

## Содержание

Лекция 1. Задача UPATH	2
1 Рандомизированный алгоритм для UPATH	2
Лекция 2. Практические методы дерандомизации	3
2 Задача MAXCUT	3
3 Задача о максимальном дизайне	3
Лекция 3. Вершинные экспандеры	4
4 Экспандеры и их спектральные свойства	4
Лекция 4. Амплификация	5
5 Простые техники амплификации	5
6 Амплификация экспандерами	5
Лекция 5. Экспандеры на основе зигзаг-произведения	6
7 Squaring	6
8 Tensor product	7
9 Zigzag product	7
10 Конструкции экспандеров	8

# Лекция 1. Задача UPATH

## 1 Рандомизированный алгоритм для UPATH

Главный вопрос:  $P = BPP$ ? В книжке «Hardness and randomness» есть некоторые результаты на тему того, что из дерандомизации может следовать  $P \neq NP$ .

Успешные примеры дерандомизации: проверка на простоту (алгоритм AKS), задача UPATH или **S-T-CONN** =  $\{(G, s, t) : \text{в неорграфе } G \text{ есть путь из } s \text{ в } t\}$ .

**Теорема 1.**  $UPATH \in RL$  (randomized logspace).

*Доказательство.* Запустим блуждание из  $s$  на  $N$  шагов. Если в блуждании встретится  $t$ , сказать, что достижимо, иначе нет.

Предельная частота (hitting time) ребра  $P_{uv} = \lim_{n \rightarrow \infty} \frac{E\#\{(s_i, s_{i+1})=(u,v)\}}{n}$  (добавим петли, применим теорию марковских процессов).

$$P_{u,v} = \frac{1}{\text{ожидаемое время первой встречи } (u, v) \text{ после выхода из } v}$$

Аналогично, существует предельная частота вершины.

Так как блуждание равномерно, то  $P_{uv} = \frac{1}{\deg u} P_u$  и  $P_u = \sum_{t:(t,u) \in E} P_{tu}$ .

Тогда  $P_{uv} = \frac{1}{\deg u} \sum_{t:(t,u) \in E} P_{tu}$ . Из этого следует, что все частоты одинаковы, так если есть максимальная частота, а у какого-то смежного меньше, то получается противоречие с равенством. То есть  $P_{uv} = \frac{1}{2m}$ ,  $P_u = \frac{\deg u}{2m}$ .

Пусть  $t_0 = s, t_1, \dots, t_{k-1}, t_k = t$  — путь из  $s$  в  $t$ . Рассмотрим вершину  $t_0$ . Среднее время возврата в  $t_0$  не зависит от истории блуждания, поэтому оно ровно такое, как в пределе. Поэтому мы в среднем не менее, чем за  $\frac{2m}{\deg u}$  мы будем возвращаться в  $t_0$  и рано или поздно пойдем по ребру  $(t_0, t_1)$ . Такими рассуждениями, по неравенству Маркова можно проделать  $4km$  шагов, чтобы с вероятностью  $\geq \frac{1}{2}$  прийти в  $t_k = t$ .  $\square$

**Определение 1.** Граф  $d$ -регулярный, если степени всех вершин равны  $d$ .

**Утверждение 1.** Существует универсальная последовательность поворотов полиномиальной длины, которая посещает все вершины.

Идея доказательства состоит в следующем: можно сделать случайное блуждание, такое длинное, что доля графов, на которых оно не посещает все вершины крайне мала. Тогда, так как таких графов не более  $n^{dn}$ , то можно сделать долю такой маленькой, что найдется последовательность, удовлетворяющая всем графам.

## Лекция 2. Практические методы дерандомизации

### 2 Задача MAXCUT

MAXCUT: разбить вершины графа на 2 множества  $S, T$ , так чтобы между ними было как можно больше ребер.

Если выбрать  $S$  случайно, то ожидаемый размер разреза  $\frac{1}{2}|E|$ , то есть легко можно посторить  $\frac{1}{2}$ -оптимальное приближение. Вопрос в том, как найти его, не используя случайность.

