Задание 5 (на 21.03.18)

$\boxed{\textbf{28.}}$ Докажите, что если есть такой вероятностный полиномиальный по времени алгоритм A с оракулом SAT, который на любой формуле с вероятностью $\frac{9}{10}$ выдает точное число ее выполняющих наборов, то полиномиальная иерархия схлопывается. (В решении можно пользоваться теоремой Тода о том, что любой язык из полиномиальной иерархии решается за полиномиальное время с использованием оракула, который считает число выполняющих наборов любой пропозициональной формулы.)

$\boxed{\textbf{29.}}$ (Лемма о перемешивании для хеш-функций) Пусть $m < n$ и $H_{n,m}$ — семейство попарно независимых хеш-функций $\{0,1\}^m \to \{0,1\}^n$. Тогда для лбого $\epsilon > 0$ и любых $S \subseteq \{0,1\}^n, T \subseteq \{0,1\}^m$ выполняется

$$\Pr_{h \leftarrow H_{n,m}}[||\{x \in S : h(x) \in T\}| - |T||S|/2^m| > \epsilon|T||S|/2^m] \leq \frac{2^m}{|T||S|\epsilon^2}.$$

$\boxed{\textbf{30.}}$ Пусть $n = 2^k - 1$. H — это матрица размера $k \times n$, все столбцы которой — это все различные ненулевые вектора из $\{0,1\}^k$. а) Проверьте, что множество $= \{x \in \{0,1\}^n \mid Hx = 0\}$ является кодом с расстоянием 3, т.е. расстояние Хемминга между любыми двумя точками C не меньше трех. (Все операции над $\mathbb{F}_2$). б) Проверьте, что множество $W = \{y^T H \mid y \in \{0,1\}^k\}$ является 2-независимым множеством размера $n+1$. 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.

$\boxed{\textbf{31.}}$ 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.

$\boxed{\textbf{32.}}$ Покажите, что для любого полинома p для пропозициональной формулы ϕ вычисление приближения $\sharp\phi$ с (мультпликативной) точностью $\frac{1}{p}$ и ошибкой $\delta < 1/2$ сводится за полиномиальное время к вычислению приближения $\sharp\phi$ с точностью $\frac{1}{2}$ и ошибкой $\delta < 1/2$.

---

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.