Алгоритмы и модели вычислений, группы $774 - 775$, задание 3

- Кормен–Лейзерсон–Ривест–Штайн, глава 34, параграфы 2 и 3. 2-й параграф является обязательным, а 3 стоит начать, более подробно речь пойдёт на семинаре.
- Конспекты 2 и 3 лекций Мусатова по курсу теории сложностей у ФИВТов:
http://ru.discrete-mathematics.org/fall2017/3/complexity/compl-book.pdf.
Лекцию 2 теперь уже нужно прочитать полностью, а лекцию 3 стоит начать читать.
- Хорошая книжка по теории сложностей на английском - http://theory.cs.princeton.edu/complexity/book.pdf. Пока можно ограничиться параграфом 2.1, но вся 2-я глава будет нужна для следующей темы $\mathcal{NP}$-полноты. Разделы про $\mathcal{EXP}, \mathcal{NEXP}$ можно спокойно пропустить. Не бойтесь математического английского! Он простой, серьёзно.
- Также рекомендуем книгу блестящих математиков Гача и Ловаса по вычислительной сложности:
http://www.cs.elte.hu/∼lovasz/complexity.pdf. Здесь вам стоит разобраться с главой 6 (кроме $\mathcal{NP}$-полноты, про неё речь пойдёт на следующем семинаре), в ней разобраны много примеров доказательства принадлежности языков классу $\mathcal{NP}$.

Задание 3

В задачах можете пользоваться любым из определений класса $\mathcal{NP}$ - через недетерминированные машины Тьюринга или сертификаты.

1. Докажите следующие свойства класса $\mathcal{NP}$:
   (i) Класс $\mathcal{NP}$ замкнут относительно итерации. ($A \in \mathcal{NP} \ \Rightarrow\ A^* \in \mathcal{NP}$)
   (ii) Имеет место вложение $\mathcal{P} \in co-\mathcal{NP}$ ($A \in \mathcal{P} \ \Rightarrow\ A \in co-\mathcal{NP}$)
2. Докажите, что следующие языки лежат в классе $\mathcal{NP}$:
   (i) $3-SAT$ - язык, состоящий из описания булевых формул в виде 3-КНФ, таких, что они обращаются в истину на некотором наборе переменных.
   (ii) $VCOVER$ - язык графов, имеющих вершинное покрытие заданной мощности.
   $VCOVER = \{(G,k) \mid \exists H \subseteq V(G) : |H| \le k,\ \forall (v,u) \in E(G) \to\ u \in H \text{ or } v \in H\}$
   (iii) Язык, состоящий из описаний всех ориентированных графов, в которых есть эйлеров путь.
   (iv) Язык, состоящий из описаний всех ориентированных взвешенных графов, в которых нет цикла отрицательной длины.
   (v) Язык, состоящий из пар (G, w), где G - набор правил, описывающих контекстно-свободную грамматику над алфавитом $\{1,2\}$, а $w \in \{1,2\}^*$ - слово, невыводимое в этой грамматике.
   (vi) $PLANARITY$ - язык описаний планарных графов, то есть графов, которые можно разместить на плоскости без пересечения ребер.
3. Докажите, что следующие языки лежат в классе $co-\mathcal{NP}$, внимательно оговаривайте способ кодирования входа и следите за тем, что чему является дополнением:
   (i) $TAUT$ - язык, состоящий из описаний булевых формул, являющихся общезначимыми (тавтологиями).
   (ii) Язык, состоящий из пар (G, k) где G - описание графа, такого, что для любых k вершин найдется ребро, соединяющее хотя бы 2 из них.
   (iii) $FACTORING$ - язык натуральных троек (a, b, c) таких, что a имеет простой делитель из отрезка $[b, c]$
   (iv) Язык описаний графов, в которых есть клика на 2019 элементах (клика - это подмножество вершин графа, таких, что каждая соединена ребром с каждой).
   (v) * $PLANARITY$ - язык описаний планарных графов, то есть графов, которые можно разместить на плоскости без пересечения ребер.
4. Пусть $f(x, y)$ - некоторый предикат, вычислимый за время, полиномиальное от суммы длин аргументов. Правда ли, что для произвольного фиксированного y_0 задача проверки общезначимости предиката $g(x) = f(x, y_0)$ лежит в $co-\mathcal{NP}$?

5. На семинаре мы обсуждали принадлежность языка, состоящего из десятичных описаний простых чисел, классу $co-\mathcal{NP}$, к сожалению, вышло достаточно скомкано. Просим вас как следует разобраться с этим материалом, обратившись к литературе по ключевому слову "сертификат Пратта". Докажите полиномиальность длины построенного сертификата, построив и оценив соответствующую рекурренту. После чего постройте сертификат простоты для числа 100091237.

6. Докажите, что для языков над унарным алфавитом (языки входа и сертификата обычно подразумевают совпадающими, если явно не сказано обратное) $\mathcal{P} = \mathcal{NP}$ в смысле наших определений.

7. Задача называется лежащей в классе $\mathcal{NP}$, если она решается за полиномиальное время по входу в том предположении, что существует полиномиальная процедура разрешения некоторого $\mathcal{NP}$ языка. Докажите, что следующие задачи лежат в $\mathcal{NP}$:

   (i) Два графа являются изоморфными

   (ii) Найти максимальную по количеству вершин клику в графе

   (iii) Проверить, что система линейных уравнений с 2019 целочисленными переменными и целочисленными коэффициентами не имеет решений

   В задаче нужно: 1) сформулировать определение связанного с задачей языка; 2) показать, что этот язык лежит в классе $\mathcal{NP}$; 3) В предположении, что существует некоторая подпрограмма, разрешающая этот язык за полиномиальное по входу время, построить полиномиальный алгоритм решения задачи.