{0,1\}^{poly(n)}$ $A(x,r) = 1$*
2. *для $x \notin L$ не менее, чем для половины всех $r \in \{0,1\}^{poly(n)}$ выполнено $A(x,r) = 0$*

Пусть для некоторого языка L имеется полиномиальный вероятностный алгоритм A с односторонней ошибкой ($L \in$ coRP). Мы докажем, что вероятность успеха можно улучшить, не увеличивая количества используемых случайных битов. А именно, для любого $\varepsilon > 0$ существует вероятностный алгоритм A', который использует столько же случайных битов, что и исходный алгоритм A, для всех $x \in L$ алгоритм A' всегда выдаёт правильный ответ, а для $x \notin L$ веротяность ошибки меньше ε.

Время работы алгоритма A' будет по-прежнему полиномиальным *в предположении, что используемый им экспандер (см. ниже) можно построить эффективно.*

Пусть исходный алгоритм A использует $k = k(n)$ случайных битов на входах длины n. Зафиксируем $[2^k, d, \delta]$-экспандер. Наборы случайных битов для A можно отождествить с вершинами данного графа. Пусть $R = R(\varepsilon, \delta)$ некоторое целое число (мы уточним его значение ниже).

Новый алгоритм A' действует следующим образом. Выбирается случайная вершина графа v; находятся все соседи v, соседи соседей, ..., и вообще все вершины графа, находящиеся на расстоянии не более R от v (вершины, в которые можно попасть из v по некотрому пути, состоящему из не более, чем R рёбер). Затем исходный алгоритм A последовательно запускается на всех наборах случайных битов, соответствующих выбранным вершинам (вершина v вместе с её R-окрестностью). Если все полученные ответы равны 1, новый алгоритм также возвращает единицу; в противном случае возвращается ноль.

Покажем, что у нового алгоритма веротяность ошибки мала. В самом деле, обозначим $B = B(x)$ множество таких вершин графа, для которых исходный алгоритм A возвращал неправильный ответ на входе x. Аналогично, обозначим $C = C(x)$ множество таких вершин v графа, для которых новый алгоритм даёт неверный ответ на входе x. Очевидно, C состоит из вершин, у которых вся их окрестность радиуса R лежит в B.

Поскольку само множество C содержится в B, в нём не может быть больше $2^k/2$ вершин (B состоит из наборов случайных битов, которые дают неверный ответ в алгоритме A; по условию их не более 50%). Следовательно, к множеству C применимо свойство расширения: $E(C, \bar{C}) \geq \delta d|C|$.

Следовательно, число соседей C не меньше $\delta|C|$ (не менее $\delta d|C|$ рёбер ведут из C наружу; при этом в каждую вершину–соседа C приходят не более d рёбер из C). Таким образом, размер множества C вместе с его соседями не меньше $(1+\delta)|C|$. Аналогично, C вместе с соседями и соседями соседей имеет размер не менее $(1+\delta)^2|C|$, и т.д. Таким образом, R-окрестность C содержит не менее $(1+\delta)^R|C|$ вершин. Следовательно,

$$|C| \le \frac{|B|}{(1+\delta)^R} \le \frac{(1/2)\cdot 2^k}{(1+\delta)^R}.$$

Теперь ясно, что можно выбрать такой радиус окрестности $R = R(\varepsilon, \delta)$, что число вершин в C будет не больше доли ε от общего числа вершин графа.

Отметим, что R не зависит от k, так что размер R-окрестности вершины графа ограничен (не зависит от k).

Для того, чтобы описанный выше алгоритм A' был полиномиальным, нам нужна явная конструкция экспандера в довольно сильном смысле. Размер использовавшегося графа был экспоненциален по k, и нам необходим алгоритм, который по заданному номеру вершины v (двоичное представление номера вершины состоит из k битов) за время $poly(k)$ находит список номеров всех соседей вершины v. На следующих лекциях мы опишем такую конструкцию графа.

Часть 2. Алгебраические экспандеры.

Нашей текущей задачей является эффективное построение экспандеров. Экспандер описывается *матрицей смежности* M, в которой m_{ij} равно числу рёбер, соединяющих вершины i и j. Эта матрица симметрична; сумма чисел в любой её строке или столбце равна d. На диагонали матрицы стоят нули (мы рассматриваем графы без петель).

Различные свойства графа удобно описывать в терминах этой матрицы:

- (i,j)-й элемент матрицы M^k есть число путей длины k, идущих из вершины i в вершину j;
- если разделить матрицу M на d, то получится матрица, у которой сумма любой строки и любого столбца равна 1 (дважды стохастическая матрица). Умножение на эту матрицу описывает случайное блуждание: если $\mathbf{p} = (p_1, \ldots, p_n)^T$ — это вектор-столбец, состоящий из вероятностей, описывающих распределение по вершинам в какой-то момент, то произведение $\frac{1}{d}M \cdot \mathbf{p}$ есть распределение через один шаг случайного блуждания (мы выбираем случайную вершину согласно распределению $\mathbf{p}$ и переходим к её соседу, выбрав случайно одно из d рёбер).

Отметим на будущее, что случайное блуждание по графу (из текущей вершины мы равновероятно переходим по одному из рёбер в другую вершину, и так далее) связано со степенями матрицы $\frac{1}{d}M$: чем ближе эти степени

к матрице равномерного перемешивания (в которой все элементы, включая диагональные, равны $1/n$), тем более равномерно распределен результат случайного блуждания. Изучать степени матрицы естественно в собственном базисе.

Заметим,что в терминах собственных чисел матрицы M удобно выражать некоторые комбинаторные свойства графа. Сделаем несколько несложных наблюдений:

Наблюдение 1: Матрица M симметрична и потому имеет ортогональный собственный базис над полем вещественных чисел, с вещественными собственными значениями.

Наблюдение 2: Поскольку сумма всех чисел в каждой строке равна d, вектор $(1, 1, \ldots, 1)$ (соответствующий столбец) является собственным вектором и имеет собственное значение d.

Наблюдение 3: Все собственные значения не превосходят d по модулю: поскольку суммы элементов во всех строках матрицы равны d, то максимум модулей собственного вектора при умножении на M увеличивается не более чем в d раз.

Наблюдение 4: Если граф состоит из нескольких компонент связности, то есть несколько собственных векторов с собственным значением d (для вершин в одних компонентах связности берём единицы, для других нули).

Наблюдение 5: Если граф связен, то собственный вектор со значением d единственный: возьмём максимальную по модулю координату этого вектора (вершину графа); она равна среднему арифметическому по всем своим соседям, а потому во всех соседях должно стоять такое же значение; то же верно для соседей соседей, и т.д.

Наблюдение 6: Для двудольного графа имеется собственный вектор со значением $-d$: для вершин в одной доле нужно взять единицы, а для вершин в другой доле минус единицы.

Наблюдение 7: Если имеется собственный вектор со значением $-d$, то граф имеет двудольную связную компоненту: возьмём максимальную по модулю координату; в её соседях будет то же число с противоположным знаком, и так далее. таком образом, связная компонента данной вершины делится на две доли.

Интересные комбинаторные свойства обнаруживаются у второго (по абсолютной величине) собственного значения графа. Мы увидим, что это собственное число связано со свойствами расширения и перемешивания в графе.

Определение 3 *Однородный граф степени d с n вершинами называется алгебраическим $[n, d, \alpha]$-экспандером, если все его собственные значения кроме максимального (которое в регулярном графе степени d обязательно равно d) не превосходят по модулю αd.*

Начнём мы с теоремы о связи между алгебраическим и комбинаторным определениями экспандера.

Теорема 2 (Теорема о рёберном расширении) *Во всяком алгебраическом $[n, d, \alpha]$-экспандере, для любого множества вершин S размера не более $n/2$, число рёбер, ведущих из множества S в его дополнение не меньше $(1 - \alpha)/2$.*

Лекция 2, 25 февраля.

Часть 3. От спектрального определения экспандера к комбинаторному.

Теорема 3 *Если граф G является алгебраическим $[n, d, \alpha]$-экспандером, то он является и комбинаторным $[n, d, \delta]$-экспандером для $\delta \geq \frac{1-\alpha}{2}$.*

Доказательство: Обозначим M матрицу графа. Мы уже знаем, что у этой матрицы есть собственный вектор $\mathbf{e}_1 = (1, \ldots, 1)$, соответствующий собственному числу $\lambda_1 = d$. Второе по модулю собственное число матрицы M можно представить как максимум отношения Релея по всем векторам, ортогональным $\mathbf{e}_1$:

$$(*) \qquad |\lambda_2| = \max_{0 \neq \mathbf{x} \perp (1,\ldots,1)} \left\{ \frac{\mathbf{x} M \mathbf{x}^T}{\|\mathbf{x}\|^2} \right\}$$

Теорема утверждает, что это отношение больше или равно

$$(**) \qquad d - 2 \cdot \min_{|A| \leq n/2} \frac{E(A, \bar{A})}{|A|}$$

(минимум по всем множествам A, состоящим из не более чем $n/2$ вергин графа). Выберем то самое множество вершин A, на котором этот минимум достигается. Для доказательства теоремы нам нужно построить такой вектор $\mathbf{x}$, что

(i) сумма координат $\mathbf{x}$ равна нулю (т.е., он ортогонален $\mathbf{e}_1$), и

(ii) отношение (*) не меньше $d - \frac{2E(A,\bar{A})}{|A|}$.

В качестве A мы возьмём вектор, у которого на позициях, соответствующих вершинам A стоит число $|\bar{A}|$, а остальные координаты равны $-|\bar{A}|$. Свойство (i) очевидно, остаётся проверить (ii).

Прежде всего, заметим, что $\|\mathbf{x}\|^2 = |A| \cdot |\bar{A}| \cdot n$. Далее, подситаем $\mathbf{x} M \mathbf{x}^T$. Вспоминая, что M есть матрица смежности графа, получаем

$$\mathbf{x} M \mathbf{x}^T = E(A, A) \cdot |\bar{A}|^2 + E(\bar{A}, \bar{A}) \cdot |A|^2 - 2E(A, \bar{A}) \cdot |A| \cdot |\bar{A}|$$

Поскольку сумма $|A|$ и $|\bar{A}|$ равна числу всех вершин в графе, эту сумму можно переписать как

$$\mathbf{x} M \mathbf{x}^T = n|A| \cdot |\bar{A}| \left(d - \frac{E(A, \bar{A})}{|A| \cdot |\bar{A}|} \right)$$

Разделив на квадрат модуля $\mathbf{x}$, получим

$$\frac{\mathbf{x} M \mathbf{x}^T}{\|\mathbf{x}\|^2} = \left(d - \frac{E(A, \bar{A})}{|A| \cdot |\bar{A}|} \right) \geq \left(d - \frac{2E(A, \bar{A})}{|A|} \right)$$

(в последнем неравенстве мы использовали, что A состоит из не более, чем $n/2$ вершин). Теорема доказана.

Замечание: Мы построили такой вектор $\mathbf{x}$, для которого величина $\mathbf{x}M\mathbf{x}^T$ положительна (и не меньше, чем (**)). Это не означает, что второе собственное число положительно. Второе (по абсолютной величине) собственное число графа может оказаться и отрицательным; мы лишь доказали, что $|\lambda_2|$ не может быть меньше значения (**).

Теорема th-alg-comb показывает, что алгебраический экспандер является и коминаторным (с некоторым параметром расширения). Верно и обратное: если граф удовлетворяет комбинаторному определеню экспандера, то можно доказать верхнюю оценку на его второе собственное число.

Теорема 4 *Если граф G является комбинаторным $[n, d, \delta]$-экспандером, то он также является и алгебраическим $[n, d, \alpha]$-экспандером для такого α, что $\delta \leq d\sqrt{2(1-\alpha)}$.*

Мы оставим эту теорему без доказательства.

Часть 4. Лемма о перемешивании (expander mixing lemma).

Лемма 1 *Пусть задан некоторый алгебраический $[n, d, \alpha]$-экспандер, и пусть A и B — произвольные (возможно, пересекающиеся) множества вершин этого графа. Тогда число $E(A, B)$ ребер, ведущих из A в B (сумма по $a \in A$ чисел рёбер из a в B или наоборот) удовлетворяет следующей оценке:*

$$\left| E(A,B) - \frac{d \cdot |A| \cdot |B|}{n} \right| \leq \alpha d \sqrt{|A| \cdot |B|}$$

Доказательство: Обозначим M матрицу графа, её собственные числа

$$d = \lambda_1 \geq |\lambda_2| \geq \cdots \geq |\lambda_n|,$$

а соответствующие собственные векторы $\mathbf{e}_2, \ldots, \mathbf{e}_n$. Будем считать, что векторы $\mathbf{e}_i$ образуют ортонормированный базис. Первый состенный вектор мы знаем: $\mathbf{e_1} = \frac{1}{\sqrt{n}}(1, \ldots, 1)$.

Обозначим $\mathbf{1}_A$ и $\mathbf{1}_B$ характеристические векторы множеств A и B соответственно (в этих векторах единицы стоят в позициях, соответствующих вершинам A и B, и нули на остальных местах). Отметим, что

$$\|\mathbf{1}_A\| = |A|, \text{ и } \|\mathbf{1}_B\| = |B|.$$

Далее, нам нужно подсчитать $E(A, B)$ (число рёбер графа, ведущих из A в B). Это значение можно представить как $\mathbf{1}_A M \mathbf{1}_B^T$. Чтобы оценить это число, разложим $\mathbf{1}_A$ и $\mathbf{1}_B$ по собственному базису:

$$\mathbf{1}_A = \sum_{i=1}^{n} a_i \mathbf{e_i}, \ \mathbf{1}_B = \sum_{i=1}^{n} b_i \mathbf{e_i}$$

Теперь число ребер между A и B можно представить в виде

$$E(A,B) = \mathbf{1}_A M \mathbf{1}_B^T = (\sum_{i=1}^{n} a_i \mathbf{e_i}) M (\sum_{i=1}^{n} a_i \mathbf{e}_i^T) = \sum_{i=1}^{n} \lambda_i a_i b_i$$

Ясно, что $a_1 = \frac{|A|}{\sqrt{n}}$ и $b_1 = \frac{|B|}{\sqrt{n}}$. Это значит, что

$$E(A,B) = d\frac{|A|}{\sqrt{n}} \cdot \frac{|B|}{\sqrt{n}} + \sum_{i=2}^{n} \lambda_i a_i b_i$$

Первое слагаемое даёт нам 'главный член' суммы; он равен $\frac{d|A|\cdot|B|}{n}$. Остаётся доказать, что все остальные слагаемые дают сравнительно небольшой вклад. Мы воспользуемся тем, что все собственные числа (кроме первого) по модулю не превосходят αd, а затем применим неравенство Коши–Буняковского:

$$\left| \sum_{i=2}^{n} \lambda_i a_i b_i \right| \leq \alpha d \sum_{i=2}^{n} |a_i| \cdot |b_i| \leq \alpha d \sum_{i=1}^{n} |a_i| \cdot |b_i| \leq \alpha d \sqrt{\|\mathbf{1}_A\|} \cdot \sqrt{\|\mathbf{1}_B\|}$$

Остаётся вспомнить, чему равны модули векторов $\mathbf{1}_A$ и $\mathbf{1}_B$. Собрав всё вместе, получаем, что разница между $E(A,B)$ и $\frac{d\cdot|A|\cdot|B|}{n}$ не превосходит $\alpha d\sqrt{|A|\cdot|B|}$. Лемма доказана.

