Задание на вторую неделю.

№10(Доп)

Из Теоремы Кука-Левина SAT это NP-полный язык. $\Rightarrow SAT \leq_p A$ и $A \leq_p SAT$. Пусть соответствующие функции сведения: $f(x)$ и $g(x)$. Построим полиномиальный алгоритм для поиска в языке SAT(т. е. алгоритм, который для данного y находит $s : V(y, s) = 1$, где V - алгоритм верификации для SAT) :
Пусть y содержит переменные: $t_1, \dots, t_k$. Передадим в оракул $f(y)$, полученый ответ определяет(это следует из определения сводимости) принадлежность y языку SAT(выполнимость/невполнимость формулы). Если y не принадлежит языку, то поиск завершен, такого сертификата не существует. Иначе, проверим тем же методом выполнимость формул $y(0, t_2, \dots, t_k)$ и $y(1, t_2, \dots, t_k)$. Как минимум одна из них точно выполнима(для определенности, первая). Тогда, далее рассмотрим $y(0, 1, \dots, t_k)$ и $y(1, 0, \dots, t_k)$, и т. д. пока не присвоим значения всем переменным до t_k. Таким образом, за $O(1) \cdot O(|y|) \cdot$(полиномиальная сложность вычисления $f(x)$) был востановлен набор значений переменных, на котором выполнима данная формул y. Этот набор можно принять за сертификат s: $V(y, s) = 1$, где V проверяет, что формула y выполняется на наборе s. $\Rightarrow$ Полиномиальный алгоритм для поиска в языке SAT построен.
Введем $V_1(x, s)$, алгоритм верификации для языка A, следующим образом:

$$V_1(x, s) = V(g(x), s).$$

Этот алгоритм работает корректно из условия сводимости. Тогда для нахождения для данного x сертификата $s_1 : V_1(x, s_1) = 1$(т. е. выполнения задачи поиска в A) выполним поиск в SAT для $y = g(x)$ и найденный сертификат s и будет искомым. Вычисление $g(x)$ полиномиально(из условия сводимости), поиск в SAT, как показано выше, тоже полиномиален. Значит, алгоритм поиска в A полиномиален.