Филиппова Анастасия

Домашнее задание 6

1

Язык L принадлежит классу RP, если существует такой предикат $V(x,r) \in P$ и такой полинома $q(|x|) = |r|$, что:
если $x \in L$, то $P(V(x,r) = 1) \geqslant \frac{1}{2}$,
если $x \notin L$, то $P(V(x,r) = 1) = 0$. (r — результаты "бросаний монетки"в результате работы МТ, то есть случайная последовательность битов).
Тогда любое значение r, при котором $V(x,r) = 1$ будет доказательством того, что $x \in L$. То есть можем передать его как сертификат и получим, что $L \in NP$.

4

(i) Проверим следующим образом: $AB = C \iff AB - C = E_0 \iff (AB - C)x = 0$, где E_0 — нулевая матрица. Следовательно, получаем систему из n полимонов степени не выше 1 каждый. Выберем какой-то вектор ξ. Тогда каждый из полиномов обращается при данных значениях с вероятностью не больше чем $\frac{n}{N}$. То есть все одновременно обращаются в ноль с вероятностью не более $(\frac{n}{N})^n$. Получается, если матрицы не равны, случайный вектор оказывается "удачным"с вероятностью не больше $(\frac{n}{N})^n$. Тогда $p = (\frac{n}{N})^n, N = \frac{n}{p^{1/n}}$.
(iv) Чтобы уменьшить N можно выполнять немного другую проверку: $A(Bx)x = (Cx)x$, тогда, в результате умножения, получаем один полином от n переменных степени не выше 2. Тогда вероятность того, что полином не равен нулю, но при подобранном x обнуляется не более $\frac{2n}{N}$ по лемме. $N = \frac{2n}{p}$.
При проверке $A(Bx)y = (Cx)y$ тоже самое, но полином от $2n$ переменных, $N = \frac{2n}{p}$.

3

(i) Пусть язык $L \in BPP$. Пусть BPP_w — класс таких языков, на входе из языка вероятностная машина Тьюринга ошибается с вероятностью не больше чем $\frac{1}{2} + \epsilon$, где $0 < \epsilon \leq 1/2$ и дает ответ за полиномиальное в среднем число шагов. Докажем, что $BPP = BPP_w$.
$BPP \subset BPP_w$, так как $\frac{1}{3} < \frac{1}{2} + \epsilon$.
Покажем обратное включение: пусть есть машина M, принимающая слово из языка с вероятностью строго больше $\frac{1}{2}$. Построим машину M': запустим M n раз, получим последовательность из 0 и 1. Если, количество 1 больше половины — выдаем 1, иначе 0. Покажем, что вероятность правильного ответа M' при $n = poly(|x|)$ не меньше $\frac{2}{3}$. Машина M выдает правильный ответ с вероятностью строго больше $1/2$. Тогда вероятность i успехов в n испытаниях (машина M не ошибакется) равна $C_n^i p^i (1-p)^{n-i}$. Оценим эту вероятность с помощью неравенства Хефдинга, с вероятностью успеха $p + \epsilon$ $P(M'$ не ошибется $\geqslant 1 - e^{-2\epsilon^2 n}$. В нашем случае $p = 1/2$. Тогда при $n = \lfloor \frac{\ln 3}{2\epsilon^2} \rfloor + 1$, вероятность того, что машина вероятностная машина Тьюринга M' дает правильный ответ будет не меньше $2/3$. Следовательно, $BPP_w \subset BPP$.
В общем, идея в том, что вероятность ошибки можно уменьшить с помощью увеличения числа запуском машины.
(ii) Скажем, что язык $L \in BPP$, если

2

Задача сравнить 2 бинарных файла размера n. Представим файлы X и Y как битовые строки длины n. Выбираем простое число на отрезке от $[2; N]$. Вычисляем $u = X \ mod \ p, v = Y \ mod \ p$. Передаем v и u и сравниваем. Получается, алгоритм ошибается, если $X\overline{Y}$, но $|X - Y|$ делится на p. $\pi(n) \sim \frac{n}{\ln n}$. Количество простых делителей в разложении числа $|X - Y|$ не превосходит n. Возьмем за $N = n^2$. Тогда вероятность найти среди простых делителей числа $|X - Y|$ число p не больше $(\frac{n}{n^2/2\ln n}) = \frac{2\ln n}{n} \to 0$ при $n \to \infty$. При $n \leq 32$ $P \leq \frac{\ln 32}{16} < 3/4$.

5

(i) Пусть в графе G минимальный разоер состоит из k ребер. Тогда в графе по крайней мере $\frac{nk}{2}$ ребер, где n — число вершин. Тогда P(случайно выбранное ребро входит в минимальный разрез) $\leq \frac{2k}{nk} = \frac{2}{n}$.
(ii) Вероятность того, что полученный в результате алгоритма разрез будет минимальным равна вероятности того, что в ходе алгоритма мы не стянули ни одно ребро, входящее в минимальный разрез. Посчитаем вероятность того, что на $i-$ом шаге стянули ребро из разреза. Число вершин уменьшилось, тогда число ребер в полученном графе не превосходит $\frac{k(n-i+1)}{2}$. Вероятность того, что стянем ребро из разреза не больше $\frac{2}{n-i+1}$. Тогда вероятность того, что это будет резро не из разреза не меньше $1 - \frac{2}{n-i+1}$. Тогда вероятность того, что ни разу не стянули ребро из разреза не меньше $\prod\limits_{i=1}^{n-2}(1 - \frac{2}{n-i+1}) = \prod\limits_{i=1}^{n-2}(\frac{n-i-1}{n-i+1}) = \frac{n-2}{n} \cdot \frac{n-3}{n-1} \cdot ... \cdot \frac{n-n+3-1}{n-n+3+1} = \frac{2}{n(n-1)}$. Следовательно, вероятность того, что $MINCUT$ выдает минимальный разрев не меньше $\frac{2}{n(n-1)}$.
(iii) Запустим алгоритм $MINCUT$ n^2 раз. Тогда вероятность того, что алгоритм ни разу не выдаст минимальный разрев не превышает $(1 - \frac{2}{n(n-1)})^{n^2} < (1 - \frac{2}{n^2})^{n^2} \to \frac{1}{e^2}$ при $n \to \infty$, $\frac{1}{e^2} \approx 0.14$, следовательно, минимальный разрез найдется с вероятностью > 0.85.

