

# Алгоритмы и модели вычислений.

## Задание 5: сложность вычислений: классы P, NP, co-NP II

Сергей Володин, 272 гр.

задано 2014.03.13

### Задача 1

1. Докажем, что  $\text{НАМРАТН} \leq_m^p \text{УНАМРАТН}$ .

$\text{НАМРАТН} = \{(G, s, t) \mid G \text{ — ориентированный граф, в } G \text{ существует гамильтонов путь из } s \text{ в } t\}$ ,

$\text{УНАМРАТН} = \{(G, s, t) \mid G \text{ — неориентированный граф, в } G \text{ существует гамильтонов путь из } s \text{ в } t\}$ .

Пусть  $G$  — ориентированный граф,  $s$  и  $t$  — его вершины.  $x = (G, s, t)$ . Определим  $f(x) = (G', s', t')$ . Для каждой вершины  $v \in V(G)$ , кроме  $s$  и  $t$ , добавим в  $V(G')$  три вершины  $v_i, v_m, v_o$ . Для  $s$  и  $t$  добавим  $s_o$  и  $t_i$ . Соединим  $v_i \leftrightarrow v_m$  и  $v_m \leftrightarrow v_o$  (стрелкой  $\leftrightarrow$  обозначено неориентированное ребро). Для каждого  $(u, v) \in E(G)$  добавим  $(u_o, v_i) \in E(G')$ .  $G'$  — получившийся граф,  $s' = s_o, t' = t_i$ .

- (а) Пусть  $x = (G, s, t) \in \text{НАМРАТН}$ . Тогда существует путь  $s \rightarrow v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_n \rightarrow t$ . По построению, тогда существует путь  $s_o \leftrightarrow v_{1i} \leftrightarrow v_{1m} \leftrightarrow v_{1o} \leftrightarrow \dots \leftrightarrow v_{ni} \leftrightarrow v_{nm} \leftrightarrow v_{no} \leftrightarrow t_i$ , который является гамильтоновым путем в  $G'$  (все вершины по построению: для каждой вершины исходного графа, кроме  $s$  и  $t$  добавляются 3 в образе, все они посещены.  $s_o$  и  $t_i$  также посещены. Если есть повтор  $v_{i.} = v_{j.}$ , то (структура пути в образе) есть повтор  $v_{im} = v_{jm}$ . Значит, есть повтор в исходном пути — противоречие), поэтому  $f(x) \in \text{УНАМРАТН}$

- (б) Пусть  $f(x) = (G', s_o, t_i) \in \text{УНАМРАТН}$ . Из вершины с индексом  $_o$  по построению есть ребра только в вершины с индексом  $_i$ . Из вершины  $v_i$  есть ребро только в  $v_m$ , из вершины  $v_m$  — только в  $v_o$ . Поэтому гамильтонов путь имеет вид  $s_o \leftrightarrow v_{1i} \leftrightarrow v_{1m} \leftrightarrow v_{1o} \leftrightarrow \dots \leftrightarrow v_{ni} \leftrightarrow v_{nm} \leftrightarrow v_{no} \leftrightarrow t_i$ , значит, в исходном графе  $G$  есть путь  $s \rightarrow v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_n \rightarrow t$ , и он гамильтонов (аналогично: все вершины по построению, повтор означает повтор в другом пути — противоречие), поэтому  $x \in \text{НАМРАТН}$

- (с)  $f$  — вычислима за полиномиальное время (линейное по количеству ребер и вершин время)

2. Поскольку  $\text{НАМРАТН} \in \text{NP-с}$ ,  $\text{НАМРАТН} \leq \text{УНАМРАТН}$ ,  $\text{УНАМРАТН} \in \text{NP}$ , то (см. решение 4-го задания, вспомогательные утверждения, 2)  $\text{УНАМРАТН} \in \text{NP-с}$  ■

### Задача 2

См. (каноническое) 21

## Задача 3

Получилось доказать не совсем то, что нужно

1.  $\mathcal{C} \supset \text{NP} \cup \text{co-NP}$ .

