Задание 5. (на 14.03)

Число задач для записи: 2.

CR 23. Покажите, что если $\mathrm{E}_{x \leftarrow D_n}[t(x)] = poly(n)$, то найдется такое $\epsilon > 0$, что $\mathrm{E}_{x \leftarrow D_n}[t^\epsilon(x)] = O(n)$.

CR 24. Придумайте полиномиальный от n алгоритм, который в интервале $[a, b]$, где a и b — это двоично рациональные числа из не более, чем n цифр, находит наибольший стандартный интервал(вида $[0.r0, 0.r1]$).

CR 25. Ансамбль распределений D_n называется вычислимым за полиномиальное время, если функция распределения ($F_{D_n}(x) = \sum_{y<x} D_n(y)$ где $<$ — это лексикографический порядок на строках) вычислима за полиномиальное время. Пусть S — это сэмплер для некоторого распределения. Если сэмплер S, используя случайную строку r, генерит строку x, то будем считать, что сэмплер отображает отрезок $[0.r0, 0r1)$ в строку x. Полиномиально моделируемый ансамбль D_n называется обратимым, если сэмплер S для этого ансамбля обладает такими свойством: прообраз каждой строки x — это один отрезок, концы которого вычисляются за полиномиальное от $|x|$ время. Докажите, что вычислимое распределение является а) полиномиально моделируемым; б) обратимым полиноимально моделируемым.

CR 26. Будем говорить, что распределенная задача (L, D) лежит в классе HeurBPP, если существует такой вероятностный алгоритм $A(x, \delta, 1^n)$, что при всех x из носителя D_n время работы $A(x, \delta, 1^n)$ ограничено $poly(n/\delta)$ и $\mathrm{Pr}_{x \leftarrow D_n}[\mathrm{Pr}[A(x, \delta, 1^n) \neq L(x)] \geq \frac{1}{4}] < \delta$, внутренняя вероятность берется по случайным битам алгоритма A. Докажите, что второе условие можно эквивалентным образом заменить на более простое: $\mathrm{Pr}_{x \leftarrow D_n}[\mathrm{Pr}[A(x, \delta, 1^n) \neq L(x)] < \delta$, тут вероятность берется также и по случайным битам алгоритма A.

CR 15. б) Покажите, что существуют такие величины α_n и β_n, которые вычислительно неразличимые, но различимы схемами полиномиального размера.

CR 21. Пусть стратегия F_x разглашает только $f(x)$, а стратегия G_x разглашает только $g(x)$. Докажите, что при последовательном применении стратегия $F_x G_x$ разглашает только $(f(x), g(x))$.