

Задание 6 (на 26.03.14)

31. Пусть некоторое свойство m -битных строк имеет РСРР длины $\ell(m)$. Покажите, что для этого свойства существует РСРР длины $\text{poly}(\ell(m))$, в котором проверяющий алгоритм делает 3 запроса и затем использует один из восьми возможных OR-предикатов: $v_{i_1} \vee v_{i_2} \vee v_{i_3}, \neg v_{i_1} \vee v_{i_2} \vee v_{i_3}, \dots, \neg v_{i_1} \vee \neg v_{i_2} \vee \neg v_{i_3}$.

28. Предположим, что есть оракульный доступ к двум функциям $\ell : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ и $q : \mathbb{F}_2^{n \times n} \rightarrow \mathbb{F}_2$. Предложите 4-запросовый тестирующий алгоритм, который обладает следующими свойствами: (1) Если $\ell = \chi_\gamma$ и $q = \chi_{\gamma\gamma^T}$, то тест принимает с вероятностью 1. (2) Если тест принимает с вероятностью хотя бы $1 - \lambda\epsilon$, то существует некоторое $\gamma \in \mathbb{F}_2^n$, что ℓ является ϵ -близким к χ_γ , а q является ϵ -близким к $\chi_{\gamma\gamma^T}$.

29. Пусть L — это список однородных полиномиальных равенств степени 2 над переменными $w_1, w_2, \dots, w_n \in \mathbb{F}_2$. Пусть \mathcal{L} состоит из $w \in \mathbb{F}_2^n$, которые выполняют все равенства из списка L . Покажите, что существует 4-запросовая РСРР с длиной доказательства $2^n + 2^{n^2}$ для L .

30. Дана булева схема C с n входами. Докажите, что для множества для множества выполняющих наборов схемы C можно построить 3-запросовую РСРР с длиной доказательства $2^{\text{poly}(|C|)}$.