Вычислительно трудные задачи и дерандомизация
Лекция 9: Экспандеры и понижение вероятности ошибки

Дмитрий Ицыксон

ПОМИ РАН

26 апреля 2009

План

1. Полиномиальное понижение ошибки без использования дополнительных случайных битов
2. Экспоненциальное понижение ошибки с использованием очень маленького числа дополнительных случайных битов

RP: вероятностные алгоритмы с односторонней ошибкой

Определение:

Язык $L \in \mathbf{RP}$, если существует полиномиальный вероятностный алгоритм A, такой что

- $A(x) = 0$, при $x \notin L$
- $P\{A(x) = 1\} \geq \frac{1}{2}$, при $x \in L$

Цель

Уменьшить вероятность ошибки, используя как можно меньше дополнительных случайных битов.

Комбинаторные экспандеры

Граф $G(V, E)$ называется (n, d, c)-комбинаторным экспандером, если:

- В нем n вершин
- Все вершины имеют степень d
- $\forall A \subset V, |A| \leq \frac{n}{2}$ выполняется $|A \cup \Gamma(A)| \geq (1 + c)|A|$.
- $\Gamma(A) = \{v \in V \mid \exists a \in A : (v, a) \in E\}$

Экспандер называется явным, если существует полиномиальный алгоритм, который по номеру вершины выдает номера его соседей.

Понижение вероятности ошибки

- Пусть язык L решается алгоритмом A с односторонней ошибкой.
- Пусть A использует r случайных битов
- $\epsilon 2^r$ плохих случайных строк (на которых алгоритм дает неправильный ответ)
- Рассмотрим явный $(2^r, d, c)$-комбинаторный экспандер. В каждой вершине последовательность случайных битов.
- Выберем случайным образом вершину (потратив r случайных битов). И запустим алгоритм со всеми последовательностями случайных битов, которые лежат на расстоянии l от данной вершины. Выдадим 1, если ≥ 1 из ответов был 1.
- Пусть B — множество плохих вершин (из которых мы не запустим алгоритм в хороших вершинах).
- $|B|(1+c)^l \leq \epsilon 2^r \implies$ доля плохих вершин $\frac{\epsilon}{(1+c)^l}$.

Понижение вероятности ошибки

- Если $l = \log n$, то потеря по времени $poly(n)$, ошибка уменьшается в $poly(n)$ раз.
- А если надо уменьшить ошибку в 2^n раз?
- Случайно выберем вершину графа (потратив r случайных битов).
- Устроим случайное блуждание длины k (потратим O(k) битов).
- Запустим алгоритм на строчках в k вершинах блуждания. Выдадим 1, если ≥ 1 из ответов был 1.
- Наша цель показать, что так можно уменьшить ошибку до $2^{\Omega(k)}$.

Алгебраический экспандер

Граф $G(V, E)$ называется (n, d, α)-алгебраическим экспандером, если:

- В нем n вершин
- Все вершины имеют степень d
- A — нормированная матрица смежности $A_{i,j} = \frac{k}{d}$, если вершины i и j соединены k ребрами.
- λ — второе по абсолютной величине собственное число матрицы A, $|\lambda| \leq \alpha < 1$.

Теорема. Если G является (n, d, α)-алгебраическим экспандером, то он является и $(n, d, \frac{1-\alpha}{2d})$-комбинаторным экспандером.

Определение. $\|A\| = \max\{\|Av\|_2 : \|v\|_2 = 1\}$

Лемма. Пусть A — нормализованная матрица (n, d, α)-экспандера. Тогда $A = (1-\alpha)J + \alpha C$, где J — матрица $n \times n$, $J_{ij} = \frac{1}{n}$, а $\|C\| \leq 1$.

Доказательство.

- $C = \frac{1}{\alpha}(A - (1-\alpha)J)$. Надо доказать: $\forall v, \|Cv\|_2 \leq \|v\|_2$.
- $v = \gamma\mathbf{1} + w$, где $w \perp \mathbf{1}$.
- $A\mathbf{1} = \mathbf{1}$, $J\mathbf{1} = \mathbf{1}$, $Jw = 0$.
- $Cv = \frac{1}{\alpha}(A - (1-\alpha)J)(\gamma\mathbf{1} + w) = \gamma\mathbf{1} + \frac{1}{\alpha}Aw$.
- $\|Cv\|^2 = \|\gamma\mathbf{1}\|^2 + \frac{1}{\alpha}\|Aw\|^2 \leq \|\gamma\mathbf{1}\|^2 + \|w\|^2 = \|v\|^2$

Случайное блуждание

- Есть $(n = 2^r, d, \alpha)$ — алгебраический экспандер.
- Каждой вершине сопоставлена строка из r случайных битов.
- Пусть X — это множество плохих вершин. $|X| = \epsilon n$.
- Оценим вероятность при случайном блуждании ни разу не выйти из X.
- Пусть B — это матрица проекции на X. Т.е., если $i \in X$, то $(Bu)_i = u_i$, иначе $(Bu)_i = 0$.
- $p_0 = (\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n})$ — начальное распределение.
- $p_1 = Bp_0$ — вектор, ненулевые координаты соответствуют X. i-я координата — вероятность случайного блуждания длины 1 по вершинам из X, заканчивающегося в i.

Случайное блуждание

- $p_0 = (\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n})$ — начальное распределение.
- $p_1 = Bp_0$ — вектор, ненулевые координаты соответствуют X. i-я координата — вероятность случайного блуждания длины 1 по вершинам из X, заканчивающегося в i.
- $p_2 = BABp_0$
- $p_l = (BA)^{l-1}p_0$ — вектор, ненулевые координаты соответствуют X. i-я координата — вероятность случайного блуждания длины l по вершинам из X, заканчивающегося в i.
- Наша цель оценить $\|p_k\|_1 = \|(BA)^{k-1}Bp_0\|_1$
- $\|v\|_1 \leq \sqrt{n}\|v\|_2$
- $BA = B((1-\alpha)J + \alpha C)$
- $\|BA\| \leq (1-\alpha)\|BJ\| + \alpha\|BC\|$
- $\|Bp_0\| = \sqrt{\frac{\epsilon n}{n^2}} = \frac{\sqrt{\epsilon}}{\sqrt{n}}$

Случайное блуждание

- Наша цель оценить $\|p_k\|_1 = \|(BA)^{k-1}Bp_0\|_1$
- $\|v\|_1 \leq \sqrt{n}\|v\|_2$
- $BA = B((1-\alpha)J + \alpha C)$
- $\|BA\| \leq (1-\alpha)\|BJ\| + \alpha\|BC\|$
- $\|Bp_0\| = \sqrt{\frac{\epsilon n}{n^2}} = \frac{\sqrt{\epsilon}}{\sqrt{n}}$
- $\|BJ\| = \sqrt{\epsilon}$
- $\|B\| \leq 1$
- $\|BA\| \leq (1-\alpha)\sqrt{\epsilon} + \alpha$
- $\|(BA)^{k-1}Bp_0\|_2 \leq ((1-\alpha)\sqrt{\epsilon} + \alpha)^{k-1}\frac{\sqrt{\epsilon}}{\sqrt{n}}$
- $\|p_k\|_1 = \|(BA)^{k-1}Bp_0\|_1 \leq ((1-\alpha)\sqrt{\epsilon} + \alpha)^{k-1}\sqrt{\epsilon}$