Часть 5. Построение экспандера из аффинной плоскости.

Сейчас мы опишем 'явную' алгебраическую конструкцию алгебраического экспандера. Для него мы докажем очень хорошую оценку для второго собственного числа (а значит, и для коёффициента рёберного расширения). Недостатком этой конструкции явдяется большая степень графа: у графа с n вершинами степень будет равна $d = \sqrt{n}$, а второе собственное число $\lambda_2 = \sqrt{d}$. (Напомним: наша цель состоит в том, чтобы научиться строить экспандеры с ограниченной степенью $d = O(1)$).

Граф будет иметь наглядный геометрический смысл: это граф аффинной плоскости над конечным полем. Пусть q – пнекоторое ростое число. Рассмотрим граф AP_q, вершинами которого являются все пары $(a,b) \in \mathbb{Z}^2$, а рёбрами соединены такие вершины (a,b), (c,d), что

$$ac = b + d \ mod \ q$$

Полезно представлять себе пару (a,b) точкой аффинной плоскости над $\mathbb{Z}_q$, а (c,d) – прямой с уравнением $y = cx - d$, которая проходит через эту точку.

Таком образом, граф состоит из q^2 вершин, и степень каждой вершины равна q. Покажем, что второе по абсолютной величине собственное число графа равно $\sqrt{q}$.

Можно заранее догадаться, что данный граф обладает хорошими свойствами перемешивания. В самом деле, за два шага блуждания по такому

графу из любой вершины можно попасть в подавляющее большинство других вершин (первый шаг блуждания: от точки плоскости мы переходим к случайной прямой, проходящей через эту точку; второй шаг блуждания: от прямой мы переходим к случайной точке на ней). Какова бы ни была исходная точка, после двух шагов случайного блуждания мы получаем распределение, очень близкое к равномерному. Это означает, что вторая степень данного графа (которая и соответствует блужданию по графу AP_q по путям длины два) очень близка к полному перемешиванию. Поэтому удобно произвести спектральный анализ не для самого AP_q, а для его квадрата.

Обозначим M матрицу графа AP_q. Будем считать, что вершины (a, b) нумеруются сначала по первой, а потом по второй координате. Таким образом, матрица M состоит из q^2 квадратных блоков размера $q \times q$; в каждом таком блоке (i-ом по горизонтали, j-ом по вертикали) ребра соответствуют переходу из вершин вида $(i, *)$ в вершины $(j, *)$.

Матрицу M^2 нетрудно выписать в явном виде. Действительно, M^2 описывает пути длины 2 в графе AP_q. Если $i \neq j$, то есть ровно один такой путь из (i, k) в (j, l) (поскольку на плоскости есть ровно одна прямая, которая проходит через точки (i, k) и (j, l)). Если $k \neq l$, то из (i, k) в (i, l) нет путей длины два (поскольку мы не рассматриваем вертикальные прямые на плоскости). Наконец, из для каждой вершины (i, k) имеется q циклов длины два.

Таким образом, матрица M^2 имеет вид

$$\begin{pmatrix} qI & J & J & \dots & J \\ J & qI & J & \dots & J \\ \dots & \dots & \dots & \dots & \dots \\ J & J & J & \dots & qI \end{pmatrix}$$

где I — диагональная единичная матрица $q \times q$, а J — матрица $q \times q$, в которой на всех местах стоят единицы.

В тензорных обозначениях это можно записать так:

$$M^2 = I_{q\times q} \otimes (qI_{q\times q}) + (J_{q\times q} - I_{q\times q}) \otimes J_{q\times q}$$

У матрицы $I_{q\times q}$ все собственные числа равны единице; у $J_{q\times q}$ есть собственное число 1 кратности один и собственное число 0 кратности $(q-1)$. У этих матриц есть общий собственный базис (у матрицы I все векторы собственные!). Несложный подсчёт показывает, что у M^2 спектр состоит из чисел q^2 (кратность 1), 0 (кратность $(q-1)$) и q (кратность $q(q-1)$). Следовательно, у самой матрицы M второе собственное число равно $\sqrt{q}$.

Лекция 3, 4 марта.

Часть 6. Отступление: о графах Кэли.

Эту главу при чтении можно пропустить. Здесь мы объясним, откуда взялась конструкция экспандера, которую мы обсудим в следующей главе. Однако формально следующую главу можно будет понять и не разбираясь в общем определении графов Кэли и их свойствах.

Возьмём произвольную конечную группу G. Пусть $S \subset G$ — некоторое "симметричное" подмножество группы (т.е., для всякого элемента $x \in S$ обратный к x элемент группы x^{-1} тоже принадлежит S). Графом Кэли (Cayley) (G, S) называется граф, множество вершин которого совпадает с группой G, и вершины $x, y \in G$ соединены ребром, если и только если y получается из x умножением на некоторый элемент S. Другими словами, вершины (x, y) соединяются ребром при условии, что $x^{-1}y \in S$. Данное условие для x и y симметрично: поскольку множество S замкнуто относительно операции взятия обратного элемента, $x^{-1}y \in S$ тогда и только тогда, когда $y^{-1}x \in S$.

Для любых G, S такой граф не содержит кратных рёбер. Петли в этом графе есть, только если S содержит нейтральный элемент группы G. Мы будем интересоваться графами Кэли для конечных абелевых групп (хотя определение имеет смысл для произвольных G). Каждая вершина в графе Кэли имеет степень $|S|$.

Часто в определении графа Кэли предполагают, что множество S является порождающим (любой элемент группы можно получить, перемножая элементы S). Если добавить к нашему определению это дополнительное условие, то можно утверждать, что граф Кэли обязательно связен.

Пример 1. Рассмотрим в качестве G группу $\mathbb{Z}_2^n$ (т.е., строчки из n битов с операцией побитового XOR). В качестве S возьмём n образующих элементов вида $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$. Поскольку S симметрично (каждый элемент в данной группе является обратным для самого себя), мы можем рассмотреть граф Кэли (G, S). Нетрудно видеть, что это будет граф n-мерного куба: вершинами графа будут 2^n вершин куба, а рёбрами графа – рёбра куба.

Пример 2. Рассмотрим в качестве G группу $\mathbb{Z}_n$ (вычеты по модулю n с операцией сложения). В качестве S возьмём двухэлементное множество $\{1, n-1\}$. Граф Кэли (G, S) будет циклом из n вершин.

Для графов Кэли собственные числа удобно вычислять с помощью *характеров группы*. Напомним, что характером группы G называется гомоморфизм в мультипликативную группу комплексных чисел

$$\chi \ : \ G \to \mathbb{C} \setminus \{0\}$$

Из курса алгебры известно, что если группа G конечная и абелева, то имеется ровно $n = |G|$ различных характеров (n = число элементов в группе = число вершин в графе Кэли). Будем обозначать их χ_i, $i = 1, \ldots, n$.

Напомним некоторые свойства характеров:

- $\chi(xy) = \chi(x)\chi(y)$ для любых элементов группы x, y (немедленно следует из определения характера).
- Значения характеров лежат на единичной окружности в комплексной плоскости. Для группы порядка n значения характеров являются корнями n-ой степени из единицы.
- Ортогональность: для любых двух (несовпадающих) характеров χ_i, χ_j выполнено $\sum\limits_{g\in G} \chi_i(g)\cdot\overline{\chi_j(g)} = 0$. (Вспомните, как это доказывается!)
- Для конечной абелевой группа $G = \{g_1, \ldots, g_n\}$ векторы $(\chi_i(g_1), \ldots, \chi_i(g_n))$ (для всех характеров группы χ_i) образуют базис векторного пространства $\mathbb{C}^n$.

Собственные векторы графа (G, S) можно описать с помощью характеров. Матрица графа M имеет размер $n \times n$, и её строки и столбцы соответствуют вершинам графа (= элементам группы G). Собственными векторами этой матрицы будут

$$v_i = (\chi_i(g_1), \ldots, \chi_i(g_n))$$

Эти векторы образуют базис: они попарно ортогональны, их число равно размерности пространства. Остаётся проверить, что они являются собственными для матрицы графа. Это совсем просто: скалярное произведение j-ой строки M на вектор v_i есть сумма

$$\sum_{s\in S} \chi_i(g_j s) = \chi_i(g_j) \cdot \sum_{s\in S} \chi_i(s)$$

Таким образом, действуя оператором M на v_i, мы получаем тот же самый вектор v_i, но умноженный на коэффициент $\sum\limits_{s\in S} \chi_i(s)$. Так что мы не только нашли собственные векторы матрицы графа, но и вычислили собственные числа:

$$(*) \qquad \lambda_i = \sum_{s\in S} \chi_i(s),\ i = 1, \ldots, n.$$

Тривиальный характер χ_1 тождественно равен единице. Соответствующее собственное значение $\lambda_1 = \sum\limits_{s\in S} 1 = |S|$. Как и следовало ожидать, одно из собственных чисел оказалось равно степени графа $d = |S|$.

Если мы хотим, чтобы граф Кэли оказался хорошим экспандером, то нам нужно сделать поменьше все собственные числа кроме λ_1. Это значит, что нам нужно подобрать такое множество S, чтобы сумма (*) для всех характеров кроме тривиального (тождественно равного единице) была как можно меньше. Можно доказать, что для любой конечной группы G, для случайно выбранного S (размера порядка $\Theta(\log n)$) полученный граф Кэли будет алгебраическим экспандером с достаточно малым вторым собственным числом.

Если нам нужна алгоритмически эффективная конструкция экспандера, то группу G и множество S нужно указать явно. Выбор G и подходящего $S \subset G$ является определённым искусством. В следующей главе мы рассмотрим конкретный пример — граф Кэли для $G = \mathbb{F}^{r+1}$ (линейное пространство размерности $(r+1)$ над полем $\mathbb{F}$ характеристики 2) и

$$S = \{y \cdot (1, x, \ldots, x^r) \ : \ x, y \in \mathbb{F}\}.$$

В соответствующем графе Кэли число вершин $n = |\mathbb{F}|^{r+1}$ и степень $d = |S| = |\mathbb{F}|^2$. Мы покажем, что все собственные числа этого графа (кроме тривиального, равного d) не превосходят $r|\mathbb{F}| = r\sqrt{d}$.

Часть 7. Графы $LD(q, r)$ и их собственные числа.

В этой главе мы опишем явную конструкцию графов $LD(q, r)$ с достаточно малым вторым собственным числом. Степень графа в этой конструкции будет довольно большой. Однако в дальнейшем мы используем графы $LD(q, r)$ в качестве "строительных блоков" для изготовления экспандеров с нужными нам параметрами.

Пусть $q = 2^t$. Рассмотрим поле $\mathbb{F}_q$ из q элементов (характеристика этого поля равна двум). В качестве вершин графа $LD(q, r)$ мы возьмём все строки $(a_0, a_1, \ldots, a_r) \in \mathbb{F}_q^{r+1}$; таким образом, в графе будет $n = q^{r+1}$ вершин.

Мы соединяем ребром вершины $a = (a_0, a_1, \ldots, a_r)$ и $b = (b_0, b_1, \ldots, b_r)$, если

$$b = a + y \cdot (1, x, \ldots, x^r)$$

для некоторых $x, y \in \mathbb{F}$. (Поскольку характеристика поля равна двум, прибавление и вычитание в поле совпадают; условия $b = a + y \cdot (1, x, \ldots, x^r)$ и $a = b + y \cdot (1, x, \ldots, x^r)$ эквивалентны.) Таким образом, степень каждой вершины графа будет равна q^2.

Теорема 5 *Все собственные числа графа $LD(q, r)$ кроме первого не превосходят rq.*

Доказательство: Выберем некоторой невырожденный линейный функционал $L \ : \ \mathbb{F} \to \mathbb{Z}_2$ (значения этого функционала мы иногда будем понимать как элементы поля $\mathbb{F}$, а иногда как целые числа ноль или один). С помощью L можно явно описать собственные векторы графа $LD(q, r)$. И самих собственных векторов, и координат в каждом векторе должно быть $n = q^{r+1}$. Поэтому удобно нумеровать и векторы, и их координаты вершинами графа, т.е., строчками $a = (a_0, \ldots, a_r) \in \mathbb{F}_q^{r+1}$.

Собственный вектор "номер" a мы обозначаем $v_a = (\ldots)$. В его b-ой позиции (для $b = (b_0, \ldots, b_r)$) будет стоять число

$$(-1)^{L(\sum_{i=0}^{r} a_i b_i)}$$

(т.е. собственные векторы состоят из плюс и минус единиц).

Из определения легко следует следующее свойство: для любых a, b, c из $\mathbb{F}_q^r$

$$v_a(b+c) = v_a(b) \cdot v_b(c).$$

Пояснение для тех, кто прочитал предыдущую главу: *Отображения*

$$\chi_b \ : \ \mathbb{F}_q^{r+1} \to \{1, -1\},$$

заданные как $\chi_b(a) = (-1)^{L(\sum\limits_{i=0}^{r} a_i b_i)}$ *являются характерами абелевой группы* $\mathbb{F}_q^{r+1}$ *(группа в данном случае – это линейное пространство размерности* $r+1$ *над полем* $\mathbb{F}_q$*, с операцией сложения). Поскольку характеристика поля* $\mathbb{F}$ *равна двум, характеры принимают только два значения: плюс и минус единица. Ниже мы докажем все необходимы нам свойства этого отображения непосредственно, не ссылаясь на общие свойства характеров.*

Теперь проверим, что все векторы v_a попарно ортогональны. Это несложно: для любых a, a' скалярное произведение v_a и $v_{a'}$ равно

$$\sum_{b=(b_0,\ldots,b_r)} (-1)^{L(\sum\limits_{i=0}^{r} a_i b_i)} \cdot (-1)^{L(\sum\limits_{i=0}^{r} a'_i b_i)} = \sum_{b=(b_0,\ldots,b_r)} (-1)^{\sum\limits_{i=0}^{r} L((a_i+a'_i)b_i)}$$

Нам инетересен случай $a \neq a'$. Пусть, для определённости, $a_0 \neq a'_0$. Тогда $a_0 + a'_0 = 1$, и скалярное произведение равно

$$\sum_{b_0} (-1)^{L(b_0)} \cdot \sum_{(b_1,\ldots,b_r)} (-1)^{\sum\limits_{i=1}^{r} L((a_i+a'_i)b_i)}$$

Когда b_0 пробегает все значения $\mathbb{F}$, невырожденный линейный функционал L принимает одинаковое число раз значения 0 и 1. Поэтому в первой сумме мы складываем одинаковое число $+1$ и -1. Это значит, что скалярное произведение v_a и $v_{a'}$ равно нулю (векторы попарно ортогональны).