- (а) Пусть  $L \in \text{NP}$ . Тогда (семинар)  $L \leq_m^p \text{SAT} \Leftrightarrow \exists f: \Sigma^* \rightarrow \Sigma^*: \forall x(x \in L \Leftrightarrow f(x) \in \text{SAT})$ ,  $f$  — вычислима за полиномиальное время. Определим  $M_{\text{SAT}}$ : вычисляем за полиномиальное время (определение сводимости)  $f(x)$  ( $x$  — вход), спрашиваем оракула  $f(x) \stackrel{?}{\in} \text{SAT}$  за  $O(1)$ . Ответ — ответ оракула (корректно из определения сводимости). Время работы полиномиально:  $T(|x|) = \text{poly}(|x|) + O(1) = \text{poly}(|x|)$ .
- (б) Пусть  $L \in \text{co-NP}$ . Тогда  $\bar{L} \leq_m^p \text{SAT} \Leftrightarrow \exists f: \Sigma^* \rightarrow \Sigma^*: \forall x(x \in \bar{L} \Leftrightarrow f(x) \in \text{SAT}) \Leftrightarrow \forall x(x \in L \Leftrightarrow f(x) \notin \text{SAT})$ ,  $f$  — вычислима за полиномиальное время. Определим  $M_{\text{SAT}}$ : вычисляем за полиномиальное время (определение сводимости)  $f(x)$  ( $x$  — вход), спрашиваем оракула  $f(x) \stackrel{?}{\in} \text{SAT}$  за  $O(1)$ . Ответ — противоположный ответу оракула (корректно из определения сводимости). Время работы полиномиально:  $T(|x|) = \text{poly}(|x|) + O(1) = \text{poly}(|x|)$ .

2. (Идея обсуждалась с Дарьей Решетовой). Пусть  $L \in \mathcal{C}$ . Тогда существует МТ  $M_{\text{SAT}}$ , вычисляющая  $x \stackrel{?}{\in} L$  за полиномиальное время, и делающая не более одного обращения к оракулу  $t \stackrel{?}{\in} \text{SAT}$ . Рассмотрим машину  $M_{\text{SAT}}$ . Она может обращаться к оракулу, либо не обращаться. Если она обращается к оракулу на входе  $x$ , обозначим  $n(x) = 1$ , иначе  $n(x) = 0$ . В первом случае до обращения к оракулу  $Or(x)$  она вычисляет вход  $f(x)$  для него. После обращения (получения  $f(x) \stackrel{?}{\in} L$ , 0 либо 1), машина выдает ответ (0 либо 1). Если ответ тот же, что и ответ оракула, обозначим  $s(x) = 0$ , иначе  $s(x) = 1$ . В случае, если  $M_{\text{SAT}}$  не обращается к оракулу, она выдает ответ, вычисляя  $a(x) \in \{0, 1\}$ . Поэтому  $M_{\text{SAT}}$  можно представить следующим псевдокодом:

```

1  M(x)
2  {
3    if (n(x)) return (Or(f(x)) ^ s(x));
4    else return (a(x));
5  }
```

Поскольку  $M_{\text{SAT}}$  полиномиальна,  $n(\cdot)$ ,  $s(\cdot)$ ,  $a(\cdot)$  вычислимы за полиномиальное время (в случаях, где они не используются, можно считать их значения, скажем,  $= 0$ ).

Обозначим

- (а)  $L_a = \{x | n(x) = 0 \wedge a(x) = 1\}$ ,
- (б)  $L_0 = \{x | n(x) = 1 \wedge s(x) = 0 \wedge Or(f(x)) = 1\}$ ,
- (с)  $L_1 = \{x | n(x) = 1 \wedge s(x) = 1 \wedge Or(f(x)) = 0\}$ .

