Содержание

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** = $\{(G, s, t)$: в неорграфе G есть пусть из s 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 $P_{uv} = \lim_{n\to\infty} \frac{E\#\{(s_i,s_{i+1})=(u,v)\}}{n}$ (добавим петли, применим теорию марковских процессов).

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

Аналогично, существует предельная частота вершины.

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

Пусть $t_0 = s, t_1, \ldots, t_{k-1}, t_k = t$ — 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 $\geqslant \frac{1}{2}$ прийти в $t_k = t$. □

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

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

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

Тогда найдется значение, равное 0. □

Отсюда $\forall \gamma > 0, l, m \in \mathbb{N} \to \exists (m, d, l, a)$-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 ($\leqslant \frac{n}{3}$) 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.

- $u = (\frac{1}{N}, \dots, \frac{1}{N})$ — собственый с $\lambda = 1$.
- Все собственные значения $\leqslant 1$ 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 связен, 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. $\lambda(G) = \max\limits_{\pi} \frac{|\pi M - u|}{|\pi - u|} = \max\limits_{x \perp u} \frac{|xM|}{|x|}$.

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

Доказательство. $w = \alpha_2 v^2 + \dots \alpha_n v^n \to wM = \alpha_2 \lambda_2 v^2 + \dots + \alpha_n \lambda_n v^n$.
$|wM|^2 = \alpha_2^2 \lambda_2^2 + \dots + \alpha_n^2 \lambda_n^2 \leqslant \lambda_2^2(\alpha_2^2 + \dots + \alpha_n^2) = \lambda_2^2 |w|^2$. □

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

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

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

Доказательство. $CP(\pi) = |\pi|^2$ — вероятность коллизии. $CP(\pi) = |\pi - u|^2 + \frac{1}{N}$. $CP(\pi) \geqslant \frac{1}{|\mathrm{Supp}\pi|}$ по КБШ.

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

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

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

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

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 $X_1, \ldots, X_t$ — 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. $DX = E(X-\mu)^2 = \frac{1}{t^2}\left(\sum_{i\neq j} cov(X_i, X_j) + \sum DX_i \leqslant \frac{1}{t}\right)$, значит по неравенству Чебышева утверждение доказано. □

6 Амплификация экспандерами

Экспандеры: время увеличино 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 люого множества вершин, доля которого $\leqslant \frac{1}{2}$, вероятность того, что всё блуждание останется внутри этого множества, будет эскпоненциально малой.

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

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

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

Пусть M — матрица блуждания. $vM = (v^{\parallel} + v^{\perp}) = v^{\parallel}M + v^{\perp}M = v^{\parallel} + v^{\perp}M$. Однако, $\left\|v^{\perp}M\right\| \leqslant \lambda \left\|v^{\perp}\right\|$. 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 $J = \frac{1}{N}(1, \ldots, 1)^T(1, \ldots, 1)$ — матрица из единиц.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Для **BPP** 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 ребре $(u, w) \in E' \Leftrightarrow \exists v : (u, v) \in E, (v, w) \in E$ с кратностью, равной числу таких v. В матричном виде это собственно возведение матрицы в квадрат.

Тогда $\|xM^2\| \leqslant \lambda^2\|x\|$. 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, γ_1 и $G_2 = (V_2, E_2), M_2$ с параметрами D_2, γ_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 $\forall x \in \mathbb{R}^{N_1 N_2}, x \perp u_{N_1 N_2} \to \|xM\| \leqslant \lambda \|x\|$.

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

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

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

$x^{\perp} M = x^{\perp}(I_{N_1} \otimes M_2)(M_1 \otimes I_{N_2})$. Первое уменьшает норму в λ_2 раз, второе нормы не уменьшает, поэтому $\|x^{\perp} M\| \leqslant \lambda_2 \|x\|$.

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

9 Zigzag product

Принимает на вход $G = (N, D_1, \gamma_1), H = (D_1, D_2, \gamma_2)$ и выдает $G ⓩ H$ с параметрами $(ND_1, D_2^2, \gamma = \gamma_1 \gamma_2^2), \lambda \leqslant \lambda_1 + 2\lambda_2$.

$V = V_1 \times V_2, (u \in V_1, i \in V_2)$. 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 $G ⓩ H = G \otimes H$.

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

Доказательство. Следует из конструкции. □

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

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

$$B = (\gamma_2\widetilde{J} + (1-\gamma_2)\widetilde{E})\widehat{A}(\gamma_2\widetilde{J} + (1-\gamma_2)\widetilde{E} = \gamma_2^2\widetilde{J}\widehat{A}\widetilde{J} + (1-\gamma^2)F, \|F\| \leqslant 1.$$

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

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

10 Конструкции экспандеров

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

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 $G_1 = H^2$, $G_{t+1} = (G_t \otimes G_t)^2 ⓩ H$.

