Домашнее задание по АМВ

771 группа, Христолюбов Максим

5 марта 2022 г.

1 Задача 1

1.1 (i)

Если использовать функцию $f(x) = x$, x — слово языка, то $\forall x \in A \to f(x) \in A$, значит по определению полиномиальной сходимости рефлексивность выполняется.

Если $A \leq_p B$ и $B \leq_p C$, тогда $\exists$ соответствующие $f(x)$ и $g(x)$, переводящие слово $x \in A$ в $f(x) \in B$, а потом в $g(f(x)) \in C$ за полиномиальное время. Т. к. $\phi(x) = g(f(x))$ — полином, как композиция полиномов, то $A \leq_p C$.

1.2 (ii)

Если $B \in \mathcal{P}$ и $A \leq_p B$, тогда можно определить принадлежность x языку A так: вычислить за полиномиальное время $f(x) \in B$ и определить за полиномиальное время принадлежность к B ($M(f(x))$ работает за полином), а т. к. из определения сходимость $x \in A \Leftrightarrow f(x) \in B$, то и определить принадлежность x языку A за полиномиальное время. Значит, $A \in \mathcal{P}$

1.3 (iii)

Если $B \in \mathcal{NP}$ и $A \leq_p B$, тогда можно определить принадлежность x языку A так: вычислить за полиномиальное время $f(x) \in B$ и определить за полиномиальное время (на недерминированной машине Тьюринга) принадлежность к B ($M(f(x))$ работает за полином на НМТ), а т. к. из определения сходимость $x \in A \Leftrightarrow f(x) \in B$, то и определить принадлежность x языку A за полиномиальное на НМТ время. Значит, $A \in \mathcal{NP}$

2 Задача 2

2.1 (i)

Можно проверять всевозможные тройки из всех n вершин графа, которых всего не более n^3, проверка происходит за полиномиальное время, так как можно быстро найти соответствующую клетку в матрице смежности. Проверку на двудольность можно проверить перебирая вершины и распределяя их в 2 группы, и посмотреть получить ли их распределить в 2 группы, в каждой из которых вершины не соединены. Значит, определить принадлежность графа языку за полиномиальное от кол-ва вершин время, а длина слова — размер матрицы смежности — полином от n. То есть язык лежит в $\mathcal{P}$.

2.2 (ii)

Несвязность и наличие циклов проверяется обходом в глубину, который работает полиномиально от кол-ва вершин, а значит полиномиально и от длины записи таблицы смежности, поэтому язык лежит в $\mathcal{P}$.

2.3 (iii)

Все такие подматрицы перебираются за полиномиальное от n время и их проверка на выполнение условие тоже займет полином от n времени, значит, принадлежность языку можно определить за полином от длины записи слова (матрицы), и язык лежит в $\mathcal{P}$.

3 Задача 3

3.1 (i)

При занулении первого столбца методом Гаусса, коэффициенты a_{1i}^0 в первой строчке умножаются на a_{j1}^0 и делятся a_{11}^0 получается $\frac{a_{j1}^0 a_{1i}^0}{a_{11}^0}$. После этого одна строка вычитается из другой, вычисляется $a_{ji}^1 = a_{ji}^0 - \frac{a_{j1}^0 a_{1i}^0}{a_{11}^0} = \frac{a_{ji}^0 a_{11}^0 - a_{j1}^0 a_{1i}^0}{a_{11}^0}$, в худшем случае числитель результата — порядка $2h^2$, знаменатель — h у всех чисел в матрице, кроме первой строчки.

