Домашнее задание 1

1. (1) Даны три квадратных матрицы A, B, C размера $n \times n$ над полем $\mathbb{F}_2$. Придумайте вероятностный алгоритм сложности $O(n^2)$, который будет проверять, верно ли, что $AB = C$. Алгоритм должен давать правильный ответ с вероятностью хотя бы $\frac{9}{10}$.

2. (2) Случайные величины $X_1, X_2, \ldots, X_n$ независимы

- Покажите, что для любых $A_1, A_2, \ldots, A_n \subseteq \mathbb{R}$ события $[X_i \in A_i]$ являются независимыми (т.е. вероятность пересечения этих событий равняется произведению вероятностей).
- Покажите, что для любых функций $f_1, f_2, \ldots f_n : \mathbb{R} \to \mathbb{R}$ случайные величины $f_i(X_i)$ являются независимыми.
- Пусть $I \subseteq [n]$, докажите, что случайные величины $\{X_i\}_{i \in I}$ являются независимыми.
- Пусть $I \subseteq [n]$, докажите, что для любых функций $f : \mathbb{R}^I \to \mathbb{R}, g : \mathbb{R}^{[n] \setminus J} \to \mathbb{R}$ случайные величины $f((X_i)_{i \in I})$ и $g((X_i)_{i \in [n] \setminus I})$ независимы.

3. (1) Каждый из k человек в лифте, который стоит на первом этаже выбирает случайный этаж равновероятно из оставшихся n этажей. Чему равняется математическое ожидание числа остановок, которые сделает лифт?

4. (1) Покажите, что существует такая формула ϕ в 3-КНФ, в каждом дизъюнкте которой входят ровно три различных переменных, для которой не существует набора, который выполнит больше, чем $\frac{7}{8}m$ дизъюнктов, где m — это число дизъюнктов в ϕ.

5. (3) Покажите, что для формулы в КНФ, состоящей из m дизъюнктов, в которой любые три дизъюнкта можно одновременно выполнить, существует набор значений переменных, который выполняет как минимум $\frac{2}{3}m$ дизъюнктов.

6. а) (3) Покажите, что размер любого 2-независимого подмножества $\{0,1\}^n$ имеет размер хотя бы $n+1$. б) (3) Покажите, что если $n-1 = 2^k$, то существует 2-независимое поднмножетсво $\{0,1\}^n$ размера $n+1$.

7. (3) Распределение D на $\{0,1\}^n$ называется t-независимым, если для любой случайной величины X распределенной согласно D, для любых различных $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, n\}$, случайная величина $X_{i_1 i_2 \ldots i_t}$ имеет распределение U_t. Пусть A — вероятностный алгоритм, который получает оракульный доступ к входу длины n, алгоритм A может во время своей работы адаптивно запросить t битов входа. Докажите, что если D является t-независимым, то $\Pr_{x \leftarrow D}[A(x) = 1] = \Pr_{x \leftarrow U_n}[A(x) = 1]$. Иными словами даже адаптивный алгоритм, который изучает t битов входа не может отличить распределение D от равномерного.

8. (2) (Лемма о перемешивании для хеш-функций) Пусть $m < n$ и $H_{n,m}$ — семейство попарно независимых хеш-функций $\{0,1\}^m \to \{0,1\}^n$. Тогда для лбого $\epsilon > 0$ и любых $S \subseteq \{0,1\}^n, T \subseteq \{0,1\}^m$ выполняется

$$\Pr_{h \leftarrow H_{n,m}}[||\{x \in S : h(x) \in T\}| - |T||S|/2^m| > \epsilon|T||S|/2^m] \leq \frac{2^m}{|T||S|\epsilon^2}.$$

9. Коды Уолша-Адамара.

а) (1) Каждому $a \in \{0,1\}^n$ соответствует линейная функция $f_a : \{0,1\}^n \to \{0,1\}$, определяемая так: $f_a(x_1 x_2 \ldots x_n) = \sum_{i=1}^n a_i x_i \bmod 2$. Кодом Уолша-Адамара строки $a \in \{0,1\}^n$

называется таблица значений функции f_a и обозначается $WH(a)$, нетрудно понять, что длина строки $WH(a)$ равняется 2^n. Проверьте, что для двух различных строк $a, b \in \{0,1\}^n$ их коды $WH(a)$ и $WH(b)$ отличаются ровно в половине позиций.

б) (2) Предположим, что у нас есть оракульный доступ к строке Z, которая отличается от $WH(a)$ не более, чем в доле $\frac{1}{4} - \epsilon$ позиций, где ϵ — это некоторая константа, причем строка $a \in \{0,1\}^n$ нам неизвестна. Придумайте вероятностный алгоритм, который для данного $x \in \{0,1\}^n$ вычислит $f_a(x)$ с вероятностью как минимимум $\frac{9}{10}$, причем этот алгоритм может должен делать лишь константное число запросов к строке Z и работать полиномиальное от n время.

в) (1) Пусть $r_1, r_2, \ldots r_\ell$ — взаимно независимые случайные величины, каждая из которых равномерно распределена на $\{0,1\}^n$. Для $I \subseteq \{1,2,\ldots,\ell\}$ определим $r^{(I)} = \sum_{i \in I} r_i$. Покажите, что множество случайных величин $r^{(I)}$ при $I \neq \emptyset$ является попарно независимым.

г) (5) Предположим, что у нас есть оракульный доступ к строке Z, которая отличается от $WH(a)$ не более, чем в доле $\frac{1}{2} - \epsilon$ позиций, где ϵ — это некоторая константа, причем строка $a \in \{0,1\}^n$ нам неизвестна. Придумайте вероятностный алгоритм, который за полиномиальное от $\frac{n}{\epsilon}$ время напечатает список слов из $\{0,1\}^n$ полиномиального от $\frac{n}{\epsilon}$ размера, так, что в нем с вероятностью как минимум $\frac{9}{10}$ встретится слово a.

Правила сдачи

Баллы в скобочках примерно соответствуют сложности задачи. Можно сдавать любое количество решенных задач, выбирая себе подходящие по сложности. Крайний срок сдачи: воскресенье 15-ое марта. Решения в рукописном виде сдаются во время лекции, в электронном виде решения можно посылать по адресу dmitrits at pdmi.ras.ru.