Задание 7. (на 28.03)

Число задач для записи: 1.

CR 27. Покажите, что в определени класса AvgBPP можно понизить обе константы $\frac{1}{8}$ можно понизить до 2^{-n}.

CR 28. Покажите, что AvgBPP $\subseteq$ HeurBPP.

CR 29. Покажите, что AvgBPP и HeurBPP замкнуты относительно сведений.

CR 30. Покажите, что если $(\mathrm{NP}, \mathrm{PISAMP}) \subseteq \mathrm{Heur}_{\frac{1}{n}}\mathrm{P}$, то $(\mathrm{NP}, \mathrm{PISAMP}) \subseteq \mathrm{HeurP}$.

CR 31. Покажите, что существует язык $L \in \mathrm{P}$, что $(L, U) \notin \mathrm{HeurP}$.

Дополнительные задачи

Это задачи для тех, кому не хватает баллов. Эти задачи не будут разбираться на занятии. Их можно сдавать позже

CR 32. Пусть f — сильно односторонняя функция. Докажите, что для любого вероятностного полиномиального по времени алгоритма A и любого положительного полинома p множество $B_{A,p} = \left\{x \mid \Pr[A(f(x)) \in f^{-1}(f(x))] \geq \frac{1}{p(|x|)}\right\}$ имеет пренебрежимо малую плотность (т.е. последовательность $\frac{|B_{A,p} \cap \{0,1\}^n|}{2^n}$ пренебрежимо мала).

CR 33. Постройте функцию, которая будет сильно односторонней, если односторонние функции существуют.

CR 34. Полиномимально вычислимая функция $f : \{0,1\}^* \to \{0,1\}^*$ называется распределенной односторонней, если существует такой полином p и для всех полиномиальных по времени вероятностных алгоритмов A и для всех достаточно больших n статистическое расстояние между распределениями $(U_n, f(U_n))$ и $(A(1^n, f(U_n)), f(U_n))$ больше, чем $1/p(n)$. а) Докажите, что f — слабая односторонняя, то она распределенная односторонняя. б) Докажите, что если существуют распределенные односторонние функции, то существуют и односторонние.

CR 35. Пусть $G(x)$ — это $(n+1)$-генератор. Докажите, что $G^{(p(n))}$ (многократная композиция) — то $p(n)$-генератор.

CR 36. Докажите, что если существует схема кодирования с открытым ключом для однобитового сообщения, то существует и схема кодирования с открытым ключом для произвольных сообщений полиномиальной длины.