Листок 7. Экстракторы.

В задачах 15-20 $C(f)$ обозначает минимальную глубину коммуникационного протокола, а $C_L(f)$ минимальное число листьев в дереве протокола.

$\boxed{\textbf{COMP2 30.}}$ Докажите, что если существует такая функция $f \in \mathbf{E}$, что $H_{avg}(f)(n) \geq 2^{\epsilon n}$ при всех n, то $\mathbf{MA} = \mathbf{NP}$.

$\boxed{\textbf{COMP2 31.}}$ Пусть $G : \{0,1\}^* \to \{0,1\}^*$ — это кандидат в $S(l)$-псевдослучайные генераторы, которому не удается дерандомизовать какой-то конкретный **BPP** алгоритм A в среднем. Иными словами, если $L \in \mathbf{BPP}$ — это токой язык, что $\Pr[A(x) = L(x)] \geq \frac{2}{3}$, верно для всех достаточно большиз n, то с вероятностью как минимум $\frac{1}{n}$ по выбору $x \leftarrow \{0,1\}^n$, $\Pr[A(x, G(U_{l(n)})) = L(x)] \leq \frac{1}{2}$ (выберем $l(n)$ таким, что $S(l(n)) \geq m(n)$, где $m(n)$ обозначает denotes число случайных бит которое использует A на входах длины n).

Докажите, что существует вероятностный полиномиальный алгоритм D такой, что на входе 1^n он выводит схему D_n такую, что с вероятностью как минимум $\frac{1}{2n}$ (по случайным битам D) $|\mathbb{E}[D_n(G(U_{l(n)}))] - \mathbb{E}[D_n(U_{m(n)})]| \geq 0.1$.

$\boxed{\textbf{COMP2 28.}}$ Пусть $E_1 : \{0,1\}^n \to \Sigma^m$ и $E_2 : \Sigma \to \{0,1\}^k$ — это два кода с локальными списочными декодерами. Декодер кода E_1 выдает список размера l_1 и обрабатывает $1 - \epsilon_1$ ошибок. Декодер для кода E_2 выдает список размера l_2 и обрабатывает $\frac{1}{2} - \epsilon_2$ ошибок. Докажите, что у каскадного кода $E_1 \cdot E_2$ существует локальный списочный декодер, который обрабатывает $\frac{1}{2} - \epsilon_1\epsilon_2 l_2$ ошибок и выдает список размера $l_1 l_2$.

$\boxed{\textbf{COMP2 29.}}$

(а) Покажите, что существует полиномиальный от n алгоритм A, который получает вход, распределенный согласно распределению X с $H_\infty(X) \geq n^{100}$ и имеет оракульный доступ к функции $f : \{0,1\}^n \to \{0,1\}$, который удовлетворяет следующим свойствам:

- если $\mathbb{E}[f(U_n)] \geq \frac{2}{3}$, то $\Pr[A^f(1^n, X_n) = 1] \geq 0.99$
- если $\mathbb{E}[f(U_n)] \leq \frac{1}{3}$, то $\Pr[A^f(1^n, X_n) = 0] \geq 0.99$.

Такой алгоритм будем называть аппроксиматором функции.

(б) Покажите, что не существует аппроксиматора без доступа к случайным битам.

(в) Покажите, что если распределение X находится на расстоянии более $\frac{1}{5}$ от каждого распределения Y с $H(Y) \geq \frac{n}{2}$, то не существует аппроксиматора, вход которого распределен согласно X.

$\boxed{\textbf{COMP2 1.}}$ Рассмотрим функцию $\mathrm{Maj} : \{0,1\}^n \to \{0,1\}$, которая выдает 1, если не менее половины входных битов равны 1. Докажите, что существует:

(в) монотонная формула полиномиального размера, вычисляющая функцию Maj.

$\boxed{\textbf{COMP2 12.}}$ Рассмотрим функцию $f = \bigvee_{i=1}^{n} x_i$. Докажите, что $R(f) = n$.

$\boxed{\textbf{COMP2 18.}}$ Игры Карчмера-Вигдерсона. Дана функция $f : \{0,1\}^n \to \{0,1\}$. Алиса получает $x \in f^{-1}(0)$, а Боб получает $y \in f^{-1}(1)$. Им требуется вычислить какую-нибудь координату i, что $x_i \neq y_i$. Данное отношение мы будем обозначать KW_f.

(а) Докажите, что $C(\mathrm{KW}_f) \leq d(f)$ и $C_L(\mathrm{KW}_f) \leq L(f)$, где $d(f)$ — минимальная глубина формулы, которая вычисляет f в базисе $\{\wedge, \vee, \neg\}$, а $L(f)$ — соответственно число листьев.

