Задание на шестую неделю.

№1

Построим по вероятностной машине Тьюринга M, принимающей язык $L \in RP$, недетерминированную МТ M_1, из каждой вершины которой выходят все соответствующие возможные пути (без вероятности их выбора), тогда при ее прохождение вероятность угадать правильный путь равна соответствующей вероятности. Тогда если, $x \in \bar{L}$ (т. е. $M(x) = 0$), то в M_1 не существует путя ведущего к финальному состоянию, и значит $M_1(x) = 0 = M(x)$. Если $x \in \bar{L}$ (т. е. $P(M(x) = 1) \geq 0.5$, то из построения хотя бы половина возможных путей ведет к финальному состоянию, значит один такой путь точно найдется, $\Rightarrow M_1(x) = 1$. $\Rightarrow M_1$ является МТ для того же языка L. $\Rightarrow L \in NP$, т. к. принимается недетерминированной МТ. $\Rightarrow RP \subseteq NP$.

№2

Обозначим кол-во простых чисел меньших n за $\Phi(n)$. С семинара:

$$k \leq \frac{n}{\ln n} \ln 2$$

$$0.99\frac{n}{\ln n} \leq \Phi(n) \leq 1,01\frac{n}{\ln n}$$

Тогда на интеравале $[n, 2n]$:

$$\Phi([n, 2n]) \geq 1,98\frac{\ln n}{\ln n + \ln 2} - 1,01\frac{n}{\ln n}$$

Значит, вероятность выбрать одно из чисел $p_1, \ldots, p_k$ из $P \cap [n; 2n]$:

$$P_{osh} = \frac{k}{\Phi(n, 2n)} \leq \frac{\ln 2}{1,98\frac{\ln n}{\ln n + \ln 2} - 1,01} \longrightarrow \frac{\ln 2}{0,97} < \frac{3}{4}$$

Значит при достаточно больших n ошибка не превосходит n. Оценим необходимое n для выполнения условия:

$$\ln n \geq \frac{\ln 2}{\frac{1,98}{\frac{4}{3}\ln 2 + 1,01} - 1} < 30$$

$\Rightarrow$ Условие выполняется при $n \geq e^{30} \approx 2^{43} \approx 1$Тбайт.

№5

а) Пусть в графе есть минимальный разрез из k ребер. Тогда вероятность того, что случайно выбранное ребро окажется одним из этих ребер: $P = \frac{k}{|E|}$. Если в графе есть вершина со степенью $< k$, то тогда взяв ее за первое множество, а оставшиеся вершины за второе, получим разрез графа из $< k$ ребер. Противоречие, т. к. минимальный разрез из k ребер. Значит, все вершины имеют степень $\geq k$. $\Rightarrow |E| \geq \frac{k|V|}{2}$.

$$\Rightarrow P = \frac{k}{|E|} \leq \frac{k}{\frac{k|V|}{2}} = \frac{2}{|V|}$$

б) Из первого пункта вероятность того, что на первом шаге не будет убрано ребро из минимального разреза: $P(S_1) = 1 - \frac{2}{n}$. Аналогично, на втором шаге: $P(S_2|S_1) = 1 - \frac{2}{n-1}$. На k-ом $P(S_k|S_1 \cap S_2 \dots S_{k-1}) = 1 - \frac{2}{n-k+1}$.. Всего шагов будет $n-2$. Тогда, вероятность того, что на всех шагах не было вытащено ребро из минимального разреза:

$$P = P(S_1 \cap S_2 \cdots \cap S_{n-2}) \geq P(S_1)P(S_2|S_1) \dots P(S_{n-2}|S_1 \cap S_2 \dots S_{n-3}) \geq$$

$$\geq (1 - \frac{2}{n}) \dots (1 - \frac{2}{n-(n-2)+1}) = 2\frac{(n-2)!}{n!} = \frac{2}{n(n-1)}.$$

в) Из предыдущего пункта, вероятность «неуспеха» $P(ns) =\leq (1 - \frac{2}{n(n-1)}) \leq (1 - \frac{2}{n^2})$. Вероятность того, что «неуспех» повторится n^2 раз:

$$P(ns^{n^2}) = P(ns)^{n^2} \leq (1 - \frac{2}{n^2})^{n^2} \leq \exp^{-2} \leq 0.14.$$

$\Rightarrow$ Вероятность нахождения минимального разреза: $P = 1 - P(ns^{n^2}) \geq 0.85$.

