Задание 5.

CC18. Докажите, что у случайной булевой функции с большой вероятностью $\{0,1\}^n \to \{0,1\}^n$ средняя сложность H_{avg} не меньше $2^{n/10}$ при больших n.

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

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

CC21. Let $G : \{0,1\}^* \to \{0,1\}^*$ 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, $|\,E[D_n(G(U_{\ell(n)})] - E[D_n(U_{m(n)})]| > 0.1$.

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

CC10. Пусть $f_1(x_{11}, \ldots, x_{1n1}), \ldots, f_m(x_{m1}, \ldots, x_{mn_m})$ — произвольные булевы функции, зависящие от непересекающегося множества переменных. Докажите, что выполняется неравенство:

$$L\left(f_1(x_{11}, \ldots, x_{1n1}) \oplus \cdots \oplus f_m(x_{m1}, \ldots, x_{mn_m})\right) \geq \frac{1}{2} \sum_i L(f_i),$$

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 $2^{\Omega(e(G))}$.