1й-способ: метод условных матожиданий: первую вершину кладем куда угодно, для каждой следующей рассматриваем 2 ситуации: поместить её в левую долю или в правую. Делаем это, максимизируя условное матожидание. Получается обычный жадный алгоритм — поместить вершину так, чтобы было как можно больше ребер между долями.

2й-способ: использование попарной независимости. Используем случайные биты, не независимые в совокупности, а независимые попарно. Суть в том, что обеспечение попарной независимости требует только логарифмического количества случайных бит.

Матрица кода Адамара:  $A$  размером  $(2^l - 1) \times l$ , по строкам все ненулевые вектора из нулей и единиц. Тогда  $y = A \cdot x$ , где  $x$  вектор случайных величин длины  $l$ , будет вектор из равномерно распределенных попарно независимых случайных величин.

Таким образом, если перебрать все случайные биты, мы можем выбрать из них оптимальный и затратить на это полином времени.

### 3 Задача о максимальном дизайне

**Определение 1.**  $S_1, \dots, S_m \subset \{1, \dots, d\}$  есть  $(m, d, l, a)$ -дизайн, если  $|S_i| = l$ , а  $\forall i \neq j \rightarrow |S_i \cap S_j| < a$ .

**Утверждение 1.** Если  $d, l, a$  — фиксированные, то для  $m = \frac{C_d^a}{(C_l^a)^2}$  существует дизайн с такими параметрами.

*Доказательство.* Рассмотрим случайный дизайн.  $E_{S_i}(\#\{j < i, |S_j \cap S_i| \geq a\}) = (i-1)P(|S_j \cap S_i| \geq a) < m \frac{C_l^a C_d^{l-a}}{C_d^l} < 1$ .

Тогда найдется значение, равное 0. □

Отсюда  $\forall \gamma > 0, l, m \in \mathbb{N} \rightarrow \exists (m, d, l, a)$ -дизайн,  $a = \gamma \log m, d = o(\frac{l^2}{a})$ . То есть в полиномиальную кастрюлю можно напихать экспоненциально много сарделек с пересечением в какую-то константную долю, скажем 10%.

Полученный результат можно дерандомизировать с помощью метода условных матожиданий.

## Лекция 3. Вершинные экспандеры

### 4 Экспандеры и их спектральные свойства

Вершинный экспандер — двудольный граф, где любое не слишком большое подмножество левой доли ( $\leq \frac{n}{3}$ ) хорошо расширяется (хотя бы в константу раз).

**Утверждение 1.** Вершинный экспандер существует.

По  $D$ -регулярному графу построим матрицу случайного блуждания  $M = \frac{A}{D}$ , где  $A$  — матрица смежности.

- $u = (\frac{1}{N}, \dots, \frac{1}{N})$  — собственный с  $\lambda = 1$ .
- Все собственные значения  $\leq 1$  по модулю.
- Граф несвязен  $\Leftrightarrow \lambda = 1$  имеет кратность  $> 1$ . В одну сторону очевидно, в другую нужно рассмотреть любой СВ, не пропорциональный  $(1, \dots, 1)$  и взять максимальную компоненту и минимальную — это и есть две компоненты связности.
- Пусть граф связан, тогда  $\lambda = -1$  — СЗ  $\Leftrightarrow$  граф двудольный. В одну сторону очевидно, в другую нужно показать, что у СВ с СЗ  $\lambda = -1$  максимальная компонента равна минус минимальной, далее аналогично предыдущему.