№8(2)

(iv) Из 5в) чтобы найти минимальный разрез с вероятностью ϵ необходимо совершить $k = \frac{1}{2} \log \frac{1}{1-\epsilon} n^2$ итераций:

$$P(ns^k) = P(ns)^k \leq (1 - \frac{2}{n^2})^k \leq \exp^{-2 \cdot \frac{1}{2} \log \frac{1}{1-\epsilon}} \leq 1 - \epsilon.$$

№6

Покажем, что $2SAT \in P$.
Пусть дано x. Построим, соответствующий ему ориентированный граф $G(x)$. Вершины это все переменные из формулы и противоположные им литералы. Для каждого дизъюнкта вида $(a \vee b) = (\bar{a} \to b \wedge \bar{b} \to a)$ проведем ребра $(\bar{a}, b), (\bar{b}, a)$. Если в полученном графе для какой-то переменной x есть путь из $\bar{x}$ в x и из x в $\bar{x}$, то значит из исходной формулы следует $\bar{x} \to x_{k_1} \to \ldots x$, и $x \to x_{m_1} \to \ldots \bar{x}$. Но эти два выражения не могут быть верны одновременно не при каких x. $\Rightarrow$ искомая формула невыполнима.
Если в графе нет ни одного такого цикла, содержащего x и $\bar{x}$, тогда возьмем произвольную переменную x и $\bar{x}$, если есть ребро $(x, \bar{x})$, то присвоим $x = 0$, иначе $x = 1$. Пусть для определенности $x = 1$, тогда ту же операцию повторяем для всех вершин, соединенных с ней, пока все вершины не закончатся. Т. к. пути $x_k \bar{x_k} x_k$ нет, то в процессе не может возникнуть противоречий. Таким образом, получим набор переменных $\vec{x}$, который из построения является выполнимым. $\Rightarrow$ За полиномиальное время можно свести задачу к задаче проверки наличия цикла с x_k и $\bar{x_k}$ в графе G.
Проверить для каждой из n вершины, есть ли путь из x_n в $\bar{x_n}$, и наоборот, можно за $O(n^2)$, запустив обход в глубину из вершины x_n и проверив зайдет ли он в вершину $\bar{x_n}$. Таким образом, вся задача решается за полиномиальное время.
Алгоритм случайных блужданий для решения $2SAT$, разобранный на семинаре, доказывает, что $2SAT \in RP$.

№3

а) Обозначим за BPP_ε и BPP_ϵ классы с константой $\varepsilon < \epsilon < 1/2$. Очевидно, что $BPP_\varepsilon \subseteq BPP_\epsilon$. Покажем, что $BPP_\epsilon \subseteq BPP_\varepsilon$: Возьмем k независимых вероятностных МТ для BPP_ϵ, и будем определять результат по большинству полученных результатов. Тогда с увеличение k вероятность ошибки падает (при этом время увеличивается полиномиально) и при достаточно больших k станет не превосходить ε. Значит, если задача принадлежит BPP_ϵ, то она принадлежит и BPP_ε. $\Rightarrow BPP_\varepsilon \subseteq BPP_\epsilon$.

$$\Rightarrow BPP_\epsilon = BPP_\varepsilon = BPP.$$

б) Пусть дан алгоритм, работающей за полином (за $poly(n)$)в среднем с вероятностью ошибки $1/3$. Преобразуем его в новый алгоритм следующим образом: как только время работы алгоритма превысило $poly(n)$ (а это случается с вероятностью $p < 1$) алгоритм определяет результат подбрасыванием монетки (т. е. выдает 1 или 0 с равной вероятностью). Тогда вероятность ошибки нового алгоритма:

$$p_{osh} = 1/3 \cdot (1-p) + p \cdot 1/2 < 1/2 \cdot (1-p) + p \cdot 1/2 = 1/2.$$

Таким образом, новый алгоритм работает за полиномиальное время с вероятностью ошибки $< 1/2$. Из пункта а) этот алгоритм попрежнему решает задачу класса BPP.

