Что такое проблема P vs NP?

Занятие 4. Приближённые алгоритмы
Определения и задачи

До сих пор мы подразумевали, что нам необходимо решать задачи точно. Оказывается, иногда гораздо легче решить задачу приближённо.

1. Назовём покрытием неориентированного графа такое подмножество множества его вершин, что каждое ребро графа соприкасается хотя бы с одной вершиной этого подмножества. Пусть $VERTEXCOVER = \{\langle G, k\rangle$: граф G имеет покрытие размера $k\}$. **а)** Докажите, что $VERTEXCOVER \in$ NP. **б)** Докажите, что язык $VERTEXCOVER$ является NP-полным. Из этого следует, что задача поиска минимального покрытия графа сложная. **в)** Докажите, что можно за полиномиальное время находить покрытие графа, не больше чем в два раза превосходящее минимальное.

2. Назовём разрезом неориентированного графа разбиение множества его вершин на два подмножества, и назовём размером этого разреза количество рёбер, соединяющих вершины из разных подмножеств. $MAXCUT = \{\langle G, k\rangle$: граф G имеет разрез размером не меньше $k\}$. **а)** Докажите, что язык $MAXCUT$ является NP-полным. **б)** Докажите, что можно за полиномиальное время находить разрез в графе, меньший максимального не более чем в два раз.

Вероятностная машина Тьюринга — это недетерминированная машина Тьюринга, у которой каждый недетерминированный шаг имеет два равновероятных варианта. Такой шаг будем называть бросанием монеты. Вероятностью ветви вычисления мы считаем число 2^{-k}, где k — количество бросаний монеты на этой ветви. Вероятностью $\Pr(M$ принимает $w)$ того, что вероятностная машина M принимает слово w, назовём сумму вероятностей всех ветвей вычисления этой машины, на которых слово w принимается. Разрешающая вероятностная машина M разрешает язык A с вероятностью ошибки ε, если при $w \in A$ выполнено $\Pr(M$ принимает $w) \geqslant 1-\varepsilon$, и при $w \notin A$ выполнено $\Pr(M$ принимает $w) \leqslant \varepsilon$. Вероятность ошибки ε может зависеть от длины входа n. Класс всех языков, которые разрешаются за полиномиальное время (на всех входах на всех ветвях вычисления) с вероятностью ошибки $\frac{1}{3}$, обозначим BPP (bounded-error probabilistic polynomial-time).

3. а) Докажите, что если константу $\frac{1}{3}$ в определении класса BPP заменить на любую другую константу строго между 0 и $\frac{1}{2}$, класс не изменится. **б)** Докажите, что если в определении класса BPP взять вероятность ошибки $\varepsilon = 2^{-\mathrm{poly}(n)}$, где $\mathrm{poly}(n)$ — произвольный полином, зависящий от n, то класс не изменится.

В некотором смысле вероятностным аналогом класса NP являются интерактивные доказательства. В схеме интерактивного доказательства есть Доказывающий P (prover) и Проверяющий V (verifier). Вычислительные возможности Проверяющего — полиномиально ограниченная по времени вероятностная машина Тьюринга, вычислительные возможности Доказывающего не ограничены. Им известно входное слово w длины n. Они обмениваются сообщениями полиномиальной от n длины, пока Проверяющий не примет или отвергнет слово. Он должен сделать это за полиномиальное от n время. Вероятностью $\Pr(V \leftrightarrow P$ принимает слово $w)$ называется сумма вероятностей по всем ветвям вычисления на слове w, в которых Проверяющий принял слово. Язык A принадлежит классу IP (interactive proofs), если для него существует схема интерактивного доказательства $V \leftrightarrow P$, такая что при $w \in A$ выполнено $\Pr(V \leftrightarrow P$ принимает слово $w) \geqslant \frac{2}{3}$ и при $w \notin A$ выполнено $\Pr(V \leftrightarrow P$ принимает слово $w) \leqslant \frac{1}{3}$.

4. а) $ISO = \{\langle G, H\rangle$: графы G и H изоморфны$\}$. Докажите, что $ISO \in$ NP. **б)** $NONISO = \{\langle G, H\rangle$: графы G и H не изоморфны$\}$. Докажите, что $NONISO \in$ IP.

Класс coNP состоит из всех задач, дополнения к которым лежат в NP. Класс PSPACE состоит из всех задач, которые разрешимы машиной Тьюринга с полиномиальной памятью. EXPTIME — класс задач, разрешимых за экспоненциальное время.

5. Докажите включения (это известные, но иногда трудные результаты): **а)** P $\subseteq$ NP; **б)** P $\subseteq$ coNP; **в)** P $\subseteq$ BPP; **г)** NP $\subseteq$ IP; **д)** BPP $\subseteq$ IP; **е)** NP $\subseteq$ PSPACE; **ж)** BPP $\subseteq$ PSPACE; **з)** IP = PSPACE; **и)** P $\subsetneq$ EXPTIME.

6. Здесь мы перечисляем трудные открытые проблемы теории сложности вычислений. В каждом пункте надо доказать или опровергнуть соотношение (указана более общепринятая гипотеза). **а)** P $\subsetneq$ NP; **б)** BPP $\subseteq$ P; **в)** NP $\neq$ coNP; **г)** P $\subsetneq$ NP$\cap$coNP; **д)** NP $\subsetneq$ PSPACE.