**Определение 1.**  $\lambda(G) = \max_{\pi} \frac{|\pi M - u|}{|\pi - u|} = \max_{x \perp u} \frac{|xM|}{|x|}$ .

**Утверждение 2.**  $\lambda(G)$  — модуль второго СЗ матрицы  $M$ .

*Доказательство.*  $w = \alpha_2 v^2 + \dots + \alpha_n v^n \rightarrow wM = \alpha_2 \lambda_2 v^2 + \dots + \alpha_n \lambda_n v^n$ .

$$|wM|^2 = \alpha_2^2 \lambda_2^2 + \dots + \alpha_n^2 \lambda_n^2 \leq \lambda_2^2 (\alpha_2^2 + \dots + \alpha_n^2) = \lambda_2^2 |w|^2. \quad \square$$

$|\pi M^t - u| \leq \alpha(G)^t |\pi - u| \leq \lambda(G)^t$ , то есть  $\lambda(G)$  — задает скорость сходимости распределения к равномерному.

Утверждается, что если граф связный и не двудольный, то  $\lambda(G) < 1 - \frac{1}{N \cdot D \cdot \text{diam}(G)}$ .

**Теорема 1.** Если  $\lambda(G) \leq \lambda \Rightarrow \forall \alpha \rightarrow G$  —  $(\alpha N, \frac{1}{\alpha + (1-\alpha)\lambda^2})$ -экспандер

*Доказательство.*  $CP(\pi) = |\pi|^2$  — вероятность коллизии.  $CP(\pi) = |\pi - u|^2 + \frac{1}{N}$ .  $CP(\pi) \geq \frac{1}{|\text{Supp} \pi|}$  по КВШ.

$CP(\pi M) - \frac{1}{N} = |\pi M - u|^2 \leq \lambda(G)^2 |\pi - u|^2 \leq \lambda^2 (CP(\pi) - \frac{1}{N})$ . Если  $\pi$  равномерное на  $S$ , то  $CP(\pi) = \frac{1}{|S|}$ , а  $CP(\pi M) \geq \frac{1}{|\text{Supp} \pi M|} = \frac{1}{|N(s)|}$ .

Итого,  $\frac{1}{|N(s)|} - \frac{1}{N} \leq \lambda^2 (\frac{1}{|S|} - \frac{1}{N})$ , подставляя  $|S| \leq \alpha N$ ,  $\frac{1}{N} \leq \frac{\alpha}{|S|}$ , получаем требуемое.  $\square$

Спектральный разрыв:  $\gamma(G) = 1 - \lambda(G)$ .

Известно, что если граф  $D$ -регулярный и является  $(\frac{N}{2}, 1 + \delta)$ -экспандер, то  $\gamma(G) = \Omega\left(\frac{\delta^2}{D}\right)$ .

## Лекция 4. Амплификация

### 5 Простые техники амплификации

Хотим в **RP** уменьшить ошибку с  $\frac{1}{2}$  до  $\frac{1}{2^k}$ . Стандартный метод: повторить  $k$  раз с новыми случайными битами: время увеличится в  $k$  раз, случайных битов нужно  $mk$  вместо  $m$ .

Техника попарной независимости: время увеличено в  $2^k$  раз, но требуется  $m + k$  случайных битов.

**Утверждение 1.** Пусть  $X_1, \dots, X_t$  — попарно независимые СВ со значениями в  $\{0, 1\}$ .  $X = \frac{1}{t} \sum X_i$ ,  $EX = \mu = \frac{1}{t} \sum \mu_i$ . Тогда  $P(|X - \mu| > \varepsilon) < \frac{1}{t\varepsilon^2}$ .

*Доказательство.*  $DX = E(X - \mu)^2 = \frac{1}{t^2} \left( \sum_{i \neq j} \text{cov}(X_i, X_j) + \sum DX_i \right) \leq \frac{1}{t}$ , значит по неравенству Чебышева утверждение доказано.  $\square$

### 6 Амплификация экспандерами

Экспандеры: время увеличено в  $k$  раз, требуется в  $mk$  случайных битов.

Идея: возьмём экспандер, в нём случайную вершину, запустим случайное блуждание длины  $t$  и все вершины по дороге используем в качестве случайных битов для алгоритма.

Нужно показать, что для любого множества вершин, доля которого  $\leq \frac{1}{2}$ , вероятность того, что всё блуждание останется внутри этого множества, будет экспоненциально малой.

