Домашняя работа № 1

Автор: Минеева Екатерина

Задача 3

Опишем алгоритм решения задачи:

1. При помощи двочного возведения в степень вычисляем q^t. Делается это следующим образом: пусть $t = \overline{t_1 t_2 \dots t_h}$ – двоичная запись числа. Будем в цикле вычислять q^t. Инициализируем $q^t = id$. Далее в цикле $i = h,\ h-1, \dots, 2,\ 1$:

$$q^t = \begin{cases} (q^t)^2, & \text{если } t_i = 0 \\ q \cdot (q^t)^2, & \text{если } t_i = 1 \end{cases}$$

Таким образом, после завершения работы цикла, будет вычислено ровно q^t. Заметим, что на каждой итерации цикла соврешается 1 или 2 перемножения перестановок, то есть $\underline{O}(k)$ действий. Итераций цикла всего t, поэтому общая сложность $\underline{O}(kt)$. После этого осталось только сравнить подстановки q^t и p, на что уходит $\underline{O}(k)$ операций.

Итого, сложность алгоритма $\underline{O}(kt)+\underline{O}(k) = \underline{O}(tk)$. Это полиномиально от размера входа, поскольку t – длина двоичной записи t, а k – размер перестановок q и p.