Домашнее задание по АМВ

771 группа, Христолюбов Максим

29 марта 2019 г.

*При решение некоторых номеров обращался к Михаилу Сысаку.

1 Задача 1

Для каждого языка из $\mathcal{RP}$ существует вероятностная МТ, принимающая слова этого языка. Пусть ДМТ будет работать так же к и ВМТ, а вместо использования случайных битов будет брать биты из предоставленного ей сертификата. Так как вероятность принятия ВМТ слова из языка не нулевая, то существует такой сертификат, что ДМТ примет его, а для слова не из языка не существует такого сертификата, посколько вероятность его принятия равна 0. Причем длина сертификата полиномиальна, так как он состоит из всех используемых ВМТ битов, а из полиномиальной работы ВМТ следует полиномиальность используемых битов. Значит, существует ДМТ, распознающая этот язык с сертификатом, и этот язык $\mathcal{NP}$.

2 Задача 2

$2^n \geq |x-y| \geq p_1 p_2 \dots p_k \geq n^k$, значит, $k \leq \frac{n}{\ln n} \ln 2$.
Так как $0{,}99\frac{n}{\ln n} \leq \pi(n) \geq 1{,}01\frac{n}{\ln n} \ln n$, то $\pi(n{,}2n) \geq 1{,}98\frac{n}{\ln 2n} - 1{,}01\frac{n}{\ln n}$
$P\{\text{выбрать простое число} - \text{делитель}\} = \frac{k}{\pi(n{,}2n)} \leq \frac{n \ln 2}{1{,}98\frac{n \ln n}{lnn + \ln 2} - 1{,}01\frac{n \ln n}{\ln n}} = \frac{\ln 2}{1{,}98\frac{\ln n}{\ln n + \ln 2} - 1{,}01} \leq \frac{3}{4}$
$n \geq e^{30}$, что около 1 теробайта.

3 Задача 3

3.1 (i)

Заменим вероятность ошибки $\frac{1}{3}$ на число $\frac{1-\alpha}{2}$. Тогда можно применить этот алгоритм n нечетное кол-во раз и смотреть какой ответ будет дан чаще и его выдавать. Вероятность ошибки результата будет

$P = \sum\limits_{i=0}^{\frac{n-1}{2}} C_n^i (\frac{1-\alpha}{2})^{n-i} (\frac{1+\alpha}{2})^i \leq \sum\limits_{i=0}^{\frac{n-1}{2}} C_n^i (\frac{1-\alpha}{2})^{\frac{n+1}{2}} (\frac{1+\alpha}{2})^{\frac{n-1}{2}} \leq (\frac{1-\alpha}{2})^{\frac{n+1}{2}} (\frac{1+\alpha}{2})^{\frac{n-1}{2}} \sum\limits_{i=0}^{\frac{n-1}{2}} C_n^i \leq (1-\alpha^2)^{\frac{n-1}{2}} (1-\alpha) \frac{1}{2^n} 2^n = (1-\alpha^2)^{\frac{n-1}{2}} (1-\alpha) \to 0$ при $n \to \infty$

Значит, существует такое n, что вероятность ошибки меньше $\frac{1}{3}$. И каждый язык, удовлетворяющий определению с $\frac{1-\alpha}{2}$ удовлетворяет определению с $\frac{1}{3}$.

3.2 (ii)

Изменим алгоритм — в случае превышения полиномиального времени работы будем случайно выдавать 0 или 1 с вероятностью $\frac{1}{2}$. p - вероятность, что будет превышено полиномиальное время работы, $\epsilon \leq \frac{1}{2}$ - вероятность ошибки изначального алгоритма. Тогда ошибка измененного алгоритма

$\epsilon' = \frac{1}{2}p + \epsilon(1-p) \leq \frac{1}{2}p + \frac{1}{2}(1-p) = \frac{1}{2}$.

Значит измененный алгоритм будет удовлетворять определению, так как работает полиномиальное время.

4 Задача 4

4.1 (i)

Вероятность совпадения компоненты в равенстве $A(Bx) = Cx$ $\frac{1}{N}$, а вероятность совпадения векторов $\frac{1}{N^n} < p$, $N > \frac{1}{p^{\frac{1}{n}}}$.

4.2 (iv)

$(ABx)^T x = (Cx)^T x$ и $(ABx)^T y = (Cx)^T y$ — равенства двух многочленов степени 2. По лемме Шварца-Зиппеля

$P\{\text{ошибка}\} \leq \frac{2}{N} < p$, $N > \frac{2}{p}$

5 Задача 5

5.1 (i)

Пусть кол-во ребер минимального разреза e, тогда из каждой вершин выходит не более e ребер, иначе существовал бы разрез минимальнее.

