



# Алгоритмы и структуры данных

Лекция 7. P versus NP.

(с) Глухих Михаил Игоревич, [glukhikh@mail.ru](mailto:glukhikh@mail.ru)

# Класс P

- Задачи, для решения которых существует алгоритм с полиномиальным временем работы
- Трудоёмкость  $O(N^k)$
- Считаются имеющими «быстрое» решение

# Класс P

- Задачи, для решения которых существует алгоритм с полиномиальным временем работы
- Трудоёмкость  $O(N^k)$
- Считаются имеющими «быстрое» решение
  
- Формально – на детерминированной машине Тьюринга (что это?)

# Класс NP

- Задачи, для ПРОВЕРКИ решения которых существует алгоритм с полиномиальным временем работы
- Трудоёмкость ПРОВЕРКИ решения  $O(N^P)$

# Класс NP

- Задачи, для ПРОВЕРКИ решения которых существует алгоритм с полиномиальным временем работы
- Трудоёмкость ПРОВЕРКИ решения  $O(N^P)$
- Класс NP **включает в себя** класс P
- Т.е. любая задача из класса P входит в класс NP

# NP-полные задачи (класс NPC)

- ▶ ПОДКЛАСС класса NP (то есть, не то же самое)
- ▶ Задача из класса NP является NP-полной, если...

## NP-полные задачи (класс NPC)

- ▶ ПОДКЛАСС класса NP (то есть, не то же самое)
- ▶ Задача из класса NP является NP-полной, если...
- ▶ ...к ней можно свести ЛЮБУЮ ДРУГУЮ NP-полную задачу за полиномиальное время –  $O(N^k)$

# NP-полные задачи (класс NPC)

- ▶ ПОДКЛАСС класса NP (то есть, не то же самое)
- ▶ Задача из класса NP является NP-полной, если...
- ▶ ...к ней можно свести ЛЮБУЮ ДРУГУЮ NP-полную задачу за полиномиальное время –  $O(N^k)$
- ▶ Как правило, применяется к задачам с ответом Да / Нет (но обобщается и на другие задачи)



# NP-полные задачи (класс NPC)

- ▶ ПОДКЛАСС класса NP (то есть, не то же самое)
- ▶ Задача из класса NP является NP-полной, если...
- ▶ ...к ней можно свести ЛЮБУЮ ДРУГУЮ NP-полную задачу за полиномиальное время –  $O(N^k)$
- ▶ Как правило, применяется к задачам с ответом Да / Нет (но обобщается и на другие задачи)
- ▶ NB: для работы такого определения нужна хотя бы одна «базовая» NP-полная задача

# Базовая NP-полная задача

- ▶ SAT CNF (выполнимость булевых формул)

# Базовая NP-полная задача

- ▶ SAT CNF (выполнимость булевых формул)
- ▶ Верно ли, что существуют булевы значения  $x_1, \dots, x_N$ , такие, что заданная  $f(x_1, \dots, x_N) = 1$ ?

# Базовая NP-полная задача

- ▶ SAT CNF (выполнимость булевых формул)
- ▶ Простейшая формулировка: есть логическая схема из элементов И, ИЛИ, НЕ,  $m$  входов, 1 выход

# Базовая NP-полная задача

- SAT CNF (выполнимость булевых формул)
- Простейшая формулировка: есть логическая схема из элементов И, ИЛИ, НЕ,  $m$  входов, 1 выход
- Существуют ли такие значения входов, при которых на выходе – 1?

## Базовая NP-полная задача

- ▶ SAT CNF (выполнимость булевых формул)
- ▶ Дана  $CNF(X) = T_1(X) * T_2(X) * \dots * T_n(X)$ , где  $X$  – вектор из  $m$  булевых переменных, а  $T_i(X)$  – термы-дизъюнкции
- ▶ Вопрос формулируется точно так же

## Варианты SAT: ДНФ

- $F(x_1, \dots, x_5) = x_1 * !x_2 * x_3 + x_2 * x_3 * !x_4 + !x_3 * x_4 * x_5$
- $x_1, \dots, x_5: F = 1?$

## Варианты SAT: ДНФ

- $F(x_1, \dots, x_5) = x_1 * !x_2 * x_3 + x_2 * x_3 * !x_4 + !x_3 * x_4 * x_5$
- $x_1, \dots, x_5: F = 1?$
- Решение очевидно существует:  $O(1)$



## Варианты SAT: 2-КНФ

- ▶  $F(x_1, \dots, x_5) = (x_1 + !x_2) * (x_3 + x_5) * (x_4 + !x_1) * (x_2 + !x_5)$
- ▶  $x_1, \dots, x_5: F = 1?$