Осталось проверить, что данные векторы v_a действительно являются собственными векторами графа. Обозначим матрицу графа M. Умножая M на v_a мы получим некоторый вещественный вектор размерности n (как и раньше, удобно нумеровать его компоненты строчками $b = (b_0, \ldots, b_r)$, соответствующими вершинам графа). Тогда b-ая компонента вектора $M \cdot v_a$ равна

$$(Mv_a^T)(b) = \sum_{c \in \mathbb{F}_q^{r+1}} M_{bc} v_a(c) = \sum_{x,y \in \mathbb{F}_q} v_a(b + y(1, x, \ldots, x^r)) = \left(\sum_{x,y \in \mathbb{F}_q} v_a(y \cdot (1, x, \ldots, x^r)) \right) \cdot v_a(b)$$

Таким образом,

$$Mv_a^T = \left(\sum_{x,y \in \mathbb{F}_q} v_a(y \cdot (1, x, \ldots, x^r)) \right) \cdot v_a^T$$

Мы не только доказали, что v_a является собственным вектором, но и вычислили собственное значение

$$\lambda_a = \sum_{x,y \in \mathbb{F}_q} v_a(y \cdot (1, x, \ldots, x^r))$$

Осталось понять, что же это за число.

Обозначим $p_a(x) = a_0 + a_1 x + \ldots + a_r x^r$ (многочлен от x степени не более r). Значение λ_a можно переписать в виде

$$\lambda_a = \sum_{x,y \in \mathbb{F}_q} (-1)^{L(y \cdot p_a(x))}$$

Разобьём эту сумму на две части: на те x, на которых многочлен $p_a(x)$ обращается в ноль, и на все остальные.

$$\lambda_a = \sum_{x : p_a(x) = 0} \sum_y (-1)^{L(y \cdot p_a(x))} + \sum_{x : p_a(x) \neq 0} \sum_y (-1)^{L(y \cdot p_a(x))}$$

В первой сумме $L(y \cdot p_a(x))$ всегда равно нулю. А во второй сумме, когда y пробегает все элементы поля, произведение $y \cdot p_a(x)$ тоже пробегает все элементы $\mathbb{F}_q$; при этом функционал L равное число раз принимает значения 1 и 0. Следовательно,

$$\lambda_a = \sum_{x : p_a(x) = 0} \sum_y 1 + \sum_{x : p_a(x) \neq 0} \sum_{z \in \mathbb{F}_q} (-1)^{L(z)} = q \cdot [\text{ число корней } p_a(x) \text{ }] + 0$$

Если $a = (0, 0, \ldots, 0)$, то многочлен $p_a(x)$ тождественно равен нулю, и соответствующее собственное число равно q^2 (= степень графа). Для всех остальных a многочлен $p_a(x)$ имеет не более r корней, и $0 \leq \lambda_a \leq rq$.

Часть 8. Подстановочное произведение.

В этой главе мы опишем способ строить экспандеры с большим числом вершин из нескольких маленьких. Для этого мы определим особое произведение графов. С помощью этого произведения мы сможем изготавливать экспандеры нужного нам размера из маленьких "строительных блоков". Подходящего вида строительные блоки мы иногда будем находить перебором, а иногда будем использовать построенные выше графы AP_q и $LD(q, r)$.

Пусть даны графы G_1 и G_2; пусть G_1 состоит из n вершин, и все вершины имеют степень D, а G_2 состоит из D, и все они имеют степень d. Мы определим *подстановочное произведение* этих графов $G_3 = G_1 \circ G_2$; новый граф будет иметь nD вершин, и все они будут иметь степень $2d$.

Чтобы построить $G_1 \circ G_2$, мы заменим каждую вершину графа G_1 копией второго графа, прикрепив рёбра первого графа к вершинам второго. Это можно сделать, поскольку в маленьком графе как раз нужное число вершин. В таком прикреплении есть определённый произвол — конкретный выбор соответствия в каждой вершине G_1 не играет роли. Получился

граф с nD вершинами и рёбрами двух сортов — рёбрами, унаследованными из первого графа и рёрами, скопированными из второго. Возьмём каждое ребро первого сорта с кратностью d. Теперь в полученном графе из каждой вершины выходит $2d$ рёбер: d *локальных* (перенесённых из G_2) и d *глобальных* (копии одного из рёбер G_1). Построенный граф и называется подставновочным произведением G_1 и G_2.

Теорема 6 *Если G_1 является комбинаторным экспандером с параметрами $[n, D, \delta_1]$, а G_2 — комбинаторным экспандером с параметрами $[D, d, \delta_2]$, то их подстановочное произведение $G_3 = G_1 \circ G_2$ является комбинаторным экспандером с параметрами $[nD, 2d, \varepsilon]$ для некоторого $\varepsilon > \frac{\delta_1^2\delta_2}{120}$.*

Доказательство: Пусть S некоторое множество вершин нового графа, $|S| \leq nD/2$. Мы должны доказать, что в графе G_3 число рёбер в $E(S, \bar{S})$ не менее $\frac{\delta_1^2\delta_2}{120} \cdot (2d)|S|$.

Вершины G_3 состоят из n 'галактик' (соответствующих вершинам графа G_1) по D вершин в каждой. Обозначим эти галактики $C_1, \ldots, C_n$. Множество S представляется в виде дизъюнктного объединения

$$S = S_1 \cup \ldots \cup S_n,$$

где $S_i = S \cap C_i$ (S_i состоит из тех вершин S, которые попали в i-ую галактику). Галактики разделим на два сорта: 'неполные', в которых не очень много вершин из S, и 'почти полные', которые почти полностью состоят из вершин множества S. Нужно выбрать условную границу, отделяющую полные галактики от и неполных. Удобно будет это сделать так: галактика объявляется *неполной*, если $|S_i| \leq (1 - \frac{\delta_1}{4})D$, и *полной* в противном случае.

Всё множество S делится на две части: $S = S' \cup S''$, где S' состоит из точек в неполных галактиках, а S'' — из точек, которые попали в полные галактики.

1-ый случай: предположим, что $\geq \frac{1}{10}\delta_1|S|$ точек S принадлежат неполным галактикам (множество S' достаточно велико). Покажем, что тогда только за счёт одни лишь 'локальных' рёбер внутри неполных галактик набирается достаточно много рёбер, ведущих из S в $\bar{S}$. Мы воспользуемся следующей простой леммой:

Лемма 2 *Если множество вершин A в $[k, d, \rho]$-экспандере имеет размер αk, то*

$$E(A, \bar{A}) \geq \min\{\alpha, (1 - \alpha)\}\rho dk.$$

Доказательство леммы: Если $\alpha \leq 1/2$, мы применяем свойство рёберного расширения к самому множеству A. В противном случае применяем свойство рёберного расширения к дополнению A.

Внутри каждой неполной галактики содержится не более $(1 - \frac{\delta_1}{4})D$ вершин из S. Применяем Лемму 2 к каждому множеству S_i внутри неполной

галактики (напомним: внутренние рёбра галактики — это рёбра графа G_2). Получаем, что число рёбер $E(S_i, C_i \setminus S_i)$ не меньше

$$\delta_2 d \cdot \frac{\delta_1}{4}|S_i|.$$

Суммируя количество таких рёбер по всем неполным галактикам, получаем

$$\delta_2 d \cdot \frac{\delta_1}{4}|S'| \geq \frac{\delta_1^2\delta_2}{80} \cdot (2d)|S|$$

(тут мы использовали условие $|S'| \geq \frac{1}{10}\delta_1|S|$). Первый случай мы рассмотрели.

2-ой случай: предположим, что $< \frac{1}{10}\delta_1|S|$ точек S попали в неполные галактикам (множество S' достаточно мало). В этом случае нужное нам число рёбер из S в $\bar{S}$ наберётся среди 'межгалактических' рёбер. Причём достаточно учесть только те рёбера, которые выходят из точек множества S в полных галактиках и приходят в точки $\bar{S}$ в неполных.

Оценим число *полных* галактик. С одной стороны, оно не больше, чем число всех вершин в S, делённое на минимальное число вершин, разрешённое для полной галактики. С другой стороны, он не меньше, чем размер S'', делённый на число всех вершин в каждой из галактик. Получаем

$$\frac{9}{10} \cdot \frac{|S|}{D} \leq \frac{|S''|}{D} \leq [\text{ число полных галактик }] \leq \frac{|S|}{(1-\frac{\delta_1}{4})D} \leq \frac{nD/2}{(3/4)D} = \frac{2}{3}n$$

Применяем лемму 2 к 'межгалактическим' рёбрам (вспоминаем, что граф G_1 является экспандером с параметром δ_1, и учитываем, что каждое 'межгалактическое' ребро имеет кратность d). Поучаем, что этих рёбер не меньше

$$\delta_1 dD \cdot \min\{[\text{ число полных галактик }], [\text{ число неполных галактик }]\} \geq \delta_1 dD\frac{|S''|}{2D} \geq \frac{9\delta_1(2d)|S|}{40}$$

Как мы увидим, большинство этих рёбер ведут из S в $\bar{S}$. Однако часть рёбер нужно всё же вычесть. Во-первых, нужно исключить из этой суммы рёбра, выходящие из немногочисленных вершин из $\bar{S}$, которые попали в полные галактики. Таких рёбер не больше

$$\frac{\delta_1 D}{4} \cdot d \cdot [\text{ число полных галактик }] \leq \frac{\delta_1 D}{4} \cdot d \cdot \frac{|S|}{\frac{3}{4}D} \leq \frac{\delta_1(2d)|S|}{6}$$

Во-вторых, нужно вычесть межгалактические рёбра, которые соединяют полную и неполную галактики, но в в неполной галактике попадают в вершину S. Таких рёбер заведомо не больше

$$d|S'| \leq d \cdot \frac{1}{10}\delta_1|S| \leq \frac{\delta_1(2d)}{20}|S|.$$

Получаем, что среди межгалактических рёбер найдётся не меньше

$$\frac{9\delta_1(2d)|S|}{40} - \frac{\delta_1(2d)|S|}{6} - \frac{\delta_1(2d)}{20}|S| = \frac{\delta_1 \cdot 2d}{120}|S|$$

таких, которые ведут из S в $\bar{S}$.

Остаётся объединить результаты случая 1 и случая 2. Положим $\varepsilon := \min\{\frac{\delta_1^2\delta_2}{80}, \frac{\delta_1}{120}\} \geq \frac{\delta_1^2\delta_2}{120}$, и теорема доказана.

Лекция 4, 11 марта.

Часть 9. Явная (в слабом смысле) конструкция экспандера.

У нас готова вся необходимая техника для "явного" построения экспандеров. Сейчас мы опишем конструкцию (комбинаторного) экспандера с n вершинами, который можно построить за время $\mathrm{poly}(n)$.

Теорема 7 *Существует $\delta > 0$ такое, что для всех достаточно больших степеней двойки $q = 2^t$ и для любого целого r такого, что*

$$q^2 \le r \le q^4/4,$$

существует комбинаторный экспандер с параметрами $[n = q^{4r+12}, 12, \delta]$, и построить его (выписать матрицу инцидентности) можно за время $\mathrm{poly}(n)$.

Доказательство:

Мы получим интересующий нас граф в виду подстановочного произведения трех сравнительно небольших графов

- G_1: комбинаторный экспандер с парамтерами $[q^2, 3, \delta']$;
- G_2: комбинаторный экспандер с парамтерами $[q^6, q^2, 1/4]$;
- G_3: комбинаторный экспандер с парамтерами $[q^{4r+4}, q^8, 1/4]$.

Граф G_1 мы найдём грубым перебором. Существование такого графа гарантирует Теорема 1. Перебор всех графов степени 3 с q^2 вершинами требует времени $q^{O(q^2)}$. Как мы приверим ниже, это время невелико по сравнению с общим числом вершин в итоговом графе.

В качестве графа G_2 мы возьмём граф $LD(q, 5)$, а в качестве G_3 возьмём граф $LD(q^4, r)$. Чтобы эти графы были хорошими экспандерами (алгебраическими, а зничит и комбинаторными), отношения $5/q$ и r/q^4 должны быть бостаточно маленькими. С отношением $5/q$ всё совсем просто — оно стремится к нулю с ростом $q = 2^t$. Малость отношения r/q^4 гарантируется условием $r \le q^4/4$.

По теореме 6 подстановочное произведение $G_2 \circ G_3$ является экспандером с параметрами $[q^8, 6, \delta'' \ge \frac{\delta'}{4^2 \cdot 120}]$, а

$$g_1 \circ (G_2 \circ G_3)$$

оказывается экспандером с параметрами $[q^{4r+12}, 12, \delta \ge \frac{\delta''}{4^2 \cdot 120}]$.

Остаётся проверить, что граф G_1 можно найти за время, полиномиально зависящее от $n = q^{4r+12}$. Здесь мы пользуемся условием теоремы $q^2 \le r$, которое гарантирует $q^{O(q^2)} \le \mathrm{poly}(q^{4r+12})$. Теорема доказана.

Упражнение 3: Покажите, что для любого n доказанная теорема позволяет построить экспандер с параметрами $[N, 12, \delta]$ для неоктрого N, удовлетворяющего

$$n \le N \le O(n \log n)$$

Указание: воспользуйтесь свободой в выборе параметра r.

Часть 10. Оценка второго собственного числа при подстановочном произведении графов.

Мы покажем, что если у графов G и H вторые собственные числа достаточно далеко отделены от степени графов (таким образмо, графы являются алгебраическими экспандерами), то аналогичное свойство верно и для их подстановочного произведения.

Теорема 8 *Пусть графы G и H являются алгебраическими экспандерами с параметрами $[n, D, 1-\varepsilon]$ и $[D, d, 1-\delta]$ соответственно. Тогда их подстановочное произведение $G \circ H$ имеет параметры $(nD, 2d, \geq 1 - \varepsilon\delta^2/24)$.*

Доказательство. В этом рассуждении удобнее описывать происходящее в терминах случайных блужданий на графах. Преобразование распределения веротянсотей на вершинах при одном шаге случайного блуждания соответствует умножению на нормализованную матрицу графа (полученную делением матрицы смежности на степень графа).

Блуждание по графу–подставновочному произведению G и H является полусуммой двух блужданий: 'локального', где мы движемся внутри одной 'галактики' в соответствии с матрицей графа H, и глобального, где мы движемся по рёбрам графа G (а выбор ребра определяется текущей H-координатой: вершин в графе H ровно столько, сколько рёбер в G, и мы предполагаем, что для каждой галактики фиксировано некоторое соответствие). Таким образом, матрицу блуждания можно записать как

$$M = \frac{1}{2}\hat{G} + \frac{1}{2}\hat{H},$$

где G и H — соответствующие матрицы исходных графов. Чтобы оценить второе собственное число M, достаточно оценить второе собственное число M^3 и доказать, что оно не больше $1 - \varepsilon\delta^2/8$, а затем воспользоваться неравенством Бернулли.

