Задачи к курсу
Алгоритмические методы в теории сложности.
(мехмат, весна 2013).

Некоторые из предлагаемых задач обсуждались на лекциях курса (this is not a bug, this is a feature). При решении задач разрешается пользоваться любой литературой.

Задача 1. Пусть множество $S \subset \{0,1\}^n$ содержит не менее двух элементов. Для каждой пары n-ок битов x, y будем обозначать

$$(x,y) = x_1y_1 + \ldots + x_ny_n \ mod\ 2.$$

Выберем наборы битов $v_1, \ldots, v_n \in \{0,1\}^n$ случайно (каждое по равномерному распределению и независимо друг от друга). Докажите, что с вероятностью не менее $1/4$ найдётся такое число $i \leq n$, что

$$(x, v_1) = \ldots = (x, v_i) = 0$$

для ровно одного элемента $x \in S$.

Задача 2. Предположим, что существует вероятностный полиномиальный алгоритм, вычисляющий *четность* числа клик заданного размера k в заданном графе G. Докажите, что тогда NP $\subset$ BPP.

Задача 3. (а) Докажите, что если существует детерминированный или вероятностный полиномиальный алгоритм решения задачи SAT (задача распознавания свойства выполнимости булевой формулы), то существует также и полиномиальный вероятностный алгоритм, который по заданной выполнимой булевой формуле находит выполняющий набор.

(б) Предположим, что для любого языка в NP и для любого $\delta(n) = 1/\mathrm{poly}(n)$ найдется полиномиальный вероятностный алгоритм $A(x,r)$ такой, что для всех n

$$\forall x \in L\ \mathrm{Prob}_{x,r}[A(x,r) = \text{да}] \geq 1 - \delta(n),$$

и

$$\forall x \in L\ \mathrm{Prob}_{x,r}[A(x,r) = \text{нет}] \geq 1 - \delta(n)$$

(вероятность берется по случайным входам x длины n и по датчику случайных битов r алгоритма A).

Докажите, что тогда для любого $\delta'(n) = 1/\mathrm{poly}(n)$ найдется полиномиальный вероятностный алгоритм $B(\varphi, r)$ такой, что для каждого n и для 99% выполнимых формул φ длины n

$$\mathrm{Prob}_r[B(\varphi,r) = \text{выполняющий набор булевых значений для } \varphi] \geq 1 - \delta'(n).$$

Другими словами, если есть полиномиальный вероятностный алгоритм для случайных переборных задач распознавания, то есть полиномиальный вероятностный алгоритм и для случайных переборных задач поиска.

Задача 4. Докажите, что задача распознавания гамильтоновости графа (существование в графе гамильтонова цикла) является NP-полной.

Задача 5. Докажите, что для любого n и любого $k < n$ существует семейство $\mathcal{H}$ из $2^{O(n)}$ хэш-функций $h : \{0,1\}^n \to \{0,1\}^k$, обладающее свойством 3-независимости: для любой тройки попарно различных $x, x', x'' \in \{0,1\}^n$ и любой тройки $y, y', y'' \in \{0,1\}^k$

$$\mathrm{Prob}_{h\in\mathcal{H}}[h(x) = y \;\&\; h(x') = y' \;\&\; h(x'') = y''] = 1/2^{3k}.$$

Задача 6. (а) Придумайте для языка *квадратичных невычетов x по заданному модулю n* протокол интерактивного доказательства.

(б) Придумайте для языка *квадратичных невычетов x по заданному модулю n* игру Артура и Мерлина (с открытыми для Мерлина случайными битами Артура).

Задача 7. Придумайте для задачи *неизоморфизм графов* протокол игры Артура и Мерлина, состоящий из двух раундов: сначала Артур посылает Мерлину своё сообщение, затем Мерлин посылает ответ Артуру, после чего Артур дает окончательный ответ (без нового бросания монетки). При этом для неизоморфных графов ответ всегда (с вероятностью 1) должен быть положительным, а для изоморфных с вероятностью не менее 3/4 отрицательным.

Задача 8. Будем обозначать AM, MA, MAM типы игр Артура и Мерлина следующего вида.

- AM: в первом раунде Артур бросает случайную монету и сообщает результаты бросания Мерлину, во втором раунде Мерлин присылает сообщение Артуру, после чего Артур детерминированно (без нового бросания монетки) выносит вердикт;
- MA: в первом раунде своё сообщение посылает Мерлин, после чего Артур бросает случайную монету и выносит вердикт;
- MAM: в первом раунде сообщение посылает Мерлин, во втором раунде Артур бросает случайную монету и сообщает результаты бросания Мерлину, в третьем раунде Мерлин посылает Артуру новое сообщение, после чего Артур детерминированно выносит вердикт.

(а) Докажите, что для всякого языка, для которого существует протокол вида MA, можно построить протокол вида AM.

(б) Докажите, что для всякого языка, для которого существует протокол вида MAM, можно построить протокол вида AM.

Задача 9. (а) Докажите, что если для языка L есть интерактивная система доказательств (в котором случайные биты Верифайера скрыты от Прувера), то для L есть также игра Артура и Мерлина (в которой случайные биты Артура открыты для Мерлина).

(б) Докажите, что любой протокол интерактивного доказательства можно переделать в протокол игры Артура и Мерлина (с открытыми для Мерлина случайными битами Артура), увеличив число раундов не более, чем на $O(1)$.

Задача 10. Предположим, что задача *изоморфизм графов* NP-полна. Докажите, что $\mathrm{PH} = \Sigma_2^p$.

Задача 11. Сформулируйте понятия доказательства с абсолютно нулевым разглашением информации и статистически нулевым разглашением информации (perfect zero knowledge proof и statistical zero knowledge proof). Докажите, что свойство *изоморфизма графов* имеет доказательство со статистически нулевым разглашением.

Задача 12. Обозначим MOD_{1069}^n следующую функцию n булевых аргументов

$$\mathrm{MOD}_{1069}^n(x_1, \ldots, x_n) = \begin{cases} 1 & \text{если } x_1 + \ldots + x_n \text{ делится на 1069} \\ 0 & \text{иначе.} \end{cases}$$

Докажите, что MOD_{1069}^n можно вычислить ветвящейся программой ширины 5 и длины $\mathrm{poly}(n)$.