**Теорема 1.** Пусть  $G$  —  $d$ -регулярный экспандер с параметром  $\lambda = 1 - \gamma$ .  $B \subset V(G)$ ,  $\frac{|B|}{|V(G)|} = \mu$ .  $v_1, \dots, v_t$  — случайное блуждание со стартом в начальной вершине.

Тогда  $P(\forall i v_i \in B) \leq (\mu + \lambda(1 - \mu))^t$ .

*Доказательство.* Будем считать, что любой вектор разложен на компоненты  $v = v^\parallel + v^\perp$ ,  $v^\parallel = \frac{\langle u, v \rangle}{\langle u, u \rangle} u$ ,  $u = (\frac{1}{n}, \dots, \frac{1}{n})$ ,  $v^\perp = v - v^\parallel$ .

Пусть  $M$  — матрица блуждания.  $vM = (v^\parallel + v^\perp) = v^\parallel M + v^\perp M = v^\parallel + v^\perp M$ . Однако,  $\|v^\perp M\| \leq \lambda \|v^\perp\|$ . Отметим, что для распределения вероятностей очевидно  $v^\parallel = u$ .

Также рассмотрим матричное разложение:  $vM = v^\parallel + v^\perp = \gamma v^\parallel + (\lambda v^\parallel + v^\perp M) = \gamma vJ + \lambda vE = v(\gamma J + \lambda E)$ , где  $J = \frac{1}{N}(1, \dots, 1)^T(1, \dots, 1)$  — матрица из единиц.

$vJ = v^\parallel$ ,  $v^\perp J = v^\parallel$ ,  $v^\perp J = 0$ .  $E$  определена как остаточная матрица и мы будем показывать про нее, что  $\|vE\| \leq \|v\|$ .

**Утверждение 2.** Граф — экспандер с параметром  $\lambda \Leftrightarrow M = \gamma J + \lambda E$ ,  $\|E\| \leq 1$ .

*Доказательство.*  $E = \frac{M-\gamma J}{\lambda}$ .  $uE = \frac{uM-\gamma uJ}{\lambda} = \frac{u(1-\gamma)}{\lambda} = u$ .

Если  $v \perp u$ , то  $vE = \frac{v^\perp - \gamma v^\perp J}{\lambda} = \frac{1}{\lambda} v^\perp M \Rightarrow \|v^\perp E\| = \frac{1}{\lambda} \|v^\perp M\| \leq \|v^\perp\|$ .  $\square$

Пусть  $P = \text{diag}\{\chi_B(i)\}$ ,  $P(i, j) = I(i = j, i \in B)$ . Тогда  $P(v \in B) = |\pi P|_1$ .

**Утверждение 3.**  $P(v_1, \dots, v_t \in B) = |uP(MP)^{t-1}|_1$ .

*Доказательство.* Более того,  $P(v_1, \dots, v_{l+1} \in B, v_{l+1} = i) = (uP(MP)^l)_i$ . Докажем индукцией по  $l$ :

База  $l = 0$  очевидна. Показываем переход: ясно, что  $(uP(MP)^l \cdot M)_i = P(v_1, \dots, v_{l+1} \in B, v_{l+2} = i)$ . Если еще раз умножить на  $P$ , то все координаты для  $i \notin B$ .  $\square$

$P^2 = P$ , а значит  $uP(MP)^{t-1} = uP(PMP)^{t-1}$ .

**Утверждение 4.**  $\|PMP\| \leq \mu + \lambda(1 - \mu)$ .

*Доказательство.*  $\|PMP\| = \|P(\gamma J + \lambda E)P\| = \gamma \|PJP\| + \lambda \|PEP\| \leq \gamma \|PJP\| + \lambda$ .

$xPJP = yJP = N(yu^T)(uP) = (\sum y_i)(uP)$ ,  $\|xPJP\| = (\sum y_i)\|uP\| \leq (\sqrt{\mu N}\|y\|)\sqrt{\frac{P}{N}} = \mu\|y\| \leq \mu\|x\| \Rightarrow \|PJP\| \leq \mu$ .

