Домашняя работа 6 — Кузнецов

1 Задание 6

1. C40. $\mathrm{NSpace}(n^2) \subsetneq \mathrm{NSpace}(n^3)$. Нестрогое включение очевидно, достаточно показать, что $\mathrm{NSpace}(n^2) \neq \mathrm{NSpace}(n^3)$.

   Я могу показать только $\mathrm{NSpace}(n^2) \neq \mathrm{coNSpace}(n^3)$.

   Занумеруем все машины Тьюринга с лентой подсказки $M_1, M_2, \ldots$, так, что любая машина Тьюринга встречается в этой нумерации бесконечно много раз. Теперь построим язык, который лежит в $\mathrm{coNSpace}(n^3)$, но не лежит в $\mathrm{NSpace}(n^2)$. Для этого построим новую машину Тьюринга следующим образом. На входе 1^i мы запускаем машину Тьюринга M_i с подсказкой для 1^i, если таковая имеется (то есть в роли подсказки для машины, которую мы строим, мы берём подсказку для M_i), даём ей поработать время 2^{2^i}, но если она выходит за память $i^{2.5}$, то останавливаем её и выдаём ответ, что слово 1^i не принадлежит языку. Если же машина не выходит за предоставленную память и выдаёт ответ, то мы выдаём противоположный ответ. Построенная нами машина использует память $O(n^3)$, но подсказка для неё свидетельствует, что слово не лежит в языке, то есть определяемый ею язык лежит в классе $\mathrm{coNSpace}(n^3)$.

2. C44. Существует оракул A, такой, что $\mathrm{NP}^A \neq \mathrm{coNP}^A$.

   Заметим, что язык L лежит в coNP^A, если непринадлежность слова языку L можно коротко (полиномиальным образом) сертифицировать.

   Воспользуемся приведённой подсказкой. Мы уже знаем, что для любого языка B $U_B \in \mathrm{NP}^B$, где $U^B = \{1^i \mid \exists x \in B \colon |x| = i\}$. Теперь построим язык A, такой, что $U^A \notin \mathrm{coNP}^A$.

   Будем последовательно определять принадлежность строк языку A. Для этого занумеруем все пары (M, k), где $k \in \mathbb{N}$, а M — "проверяющая" машины Тьюринга (которая принимают на вход слово x и подсказку для него y и проверяет, подходит ли подсказка) с оракулом A, так, что каждая пара (M, k) встречается в этой нумерации бесконечное число раз.

Итак, вначале язык A пустой.

Опишем i-ый этап. На этом этапе мы уже определили принадлежность конечного числа строк языку A. Возьмём достаточно большое $n > i$, такое, что длины всех этих строк меньше n. Относительно всех строк длины меньше n с неопределённым статусом решаем, что они не лежат в A. Теперь рассматриваем i-ю пару (M, k). Сначала будем считать, что язык A состоит только из тех слов, которые мы к нему уже отнесли. Тогда мы однозначно можем сказать, принадлежит ли 1^n языку, определяемому парой (M, k), то есть языку

$$B = \{x\colon \forall y \ \ |y| \leq |x|^k \Rightarrow M(x, y) = 0\}.$$

Имеем, следовательно, два варианта.

- Слово 1^n лежит в языке B. Тогда запускаем машину Тьюринга M для 1^n поочерёдно со всеми подсказками длины не более n^k на $2^n/10$ шагов и для всех слов, на которых эта машина обращалась к оракулу и статус которых не был определён, решаем, что они не лежат в языке A. Также решаем, что все слова длины n не лежат в языке A. После этой операции слово 1^n не будет лежать в U_A, но будет лежать в языке B, определяемом парой (M, k).
- Слово 1^n не лежит в языке B. Тогда для слова 1^n имеется подсказка-сертификат y длины не более n^k, такая, что

  $$M(1^n, y) = 1.$$

  Тогда запустим машину Тьюринга M на паре $(1^n, y)$ на $2^n/10$ шагов и на всех её обращениях к оракулу A будем говорить "нет" и исключать соответствующее слово из языка A. Поскольку за $2^n/10$ шагов мы запрашивали не про все слова длины n, то есть некоторое слово z длины n, про которое мы (точнее, не мы, а машина M) не спрашивали у оракула, и мы включим это слово в язык A. После этой операции слово 1^n будет лежать в U_A, но не будет лежать в языке B, определяемом парой (M, k).

Почему язык U_A не лежит в coNP^A? Допустим, он лежит в coNP^A. Тогда существует машина Тьюринга M и число k, такие, что

$$U_A = \{x \colon \forall y, |y| \le k|x|^k, M(x,y) = 0\},$$

причём M работает не более $k(|x| + |y| + 1)^k$ времени. Эта пара (M,k) встречается в нашей нумерации бесконечно много раз, и для достаточно больших n имеет место $k(n+n^k+1)^k < 2^n/10$. Поэтому был момент, когда мы рассматривали нашу пару в построении языка A, и использовали как раз такое, достаточно большое n. Тогда из построения видно, что одновременно $1^n \in U_A$ и $1^n \notin U_A$, противоречие.