

Список задач 1. Задачи курса.

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

- (а) схема
- (б) монотонная схема
- (в) монотонная формула полиномиального размера, вычисляющая функцию Maj .

COMP2 2. Докажите, что для любой симметрической булевой функции (симметрическая функция зависит только от числа единиц во входе) существует вычисляющая ее

- (а) схема
- (б) монотонная схема полиномиального размера.

COMP2 3. Докажите, что любая формула в КНФ (ДНФ), которая вычисляет функцию

- (а) $x_1 + x_2 + x_3 + \dots + x_n \pmod 2$;
- (б) $\text{Maj}(x_1, \dots, x_n)$ имеет экспоненциальный размер.

COMP2 4. Докажите, что существует формула от \wedge, \vee, \neg размера $O(n^2)$, которая вычисляет функцию $x_1 + x_2 + x_3 + \dots + x_n \pmod 2$.

COMP2 5. Докажите, что функция Maj не может быть вычислена при помощи схем полиномиального размера константной глубины из гейтов \wedge, \vee, \neg .

COMP2 6. Формальной мерой сложности называется отображение $\text{FC} : B_n \rightarrow \mathbb{N}$, обладающее следующими свойствами:

- $\text{FC}(x_i) = 1$;
 - $\text{FC}(f) = \text{FC}(\neg f)$;
 - $\text{FC}(f \vee g) \leq \text{FC}(f) + \text{FC}(g)$.
- (а) Докажите, что $\text{FC}(f \wedge g) \leq \text{FC}(f) + \text{FC}(g)$;
 - (б) Покажите, что $L(f)$ — это формальная мера сложности;
 - (в) (лемма Патерсона) Докажите, что для любой формальной меры сложности FC выполняется неравенство: $\text{FC}(f) \leq L(f)$.

COMP2 7. Для множеств $A, B \subseteq \{0, 1\}^n$ обозначим через $H(A, B)$ — множество пар соседей $\{(a, b) \in A \times B \mid \rho(a, b) = 1\}$, где ρ — расстояние Хемминга. Определим $K_{AB} = \frac{|H(A, B)|^2}{|A||B|}$ и $K(f) = \max\{K_{AB} \mid A \subseteq f^{-1}(1), B \subseteq f^{-1}(0)\}$. Докажите, что

- (а) $K(f)$ — формальная мера сложности;
- (б) (теорема Храпченко) $L(f) \geq K(f)$;
- (в) $K(f) \leq n^2$;
- (г) $L(Maj) = \Omega(n^2)$.

COMP2 8. Покажите, что представление $\bigwedge_{i=1}^n x_i$ в виде полинома $\mathbb{F}_q[x_1, \dots, x_n]$ (q — простое число) требуют степень ровно n .

COMP2 9. Докажите, что у любой формулы размера s существует эквивалентная формула глубины $O(\log(s))$.

COMP2 10. Какие значения может принимать глубина дерева решений (decision tree) для функции $f : \{0, 1\}^n \rightarrow \{0, 1\}$, где все аргументы не являются фиктивными (т.е. для каждого номера i найдется вход x , что $f(x) \neq f(x^i)$).

COMP2 11. Пусть $n = k^2$. Рассмотрим функцию $f : \{0, 1\}^n \rightarrow \{0, 1\}$, заданную следующим образом: вход разделен на блоки по k битов, функция равно 1 тогда и только тогда, когда существует блок в котором два последовательных бита равны единице, а остальные биты равны нулю. Оцените $s(f)$, $bs(f)$, $C(f)$, $D(f)$.

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

COMP2 13. Докажите, что $\mathbf{PCP}(0, \log(n)) = \mathbf{P}$.

COMP2 14. Докажите, что если $\mathbf{SAT} \in \mathbf{PCP}(o(\log(n)), 1)$, то $\mathbf{P} = \mathbf{NP}$.

COMP2 15. Докажите, что $C(f) = O(\log(C_L(f)))$.