В разложении для M^3 имеется восемь членов. Все эти члены имеют два инвариантных подпространства: одномерное — векторы, у которых все координаты равны (все восемь членов на этом подпространстве единичные, и при каждом стоит коэффициент $1/8$), и ортогональное дополнение к этому подпространству (состоящее из векторов, у которых сумма координат равна нулю). Во втором собственном подпространстве максимальное с обственное значение (и тем самым норма ограничения на это подпространство) и есть интересующий нас параметр. Если мы докажем, ч то для одного из этих восьми произведений второе собственное число не больше $1 - \varepsilon\delta^2$, то это будет означать, что для M^3 это второе собственное число не больше $1 - \varepsilon\delta^2/8$, поскольку у оставшихся семи произведений норма не больше 1.

Какое из восьми слагаемых выбрать? Кажется, что наилучшие шансы на перемешивание у $\hat{H}\hat{G}\hat{H}$ (сначала перемешиваем внутри галактики с

помощью графа H, потом идём по ребру большого графа, потом перемешиваем внутри другой галактики — как в зизаг-произведении). Если бы перемешивание внутри галактики было полным (переход в случайную точку галактики), то такой переход был бы переходом в случайную вершину случайной соседней галактики. Соответствующее преобразование является тензорным произведением G и полного перемешивания, и потому имеет второе собственное число равное $1-\varepsilon$, как у матрицы первого графа G.

Однако случайное блуждание внутри галактики (по рёбрам из H) не является полным перемешиванием. Поэтому рассуждение придётся усложнить. При этом вместо $1-\varepsilon$ мы получим для второго собственного числа M^3 оценку не $1-\varepsilon$, а $1-\varepsilon\delta^2/8$.

Лемма. Пусть S — матрица блуждания по некоторому графу (первое собственное число равно 1), и все остальные собственные числа по модулю не превосходят $1-\delta$. Тогда S можно представить в виде $(1-\delta)S'+\delta J$, где S' — матрица с нормой не больше 1, а J — матрица полного перемешивания (все матричные элементы равны $1/$(число вершин)).

Доказательство: вычитая из S матрицу δJ, мы уменьшаем первое собственное число (единицу) на δ, а остальные не меняем, так что все собственные числа становятся не больше $1-\delta$ по модулю.

Теперь мы можем повторить примерно те же рассуждения, но с тремя слагаемыми. Применим лемму к блужданию по графу H и разложим его в сумму $(1-\delta)H'+\delta J$. Это разложение можно провести в каждой галактике и получить разложение $\hat H=(1-\delta)\hat H'+\delta\hat J$, где $\hat H'$ — некоторый оператор с нормой не больше 1, а J — то самое полное перемешивание внутри галактик, о котором мы рассуждали выше.

Теперь повторяем то же рассуждение, что и раньше, но в разложении

$$M=\frac{1}{2}\hat G+\frac{1-\delta}{2}\hat H'+\frac{\delta}{2}\hat J$$

будет уже не 8, а 27 слагаемых. В одном из слагаемых (в $\hat J\hat G\hat J$) второе собственное значение не превосходит $1-\varepsilon$, а остальные представляют собой оператор с нормой не больше 1 с некоторым скалярным коэффициентом. Поэтому второе собственное значение M не больше $1-\varepsilon\delta^2/8$, что и требовалось доказать.

Лекция 5, 18 марта.

Часть 11. Явная конструкция алгебраических экспандеров.

У нас подготовлена вся необходимая техника для построения явной конструкции экспандера. Для каждого n мы построим алгебраический экспандер G_n с $2^{O(n)}$ вершинами, некоторой фиксированной степенью $D = O(1)$ (не зависящей от n), и вторым собственнм числом $\alpha D < (49/50)dD$. При этом конструкция будет алгоритмически эффективной: проверить, есть ли в этом графе ребро между вершинами с номерами i и j можно будет за время $\mathrm{poly}(n)$.

Конструкция графов G_n будет индуктивной. В качестве базы индукции мы возьмём некоторые алгебраические экспандеры G_1 и G_2 с достаточно хорошими параметрами, а шаг индукции мы будем делать с помощью некоторого подходящего графа H. Мы возьмём эти графы со следующими параметрами:

$$\begin{array}{ccc} G_1 & : & [(2d)^{100}, 2d, < 49/50] \\ G_1 & : & [(2d)^{200}, 2d, < 49/50] \\ H & : & [(2d)^{100}, d, < 1/100] \end{array}$$

Каждый следующий граф G_n будет строиться из уже имеющихся по правилу

$$G_n = \left(G_{\lfloor \frac{n-1}{2} \rfloor} \otimes G_{\lceil \frac{n+1}{2} \rceil}\right)^{50} \circ H$$

Покажем по индукции, что G_n будет алгебраическим экспандером с параметрми $[(2d)^{100n}, 2d, < 49/50]$. В самом деле, если для всех графов $G_1, \ldots, G_{n-1}$ эта оценка уже доказана, то в произведении $G_{\lfloor \frac{n-1}{2} \rfloor} \otimes G_{\lceil \frac{n+1}{2} \rceil}$ число вершин будет равно $(2d)^{100(n-1)}$, степень $(2d)^2$, а второе собственное число не превосходит $\frac{49}{50} \cdot (2d)^{100(n-1)}$. При возведении в степень 50 число вершин не меняется, степень возрастает до $(2d)^100$, а второе собственное число становится меньше $(49/50)^{50} < 1/2$ от степени графа. Число вершин теперь как раз такое, чтобы можно было осуществить подстановочное произведение с графом H. Согласно теореме 8 мы получаем в итоге алгебраический экспандер с параметрами

$$[(2d)^{100n}, 2d, \alpha_n < 1 - \frac{\frac{1}{2} \cdot (1 - 1/100)^2}{24} < 1 - 1/50],$$

что и требовалось.

Нам осталось объяснить, как построить графы G_1, G_2, H. Их можно построить с помощью конструкции графов $LD(q, r)$ из главы 7.

Граф $LD(q, r)$ имеет параметры $[q^{r+1}, q^2, \frac{r}{q}]$ для подходящих $q = 2^t$ и r. Чтобы получить H, нам нужно, чтобы $[2^{(r+1)t}, 2^{2t}, \frac{r}{2^t}] = [(2d)^{100}, d, < 1/100]$. Достаточно положить $r = 200$ и $t = 100$.

В качестве G_1 можно взять граф H, в котором каждое ребро получает кратность два.

Чтобы построить G_2 (с параметрами $[(2d)^{200}, d, < 49/50]$), мы берем $LD(q, \hat{r})$ с прежним $q = 2^{100}$, находим $\hat{r}$ из условия

$$q^{\hat{r}+1} = (2d)^{200},$$

и удаиваем в полученном графе все рёбра. Таким образом, описание конструкции G_n полностью закончено.

Упражнение: Покажите, что существует алгоритм, который по заданным номерам i, j за время $\mathrm{poly}(n)$ на зоне $O(n)$ проверяет наличие или отстутствие в G_n ребра между вершинами с номерами i и j.

Мы показали, как строить алгебраические экспандеры с параметрами $[2^{cn}, d, < 49/50]$ для некоторой константы c. Если нам потребуется экспандер с 2^m вершинами для m не кратного c, это тоже нетрудно устроить: тензорно умножая G_n на полный граф на 2^l вершинами, мы получаем экспандер с 2^{cn+l} вершинами. Если мы захотим уменьшить втрое собственное число с $49/50$ до $1/2$ или какой-то другой константы, это тоже просто: нужно возвести имеющийся граф в некторую степень s; при этом второе собственное число (нормализованное относительно степени графа) тоже возведется в степень s.

Формально мы выполнили своё обещание – предъявили "явную" конструкцию экспандеров. Однако построенные нами графы G_n и соответствующий алгоритм слишком громоздки для разумных практических применений. Для 'реальной жизни' известны другие конструкции экспандеров, с гораздо лучшими параметрами. Однако для 'практически полезных' конструкций экспандеров как правило труднее оказать из свойства (комбинаторное свойство расширения или оценку на второе собственное число).

Часть 12. Блуждание на экспандере.

Свойство алгебраичкского экспандера гарантирует, что при случайном блуждании по графу мы быстро "забываем" информацию о начальной вершине блуждания. При этом вероятность того, что все шаги случайного блаждания по графу $v_0 - v_1 - v_2 - \ldots - v_k$ попадут в некоторое малое множество B, оказывается экспоненциально малой (экспоненциально убывающей с ростом числа шагов k). Более точно, имеет место следующая теорема:

Теорема 9 *Пусть G является алгебраическим экспандером с параметрами $[n, d, \alpha]$, и B — некоторое множество, состоящее из βn вершин. Рассмотрим процесс случайного блуждания по графу $v_0 - v_1 - v_2 - \ldots - v_k$ (первая вершина v_0 выбирается равномерно среди всех вершин графа, затем каждая следующая вершина v_{i+1} получается из предыдущей вершины v_i переходом по случайно выбранному ребру). Тогда вероятность того, что все вершины $v_0, \ldots, v_k$ принадлежат множеству B, не превосходит $(\alpha + \beta)^k$.*

Если бы мы выбирали вершины графа $v_0, \ldots, v_k$ независимо, то вероятность того, что все они оказались в множестве B была ещё меньше –

β^k. Однако для выбора k *независимых* вергин графа нужно больше случайных битов. Таким образом, данная теорема позволяет сэкономить число случайных битов при в вероятностных алгоритме.

Действительно, пусть у нас имеется вероятностный алгоритм с односторонней ошибкой: для слов $x \in L$ алгоритм всегда возвращает ответ *да*, а для $x \notin L$ ответ *нет* возвращается с вероятностью не менее $(1-\beta)$ (для некоторого достаточно малого β). Пусть алгоритм использует в своей работе $n = n(x)$ случайных битов.

Веротяность ошибки можно уменьшить до β^k, повторив вычисления с k копиями независимых случайных битов. При этом общее число случайных битов будет равно kn. Теорема 9 позволяет сделать вероятность ошибки экспоненуиально малой с меньшим числом случайных битов. Рассмотрим алгебраический экспандер с параметрами $[2^n, d, \alpha]$. Отождествим всме возможные наборы из n случайных битов с вергинами этого графа. Теперь вместо того, чтобы выбирать k независимых копий наборов из n битов, мы возьмём случайное блуждание $v_0 - v_1 - v_2 - \ldots - v_k$ на вершинах этого экспандера. Если B — множество вершин (=наборов случайных битов), на которых алгоритм возвращает неверный ответ для заданного входа x, то веротяность того, что все вершины v_i попадут в "плохое" множество B не превосходит $(\alpha+\beta)^k$. При этом число случайных битов, которое нужно для получения случайной траектории $v_0 - v_1 - v_2 - \ldots - v_k$, равно $n + k \log d = n + O(k)$ (что много меньше nk). Теперь перейдем к доказательству теоремы.

Доказательство теоремы: Обозначим через M нормализованную матрицу графа G — матрицу графа, делённую на степень вершин графа d. Сумма чисел в каждой строке и каждой столбе матрицы равна 1. Матрица M описывает марковский процесс: если у нас есть распределение веротяностей на врешинах графа $(p_1, \ldots, p_n)$, то умножая вектор-столбец с данными координатами на M мы получим распределение на графе через один шаг случайного блуждания:

$$\begin{pmatrix} p'_1 \\ p'_2 \\ \ldots \\ p'_n \end{pmatrix} = M \begin{pmatrix} p_1 \\ p_2 \\ \ldots \\ p_n \end{pmatrix}$$

Введём ещё одно обозначение: назовём P опереатор проектирования на координаты, соответствующие вершинам B. Матрица P устроена очень просто – если i-ая вершина графа входит в B, то $P_{ii} = 1$; все остальные элементы матрицы (в том числе, все элементы вне диагонали) равны нулю.

Лемма 1. Обозначим вектор равномерного распределения на врешинах графа G

$$\mathbf{u} = (1/n, \ldots, 1/n)^t$$

Вероятность того, что на всех шагах случайного блуждания $v_0, \ldots, v_t$ мы остаёмся в B, равна $\|(PM)^k P\mathbf{u}\|_1 = \|(PMP)^k \mathbf{u}\|_1$

Доказательство леммы: При умножении вектора-распредления веротяностей на P мы обнуляем те вероятности, которые приходятся на вергины

вне B, и оставляем прежними значения вероятностей для вершин B. Таким образом, вектор $P\mathbf{u}$ содержит $1/n$ на всех позициях, соответствующих вершинам B, и нули на остальных местах.

Индукцией по t нетрудно показать, что i-ая компонента в векторе

$$(PM)^k P\mathbf{u}$$

есть вероятность того, что случайный путь $v_0 = \ldots - v_k$ заканчивается в вершине i (т.е., $v_k = i$), и при этом ни разу не выходит за пределы B. Остаётся просуммировать все эти вероятности, что и есть l_1-норма данного вектора. Лемма 1 доказана.

Лемма 2. $\|PMP\|_2 \leq (\alpha + \beta)$

Доказательство леммы: Пусть $v = (v_1, \ldots, v_n)^k$ – произвольный вектор-столбец. Нам нужно доказать, что $\|PMPv\|_2 \leq (\alpha+\beta)\|v\|_2$. Без ограничения общности, можно сделать несколько предположений о векторе v:

- Носитель v содержится в B (все ненулевые координаты v соответствуют вершинам из множества B). В самом деле, если это не так, мы можем заменить v на Pv; при этом левая часть неравенства не измениться, а правая часть станет меньше; таким образом, доказываемое утверждение станет только сильнее.

- Можно считать, что все ненулевые координаты v имеют один знак (для определённости, $v_i \geq 0$ для всех i). Действительно, если в произвольном v поменять знаки всех ненулевых координат на полодительный, то правая часть неравенства не измениться, а левая может стать тольо больше.

- Поскольку обе части неравенства линейны по v, можно считать, что $\sum v_i = 1$.

