Домашнее задание 3

Турков Матвей, группа 777

1

Решение:

1. Сошлюсь на существующее доказательство , которое я понял и не вижу смысла просто перепечатывать . Тык

2. $\mathcal{P} \in co - \mathcal{NP} \to L \in \mathcal{P} \Rightarrow L \in co - \mathcal{NP}$. Ясно, что $\mathcal{P} \subseteq \mathcal{NP}$, так как $\forall L \in \mathcal{P}\, \exists$ полиномиальный алгоритм, разрешающий язык(вроде как было показано на семинаре). Рассмотрим язык $co - \mathcal{NP} = \{L | \overline{L} \in \mathcal{NP}\}$.В силу замкнутости языков из $\mathcal{P}$ относительно дополнения и $\mathcal{P} \subseteq \mathcal{NP} \to \mathcal{P} \subseteq co - \mathcal{NP}$

2

Решение:

1. $3-$SAT .Данный язык лежит в классе $\mathcal{NP}$,$\forall x \exists$ сертификат y, при котором x истина, если такого нет, то y ,например, набор нулей.

2. VCOVER - Сертификат y в данном случае - то вершинное покрытие мощности k, или любое множество, например, пустое, если не существует Легко понять, что МТ работает за полиномиальное время и при этом $|y| = O(|(G, k)|^c)$

3. Язык, состоящий из графов, содержащий эйлеров путь. Сертификат y набор ребер, образующий эйлеров путь, а МТ $A(x, y)$ будет идти по графу и убирать встретившиеся ребра, если встретилось дважды или не было пройдено - МТ вернет 0, иначе 1, в случае графов, в которых нет эйлерова пути сертификатом произвольное множество ребер Данный алгоритм полиномиален

4. Язык, состоящий из описаний всех ориентированных взвешенных графов, в которых нет цикла отрицательной длины. Сертификат y вершины, образующие цикл отрицательной длины, если такого не существует, то сертификат произвольное множество. МТ проверяет содержит ли граф ребра из y, образуют ли они цикл отрицательной длины, идя последовательно и считая сумму ребер. Если сумма < 0, тогда МТ вернет 1 иначе 0. Данный алгоритм полиномиален и $|y| = O(|x|^c)$

5. Язык состоящий из пар (G, ω), где G - набор правил, описывающих КС-граматику над алфавитом $\{1, 2\}$, а $\omega \in \{1, 2\}^*$ - слово невыводимое в этой граматике. По КС-грамматике легко строится МП автомат за полином. Если слово лежит в языке, то запустим МП автомат G на ω,в качестве сертификата y переходы, по которым получим ω, если оно выводимо в граматике или любое множество, если нет. МП автомат остановится в принимающем состоянии МТ вернет 0 и 1 соответственно . Сертификат $|y| = O(|G|^c)$, язык лежит в $\mathcal{NP}$

6. PLANARITY - язык описаний планарных графов. Данный язык принадлежит классу $\mathcal{P}$, так как достаточно посчитать $V - E + F$ Таким образом, язык принадлежит $\mathcal{P}$ и $\in \mathcal{NP}$

3

Решение:

1. TAUT. Докажем, что язык $L = \overline{\text{TAUT}}$ лежит в $\mathcal{NP}$. Рассмотрим МТ $A(x, y)$, выводяющую значение $\overline{x(y)}$.Данная МТ работает за полином. $\forall$ формулы $\exists$ сертификат: для общезначимых - любой, для остальных- набор, на котором формула обращается в ноль, при этом также$\exists$ МТ $A(x, y)$, выдающая 1 , когда x - не является общезначимой за полиномиальное время и $|y| = O(|x|^c)$. Принадлежность доказана

2. L - язык, состоящий из пар (G, m), где G - описание графа такого, что для любых m вершин найдется ребро, соединяющее хотя бы 2 из них. Рассмотрим сертификатy для $\overline{L}$. Это набор из m вершин, причем МТ $A((G, m), y)$ для каждой пары вершин из y проверяет лежит ли эта пара в множестве ребер графа G. Эта операция полином по входу и $|y| = O(|(G, m)|^c)$. Принадлежность доказана

3. FACTORING - язык натуральных троек (a, b, c) таких, что a имеет простой делитель из $[b, c]$. Рассмотрим МТ $A(x, y)$ для $L = \overline{\text{FACTORING}}$, в которой $x = (a, b, c)$ которая используя решето Эратосфена проверяет есть ли $[b, c]$ простые числа, если нет, то 1. Проверим делимость числа a на y простым перебором $z \in [1, a]$, если нет такого z , то возвращаем 1, иначе 0 . Таким образом, данная МТ работает за полином. Сертификатом простое число из $[b, c]$, если оно существует и, 0, если нет. $|y| = O(|x|^c)$ Принадлежность доказана

4. Язык описаний графов в в которых есть клика на 2019 элементов. Алгоритм из $\mathcal{P}$, так как существует ровно $C_n^{2019} = O(n^{2019})$ способов выбрать n из 2019, при этом каждая клика проверяется за

полином на "кликовость $\to \mathcal{P}$, как было доказано в первой задаче и $\in co - \mathcal{NP}$

5

Решение:

Покажем полиномиальность

Получим необходимое из порождающего элемента за $O(\log p)$ умножений , $O(\log p)$ получений остатка по необходимому модулю, поэтому $O(\log^3 p)$(текущая оценка сложности). Всего чисел $k^{\frac{p-1}{p_i}}$ $O(\log p)$, значит проверка выполняется за $O(\log^4 p)$ (p_i простые делители $p-1$). Проверка того, что простыми делителями $p-1$ являются p_i делается за $O(\log^3 p)$. Отсэда получим необходимую рекуренту :

$$T(p) = O(\log p) + \sum_{i=1}^{k} T(p_i)$$

Из свойств неравенств , получим ,что сумму на каждом уровне можно оценить как $O(\log^4 p)$, всего таких уровней $\log p$. А значит, данная задача имеет сложность $O(\log^5 p)$ и является полиномиальной .

$$100091236 = 2^2 \cdot 7 \cdot 3574687 = 2^2 \cdot 7 \cdot 2 \cdot 3 \cdot 233 \cdot 2557 + 1 \cdot 2^2 \cdot 7$$

$$232 = 2^3 \cdot 29 = 2^3 \cdot 2^2 \cdot 7 + 1 \cdot 2^3$$

$$2556 = 2^2 \cdot 3^2 \cdot 71 = 2^2 \cdot 3^2 \cdot 2 \cdot 5 \cdot 7 + 1 \cdot 2^2 \cdot 3^2$$

Порождающие

100091237 − 2
3574687 − 62
2557 − 2
233 − 2
71 − 14
29 − 2
7 − 2

6

Решение:

Предоставляю две ссылки , которые содержат решение данной задачи.

Раз (Th 2) и Два.

Я вроде как в них разобрался, поэтому посчитал нужным не заниматься простым переписыванием