№4

(i) Пусть $b = (b_1, \ldots, b_n)$ и $a = (a_1, \ldots, a_n)$ два целочисленных вектора и $a \equiv b$, а $x = (x_1, \ldots, x_n)^T$, вектор описанный в условие. Оценим вероятность $P(a \cdot x = b \cdot x)$:
Т. к. $a \equiv b$, то $\exists i : a_i \equiv b_i$. Тогда заметим, что

$$a \cdot x = b \cdot x \Leftrightarrow (a_i - b_i)x_i = \sum_{j \equiv i} (b_j - a_j)x_j \Leftrightarrow x_i = \frac{\sum_{j \equiv i}(b_j - a_j)}{a_i - b_i}$$

$\Rightarrow x_i$ однозначно определяется оставшимися компонентами вектора x и векторами a и b. Но т. к. x_i генерируется рандомно, то вероятность того, что он окажется равным определенному значению: $P \leq 1/N$.
При умножении матриц $S = AB$ и C на $x = (x_1, \ldots, x_n)^T$, если $S \equiv C$ и $Sx = Cx$, то $\exists i : S_i \equiv C_i$, где C_i, S_i строки соответствующих матриц. Тогда,

$$\Rightarrow S_i \cdot x = (Sx)_i = (Cx)_i = C_i \cdot x.$$

А вероятность этого из вышесказанного $P \leq 1/N$.
$\Rightarrow$ Вероятность того, что $ABx = Cx$, но $AB \equiv C$: $P \leq \frac{1}{N}$. Таким образом, необходимо взять $N \geq \frac{1}{p}$.
(iv) $(A(Bx)x) = (Cx)x \Leftrightarrow (ABx)^T x = (Cx)^T$. А это равенство двух скалярных полиномов от $x^1, \ldots x_n$ стпени два. $\Rightarrow$ По лемме Шварца-Зиппеля вероятность ошибки: $P \leq 2/N$. $\Rightarrow N > 2/p$.

Во втором случае, исходное равенство равносильно $(ABx)^T = (Cx)^T y$ и вероятность его ошибки так же получается: $P \leq 2/N$.

№7

(i), (ii) Сначала покажем (ii). Пусть колода равномерно перемешена, т. е. все перестановки равновероятны. После того как в нее вставили рандомно новую карту, все перестановки попрежнему должны быть равновероятны, иначе отсюда будет следовать, что вставление карты было зависимо от расстановки карт в колоде. Пользуясь (ii), докажем по индукции (i). Изначально под $(n-1)$ одна карта и все перестановки очевидно равновероятны. Если на kом шаге под $(n-1)$ой картой равномерно перемешенная колода, то из (ii) после вставки новой карты она остается равновероятной.
(iii) Пусть $(n-1)$ая карта в данный момент на kом снизу месте. Под нее вставят карту через одну итерацию с вероятностью $\frac{k}{n}$, через две с $\frac{k(n-k)}{n^2}$, и т. д. $\Rightarrow$ Матожидание кол-ва итераций после которых под нее вставят одну карту:

$$E_k = \sum_{i=1}^{\infty} \frac{k(n-k)^{i-1}}{n^i} \cdot i = \frac{k}{n-k} \sum_{i=1}^{\infty} i \cdot (\frac{n-k}{n})^i = \frac{k}{n-k} \cdot \frac{\frac{n-k}{n}}{(1-\frac{n-k}{n})^2} = \frac{n}{k}.$$

Алгоритм завершит работу, когда $n-1$ карта пройдет все места снизу доверху и будет вставлена, значит матожидание кол-ва итераций цикла:

$$E = \sum_{k=2}^{n} E_k = n/2 + n/3 + \ldots n/n = n(\ln n + C) = \Theta(n \ln n)$$

Предпоследний переход получен по формуле Эйлера для частичной суммы гармонического ряда.

