Домашнее задание №3

Дедлайн: 3 марта 2019 г., 23:00

Основные задачи

1. (1 балл) Докажите , что следующие язык двудольных графов, содержащих не менее 2019 треугольников (трех попарно смежных вершин) принадлежит классу $\mathcal{P}$. Можно считать, что графы кодируются соответствующими матрицами смежности.

2. (1 + 2 балла) **Полиномиальность метода Гаусса.** Рассмотрим систему линейных уравнений $Ax = b$ с целыми коэффициентами, имеющую m уравнений и n неизвестных, причем максимальный модуль целых коэффициентов A, b равен h.

   (i) Оцените сверху числители и знаменатели чисел, которые могут возникнуть при непосредственном применении алгоритма Гаусса

   Из решения этой задачи следует, что при прямом использовании алгоритма исключения Гаусса промежуточные результаты могут в принципе расти дважды экспоненциально, и потому, в частности, метод исключений не является полиномиальным по входу в битовой арифметике. Но оказывается, что метод Гаусса можно модифицировать так, что получится полиномиальный алгоритм. Модификация заключается в эмуляции *рациональной арифметики*. Для этого каждый (рациональный) коэффициент $\frac{p}{q}$ представляется парой (p', q') взаимно простых чисел $\frac{p}{q} = \frac{p'}{q'}$. Все арифметические действия над коэффициентами моделируются действиями над соответствующими парами, а в конце каждой операции, используя алгоритм Евклида, мы принудительно добиваемся взаимной простоты числителя и знаменателя. Скажем, эмуляция сложения коэффициентов, заданных парами $(7, 10)$ и $(5, 6)$, состоит в вычислении пары $(7 \cdot 6 + 5 \cdot 10 = 92,\ 6 \cdot 10 = 50)$, определении $\text{НОД}(92, 60) = 2$ и записи ответа $(23, 15)$.

   Полиномиальность указанной модификации вытекает из следующего утверждения: **все элементы матриц, возникающих в методе Гаусса, являются отношением каких-то миноров исходной расширенной матрицы системы.**

   Докажем это. Без ограничения общности будем считать, что ведущие элементы расположены на главной диагонали, и обозначим $(a_{ij}^{(k)})$ матрицу, полученную после k-го исключения. Также обозначим $d_1, \ldots, d_n$ элементы главной диагонали результирующей верхнетреугольной матрицы, так что $d_i = a_{ii}^{(n)}$. Пусть $D^{(k)}$— подматрица, образованная первыми k столбцами и первыми k строками *исходной матрицы системы*, а $D_{ij}^{(k)}$, $k + 1 \leq i, j \leq n$— подматрица, образованная первыми k столбцами и столбцом i и первыми k строками и строкой j, матрицы, полученной после k-го исключения. Пусть $d_{ij}^{(k)} = \det(D_{ij}^{(k)})$. По определению, $det(D^{(k)}) = d_{kk}^{(k-1)}$.

   Ключом является следующая формула: $a_{ij}^{(k)} = \frac{d_{ij}^{(k)}}{det(D^{(k)})}$, поскольку, в соответствии с процедурой исключений $d_{ij}^{(k)} = d_1 \ldots d_k a_{ij}^{(k)}$ и $det(D^{(k)}) = d_1 \ldots d_k$. Таким образом, можно все время работать с дробями, числители и знаменатели которых *являются минорами* **исходной** *матрицы*, так что длина записи остается полиномиальной[1], а все вычисления по методу Гаусса (включая, конечно, вычисления НОД получаемых дробей) будут также полиномиальными.

   (ii) Оцените трудоемкость модифицированного метода Гаусса в виде формулы от $m, n \log h$. Трудоемкость алгоритма Евклида считайте линейной по длине входа. Покажите, что модифицированный алгоритм будет полиномиальным по входу.

3. (2 балла) Покажите, что класс $\mathcal{P}$ замкнут относительно $*$-операции Клини ($L^* = \varepsilon \cup L \cup L^2 \cup \ldots$).

