Задание 6 (на 28.03.18)

23. Покажите, что существует такое распределение D на $\{0,1\}^n$, которое является $(t, t2^{-t})$-независимым для которого существует такой вероятностный алгоритм A, который получает оракульный доступ к входу длины n и может во время своей работы адаптивно запросить t битов входа, что $|\Pr_{x\leftarrow D}[A(x)=1] - \Pr_{x\leftarrow U_n}[A(x)=1]| \geq \frac{1}{2}$.

24. Пусть S — это множество n-битных, в которых число единиц делится на 3. Докажите, что равномерное распределение на S является ϵ-смещенным при $\epsilon = 2^{-\Omega(n)}$.

25. Пусть $G : \{0,1\}^k \to \{0,1\}^n$ задает ϵ-смещенное распределение на $\{0,1\}^n$ (имеется в виду, что $maxbias(G(U_k)) \leq \epsilon$) при $\epsilon < 1$. а) Пусть каждый бит выхода G задается многочленом над $\mathbb{F}_2$ степени не больше d от k входов. Докажите, что $n \leq \sum_{i=1}^{d} \binom{k}{d}$. б) Покажите, что $n < 2^k$; в) Покажите, что если $n > k$, то G не может быть линейным.

26. Покажите, что если выбрать Cn/ϵ^2 случайных независимых элементов $\{0,1\}^n$, то равномерное распределение на полученном мультимножестве будет ϵ-смещенным с вероятностью не менее $1 - 2^{-\Omega(n)}$ при достаточно большой константе C.

---

23. Покажите, что для формулы в КНФ, состоящей из m дизъюнктов, в которой любые три дизъюнкта можно одновременно выполнить, существует набор значений переменных, который выполняет как минимум $\frac{2}{3}m$ дизъюнктов.

30. в) Линейным кодом называется линейное подпространство $C \subseteq \mathbb{F}^n$, расстояние линейного кода — это минимальное число ненулевых элементов, которые бывает у элементов C (или, эквивалентно, минимальное число различий между двумя элементами C). Как из линейного кода с расстоянием $k+1$ построить k-независимое множество.

31. Придумайте вероятностный алгоритм A, который получает на вход формулу ϕ в ДНФ, ϵ и δ, работает время $poly(|\phi|, \frac{1}{\epsilon}, \log\frac{1}{\delta})$ и $\Pr[|A(\phi,\epsilon,\delta) - \sharp\phi| \geq \epsilon\sharp\phi] \leq \delta$, где $\sharp\phi$ — это число выполняющих наборов формулы ϕ.