COMP2 16. Каждая функция $f : X \times Y \rightarrow Z$ задает раскраску элементов матрицы $M[X, Y]$ в цвета из множества Z . Прямоугольником называется множество $X' \times Y'$, где $X' \subseteq X$ и $Y' \subseteq Y$. Прямоугольник называется одноцветным если все элементы $M[X', Y']$ покрашены в один цвет. Пусть $\chi(f)$ — минимальное число непересекающихся одноцветных прямоугольников, которыми можно покрыть все элементы M .

- (а) Докажите, что $C_L(f) \geq \chi(f)$.
- (б) Докажите, что $\chi(f) \geq rk(M)$, если Z — некоторое поле.
- (в) Докажите, что коммуникационная сложность функции GT : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$, которая равна 1 тогда и только тогда, когда $x > y$ (как натуральные числа в двоичной записи), не менее n .

COMP2 17. Пусть у Алисы и Боба есть множества $X, Y \subseteq \{1, \dots, n\}$. Они хотят посчитать функцию $\text{MED}(X, Y)$, которая возвращает медиану мультимножества $X \cup Y$. Докажите, что для этого им достаточно: $O(\log^2(n))$ битов коммуникации.

COMP2 18. Игры Карчмера-Вигдерсона. Дана функция $f : \{0, 1\}^n \rightarrow \{0, 1\}$. 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 $C(KW_f) \leq d(f)$ и $C_L(KW_f) \leq L(f)$, где $d(f)$ — минимальная глубина формулы, которая вычисляет f в базисе $\{\wedge, \vee, \neg\}$, а $L(f)$ — соответственно число листьев.
 (б) Докажите, что $C(KW_f) \geq d(f)$ и $C_L(KW_f) \geq L(f)$.

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

На основе сэмплера $S_{\epsilon, \delta}$ определим функцию $\text{Ext} : \{0, 1\}^r \times \{0, 1\}^{\log(q)} \rightarrow \{0, 1\}^n$ так, что $\text{Ext}(x, i)$ 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 $q = O(\frac{1}{\epsilon^2 \delta})$?

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

- (а) Докажите, что $\chi(M) \cdot T(M) \geq |X|^2$, где $T(M)$ — число единиц в матрице.
 (б) Докажите при помощи этой техники, что $L(\text{MOD}_2) = \Omega(n^2)$.

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

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

COMP2 22. Будем говорить, что коммуникационный протокол является протоколом с k раундами, если в этом протоколе количество “переходов хода” между 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 $C^{(k)}(f) = O(\log(L^{(k)}(f)))$, 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 $C^{(k)}(f) = \Omega(n^{1/k})$.

(в) Пусть G — это связный граф степени d , а $c : V(G) \rightarrow \{0, 1\}^n$. Будем называть цейтинской формулой $\text{TS}_{G,c}$ конъюнкцию уравнений $\sum_{u:(v,u) \in E(G)} x_{(u,v)} = c(v)$ для всех $v \in V$ записанную в КНФ.

Докажите, что $\text{TS}_{G,c}$ тогда и только тогда, когда $\sum_{v \in V(G)} c(v) = 1$.

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

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

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

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

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

COMP2 24. Покажите, что у случайной булевой функции $f : \{0, 1\}^n \rightarrow \{0, 1\}$ с большой вероятностью средняя сложность функции f не менее $2^{\frac{n}{10}}$ при больших n .

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

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

COMP2 27. Докажите, что любой (n, k) — источник является выпуклой комбинацией плоских (n, k) -источников.

COMP2 28. Пусть $E_1 : \{0, 1\}^n \rightarrow \Sigma^m$ и $E_2 : \Sigma \rightarrow \{0, 1\}^k$ — 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 $l_1 l_2$.

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 $f : \{0, 1\}^n \rightarrow \{0, 1\}$, 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 .

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 $\mathbf{MA} = \mathbf{NP}$.

COMP2 31. Пусть $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$ — это кандидат в $S(l)$ -псевдослучайные генераторы, которому не удастся дерандомизовать какой-то конкретный **ВРР** 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 больших 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 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) $|\mathbb{E}[D_n(G(U_{l(n)}))] - \mathbb{E}[D_n(U_{m(n)})]| \geq 0.1$.