Что такое проблема P vs NP?

Занятие 2. Классы P и NP
Определения и задачи

Пусть $f, g\colon \mathbb{N} \to \mathbb{N}$ — функции. Говорят, что "f есть о большое от g при n стремящемся к бесконечности" и пишут $f = O(g)$, если существует такая константа $C > 0$ и такое $n_0 \in \mathbb{N}$, что для всех $n > n_0$ выполнено $f(n) \geqslant Cg(n)$.

Мы говорим, что машина Тьюринга работает за полиномиальное время, если для некоторого k максимальное её время работы на входе длины n есть $O(n^k)$ при $n \to \infty$.

Недетерминированная машина Тьюринга называется разрешающей, если она заканчивает работу на каждой своей ветви вычисления. Разрешающая машина Тьюринга работает за полиномиальное время, если для некоторого k максимальное время её работы на любой ветви вычисления на входе длины n есть $O(n^k)$ при $n \to \infty$.

Класс всех языков, для которых существует разрешающая их машина Тьюринга, работающая за полиномиальное время, обозначается P. Класс всех языков, для которых существует разрешающая их недетерминированная машина Тьюринга, обозначается NP. Как несложно видеть, $\mathrm{P} \subseteq \mathrm{NP}$.

1. Докажите, что язык $A = \{0^k1^k : k \geqslant 0\}$ лежит в классе P. Какова его реальная сложность (асимптотически)?

2. а) Как кодировать словами в двоичном алфавите последовательности произвольной длины слов в двоичном алфавите? Как кодировать словами конечного алфавита **б)** натуральные числа? **в)** графы? **г)** Как кодировать числа и графы двоичными словами?

Таким образом, мы можем рассматривать не только задачи о словах, но и о числах, графах, других объектах. Напоминаем, что такое кодирование мы обозначаем угловыми скобками $\langle\cdot\rangle$.

3. Докажите, что следующие языки лежат в классе P:
а) $PATH = \{\langle G, s, t\rangle$: в ориентированном графе G есть путь из s в $t\}$; **б)** $RELPRIME = \{\langle x, y\rangle$: x и y взаимно просты$\}$; **в)** $MODEXP = \{\langle a, b, c, p\rangle : a, b, c, p$ — записанные в двоичной системе счисления натуральные числа, такие что $a^b \equiv c \pmod{p}\}$.

4. Докажите, что следующие языки лежат в классе NP:
а) $HAMPATH = \{\langle G, s, t\rangle$: в неориентированном графе G есть гамильтонов (проходящий по всем вершинам ровно по одному разу) путь из s в $t\}$; **б)** $COMPOSITES = \{x : x = pq$ для каких-то целых чисел $p, q > 1\}$; **в)** $CLIQUE = \{\langle G, k\rangle : G$ содержит полный подграф с k вершинами$\rangle\}$;
г) $SUBSETSUM = \{\langle S, t\rangle : S = \{x_1, \ldots, x_k\}$, и для некоторого подмножества $\{y_1, \ldots, y_l\} \subset \{x_1, \ldots, x_k\}$ выполнено $\sum y_i = t\}$.

5. Верно ли, что $COMPOSITES \in \mathrm{P}$?

6. Все слова языка L принимаются машиной Тьюринга M за полиномиальное время, и никакие другие слова машиной M не принимаются (но, возможно, и не отвергаются). Верно ли, что L лежит в P?

Проблема: равны ли классы P и NP?

В настоящее время эта проблема — одна из основных задач theoretical computer science и математики вообще. Обычно она датируется 1971 годом (поставлена независимо Левиным и Куком) и с тех пор остаётся открытой.