Рябых Владислав, Б05-905

Алгоритмы и модели вычислений.
Домашнее задание № 4

Задача 1. Постройте NP-сертификат простоты числа $p = 3911$, $g = 13$. Простыми в рекурсивном построении считаются только числа 2, 3, 5.

Решение. g — первообразный корень, является NP-сертификатом простоты числа $p = 3911$.
$g^{p-1} = 13^{3910} \underset{3911}{\equiv} 1$ — по малой теореме Ферма.
Решающей структурой будет дерево, в корне которого находится само число p со своим сертификатом g, а в его детях — делители числа $p-1$ и их сертификаты соответственно (и так далее по рекурсии).
$p - 1 = 3910 = 23 \cdot 17 \cdot 5 \cdot 2$, раскладываем дальше:

- 2, 5 считаем простыми по условию задачи.
- 17 имеет своим сертификатом 3, $17 - 1 = 16 = 2^4 \Rightarrow 17$ — простое.
- 23 имеет своим сертификатом 5, $23 - 1 = 22 = 11 \cdot 2$, таким образом либо 23 и 11 просты одновременно, либо одновременно являются составными.
  - 11 имеет своим сертификатом 2: $11 - 1 = 10 = 5 \cdot 2 \Rightarrow 11$ — простое.

Таким образом, $p = 3911$ является простым.

Задача 2. Найдите Θ-асимптотику суммы $\sum\limits_{k=1}^{n} \sqrt{k}$, оценив её с помощью интеграла $\int_1^n \sqrt{x}dx$ сверху и снизу. Выведите аналогичную формулу для асимптотики $\sum\limits_{k=1}^{n} k^\alpha$ для $\alpha > 0$.

Решение.

$$\int_0^n \sqrt{x}dx \leqslant \sum_{k=1}^{n} \int_{k-1}^{k} \sqrt{x}dx \leqslant \sum_{k=1}^{n} \int_{k-1}^{k} \sqrt{k}dx = \sum_{k=1}^{n} \sqrt{k} = \sum_{k=1}^{n} \int_{k}^{k+1} \sqrt{k}dx \leqslant \sum_{k=1}^{n} \int_{k}^{k+1} \sqrt{x}dx \leqslant \int_1^{n+1} \sqrt{x}dx$$

Таким образом получаем, что $\int_0^n \sqrt{x}dx \leqslant \sum\limits_{k=1}^{n} \sqrt{k} \leqslant \int_1^{n+1} \sqrt{x}dx$

То есть $\frac{2}{3} \cdot n^{\frac{3}{2}} \leqslant \sum\limits_{k=1}^{n} \sqrt{k} \leqslant \frac{2}{3} \cdot ((n+1)^{\frac{3}{2}} - 1)$, таким образом $\sum\limits_{k=1}^{n} \sqrt{k} = \Theta(n^{\frac{3}{2}})$

Так как $\sum\limits_{k=1}^{n} \sqrt{k} = \sum\limits_{k=1}^{n} k^{\frac{1}{2}}$, проведём теперь аналогичные действия для произвольного $\alpha > 0$:

$$\int_0^n x^\alpha dx \leqslant \sum_{k=1}^{n} \int_{k-1}^{k} x^\alpha dx \leqslant \sum_{k=1}^{n} \int_{k-1}^{k} k^\alpha dx = \sum_{k=1}^{n} k^\alpha = \sum_{k=1}^{n} \int_{k}^{k+1} k^\alpha dx \leqslant \sum_{k=1}^{n} \int_{k}^{k+1} x^\alpha dx \leqslant \int_1^{n+1} x^\alpha dx$$

Таким образом получаем, что $\int_0^n x^\alpha dx \leqslant \sum\limits_{k=1}^{n} k^\alpha \leqslant \int_1^{n+1} x^\alpha dx$

То есть $\dfrac{1}{\alpha+1}\cdot n^{\alpha+1} \leqslant \sum\limits_{k=1}^{n}\sqrt{k} \leqslant \dfrac{1}{\alpha+1}\cdot((n+1)^{\alpha+1}-1)$, таким образом $\sum\limits_{k=1}^{n} k^{\alpha} = \Theta(n^{\alpha+1})$

Задача *3.* а) Верно ли что язык 5-ДНФ-Л является полиномиально полным в **co**–$\mathcal{NP}$?
Язык 5-ДНФ-Л состоит из всех формул в дизъюнктивной нормальной форме, принимающих истинное значение при каких-то значениях переменных, в каждый конъюнкт которых входит не более пяти переменных.
б) Верно ли что язык 5-КНФ-Л является полиномиально полным в $\mathcal{NP}$?
Язык 5-КНФ-Л состоит из всех формул в конъюнктивной нормальной форме, принимающих ложное значение при каких-то значениях переменных, в каждый дизъюнкт которых входит не более пяти переменных.
Можно использовать гипотезы $\mathcal{P} \neq \mathcal{NP}$ *и* $\mathcal{NP} \neq$ ***co***–$\mathcal{NP}$.

