Домашнее задание № 3.
Алгоритмы и модели вычислений

Матвей Морозов, 678 группа

7 марта 2018 г.

Задача 1

Докажите, что следующие языки лежат в **NP**

Задача 1.1

Язык описаний графов, у которых максимальная клика имеет размер не меньше k

Решение:

1. По определению **NP**
$$L \in \mathbf{NP} \Leftrightarrow L = \{x \in \Sigma^* | \exists y : |y| \leq poly(|x|) \ \ \& \ \ R(x, y) = 1\}$$

2. Пусть граф из $n = |V|$ задан матрицей смежности $n \times n$, то есть длина входа n^2. В качестве сертификата возьмём k вершин $s_1, s_2, \ldots, s_k$, которые составляют клику в исходном графе, то есть максимально полном подграфе.

3. Проверять этот подграф на полноту будем так: $\forall i, j : i \neq j$ будем искать хотя бы один нуль в матрице. Если он будет в этой части матрицы смежности $\Rightarrow$ подграф не полный и размер клики явно меньше k, что означает, что слово не пренадлежит языку L ну или же нам подсунули ложный сертификат.

   Если же в строках и столбцах матрицы смежности нет нулей, значит, что между любыми двумя вершинами существует ребро и это действительно клика размера $k \Rightarrow$ слово принадлежит языку.

4. Проверка $k \times k$ клеток матрицы смежности, где $k \leq n$, осуществляется за $O(n^2)$, значит, языку принадлежит классу **NP**.

Задача 1.2

Задача проверки того, что два графа являются изоморфными.

Решение:

Т.к. графы изоморфны, то существует биекция $V \Rightarrow V'$ и значит в качестве сертификата достаточно предъявить перестановку вершин, чтобы графы (и их матрицы смежности совпали). Графы A и B заданы их матрицами смежности a, b размера n^2, где n- количество вершин. Тогда для проверки мы просто за $O(poly(n^2))$ меняем местами строки и стобцы второй матрицы смежности в соответствии с перестановкой вершин и сравниваем ячейки в них. Если они полностью совпали - победа, после перестановки получился один и тот же граф, значит они были изоморфны.

Задача 2

Покажите, что два определения класса **NP**, которые были даны на семинаре, эквивалентны.

Решение:

1. Запишем два определения класса **NP**
$$\mathbf{NP} = \bigcup_{k=1}^{\infty} NTime(n^k) \quad (1)$$
$$L \in \mathbf{NP} \Leftrightarrow L = \{x \in \Sigma^* | \exists y : |y| \leq poly(|x|) \ \ \& \ \ R(x, y) = 1\} \quad (2)$$

2. **(1) ⇒ (2)**
Пусть L распознаётся недерминированной МТ M, которая работает за полиномиальное время, то есть за $O(n^c)$. В качестве сертификата y возьмём последовательность значений функции перехода, а $R(x, y)$ пусть эмулирует M, используя данные y для выбора одной из ветвей алгоритма.

3. **(2) ⇒ (1)**
Построим недетерминированную МТ таким образом: сначала недетерминированно напишем на ленте наш сертификат $y : |y| \leq poly(|x|)$, затем запустим МТ $R(x, y)$.

4. Честно, решение не мое, его подсмотрел *тут* (стр. 5)

Задача 5

Постройте **NP**-сертификат простоты для числа $p = 3911, g = 13$. Простыми в рекурсивном построении считаются только числа $2, 3, 5$ (они сами являются своими сертификатами).

Решение:

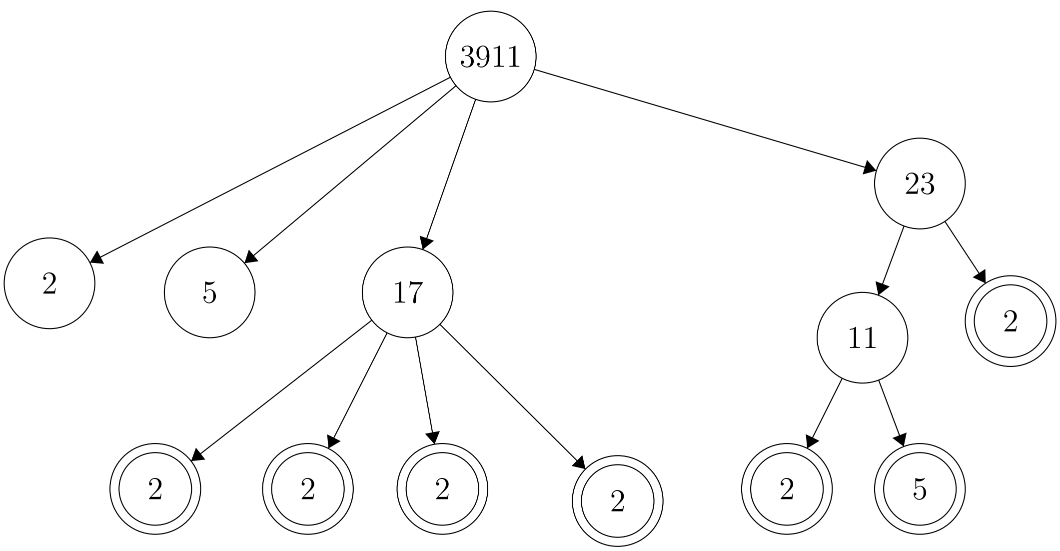
1. $p - 1 = 3910 = 2 \cdot 5 \cdot 17 \cdot 23 = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot p_4^{k_4}$

   Для 3911 порождающий элемент по условию 13.

2. Числа 2 и 5 мы считаем простыми и на них наша рекурсия останавливается.

3. $17 - 1 = 16 = 2^4$
   $23 - 1 = 22 = 2 \cdot 11$

4. $11 - 1 = 10 = 2 \cdot 5$
   Сертификат:



$$13^{3910/2} \mod 3911 \neq 1$$
$$13^{3910/5} \mod 3911 \neq 1$$
$$13^{3910/17} \mod 3911 \neq 1$$
$$13^{3910/23} \mod 3911 \neq 1$$

Для 17 выберем порождающий элемент 5.

$$5^{16/2} \mod 17 \neq 1$$

Для 23 выберем порождающий элемент 5.

$$5^{22/11} \mod 23 \neq 1$$

$$5^{22/2} \mod 23 \neq 1$$

Для 11 выберем порождающий элемент 2.

$$2^{10/2} \mod 11 \neq 1$$

$$2^{10/5} \mod 11 \neq 1$$

Вычисления : Вольфрам

Задача 4

Покажите, что классу **NP** принадлежит язык несовместных систем линейных уравнений с целыми коэффициентами от 2018 неизвестных, и постройте соответствующий сертификат y и проверяющий алгоритм $R(x, y)$.

Решение:

По теореме Фредгольма $Ax = b-$ совместна $\Leftrightarrow$ каждое решение сопряжённой однородной системы $c^T A = 0$ удовлетворяло уравнению $c^T b = 0$.

Значит мы можем в качестве сертификата предъявлять такое решение c_0 сопряжённой однородной системы, что $c_0^T b \neq 0$. Тогда проверка осуществляется подстановкой в расширенную матрицу системы $||A|B||$ решение c_0. И далее операциями над матрицей убеждаемся в нарушении теоремы Фредгольма.

Находить c_0 можно решая методом Гаусса сопряжённую однородную систему. Причём это происходит за полином т.к. каждый элемент c_0 - полином от элементов исходной матрицы, степени не выше 2018 (из определения детерминанта). Размеры миноров ограничены 2018 (что есть константа).

Значит мы предъявили сертификат и алгоритм проверки, за полиномиальное время. Это и доказывает принадлежность языка **NP**.

Задача 3

Покажите, что класс **NP** замкнут относительно $*$-операции Клини. Укажите, как построить для результирующего языка L^*, $L \in \mathrm{NP}$ соответсвующий сертификат y и проверяющий алгоритм $R(x, y)$.

Решение:

В качестве сертификата y достаточно взять разбиение слова из L^* на подслова из L, и сертификаты слов из L, конкатенация которых образует исходное слово из L^*.

В качестве алгоритма $R(x, y)$ мы будем запускать алгоритм $V(x, y)$ (который проверяет сертфикаты для L) на словах, которые образуют исходное слово из L^*, и их сертификатах.