Итак, мы рассматриваем вектор $\mathbf{v} = (v_1, \ldots, v_n)^t$, у которого все координаты неотрицательны, их сумма рана 1 (можно представлять себе v как распределение вероятностей), и $Pv = v$. Нам остаётся доказать, что длявсякого такого вектора v справедливо неравенство

$$\|PM\mathbf{v}\|_2 \leq (\alpha + \beta)\|v\|_2.$$

Поскольку сумма координат v равна единице, его можно представить в виде $\mathbf{v} = \mathbf{u}+\mathbf{w}$, где $\mathbf{u} = (1/n, \ldots, 1/n)^t$, а в векторе w сумма всех координат равна нулю. Покажем, что

$$\|PM(\mathbf{u} + \mathbf{w})\|_2 \leq \|P\mathbf{u}\|_2 + \|PM\mathbf{w}\|_2 \leq \|P\mathbf{u}\|_2 + \|M\mathbf{w}\|_2 \leq \beta\|\mathbf{v}\|_2 + \alpha\|\mathbf{v}\|_2.$$

Неравенство $\|M\mathbf{w}\|_2 \leq \alpha\|\mathbf{v}\|_2$ следует из того, что $\mathbf{w}$ ортогонален вектору $(1, \ldots, 1)$, а второе собственное занчение M по модулю не превосходит

α. Чтобы доказать неравенство $\|P\mathbf{u}\|_2 \leq \beta\|\mathbf{v}\|_2$, заметим сначала, что из неравенства Коши–Буняковского

$$1 = \|\mathbf{v}\|_1 \leq \sqrt{\beta n} \cdot \|\mathbf{v}\|_2.$$

Теперь сравним нормы $\mathbf{v}$ и $P\mathbf{u}$:

$$\|P\mathbf{u}\|_2 = \sqrt{\frac{\beta}{n}} = \beta \cdot \sqrt{\frac{1}{\beta n}} \leq \beta\|\mathbf{v}\|_2.$$

Лемма 2 доказана.

Для доказательства теоремы остаётся сравнить l_1 и l_2 нормы векторов:

$$\|(PM)^k P\mathbf{u}\|_1 \leq \sqrt{n}\|(PM)^k P\mathbf{u}\|_2 \leq \sqrt{n}(\alpha+\beta)^k\|\mathbf{u}\|_2 \leq (\alpha+\beta)^k$$

Лекция 6, 25 марта.

Блуждание на экспандере — продолжение.

Продолжим изучать случайное блуждание на экспандере. По-прежнему считаем, что граф G является алгебраическим экспандером с параметрами $[2^n, d, \alpha]$. Случайным блужданием (из k шагов) называем случайную последовательность вершин графа $v_0, v_1, \ldots, v_k$, где v_0 выбирается среди всех вергин графа равномерно, а каждая следующая v_{i+1} получается из v_i переходом по случайно выбранному ребру.

Пусть B — множество из βn вершин. На прошлой лекции мы оценивали веротсноть того, что *вся* траектория случайного блуждания $v_0, \ldots, v_k$ лежит в B. Сейчас мы оценим вероятность того, что *достаточно много* вершин в случайном пути длины k попали в B.

Теорема 10 *Рассмотрим случайное блуждание $v_0, \ldots, v_k$ на множестве вершин алгебраического $[2^n, d, \alpha]$-экспандера G. Пусть $I = \{i_1, \ldots, i_s\} \subset \{0, 1, \ldots, k\}$. Тогда вероятность того, что все вершины для каждого номера шага $i \in I$ вершина v_i принадлежат множеству B, не превосходит $(\alpha + \beta)^{|I|-1}$.*

Доказательство: Рассуждение аналогично доказательству теоремы 9. Пусть M — нормализованная матрица графа, и P — оператор проектирования на вершины из B. Обозначим равномерное распределение вероятностей через $\mathbf{u} = (1/n, \ldots, 1/n)^t$. Нам нужно оценить l_1-норму произведения

$$P \cdot M^{i_s - i_{s-1}} \cdot P \cdots P \cdot M^{I_2 - i_1} P M^{i_1} P \mathbf{u}$$

Ясно, что второе собственное число кажой матрицы $M^{i_{r+1}-i_r}$ не меньше α. Поэтому $\|PM^{i_{r+1}-i_r}P\|)2$ не меньше $(\alpha + \beta)$. Далее остаётся сравнить l_1 и l_2 норму вектора, как и в доказательстве теоремы 9.

Теорема 10 показывает, как уменьшить ошибку в вероятностных алгоритмах с двусторонней ошибкой. Действительно, пусть некоторый алгоритм отвечает на любой вопросы "$x \in L$?" с вероятностью ошибки не более $\beta < 1/4$, используя при этом $n = n(x)$ случайных битов. Если повторить вычисления k раз с k независимыми копиями случайных битов, а затем выбрать среди полученных ответов тот: который встречается чаще, то вероятность ошибки будет экспоненциально (по k) стремиться к нулю – это нетрудно доказать с помощью неравенства Чернова. При этом мы используем kn случайных битов.

Покажем, как получить аналогичную оценку с меньшим числом истинно случайных битов. Отождествим наборы из n случайных битов с вершинами алгебраического $[2^n, d, \alpha]$-экспандера. Обозначим через B те наборы случайных битов, которые приводят к неверному (для данного x) ответу в исходном алгоритме. Рассмотрим случайное блуждание $v_0 \ldots v_k$ на данном графе. Согласно теореме 10, вероятность того, что мы попадаем в B на

шагах $i_1, i_2, \ldots, i_s$ не превеосходит

$$(\alpha+\beta)^{s-1}.$$

Остаётся просуммировать эту вероятность по всем наборам $i_1, i_2, \ldots, i_s$, составляющим большинство из множества $0, 1, \ldots, k$. Таким образом, вероятность ошибки в новом алгоритме не больше

$$2^n \cdot (\alpha+\beta)^{\frac{n}{2}-1} = O((2\sqrt{\alpha+\beta})^n)$$

При этом мы используем $n + O(k)$ случайных битов (вместо kn битов в стандартном алгоритме с независимыми повторениями испытаний).

Упражнение: Пусть G является алгебраическим экспандером с параметрами $[n, d, \alpha]$, и $B_0, \ldots, B_k$ — некоторые множества вершин. Обозначим $\beta_i = |B_i|/2^n$. Рассмотрим процесс случайного блуждания по графу $v_0 - v_1 - v_2 - \ldots - v_k$ (как всегда, первая вершина v_0 выбирается равномерно среди всех вершин графа, затем каждая следующая вершина v_{i+1} получается из предыдущей вершины v_i переходом по случайно выбранному ребру). Докажите, что

$$\text{Prob}[v_i \in B_i \text{ для всех } i] \leq \prod_{i=1}^{k-1} (\sqrt{\beta_i \beta_{i+1}} + \alpha)$$

Часть 13. Экстракторы.

Полезной мерой "случайности" в распределении вероятностей является мин-энтропия. Мин-энтропией случайной величины X называется логарифм макимальной веротяности среди всех значений X со знаком минус. Мы будем обозначать мин-энтропию $H_\infty(X)$:

$$H_\infty(X) = -\log(\max_a \text{Prob}[X = a])$$

Рассмотрим несколько простых примеров:

- Случайная величина, равномерно распределённая на $\{0,1\}^n$ имеет мин-энтропию n.
- Если каждая случайная величина X_i равна единице с вероятностью $\delta < 1/2$ и нулю с вероятностью $1-\delta$, и $X_1, \ldots, X_n$ независимы, то $H_\infty(X_1 \ldots X_n) \geq \log \frac{1}{1-\delta}$.
- Если с веротяностью 1 значение X лежит в множестве A, то $H_\infty(X) \leq \log |A|$.
- Если $X_1, \ldots, X_n$ равномерно распределены среди точек k-мерного подпространства в $(\mathbb{Z}/2\mathbb{Z})^n$, то $H_\infty(X_1 \ldots X_n) = k$.

Определим статистическое расстояние между двумя случайными величинами X, Y, распределёнными на некотором множестве A, как

$$dist(X,Y) = \max_{S \subset A} |\text{Prob}[X \in S] - \text{Prob}[Y \in S]|$$

Если веротяности того, что $X = a_1, a_2, \ldots$ равны $p_1, p_2, \ldots$, а веротяности $Y = a_1, a_2, \ldots$ равны $q_1, q_2, \ldots$, то нетрудно проверить, что

$$dist(X,Y) = \frac{1}{2}(|p_1 - q_1| + |p_2 - q_2| + \ldots)$$

Таким образом, статистическое расстояние есть просто l_1-норма между двумя рсапределениями (с поправочным коэффициентом $1/2$).

Определение 4 *Отображение* $Ext : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ *называется* (k,ε)*-экстрактором, если для любого распределения* X *на* $\{0,1\}^n$ *с мин-энтропией не меньше* k*, для независимого распределения* U_t *на* $\{0,1\}^t$*, значение* $Ext(X,U_t)$ *находится на расстоянии не более* ε *от равномерно распределения на* $\{0,1\}^m$*.*

Экстрактор – это средство выделить случайность из "некачественного" распределения X и превратить в распределение, статистически близкое к равномерному распределению. Для этого используется сравнительно небольшое количество истинно случацных битов (t в обозначениях данного определения).

Теорема 11 *Для любого* $\varepsilon > 0$*, любого* n *и* $k \leq n$ *существует* (k,ε)*-экстрактор*

$$Ext : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$$

для $t = O(n - k + \log \frac{1}{\varepsilon})$*, вычилисмый за полиномиальное время* $\text{poly}(n)$*.*

Доказательство: Рассмотрим алгебраический экспандер G с параметрами $[N = 2^n, d, < 1/2]$. Экстрактор будет устроен следующим образом: первый вход экстрактора $x \in \{0,1\}^n$ мы интерпретируем как номер вершины в графе; второй вход $z \in \{0,1\}^t$ мы интерпретируем как выбор l шагов случайного блуждания в графе, начинающегося в вершине x (ясно, что t должно быть равно $l \cdot \log d$). Конечная вершина этого блуждания и будет значением Ext для данных значений аргументов.

Далее мы покажем, что при правильном выборе числа шагов l (мы положим $l = n/2 - k/2 + \log 1/\varepsilon$) распределение на выходе экстрактора ε-близно к равномерному.

Обозначим через M нормализованную мтарицу экспандера G. Пусть $\mathbf{p}$ — распределение на вергинах G, соответствуюшее случайной величние X. Об этом распределении мы знаем лишь, что оно имеет мин-энтропию не меньше k.

Нам нужно оценить близость к равномерному того распределения, которок мы получим после l шагов случайного блуждания:

$$\|M^l\mathbf{p} - (1/N,\ldots,1/N)^T\|_1 = ?$$

Сначала оценим l_2-норму разности этих векторов:

$$\|M^l\mathbf{p} - (1/N,\ldots,1/N)^T\|_2 = \|M^l(\mathbf{p} - (1/N,\ldots,1/N)^T)\|_2 = ?$$

Прежде всего заметим, что разность $\mathbf{p} - (1/N,\ldots,1/N)^T)$ является вектором, у которой сумма координат равна нулю. Значит, эта разность ортогонална вектору $(1,\ldots,1)$, и лежит в собственном подпространстве оператора M, в котором все собственные числа не превосходят α. Таким образом, каждое умножение этой разности на M уменьшает её l_2 норму по крайней мере в α раз. Оценим норму данной разности до умножения на M_l.

Отметим, что $\|\mathbf{p}\|_2^2 = p_1^2 + \ldots + p_N^2 \leq (p_1 + \ldots + p_N)\cdot\max\{p_i\} = 2^{-H_\infty(X)}$. А значит,

$$\|\mathbf{p} - (1/N,\ldots,1/N)^T\|_2 \leq \|\mathbf{p}\| + \|(1/N,\ldots,1/N)\|_2 \leq \sqrt{2^{-k}} + \sqrt{2^{-n}} \leq 2\cdot 2^{-k/2}.$$

Следовательно,

$$\|M^l(\mathbf{p} - (1/N,\ldots,1/N)^T)\|_2 \leq \alpha^l \cdot 2 \cdot 2^{-k/2} = (1/2)^l \cdot 2 \cdot 2^{-k/2}.$$

Вспоминаем, что статистическое расстояние между распределениями есть половина l_1-нормы их разности. Сравнивая l_1 и l_2 нормы получаем:

$$\frac{1}{2}\|M^l\mathbf{p} - (1/N,\ldots,1/N)^T\|_1 \leq \frac{1}{2}\sqrt{N}\|M^l\mathbf{p} - (1/N,\ldots,1/N)^T\|_2 \leq 2^{-l}\cdot 2^{n/2-k/2} \leq \varepsilon$$

(в последнем неравенстве мы использовали выбор l). Теорема доказана.

Лекции 7, 1 апреля.

Часть 14. Лемма о переработке мусора и её простые применения.

Лемма 3 (О вторсырье) *Пусть $f : \{0,1\}^n \to \{0,1\}^m$ некоторая функция (мы ничего не предполагаем о её быстрой вычислимости), и пусть*

$$Ext : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$$

является $(k,\varepsilon/2)$-экстрактором для $k = n - (m+1) - \log\frac{1}{\varepsilon}$. Тогда для случайной величины X равномерно распределённой на $\{0,1\}^n$ имеем

$$dist(f(X)\circ U_n, f(X)\circ Ext(X,U_t)) \leq \varepsilon$$

Доказательство: По определению статистического расстояния между распределениями мы имеем

$$dist(f(X) \circ U_n, f(X) \circ Ext(X, U_t)) =$$
$$= \frac{1}{2} \sum_{a \in \{0,1\}^n, b \in \{0,1\}^n} |\text{Prob}[f(X) = a, U_n = b] - \text{Prob}[f(X) = a, Ext(X, z) = b]| =$$
$$\sum_a \text{Prob}[f(X) = a] \cdot dist(U_n, Ext(X_a, z)),$$

где X_a есть равномерное распределение на множестве $f^{-1}(a)$.

Обозначим $A = \{a \ : \ \text{Prob}[f(X) = a] \geq \frac{\varepsilon}{2^{m+1}}$ – множество a, имеющий не слишком мало f-прообразов. Для $a \in A$ случайная велична X_a имеет мин-энтропию не меньше $k = n - (m + 1 + \log \frac{1}{\varepsilon})$. По определению $(k, \varepsilon/2)$-экстрактора, статистическое расстояние между $Ext(X_a, z)$ (где z равномерно распределено на $\{0,1\}^t$) и U_n не превосходит $\varepsilon/2$. Следовательно,

$$dist(f(X) \circ U_n, f(X) \circ Ext(X, U_t)) \leq 2^m \cdot \frac{\varepsilon}{2^{m+1}} + \varepsilon/2 = \varepsilon,$$

и лемма доказана.

Далее мы используем лемму о вторсырье для помтроения генератора псевдослучайных битов. Этот генератор будет достаточно хорош, чтобы использовать его псевдослучайные биты вместо истинно случайных (независимых, равномерно распределённых) в некоторых классах вероятностных алгоритмов. А именно, мы будем применять этот генератор, чтобы деранжомизовать алгоритмы, использующие небольшую память (основным применением будут генератворы для машин с логарифмической памятью).

Прежде всего, нам нужно уточить, как мы измеряем память алгоритма. Для алгоритмов с очень малой рабочей памятью небольшие нюансы в способе "измерения" ёмкости памяти могут иметь существенное значение. Рассмотрим стандартную модель вычислений — машину Тьюринга, которая получает входные данные (слово длины n) на входной ленте, доступной только для чтения, использует для вычислений рабочую память (конечную ленту, доступную для чтения и записи) размера m, и ленту (доступную толко для записи), на которой выводится ответ. Кроме того, машина может образаться к генератору случайных битов. Можно представлять его себе как оносторонню ленту с последовательностью случайно выбранных битов; машина может читать биты с этой ленты, причём читающая головка жвижется только в одном направлении, т.е., однажды прочитанные случайные биты нельзя перечитать ещё раз.