$\boxed{\textbf{COMP2 19.}}$ Будем называть алгоритм $S_{\epsilon,\delta}$ усредняющим булевым сэмплером, если он используя r случайных битов, генерирует q запросов длины n к функции $f : \{0,1\}^n \to \{0,1\}$ и возвращает среднее арифметическое полученных значений так, чтобы результат отличался от $\overline{f}$ больше, чем на ϵ с вероятностью меньше, чем δ.

На основе сэмплера $S_{\epsilon,\delta}$ определим функцию $\mathrm{Ext} : \{0,1\}^r \times \{0,1\}^{\log(q)} \to \{0,1\}^n$ так, что $\mathrm{Ext}(x,i)$ равняется i-му запросу сэмплера, если он использует строку x вместо случайных битов.

(а) Докажите, что Ext является $(r - \log(\frac{\epsilon}{\delta}), 2\epsilon)$ экстрактором.

(б) Какой получится экстрактор, если воспользоваться сэмплером Рамануджана, у которого $r = n$ и $q = O(\frac{1}{\epsilon^2\delta})$?

$\boxed{\textbf{COMP2 20.}}$ Пусть $M[X,X]$ — 0/1-матрица, которая содержит перестановочную матрицу размера $|X|$ (т.е. ее перманент над $\mathbb{R}$ не ноль).

(б) Докажите при помощи этой техники, что $L(MOD_2) = \Omega(n^2)$.

$\boxed{\textbf{COMP2 21.}}$ Пусть S_t — биномиальное распределение с t сбалансированными монетами. Докажите, что для любого $\delta < 1$,

$$\sum_{i=0}^{t+\delta\sqrt{t}} |\Pr[S_t = i] - \Pr[S_{t+\delta\sqrt{t}} = i]| \leq 20\delta.$$

$\boxed{\textbf{COMP2 22.}}$ Будем говорить, что коммуникационный протокол является протоколом с k раундами, если в этом протоколе количество "переходов хода" межу Алисой и Бобом равно k. Например, если сначала Алиса посылает что-то и после этого Боб знает ответ, то это однораундовый протокол. Обозначим сложность отношения R для протоколов с не более чем k раундами, как $C^{(k)}(R)$.

(а) Докажите, что для любой функции f верно, что $C^{(k)}(f) = O\left(\log\left(L^{(k)}(f)\right)\right)$, где $L(f)$ — число листьев формулы, которая вычисляет f в базисе $\{\wedge, \vee, \neg\}$ и эта формула глубины k (арность операций неограничена).

(б) Пусть $P \subseteq \{0,1\}^n \times \{0,1\}^n \times [n]$ — это такое отношение, что $(x, y, i) \in P$ тогда и только тогда, когда $\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$, $\sum_{i=1}^{n} y_i \equiv 1 \pmod 2$ и $x_i \neq y_i$. Докажите, что $C^{(k)}(f) = \Omega(n^{1/k})$.

(г) Пусть G — это граф квадратная решетка на n^2 вершинах, а $c : V \to \{0,1\}$ — это такое отображение, что есть только одна вершина v с $c(v) = 1$.

Докажите, что если $\mathrm{Search}_{\mathrm{TS}_{G,c}}$ — это такое отношение что Алисе дают значение переменных на нижнем треугольнике, а Бобу на верхнем и им надо найти клоз противоречия, то коммуникационная сложность этой задачи при ограничении, что раундов не больше чем k не меньше чем $\Omega(n^{1/k})$.

COMP2 23. Пусть $f_1(x_{11}, \ldots, x_{1n_1})$, $\ldots$, $f_m(x_{m1}, \ldots, x_{mn_m})$ — произвольные булевы формулы, зависящие от непересекающегося множества переменных. Докажите, что выполняется неравенство:

$$L(f_1(x_{11}, \ldots, x_{1n_1}) \oplus \cdots \oplus f_m(x_{m1}, \ldots, x_{mn_m})) \geq \frac{1}{2} \sum_i L(f_i),$$

где $L(f)$ — минимальное количество гейтов в формуле $\{\wedge, \vee, \neg\}$, вычисляющей f.

COMP2 25. Докажите, что если существует $S(n)$ псевдослучайный генератор, то существует такая функция $f \in E$, что $H_{wrs}(f|_{\{0,1\}^n}) \geq S(n)$.

COMP2 26. Докажите, что если перманент является полной задачей в классе $\sharp\mathbf{P}$ относительно сведений, сохраняющих число решений, то $\mathbf{NP} = \mathbf{RP}$.