Итого,  $\|PMP\| \leq \gamma\mu + \lambda = \mu + \lambda(1 - \mu)$ .  $\square$

Итого,  $P(\forall i v_i \in B) \leq |uP(MP)^{t-1}|_1 \leq \sqrt{\mu N}\|uP(PMP)^{t-1}\| = \sqrt{\mu N}\|uP\|\|PMP\|^{t-1} \leq \mu(\mu + (1 - \mu)\lambda)^{t-1} < (\mu + (1 - \mu)\lambda)^t$ .  $\square$

Для ВРР применима аналогичная техника.

## Лекция 5. Экспандеры на основе зигзаг-произведения

Строим граф с тремя параметрами  $N$  — число вершин,  $D$  — степень каждой вершины,  $\gamma = 1 - \lambda$  — spectral gap.

Рассмотрим три операции, для которых оценим влияние на каждый параметр.

## 7 Squaring

Эта операция преобразует  $G = (V, E) \mapsto (V, E') = G^2$ , причем ребро в новом графе есть ребро  $(u, w) \in E' \Leftrightarrow \exists v : (u, v) \in E, (v, w) \in E$  с кратностью, равной числу таких  $v$ . В матричном виде это собственно возведение матрицы в квадрат.

Тогда  $\|xM^2\| \leq \lambda^2\|x\|$ . При такой операции  $(N, D, 1 - \lambda) \mapsto (N, D^2, 1 - \lambda^2)$ .

## 8 Tensor product

Принимает на вход  $G_1 = (V_1, E_1), M_1$  с параметрами  $D_1, \gamma_1$  и  $G_2 = (V_2, E_2), M_2$  с параметрами  $D_2, \gamma_2$ . Результата  $G_1 \otimes G_2 = (V_1 \times V_2, E), D = D_1 D_2$ .  $(i, j)$  сосед пары  $(v_1, v_2)$  есть пара из  $i$ -го соседа  $v_1$  и  $j$ -го соседа  $v_2$ .

Случайное блуждание по такому графу — это независимое одновременное случайное блуждание по двум сомножителям.

**Утверждение 1.**  $\gamma(G) = \min\{\gamma(G_1), \gamma(G_2)\}$ .

*Доказательство.* Покажем, что для  $\forall x \in \mathbb{R}^{N_1 N_2}, x \perp u_{N_1 N_2} \rightarrow \|xM\| \leq \lambda \|x\|$ .

$x = x^\parallel + x^\perp, x^\parallel \parallel u_{N_2}$  в каждом облаке.  $x^\parallel = y \times u_{N_2}$ , где  $y \perp u_{N_1}$ .

$\|xM\| = \|y \otimes u_{N_2}\| = \|x^\parallel M + x^\perp M\|^2 = \|x^\parallel M\|^2 + \|x^\perp M\|^2 \leq \lambda_1^2 \|x^\parallel\|^2 + \lambda_2^2 \|x^\perp\|^2$ . Поясним, почему это так:

$x^\parallel M = (y \otimes u_{N_2})(M_1 \otimes M_2) = (yM_1) \otimes (u_{N_2}M_2) = yM_1 \otimes u_{N_2} \cdot \|yM_1\| \leq \lambda_1 \|y\| \Rightarrow \|x^\parallel M\| \leq \lambda_1 \|x^\parallel\|$ .

$x^\perp M = x^\perp (I_{N_1} \otimes M_2)(M_1 \otimes I_{N_2})$ . Первое уменьшает норму в  $\lambda_2$  раз, второе нормы не уменьшает, поэтому  $\|x^\perp M\| \leq \lambda_2 \|x^\perp\|$ .

Из конструкции видно, что  $x^\parallel M \perp x^\perp M$ , значит утверждение доказано.  $\square$

## 9 Zigzag product

Принимает на вход  $G = (N, D_1, \gamma_1), H = (D_1, D_2, \gamma_2)$  и выдает  $G \mathbin{\textcircled{Z}} H$  с параметрами  $(ND_1, D_2^2, \gamma = \gamma_1 \gamma_2^2), \lambda \leq \lambda_1 + 2\lambda_2$ .

