

Задание 6.

CC22. 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 $E_1 \circ E_2$ существует локальный списочный декодер, который обрабатывает $\frac{1}{2} - \epsilon_1 \epsilon_2 \ell_2$ ошибок и выдает список размера $\ell_1 \ell_2$.

CC23. Докажите, что если существует δ -плотное распределение H на $\{0, 1\}^n$, что $\Pr_{x \leftarrow H}[C(x) = f(x)] \leq \frac{1}{2} + \epsilon$ для любой схемы C размера $S \leq \sqrt{\epsilon^2 \delta 2^n / 100}$, то существует подмножество $I \subseteq \{0, 1\}^n$ размера хотя бы $\frac{\delta}{2} 2^n$, что $\Pr_{x \leftarrow U(I)}[C(x) = f(x)] \leq \frac{1}{2} + \epsilon$.

CC24. а) Покажите, что существует детерминированный $poly(n)$ 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 $E[f(U_n)] \geq 2/3$, то A отвечает 1 с вероятностью хотя бы 0.99;
- Если $E[f(U_n)] \leq 1/3$, то A отвечает 0 с вероятностью хотя бы 0.99.

Такой алгоритм будем называть аппроксиматором функции.

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

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

CC1. Рассмотрим функцию $Maj : \{0, 1\}^n \rightarrow \{0, 1\}$, которая выдает 1, если не менее половины входных битов равны 1. Докажите, что существует полиномиального размера v монотонная формула (т.е. схема, использующая только гейты \vee и \wedge), вычисляющая функцию Maj .

CC10. Пусть $f_1(x_{11}, \dots, x_{1n_1}), \dots, f_m(x_{m1}, \dots, x_{mn_m})$ — произвольные булевы функции, 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 $L(f)$ обозначает минимальное количество гейтов в $\{\wedge, \vee, \neg\}$ -формуле, вычисляющей f .

CC13. а) Пусть $M[X, X]$ это 0/1-матрица, которая содержит перестановочную матрицу размера $|X|$ (т.е. ее перманент над \mathbb{R} не ноль). Докажите, что $R(M) \cdot T(M) \geq |X|^2$, где $T(M)$ — это число единиц в M . б) Докажите с помощью этой техники, что $L(MOD_2) = \Omega(n^2)$.

CC16. Для графа G обозначим через G' граф, в котором к каждому ребру нарисовали параллельную копию. Мы рассматриваем невыполнимую цейтинскую формулу $T_{G'}$, построенную по графу G' а) Рассмотрим случайную частичную подстановку: из каждого из двух параллельных ребер графа G' выбирается одно и переменной, которая этому ребру соответствует, подставляется случайное значение из $\{0, 1\}$, переменной из второго ребра ничего не подставляется. Для дизъюнкта размера W оцените вероятность того, что он не будет выполнен этой подстановкой. б) Докажите, что резолюционное доказательство формулы $T_{G'}$ имеет размер $2^{\Omega(\epsilon(G))}$.

CC19. Докажите, что если существует $S(\ell)$ -псевдослучайный генератор, то существует такая функция $f \in E$, что $H_{wrs}(f)(n) \geq S(n)$.

CC20. Докажите, что если существует $f \in E$ и $\epsilon > 0$, что $H_{avg}(f)(n) \geq 2^{\epsilon n}$ при всех n , то $MA = NP$.

CC21. Let $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be an $S(\ell)$ -length candidate pseudorandom generator that fails to derandomize a particular BPP algorithm A on the average case. That is, letting $L \in BPP$ be the language such that $\Pr[A(x) = L(x)] \geq 2/3$, it holds that for every sufficiently large n , with probability at least $1/n$ over the choice of $x \leftarrow \{0, 1\}^n$, $\Pr[A(x; G(U_{\ell(n)})) = L(x)] < 1/2$ (we let $\ell(n)$ be such that $S(\ell(n)) = m(n)$ where $m(n)$ denotes the length of random tape used by A on inputs of length n). Prove that there exists a probabilistic polynomial-time algorithm D that on input 1^n outputs a circuit D_n such that with probability at least $1/(2n)$ over the randomness of D , $|E[D_n(G(U_{\ell(n)}))] - E[D_n(U_{m(n)})]| > 0.1$.