На следующем шаге коэффициенты a_{2i} в первой строчке умножаются на a_{j2} и делятся a_{22} получается $\frac{a_{j2}^1 a_{2i}^1}{a_{22}^1} = \frac{(a_{j2}^0 a_{11}^0 - a_{j1}^0 a_{12}^0)(a_{2i}^0 a_{11}^0 - a_{21}^0 a_{1i}^0) a_{11}^0}{a_{11}^0 a_{11}^0 (a_{22}^0 a_{11}^0 - a_{21}^0 a_{12}^0)}$. После этого одна строка вычитается из другой, вычисляется $a_{ji}^2 = a_{ji}^1 - \frac{a_{j1}^1 a_{1i}^1}{a_{22}^1} =$

$\frac{a^1_{ji}a^1_{22}-a^1_{j1}a^1_{1i}}{a^1_{22}}$, числитель — $8h^4 \cdot h = 8h^5$, знаменатель — $2h^2 \cdot h^2 = 2h^4$ у всех чисел в матрице, кроме первой строчки. Вообще, если на предыдущем шаге у чисел в матрице числитель был пропорционален bh^k, а знаменатель ch^p, то на следующем шаге числитель — $2b^2h^{2k} \cdot ch^p$, а знаменатель $bh^k{\cdot}c^2h^{2p}$. Что означает, что на каждом шаге в худшем случае числитель и знаменатель увеличиваются как минимум в квадрат. После $\min(n,m)-1$ итераций, которые нужны для диагонализации матрицы размеры числителя и знаменателя будут не менее $h^{2^{(\min(m,n)-1)}}$ и $h^{2^{(\min(m,n)-1)-1}}$ соответственно, а длинны их записи $\log h^{2^{(\min(m,n)-1)}}$ и $\log h^{2^{(\min(m,n)-1)-1}}$, что $\Theta(2^{\min(m,n)})$ и не является полиномиальной оценкой.

3.2 (ii)

Так как при вычислении методом Гаусса $a^{(k)}_{ij} = \frac{det(D^{(k)}_{ij})}{det(D^{(k)})}$, то из формулы детерминанта коэффициенты матрицы при преобразовании методом Гаусса будут $O(h^k k)$, где $k = \min(m,n)$. Их умножение за $O(\log^2 h^k) = O(k^2 \log^2 h)$, а кроме того их нужно сокращать алгоритмом Евклида за $\Theta(k \log h)$, то есть $O(k^3 \log^3 h)$. На всех k шагах диагонализация произойдут за $O(k^3 \log^3 h \cdot n \cdot k)$ действий. Дальнейшее вычисление корней произойдет за меньшее кол-во умножений этих чисел Значит сложность $O(n(\min(m,n))^4 \log^3 h)$.

4 Задача 4

Если $L \in \mathcal{P}$, то существует алгоритм $A(x)$ определяющий принадлежность языку за полиномиальное время $t(|x|)$. Построим алгоритм $A^*(x)$ для проверки принадлежности языку L^*. Заведем массив индексов концов слов из L, изначально $e = \{0\}$. Будем перебирать всевозможные подслова $x_1 \dots x_i$ и проверять алгоритмом A их принадлежность L, а так же заносить их индексы в e. На следующей итерации переберем всевозможные слова с началом в $e_k + 1$ и концом во всевозможных позициях i. Итерации будут продолжаться пока в e не перестанут появляться новые позиции. Таким образом, в e будут концы из всевозможных цепочек слов из L, конкатенация которых принадлежит префиксу x. Поэтому $x \in L^*$ тогда и только тогда, когда в e будет $|x|$. Всего проверок на принадлежность L будет не больше, чем подслов в x, не больше чем $|x|^2$, значит проверка займет не больше, чем $|x|^2 t(|x|)$ — полиномиальное время.

С замыканием $L^*, L \in \mathcal{NP}$ можно сделать то же самое. В качестве сертификата можно взять $s^* = \{s(x_i \dots x_j) | x_i \dots x_j$ — подслово x,

s – сертификат для алгоритма A проверки принадлежности к $L\}$ и использовать их для определения принадлежности подслов языку L, поэтому с этим сертификатом алгоритм будет работать $|x|^2 t(|x|)$.