Классом BPL называют языки, которые распознаются вероятностной машиной Тьюринга, с рабочей памятью размера $O(\log n)$, *всегда* (при любом значении случайных битов) завершающую работу, и для каждого входа выдающую правильный ответ с вероятностью не менее 2/3. Условие *остановки* означает, что машина работает не более $\text{poly}(n)$ шагов. Это означает, что число используемых случайных битов заведомо не превосходит $R = \text{poly}(n)$.

Мы построим генератор псеводслучайных битов, перерабатывающий случайное зерно из $O(\log^2 n)$ случайных битов в R псевдослучайных, которые позволяют "обмануть" машину с логарифмической памятью: такая машина для любого входа x будет выдавать ответы "да" и "нет" с примерно равными вероятностями для истинно случайных и псевдослучайных R битов. Данный генератор будет вычисляться быстро и на небольшой памяти, так что мы получим доказательство теоремы $\mathrm{BPL} \subset \mathrm{DSpace}[\log^2 n]$.

Заметим, что у машины Тьюринга с рабочей лентой из m ячеек её внутрення память (в неформальном смысле) может быть несколько больше, чем $O(m)$. Дело в том, что мы можем схитрить и использовать в качестве хранилища информации положение головки на входной ленте (доступной только для чтения). таким образом, мы долдны определенить размер памяти машины чуть аккуратнее.

Будим называть *конфигурацией машины* содержание всех её лент и положение всех читающих/пишуших головок. Зафиксируем вход машины x и подсчитаем число всех конфигураций машины, соответствующих этому входу. Размером *памяти* машины назовем логарифм числа всех её конфигураций. Заметим, что для машины Тюринга с входом x длины n и рабочей лентой из $O(\log n)$ ячеек размер *памяти* есть $S = O(\log n)$.

Можно рассматривать не только машины Тьюринга, но и более общий случай – вероятностные автоматы с конечным числом состояний (входные данные фиксируются и определяют структуру такого автомата). Памятью такой машины (Finite State Machine) называется логарфм числа состояний.

Покажем на простом примере, как для вероятнсотной машины с памятью S сократить число истинно случайных битов с R примерно вдвое (до $R/2 + O(S)$). Для этого мы построим псевдослучайный генератор с зерном размера $R/2 + O(S)$ и выходом длины R. При этом веротяности различных ответов у нашего алгоритма изменятся (по сравнению с истоинно случайными битами) не более чем на 2^{-S}.

Генеравтор будет устроен слежующим образом. Первые $R/2$ битов X мы выберем по-настоящему случайными. Затем мы хотели бы повторно использовать эти же самые биты ещё раз. Разумеется, так поступить нельзя. Но оказывается, уже использованные биты будыт выглядеть "почти как новые", если мы их переработаем с помощью леммы о вторсырье. А именно, в качестве вторых $R/2$ битов мы возьмем значение экстрактора $Ext(X, z)$ (для случайно выбранного значения z). Если Ext является экстрактором с параметрами $(k = R/2 - S - 1 - \log(2^{-S}), 2^{-S}/2)$, то леммы о вторсырье гарантирует, что для алгоритма с памятью S псевдослучайные биты выглядят почти неотличимо от настоящих. Остаётся заметить, что мы умеем строить экстракторы с указанными параметрами и размером z порядка $O(S)$.

Описанную конструкцию можно итерировать, многократно уменьшая размер зерна генератора. Далее мы обсудим эту идею более подробно.

Лекции 8, 8 апреля.

Часть 15. Генератор Нисана.

Мы хотим дерандомизовать вероятнстные алгоритмы, исользующие R случайных битов и память S. Для этого мы постром генератор псевдослучайных битов Нисана, которые расширяет случайное зерно размера $O(S \log R)$ до R битов, и "обманывает" машины с памятью S. Более точно, мы докажем следующую теорему:

Теорема 12 *Для любого S и $R \leq 2^S$, любого $\varepsilon > 0$ существует отображение (генератор Нисана)*

$$PRG \ : \ \{0,1\}^{O(S+\log \frac{1}{\varepsilon}) \cdot \log R} \to \{0,1\}^R$$

такое, что каждый бит $PRG(z)$ вычислим на зоне $O(S + \log \frac{1}{\varepsilon}) \cdot \log R$ за время $\mathrm{poly}(R)$*, и для всякой машины M с памятью S*

$$|\mathrm{Prob}_{x \in \{0,1\}^R}[M(x) = 1] - \mathrm{Prob}_{z \in \{0,1\}^R}[M(PRG(z)) = 1]| < \varepsilon.$$

Следствие 1 $\mathrm{BPL} \subset \mathrm{DSpace}[\log^2 n]$.

Генератор Нисана мы определим рекурсивно. Пусть r – некоторое целое число. Генератор $G_m : \{0,1\}^{rm} \to \{0,1\}^{r2^{m-1}}$ мы определим по индукции: если $|x| = (m-1)r$, а $|y| = r$, то

$$G_m(x \circ y) = \begin{cases} y, & \text{если } m = 1, \\ G_{m-1}(x) \circ G_{m-1}(Ext_{m-1}(x,y)), & \text{если } m > 1, \end{cases}$$

где $Ext_m \ : \{0,1\}^{(m-1)r} \times \{0,1\}^r \to \{0,1\}^{(m-1)r}$ экстрактор с параметрами $(k = (m-1)r - S - 1 - \log \frac{1}{\delta}, \delta/2)$. В конструкции используются два параметра — r и δ; мы зафиксируем из ниже.

Будем обозначать $Comp_L(u,s)$ результат вычисления нашей машины, стартовавшей из конфигурации u (одной из 2^S возможных конфигураций машины) и получившей от датчика случайных чисел L битов $s = s_1 \ldots, s_L$. Значением отображения $Comp_L(u,s)$ будет некоторая другая конфигурация машины. Если в подставить вместо s не фиксированный набор битов, а некоторую случайную величину V, то значение $Comp_L(u,V)$ будет каким-то распределением вероятностей на множестве конфигураций нашей машины.

Основное свойство генератора Нисана, которое нам нужно доказать:

Лемма 4 *Если в генераторе Нисана используются (k_m, δ)-экстракторы для $k = (m-1)r - (s + 1 + \log \frac{1}{\delta})$, то для любой конфигурации u*

$$dist(Comp_{2^m r}(u, U_{2^m r}), Comp(u, G_m(U_{mr})) < 4^m \delta$$

Сначала покажем, как из этой леммы вытекает теорема. Возьмем в качестве конфигурации u начальное состояние машины. Далее, положим $m = \log R$ (для простоты мы делаем не самый оптимальный выбор параметров; нам

было бы достаточно получить $2^m r \geq R$). Наконец, подбирает δ такое, что $4^m \delta < \varepsilon$; ёто значит, что $\log \frac{1}{\delta} = \log \frac{1}{\varepsilon} + O(\log R)$.

В конструкции генератора нам требуется экстрактор с параметрами $((m-1)r - (s + 1 + \log(1/\delta)))$. У нас есть явная конструкция такого экспандера с длиной вспомогательного входа $r = O(s + 1 + \log(1/\delta))$. Такое значение r мы и берём в качестве параметра конструкции генератора.

Нетрудно проверить, что для генератора с указанными параметрами Лемма 4 немедленно влечёт Теорему 12.

Доказательство Леммы 4: Докажем лемму индукцией по m. База ($m = 1$) очевидна. Для $m > 1$ нам нужно оценить статистчиеское расстояние между двумя распределениями

$$dist(Comp_{2^m r}(u, U_{2^m r}), Comp(u, G_m(U_{mr})).$$

Мы вставим между интересующими нас распределениями $\mathcal{D}_1 = Comp_{2^m r}(u, U_{2^m r}))$ и $\mathcal{D}_2 = Comp(u, G_m(U_{mr}))$ два промежуточных:

$$\mathcal{D}_3 = Comp_{2^m r}(u, U_{2^{m-1} r} \circ G_{m-1}(U_{(m-1)r}))$$

(первая половина битов берётся истинно случайными, а вторая половина порождается генератором G_{m-1}), и

$$\mathcal{D}_4 = Comp_{2^m r}(u, G_{m-1}(U_{(m-1)r} \circ G_{m-1}(U'_{(m-1)r}))$$

(обе первая и вторая половина псеводослучайных битов получаются с помощью генератора G_{m-1} из независимо выбранных зёрен – распределения на зёрнах $U_{(m-1)r}$ и $U'_{(m-1)r}$ одинаковы, но независимы).

Из предположения индукции нетрудно получить, что расстояния $dist(D_1, D_3)$ и $dist(D_3, D_4)$ не превосходят $4^{m-1}\delta$. А расстояние $dist(D_3, D_2)$ не превосходит δ по лемме о вторсырье: всё, что помнить машина после получения первой половины псевдослучайных битов, есть её текущее внутреннее состояние (одно из 2^S); лемма о вторсырье гарантирует, что экстрактор достаточно хорошо 'перемешивает' первое значение зерна генератора, чтобы использовать его ещё раз. Лемма доказана.

Упражнение: Докажите, что машину с памятью S, использующую R случайных битов, можно ε-обмануть вычислимым за полиномиальное время генератором $PRG : \{0,1\}^{S \log \frac{R}{S}} \to \{0,1\}^R$ для $\varepsilon = 2^{-S}$ (таким образом, размер зерна построенного нами генератора можно немного уменьшить).

Часть 16. Сколько раз можно читать выход генератор Нисана?

Будет ли генератор Нисана по-прежнему надёжен, если разрешить читать его биты дважды? Формально это означает, что у машины теперь есть команда *вернуться на началу ленты со случайными битами*, причём выполнить эту команду можно только один раз.

Эквивалентный способ смотреть на эту задачу такой: мы считаем, что значение генератора записывается на ленты два раза подряд, и мы интересуемся, может ли машина с маленькой памятью отличить псевдослучайные $2R$ битов от R истинно случайных битов, записанных два раза подряд.

Оказывается, если немного увеличить размер зерна генератора Нисана, то повторное чтение псевдослучайных битов не позволят отличить их от случайных.

Теорема 13 *Если генератор Нисана G_m ε-обманывает машины с памятью $2S$, то генератор G_m^2 (определенный как $G_m^2(z) = G_m(z) \circ G_m(z)$) ε'-обманывает машины с памятью S для $\varepsilon' = \varepsilon \cdot 2^{2S}$.*

Доказательство: Пусть у нас есть машина M с памятью S, которая ε'-отличает $G_m^2(z)$ от $X \circ X$ для равномерно распределённой на $\{0,1\}^R$ случайной величины X. Это означает, что найдутся такие конфигурации машины (назорвём их q_0, q_i, q_j), что веростность того, что на случайной последовательности $X \circ X$ машина M из конфигурации q_0 сначала (прочитав первые R битов на ленте генератора) попадет в q_i, а затем (прочитав следующие R битов) попадёт в q_j, отличается от аналогичной вероятности для псевдослучайных битов $G_m(z) \circ G_m(z)$ по крайней мере на $\varepsilon'/2^{2S}$ (поскольку мы переходим от статистического расстояния между распределениями к максимальной разнице веротяностей, нам приходится разделить вероятность на число всевозможных пар q_i, q_j).

Теперь рассмотрим машину M' с памятью $2S$, которая читает набор (псевдо)случайных R битов только один раз. Новая машина моделирует две копии вычислений машины M. Таким оразом, внутренним состоянием машины M' является пара состояний машины M. Если начальной конфигурацией M' будет пара (q_0, q_i), то вероятность получить на выходе (q_i, q_j) для случайных битов X и псевдослучацных битов $G_m(z)$ отличается не менее, чем на $\varepsilon = \varepsilon'/2^{2S}$, что противоречит условию теоремы.

Упражнение: Пусть вероятностная машина Тьюринга с рабочей лентой размера $O(\log n)$, используетn случайных битов и может $k = O(\log^c n)$ раз возвращаться к началу чтения последовательности случайных битов. Докажите, что существует полиномально вычислимый генератор $PRG : \{0,1\}^{\log^d n} \to \{0,1\}^n$ (для некоторой константы d), который $(1/n)$-обманывает эту машину.

Часть 16. Сколько нужно случайных битов, чтобы сгенерировать большое простое число?

Пусть нам нужно случайно выбрать n-битое простое число (по равномерному распределению). Простейший способ для этого – выбирать случайные n битов и проверять, не является ли это число простым (для проверки простоты числа есть полиномиальный детерминированный алгоритм AKS). Из теоремы о плотности распределения простых чисел следует, что вероятность успеха – веротяность того, что случайно выбранное n-битное число

окажется простым – равна $\Theta(1/n)$. Таким образом, если повторить попытку $O(n^2)$ раз, вероятность отказа уменьшится до 2^{-n}.

В этом алогритме мы используем $O(n^3)$ случайных битов. Далее мы покажем, что их количество можно уменьшить до $O(n \log n)$. Для этого мы снова воспользуемся генератором Нисана.

На первый взгляд кажется, что использовать генератор Нисана нельзя, поскольку наш алгоритм требует двольно много памяти. Но на самом деле нам не важно, сколько памяти использует алгоритм во время проверки на простоту очередного канидата; важно, сколько памяти нужно алгоритмы в 'контрольных точках', при переходе к следующему блоку случайных/псевдослучайных битов.

Рассмотрим следующий 'тест' для генератора псевдослучайных битов $G : \{0,1\}^{O(n \log n)} \to \{0,1\}^{O(n^3)}$. Мы рассматриваем последовательность из $O(n^3)$ битов как конкатенацию $O(n^2)$ n-битных блоков. Тестирование состоит в том, что про каждый блок мы проверяем, не является ли он двоичной записью простого числа. Тест говорит в конце проверки *да*, если хотя бы один из блоков был простым числом, и *нет* иначе. Мы значем, что для истинно случайной последовательности битов тест скажет *да* с вероятностью $> 1 - 2^{-n}$. Заметим, что при переходе от рассмотрения одного блока к слудеющему нашему тесту нужна память всего в один бит (нужно помнить, встречалось ли нам уже простое число, или ещё нет). Следовательно, если мы возьмём генератор Нисана с размером зерна

$$O(S + \log 1/\varepsilon) \cdot \log R = O(n \log n)$$

(память $S = 1$, точность приближения $\varepsilon = 2^{-n}$, число псевослучайных биотов $R = O(n^3)$), то тест выдаст ответ *да* с веротяностью не менее $1 - 2^{-n} - \varepsilon = 1 - 2 \cdot 2^{-n}$.

Лекции 9, 15 апреля (Рассказано и записано А. Шенем).