Тогда  $L = L_a \cup L_0 \cup L_1$  (все случаи в псевдокоде выше).

- (а) Получаем, что  $L_a \in P$  (так как  $a(\cdot)$  и  $n(\cdot)$  вычислимы за полиномиальное время).
- (б) Докажем, что  $L_0 \in \text{NP}$ .  $Or(f(x)) = 1 \Leftrightarrow f(x) \in \text{SAT}$ . Поскольку  $\text{SAT} \in \text{NP}$ , то  $\forall t(t \in \text{SAT} \Leftrightarrow \exists y: R_{\text{SAT}}(t, y) = 1)$ ,  $R_{\text{SAT}}$  — вычислима за полиномиальное время,  $|y| = \text{poly}(|x|)$ . Определим  $R(x, y) = n(x) \wedge \neg s(x) \wedge R_{\text{SAT}}(f(x), y)$  — вычислима за полиномиальное время.
- i. Пусть  $x \in L_0$ . Тогда  $n(x) = 1$ ,  $s(x) = 0$ , и  $f(x) \in \text{SAT} \Rightarrow \exists y: R_{\text{SAT}}(f(x), y) = 1$ . Получаем  $x \in L_0 \Rightarrow \exists y: R(x, y) = 1$ .
- ii. Пусть  $x \notin L_0$ . Тогда, либо  $n(x) = 0$ , и тогда для всех  $y \hookrightarrow R(x, y) = 0$ , аналогично в случае  $s(x) = 1$ :  $\forall y \hookrightarrow R(x, y) = 0$ . Если  $n(x) = 1$  и  $s(x) = 0$ , то  $f(x) \notin \text{SAT}$ , и для всех  $y \hookrightarrow R_{\text{SAT}}(f(x), y) = 0$ , откуда  $\forall y \hookrightarrow R(x, y) = 0$ .

Итак,  $\forall x(x \in L_0 \Leftrightarrow \exists y: R(x, y) = 1)$  ■

- (с) Докажем, что  $L_1 \in \text{co-NP}$ . Определим  $R(x, y) = \neg n(x) \vee \neg s(x) \vee R_{\text{SAT}}(f(x), y)$  — вычислима за полиномиальное время.

- i. Пусть  $x \in L_1 \Leftrightarrow x \notin \bar{L}_1$ . Тогда  $n(x) = 1 \Rightarrow \neg n(x) = 0$ ,  $s(x) = 1 \Rightarrow \neg s(x) = 0$ , и  $f(x) \notin \text{SAT}$ , откуда  $\forall y \hookrightarrow R_{\text{SAT}}(f(x), y) = 0$ . Получаем  $x \notin \bar{L}_1 \Rightarrow \forall y \hookrightarrow R(x, y) = 0 \vee 0 \vee 0 = 0$ .
- ii. Пусть  $x \notin L_1 \Leftrightarrow x \in \bar{L}_1$ . Тогда, либо  $n(x) = 0$ , и тогда для всех  $y \hookrightarrow R(x, y) = 1$ , аналогично в случае  $s(x) = 0$ :  $\forall y \hookrightarrow R(x, y) = 1$ . Если  $n(x) = 1$  и  $s(x) = 1$ , то  $f(x) \in \text{SAT}$ , и  $\exists y: R_{\text{SAT}}(f(x), y) = 1$ , откуда  $\exists y: R(x, y) = 1$ .

Итак,  $\forall x(x \in \bar{L}_1 \Leftrightarrow \exists y: R(x, y) = 1)$  ■

Получаем, что  $L = \underbrace{L_a}_{\in P} \cup \underbrace{L_0}_{\in \text{NP}} \cup \underbrace{L_1}_{\in \text{co-NP}}$ .