5 Задача 5

Для проверки можно воспользоваться модифицированным методом Гаусса и диагонализировать расширенную матрицу системы. Если будет получена строчка, в которой все коэффициенты при $x_i = 0$, а $b_j \neq 0$, тогда эта система несовместна. Как показано в пункте (ii) 3 номера размер дробей будет полиномиальным от размера системы, значит все коэффициенты, на которые умножаются строки матрицы, чья линейная комбинация в итоге обращаются в ноль, имеют размер полиномиальный от размеров матрицы. Значит, в качестве сертификата y можно взять эти коэффициенты, с которыми нужно взять строки матрицы, чтобы получить нулевую строку, причем их длина y будет полиномиальной от размера матрицы. Проверка на то что эта линейная комбинация действительно дает нулевую строку, а $b_j \neq 0$, произойдет за полиномиальное время, значит язык в классе $\mathcal{NP}$.

6 Задача 6

Если вместе с парой (N,M) на вход машины Тьюринга предоставить сертификат d, которой является делителем N и $1 < d < M$, то МТ нужно будет только проверить, что d удовлетворяет условиям, а так как алгоритм Евклида и сравнение работает за полиномиальное время, то проверка пройдет за полиномиальное время, значит $L_{factor} \in \mathcal{NP}$.

С другой стороны если в качестве сертификата предоставить все разложение N на множители $p_1^{\alpha_1} \dots p_k^{\alpha_k}$. (в таком случае длина сертификата будет полиномиальна от длины N, так как всего делителей у числа не более N, а длины чисел не превосходят $\log N$). Проверив делением, что они делители N, а так же их произведение дает N (для того, чтобы убедиться, что больше делителей нет), а так же сравнив эти делители с M можно будет проверить существует ли такой делитель d, удовлетворяющий условию, а значит, за полиномиальное время определить принадлежность дополнению L_{factor}, то есть $L_{factor} \in co-\mathcal{NP}$.

7 Задача 7

ГП можно полиномиально свести к ГЦ с помощью $f(x) = x$ — чтобы проверить принадлежность x к ГП можно проверив $x \in$ ГЦ. Если это так,то $x \in$ ГП. Действительно, если в графе есть гамильтонов цикл, то выкинув из гамильтонова цикла одно ребро можно получить гамильтонов путь, значит ГП $\subseteq$ ГЦ.

Если есть МТ, распознающая ГП за полиномиальное время построим алгоритм, проверяющий принадлежность к ГЦ за полиномиальное время. Если добавить к графу 2 ребра соединяющие вершины i и новую вершину, а так же вершину j и другую новую вершину, то МТ, распознающая ГП, даст положительный ответ тога и только тогда, когда i и j — вершина, которые являются началом и концом для некоторого гамильтонова пути в изначальном графе. Перебрав все i,j, принадлежащие графу, так можно составить список всех пар вершин, которые являются началом и концом некоторых гамильтоновых путей. Если какая-то пара соединена ребром, то в изначальном графе есть гамильтонов цикл, совпадающий с соответствующим гамильтоновым путем плюс это ребро. Реализовав этот алгоритм на МТ получиться полиномиально работающий МТ, распознающую ГЦ, построенный на основе МТ, полиномиально распознающей ГП.

8 Задача 8

Пусть длина входа |РВ| + $|w|$.

Построим по РВ НКА, воспользовавшись стандартными реализациями |,$*$ и конкатенации — на месте конкатенации переход к следующему блоку по эпсилон переходу, на месте объединения эпсилон переходы к блокам, входящим в объединение, а на месте замыкании Клини эпсилон переход в начало, иначе говоря алгоритм построения НКА по РВ из курса ТРЯП. Время преобразования, как и кол-во вершин в НКА будет полиномиально зависеть от длины РВ. Для проверки $w \notin L$ подадим на вход НКА w. Из-за наличия эпсилон переходов будет образовываться дерево возможных путей. Будем обходить это дерево в ширину, для этого придется хранить массив вершин-состояний НКА, в которых может находится НКА на данный момент. Размер этого массива не превышает размера всего графа $|V|$, то есть полиномиален от длины РВ. Перебирать этот массив нужно будет не более $|w|$, значит всего не более $|V||w|$ переходов, что не более $(|V| + |w|)^2$. Значит, алгоритм полиномиален.

*При решении советовался с Александром Жоговым.