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

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

Лекция 6. Логарифмический алгоритм для UPATH

11 Общая идея

Первый шаг — доказать, что диаметр экспандера есть $O(\log_{\frac{1}{\lambda}})$ при константном λ.

Если степень экспандера константна, то все пути длины $O(\log N)$ можно перебрать за полиномиальное время на логарифмической памяти.

Следующая идея: с помощью зигзаг-произведения превращать граф в экспандер, сохраняя связность. В полученном экспандере проверим наличие пути перебором.

12 Диаметр экспандера

Утверждение 1. Если π — распределение верятностей, M — матрица случайного блуждания, $u = (\frac{1}{N}, \ldots, \frac{1}{N})$, то $\|\pi M^l - u\|_2 \leqslant \lambda^l$.

Доказательство. $\pi = \pi^{\|} + \pi^{\perp} = u + \pi^{\perp}$. $\pi M^l = u + \pi^{\perp}M^l \Rightarrow \|\pi M^l - u\| = \|\pi^{\perp}M^l\| \leqslant \lambda^l\|\pi\| \leqslant \lambda^l\|\pi\|_1 = \lambda^l$. □

13 Приведение графа к экспандеру

Утверждение 2. Можно считать, что данный граф 3-регулярный.

Доказательство. Каждую точку, у которой меньше трёх соседей, дополним кратными петлями. Каждую точку, из которой выходит больше трёх ребер преобразуем в цикл длины равной её степени с торчащими рёбрами куда надо. □

Алгоритм будет следующий:

- Выберем граф H с параметрами $(D^4, D, \frac{3}{4})$, D — константа.
- D^2-регуляризуем граф, притом сделаем его не двудольным (петлей, например).
- $k = 1, \ldots, l = O(\log N)$, $G_k = G_{k-1}^2 ⓩ H$, s_k, t_k — произвольные вершины из облаков s_{k-1}, t_{k-1}.
- Проверяем s — t связность в экспандере перебором.

Утверждение 3. Алгоритм корректен.

Доказательство. Граф недвудольный и связный, значит λ отделено от 1, и после шага алгоритма все так и останется. Это рассуждение можно применить для каждой связной компоненты исходного графа, значит компоненты сохраняются.

Пусть C_k — компонента связности G_k, содержащая s_k. $\gamma(C_0) = \frac{1}{poly(N)}$. $\gamma(C_{k-1}^2) \geqslant 2\gamma(C_{k-1}) - \gamma^2(C_{k-1})$. Тогда:

$$\gamma(C_{k-1}^2 ⓩ H) \geqslant \frac{2 \cdot 9}{16}\gamma(C_{k-1})(1 - \frac{\gamma(C_{k-1})}{2}) \geqslant \min\left\{\frac{35}{32}\gamma(C_{k-1}), \frac{1}{18}\right\}$$

.

Для вычисления соседа в G_k нужен 1 переход в G_{k-1}^2 и 2 перехода в H. Переходы в H памяти не требуют, то есть в итоге получаем два перехода в G_{k-1}.

Логарифмическая память не зависит от модели вычислений, но доказать, что на каждой итерации добавляется константная память можно только в конкретной модели. Мы рассматрим такую модель: лента с исходным графом G, лента с u, i + дополнительная информация, рабочая лента. При запросе мы меняем (u, i) на (v, j), не меняя дополнительной информации. В такой модели нетрудно придумать, как вычислять квадрат и нормально так попотеть. По сути, утверждается, что рекурсия здесь почти хвостовая. □

Лекция 9. Экстракторы I

14 Общая идея

Есть ряд процессов, результат которых довольно случайный, но никаких гарантий, как можно использовать такую случайность, нет. Так появляется задача получения независимых случайных бит из не совсем случайной последовательности.

Пример 1. Если есть независимые одинаково распределенные случайные биты, но вероятность единицы не равна $\frac{1}{2}$, то можно получать случайные биты так двукратным бросанием: если выпало 01, то вернем 0, если 10, то 1, в противном случае бросим еще раз.

Если биты независимые, но вероятности разные на отрезке $[\delta; 1-\delta]$, то $P(b_1 \oplus \ldots \oplus b_m = 1) \to \frac{1}{2}$, так как $p(1-\delta_m) + (1-p)\delta_m$ это выпуклая комбинация.

Более общий класс источников это k-слабые источники случайности. *Мин-энтропия* это $H_\infty(B) = -\log_2 \left(\max\limits_x P(\vec{b} = x)\right)$.

$H_\infty(\vec{b}) \geqslant k \Leftrightarrow \forall x P(\vec{b} = x) \leqslant \frac{1}{2^k}$. В этом случае $\vec{b}$ содержит хотя бы k случайных битов.

Плоские распределения на $K \subset \{0,1\}^n$, $|K| = 2^k$ — это равномерные распределения.