4. (1 + 1 балл) Докажите, что следующие задачи лежат в $\mathcal{NP}$:

   (i) язык описаний графов, у которых максимальная клика[2] имеет размер не меньше k;

   (ii) задача проверки того, что два графа являются изоморфными.

   Замечание. По задаче нужно сформулировать определение языка, а затем показать, что этот язык лежит в $\mathcal{NP}$.

5. (1 балл) Покажите, что два определения класса $\mathcal{NP}$, которые были даны на семинаре, эквивалентны.

[1] Контрольные вопросы: почему? Можете ли вы привести оценки?
[2] Клика — полный подграф.

6. (1 балл) Покажите, что класс $\mathcal{NP}$ замкнут относительно $*$-операции Клини. Укажите, как построить для результирующего языка L^*, $L \in \mathcal{NP}$ соответствующий сертификат y и проверяющий алгоритм $R(x, y)$.
Приведем теперь пример языка, принадлежность которого классу $\mathcal{NP}$ совершенно не очевидна.

   Сначала вспомним кое-какие элементарные сведения о поле вычетов $\pmod p$ Просто понять, что в $\mathcal{NP}$ лежит язык составных чисел $A = \{1, 4, 6, 8, 9, 10, \ldots\}$ (сертификатом служат предъявляемые сомножители). Но оказывается, что в $\mathcal{NP}$ лежит и язык $B = \mathbb{N} \setminus A = \{2, 3, 5, 7, 11, \ldots\}$ простых чисел[3]. Полиномиальный сертификат устроен хитро. Как мы знаем, $p \in B \Leftrightarrow \exists g : \{g^i \pmod p, i = 1, 2, \ldots, p-1\} = \{1, 2, \ldots, p-1\}$ (написано равенство множеств). Поскольку длина записи числа p составляет $\log p$, то длина сертификата должна быть $poly(\log p)$. И если быстро возводить числа $\pmod p$ в степень мы еще умеем[4], то все равно массив $\{g^i \pmod p\}$ слишком длинный. Но, как мы помним, вычет g с нужными свойствами существует тогда и только тогда, когда выполнено $g^{p-1} = 1 \pmod p$, $g^{\frac{p-1}{p_1}} \neq 1 \pmod p, \ldots, g^{\frac{p-1}{p_k}} \neq 1 \pmod p$, где $p_1, \ldots, p_k$ — это все простые делители числа $p - 1 = p_1^{l_1} \ldots p_k^{l_k}$. Число проверок действительно уменьшилось и стало полиномиальным (их заведомо не больше $\log p$), но, кажется, что мы ничего не выиграли: нам ведь нужно решить **ту же задачу построения сертификата простоты** для всех p_j, $j = 1, 2, \ldots, k$. Хитрость заключается в том, что нужно применить ту же идею рекурсивно, поскольку длина сертификатов для всех p_i сильно уменьшилась! Фактически сертификатом будет дерево с нужными пометками в вершинах, и нам нужно показать, что суммарная длина всех участвующих в описании дерева компонентов останется полиномиальной по $\log p$.

7. (2 балла) Постройте $\mathcal{NP}$-сертификат простоты для числа $p = 3911$, $g = 13$. Простыми в рекурсивном построении считаются только числа $2, 3, 5$ (они сами являются своими сертификатами).

8. (1 балл) Покажите, что язык *разложения на множители (факторизации)* $L_{factor} = \{(N, M) \in \mathbb{Z}^2 \mid 1 < M < N$ и N имеет делитель d, $1 < d \leq M\}$ принадлежит $\mathcal{NP} \cap$ co-$\mathcal{NP}$.

[3] В 2002 году появилась сенсационная работа, показывающая, что $B \in \mathcal{P}$. Если вы будете ссылаться на ее результаты, то **обязаны** привести доказательство.

[4] Вспомните индийский алгоритм возведения в степень