Поскольку  $L_a \cup L_0 \in \text{NP}$  (сертификат для слов из  $L_0$  тот же, в предикат добавляется «или ( $y = \varepsilon$  и  $x \in L_a$ )» — вычислимо за полиномиальное время), для краткости запишем  $L = L_0 \cup L_1$ , где  $L_0 \in \text{NP}$ ,  $L_1 \in \text{co-NP}$ .

Итак,  $\text{NP} \cup \text{co-NP} \subset \mathcal{C} \subset \{L | L = L_0 \cup L_1 : L_0 \in \text{NP}, L_1 \in \text{co-NP}\}$

## (каноническое) Задача 21

ГЦ =  $\{G \text{ — ориентированный граф} \mid \text{в } G \text{ существует гамильтонов цикл}\}$ .

ГП =  $\{(G, s, t) \text{ — ориентированный граф, две его вершины} \mid \text{в } G \text{ существует гамильтонов путь из } s \text{ в } t\}$ .

1. Докажем, что  $\text{ГП} \leq_m^p \text{ГЦ}$ . Пусть  $x = (G, s, t)$  — граф и две его вершины. Определим граф  $f(x)$ : возьмем  $G$ , удалим все ребра между  $s$  и  $t$ , все ребра в  $s$ , все ребра из  $t$ . Добавим одно  $t \rightarrow s$ .

- (a) Пусть  $x \in \text{ГП}$ , то есть, в  $G$  есть гамильтонов путь из  $s$  в  $t$ . Тогда в этом пути нет ребер из  $t$  в  $s$  (иначе через  $t$  или  $s$  путь пройдет дважды). Значит, путь будет гамильтоновым и в  $f(x)$ . Но в  $f(x)$  есть ребро  $t \rightarrow s$ , получаем гамильтонов цикл, составленный из пути и одного ребра. Значит,  $f(x) \in \text{ГЦ}$
- (b) Пусть  $f(x) \in \text{ГЦ}$ , то есть, в  $f(x)$  есть гамильтонов цикл. В этот цикл входят вершины  $s$  и  $t$ , так как в него входят все вершины графа. Но из  $t$  нет других ребер, кроме как в  $s$  (по построению), значит, в цикл входит ребро  $t \rightarrow s$ . Рассмотрим весь путь без этого ребра. Он гамильтонов, так как является гамильтоновым циклом без одного ребра. Этот путь будет также путем в  $G$ , так как не содержит ребра  $t \rightarrow s$ , а в  $G$  ребер больше (кроме  $t \rightarrow s$ ). Также этот путь будет гамильтоновым, так как множества вершин  $G$  и  $f(x)$  совпадают. Значит,  $x \in \text{ГП}$
- (c) Сводимость  $f$  в явном виде.  $A[i][j]$  — матрица графа  $G$ ,  $B[i][j]$  — матрица графа  $f(x)$ .  $A[i][j] = 1 \Leftrightarrow$  есть ребро из  $i$ -й вершины в  $j$ -ю.  $|V(G)| = n$ . Считаем, что  $s$  и  $t$  — индексы вершин  $s$  и  $t$ . Алгоритм:

---

```
1  for(i = 0; i < n; i++)
2      for(j = 0; j < n; j++)
3          B[i][j] = A[i][j]; // copying graph f(x) := G
4
5  for(i = 0; i < n; i++)
6  {
7      B[i][s] = 0; // removing edges to s
8      B[t][i] = 0; // removing edges from t
9  }
10
11 B[t][s] = 1; // adding edge from t to s
```

---

Получаем, что  $f$  — вычислима за полиномиальное время:  $T(G) = O(n^2) + O(n) + O(1) = O(n^2)$ . Длина записи графа  $l(G) = \Omega(n^2)$  (элементы матрицы  $n \times n$ ), поэтому  $T(G) = O(l(G))$ , т.е. время вычисления  $f$  линейно по длине входа.

