

Задание 14 (на 13.05).

СС 26. (подсказка: NEXP^{NP} vs. NEXP) Докажите, что если $\mathbf{P} = \mathbf{NP}$, то существует язык из \mathbf{EXP} , схемная сложность которого не меньше $\frac{2^n}{10n}$.

СС 44. Покажите, что:

(в) $\mathbf{BPP} \subseteq \mathbf{VTime}(n^{\log n}) \subsetneq \mathbf{VTime}(2^n)$.

СС 45. Определим язык

$$\mathbf{QNR} = \{(y, m) \mid y \text{ не является квадратичным вычетом по модулю } m\}.$$

Докажите, что $\mathbf{QNR} \in \mathbf{IP}$.

Определим класс \mathbf{UP} . $L \in \mathbf{UP}$, если существует такая недетерминированная машина Тьюринга M , что для любого x выполнено: $M(x) = L(x)$ и существует не более одной подсказки, которая принимается машиной M .

СС 54. Докажите, что:

(а) язык простых чисел лежит в классе \mathbf{UP} ;

(б) если $\mathbf{USAT} \in \mathbf{UP}$, то $\mathbf{NP} = \mathbf{co-NP}$.

СС 55. Покажите, что существует такой оракул A и язык $L \in \mathbf{NP}^A$, что L не сводится по Тьюрингу к $\mathbf{3SAT}$, даже если сведение может использовать оракул A .

СС 57. Покажите, что $\mathbf{AM} = \mathbf{AM}_1$

СС 59. Покажите, что если $\mathbf{PSPACE} \subseteq \mathbf{P/poly}$, то $\mathbf{PSPACE} = \mathbf{MA}$ (подсказка: используйте $\mathbf{IP} = \mathbf{PSPACE}$).

СС 62. Пусть есть оракул, который считает перманент матрицы $n \times n$ над полем \mathbb{F} верно для доли матриц $1 - \frac{1}{3n}$. Пусть $|\mathbb{F}| > 3n$. Докажите, что используя этот оракул можно построить вероятностный полиномиальный по времени алгоритм, который для каждой матрицы с большой вероятностью находит ее перманент.