№8(1)

Докажем теорему Татта: *В графе* G *есть совершенное паросочетание* $\Leftrightarrow$ *детерминант матрица Татта* $D(G) \equiv 0$.

$$D = \sum_{k=1}^{n!} (-1)^{y(k)} a_{1y_1(k)} \dots a_{ny_n(k)},$$

где $y_1(k), \dots y_n(k)$ это k-ая перестановка n множества вершин $\{1, , n\}$. Поставим в соответствие каждому ненулевому произведению $P_k = (-1)^{y(k)} a_{1y_1(k)} \dots a_{ny_n(k)}$ граф G_k, с n вершинами и ребрами между $(1, y_1(k))$, $(2, y_2(k))$, и т. д. Получим граф, покрывающий все вершины исходного и в котором из каждой вершины выходит ровно одно ребро и входит одно. Этот граф разбивается на циклы. Если в каком-нибудь G_k все циклы четной длины, то тогда легко разбить каждый цикл на совершенные паросочетания, а значит и весь граф G_k. Т. к. все ребра из графа G_k есть и в G, то это разбиение так же разбивает и исходный граф G на совершенные паросочетания.

Если в каждом из G_k есть цикл нечетной длины, то рассмотрим произвольный G_m, соответствующей P_m. Поменяем направление ребер во всех его нечетных циклах (суммарное число вершин в этих циклах $2t + 1$). Заметим, что полученный граф G_n так же принадлежит мн-ву графов вида G_k, при этом соответствующая G_n получается из G_m четным кол-вом перестановок: 2t , т. е. $(-1)^{y(m)} = (-1)^{y(n)}$. А т. к. в них различаются только напраления у начетного кол-во ребер, то нечетное кол-во множителей $a_{iy_i(n)} = -a_{iy_i(n)}$. $\Rightarrow P_m = -P_n$. Таким образом, все графы вида G_k, можно разбить на такие пары (они, очевидно не пересекаются). Т. к. в сумме произведения, соответсвующие оной паре, дают нуль, то и детерминант матрице будет равен нулю. $\Rightarrow D(G) \equiv 0 \Rightarrow$ в графе G есть совершенное паросочетание. Покажем в другую сторону:

Пусть в графе G есть совершенное паросочетание. Посчитаем $D = \sum_{k=1}^{n!} P_k$. Как было показано выше, слагаемые, соответствующие графам, где есть нечетные циклы, сокращаются друг с другом. Таким образом, в сумме остаются только слагаемые, соответствующие графам с четными циклами, которые можно разбить на совершенные паросочетания. Сумма таких P_k из построения не может равняться нулю. $\Rightarrow D(G) \equiv 0$.

№8(2)

(i) Обозначим асимптотику функции СТЯГИВАНИЕ(G, k), где n число вершин в G, за $S(n, k)$. Тогда рекуррентная сложность для МИНИРАЗРЕЗ состоит из четырех реккурсивных вызовов, функции СТЯИВАНИЯ и операция нахождения минимума (асимпттика которой равна кол-ву ребер, т. е. $\theta(n^2)$:

$$R(n) = 4R(n/2) + 4F(n, n/2) + \theta(n^2).$$

(ii) Алгоритм СТЯГИВАНИЕ выполняет операцию сложностью $\Theta(n)$ $n - k$ раз. Значит сложность данной функции $\Theta(n(n-k))$. Тогда из предыдущего пункта:

$$R(n) = 4R(n/2) + \theta(n^2).$$

Из Мастер теоремы: $R(n) = \theta(n^2 \log n)$.