2. (Идея обсуждалась с Игорем Силиным). Докажем, что  $\text{ГЦ} \leq_m^p \text{ГП}$ . Пусть  $x = G$  — граф. Фиксируем некоторую его вершину  $v$ . «Разделим» ее на две вершины  $s$  и  $t$ , из  $s$  добавим все ребра из  $v$ , в  $t$  направим все ребра в  $v$ . Удалим ребра между  $s$  и  $t$ . Получим граф  $G'$ . Определим  $f(x) = (G', s, t)$ .

- (a) Пусть  $x \in \text{ГЦ}$ . Тогда в  $x = G$  существует гамильтонов цикл. Он содержит все вершины, в том числе и вершину  $v$ :  $v \rightarrow v_1 \rightarrow \dots \rightarrow v_n \rightarrow v$ . Тогда в графе  $G'$  образа  $f(x)$  будет путь  $s \rightarrow v_1 \rightarrow \dots \rightarrow v_n \rightarrow t$ , и он будет гамильтоновым (все вершины по построению, вершины  $v_i$  не повторяются, т.к. исходный цикл гамильтонов, если  $t$  или  $s$  повторяется, то  $v$  встречается более 2-х раз в цикле — противоречие), т.е.  $f(x) \in \text{ГП}$
- (b) Пусть  $f(x) \in \text{ГП}$ . Тогда существует гамильтонов путь  $s \rightarrow \dots \rightarrow t$ . Значит, в  $G$  есть цикл  $v \rightarrow \dots \rightarrow v$ , и он гамильтонов (в  $\dots$  все вершины, кроме  $s$  и  $t$  для образа, значит, там все вершины, кроме  $v$  для исходного графа). Получаем  $x \in \text{ГЦ}$ .
- (c) Сводимость  $f$  в явном виде.  $A[i][j]$  — матрица графа  $x = G$ ,  $B[i][j]$  — матрица графа из  $f(x)$ .  $|V(G)| = n$ . Алгоритм:

---

```
1  v = n - 1; // any vertex of G
2  s = v;
3  t = v + 1; // new vertex
4
5  for(i = 0; i < n + 1; i++)
6      for(j = 0; j < n + 1; j++)
7          B[i][j] = 0;
8
9  for(i = 0; i < n; i++)
10 {
11     if(A[v][i] == 1)
12         B[s][i] = 1; // (v, i) in E <=> (s, i) in E'
13     if(A[i][v] == 1)
14         B[i][t] = 1; // (i, v) in E <=> (i, t) in E'
15 }
16
17 for(i = 0; i < n - 1; i++)
18     for(j = 0; j < n - 1; j++)
19         B[i][j] = A[i][j]; // copying rest of the graph
20
21 B[t][s] = 0; // (t, s) not in E'
22 B[s][t] = 0; // (s, t) not in E'
```

---

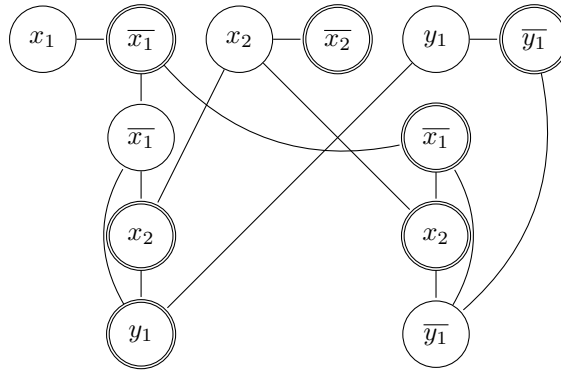
Получаем, что  $f$  — вычислима за полиномиальное время:  $T(G) = O(n^2) + O(n) + O(1) = O(n^2)$ , аналогично  $T(G) = O(l(G))$ .