$P\{$выбрать ребро из разреза$\} = \frac{e}{E} = \frac{e}{\frac{1}{2}eV} = \frac{2}{V}$

5.2 (ii)

Алгоритм выдаст верный ответ, если по ходу работы не будет стянуто ни одно из ребер, его пересекающих. На первом шаге вероятность выбрать ребро не из разреза $\frac{n-2}{n}$, на втором $\frac{n-3}{n-1}$ и так далее, вероятность выдать верный ответ $\frac{n-2}{n}\frac{n-1}{n-3}\dots frac13 = \frac{2}{(n-1)n}$

5.3 (ii)

Если повторять алгоритм n^2 раз

$P\{$ошибки$\} \leq \left(1 - \frac{2}{n(n-1)}\right)^{n^2} \leq \left(1 - \frac{2}{n^2}\right)^{n^2} \to e^{-2} < 0{,}15$

Значит, начиная с достаточно большого n_0 вероятность правильного ответа будет превышать 0,85.

6 Задача 6

Заменив каждую дезъюнкцию $(a \vee b)$ на $(\overline{a} \to b) \wedge (\overline{b} \to a)$. Теперь построим граф на всех литералах, такой что ребро (u,v) принадлежит графу, если в конъюнкцию входит $(u \to b)$. Покажем, что формула выполнима тогда и только тогда, когда для любой переменной x нельзя достичь x из $\overline{x}$ и $\overline{x}$ из x.

Пусть формула выполнима. Предположим, для x можно достичь его из отрицания и наоборот. Если $x = 0$ в выполняющем наборе, тогда в одной из импликаций, которая ведет от отрицания к переменной импликация не выполнена, что противоречит выполнимости. Аналогично, если $x = 1$.

Обратно, все x, из которого можно достичь $\overline{x}$ обозначим его $x = 0$. Из единичной вершины не может быть достижима нулевая вершина, так как тогда бы формула была б невыполнимой. Всем вершинам, достижимых из единичных, присвоим 1. Это присваивание непротиворечиво, так как если бы x и $\overline{x}$ были бы достижимы из $y = 1$ это значило бы что они достижимы друг из друга, что не возможно. Остальным вершинам значения можно присвоить произвольно и получить выполняющий набор, значит, формула выполнима.

Преобразование импликаций, построение графа, поиск компонент сильной связности (для проверки достижимости каждой переменной ее отрицания и наоборот) потребует полиномиального времени, значит, $2-SAT \in \mathcal{P}$.

7 Задача 7

7.1 (i)

Доказательство по индукции. На 1 шаге колода равновероятно перемешана. Если на k шаге все карты под $n-1$ были равномерно перемешаны, тогда на $(K+1)$ шаге мы засовываем верхнюю карту в случайное место. Если засунули карту выше $n-1$ карты, то под ней ничего не изменилось. Если ниже $n-1$ карты, под которой $p-1$ карта, то фактически карта была вставленно в случайное из p мест. То есть новая перестановка была составлена сначала выбором одного из p мест, а потом заполнением оставшихся мест одной из случайных перестановок, чья вероятность $\frac{1}{(p-1)!}$, тогда вероятность новой перестановки из p карт $\frac{1}{(p-1)!}\frac{1}{p} = \frac{1}{p!}$, то есть они равновероятны.

7.2 (ii)

Вставка в равновероятно перемешанную колоду эквивалента вставке в одно из случайных мест между картами, что как было показано ранее порождает равновероятную перестановку.

7.3 (iii)

Матожидание времени работы алгоритма найдем как сумму матожиданий времени работы на $n-1$ шагах работы алгоритма, где матожидание k-ого шага — это сколько нужно раз в среднем попытаться засунуть верхнюю карту колоды, в которой под $n-1$ картой k карт, чтобы она вставилась под $n-1$ карту, и под ней оказалось $k+1$ карт. Вероятность засунуть карту под $n-1$ на k-ом шаге $\frac{k+1}{n}$, значит, матожидание времени работы k-ого шага равно $\frac{n}{k+1}$. Матожидание алгоритма:

$$E = \sum_{k=1}^{n-1} \frac{n}{k+1}$$

8 Д-1 из файла

8.1 (i)

$T(n) = 4T(\frac{n}{2})+4F(n,\frac{n}{2})+\Theta(n^2)$, где $F(n,k)$ — время стягивание графа на n вершинах и порогом k.

8.2 (ii)

$F(n,k) = \Theta(n(n-k)) = \Theta(n^2)$, так как нужно избавиться от $n-k$ вершин, которые в худшем случае соеденены со всеми остальными вершинами.

$T(n) = 4T(\frac{n}{2}) + \Theta(n^2)$

По мастер теореме $T(n) = \Theta(n^2 \log n)$.

8.3 (ii)

$\frac{dp}{dk} = p_{k+1} - p_k = -\frac{3}{8}p_k^2$, $p_0 = 1$ — задача Коши, $p_k = \frac{8}{3k+8}$.