## Варианты SAT: 2-КНФ

- ▶  $F(x_1, \dots, x_5) = (x_1 + !x_2) * (x_3 + x_5) * (x_4 + !x_1) * (x_2 + !x_5)$
- ▶  $x_1, \dots, x_5: F = 1?$
- ▶ Решается за линейное время
  - ▶  $x_1 = 0 \Rightarrow x_2 = 0, \quad x_2 = 1 \Rightarrow x_1 = 1$
  - ▶  $x_3 = 0 \Rightarrow x_5 = 1, \quad x_5 = 0 \Rightarrow x_3 = 1$
  - ▶  $x_4 = 0 \Rightarrow x_1 = 0, \quad x_1 = 1 \Rightarrow x_4 = 1$
  - ▶  $x_2 = 0 \Rightarrow x_5 = 0, \quad x_5 = 1 \Rightarrow x_2 = 1$
- ▶  $x_1 = 0 \Rightarrow x_2 = 0 \Rightarrow x_5 = 0 \Rightarrow x_3 = 1 \quad (x_4 = 0/1)$

## Другие NP-полные задачи

- Задача коммивояжёра
- Задача о сумме подмножеств
- Задача о ранце
- Задача о раскраске графа

# Задача коммивояжера

- Поиск «самого дешёвого» пути через ВСЕ вершины на графе
- Решение?

# Задача коммивояжера

- Поиск «самого дешёвого» пути через ВСЕ вершины на графе
- Решение?
  
- А) Перебор
- Б) Сокращённый перебор
- В) Эвристические методы

# Задача о сумме подмножеств

- Есть множество из целых чисел
- Найти в нём подмножество с нулевой суммой
- Решение?

# Задача о сумме подмножеств

- Есть множество из целых чисел
- Найти в нём подмножество с нулевой суммой
- Решение?
  
- А) Перебор всех вариантов

# Задача о сумме подмножеств

- Есть множество из  $N$  целых чисел
- Найти в нём подмножество с нулевой суммой
- Решение?
  
- А) Перебор всех вариантов
- Б) Динамическое программирование
  - Введём  $Q(K, S) = \text{TRUE}$ , если и только если существует подмножество первых  $K$  чисел, дающих в сумме  $S$
  - $S$  ограничено снизу суммой отрицательных чисел и сверху суммой положительных



# Задача о сумме подмножеств

- ▶ Есть множество  $X$  из  $N$  целых чисел
- ▶ Найти в нём подмножество с нулевой суммой
- ▶ Решение?
  
- ▶ А) Перебор всех вариантов
- ▶ Б) Динамическое программирование
  - ▶ Введём  $Q(K, S) = \text{TRUE}$ , если и только если существует подмножество первых  $K$  чисел, дающих в сумме  $S$
  - ▶  $S$  ограничено снизу суммой отрицательных чисел и сверху суммой положительных
  - ▶  $Q(1, S) = (X_1 == S)$
  - ▶  $Q(K, S) = Q(K - 1, S) \text{ OR } (X_K == S) \text{ OR } Q(K - 1, S - X_K)$

# Задача о раскраске графа

- Необходимо раскрасить все вершины графа таким образом, чтобы все соседние вершины были разного цвета
- Хроматическое число = Минимальное количество цветов, для которых задача разрешима

# Задачи с недоказанной NP-полнотой

- Факторизация целых чисел (разложение на простые множители)

# P versus NP

- Фундаментальная проблема: совпадают ли классы задач P и NP?

# P versus NP

- Фундаментальная проблема: совпадают ли классы задач P и NP?
- Если НЕТ, то класс NPC не пересекается с классом P, то есть, NP-полные задачи нельзя решить за полиномиальное время

# P versus NP

- Фундаментальная проблема: совпадают ли классы задач P и NP?
- Если НЕТ, то класс NPC не пересекается с классом P, то есть, NP-полные задачи нельзя решить за полиномиальное время
- Если ДА, то  $P = NP = NPC$ , то есть, NP-полные задачи можно решить за полиномиальное время

# P versus NP

- ▶ Большинство учёных сейчас склоняется к мнению, что  $P \neq NP$

# P versus NP

- Большинство учёных сейчас склоняется к мнению, что  $P \neq NP$
- Предположим, тем не менее оказалось, что  $P = NP$  – какими будут последствия?



# P versus NP

- ▶ Большинство учёных сейчас склоняется к мнению, что  $P \neq NP$
- ▶ Предположим, тем не менее оказалось, что  $P = NP$  – какими будут последствия?
  - ▶ Есть приложения, предполагающие  $P \neq NP$ , и они «сломаются»

# P versus NP

- ▶ Большинство учёных сейчас склоняется к мнению, что  $P \neq NP$
- ▶ Предположим, тем не менее оказалось, что  $P = NP$  – какими будут последствия?
  - ▶ Есть приложения, предполагающие  $P \neq NP$ , и они «сломаются»
    - ▶ А) Криптосистемы с открытым ключом

Спасибо за внимание!