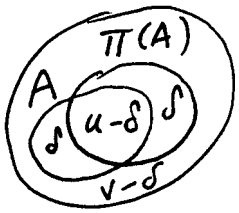
Часть 17. Преобразования тора и экспандеры.

Перестановки, экспандеры, квадратичные формы

Пусть X — конечное множество, $\pi : X \to X$ — перестановка. Будем считать соседями точки x её саму и $\pi(x)$. Попробуем оценить качество этого графа как экспандера. Для этого надо понять, насколько $\pi(A)$ выходит за пределы A. Удобно использовать линейную алгебру, рассмотрев пространство (комплексных) функций и линейное отображение P этого пространства в себя: $Pf(x) = f(\pi^{-1}(x))$. Можно сказать и так: мы рассматриваем формальные линейные комбинации элементов X, и продолжаем π на них, получая P.

На пространстве функций мы рассматриваем обычное скалярное произведение: $(f, g) = \mathsf{E}_x\, f(x)\overline{g(x)}$ (удобно взять не сумму, как обычно, а среднее арифметическое по всем x). Мы хотим связать параметры графа и свойства квадратичной формы (Pf, f) на подпространстве функций с нулевой суммой: если $(Pf, f) < (1-\varepsilon)(f, f)$ для некоторого $\varepsilon > 0$, то граф обладает свойствами экспандера.

Для этого надо проделать небольшое вычисление. Пусть множество A составляет долю u в X, а его дополнение — долю v, так что $u + v = 1$. Пусть $\pi(A)$ выходит за пределы A на δ (и, наоборот, δ-часть A не входит в $\pi(A)$. Рассмотрим функцию f, которая равна v на A и $-u$ на дополнении (так что среднее равно нулю). Функция Pf будет такой же с заменой A на $\pi(A)$, и произведение (Pf, f) равно



$$(u-\delta)v^2+(v-\delta)u^2-2\delta uv = (u+v)uv-\delta(u+v)^2 = uv-\delta,$$

при $\delta = 0$ получаем скалярный квадрат $(f, f) = uv$. Таким образом, оценка вида $(Pf, f) \le (1-\varepsilon)(f, f)$ для функций f с нулевым средним даст расширение εuv (и если A составляет менее половины X, то будет как минимум $(\varepsilon/2)|A|$ новых вершин).

Вместо одной перестановки можно рассматривать две перестановки π_1 и π_2, тогда получится граф степени 3 (у вершины x соседи $x, \pi_1(x), \pi_2(x)$). Чтобы показать, что он обладает свойствами экспандера, достаточно показать, что для любой функции f с нулевым средним выполнено одно из неравенств $(P_1 f, f) < (1-\varepsilon)(f, f)$ и $(P_2 f, f) < (1-\varepsilon)(f, f)$ (тогда соответствующая перестановка уже одна даст расширение). А это, в свою очередь, следует из усреднённого неравенства

$$\Big(\frac{P_1 + P_2}{2} f, f\Big) \le (1-\varepsilon)(f, f). \qquad (*)$$

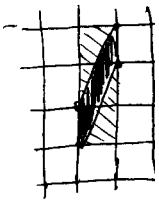
Таким образом, для построения экспандера достаточно найти две перестановки, для которых среднее соответствующих операторов удовлетворяло бы неравенству $(*)$ для всех f.

Замечание. Это очень похоже на оценку с собственными значениями, но технически есть разница: матрица преобразования P не симметрична (её можно сделать таковой, что соответствует добавлению обратных переходов). Интересно, как связаны получающиеся параметры.

Непрерывный и дискретный экспандеры

Можно вместо конечного множества рассматривать пространство с мерой (для нас основным примером будет двумерный тор $\mathbb{R}/\mathbb{Z})^2$), а вместо перестановок — сохраняющие меру обратимые преобразования. Свойство расширения формулируется естественным образом (для каждого подмножества A, мера которого не слишком близка к единице, его объединение с $\pi_1(A)$ и $\pi_2(A)$ имеет меру, превосходящую меру A в некоторое фиксированное число раз).

План действий таков: мы докажем, что это выполнено для двух преобразований тора $\mathbb{T}^2 = \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$:



$$\pi_1(x, y) = (x, y + 2x); \quad \pi_2(x, y) = (x + 2y, y).$$

Из этого можно будет получить экспандер на конечном множестве. В самом деле, разобьём тор на $N \times N$ маленьких квадратиков. Для каждого из них рассмотрим его π_1 и π_2-образы (наклонённые параллелограммы) и все квадратики, с ними пересекающиеся. Их будет конечное число (на самом деле три для каждого, всего шесть). Другими словами, мы рассматриваем граф, каждая доля которого состоит из квадратиков разбиения, и считаем V соседом U, если V пересекается (внутренностью) с $\pi_1(U)$ или $\pi_2(U)$, а также если $V = U$. Если множество A составлено из квадратиков, то его образ будет целиком покрыт соседями этих квадратиков, откуда получаем искомую оценку на число соседей.

Для непрерывного случая также можно применить линейную алгебру. Надо рассматривать гильбертово пространство $L_2(\mathbb{T}^2)$ и линейные операторы $P_i(f)\colon x \mapsto f(\pi_i^{-1}(x))$. Как и раньше, достаточно показать, что для любой функции f с нулевым средним выполнено неравенство $(*)$. Это можно сделать с помощью преобразования Фурье.

Преобразование Фурье

Характеры на торе имеют вид

$$\xi_{u,v}(x, y) = e^{2\pi i(ux+vy)}$$

и параметризуются точками решётки $(u, v) \in \mathbb{Z}^2$. Преобразования на функциях тоже легко описываются:

$$(P_1\chi_{u,v})(x, y) = \chi_{u,v}(\pi_1^{-1}(x, y)) = \chi_{u,v}(x, y - 2x) = \\ = e^{2\pi i(ux+v(y-2x))} = e^{2\pi i((u-2v)x+vy)} = \chi_{u-2v,v}(x, y).$$

Преобразование Фурье является изоморфизмом гильбертовых пространств $L_2(\mathbb{T}^2)$ и $L_2(\mathbb{Z}^2)$, поэтому можно перейти к операторам P_1 (переводит базисный вектор (u,v) в $(u-2v,v)$) и P_2 (аналогично).

Как можно описать $\left(\frac{P_1+P_2}{2}f, f\right)$ после преобразования Фурье? Рассмотрим граф с вершинами из $\mathbb{Z}^2$, у которого из каждой вершины (u,v) выходят два ребра в $(u-2v,v)$ и $(u,v-2u)$. (Преобразования π_1 и π_2 являются перестановками, так что в каждую вершину входит тоже два ребра.) Оцениваемое выражение можно записать как сумму произведений $f(a)f(b)$ для всех рёбер (a,b) описанного графа. Каждая вершина входит в четыре слагаемых (для двух входящих и двух выходящих рёбер; надо только оговориться, что бывают петли, если вершина находится на одной из осей координат; тогда вместо двух слагаемых получается одно, в которое она входит дважды). И эту сумму надо сравнить с суммой квадратов модулей всех $f(a)$ для всех вершин a.

Для оценки будем использовать неравенство $|uv| \le \frac{1}{2}|u|^2 + \frac{1}{2}|v|^2$. Если применить его ко всем рёбрам безо всяких хитростей, то получится $((P_1 f + P_2 f)/2, f) \le (f,f)$: каждая вершина войдёт четыре раза с коэффициентом $\frac{1}{2}$, да ещё надо делить на 2. Чтобы получить нужную оценку, надо заметить две вещи:

(1) функция f не произвольная, а соответствовала функции с нулевым средним на торе: в терминах коэффициентов Фурье это значит, что коэффициент при базисном векторе $(0,0)$ равен нулю.

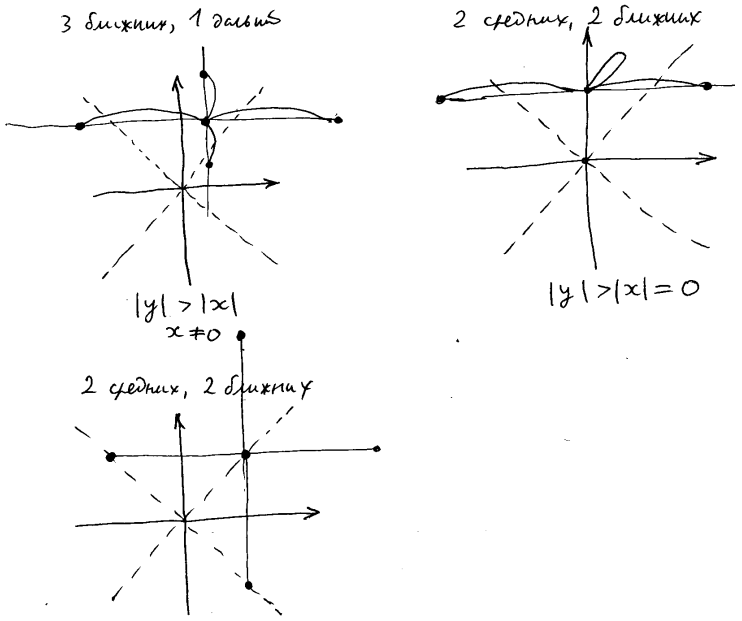
(2) оценивая $|uv|$ с помощью приведённого неравенства, можно предварительно умножить u и поделить v на что-нибудь, так что

$$|uv| \le \frac{\alpha}{2}|u|^2 + \frac{1}{2\alpha}|v^2|.$$

Надо только решить, как выбирать эти коэффициенты для разных рёбер.

Будем использовать такую стратегию: стараться, чтобы для ближнего (к началу координат) конца ребра коэффициент был поменьше, а для дальнего побольше. Если оба конца ребра одинаково удалены (например, если это

петля), то для обоих берём коэффициент 1/2.



Из картинки видно, что есть два случая — (1) сходятся два ближних конца и два средних; (2) сходится один дальний конец и три ближних. Соответственно получаются коэффициенты $(1/4)(1+1+1/\alpha+1/\alpha)$ и $(1/4)(\alpha+1/\alpha+1/\alpha+1/\alpha)$, первый не превосходит второго, так что надо минимизировать второй, что получается при $\alpha = 3/\alpha$, то есть $\alpha = \sqrt{3}$. В итоге получаем оценку

$$\Big(\frac{P_1+P_2}{2}f, f\Big) \le \frac{\sqrt{3}}{2}(f,f). \qquad (*)$$

(Где мы использовали, что нулевой коэффициент равен нулю? У соответствующей вершины оба ребра — петли, так что все четыре конца рёбер — средние, и оценка получается только с коэффициентом 1.)

Собирая всё вместе, получаем для каждого N двудольный граф с N^2 вершинами в каждой доле, имеющий степень 7 в каждой вершине, у которого любое множество (относительного) размера a в одной доле имеет $a + a(1-a)(1-\sqrt{3}/2)$ соседей.

Лекции 10, 22 апреля.

Часть 18: Теорема Рейнголда

Ранее мы использовали подстановочное произведение, чтобы собирать из маленьких экспандеров сколь угодно большие экспандеры с ограниченной степенью и достаточно малым вторым собственным числом. Теперь мы рассмотрим ещё одно красивое применение этой операции. Мы докажем теорему Рейнгольда (Omer Reingold) о дерандомизации одного из самых знаменитых вероятностных алгоритмов – алгоритма проверки на логарифмической памяти связности в неориентированном графе (задача UPATH).

Описание задачи UPATH: задан неориентированный граф $G = (V, E)$, в котором выделены две вершины $s, t \in V$. Требуется выяснить, есть ли в графе путь из вершины s в вершину t.

Теорема 14 *Задача UPATH может быть решена вероятностным алгоритмом с логарифмической памятью.*

Вероятностный алгоритм для решения задачи UPATH устроен очень просто: нужно сделать $N = \mathrm{poly}(|V|)$ (выбор полинома мы утоним чуть позже) шагов случайного блуждания по графу, начав с вершины s. Если за N шагов нам удастся побывать в вершине t, мы точно знаем, что в графе есть путь из s в t. В противном случае мы полагаем, что такого пути нет.

В каждый момент работы алгоритма нам требуется помнить номер текущего шага блуждания (от 1 до N) и номер вершины, в которой мы в данным момент находимся. Для хранения этой инофрмации достаточно памяти размера $O(\log |V|)$.

Ясно, что если пути из s в t нет, то алгоритм выдаст правильный ответ. Остаётся оценить вероятность другой ошибки: путь из s в t существует, но за N шагов блуждания мы его не обнаружим. Без ограничения общности можно считать, что граф регулярен и недвудолен (мы всегда можем добиться этого, добавив в граф некоторое количество петель). Далее покажем, что при случайном блуждании по связному однородному и недвудольному графу распределение вероятностей на вершинах быстро приближается к однородному. Ключевое свойство графа:

Лемма В связном d-регулярном однородном и недвудольном графе с n вершинами щель между первым и вторым по абсолютной величине собственными числами не может быть меньше $1/\mathrm{poly}(n)$, т.е.

$$\lambda/d \geq 1 - \Theta(1/n^c)$$

для некоторой константы c (не зависящей ни от n, ни от d).

Доказательство: Если у графа есть отрицательные собственные числа, мы перейдём от исходного графа G к его квадрату G^2. При возведении в квадрат все собственные числа также возведутся в квадрат и станут положительными (щель между перым и вторым по модулю собственным числом

также измениться в полином раз — умножится на $O(d)$). Связный недвудольный граф при возведении в квадрат остаётся связным. А поскольку исходный граф G не был двудольным, в его квадрате максимальное собственное число имеет кратность 1 .

Таким образом, остаётся доказать лемму для связного графа, у которого все собственные значения положительны. Обозначим $\bar{f} = (f_1, \ldots, f_n)$ собственный вектор, соответствующий второму собственному числу G^2 (он ортогонален первому собственному вектору $(1, 1, \ldots, 1)$, т.е., $\sum f_i = 0$).

Можно считать, что норма $\bar{f}$ равна единице. Тогда найдётся координата i такая, что $|f_i| \geq 1/\sqrt{n}$. Предположим для определённости, что f_i положительно. Поскольку сумма всех координат $\bar{f}$ равна нулю, то найдётся и координата j, для которой $f_j \leq 0$.

Рассмотрим в графе кратчайший путь из i-ой вершины в j-ую: $f_i - \ldots - f_j$. В этом пути найдётся хотя бы одно ребро $f_s - f_l$, для которого

$$|f_s - f_l| \geq |f_i - f_j|/n \geq \frac{1}{n\sqrt{n}}$$

Итак, мы нашли в графе такую пару вершин, соединённых ребром, что разница $|f_s - f_l|$ не меньше $1/n^{1.5}$.