Теорема 1. *Если $H_\infty(\vec{b}) \geqslant k$, то $\vec{b}$ — выпуклая комбинация плоских источников.*

Определение 1. *Seeded-экстрактор* $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ с параметрами (k, ε) обладает свойством, что: $\forall \xi, H_\infty(\xi) \geqslant k \Rightarrow Ext(\xi, U_d)$ ε-близка к U_m.

Вероятностно можно показать существование seeded-экстрактора с параметрами $m = k + d - 2\log\frac{1}{\varepsilon} - O(1)$ и $d = \log(n-k) + 2\log\frac{1}{\varepsilon} + O(1)$.

Определение 2. *Multisource-экстрактор* $MExt : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ с параметрами (k, ε) обладает свойством, что: $\forall \xi, \eta : H_\infty(\xi), H_\infty(\eta) \geqslant k, \xi \perp \eta \Rightarrow Ext(\xi, \eta)$ ε-близка к U_m.

Лекция 10. Экстракторы II

Про каждый из описанных объектов есть вероятностное доказательство существоввования, которое не приводится

15 Комбинаторная интерпретация

Seeded-экстрактор можно представить как двудольный граф с долями $\{0,1\}^n$ и $\{0,1\}^m$ и рёбрами проведенными естественным образом. Тогда условие на

экстактор запишется как

$$\forall S : |S| = 2^k \to \left| \frac{|E(S,T)|}{|S|D} - \frac{|T|}{2^m} \right|$$

.

Multisource-экстрактор удобно рассматривать как таблицу, раскрашенную в один из $\{0,1\}^m$ цветов. Тогда условие на экстрактор будет выглядеть так: для любых достаточно больших наборов столбцов и строк S, T число клеток x, покрашенных в цвета из множества $Q \subset \{0,1\}^m$ удовлетворяет следующему неравенству:

$$\left| \frac{x}{|S||T|} - \frac{|Q|}{2^m} \right| < \varepsilon.$$

16 Некоторые усиления и родственные объекты

Если, например, взять multisource-экстрактор, и испортить в нём распределение битов в первой строке, то общее распределение пострадает не сильно. Поэтому можно рассматривать экстраткторы в сильном смысле.

Определение 1. Multisource-экстрактор называется *экстрактором в сильном смысле*, если условные распределения $MEXt(x,y) \mid y$ и $Mext(x,y) \mid x$ тоже ε-близки к равномерному.

Определение 2. Seeded-экстрактор называется *экстрактором в сильном смысле*, если $(y, Ext(x,y))$ — ε-близко к равномерному.

Определение 3. Двудольный граф, в котором можно пошагово на запрос вершины в левой доле говорить соседа в правой доле (так, чтобы набор рёбер оставался парасочетанием), называется *графом, допускающим online-парасочетание.*

Определение 4. *Дисперсер* это функция $Disp(x,y)$ такая, что для $\forall \xi, H_\infty(\xi) \geqslant k, \eta \sim U_{2^d}, \eta \perp \xi \to Disp\left(\{0,1\}^n \times \{0,1\}^d\right)$ занимает $\geqslant 1-\varepsilon$ от $\{0,1\}^m$.

17 Конструкции экстракторов

Пусть $H : \{0,1\}^n \to \{0,1\}^m$ — семейство хеш-функций, тогда организуем экстрактор следующим образом: $Ext(x,h) = h(x)$.

Лемма (Leftover hash lemma)**.** *Если $m = k - 2\log\frac{1}{\varepsilon}$, то полученный объект — сильный $\left(k, \frac{\varepsilon}{2}\right)$-экстрактор.*

Доказательство. Нужно доказать, что $(h, h(x)) \sim U_d \times U_m$. Обозначим $D = 2^d, M = 2^m, N = 2^n$, тогда $M = K\varepsilon^2$.

Оценим вероятность коллизии: $P_{x,h,x',h'}\{Ext(x,h) = Ext(x',h') \wedge h = h'\} = P_{x,h,x',h'}\{h = h' \wedge (x = x' \vee (x \neq x' \wedge h(x) = h(x')))\} \leqslant \frac{1}{DK} + \frac{1}{DM} = \frac{1}{DK}(1+\varepsilon^2)$.

Теперь оценим L_2 расстояние от нашего распределения до равномерного: $\|(h,h(\xi)) - U_d \times U_m\|^2 = \sum\limits_{z,t}(P(h-z, h(\xi) = t) - \frac{1}{DM})^2 = P(\text{коллизии}) - \frac{2}{DM}\sum\limits_{z,t} P(h=z, h(\xi)=t) - \frac{1}{DM} \leqslant \frac{1}{DK} + \frac{1}{DM} - \frac{1}{DM} = \frac{\varepsilon^2}{DM}$.

Тогда $|(h,h(\xi)) - U_d \times U_m|_1 \leqslant \varepsilon$, а значит статистическое расстояние не больше $\frac{\varepsilon}{2}$. □

Это довольно плохой экстрактор, однако, лучшие построенные ограничиваются $O(\log^2 n)$ дополнительными чисто-случайными битами.