6

1) $2-CNF$ — язык, состоящий из выполнимых КНФ, в каждом дизъюнкте которой не более двух литералов. Покажем, что язык разрешим за полимон. Для это преобразуем исходную КНФ в РОВНО-2-КНФ, преобразовав дизъюнкты вида x_i в $x_i \vee x_i$. Распишем каждый дизъюнкт по формуле: $x_i \vee x_j = \bar{x}_i \to x_j$. Представим данную КНФ в виде ориентированного графа. Для это для каждой переменной x_i создадим 2 вершины: x_i и $\bar{x}_i$. Будем проводить ребро $(\bar{x}_i, x_j)$, если в преобразованной КНФ есть подформула вида $(\bar{x}_i \to x_j)$. Получим ориентированный граф. Тогда КНФ будет выполнима тогда и только тогда, когда построенный граф не будет иметь ребра $(x_i, \bar{x}_j)$ и $(\bar{x}_i, x_j)$, так как данные ребра в данном представлении графа соответсвуют формуле $(x_i \vee x_j) \wedge (\bar{x}_i \vee \bar{x}_j)$, которая не выполнима. Следовательно, КНФ выполнима тогда и только тогда, когда граф имеет более одной компаненты сильной связности. А это проверяется за $O(|V| + |E|)$ ($|V| = 2n, n$ — число переменных в КНФ $\Rightarrow$ полиномиально от длины входа) с помощью модифицировнного алгоритма поиска в глубину. Таким образом, доказали, что $2 - SAT \in P$.
(ii) В класс RP. Если КНФ не выполнима, то никогда не найдется выполняющий набор. Следовательно, если $x \notin 2 - SAT$, то $P(m(x) = 1) = 0$, где m — вероятностная машина Тьюринга. А если $x \in 2 - SAT$, то $P(m(x) = 1) \geqslant 1/2^n$, А так константа $1/2$ в определении RP может быть заменена на любую другую из промежутка $(0, 1)$, поскольку требуемой вероятности можно добиться множественным запуском программы, то $2 - SAT \in RP$.

7

(i) Докажем по индукции, что все, что находится под $n-1$-ой картой равномерно перемешано на любом шаге цикла. База: на первом шаге (берем первую карту из колоды) под $n-1$ одна карта.
Индукционный переход: пусть на $k-$ом шаге (берем $k-$ую карту из колоды, то есть под $n-1$-ой картой не больше k карт) все под $n-1$-ой картой равномерно перемешано. Докажем, что на $k+1$ шаге все перемешено равномерно. Возможны 2 случая:
1)$n-1$-ая карта поднимается, то есть для k-ой карты выбираем с вероятностью $\frac{1}{k+1}$ одно из $k+1$ мест. Так как до этого перемешаны карты были равномерно и так как карта может занять любое место с одинаковой вероятностью, получаем снова равномерно перемешанные карты.
2)$n-1$-ая карта не поднимается: ничего не меняется карты остаются равномерно перемешанными.
(ii) Доказано в пункте 1). Идея в том, что перестановки k карт под $n-1$-ой все равно вероятны, так как мы выбираем место, куда кладем следующую карту независимо.
(iii) Найдем математическое ожидание числа шагов. Пусть ξ — число шагов, которые нужно совершить, чтобы $n-1$-ая карта окажется наверху колоды и будет рандомно поставлена в любое место колоды. Определим величину ξ_i как число шагов при условии, что под $n-1$-ой картой находится ровно i карт. Тогда $E\xi = \sum E\xi_i$ в силу линейности математического ожидания.
$E\xi_i = \sum\limits_{k=1}^{\infty} k \cdot (1-p)^{k-1} \cdot p$, p — вероятность того, что карта поднимется (то есть мы положим под

нее карту, взятую с верху колоды), k — номер "попытки с которой карта поднимется. То есть мы выбираем этот номер попытки k, причем предыдущие $k-1$ раз $n-1$-ая карта оставалась на месте, поэтому домножаем на вероятность того, что карта не поднимется в степени $k-1$, $p = \frac{i+1}{n}$.

$E\xi = \sum\limits_{i=1}^{n-2} \sum\limits_{k=1}^{\infty} k \cdot (1-p)^{k-1} \cdot p + 1,$

$\frac{1}{1-x} = \sum\limits_{k=0}^{\infty} x^k, \frac{1}{(1-x)^2} = \sum\limits_{k=0}^{\infty} kx^{k-1},$

$1 - x = p, \frac{1}{p^2} = \sum\limits_{k=1}^{\infty} k(1-p)^{k-1} \Rightarrow E\xi_i = \frac{n}{i+1},$

$E\xi = 1 + \sum\limits_{i=1}^{n-2} \frac{n}{i+1} = 1 + \sum\limits_{i=1}^{n-2} \frac{n}{i+1} = 1 + n \sum\limits_{i=1}^{n-2} \frac{1}{i+1} = 1 + n \cdot (\frac{1}{2} + ... + \frac{1}{n-1}) = n \cdot H(n) - n.$