Просуммируем $(f_s - f_t)^2$ по всем рёбрам (s, t) графа. При этом каждое ребро мы считаем по одному разу:

$$\sum_{s \leq t,\ (s,t) \in E} (f_s - f_t)^2 = \sum_{s \leq t,\ (s,t) \in E} (f_s^2 + f_t^2 - 2 f_s f_t) = d \sum_{s=1}^{n} f_s^2 - \bar{f}^t M \bar{f} = 2d^2 - 2\lambda$$

(здесь M обозначает матрицу графа, d — его степень). Это равенство верно независимо от того, если в графе петли. Данная сумма снизу ограничена $(f_s - f_l)^2 \geq \frac{1}{n^3}$. Следовательно, разность $d - \lambda$ ограничена снизу $\Theta(1/n^3)$. Лемма доказана.

С помошью леммы легко оценить корректность работы нашего алгоритма. Обозначим $\bar{p}(i)$ распределение веротяностей на вершинах после i шагов случайного блуждания по графу (распределение $\bar{p}(0)$ сосредоточено в единственной вершине s). Пусть обозначим равномерное распределение $\bar{u} = (\frac{1}{n}, \ldots \frac{1}{n})$ на вершинах компоненты связности s, и разложим $\bar{p}(i)$ в сумму $\bar{u}$ и некоторого вектора из его ортогонального дополнения:

$$\bar{p}(i) = \bar{u} + \bar{q}(i),$$

где сумма координат вектора $\bar{q}(i)$ равна нулю. Если M — нормализованная матрица графа, то $\bar{q}(i+1) = M\bar{q}(i)$. На подпространстве векторов с нулевой суммой норма линейного оператора M равна (нормализованному) второму собственному числу графа; по лемме это число не может быть больше $1 - \Theta(1/n^c)$, где n есть число вершин в компоненте связности вершины t. Следовательно, на каждом шаге норма $\bar{q}(i)$ уменьшается по крайней мере в $(1 - \Theta(1/n^c))$ раз, и через $\mathrm{poly}(n)$ шагов распределение $\bar{p}(i)$ станет

очень близко к равномерному (на компоненте связности графа). Таким образом, если s и t принадлежат одной компоненте связности, то вероятность попасть через $\mathrm{poly}(n)$ шагов в вершину t будет близка к $1/n$. Если же увеличить число шагов ещё в полином раз, то веротяность хотя бы раз побывать в t станет близка к единице.

Рейнголд придумал, как дерандомизовать алгоритм блуждания на графе без значительного увеличения используемой памяти:

Теорема 15 *Задача UPATH может быть решена* детерминированным *алгоритмом с логарифмической памятью.*

Прежде чем доказывать теорему, заметим, что мы уже умеем решать на логарифмической памяти задачу UPATH для $(n, d, 0.99)$-экспандеров. В самом деле, мы знаем, что диаметр такого экспандера равен $O(\log n)$. Мы можем перебрать все пути длины $C \log n$ с началом в вершине s и проверить, ведёт ли хотя бы один из них в t; такая проверка очевидно требует лишь логарифмической памяти (и полиномиального времени).

Чтобы решить задачу для произвольного графа G, мы превратим его в экспандер с помощью произведения. Для этой цели годится и зигзаг-произведение, и сбалансированное подстановочное произведение. В оригинальной работе Рейнгольда применялось загзаг-произведение (этот способ даёт лучшие оценки для мультипликативной константы в оценке размера памяти алгоритма). Мы приведём немного другое рассжудение, воспользовавшись сбалансированным подстановочным произведением. Для этого у нас уже готова вся необходимая техника – нужные оценки для собственных чисел подстановочного призведения графов.

Доказательство теоремы: Мы предполагаем, что нам задан (в виде оракула) неориентированный граф G с n вершинами, без петель и параллельных рёбер. Далее мы построим на основе G несколько 'воображаемых' графов; мы сможем моделировать блуждание по каждому из этих воображаемых графов с помощью исходного оракула и дополнительной памяти размера $O(\log n)$.

Воображаемый граф G': заменим в исходном графе каждую вершину степени $deg > 3$ на цикл длины deg; рёбра, входившие ранее в данную вершину мы по одному присоединим к вершинам этого цикла. Таким образом, в графе G' степень каждой вершины не превосходит 3. Обозначим через n' число вершин в G' (это число не превосходит $\mathrm{poly}(n)$).

Воображаемый граф G'': Добавим к каждой из вершин G_1 нужное число петель так, чтобы получился d-регулярный граф (константу d мы выберем так, чтобы существовал алгебраический $(d^{50}, d/2, < 0.01)$-экспандер H).

Воображаемые графы G_i : $G_0 = G''$; каждый следующий граф G_{i+1} определяется рекурсивно:

$$G_{i+1} = (G_i \circ H)^{50}$$

При этом каждый граф G_i будет алгебраическим экспандером с параметрами

$$(n' \cdot d^{50i}, d^{50}, < 1 - \varepsilon_i)$$

Если ε_i достаточно мало, то число ε_{i+1} получается из ε_i умножением сначала на $(0.99)^2/24$ (свойство подстановочного произведения), а затем умножением на 50 (для малых x имеем $(1-x)^{50} \approx 1 - 50x$). Таком образом, $\varepsilon_{i+1} \approx 2\varepsilon_i$.

Применим Лемму о втором собственном числе произвольного регулярного графа к G_0: $\varepsilon_0 \geq \Theta(1/(n')^c)$. Следовательно, для $k = O(\log n)$ граф G_i оказывается экспандером, у которого нормализованное второе собственное число не превосходит 0.99.

Вершины G_i получаются как тензорное произведение вершины графа G'' и i копий вершин графа H. Подстановочное произведение устроено так, что вопрос о существовании пути из s в t в исходном графе G эквивалентен вопросу о существовании пути в G_i из вершин, у которых первая тензорная компонента равна s, в вершины, у которых первая тензорная компонента рана t. Поскольку для $k = O(\log n)$ у графа G_i второе собственное число не превосходит 0.99, мы можем проверить данное свойство, перебрав все пути логарифмической длины.

Нужно проверить, что моделирование блуждания по графу G_k моделируется на логарфимической памяти. В самом деле, для хранения номера вершины G_k нам нужно хранить набор из $(i+1)$ компонент; самая первое содержит некоторый номер вершины $G_0 = G''$, а каждая следующая — номер одной из вершин H. Ребро в графе G_i есть путь длины 50 в графе $(G_i \circ H)$. Остаётся понять, как организовать рекурсивный вызов для моделирования одного шага по ребру $(G_i \circ H)$. Если ребро является локальным (соответствует переходу внутри 'галактики' вершин, являющейся копией H), то нам нужно только пересчитать координаты в i-ой компоненте в соответствии с матрицей графа H. Если же ребро соединяет вершины двух соседних галактик, мы рекурсивно вызываем операцию перехода для графа G_{i-1}; (при этом запись в i-ой компоненте текущей вершины нужно интерпретировать как номер ребра, по которому мы выходим из текущей вершины в графе G_{i-1}). Рекурсивный вызов возвращает, во-первых, номер новой вершины v графа G_{i-1} (это содержимое компонент с 0-ой по $(i-1)$-ую), а также номер ребра графа G_i, по которому мы только что прошли, *с точки зрения вершины* v, в которую мы попали (этот номер мы запишем в i-ую компоненту текущей вершины).

Мы предлагаем читателю убедиться, что организация рекурсии требует лишь $O(1)$ ячеек памяти на каждую компоненту $i = 1, \ldots, i_{\max} = O(\log n)$. Таким образом, вся процедура работает на зоне $O(\log n)$.

Лекции 11, 29 апреля.

Часть 19: Тестирование свойств: постановка задачи о формулировка результатов

В этой и следующих лекциях мы рассмотрим алгоритмы, которые "тестируют" некоторые свойства графов, такие как двудольность, расскрашиваемость в определённое число цветов, отсутствие подграфов определённого вида, и т.п. Нас интересуют алгоримы, которые работают очень быстро. Мы хотим, чтобы время работы такого "теста" было значительно меньше, чем число вершин и рёбер в графе (как говорят, алгоритм должен работать за сублинейное время). Понятно, что за такое время алгоритм не может даже полностью прочитать входные данные, т.е., описание графа. Алгоритмы тестирования запрашивают информацию о небольшой (случайно выбранной) части графа и по этим небольшим данным вычисляют ответ.

Поскольку мы не можем позволить себе прочитать данные полностью, форма представления входных данных становится существенной. Мы будем полагать, что граф задан в виде оракула, и мы можем спрашивать у этого оракула про любую пару вершин, соединены ли они ребром.

Разумеется, тест, который не читает описание графа полностью, не может гарантированно определить, является ли заданный граф двудольным, 3-раскрашиваемым, свободным от треугольников, и т.д. Мы берёмся лишь различить между собой две ситуации: графы, которые обладают заданным свойством, и графы, которые *далеки* от любого графа с заданным свойством. Так, в случае с тестированием двудольности мы хотим построить алгоритм, который принимает все действительно двудольные графы и с большой вероятностью отвергает такие графы, которые не станут двудольными, даже если в них удалить небольшой процент рёбер.

Приведём общее определение тестирования совйства. Для определённости будем говорить о графах без параллельных (кратных) рёбер.

Определение. Пусть $\mathcal{P}$ есть некоторое множество графов (если граф G принадлежит $\mathcal{P}$, мы будем говорить, что G обладает свойством $\mathcal{P}$). Дероятностный алгоритм тестирует свойство $\mathcal{P}$ с точностью ε, если выполнены два свойства:

1. Если G с n вершинами обладает свойством $\mathcal{P}$, то с вероятностью 1 алгоритм допускает G.

2. Если любой граф G', который получается из G добавлением или удалением не более εn^2 рёбер, не обладает $\mathcal{P}$, то с вероятностью $> 2/3$ алгоритм отвергает G.

Нас будет интересовать число запросов q, которые алгоритм задаёт оракулу (число ребёр, о наличии или отсутствии которых в данном графе алгоритм узнаёт).

Во всех примерах, которые мы рассмотрим на лекциях, алгоритмы тестирования будут очень простыми. В этой и двух следующих лекциях мы изучим три алгоритма тестирования свойств и докажем их корректность.

Пример 1 тестирования свойства: двудольность. В качестве $\mathcal{P}$ мы берем двудольные графы. Хотим построить такой тест, который с вероятностью 1 допускает все двудольные графы и с вероятностью более $2/3$ отвергает такие графы, которые не станут двудольными даже если в них удалить εn^2 рёбер.

Отметим, что в общем определении тестирования свойств в пункте (2) мы рассматривали G', котрые отличаются от G удалением *и добалением* небольшого числа рёбер. Но свойство двудольности монотонно (добавление новых рёбер не сделает недвудольный граф двудольным). Поэтому в данном случае достаточно рассматривать G', которые получаются из G только удалением небольшой доли рёбер.

Мы покажем, что свойство двудольности тестирует очень простой алгоритм: нужно случайно выбрать в графе $q = O(\frac{1}{\varepsilon^2}\log\frac{1}{\varepsilon})$ вершин, спросить у оракула про все пары из этих вершин и допустить граф, если выбранный подграф окажется двудольным. Таким образом, при каждом фиксированном $\varepsilon > 0$ для тестировнаия двудольности достаточно задать оракулу лишь ограниченное (не зависящее от размера графа!) число вопросов.

Очевидно, что описанный алгоритм тестирования с вероятностью 1 допускает любой двудольный граф. Нетривиальна проврека второй части определения. По существу, нам нужно доказать такой результат из теории графов:

Для всякого графа G выполнено хотя бы одна из двух свойств: либо его можно сделать двудольным, удалив εn^2 рёбер, либо больше $2/3$ индуцированных подграфов в G на $q = O(\frac{1}{\varepsilon^2}\log\frac{1}{\varepsilon})$ вершинах не являются двудольными.

Доказательство этого утверждения и займёт большую чать этой лекции.

Пример 2 тестирования свойства: k-раскрашиваемость. Пусть $k \geq 2$ некоторое целое число. В качестве $\mathcal{P}$ мы берем множество всех графов, вершины которых можно раскрасить в k цветов так, чтобы любые две соседние вершины имели разные цвета (для $k = 2$ получаем свойство двудольности). Требуется построить такой тест, который с вероятностью 1 допускает все k-раскрашиваемые графы и с вероятностью более $2/3$ отвергает такие графы, которые не станут k-раскрашиваемыми даже если в них удалить εn^2 рёбер.

Это свойство также монотонно (добавление новых рёбер может только нарушить свойство k-раскрашиваемости). Поэтому достаточно рассматривать только графы G', которые получаются из G удалением εn^2 рёбер.

Для этой задачи также существует очень простой алгоритм тестирования: нужно случайно выбрать в графе $q = O(\frac{k^2\log k}{\varepsilon^3})$ вершин, спросить у оракула про рёбра между всеми парами выбранных вершин и допустить

граф, если выбранный подграф окажется k-раскрашиваемым. Как и в первом примере очевидно, что тест принимает все k-тестируемые графы. Для доказательства корректности теста остаётся показать, что

для всякого графа G выполнено хотя бы одна из двух свойств: либо его можно сделать k-раскрашиваемым, удалив не более εn^2 рёбер, либо больше $2/3$ индуцированных подграфов в G на $q = O(\frac{k^2 \log k}{\varepsilon^3})$ вершинах нельзя раскрасить в k цветов.

Это утверждление мы докажем в следующей лекции.

Пример 3 тестирования свойства: отсутствие треугольников. В этом примере в качестве $\mathcal{P}$ мы берем множество всех графов, в которых нет труегольников (троек вершин, попарно соединённых рёбрами).

И для этой этой задачи есть простой способ тестирования: нужно случайно выбрать в графе $q(\varepsilon)$ вершин, спросить у оракула про рёбра между всеми парами выбранных вершин и допустить граф, если в выбранном подграфе не окажется теругольников. Как и в первых двух примерах, понятно, что данный тест не ошибается на графах без треуегольников. Для доказательства корректности теста о нужно показать, что выполнена слудющая альтернатива:

Для всякого графа G выполнено хотя бы одна из двух свойств: либо в нём можно разрушить все труегольники, удалив не более εn^2 рёбер, либо больше $2/3$ индуцированных подграфов в G некотрого фиксированного размера $q = q(\varepsilon)$ вершинах содержат хотя бы один треугольник.

Мы докажем нужно нам свойство с помощью леммы Семереди (Szemerédi) о регулярности. Этим мы займёмся на последней лекции курса.

Упраженение: В трёх рассмотренным нами примерах, алгоритмы тестирования свойств существенно использовали случайность. Докажите, что эта особенность тестов неустранима: не существует *детерминированных* алгоритмов тестирования свойств k-раскрашиваемости или отсутствия треугольников, которые задаёт оракулу $O(1)$ вопросов.

Часть 20: Тестирование двудольности графа

Лекции 12, 6 мая.

TODO

Часть 21: Тестирование свойств: проверка k-раскрашиваемости графа

TODO

Лекции 14, 13 мая.

TODO

Часть 22: Лемма Семереди и тестирование графа на отсутствие треугольников

TODO

Часть 23: Доказательство леммы Семереди

TODO (см. статью Yuri Lima, Szemerédi Regularity Lemma).