(каноническое) **Задача 23**

1.  $\Psi(x_1, x_2) \stackrel{\text{def}}{=} (\neg x_1 \vee x_2)$ . Базовое множество ( $n = 2$ )  $\{x_1, x_2, \neg x_1, \neg x_2\}$ .  
Семейство подмножеств  $A_\Psi = \{\{x_1, \neg x_1\}, \{x_2, \neg x_2\}, \{\neg x_1, x_2\}\}$ .  
 $\nexists A \stackrel{\text{def}}{=} \{x_1, x_2\}$ . Получаем  $A \cap \{x_1, \neg x_1\} \ni x_1$ ,  $A \cap \{x_2, \neg x_2\} \ni x_2$ ,  $A \cap \{\neg x_1, x_2\} \ni x_2$ .  
Значит,  $A$  — протыкающее множество для  $A_\Psi$ , и  $|A| = 2$ .
2.  $\chi(x_1, x_2, x_3) \stackrel{\text{def}}{=} (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge \neg x_3$ . Семейство подмножеств ( $n = 3$ )  $A_\chi = \{\{x_1, \neg x_1\}, \{x_2, \neg x_2\}, \{x_3, \neg x_3\}, \{x_1, x_2, x_3\}, \{\neg x_1, \neg x_2\}, \{x_1, \neg x_2\}, \{\neg x_1, x_2, x_3\}, \{\neg x_3\}\}$ . Пусть  $A$  — протыкающее множество. Тогда  $A \cap \{\neg x_3\} \neq \emptyset \Rightarrow A \ni \neg x_3$ . Также  $A \cap \{x_1, \neg x_1\} \neq \emptyset$ , поэтому  $A$  содержит  $x_1$  или  $\neg x_1$ . Аналогично  $x_2 \in A$  или  $\neg x_2 \in A$ . Получаем, что  $A$  содержит не менее трех элементов. Предположим, что их ровно 3. Рассмотрим все возможные 4 случая (или×или раньше по тексту):
  - (a)  $A = \{x_1, x_2, \neg x_3\}$ . Тогда  $A \cap \{\neg x_1, \neg x_2\} = \emptyset$  — противоречие.
  - (b)  $A = \{x_1, \neg x_2, \neg x_3\}$ . Тогда  $A \cap \{\neg x_1, x_2, x_3\} = \emptyset$  — противоречие.
  - (c)  $A = \{\neg x_1, x_2, \neg x_3\}$ . Тогда  $A \cap \{x_1, \neg x_2\} = \emptyset$  — противоречие.
  - (d)  $A = \{\neg x_1, \neg x_2, \neg x_3\}$ . Тогда  $A \cap \{x_1, x_2, x_3\} = \emptyset$  — противоречие.

Получаем, что  $A$  содержит более трех элементов ■

3. Ровно-3-КНФ:  $\Psi' = (\overline{x_1} \vee x_2 \vee y_1) \wedge (\overline{x_1} \vee x_2 \vee \overline{y_1})$ . Если  $\Psi = \overline{x_1} \vee x_2 = 1$ , то  $\Psi' = 1$ , если  $\Psi = 0$ , то  $\Psi' = y_1 \wedge \overline{y_1} = 0$ . Граф:



$n_{\text{new}} + 2m_{\text{new}} = 3 + 2 \times 2 = 7$ . Кружками выбрано 7-вершинное покрытие.

4.  $\varphi' = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee y_1) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{y_1}) \wedge (x_1 \vee \overline{x_2} \vee y_2) \wedge (x_1 \vee \overline{x_2} \vee \overline{y_2}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_3} \vee y_3 \vee y_4) \wedge (\overline{x_3} \vee y_3 \vee \overline{y_4}) \wedge (\overline{x_3} \vee \overline{y_3} \vee y_4) \wedge (\overline{x_3} \vee \overline{y_3} \vee \overline{y_4})$ .  $n_{\text{new}} = 7$ ,  $m_{\text{new}} = 10 \Rightarrow n_{\text{new}} + 2m_{\text{new}} = 7 + 2 \times 10 = 27$  (не дописано).