$V = V_1 \times V_2, (u \in V_1, i \in V_2)$ . Сосед  $(u, i)$  с номером  $(a, b)$  — это:

- $i'$  —  $a$ -й сосед  $i$  в  $H$ .
- $v$  —  $i'$ -й сосед  $u$  в  $G$ .
- $j'$  — номер  $u$  среди соседей  $v$ .
- $j$  —  $b$ -й сосед  $j'$  в  $H$ .
- $(v, j)$  — результат.

Если  $H$  — полный граф с петлями, то  $G \mathbin{\textcircled{Z}} H = G \otimes H$ .

**Утверждение 2.** Если  $A, B, M$  — матрицы случайных блужданий графов  $G, H, G \mathbin{\textcircled{Z}} H$ , то  $M = \tilde{B} \tilde{A} \tilde{B}$ , где  $\tilde{B} = I_{N_1} \otimes B$ ,  $\tilde{A}_{(u,i),(v,j)} = 1$ , если ребро  $(u, v)$  присутствует в  $G$ , имеет номер  $i$  среди соседей  $u$  и номер  $j$  среди соседей  $v$ .

*Доказательство.* Следует из конструкции.  $\square$

$B = \gamma_2 J + (1 - \gamma_2)E$ , где  $J$  есть матрица из  $\frac{1}{D_1}$ , а  $\|E\| \leq 1$ .

Тогда  $\tilde{B} = \gamma_2 \tilde{J} + (1 - \gamma_2) \tilde{E}$ .

$$B = (\gamma_2 \tilde{J} + (1 - \gamma_2) \tilde{E}) \hat{A} (\gamma_2 \tilde{J} + (1 - \gamma_2) \tilde{E}) = \gamma_2^2 \tilde{J} \hat{A} \tilde{J} + (1 - \gamma_2^2) F, \|F\| \leq 1.$$

При этом  $\tilde{J} \hat{A} \tilde{J} = A \otimes J$  так как  $J$  соответствует полному графу. Тогда  $M = \gamma_2^2 A \otimes J + (1 - \gamma_2^2) F$ .

$$\|xM\| \leq \gamma_2^2 \|xA \otimes J\| + (1 - \gamma_2^2) \|xF\| \leq (\gamma_2^2(1 - \gamma_1) + (1 - \gamma_2^2)) \|x\| = (1 - \gamma_1 \gamma_2^2) \|x\|.$$

## 10 Конструкции экспандеров

Первая конструкция. Пусть есть экспандер  $H$  с параметрами  $(D^4, D, \frac{7}{8})$ . Будем итерировать процесс  $G_1 = H^2, G_{t+1} = G_t^2 \otimes H$ .

$G_1$  тогда будет иметь параметры  $(D^4, D^2, \frac{63}{64})$ . Если  $G_t$  имеет параметры  $(N, D^2, 1 - \lambda)$ , то у  $G_t^2$  они будут  $(N, D^4, 1 - \lambda^2)$ . Тогда  $G_{t+1}$  имеет параметры  $(ND^4, D^2, (1 - \lambda^2) \frac{49}{64})$ . Если  $\lambda > \frac{1}{2}$  (что верно для  $G_1$ ), то разрыв сохраняется  $> \frac{1}{2}$ .

Вторая конструкция дает более быстрый рост графа. Если  $H$  — экспандер с параметрами  $(D^8, D, \frac{7}{8})$ , то  $G_1 = H^2, G_{t+1} = (G_t \otimes G_t)^2 \otimes H$ .

$(G_t \otimes G_t)^2$  имеет параметры  $(N^2, D^8, > \frac{3}{4})$ .  $(G_t \otimes G_t)^2 \otimes H$  тогда имеет параметры  $(N^2 D^8, D^2, > \frac{1}{2})$ .

Если считать таким образом, то можно за полилог перечислить всех соседей конкретной вершины.