в) Расставьте и обоснуйте $\mathcal{P}$, $\mathcal{NP}-complete$, $co-\mathcal{NP}-complete$:

	Выполнимость	Тавтологичность
КНФ		
ДНФ		

Под выполнимостью понимается задача проверки наличия набора значений переменных, на котором формула равна 1. Под тавтологичностью понимается задача проверки свойства формулы принимать значение 1 на всех наборах.

Решение. 1. Пусть $\overline{A}$ = 5-ДНФ-Л. Допустим, что $\overline{A}$ — полиномиально полный в **co**–$\mathcal{NP}$, то есть $\forall L \in \mathcal{NP} \hookrightarrow \overline{L} \leqslant_p \overline{A}$

Рассмотрим язык $\overline{\overline{A}} = A$. $A \in \mathcal{NP}$, так как $\overline{A} \in$ **co**–$\mathcal{NP}$ по предположению. A — язык, содержащий либо не ДНФ, либо те ДНФ, в которых есть конъюнкт с не менее 6 литералами, либо невыполнимые 5-ДНФ. Все эти 3 кластера мы легко можем проверить за полиномиальное время: первые два очевидно, а для проверки невыполнимости будем пользоваться следующим. ДНФ невыполнима $\Leftrightarrow$ каждый из конъюнктов тождественно ложен, то есть в каждом конъюнкте присутствует некоторый литерал со своим отрицанием — мы можем легко это проверить для каждого из конъюнктов, которых в свою очередь $\leqslant n$, где n — длина формулы, то есть по сути длина входа. Таким образом выходит, что мы за полиномиальное время детерминированно проверяем принадлежность входа к A, то есть таким образом $A \in \mathcal{P}$. А это означает, что $\overline{A} \in \mathcal{P}$, а следовательно, так как $\forall L \in \mathcal{NP} \hookrightarrow \overline{L} \leqslant_p \overline{A}$, то получаем, что $\forall L \in \mathcal{NP} \hookrightarrow \overline{L} \in \mathcal{P} \hookrightarrow \overline{\overline{L}} = L \in \mathcal{P} \Rightarrow \mathcal{P} = \mathcal{NP}$, что неверно по гипотезе. Таким образом мы пришли к противоречию, так что язык $\overline{A}$ = 5-ДНФ-Л не является полиномиально полным в **co**–$\mathcal{NP}$.

2. Пусть A = 5-КНФ-Л. Формула в КНФ принимает ложное значение $\Leftrightarrow$ существует дизъюнкт, обращающийся в 0, то есть все литералы в дизъюнкте должны обратиться в 0. Соответственно, мы можем подобрать подходящий набор переменных тогда и только тогда, когда существует дизъюнкт, в котором не находятся одновременно литерал со

своим отрицанием. Аналогично прошлому пункту, мы можем легко проверить наличие такого дизъюнкта, причём, так как всего их $\leqslant n$, где n — длина формулы, то есть по сути длина входа, выходит, что мы за полиномиальное время детерминированно проверяем принадлежность входа к A, то есть таким образом $A \in \mathcal{P}$. Поэтому A не может быть $\mathcal{NP}$-полным, так как иначе каждый язык из $\mathcal{NP}$ сводился бы к $A \in P$, то есть язык сам лежал бы в $\mathcal{P}$, и тогда мы бы получили $\mathcal{P} = \mathcal{NP}$, что неверно по гипотезе.

3. (a) КНФ тавтологична тогда и только тогда, когда каждый из её дизъюнктов обращается в 1 на любом наборе переменных, то есть на любом наборе переменных невозможно ни один из дизъюнктов обратить в 0. Это же выполняется тогда и только тогда, когда каждый из дизъюнктов содержит некоторый литерал со своим отрицанием. Соответственно, проверить это мы можем за $O(m^2) = O(n^2)$, где $m \leqslant n$ — длина наибольшего из дизъюнктов, n — длина всей формулы. Всего таких дизъюнктов $\leqslant n$, поэтому итоговая сложность алгоритма $O(n^3)$ — полиномиальна, так что проверка тавтологичности КНФ лежит в $\mathcal{P}$.

   (b) Аналогично с выполнимостью ДНФ, только теперь нам надо проверять, что существует конъюнкт, в котором не содержится некоторого литерала с его отрицанием. Также это можно выполнить за $O(n^3)$, так что проверка выполнимости ДНФ лежит в $\mathcal{P}$.

   (c) Язык выполнимых КНФ есть SAT — фундаментальный пример $\mathcal{NP}_c$ языка, полнота которого в $\mathcal{NP}$ следует из теоремы Кука-Левина.

   (d) ДНФ тавтологична $\Leftrightarrow$ её отрицание является невыполнимой КНФ. Задача о выполнимости КНФ является $\mathcal{NP}$-полной, поэтому задача о её невыполнимости является **co**–$\mathcal{NP}$-полной.

Таким образом, табличка примет следующий вид:

	Выполнимость	Тавтологичность
КНФ	$\mathcal{NP}_c$	$\mathcal{P}$
ДНФ	$\mathcal{P}$	**co**–$\mathcal{NP}_c$